DISCRETE STRUCTURES

Laurie Lacey
SUNY Schenectady County Community College

LibreTexts™

Discrete Structures, Fifth Version

Remixed from

"Mathematical Reasoning - Writing and Proof" (Sundstrom)

"Applied Discrete Structures" (Doerr, Levasseur)

"Discrete Mathematics" (Levin)

A note from Laurie Lacey, PhD: It is my hope that I have managed to construct this remix so as to cover the topics in the SUNY Transfer Pathway description of Discrete Math.

This text is disseminated via the Open Education Resource (OER) LibreTexts Project (https://LibreTexts.org) and like the hundreds of other texts available within this powerful platform, it is freely available for reading, printing and "consuming." Most, but not all, pages in the library have licenses that may allow individuals to make changes, save, and print this book. Carefully consult the applicable license(s) before pursuing such effects.

Instructors can adopt existing LibreTexts texts or Remix them to quickly build course-specific resources to meet the needs of their students. Unlike traditional textbooks, LibreTexts' web based origins allow powerful integration of advanced features and new technologies to support learning.

The LibreTexts mission is to unite students, faculty and scholars in a cooperative effort to develop an easy-to-use online platform for the construction, customization, and dissemination of OER content to reduce the burdens of unreasonable textbook costs to our students and society. The LibreTexts project is a multi-institutional collaborative venture to develop the next generation of open-access texts to improve postsecondary education at all levels of higher learning by developing an Open Access Resource environment. The project currently consists of 14 independently operating and interconnected libraries that are constantly being optimized by students, faculty, and outside experts to supplant conventional paper-based books. These free textbook alternatives are organized within a central environment that is both vertically (from advance to basic level) and horizontally (across different fields) integrated.

The LibreTexts libraries are Powered by NICE CXOne and are supported by the Department of Education Open Textbook Pilot Project, the UC Davis Office of the Provost, the UC Davis Library, the California State University Affordable Learning Solutions Program, and Merlot. This material is based upon work supported by the National Science Foundation under Grant No. 1246120, 1525057, and 1413739.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the US Department of Education.

Have questions or comments? For information about adoptions or adaptions contact info@LibreTexts.org. More information on our activities can be found via Facebook (https://facebook.com/Libretexts), Twitter (https://twitter.com/libretexts), or our blog (http://Blog.Libretexts.org).

This text was compiled on 02/04/2024

TABLE OF CONTENTS

5: Set Theory

6: Functions

7: Equivalence Relations

8: Topics in Number Theory

9: Finite and Infinite Sets

10: Graph Theory

Detailed Licensing

Info Page

This text is disseminated via the Open Education Resource (OER) LibreTexts Project (https://LibreTexts.org) and like the hundreds of other texts available within this powerful platform, it freely available for reading, printing and "consuming." Most, but not all, pages in the library have licenses that may allow individuals to make changes, save, and print this book. Carefully consult the applicable license(s) before pursuing such effects.

Instructors can adopt existing LibreTexts texts or Remix them to quickly build course-specific resources to meet the needs of their students. Unlike traditional textbooks, LibreTexts' web based origins allow powerful integration of advanced features and new technologies to support learning.

The LibreTexts mission is to unite students, faculty and scholars in a cooperative effort to develop an easy-to-use online platform for the construction, customization, and dissemination of OER content to reduce the burdens of unreasonable textbook costs to our students and society. The LibreTexts project is a multi-institutional collaborative venture to develop the next generation of open-access texts to improve postsecondary education at all levels of higher learning by developing an Open Access Resource environment. The project currently consists of 13 independently operating and interconnected libraries that are constantly being optimized by students, faculty, and outside experts to supplant conventional paper-based books. These free textbook alternatives are organized within a central environment that is both vertically (from advance to basic level) and horizontally (across different fields) integrated.

The LibreTexts libraries are Powered by MindTouch® and are supported by the Department of Education Open Textbook Pilot Project, the UC Davis Office of the Provost, the UC Davis Library, the California State University Affordable Learning Solutions Program, and Merlot. This material is based upon work supported by the National Science Foundation under Grant No. 1246120, 1525057, and 1413739.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the US Department of Education.

Have questions or comments? For information about adoptions or adaptions contact info@LibreTexts.org. More information on our activities can be found via Facebook (https://facebook.com/Libretexts), Twitter (https://twitter.com/libretexts), or our blog (http://Blog.Libretexts.org).

Licensing

*A detailed breakdown of this resource's licensing can be found in **Back Matter/Detailed Licensing**.*

CHAPTER OVERVIEW

1: Introduction to Writing Proofs in Mathematics

1.1: Statements and Conditional Statements

Much of our work in mathematics deals with statements. In mathematics, a **statement** is a declarative sentence that is either true or false but not both. A statement is sometimes called a **proposition**. The key is that there must be no ambiguity. To be a statement, a sentence must be true or false, and it cannot be both. So a sentence such as "The sky is beautiful" is not a statement since whether the sentence is true or not is a matter of opinion. A question such as "Is it raining?" is not a statement because it is a question and is not declaring or asserting that something is true.

Some sentences that are mathematical in nature often are not statements because we may not know precisely what a variable represents. For example, the equation $2x$+5 = 10 is not a statement since we do not know what x represents. If we substitute a specific value for x (such as x = 3), then the resulting equation, 2·3 +5 = 10 is a statement (which is a false statement). Following are some more examples:

Example:

- There exists a real number x such that $2x$+5 = 10.
  This is a statement because either such a real number exists or such a real number does not exist. In this case, this is a true statement since such a real number does exist, namely x = 2.5.
- For each real number x, $2x+5=2\left(x+\frac{5}{2}\right)$.
  This is a statement since either the sentence $2x+5=2\left(x+\frac{5}{2}\right)$ is true when any real number is substituted for x (in which case, the statement is true) or there is at least one real number that can be substituted for x and produce a false statement (in which case, the statement is false). In this case, the given statement is true.
- Solve the equation $x^2-7x+10=0$.
  This is not a statement since it is a directive. It does not assert that something is true.
- $(a+b)^2=a^2+b^2$ is not a statement since it is not known what a and b represent. However, the sentence, “There exist real numbers a and b such that $(a+b)^2=a^2+b^2$ " is a statement. In fact, this is a true statement since there are such integers. For example, if $a=1$ and $b=0$, then $(a+b)^2=a^2+b^2$.
- Compare the statement in the previous item to the statement, “For all real numbers a and b, $(a+b)^2=a^2+b^2$." This is a false statement since there are values for a and b for which $(a+b)^2\neq a^2+b^2$. For example, if $a=2$ and $b=3$, then $(a+b)^2=5^2=25$ and $a^2+b^2=2^2+3^2=13$.

Progress Check 1.1: Statements

Which of the following sentences are statements? Do not worry about determining whether a statement is true or false; just determine whether each sentence is a statement or not.

1. 3 + 4 = 8.
2. 2·7 + 8 = 22.
3. $(x-1)=\sqrt{(x+11)}$.
4. $2x+5y=7$.
5. There are integers x and y such that $2x+5y=7$.
6. There are integers x and y such that $23x+27y=52$.
7. Given a line L and a point P not on that line, there is a unique line through P that does not intersect L.
8. $(a+b)^3=a^3+3a^2b+3ab^2+b^3$.
9. $(a+b)^3=a^3+3a^2b+3ab^2+b^3$ for all real numbers a and b.
10. The derivative of $f(x)=\sin x$ is $f'(x)=\cos x$.
11. Does the equation $3x^2-5x-7=0$ have two real number solutions?
12. If ABC is a right triangle with right angle at vertex B, and if D is the midpoint of the hypotenuse, then the line segment connecting vertex B to D is half the length of the hypotenuse.
13. There do not exist three integers x, y, and z such that $x^3+y^2=z^3$.

Answer

Add texts here. Do not delete this text first.

How Do We Decide If a Statement Is True or False?

In mathematics, we often establish that a statement is true by writing a mathematical proof. To establish that a statement is false, we often find a so-called counterexample. (These ideas will be explored later in this chapter.) So mathematicians must be able to discover and construct proofs. In addition, once the discovery has been made, the mathematician must be able to communicate this discovery to others who speak the language of mathematics. We will be dealing with these ideas throughout the text.

For now, we want to focus on what happens before we start a proof. One thing that mathematicians often do is to make a conjecture beforehand as to whether the statement is true or false. This is often done through exploration. The role of exploration in mathematics is often difficult because the goal is not to find a specific answer but simply to investigate. Following are some techniques of exploration that might be helpful.

Techniques of Exploration

- **Guesswork and conjectures**. Formulate and write down questions and conjectures. When we make a guess in mathematics, we usually call it a conjecture.
- **Examples. Constructing appropriate examples is extremely important**. Exploration often requires looking at lots of examples. In this way, we can gather information that provides evidence that a statement is true, or we might find an example that shows the statement is false. This type of example is called a **counterexample**.

  ✔ Example:

  For example, if someone makes the conjecture that $\sin(2x) = 2\sin(x)$, for all real numbers x, we can test this conjecture by substituting specific values for x. One way to do this is to choose values of x for which $\sin(x)$is known. Using $x = \frac{\pi}{4}$, we see that

  $$\sin(2(\tfrac{\pi}{4})) = \sin(\tfrac{\pi}{2}) = 1, \text{ and}$$
  $$2\sin(\tfrac{\pi}{4}) = 2(\tfrac{\sqrt{2}}{2}) = \sqrt{2}\,.$$

  Since $1 \neq \sqrt{2}$, these calculations show that this conjecture is false. However, if we do not find a counterexample for a conjecture, we usually cannot claim the conjecture is true. The best we can say is that our examples indicate the conjecture is true. As an example, consider the conjecture that

  If x and y are odd integers, then $x + y$ is an even integer.

  We can do lots of calculation, such as $3 + 7 = 10$ and $5 + 11 = 16$, and find that every time we add two odd integers, the sum is an even integer. However, it is not possible to test every pair of odd integers, and so we can only say that the conjecture appears to be true. (We will prove that this statement is true in the next section.)

- **Use of prior knowledge.** This also is very important. We cannot start from square one every time we explore a statement. We must make use of our acquired mathematical knowledge. For the conjecture that $\sin(2x) = 2\sin(x)$, for all real numbers x, we might recall that there are trigonometric identities called "double angle identities." We may even remember the correct identity for $\sin(2x)$, but if we do not, we can always look it up. We should recall (or find) that

  for all real numbers x,

  $$\sin(2x) = 2\sin(x)\cos(x). \tag{1.1.1}$$

- We could use this identity to argue that the conjecture "for all real numbers x, $\sin(2x) = 2\sin(x)$" is false, but if we do, it is still a good idea to give a specific counterexample as we did before.
- **Cooperation and brainstorming**. Working together is often more fruitful than working alone. When we work with someone else, we can compare notes and articulate our ideas. Thinking out loud is often a useful brainstorming method that helps generate new ideas.

? Progress Check 1.2: Explorations

Use the techniques of exploration to investigate each of the following statements. Can you make a conjecture as to whether the statement is true or false? Can you determine whether it is true or false?

1. $(a+b)^2 = a^2 + b^2$, for all real numbers a and b.
2. There are integers x and y such that $2x + 5y = 41$.
3. If x is an even integer, then x^2 is an even integer.
4. If x and y are odd integers, then $x \cdot y$ is an odd integer.

Answer

Add texts here. Do not delete this text first.

Conditional Statements

One of the most frequently used types of statements in mathematics is the so-called conditional statement. Given statements P and Q, a statement of the form "If P then Q" is called a **conditional statement**. It seems reasonable that the truth value (true or false) of the conditional statement "If P then Q" depends on the truth values of P and Q. The statement "If P then Q" means that Q must be true whenever P is true. The statement P is called the **hypothesis** of the conditional statement, and the statement Q is called the **conclusion** of the conditional statement. Since conditional statements are probably the most important type of statement in mathematics, we give a more formal definition.

Definition

A **conditional statement** is a statement that can be written in the form "If P then Q," where P and Q are sentences. For this conditional statement, P is called the **hypothesis** and Q is called the **conclusion**.

Intuitively, "If P then Q" means that Q must be true whenever P is true. Because conditional statements are used so often, a symbolic shorthand notation is used to represent the conditional statement "If P then Q." We will use the notation $P \to Q$ to represent "If P then Q." When P and Q are statements, it seems reasonable that the truth value (true or false) of the conditional statement $P \to Q$ depends on the truth values of P and Q. There are four cases to consider:

- P is true and Q is true.
- P is false and Q is true.
- P is true and Q is false.
- P is false and Q is false.

The conditional statement $P \to Q$ means that Q is true whenever P is true. It says nothing about the truth value of Q when P is false. Using this as a guide, we define the conditional statement $P \to Q$ to be false only when P is true and Q is false, that is, only when the hypothesis is true and the conclusion is false. In all other cases, $P \to Q$ is true. This is summarized in Table **1.1**, which is called a **truth table** for the conditional statement $P \to Q$. (In Table **1.1**, T stands for "true" and F stands for "false.")

P	Q	$P \to Q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 1.1: Truth Table for $P \to Q$

The important thing to remember is that the conditional statement $P \to Q$ has its own truth value. It is either true or false (and not both). Its truth value depends on the truth values for P and Q, but some find it a bit puzzling that the conditional statement is considered to be true when the hypothesis P is false. We will provide a justification for this through the use of an example.

Example 1.3:

Suppose that I say

"If it is not raining, then Daisy is riding her bike."

We can represent this conditional statement as $P \to Q$ where P is the statement, "It is not raining" and Q is the statement, "Daisy is riding her bike."

Although it is not a perfect analogy, think of the statement $P \to Q$ as being false to mean that I lied and think of the statement $P \to Q$ as being true to mean that I did not lie. We will now check the truth value of $P \to Q$ based on the truth values of P and Q.

1. Suppose that both P and Q are true. That is, it is not raining and Daisy is riding her bike. In this case, it seems reasonable to say that I told the truth and that$P \to Q$ is true.
2. Suppose that P is true and Q is false or that it is not raining and Daisy is not riding her bike. It would appear that by making the statement, "If it is not raining, then Daisy is riding her bike," that I have not told the truth. So in this case, the statement $P \to Q$ is false.
3. Now suppose that P is false and Q is true or that it is raining and Daisy is riding her bike. Did I make a false statement by stating that if it is not raining, then Daisy is riding her bike? The key is that I did not make any statement about what would happen if it was raining, and so I did not tell a lie. So we consider the conditional statement, "If it is not raining, then Daisy is riding her bike," to be true in the case where it is raining and Daisy is riding her bike.
4. Finally, suppose that both P and Q are false. That is, it is raining and Daisy is not riding her bike. As in the previous situation, since my statement was $P \to Q$, I made no claim about what would happen if it was raining, and so I did not tell a lie. So the statement $P \to Q$ cannot be false in this case and so we consider it to be true.

Progress Check 1.4: xplorations with Conditional Statements

1. Consider the following sentence:

If x is a positive real number, then $x^2 + 8x$ is a positive real number.

Although the hypothesis and conclusion of this conditional sentence are not statements, the conditional sentence itself can be considered to be a statement as long as we know what possible numbers may be used for the variable x. From the context of this sentence, it seems that we can substitute any positive real number for x. We can also substitute 0 for x or a negative real number for x provided that we are willing to work with a false hypothesis in the conditional statement. (In Chapter **2**, we will learn how to be more careful and precise with these types of conditional statements.)

(a) Notice that if $x = -3$, then $x^2 + 8x = -15$, which is negative. Does this mean that the given conditional statement is false?

(b) Notice that if $x = 4$, then $x^2 + 8x = 48$, which is positive. Does this mean that the given conditional statement is true?

(c) Do you think this conditional statement is true or false? Record the results for at least five different examples where the hypothesis of this conditional statement is true.

2. "If n is a positive integer, then $n^2 - n + 41$ is a prime number." (Remember that a prime number is a positive integer greater than 1 whose only positive factors are 1 and itself.)
To explore whether or not this statement is true, try using (and recording your results) for $n = 1$, $n = 2$, $n = 3$, $n = 4$, $n = 5$, and $n = 10$. Then record the results for at least four other values of n. Does this conditional statement appear to be true?

Answer

Add texts here. Do not delete this text first.

Further Remarks about Conditional Statements

1. The conventions for the truth value of conditional statements may seem a bit strange,especially the fact that the conditional statement is true when the hypothesis of the conditional statement is false. The following example is meant to show that this makes sense.

Suppose that Ed has exactly \$52 in his wallet. The following four statements will use the four possible truth combinations for the hypothesis and conclusion of a conditional statement.

- If Ed has exactly \$52 in his wallet, then he has \$20 in his wallet. This is a true statement. Notice that both the hypothesis and the conclusion are true.
- If Ed has exactly \$52 in his wallet, then he has \$100 in his wallet. This statement is false. Notice that the hypothesis is true and the conclusion is false.
- If Ed has \$100 in his wallet, then he has at least \$50 in his wallet. This statement is true regardless of how much money he has in his wallet. In this case, the hypothesis is false and the conclusion is true.
- If Ed has \$100 in his wallet, then he has at least \$80 in his wallet. This statement is true regardless of how much money he has in his wallet. In this case, the hypothesis is false and the conclusion is false.

  This is admittedly a contrived example but it does illustrate that the conventions for the truth value of a conditional statement make sense. The message is that in order to be complete in mathematics, we need to have conventions about when a conditional statement is true and when it is false.

2. The fact that there is only one case when a conditional statement is false often provides a method to show that a given conditional statement is false. In Progress Check **1.4**, you were asked if you thought the following conditional statement was true or false.

   If n is a positive integer, then $(n^2 - n + 41)$ is a prime number.

   Perhaps for all of the values you tried for n, $(n^2 - n + 41)$ turned out to be a prime number. However, if we try $n = 41$, we ge

   $n^2 - n + 41 = 41^2 - 41 + 41$
   $n^2 - n + 41 = 41^2$

   So in the case where $n = 41$, the hypothesis is true (41 is a positive integer) and the conclusion is false 41^2 is not prime. Therefore, 41 is a counterexample for this conjecture and the conditional statement
   "If n is a positive integer, then $(n^2 - n + 41)$ is a prime number"
   is false. There are other counterexamples (such as $n = 42$, $n = 45$, and $n = 50$), but only one counterexample is needed to prove that the statement is false.

3. Although one example can be used to prove that a conditional statement is false, in most cases, we cannot use examples to prove that a conditional statement is true. For example, in Progress Check **1.4**, we substituted values for x for the conditional statement "If x is a positive real number, then $x^2 + 8x$ is a positive real number." For every positive real number used for x, we saw that $x^2 + 8x$ was positive. However, this does not prove the conditional statement to be true because it is impossible to substitute every positive real number for x. So, although we may believe this statement is true, to be able to conclude it is true, we need to write a mathematical proof. Methods of proof will be discussed in Section **1.2** and Chapter **3**.

? Progress Check 1.5: Working with a Conditional Statement

The following statement is a true statement, which is proven in many calculus texts.

If the function f is differentiable at a, then the function f is continuous at a.

Using only this true statement, is it possible to make a conclusion about the function in each of the following cases?

1. It is known that the function f, where $f(x) = \sin x$, is differentiable at 0.
2. It is known that the function f, where $f(x) = \sqrt[3]{x}$, is not differentiable at 0.
3. It is known that the function f, where $f(x) = |x|$, is continuous at 0.
4. It is known that the function f, where $f(x) = \dfrac{|x|}{x}$ is not continuous at 0.

Answer

Add texts here. Do not delete this text first.

Closure Properties of Number Systems

The primary number system used in algebra and calculus is the **real number system**. We usually use the symbol R to stand for the set of all real numbers. The real numbers consist of the rational numbers and the irrational numbers. The **rational numbers** are those real numbers that can be written as a quotient of two integers (with a nonzero denominator), and the **irrational numbers** are those real numbers that cannot be written as a quotient of two integers. That is, a rational number can be written in the form of a fraction, and an irrational number cannot be written in the form of a fraction. Some common irrational numbers are $\sqrt{2}$, π and e. We usually use the symbol $\mathbb{Q}$ to represent the set of all rational numbers. (The letter $\mathbb{Q}$ is used because rational numbers are quotients of integers.) There is no standard symbol for the set of all irrational numbers.

Perhaps the most basic number system used in mathematics is the set of **natural numbers**. The natural numbers consist of the positive whole numbers such as 1, 2, 3, 107, and 203. We will use the symbol $\mathbb{N}$ to stand for the set of natural numbers. Another basic number system that we will be working with is the set of **integers**. The integers consist of zero, the positive whole numbers, and the negatives of the positive whole numbers. If n is an integer, we can write $n = \frac{n}{1}$. So each integer is a rational number and hence also a real number.

We will use the letter $\mathbb{Z}$ to stand for the set of integers. (The letter $\mathbb{Z}$ is from the German word, $Zahlen$, for numbers.) Three of the basic properties of the integers are that the set $\mathbb{Z}$ is **closed under addition**, the set $\mathbb{Z}$ is **closed under multiplication**, and the set of integers is **closed under subtraction.** This means that

- If x and y are integers, then $x + y$ is an integer;
- If x and y are integers, then $x \cdot y$ is an integer; and
- If x and y are integers, then $x - y$ is an integer.

Notice that these so-called closure properties are defined in terms of conditional statements. This means that if we can find one instance where the hypothesis is true and the conclusion is false, then the conditional statement is false.

✔ Example 1.6: Closure

1. In order for the set of natural numbers to be closed under subtraction, the following conditional statement would have to be true: If x and y are natural numbers, then $x - y$ is a natural number. However, since 5 and 8 are natural numbers, $5 - 8 = -3$, which is not a natural number, this conditional statement is false. Therefore, the set of natural numbers is not closed under subtraction.
2. We can use the rules for multiplying fractions and the closure rules for the integers to show that the rational numbers are closed under multiplication. If $\frac{a}{b}$ and $\frac{c}{d}$ are rational numbers (so a, b, c, and d are integers and b and d are not zero), then

   $$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

   Since the integers are closed under multiplication, we know that ac and bd are integers and since $b \neq 0$ and $d \neq 0$, $bd \neq 0$. Hence, $\frac{ac}{bd}$ is a rational number and this shows that the rational numbers are closed under multiplication.

? Progress Check 1.7: Closure Properties

Answer each of the following questions.

1. Is the set of rational numbers closed under addition? Explain.
2. Is the set of integers closed under division? Explain.
3. Is the set of rational numbers closed under subtraction? Explain.

Answer

Add texts here. Do not delete this text first.

? 1.1

1. Which of the following sentences are statements?
   (a) $3^2 + 4^2 = 5^2$.
   (b) $a^2 + b^2 = c^2$.
   (c) There exists integers a, b, and c such that $a^2 + b^2 = c^2$.
   (d) If $x^2 = 4$, then $x = 2$.
   (e) For each real number x, if $x^2 = 4$, then $x = 2$.
   (f) For each real number t, $\sin^2 t + \cos^2 t = 1$.
   (g) $\sin x < \sin(\frac{\pi}{4})$.
   (h) If n is a prime number, then n^2 has three positive factors.
   (i) $1 + \tan^2 \theta = \sec^2 \theta$.
   (j) Every rectangle is a parallelogram.
   (k) Every even natural number greater than or equal to 4 is the sum of two prime numbers.
2. Identify the hypothesis and the conclusion for each of the following conditional statements.
   (a) If n is a prime number, then n^2 has three positive factors.
   (b) If a is an irrational number and b is an irrational number, then $a \cdot b$ is an irrational number.
   (c) If p is a prime number, then $p = 2$ or p is an odd number.
   (d) If p is a prime number and $p \neq 2$ or p is an odd number.
   (e) $p \neq 2$ or p is a even number, then p is not prime.
3. Determine whether each of the following conditional statements is true or false.
   (a) If 10 < 7, then 3 = 4.
   (b) If 7 < 10, then 3 = 4.
   (c) If 10 < 7, then 3 + 5 = 8.
   (d) If 7 < 10, then 3 + 5 = 8.
4. Determine the conditions under which each of the following conditional sentences will be a true statement.
   (a) If a + 2 = 5, then 8 < 5.
   (b) If 5 < 8, then a + 2 = 5.
5. Let P be the statement "Student X passed every assignment in Calculus I," and let Q be the statement "Student X received a grade of C or better in Calculus I."
   (a) What does it mean for P to be true? What does it mean for Q to be true?
   (b) Suppose that Student X passed every assignment in Calculus I and received a grade of B-, and that the instructor made the statement $P \to Q$. Would you say that the instructor lied or told the truth?
   (c) Suppose that Student X passed every assignment in Calculus I and received a grade of C-, and that the instructor made the statement $P \to Q$. Would you say that the instructor lied or told the truth?
   (d) Now suppose that Student X did not pass two assignments in Calculus I and received a grade of D, and that the instructor made the statement $P \to Q$. Would you say that the instructor lied or told the truth?
   (e) How are Parts (**5b**), (**5c**), and (**5d**) related to the truth table for $P \to Q$?
6. Following is a statement of a theorem which can be proven using calculus or precalculus mathematics. For this theorem, a, b, and c are real numbers.

   Theorem If f is a quadratic function of the form
   $f(x) = ax^2 + bx + c$ and a < 0, then the function f has a maximum value when $x = \dfrac{-b}{2a}$.

   Using **only** this theorem, what can be concluded about the functions given by the following formulas?
   (a) $g(x) = -8x^2 + 5x - 2$
   (b) $h(x) = -\dfrac{1}{3}x^2 + 3x$
   (c) $k(x) = 8x^2 - 5x - 7$
   (d) $j(x) = -\dfrac{71}{99}x^2 + 210$
   (e) $f(x) = -4x^2 - 3x + 7$
   (f) $F(x) = -x^4 + x^3 + 9$

7. Following is a statement of a theorem which can be proven using the quadratic formula. For this theorem, a, b, and c are real numbers.

   Theorem If f is a quadratic function of the form $f(x) = ax^2 + bx + c$ and ac < 0, then the function f has two x-intercepts.

   Using **only** this theorem, what can be concluded about the functions given by the following formulas?
   (a) $g(x) = -8x^2 + 5x - 2$
   (b) $h(x) = -\frac{1}{3}x^2 + 3x$
   (c) $k(x) = 8x^2 - 5x - 7$
   (d) $j(x) = -\frac{71}{99}x^2 + 210$
   (e) $f(x) = -4x^2 - 3x + 7$
   (f) $F(x) = -x^4 + x^3 + 9$

8. Following is a statement of a theorem about certain cubic equations.For this theorem, b represents a real number.

   Theorem A. If f is a cubic function of the form $f(x) = x^3 - x + b$ and b > 1, then the function f has exactly one x-intercept.

   Following is another theorem about x-intercepts of functions:

   Theorem B. If f and g are functions with $g(x) = k \cdot f(x)$, where k is a nonzero real number, then f and g have exactly the same x-intercepts.

   Using only these two theorems and some simple algebraic manipulations, what can be concluded about the functions given by the following formulas?
   (a) $f(x) = x^3 - x + 7$
   (b) $g(x) = x^3 + x + 7$
   (c) $h(x) = -x^3 + x - 5$
   (d) $k(x) = 2x^3 + 2x + 3$
   (e) $r(x) = x^4 - x + 11$
   (f) $F(x) = 2x^3 - 2x + 7$

9. **(a)** Is the set of natural numbers closed under division?
   (b) Is the set of rational numbers closed under division?
   (c) Is the set of nonzero rational numbers closed under division?
   (d) Is the set of positive rational numbers closed under division?
   (e) Is the set of positive real numbers closed under subtraction?
   (f) Is the set of negative rational numbers closed under division?
   (g) Is the set of negative integers closed under addition?

Explorations and Activities

10. **Exploring Propositions**. In Progress Check **1.2**, we used exploration to show that certain statements were false and to make conjectures that certain statements were true. We can also use exploration to formulate a conjecture that we believe to be true. For example, if we calculate successive powers of 2, $(2^1, 2^2, 2^3, 2^4, 2^5, \ldots)$ and examine the units digits of these numbers, we could make the following conjectures (among others):
    • If n is a natural number, then the units digit of 2^n must be 2, 4, 6, or 8.
    • The units digits of the successive powers of 2 repeat according to the pattern "2, 4, 8, 6."
    (a) Is it possible to formulate a conjecture about the units digits of successive powers of $4 (4^1, 4^2, 4^3, 4^4, 4^5, \ldots)$? If so, formulate at least one conjecture.
    (b) Is it possible to formulate a conjecture about the units digit of numbers of the form $7^n - 2^n$, where n is a natural number? If so, formulate a conjecture in the form of a conditional statement in the form "If n is a natural number, then ... ."
    (c) Let $f(x) = e^(2x)$. Determine the first eight derivatives of this function. What do you observe? Formulate a conjecture that appears to be true. The conjecture should be written as a conditional statement in the form, "If n is a natural number, then ... ."

Answer

Add texts here. Do not delete this text first.

1.2: Constructing Direct Proofs

Preview Activity 1 (Definition of Even and Odd Integers)

Definitions play a very important role in mathematics. A direct proof of a proposition in mathematics is often a demonstration that the proposition follows logically from certain definitions and previously proven propositions. A **definition** is an agreement that a particular word or phrase will stand for some object, property, or other concept that we expect to refer to often. In many elementary proofs, the answer to the question, "How do we prove a certain proposition?", is often answered by means of a definition. For example, in Progress Check **1.2** on page **5**, all of the examples you tried should have indicated that the following conditional statement is true:

If x and y are odd integers, then $x \cdot y$ is an odd integer.

In order to construct a mathematical proof of this conditional statement, we need a precise definition what it means to say that an integer is an even integer and what it means to say that an integer is an odd integer.

Definition

An integer a is an **even integer** provided that there exists an integer n such that $a = 2n$. An integer a is an **odd integer** provided there exists an integer n such that $a = 2n + 1$.

Using this definition, we can conclude that the integer 16 is an even integer since 16 = 2 · 8 and 8 is an integer. By answering the following questions, you should obtain a better understanding of these definitions. These questions are not here just to have questions in the textbook. Constructing and answering such questions is a way in which many mathematicians will try to gain a better understanding of a definition.

1. Use the definition given above to
   (a) Explain why 28, -42, 24, and 0 are even integers.
   (b) Explain why 51, -11, 1, and -1 are odd integers.

   It is important to realize that mathematical definitions are not made randomly. In most cases, they are motivated by a mathematical concept that occurs frequently.
2. Are the definitions of even integers and odd integers consistent with your previous ideas about even and odd integers?

Preview Activity 2 (Thinking about a Proof)

Consider the following proposition:

Proposition. If x and y are odd integers, then $x \cdot y$ is an odd integer.

Think about how you might go about proving this proposition. A **direct proof** of a conditional statement is a demonstration that the conclusion of the conditional statement follows logically from the hypothesis of the conditional statement. Definitions and previously proven propositions are used to justify each step in the proof. To help get started in proving this proposition, answer the following questions:

1. The proposition is a conditional statement. What is the hypothesis of this conditional statement? What is the conclusion of this conditional statement?
2. If $x = 2$ and $y = 3$, then $x \cdot y = 6$. Does this example prove that the proposition is false? Explain.
3. If $x = 5$ and $y = 3$, then $x \cdot y = 15$. Does this example prove that the proposition is true? Explain.

   In order to prove this proposition, we need to prove that whenever both x and y are odd integers, $x \cdot y$ is an odd integer. Since we cannot explore all possible pairs of integer values for x and y, we will use the definition of an odd integer to help us construct a proof.
4. To start a proof of this proposition,we will assume that the hypothesis of the conditional statement is true. So in this case, we assume that both x and yare odd integers. We can then use the definition of an odd integer to conclude that there exists an integer m such that $x = 2m + 1$. Now use the definition of an odd integer to make a conclusion about the integer y.

   Note: The definition of an odd integer says that a certain other integer exists. This definition may be applied to both x and y. However, do not use the same letter in both cases. To do so would imply that $x = y$ and we have not made that assumption. To

be more specific, if $x = 2m + 1$ and $y = 2m + 1$, then $x = y$.

5. We need to prove that if the hypothesis is true, then the conclusion is true. So, in this case, we need to prove that $x \cdot y$ is an odd integer. At this point, we usually ask ourselves a so-called **backward question**. In this case, we ask, "Under what conditions can we conclude that $x \cdot y$ is an odd integer?" Use the definition of an odd integer to answer this question, and be careful to use a different letter for the new integer than was used in Part (**4**).

Properties of Number Systems

At the end of Section **1.1**, we introduced notations for the standard number systems we use in mathematics. We also discussed some closure properties of the standard number systems. For this text, it is assumed that the reader is familiar with these closure properties and the basic rules of algebra that apply to all real numbers. That is, it is assumed the reader is familiar with the properties of the real numbers shown in Table **1.2**.

Constructing a Proof of a Conditional Statement

In order to prove that a conditional statement $P \to Q$ is true, we only need to prove that Q is true whenever P is true. This is because the conditional statement is true whenever the hypothesis is false. So in a direct proof of $P \to Q$, we assume that P is true, and using this assumption, we proceed through a logical sequence of steps to arrive at the conclusion that Q is true.

Unfortunately, it is often not easy to discover how to start this logical sequence of steps or how to get to the conclusion that Q is true. We will describe a method of exploration that often can help in discovering the steps of a proof. This method

For all real numbers x, y and z

Identity Properties	$x + 0 = x$ and $x \cdot 1 = x$
Inverse Properties	$x + (-x) = 0$ and if $x \neq 0$, then $x \cdot \frac{1}{x} = 1$.
Commutative Properties	$x + y = y + x$ and $xy = yx$
Associative Properties	$(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$
Distributive Properties	$x(y + z) = xy + xz$ and $(y + z)x = yx + zx$

Table 1.2: Properties of the Real Numbers

will involve working forward from the hypothesis, P, and backward from the conclusion, Q. We will use a device called the "**know-show table**" to help organize our thoughts and the steps of the proof. This will be illustrated with the proposition from Preview Activity **2**.

Proposition. If x and y are odd integers, then $x \cdot y$ is an odd integer.
The first step is to identify the hypothesis, P, and the conclusion,Q, of the conditional statement. In this case, we have the following:

P : x and y are odd integers. Q: $x \cdot y$ is an odd integer.

We now treat P as what we know (we have assumed it to be true) and treat Q as what we want to show (that is, the goal). So we organize this by using P as the first step in the know portion of the table and Q as the last step in the show portion of the table. We will put the know portion of the table at the top and the show portion of the table at the bottom.

Step	**Know**	**Reason**
P	x and y are odd integers	Hypothesis
$P1$	...	...
...	...	...
$Q1$	...	...
Q	$x \cdot y$ is an odd integer.	?
Step	**Show**	**Reason**

We have not yet filled in the reason for the last step because we do not yet know how we will reach the goal. The idea now is to ask ourselves questions about what we know and what we are trying to prove. We usually start with the conclusion that we are trying to prove by asking a so-called **backward question**. The basic form of the question is, "Under what conditions can we conclude that Q is true?" How we ask the question is crucial since we must be able to answer it. We should first try to ask and answer the question in an abstract manner and then apply it to the particular form of statement Q.

In this case, we are trying to prove that some integer is an odd integer. So our backward question could be, "How do we prove that an integer is odd?" At this time, the only way we have of answering this question is to use the definition of an odd integer. So our answer could be, "We need to prove that there exists an integer q such that the integer equals $2q+1$." We apply this answer to statement Q and insert it as the next to last line in the know-show table.

Step	**Know**	**Reason**
P	x and y are odd integers	Hypothesis
$P1$	...	...
...	...	...
$Q1$	There exists an integer q such that $xy = 2q+1$	...
Q	$x \cdot y$ is an odd integer.	Definition of an odd integer
Step	**Show**	**Reason**

We now focus our effort on proving statement $Q1$ since we know that if we can prove $Q1$, then we can conclude that Q is true. We ask a backward question about $Q1$ such as, "How can we prove that there exists an integer q such that $x \cdot y = 2q+1$?" We may not have a ready answer for this question, and so we look at the know portion of the table and try to connect the know portion to the show portion. To do this, we work forward from step P, and this involves asking a **forward question**. The basic form of this type of question is, "What can we conclude from the fact that P is true?" In this case, we can use the definition of an odd integer to conclude that there exist integers m and n such that $x = 2m+1$ and $y = 2n+1$. We will call this Step $P1$ in the know-show table. It is important to notice that we were careful not to use the letter q to denote these integers. If we had used q again, we would be claiming that the same integer that gives $x \cdot y = 2q+1$ also gives $x = 2q+1$. This is why we used m and n for the integers x and y since there is no guarantee that x equals y. The basic rule of thumb is to use a different symbol for each new object we introduce in a proof. So at this point, we have:

- Step $P1$. We know that there exist integers m and n such that $x = 2m+1$ and $y = 2n+1$.
- Step $Q1$. We need to prove that there exists an integer q such that $x \cdot y = 2q+1$.

We must always be looking for a way to link the "know part" to the "show part". There are conclusions we can make from $P1$, but as we proceed, we must always keep in mind the form of statement in $Q1$. The next forward question is, "What can we conclude about $x \cdot y$from what we know?" One way to answer this is to use our prior knowledge of algebra. That is, we can first use substitution to write $x \cdot y = (2m+1)(2n+1)$. Although this equation does not prove that $x \cdot y$ is odd, we can use algebra to try to rewrite the right side of this equation. $(2m+1)(2n+1)$ in the form of an odd integer so that we can arrive at step $Q1$. We first expand the right side of the equation to obtain

$$x \cdot y = (2m+1)(2n+1) = 4mn+2m+2n+1$$

Now compare the right side of the last equation to the right side of the equation in step $Q1$. Sometimes the difficult part at this point is the realization that q stands for some integer and that we only have to show that $x \cdot y$ equals two times some integer plus one. Can we now make that conclusion? The answer is yes because we can factor a 2 from the first three terms on the right side of the equation and obtain

$$x \cdot y = 4mn+2m+2n+1 = 2(2mn+m+n)+1$$

We can now complete the table showing the outline of the proof as follows:

Step	**Know**	**Reason**
P	x and y are odd integers	Hypothesis

$P1$	There exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$.	Definition of an odd integer.
$P2$	$xy = (2m + 1)(2n + 1)$	Substitution
$P3$	$xy = 4mn + 2m + 2n + 1$	Algebra
$P4$	$xy = 2(2mn + m + n) + 1$	Algebra
$P5$	$(2mn + m + n)$ is an integer	Closure properties of the integers
$Q1$	There exists an integer q such that $xy = 2q + 1$	Use $q = (2mn + m + n)$
Q	$x \cdot y$ is an odd integer.	Definition of an odd integer

It is very important to realize that we have only constructed an outline of a proof. Mathematical proofs are not written in table form. They are written in narrative form using complete sentences and correct paragraph structure, and they follow certain conventions used in writing mathematics. In addition, most proofs are written only from the forward perspective. That is, although the use of the backward process was essential in discovering the proof, when we write the proof in narrative form, we use the forward process described in the preceding table. A completed proof follows.

Theorem

If x and y are odd integers, then $x \cdot y$ is an odd integer.

Proof

We assume that x and y are odd integers and will prove that $x \cdot y$ is an odd integer. Since x and y are odd, there exist integers m and n such that

$$x = 2m + 1 \text{ and } y = 2n + 1 .$$

Using algebra, we obtain

$$x \cdot y = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$$

Since m and n are integers and the integers are closed under addition and multiplication, we conclude that $2mn + m + n$ is an integer. This means that $x \cdot y$ has been written in the form $2q + 1$ for some integer q, and hence, $x \cdot y$ is an odd integer. Consequently, it has been proven that if x and y are odd integers, then $x \cdot y$ is an odd integer.

Writing Guidelines for Mathematics Proofs

At the risk of oversimplification, doing mathematics can be considered to have two distinct stages. The first stage is to convince yourself that you have solved the problem or proved a conjecture. This stage is a creative one and is quite often how mathematics is actually done. The second equally important stage is to convince other people that you have solved the problem or proved the conjecture. This second stage often has little in common with the first stage in the sense that it does not really communicate the process by which you solved the problem or proved the conjecture. However, it is an important part of the process of communicating mathematical results to a wider audience.

A **mathematical proof** is a convincing argument (within the accepted standards of the mathematical community) that a certain mathematical statement is necessarily true. A proof generally uses deductive reasoning and logic but also contains some amount of ordinary language (such as English). A mathematical proof that you write should convince an appropriate audience that the result you are proving is in fact true. So we do not consider a proof complete until there is a well-written proof. So it is important to introduce some writing guidelines. The preceding proof was written according to the following basic guidelines for writing proofs. More writing guidelines will be given in Chapter 3.

1. **Begin with a carefully worded statement of the theorem or result to be proven.** This should be a simple declarative statement of the theorem or result. Do not simply rewrite the problem as stated in the textbook or given on a handout. Problems often begin with phrases such as “Show that” or “Prove that.” This should be reworded as a simple declarative statement of the theorem. Then skip a line and write “Proof” in italics or boldface font (when using a word processor). Begin the proof on the same line. Make sure that all paragraphs can be easily identified. Skipping a line between paragraphs or indenting each

paragraph can accomplish this.

As an example, an exercise in a text might read, “Prove that if x is an odd integer, then x^2 is an odd integer.” This could be started as follows:

Theorem

If x is an odd integer, then x^2 is an odd integer.

Proof

We assume that x is an odd integer ...

2. **Begin the proof with a statement of your assumptions.** Follow the statement of your assumptions with a statement of what you will prove.

Theorem 1.2.1

If x is an odd integer, then x^2 is an odd integer.

Proof

We assume that x is an odd integer and will prove that x^2 is an odd integer.

3. **Usethepronoun“we.”** If a pronoun is used in a proof, the usual convention is to use “we” instead of “I.” The idea is to stress that you and the reader are doing the mathematics together. It will help encourage the reader to continue working through the mathematics. Notice that we started the proof of Theorem **1.8** with “We assume that... .”
4. **Use italics for variables when using a word processor.** When using a word processor to write mathematics, the word processor needs to be capable of producing the appropriate mathematical symbols and equations. The mathematics that is written with a word processor should look like typeset mathematics. This means that italics font is used for variables, boldface font is used for vectors, and regular font is used for mathematical terms such as the names of the trigonometric and logarithmic functions.

   For example, we do not write $sin\, x$ or $\mathbf{sin}\, x$. The proper way to typeset this is $\sin x$.

5. **Display important equations and mathematical expressions.** Equations and manipulations are often an integral part of mathematical exposition. Do not write equations, algebraic manipulations, or formulas in one column with reasons given in another column. Important equations and manipulations should be displayed. This means that they should be centered with blank lines before and after the equation or manipulations, and if the left side of the equations do not change, it should not be repeated. For example,

   Using algebra, we we obtain

   $$x \cdot y = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1$$

   Since m and n are integers, we conclude that ... .

6. Tell the reader when the proof has been completed. Perhaps the best way to do this is to simply write, “This completes the proof.” Although it may seem repetitive, a good alternative is to finish a proof with a sentence that states precisely what has been proven. In any case, it is usually good practice to use some “end of proof symbol” such as

? Progress Check 1.9 (Proving Propositions)

Construct a know-show table for each of the following propositions and then write a formal proof for one of the propositions.

1. If x is an even integer and y is an even integer, then $x+y$ is an even integer.
2. If x is an even integer and y is an odd integer, then $x+y$ is an odd integer.
3. If x is an even integer and y is an odd integer, then $x+y$ is an even integer.

Answer

Some Comments about Constructing Direct Proofs

1. When we constructed the know-show table prior to writing a proof for Theorem **1.8**, we had only one answer for the backward question and one answer for the forward question. Often, there can be more than one answer for these questions. For example, consider the following statement:

   If x is an odd integer, then x^2 is an odd integer.

   The backward question for this could be, "How do I prove that an integer is an odd integer?" One way to answer this is to use the definition of an odd integer, but another way is to use the result of Theorem **1.8**. That is, we can prove an integer is odd by proving that it is a product of two odd integers.

   The difficulty then is deciding which answer to use. Sometimes we can tell by carefully watching the interplay between the forward process and the backward process. Other times, we may have to work with more than one possible answer.

2. Sometimes we can use previously proven results to answer a forward question or a backward question. This was the case in the example given in Comment (**1**), where Theorem **1.8** was used to answer a backward question.
3. Although we start with two separate processes (forward and backward), the key to constructing a proof is to find a way to link these two processes. This can be difficult. One way to proceed is to use the know portion of the table to motivate answers to backward questions and to use the show portion of the table to motivate answers to forward questions.
4. Answering a backward question can sometimes be tricky. If the goal is the statement Q, we must construct the know-show table so that if we know that $Q1$ is true, then we can conclude that Q is true. It is sometimes easy to answer this in a way that if it is known that Q is true, then we can conclude that $Q1$ is true. For example, suppose the goal is to prove

   $$y^2 = 4,$$

   where y is a real number. A backward question could be, "How do we prove the square of a real number equals four?" One possible answer is to prove that the real number equals 2. Another way is to prove that the real number equals 2. This is an appropriate backward question, and these are appropriate answers.

   However, if the goal is to prove

   $$y = 2$$

   where y is a real number, we could ask, "How do we prove a real number equals 2?" It is not appropriate to answer this question with "prove that the square of the real number equals 4." This is because if $y^2 = 4$, then it is not necessarily true that $y = 2$.

5. Finally,it is very important to realize that not every proof can be constructed by the use of a simple know-show table. Proofs will get more complicated than the ones that are in this section. The main point of this section is not the know-show table itself, but the way of thinking about a proof that is indicated by a know-show table. In most proofs, it is very important to specify carefully what it is that is being assumed and what it is that we are trying to prove. The process of asking the "backward questions" and the "forward questions" is the important part of the know-show table. It is very important to get into the "habit of mind" of working backward from what it is we are trying to prove and working forward from what it is we are assuming. Instead of immediately trying to write a complete proof, we need to stop, think, and ask questions such as

- Just exactly what is it that I am trying to prove?
- How can I prove this?
- What methods do I have that may allow me to prove this?
- What are the assumptions?
- How can I use these assumptions to prove the result?

? Progress Check 1.10 (Exploring a Proposition)

Construct a table of values for $3m^2 + 4m + 6$ using at least six different integers for m. Make one-half of the values for m even integers and the other half odd integers. Is the following proposition true or false?

If m is an odd integer, then $3m^2 + 4m + 6$ is an odd integer.

Justify your conclusion. This means that if the proposition is true, then you should write a proof of the proposition. If the proposition is false, you need to provide an example of an odd integer for which $3m^2+4m+6$ is an even integer.

Answer

Add texts here. Do not delete this text first.

Progress Check 1.11 (Constructing and Writing a Proof)

The **Pythagorean Theorem** for right triangles states that if a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then $a^2+b^2=c^2$. For example, if $a=5$ and $b=12$ are the lengths of the two sides of a right triangle and if c is the length of the hypotenuse, then the $c^2=5^2+12^2$ and $c^2=169$. Since c is a length and must be positive, we conclude that $c=13$.

Construct and provide a well-written proof for the following proposition.

Proposition. If m is a real number and m, $m+1$, and $m+2$ are the lengths of the three sides of a right triangle, then $m=3$.

Although this proposition uses different mathematical concepts than the one used in this section, the process of constructing a proof for this proposition is the same forward-backward method that was used to construct a proof for Theorem **1.8**. However, the backward question, "How do we prove that $m=3$?" is simple but may be difficult to answer. The basic idea is to develop an equation from the forward process and show that $m=3$ is a solution of that equation.

Answer

Add texts here. Do not delete this text first.

Exercises for Section 1.2

1. Construct a know-show table for each of the following statements and then write a formal proof for one of the statements.

   (a) If m is an even integer,then $m+1$ is an odd integer.
   (b) If m is an odd integer, then $m+1$ is an even integer.
2. Construct a know-show table for each of the following statements and then write a formal proof for one of the statements.

   (a) If x is an even integer and y is an even integer, then $x+y$ is an even integer.
   (b) If x is an even integer and y is an odd integer, then $x+y$ is an odd integer.
   (c) If x is an odd integer and y is an odd integer, then $x+y$ is an even integer.
3. Construct a know-show table for each of the following statements and then write a formal proof for one of the statements.

   (a) If m is an even integer and n is an integer, then $m\cdot n$ is an even integer.
   (b) If n is an even integer, then n^2 is an even integer.
   (c) If n is an odd integer, then n^2 is an odd integer.
4. Construct a know-show table and write a complete proof for each of the following statements:

   (a) If m is an even integer, then $5m+7$ is an odd integer.
   (b) If m is an odd integer, then $5m+7$ is an even integer.
   (c) If m and n are odd integers, then $mn+7$ is an even integer.
5. Construct a know-show table and write a complete proof for each of the following statements:

   (a) If m is an even integer, then $3m^2+2m+3$ is an odd integer.
   (b) If m is an odd integer, then $3m^2+7m+12$ is an even integer.
6. In this section, it was noted that there is often more than one way to answer a backward question. For example, if the backward question is, "How can we prove that two real numbers are equal?", one possible answer is to prove that their difference equals 0. Another possible answer is to prove that the first is less than or equal to the second and that the second is less than or equal to the first

(a) Give at least one more answer to the backward question, “How can we prove that two real numbers are equal?”
(b) List as many answers as you can for the backward question, “How can we prove that a real number is equal to zero?”
(c) List as many answers as you can for the backward question, “How can we prove that two lines are parallel?”
(d) List as many answers as you can for the backward question, “How can we prove that a triangle is isosceles?”

7. Are the following statements true or false? Justify your conclusions.

   (a) If a, b and c are integers, then $ab+ac$ is an even integer.
   (b) If b and c are odd integers and a is an integer, then $ab+ac$ is an even integer.

8. Is the following statement true or false? Justify your conclusion.
   If a and b are nonnegative real numbers and $a+b=0$, then $a=0$.

   Either give a counterexample to show that it is false or outline a proof by completing a know-show table.

9. An integer a is said to be a **type 0 integer** if there exists an integer n such that $a=3n$. An integer a is said to be a **type 1 integer** if there exists an integer n such that $a=3n+1$. An integer a is said to be a **type 2 integer** if there exists an integer m such that $a=3m+2$.

   (a) Give examples of at least four different integers that are type 1 integers.
   (b) Give examples of at least four different integers that are type 2 integers.
   (c) By multiplying pairs of integers from the list in Exercise (9a), does it appear that the following statement is true or false?

   If a and b are both type 1 integers, then $a\cdot b$ is a type 1 integer.

10. Use the definitions in Exercise (9) to help write a proof for each of the following statements:

    (a) If a and b are both type 1 integers, then $a+b$ is a type 2 integer.
    (b) If a and b are both type 2 integers, then $a+b$ is a type 1 integer.
    (a) If a is a type 1 integer and b is a type 2 integer, then $a\cdot b$ is a type 2 integer.
    (a) If a and b are both type 2 integers, then $a\cdot b$ is type 1 integer.

11. Let a, b, and c be real numbers with $a\neq 0$. The solutions of the **quadratic equation** $ax^2+bx+c=0$ are given by the **quadratic formula**, which states that the solutions are $x1$ and $x2$, where

$$x_1=\frac{-b+\sqrt{(b^2-4ac)}}{2a} \text{ and } x_2=\frac{-b-\sqrt{(b^2-4ac)}}{2a}.$$

    (a) Prove that the sum of the two solutions of the quadratic equation $ax^2+bx+c=0$ is equal to $-\frac{b}{a}$.
    (b) Prove that the product of the two solutions of the quadratic equation $ax^2+bx+c=0$ is equal to $\frac{c}{a}$.

12. (a) See Exercise (**11**) for the quadratic formula, which gives the solutions to a quadratic equation. Let a, b, and c be real numbers with $a\neq 0$. The discriminant of the quadratic equation $ax^2+bx+c=0$ is defined to be b^2-4ac. Explain how to use this discriminant to determine if the quadratic equation has two real number solutions, one real number solution, or no real number solutions.
    (b) Prove that if a, b, and c are real numbers with $a>0$ and $c<0$, then one solutions of the quadratic equation $ax^2+bx+c=0$ is a positive real number.
    (c) Prove that if a, b, and c are real numbers with $a\neq 0$, $b>0$, and $b<2\sqrt{(ac)}$, then the quadratic equation $ax^2+bx+c=0$ has no real number solutions.

Explorations and Activities

13. **Pythagorean Triples**. Three natural numbers a, b, and c with $a<b<c$ are said to form a **Pythagorean triple** provided that $a^2+b^2=c^2$. For example, 3, 4, and 5 form a Pythagorean triple since $3^2+4^2=5^2$. The study of Pythagorean triples began with the development of the **Pythagorean Theorem** for right triangles, which states that if a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then $a^2+b^2=c^2$. For example, if the lengths of the legs of a right triangle are 4 and 7 units, then $c^2=4^2+7^2=63$, and the length of the hypotenuse must be $\sqrt{63}$ units (since the

length must be a positive real number). Notice that 4, 7, and $\sqrt{63}$ are not a Pythagorean triple since $\sqrt{63}$ is not a natural number.

(a) Verify that each of the following triples of natural numbers form a Pythagorean triple.

(1) 3, 4, and 5. (2) 8, 15, and 17. (3) 12, 35, and 37
(4) 6, 8, and 10. (5) 10, 24, and 26 (6) 14, 48, and 50

(b) Does there exist a Pythagorean triple of the form m, $m+7$, and $m+8$, where m is a natural number? If the answer is yes, determine all such Pythagorean triples. If the answer is no, prove that no such Pythagorean triple exists.

(c) Does there exist a Pythagorean triple of the form m, $m+11$,and $m+12$, where m is a natural number? If the answer is yes, determine all such Pythagorean triples. If the answer is no, prove that no such Pythagorean triple exists.

14. **More Work with Pythagorean Triples**. In Exercise (**13**), we verified that each of the following triples of natural numbers are Pythagorean triples:

(1) 3, 4, and 5. (2) 8, 15, and 17. (3) 12, 35, and 37
(4) 6, 8, and 10. (5) 10, 24, and 26 (6) 14, 48, and 50

(a) Focus on the least even natural number in each of these Pythagorean triples. Let n be this even number and find m so that $n=2m$. Now try to write formulas for the other two numbers in the Pythagorean triple in terms of m. For example, for 3, 4, and 5, $n=4$ and $m=2$, and for 8, 15, and 17, $n=8$ and $m=4$. Once you think you have formulas, test your results with $m=10$. That is, check to see that you have a Pythagorean triple whose smallest even number is 20.

(b) Write a proposition and then write a proof of the proposition. The proposition should be in the form: If m is a natural number and $m \geq 2$, then .....

Answer

Add texts here. Do not delete this text first.

1.S: Introduction to Writing Proofs in Mathematics (Summary)

Important Definitions

- Statement
- Odd integer
- Conditional statement
- Even integer
- Pythagorean triple

Important Number Systems and Their Properties

- The natural numbers, $\mathbb{N}$; the integers, $\mathbb{Z}$; the rational numbers, $\mathbb{Q}$; and the real number, $\mathbb{R}$.
- Closure Properties of the Number Systems

Number System	Closed Under
Natural numbers, $\mathbb{N}$	addition and multiplication
Integers, $\mathbb{Z}$	addition, subtraction, and multiplication
Rational numbers, $\mathbb{Q}$	addition, subtraction, and multiplication, and division by nonzero rational numbers
Real number, $\mathbb{R}$	addition, subtraction, and multiplication, and division by nonzero real numbers

- Inverse,commutative,associative, and distributive properties of the real numbers.

Important Theorems and Results

- **Exercise (1), Section 1.2**
  If m is an even integer, then $m+1$ is an odd integer.
  If m is an odd integer, then $m+1$ is an even integer.
- **Exercise (2), Section 1.2**
  If x is an even integer and y is an even integer, then $x+y$ is an even integer.
  If x is an even integer and y is an odd integer, then $x+y$ is an odd integer.
  If x is an odd integer and y is an odd integer, then $x+y$ is an even integer.
- **Exercise (3), Section 1.2.**
  If x is an even integer and y is an integer, then $x \cdot y$ is an even integer.
- **Theorem1.8**. If x is an odd integer and y is an odd integer, then $x \cdot y$ is an odd integer.
- The **Pythagorean Theorem**. If a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse, then $a^2+b^2=c^2$.

CHAPTER OVERVIEW

2: Logical Reasoning

Thumbnail: The "magic eight ball" is not an example of logical reasoning to get an answer to a problem. (CC BY 2.0 Generic; Atlasowa)

2.1: Statements and Logical Operators

PREVIEW ACTIVITY 2.1.1: Compound Statements

Mathematicians often develop ways to construct new mathematical objects from existing mathematical objects. It is possible to form new statements from existing statements by connecting the statements with words such as “and” and “or” or by negating the statement. A **logical operator** (or **connective**) on mathematical statements is a word or combination of words that combines one or more mathematical statements to make a new mathematical statement. A **compound statement** is a statement that contains one or more operators. Because some operators are used so frequently in logic and mathematics, we give them names and use special symbols to represent them.

- The conjunction of the statements P and Q is the statement “P **and** Q” and its denoted by $P \wedge Q$. The statement $P \wedge Q$ is true only when both P **and** Q are true.
- The **disjunction** of the statements P and Q is the statement “P **or** Q” and its denoted by $P \vee Q$. The statement $P \vee Q$ is true only when at least one of P or Q is true.
- The **negation** (**of a statement**) of the statement P is the statement “**not** P ” and is denoted by $\neg P$. The negation of P is true only when P is false, and $\neg P$ is false only when P is true.
- The **implication** or **conditional** is the statement “**If** P **then** Q” and is denoted by $P \rightarrow Q$. The statement $P \rightarrow Q$ is often read as “P **implies** Q, and we have seen in Section 1.1 that $P \rightarrow Q$ is false only when P is true and Q is false.

Some comments about the disjunction.
It is important to understand the use of the operator “or.” In mathematics, we use the “**inclusive or**” unless stated otherwise. This means that $P \vee Q$ is true when both P and Q are true and also when only one of them is true. That is, $P \vee Q$ is true when at least one of P or Q is true, or $P \vee Q$ is false only when both P and Q are false.

A different use of the word “or” is the “**exclusive or**.” For the exclusive or, the resulting statement is false when both statements are true. That is, “P exclusive or Q” is true only when exactly one of P or Q is true. In everyday life, we often use the exclusive or. When someone says, “At the intersection, turn left or go straight,” this person is using the exclusive or.

Some comments about the negation. Although the statement, $\neg P$, can be read as “It is not the case that P,” there are often betters ways to say or write this in English. For example, we would usually say (or write):

- The negation of the statement, “391 is prime” is “391 is not prime.”
- The negation of the statement, “$12 < 9$” is “$12 \geq 9$.”

1. For the statements

   P: 15 is odd Q: 15 is prime
   write each of the following statements as English sentences and determine

   whether they are true or false.
   (a) $P \wedge Q$. (b) $P \vee Q$. (c) $P \wedge \neg Q$. (d) $\neg P \vee \neg Q$.

2. For the statements

   P : 15 is odd R: 15 < 17

   write each of the following statements in symbolic form using the operators$\wedge$, $\vee$, and $\neg$

   (a) $15 \geq 17$. (b) 15 is odd or $15 \geq 17$.
   (c) 15 is even or 15 <17. (d) 15 is odd and $15 \geq 17$.

PREVIEW ACTIVITY2.1.2: Truth Values of Statements

We will use the following two statements for all of this Preview Activity:

- P is the statement “It is raining.”
- Q is the statement “Daisy is playing golf.”

In each of the following four parts, a truth value will be assigned to statements P and Q. For example, in Question (1), we will assume that each statement is true. In Question (2), we will assume that P is true and Q is false. In each part, determine the

truth value of each of the following statements:

(a) ($P \wedge Q$) It is raining and Daisy is playing golf.

(b) ($P \vee Q$) It is raining or Daisy is playing golf.

(c) ($P \rightarrow Q$) If it is raining, then Daisy is playing golf.

(d) ($\neg P$) It is not raining.

Which of the four statements [(a) through (d)] are true and which are false in each of the following four situations?

1. When P is true (it is raining) and Q is true (Daisy is playing golf).
2. When P is true (it is raining) and Q is false (Daisy is not playing golf).
3. When P is false (it is not raining) and Q is true (Daisy is playing golf).
4. When P is false (it is not raining) and Q is false (Daisy is not playing golf).

In the preview activities for this section, we learned about compound statements and their truth values. This information can be summarized with truth tables as is shown below.

P	$\neg P$
T	F
F	T

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Rather than memorizing the truth tables, for many people it is easier to remember the rules summarized in Table 2.1.

Table 2.1: Truth Values for Common Connectives

Operator	Symbolic Form	Summary of Truth Values
Conjunction	$P \wedge Q$	True only when both P and Q are true
Disjunction	$P \vee Q$	False only when both P and Q are false
Negation	$\neg P$	Opposite truth value of P
Conditional	$P \rightarrow Q$	False only when P is true and Q is false

Other Forms of Conditional Statements

Conditional statements are extremely important in mathematics because almost all mathematical theorems are (or can be) stated in the form of a conditional statement in the following form:

If “certain conditions are met,” then “something happens.”

It is imperative that all students studying mathematics thoroughly understand the meaning of a conditional statement and the truth table for a conditional statement.

We also need to be aware that in the English language, there are other ways for expressing the conditional statement $P \to Q$ other than “If P, then Q.” Following are some common ways to express the conditional statement $P \to Q$ in the English language:

- If P, then Q.
- P implies Q.
- P only if Q.
- Q if P.
- Whenever P is true, Q is true.
- Q is true whenever P is true.
- Q is necessary for P. (This means that if P is true, then Q is necessarily true.)
- P is sufficient for Q. (This means that if you want Q to be true, it is sufficient to show that P is true.)

In all of these cases, P is the **hypothesis** of the conditional statement and Q is the **conclusion** of the conditional statement.

? Progress Check 2.1: The "Only if" statemenT

Recall that a quadrilateral is a four-sided polygon. Let S represent the following true conditional statement:

If a quadrilateral is a square, then it is a rectangle.

Write this conditional statement in English using

1. the word “whenever”
2. the phrase “only if”
3. the phrase “is necessary for”
4. the phrase “is sufficient for”

Answer

Add texts here. Do not delete this text first.

Constructing Truth Tables

Truth tables for compound statements can be constructed by using the truth tables for the basic connectives. To illustrate this, we will construct a truth table for. $(P \wedge \neg Q) \to R$. The first step is to determine the number of rows needed.

- For a truth table with two different simple statements, four rows are needed since there are four different combinations of truth values for the two statements. We should be consistent with how we set up the rows. The way we will do it in this text is to label the rows for the first statement with (T, T, F, F) and the rows for the second statement with (T, F, T, F). All truth tables in the text have this scheme.
- For a truth table with three different simple statements, eight rows are needed since there are eight different combinations of truth values for the three statements. Our standard scheme for this type of truth table is shown in Table **2.2**.

The next step is to determine the columns to be used. One way to do this is to work backward from the form of the given statement. For $(P \wedge \neg Q) \to R$, the last step is to deal with the conditional operator $(\to)$. To do this, we need to know the truth values of $(P \wedge \neg Q)$ and R. To determine the truth values for $(P \wedge \neg Q)$, we need to apply the rules for the conjunction operator $(\wedge)$ and we need to know the truth values for P and $\neg Q$.

Table **2.2** is a completed truth table for $(P \wedge \neg Q) \to R$ with the step numbers indicated at the bottom of each column. The step numbers correspond to the order in which the columns were completed.

Table 2.2: Truth Table for $(P \wedge \neg Q) \rightarrow R$

P	Q	R	$\neg Q$	$(P \wedge \neg Q)$	$(P \wedge \neg Q) \rightarrow R$
T	T	T	F	F	T
T	T	F	F	F	T
T	F	T	T	T	T
T	F	F	T	T	F
F	T	T	F	F	T
F	T	F	F	F	T
F	F	T	T	F	T
F	F	F	T	F	T
1	1	1	2	3	4

- When completing the column for $P \wedge \neg Q$, remember that the only time the conjunction is true is when both P and $\neg Q$ are true.
- When completing the column for $(P \wedge \neg Q) \rightarrow R$, remember that the only time the conditional statement is false is when the hypothesis $(P \wedge \neg Q)$ is true and the conclusion, R, is false.

The last column entered is the truth table for the statement $(P \wedge \neg Q) \rightarrow R$ using the set up in the first three columns.

? Progress Check 2.2: Constructing Truth Tables

Construct a truth table for each of the following statements:

1. $P \wedge \neg Q$
2. $\neg (P \wedge Q)$
3. $\neg P \wedge \neg Q$
4. $\neg P \vee \neg Q$

Do any of these statements have the same truth table?

Answer

Add texts here. Do not delete this text first.

The Biconditional Statement

Some mathematical results are stated in the form "P if and only if Q" or "P is necessary and sufficient for Q." An example would be, "A triangle is equilateral if and only if its three interior angles are congruent." The symbolic form for the biconditional statement "P if and only if Q" is $P \leftrightarrow Q$. In order to determine a truth table for a biconditional statement, it is instructive to look carefully at the form of the phrase "P if and only if Q." The word "and" suggests that this statement is a conjunction. Actually it is a conjunction of the statements "P if Q" and "P only if Q." The symbolic form of this conjunction is $[(Q \rightarrow P) \wedge (P \rightarrow Q]$.

? Progress Check 2.3: The Truth Table for the Biconditional Statement

Complete a truth table for $[(Q \rightarrow P) \wedge (P \rightarrow Q]$. Use the following columns: P, Q, $Q \rightarrow P$, $P \rightarrow Q$, and $[(Q \rightarrow P) \wedge (P \rightarrow Q]$. The last column of this table will be the truth for $P \leftrightarrow Q$.

Answer

Add texts here. Do not delete this text first.

Other Forms of the Biconditional Statement

As with the conditional statement, there are some common ways to express the biconditional statement, $P \leftrightarrow Q$, in the English language.

Example

- P is and only if Q.
- P is necessary and sufficient for Q.
- P implies Q and Q implies P.

Tautologies and Contradictions

Definition: tautology

A **tautology** is a compound statement S that is true for all possible combinations of truth values of the component statements that are part of S. A **contradiction** is a compound statement that is false for all possible combinations of truth values of the component statements that are part of S.

That is, a tautology is necessarily true in all circumstances, and a contradiction is necessarily false in all circumstances.

Progress Check 2.4 (Tautologies and Contradictions)

For statements P and Q:

1. Use a truth table to show that $(P \vee \neg P)$ is a tautology.
2. Use a truth table to show that $(P \wedge \neg P)$ is a contradiction.
3. Use a truth table to determine if $P \rightarrow (P \vee P)$ is a tautology, a contradiction, nor neither.

Answer

Add texts here. Do not delete this text first.

Exercises for Section 2.1

1. Suppose that Daisy says, “If it does not rain, then I will play golf.” Later in the day you come to know that it did rain but Daisy still played golf. Was Daisy’s statement true or false? Support your conclusion.
2. Suppose that P and Q are statements for which $P \rightarrow Q$ is true and for which $\neg Q$ is true. What conclusion (if any) can be made about the truth value of each of the following statements?

   (a) P
   (b) $P \wedge Q$
   (c) $P \vee Q$
3. Suppose that P and Q are statements for which $P \rightarrow Q$ is false. What conclusion (if any) can be made about the truth value of each of the following statements?

   (a) $\neg P \rightarrow Q$
   (b) $Q \rightarrow P$
   (c) $P \; veeQ$
4. Suppose that P and Q are statements for which Q is false and $\neg P \rightarrow Q$ is true (and it is not known if R is true or false). What conclusion (if any) can be made about the truth value of each of the following statements?

   (a) $\neg Q \rightarrow P$
   (b) P
   (c) $P \wedge R$
   (d) $R \rightarrow \neg P$
5. Construct a truth table for each of the following statements:

   (a) $P \rightarrow Q$
   (b) $Q \rightarrow P$

(c) $\neg P \rightarrow \neg Q$
(d) $\neg Q \rightarrow \neg P$

Do any of these statements have the same truth table?

6. Construct a truth table for each of the following statements:

(a) $P \vee \neg Q$
(b) $\neg(P \vee Q)$
(c) $\neg P \vee \neg Q$
(d) $\neg P \wedge \neg Q$

Do any of these statements have the same truth table?

7. Construct truth table for $P \wedge (Q \vee R)$ and $(P \wedge Q) \vee (P \wedge R)$. What do you observe.
8. Suppose each of the following statements is true.
   - Laura is in the seventh grade.
   - ��Laura got an A on the mathematics test or Sarah got an A on the mathematics test.
   - ��If Sarah got an A on the mathematics test, then Laura is not in the seventh grade.

   If possible, determine the truth value of each of the following statements. Carefully explain your reasoning.

   (a) Laura got an A on the mathematics test.
   (b) Sarah got an A on the mathematics test.
   (c) Either Laura or Sarah did not get an A on the mathematics test.
9. Let P stand for "the integer x is even," and let Q stand for "x^2 is even." Express the conditional statement $P \rightarrow Q$ in English using

   (a) The "if then" form of the conditional statement
   (b) The word "Implies"
   (c) The "only if" form of the conditional statement
   (d) The phrase "is necessary for"
   (e) The phrase "is sufficient for"
10. Repeat Exercise (9) for the conditional statement $Q \rightarrow P$.
11. For statements P and Q, use truth tables to determine if each of the following statements is a tautology, a contradiction, or neither.
   (a) $\neg Q \vee (P \rightarrow Q)$.
   (b) $Q \wedge (P \wedge \neg Q)$.
   (c) $(Q \wedge P) \wedge (P \rightarrow \neg Q)$.
   (d) $\neg Q \rightarrow (P \wedge \neg P)$.
12. For statements P, Q, and R:
   (a) Show that $[(P \rightarrow Q) \wedge P] \rightarrow Q$ is a tautology. **Note**: In symbolic logic, this is an important logical argument form called **modus ponens**.
   (b) Show that $[(P \rightarrow Q) \wedge (Q \rightarrow R)] \rightarrow (P \rightarrow R)$ is atautology. **Note**: In symbolic logic, this is an important logical argument form called **syllogism**.

Explorations and Activities

13. **Working with Conditional Statements.** Complete the following table:

English Form	Hypothesis	Conclusion	Symbolic Form
If P, then Q	P	Q	$P \rightarrow Q$
Q only if P	Q	P	$Q \rightarrow P$
P is necessary for Q			

P is sufficient for Q			
Q is necessary for P			
P implies Q			
P only if Q			
P if Q			
if Q then P			
if $\neg Q$ then $\neg P$			
if Q, then $Q \wedge R$			
if $P \vee Q$, then R			

14. **Working with Truth Values of Statements.** Suppose that P and Q are true statements, that U and V are false statements, and that W is a statement and it is not known if W is true or false.

    Which of the following statements are true, which are false, and for which statements is it not possible to determine if it is true or false? Justify your conclusions.

    (a) $(P \vee Q) \vee (U \wedge W)$ (f) $(\neg P \vee \neg U) \wedge (Q \vee \neg V)$
    (b) $P \wedge (Q \rightarrow W)$ (g) $(P \wedge \neg Q) \wedge (U \vee W)$
    (c) $P \wedge (W \rightarrow Q)$ (h) $(P \vee \neg Q) \rightarrow (U \wedge W)$
    (d) $W \rightarrow (P \wedge U)$ (i) $(P \vee W) \rightarrow (U \wedge W)$
    (e) $W \rightarrow (P \wedge \neg U)$ (j) $(U \wedge \neg V) \rightarrow (P \wedge W)$

Answer

Add texts here. Do not delete this text first.

2.2: Logically Equivalent Statements

Preview Activity 2.2.1: Logically Equivalent Statements

In Exercises (5) and (6) from Section 2.1, we observed situations where two different statements have the same truth tables. Basically, this means these statements are equivalent, and we make the following definition:

Definition

Two expressions are **logically equivalent** provided that they have the same truth value for all possible combinations of truth values for all variables appearing in the two expressions. In this case, we write $X \equiv Y$ and say that X and Y are logically equivalent.

1. Complete truth tables for $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$.
2. Are the expressions $\neg(P \wedge Q)$ and $\neg P \vee \neg Q$ logically equivalent?
3. Suppose that the statement "I will play golf and I will mow the lawn" is false. Then its negation is true. Write the negation of this statement in the form of a disjunction. Does this make sense?

   Sometimes we actually use logical reasoning in our everyday living! Perhaps you can imagine a parent making the following two statements:

   Statement 1. If you do not clean your room, then you cannot watch TV.
   Statement 2. You clean your room or you cannot watch TV.
4. Let P be "you do not clean your room," and let Q be "you cannot watch TV." Use these to translate Statement 1 and Statement 2 into symbolic forms.
5. Construct a truth table for each of the expressions you determined in Part(4). Are the expressions logically equivalent?
6. Assume that Statement 1 and Statement 2 are false. In this case, what is the truth value of P and what is the truth value of Q? Now, write a true statement in symbolic form that is a conjunction and involves P and Q.
7. Write a truth table for the (conjunction) statement in Part (6) and compare it to a truth table for $\neg(P \to Q)$. What do you observe?

Preview Activity 2.2.2: Converse and Contrapositive

We now define two important conditional statements that are associated with a given conditional statement.

Definition

If P and Q are statements, then

- The **converse** of the conditional statement $P \to Q$ is the conditional statement $Q \to P$.
- The **contrapositive** of the conditional statement $P \to Q$ is the conditional statement $\neg Q \to \neg P$.

1. For the following, the variable x represents a real number. Label each of the following statements as true or false.
   (a) If $x = 3$, then $x^2 = 9$.
   (b) If $x^2 = 9$, then $x = 3$.
   (c) If $x^2 \neq 9$, then $x \neq 3$.
   (d) If $x \neq 3$, then $x^2 \neq 9$.
2. Which statement in the list of conditional statements in Part (1) is the converse of Statement (1a)? Which is the contrapositive of Statement (1a)?
3. Complete appropriate truth tables to show that
   $P \to Q$ is logically equivalent to its contrapositive $\neg Q \to \neg P$.
   $P \to Q$ is not logically equivalent to its converse $Q \to P$

In Preview Activity 2.2.1, we introduced the concept of logically equivalent expressions and the notation $X \equiv Y$ to indicate that statements X and Y are logically equivalent. The following theorem gives two important logical equivalencies. They are sometimes referred to as **De Morgan's Laws**.

Theorem 2.5: De Morgan's Laws

For statements P and Q,

- The statement $\neg(P \wedge Q)$ is logically equivalent to $\neg P \vee \neg Q$. This can be written as $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$.
- The statement $\neg(P \vee Q)$ is logically equivalent to $\neg P \wedge \neg Q$. This can be written as $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$.

Proof

The first equivalency in Theorem 2.5 was established in Preview Activity 2.2.1. Table 2.3 establishes the second equivalency.

Table 2.3: Truth Table for One of De Morgan's Laws

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P$	$\neg Q$	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

It is possible to develop and state several different logical equivalencies at this time. However, we will restrict ourselves to what are considered to be some of the most important ones. Since many mathematical statements are written in the form of conditional statements, logical equivalencies related to conditional statements are quite important.

Logical Equivalencies Related to Conditional Statements

The first two logical equivalencies in the following theorem were established in Preview Activity 2.2.1, and the third logical equivalency was established in Preview Activity 2.2.2.

Theorem 2.6

For statements P and Q,

1. The conditional statement $P \to Q$ is logically equivalent to $\neg P \vee Q$.
2. The statement $\neg(P \to Q)$ is logically equivalent to $P \wedge \neg Q$.
3. The conditional statement $P \to Q$ is logically equivalent to its contrapositive $\neg Q \to \neg P$.

The Negation of a Conditional Statement

The logical equivalency $\neg(P \to Q) \equiv P \wedge \neg Q$ is interesting because it shows us that **the negation of a conditional statement is not another conditional statement**. The negation of a conditional statement can be written in the form of a conjunction. So what does it mean to say that the conditional statement

If you do not clean your room, then you cannot watch TV,

is false? To answer this, we can use the logical equivalency $\neg(P \to Q) \equiv P \wedge \neg Q$. The idea is that if $P \to Q$ is false, then its negation must be true. So the negation of this can be written as

You do not clean your room and you can watch TV.

For another example, consider the following conditional statement:

If $-5 < -3$, then $(-5)^2 < (-3)^2$.

This conditional statement is false since its hypothesis is true and its conclusion is false. Consequently, its negation must be true. Its negation is not a conditional statement. The negation can be written in the form of a conjunction by using the logical equivalency

$\neg(P \to Q) \equiv P \wedge \neg Q$. So, the negation can be written as follows:

$$5 < 3 \text{ and } \neg((-5)^2 < (-3)^2).$$

However, the second part of this conjunction can be written in a simpler manner by noting that "not less than" means the same thing as "greater than or equal to." So we use this to write the negation of the original conditional statement as follows:

$$5 < 3 \text{ and } (-5)^2 \geq (-3)^2.$$

This conjunction is true since each of the individual statements in the conjunction is true.

Another Method of Establishing Logical Equivalencies

We have seen that it often possible to use a truth table to establish a logical equivalency. However, it is also possible to prove a logical equivalency using a sequence of previously established logical equivalencies. For example,

- $P \to Q$ is logically equivalent to $\neg P \vee Q$. So
- $\neg(P \to Q)$ is logically equivalent to $\neg(\neg P \vee Q)$.
- Hence, by one of De Morgan's Laws (Theorem 2.5), $\neg(P \to Q)$ is logically equivalent to $\neg(\neg P) \wedge \neg Q$.
- This means that $\neg(P \to Q)$ is logically equivalent to$P \wedge \neg Q$.

The last step used the fact that $\neg(\neg P)$ is logically equivalent to P.

When proving theorems in mathematics, it is often important to be able to decide if two expressions are logically equivalent. Sometimes when we are attempting to prove a theorem, we may be unsuccessful in developing a proof for the original statement of the theorem. However, in some cases, it is possible to prove an equivalent statement. Knowing that the statements are equivalent tells us that if we prove one, then we have also proven the other. In fact, once we know the truth value of a statement, then we know the truth value of any other logically equivalent statement. This is illustrated in Progress Check 2.7.

Progress Check 2.7 (Working with a logical equivalency)

In Section 2.1, we constructed a truth table for $(P \wedge \neg Q) \to R$.

1. Although it is possible to use truth tables to show that $P \to (Q \vee R)$ is logically equivalent to $P \wedge \neg Q) \to R$, we instead use previously proven logical equivalencies to prove this logical equivalency. In this case, it may be easier to start working with $P \wedge \neg Q) \to R$. Start with

   $P \wedge \neg Q) \to R \equiv \neg(P \wedge \neg Q) \vee R$,

   which is justified by the logical equivalency established in Part (5) of Preview Activity 1. Continue by using one of De Morgan's Laws on $\neg(P \wedge \neg Q)$.
2. Let a and b be integers. Suppose we are trying to prove the following:

   If 3 is a factor of $a \cdot b$, then 3 is a factor of a or 3 is a factor of b.

   Explain why we will have proven this statement if we prove the following:

   If 3 is a factor of $a \cdot b$ and 3 is not a factor of a, then 3 is a factor of b.

Answer

Add texts here. Do not delete this text first.

As we will see, it is often difficult to construct a direct proof for a conditional statement of the form $P \to (Q \vee R)$. The logical equivalency in Progress Check 2.7 gives us another way to attempt to prove a statement of the form $P \to (Q \vee R)$. The advantage of the equivalent form, $P \wedge \neg Q) \to R$, is that we have an additional assumption, $\neg Q$, in the hypothesis. This gives us more information with which to work.

Theorem 2.8 states some of the most frequently used logical equivalencies used when writing mathematical proofs.

Theorem 2.8: important logical equivalencies

For statement P, Q, and R,

De Morgan's Laws $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$.
$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$.

Conditional Statement. $P \to Q \equiv \neg Q \to \neg P$ (contrapositive)
$P \to Q \equiv \neg P \vee Q$
$\neg(P \to Q) \equiv P \wedge \neg Q$

Biconditional Statement $(Pleftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P)$

Double Negation $\neg(\neg P) \equiv P$

Distributive Laws $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

Conditionals withDisjunctions $P \to (Q \vee R) \equiv (P \wedge \neg Q) \to R$
$(P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R)$

We have already established many of these equivalencies. Others will be established in the exercises.

Exercises for Section 2.2

1. Write the converse and contrapositive of each of the following conditional statements.
   (a) If $a = 5$, then $a^2 = 25$.
   (b) If it is not raining, then Laura is playing golf.
   (c) If $a \neq b$, then $a^4 \neq b^4$.
   (d) If a is an odd integer, then $3a$ is an odd integer.
2. Write each of the conditional statements in Exercise (1) as a logically equiva- lent disjunction, and write the negation of each of the conditional statements in Exercise (1) as a conjunction.
3. Write a useful negation of each of the following statements. Do not leave a negation as a prefix of a statement. For example, we would write the negation of “I will play golf and I will mow the lawn” as “I will not play golf or I will not mow the lawn.”
   (a) We will win the first game and we will win the second game.
   (b) They will lose the first game or they will lose the second game.
   (c) If you mow the lawn, then I will pay you $20.
   (d) If we do not win the first game, then we will not play a second game.
   (e) I will wash the car or I will mow the lawn.
   (f) If you graduate from college, then you will get a job or you will go to graduate school.
   (g) If I play tennis, then I will wash the car or I will do the dishes.
   (h) If you clean your room or do the dishes, then you can go to see a movie.
   (i) It is warm outside and if it does not rain, then I will play golf.
4. Use truth tables to establish each of the following logical equivalencies dealing with biconditional statements:
   (a) $(P \leftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P)$
   (b) $(P \leftrightarrow Q) \equiv (Q \leftrightarrow P)$
   (c) $(P \leftrightarrow Q) \equiv (\neg P \leftrightarrow \neg Q)$
5. Use truth tables to prove each of the **distributive laws** from Theorem 2.8.

   (a) $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
   (b $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
6. Use truth tables to prove the following logical equivalency from Theorem 2.8:

   $[(P \vee Q) \to R] \equiv (P \to R) \wedge (Q \to R)$.

7. Use previously proven logical equivalencies to prove each of the following logical equivalencies about **conditionals with conjunctions:**

   (a) $[(P \wedge Q) \rightarrow R] \equiv (P \rightarrow R) \vee (Q \rightarrow R)$
   (b) $[P \rightarrow (Q \wedge R)] \equiv (P \rightarrow R) \wedge (P \rightarrow R)$
8. If P and Q are statements, is the statement $(P \vee Q) \wedge \neg(P \wedge Q)$ logically equivalent to the statement $(P \wedge \neg Q) \vee (Q \wedge \neg P)$? Justify your conclusion.
9. Use previously proven logical equivalencies to prove each of the following logical equivalencies: (a) $[\neg P \rightarrow (Q \wedge \neg Q)] \equiv P$
   (b) $(P \leftrightarrow Q) \equiv (\neg P \vee Q) \wedge (\neg Q \vee p)$
   (c) $\neg(P \leftrightarrow Q) \equiv (P \wedge \neg Q) \vee (Q \wedge \neg P)$
   (d) $(P \rightarrow Q) \rightarrow R \equiv (P \wedge \neg Q) \vee R$
   (e) $(P \rightarrow Q) \rightarrow R \equiv (\neg P \rightarrow R) \wedge (Q \rightarrow R)$
   (f) $[(P \wedge Q) \rightarrow (R \vee S)] \equiv [(\neg R \wedge \neg S) \rightarrow (\neg P \vee \neg Q)]$
   (g) $[(P \wedge Q) \rightarrow (R \vee S)] \equiv [(P \wedge Q \wedge \neg R) \rightarrow S]$
   (h) $[(P \wedge Q) \rightarrow (R \vee S)] \equiv (\neg P \vee \neg Q \vee R \vee S)$
   (i) $\neg[(P \wedge Q) \rightarrow (R \vee S)] \equiv (P \wedge Q \wedge \neg R \wedge \neg S)$
10. Let a be a real number and let f be a real-valued function defined on an interval containing $x = a$. Consider the following conditional statement:

    If f is differentiable at $x = a$, then f is continuous at $x = a$.

    Which of the following statements have the same meaning as this conditional statement and which ones are negations of this conditional statement?

    Note: This is not asking which statements are true and which are false. It is asking which statements are logically equivalent to the given statement. It might be helpful to let P represent the hypothesis of the given statement, Q represent the conclusion, and then determine a symbolic representation for each statement. Instead of using truth tables, try to use already established logical equivalencies to justify your conclusions.

    (a) If f is continuous at $x = a$, then f is differentiable at $x = a$.
    (b) If f is not differentiable at $x = a$, then f is not continuous at $x = a$.
    (c) If f is not continuous at $x = a$, then f is not differentiable at $x = a$.
    (d) f is not differentiable at $x = a$ or f is continuous at $x = a$.
    (e) f is not continuous at $x = a$ or f is differentiable at $x = a$.
    (f) f is differentiable at $x = a$ or f is not continuous at $x = a$.
11. Let a, b, and c be integers. Consider the following conditional statement:

    If a divides bc, then a divides b or a divides c.

    Which of the following statements have the same meaning as this conditional statement and which ones are negations of this conditional statement?

    The note for Exercise (10) also applies to this exercise.

    (a) If a divides b or a divides c, then a divides bc.
    (b) If a does not divide b or a does not divide c, then a does not divide bc.
    (c) a divides bc, a does not divide b, and a does not divide c.
    (d) If a does not divide b and a does not divide c, then a does not divide bc.
    (e) a does not divide bc or a divides b or a divides c.
    (f) If a divides bc and a does not divide c, then a divides b.
    (g) If a divides bc or a does not divide b, then a divides c.

12. Let x be a real number. Consider the following conditional statement:

    If $x^3 - x = 2x^2 + 6$, then $x = -2$ or $x = 3$.

    Which of the following statements have the same meaning as this conditional statement and which ones are negations of this conditional statement? Explain each conclusion. (See the note in the instructions for Exercise (10).)

    (a) If $x \neq -2$ and $x \neq 3$, then $x^3 - x \neq 2x^2 + 6$.
    (b) If $x = -2$ or $x = 3$, then $x^3 - x = 2x^2 + 6$.
    (c) If $x \neq -2$ or $x \neq 3$, then $x^3 - x \neq 2x^2 + 6$.
    (d) If $x^3 - x = 2x^2 + 6$ and $x \neq -2$, then $x = 3$.
    (e) If $x^3 - x = 2x^2 + 6$ or $x \neq -2$, then $x = 3$.
    (f) $x^3 - x = 2x^2 + 6$, $x \neq -2$, and $x \neq 3$.
    (g) $x^3 - x \neq 2x^2 + 6$ or $x = -2$ or $x = 3$.

Explorations and Activities

13. **Working with a Logical Equivalency.** Suppose we are trying to prove the following for integers x and y:

    If $x \cdot y$ is even, then x is even or y is even.

    We notice that we can write this statement in the following symbolic form:

    $P \to (Q \vee R)$,

    where P is"$x \cdot y$ is even," Q is"x is even,"and R is "y is even."

    (a) Write the symbolic form of the contrapositive of $P \to (Q \vee R)$. Then use one of De Morgan's Laws (Theorem 2.5) to rewrite the hypothesis of this conditional statement.
    (b) Use the result from Part (13a) to explain why the given statement is logically equivalent to the following statement:

    If x is odd and y is odd, then $x \cdot y$ is odd.

    The two statements in this activity are logically equivalent. We now have the choice of proving either of these statements. If we prove one, we prove the other, or if we show one is false, the other is also false. The second statement is Theorem 1.8, which was proven in Section 1.2.

Answer

Add texts here. Do not delete this text first.

2.3: Open Sentences and Sets

Preview Activity 2.3.1: Sets and Set Notation

The theory of sets is fundamental to mathematics in the sense that many areas of mathematics use set theory and its language and notation. This language and notation must be understood if we are to communicate effectively in mathematics. At this point, we will give a very brief introduction to some of the terminology used in set theory.

A **set** is a well-defined collection of objects that can be thought of as a single entity itself. For example, we can think of the set of integers that are greater than 4. Even though we cannot write down all the integers that are in this set, it is still a perfectly well-defined set. This means that if we are given a specific integer, we can tell whether or not it is in the set of all even integers.

The most basic way of specifying the elements of a set is to list the elements of that set. This works well when the set contains only a small number of objects. The usual practice is to list these elements between braces. For example, if the set C consists of the integer solutions of the equation $x^2 = 9$, we would write

$$C = \{-3, 3\}.$$

For larger sets, it is sometimes inconvenient to list all of the elements of the set. In this case, we often list several of them and then write a series of three dots (...) to indicate that the pattern continues. For example,

$$D = \{1, 3, 5, 7, \ldots 49\}$$

is the set of all odd natural numbers from 1 to 49, inclusive.

For some sets, it is not possible to list all of the elements of a set; we then list several of the elements in the set and again use a series of three dots (...) to indicate that the pattern continues. For example, if F is the set of all even natural numbers, we could write

$$F = \{2, 4, 6, \ldots\}.$$

We can also use the three dots before listing specific elements to indicate the pattern prior to those elements. For example, if E is the set of all even integers, we could write

$$E = \{\ldots -6, -4, -2, 0, 2, 4, 6, \ldots\}.$$

Listing the elements of a set inside braces is called the **roster method** of specifying the elements of the set. We will learn other ways of specifying the elements of a set later in this section.

1. Use the roster method to specify the elements of each of the following sets:

   (a) The set of real numbers that are solutions of the equation $x^2 - 5x = 0$.
   (b) The set of natural numbers that are less than or equal to 10.
   (c) The set of integers that are greater than -2.
2. Each of the following sets is defined using the roster method. For each set, determine four elements of the set other than the ones listed using the roster method.
   $A = \{1, 4, 7, 10, \ldots\}$
   $B = \{2, 4, 8, 16, \ldots\}$
   $C = \{\ldots, -8, -6, -4, -2, 0\}$
   $D = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$

Preview Activity 2.3.2: Variables

Not all mathematical sentences are statements. For example, an equation such as

$$x^2 - 5 = 0$$

is not a statement. In this sentence, the symbol x is a **variable**. It represents a number that may be chosen from some specified set of numbers. The sentence (equation) becomes true or false when a specific number is substituted for x.

1. (a) Does the equation $x^2 - 25 = 0$ become a true statement if -5 is substituted for x?
   (b) Does the equation $x^2 - 25 = 0$ become a true statement if $\sqrt{5}$ is substituted for x?

Definition

A **variable** is a symbol representing an unspecified object that can be chosen from a given set U. The set U is called the **universal set for the variable**. It is the set of specified objects from which objects may be chosen to substitute for the variable. A **constant** is a specific member of the universal set.

Some sets that we will use frequently are the usual number systems. Recall that we use the symbol $\mathbb{R}$ to stand for the set of all **real numbers**, the symbol $\mathbb{Q}$ to stand for the set of all **rational numbers**, the symbol $\mathbb{Z}$ to stand for the set of all **integers**, and the symbol $\mathbb{N}$ to stand for the set of all **natural numbers**.

A **variable** is a symbol representing an unspecified object that can be chosen from some specified set of objects. This specified set of objects is agreed to in advance and is frequently called the **universal set**.

2. What real numbers will make the sentence "$y^2 - 2y - 15 = 0$ " a true statement when substituted for y?
3. What natural numbers will make the sentence "$y^2 - 2y - 15 = 0$ " a true statement when substituted for y?
4. What real numbers will make the sentence "$\sqrt{x}$ is a real number" a true statement when substituted for x?
5. What real numbers will make the sentence "$sin^2 x + cos^2 x = 1$ " a true statement when substituted for x?
6. What natural numbers will make the sentence "$\sqrt{n}$ is a natural number" a true statement when substituted for n?
7. What real numbers will make the sentence

$$\int_0^y t^2 dt > 9$$

a true statement when substituted for y?

Some Set Notation

In Preview Activity 2.3.1, we indicated that a set is a well-defined collection of objects that can be thought of as an entity itself.

- If $A$is a set and y is one of the objects in the set A, we write $y \in A$ and read this as "y is an element of A" or "y is a member of A." For example, if B is the set of all integers greater than 4, then we could write $5 \in B$ and $10 \in B$.
- If an object z is not an element in the set A, we write $z \notin A$ and read this as "z is not an element of A." For example, if B is the set of all integers greater than 4, then we could write $2 \notin B$ and $4 \notin B$.

When working with a mathematical object, such as set, we need to define when two of these objects are equal. We are also often interested in whether or not one set is contained in another set.

Definitions: Equal sets and Subsets

Two sets, A and B, are *equal* when they have precisely the same elements. In this case, we write $A = B$. When the sets A and B are not equal, we write $A \neq B$.

The set A is a *subset* of a set B provided that each element of A is an element of B. In this case, we write $A \subseteq B$ and also say that A is *contained* in B. When A is not a subset of B, we write $A \nsubseteq B$.

Using these definitions, we see that for any set A, $A = A$ and since it is true that for each $x \in U$, if $x \in A$, then $x \in A$, we also see that $A \subseteq A$. That is, any set is equal to itself and any set is a subset of itself. For some specific examples, we see that:

- {1, 3, 5} = {3, 5, 1}
- {5, 10} = {5, 10, 5}
- {4, 8, 12} = {4, 4, 8, 12, 12}
- {5, 10} $\neq$ {5, 10, 15} but {5,10} $\subseteq$ {5, 10, 15} and {5, 10, 15} $\nsubseteq$ {5, 10}.

In each of the first three examples, the two sets have exactly the same elements even though the elements may be repeated or written in a different order.

Progress Check 2.9 (Set Notation)

1. Let A = {-4, -2, 0, 2, 4, 6, 8, ...}. Use correct set notation to indicate which of the following integers are in the set A and which are not in the set A. For example, we could write $6 \in A$ and $5 \notin A$.

   10 22 13 -3 0 -12
2. Use correct set notation (using = or $\subseteq$) to indicate which of the following sets are equal and which are subsets of one of the other sets.

   A = {3, 6, 9}. B = {6, 9, 3, 6}
   C = {3, 6, 9, ... } D = {3, 6, 7, 9}
   E = {9, 12, 15, ... } F = {9, 7, 6, 2}

Answer

Add texts here. Do not delete this text first.

Variables and Open Sentences

As we have seen in the Preview Activities, not all mathematical sentences are statements. This is often true if the sentence contains a variable. The following terminology is useful in working with sentences and statements.

Definition: Open Sentence

An **open sentence** is a sentence $P(x_1, x_2, \ldots, x_n)$ involving variables $x_1, x_2, \ldots, x_n$ with the property that when specific values from the universal set are assigned to $x_1, x_2, \ldots, x_n$, then the resulting sentence is either true or false. That is, the resulting sentence is a statement. An open sentence is also called a **predicate** or a **propositional function**.

Notation: One reason an open sentence is sometimes called a *propositional function* is the fact that we use function notation $P(x_1, x_2, \ldots, x_n)$ for an open sentence in n variables. When there is only one variable, such as x, we write $P(X)$, which is read "P of x." In this notation, x represents an arbitrary element of the universal set, and $P(x)$ represents a sentence. When we substitute a specific element of the universal set for x, the resulting sentence becomes a statement. This is illustrated in the next example.

Example 2.10: Open Sentences

If the universal set is $\mathbb{R}$, then the sentence "$x^2 - 3x - 10 = 0$ " is an open sentence involving the one variable x.

- If we substitute $x = 2$, we obtain the false statement "$2^2 - 3 \cdot 2 - 10 = 0$."
- If we substitute $x = 5$, we obtain the true statement "$5^2 - 3 \cdot 5 - 10 = 0$."

In this example, we can let $P(x)$ be the predicate "$x^2 - 3x - 10 = 0$ " and then say that $P(2)$ is false and $P(5)$ is true.

Using similar notation, we can let $Q(x, y)$be the predicate "$x + 2y = 7$." This predicate involves two variables. Then,

- $Q(1, 1)$is false since "$1 + 2 \cdot 1 = 7$ " is false; and
- $Q(3, 2)$is true since "$3 + 2 \cdot 2 = 7$ " is false.

Progress Check 2.11: Working with Open Sentences

1. Assume the universal set for all variable is $\mathbb{Z}$ and let $P(x)$ be the predicate "$x^2 \leq 4$."
   (a) Find two values of x for which $P(x)$ is false.
   (b) Find two values of x for which $P(x)$ is true.
   (c) Use the roster method to specify the set of all x for which $P(x)$ is true.
2. Assume the universal set for all variable is $\mathbb{Z}$ and let $R(x, y, z)$ be the predicate "$x^2 + y^2 = z^2$."
   (a) Find two different examples for which $R(x, y, z)$ is false.
   (b) Find two different examples for which $R(x, y, z)$ is true.

Answer

Add texts here. Do not delete this text first.

Without using the term, Example 2.10 and Progress Check 2.11 (and Preview Activity 2.3.2) dealt with a concept called the truth set of a predicate.

Definition: truth set of an open sentence with one variable

The *truth set of an open sentence with one variable* is the collection of objects in the universal set that can be substituted for the variable to make the predicate a true statement.

One part of elementary mathematics consists of learning how to solve equations. In more formal terms, the process of solving an equation is a way to determine the truth set for the equation, which is an open sentence. In this case, we often call the truth set the **solution set**. Following are three examples of truth sets.

- If the universal set is $\mathbb{R}$, then the truth set of the equation $3x - 8 = 10$ is the set $\{6\}$.
- If the universal set is $\mathbb{R}$, then the truth set of the equation $x^2 - 3x - 10 = 0$ is {-2, 5}.
- If the universal set is $\mathbb{N}$, then the truth set of the open sentence "$\sqrt{n} \in \mathbb{N}$" is {1, 4, 9, 16, ...}.

Set Builder Notation

Sometimes it is not possible to list all the elements of a set. For example, if the universal set is $\mathbb{R}$, we cannot list all the elements of the truth set of "$x^2 < 4$." In this case, it is sometimes convenient to use the so-called **set builder notation** in which the set is defined by stating a rule that all elements of the set must satisfy. If $P(x)$ is a predicate in the variable x, then the notation

$$\{x \in U | P(x)\}$$

stands for the set of all elements x in the universal set U for which $P(x)$ is true. If it is clear what set is being used for the universal set, this notation is sometimes shortened to $\{x | P(x)\}$. This is usually read as "the set of all x such that $P(x)$." The vertical bar stands for the phrase "such that." Some writers will use a colon (:) instead of the vertical bar.

For a non-mathematical example, P could be the property that a college student is a mathematics major. Then $\{x | P(x)\}$ denotes the set of all college students who are mathematics majors. This could be written as

$$\{x \mid x \text{ is a college student who is a mathematics major}\}.$$

Example 2.12 (Truth Sets)

Assume the universal set is $\mathbb{R}$ and $P(x)$ is "$x^2 < 4$." We can describe the truth set of $P(x)$ as the set of all real numbers whose square is less than 4. We can also use set builder notation to write the truth set of $P(x)$ as

$$\{x \in \mathbb{R} | x^2 < 4\}$$

However, if we solve the inequality $x^2 < 4$, we obtain $-2 < x < 2$. So we could also write the truth set as

$$\{x \in \mathbb{R} | -2 < x < 4\ \}$$

We could read this as the set of all real numbers that are greater than -2 and less than 2. We can also write

$$\{x \in \mathbb{R} | x^2 < 4\} = \{x \in \mathbb{R} | -2 < x < 4\ \}$$

Progress Check 2.13 (Working with Truth Sets)

Let $P(x)$ be the predicate "$x^2 \leq 9$."

1. If the universal set is $\mathbb{R}$, describe the truth set of $P(x)$ using English and write the truth set of $P(x)$ using set builder notation.
2. If the universal set is $\mathbb{Z}$, then what is the truth set of $P(x)$? Describe this set using English and then use the roster method to specify all the elements of this truth set.
3. Are the truth sets in Parts (1) and (2) equal? Explain.

Answer

Add texts here. Do not delete this text first.

So far, our standard form for set builder notation has been $\{x \in U | P(x)\}$. It is sometimes possible to modify this form and put the predicate first. For example, the set

$$\{A = 3n+1 | n \in \mathbb{N}\}$$

describes the set of all natural numbers of the form $3n+1$ for some natural number.

By substituting 1, 2, 3, 4, and so on, for n, we can use the roster method to write

$$A = \{3n+1 | n \in \mathbb{N}\} = \{4, 7, 10, 13, \ldots\}.$$

We can sometimes "reverse this process" by starting with a set specified by the roster method and then writing the same set using set builder notation.

Example 2.14 (Set Builder Notation)

Let B = {..., -11. -7, -3, 1, 5, 9, 13, ...}. The key to writing this set using set builder notation is to recognize the pattern involved. We see that once we have an integer in B, we can obtain another integer in B by adding 4. This suggests that the predicate we will use will involve multiplying by 4.

Since it is usually easier to work with positive numbers, we notice that $1 \in B$ and $5 \in B$. Notice that

$$1 = 4 \cdot 0 + 1 \text{ and } 5 = 4 \cdot 1 + 1 .$$

This suggests that we might try $4n+1 | n \in \mathrm{z}$. In fact, by trying other integers for n, we can see that

$$B = \{..., -11, -7, -3, 1, 5, 9, 13, ...\} = \{4n+1 | n \in \mathbb{Z}\}.$$

Progress Check 2.15 (Set Builder Notation)

Each of the following sets is defined using the roster method.

A = {1, 5, 9, 13, ...} C = { $\sqrt{2}$, $(\sqrt{2})^3$, $(\sqrt{2})^5$, ... }

B = {..., -8, -6, -4, -2, 0} D = {1, 3, 9, 27, ...}

1. Determine four elements of each set other than the ones listed using the roster method.
2. Use set builder notation to describe each set.

Answer

Add texts here. Do not delete this text first.

The Empty Set

When a set contains no elements, we say that the set is the empty set. For example, the set of all rational numbers that are solutions of the equation $x^2 = -$[illegible]2 is the empty set since this equation has no solutions that are rational numbers.

In mathematics, the empty set is usually designated by the symbol $\emptyset$. We usually read the symbol $\emptyset$ as "the empty set" or "the null set." (The symbol $\emptyset$ is actually the last letter in the Danish-Norwegian alphabet.)

When the Truth Set Is the Universal Set

The truth set of a predicate can be the universal set. For example, if the universal set is the set of real numbers $\mathbb{R}$, then the truth set of the predicate "$x+0=x$" is $\mathbb{R}$.

Notice that the sentence "$x+0=x$" has not been quantified and a particular element of the universal set has not been substituted for the variable x. Even though the truth set for this sentence is the universal set, we will adopt the convention that unless the quantifier is stated explicitly, we will consider the sentence to be a predicate or open sentence. So, with this convention, if the universal set is $\mathbb{R}$, then

- $x+0=x$ is a predicate;

- For each real number x, $x+0=x$ is a statement.

Exercises for Section 2.3

1. Use the roster method to specify the elements in each of the following sets and then write a sentence in English describing the set.
   (a) $\{x \in \mathbb{R} | 2x^2+3x-2=0\}$
   (b) $\{x \in \mathbb{Z} | 2x^2+3x-2=0\}$
   (c) $\{x \in \mathbb{Z} | x^2<25\}$
   (d) $\{x \in \mathbb{N} | x^2<25\}$
   (e) $\{y \in \mathbb{Q} | |y-2|=2.5\}$
   (f) $\{y \in \mathbb{Z} | |y-2| \leq 2.5\}$
2. Each of the following sets is defined using the roster method.

   A= {1, 4, 9, 16, 25, ...}
   B = {..., -π^4, -π^3, -π^2, -π, 0...}
   C = {3, 9, 15, 21, 27, ...}
   D = {0, 4, 8, ..., 96, 100}

   (a) Determine four elements of each set other than the ones listed using the roster method.
   (b) Use set builder notation to describe each set.
3. Let A = $\{x \in \mathbb{R} | x(x+2)^2(x-\frac{3}{2}=0\}$. Which of the following sets are equal to the set A and which are subsets of A?

   (a) $\{-2, 0, 3\}$
   (b) $\{-2, -2, 0, \frac{3}{2}\}$
   (c) $\{\frac{3}{2}, -2, 0\}$
   (d) $\{-2, \frac{3}{2}\}$
4. Use the roster method to specify the truth set for each of the following open sentences. The universal set for each open sentence is the set of integers $\mathbb{Z}$.

   (a) $n+7=4$.
   (b) $n^2=64$.
   (c) $\sqrt{n} \in \mathbb{N}$ and n is less than 50.
   (d) n is an odd integer that is greater than 2 and less than 14.
   (e) n is an even integer that is greater than 10.
5. Use set builder notation to specify the following sets:

   (a) The set of all integers greater than or equal to 5.
   (b) The set of all even integers.
   (c) The set of all positive rational numbers.
   (d) The set of all real numbers greater than 1 and less than 7.
   (e) The set of all real numbers whose square is greater than 10.
6. For each of the following sets, use English to describe the set and when appropriate, use the roster method to specify all of the elements of the set.

   (a) $\{x \in \mathbb{R} | -3 \leq x \leq 5\}$
   (b) $\{x \in \mathbb{Z} | -3 \leq x \leq 5\}$
   (c) $\{x \in \mathbb{R} | x^2=16\}$
   (d) $\{x \in \mathbb{R} | x^2+16=0\}$
   (e) $\{x \in \mathbb{Z} | x \text{ is odd}\}$
   (f) $\{x \in \mathbb{R} | 3x-4 \geq 17\}$

Explorations and Activities

7. **Closure Explorations**. In Section 1.1, we studied some of the closure properties of the standard number systems. (See page 10.) We can extend this idea to other sets of numbers. So we say that:

   • A set A of numbers is **closed under addition** provided that whenever x and y are are in the set A, $x+y$ is in the set A.
   • A set A of numbers is **closed under multiplication** provided that whenever x and y are are in the set A, $x \cdot y$ is in the set A.
   • A set A of numbers is **closed under subtraction** provided that whenever x and y are are in the set A, $x-y$ is in the set A.

   For each of the following sets, make a conjecture about whether or not it is closed under addition and whether or not it is closed under multiplication. In some cases, you may be able to find a counterexample that will prove the set is not closed under one of these operations.
   (a) The set of all odd natural numbers
   (b) The set of all even integers
   (c) A = {1, 4, 7, 10, 13, ...}
   (d) B = {..., -6, -3, 0, 3, 6, 9, ...}
   (e) $C = \{3n+1 | n \in \mathbb{Z}\}$
   (f) $D = \{\frac{1}{2^n} | n \in \mathbb{N}\}$

Answer

Add texts here. Do not delete this text first.

2.4: Quantifiers and Negations

Preview Activity 1 (An Introduction to Quantifiers)

We have seen that one way to create a statement from an open sentence is to substitute a specific element from the universal set for each variable in the open sentence. Another way is to make some claim about the truth set of the open sentence. This is often done by using a quantifier. For example, if the universal set is $\mathbb{R}$, then the following sentence is a statement.

For each real number x, $x^2 > 0$.

The phrase "For each real number x" is said to **quantify the variable** that follows it in the sense that the sentence is claiming that something is true for all real numbers. So this sentence is a statement (which happens to be false).

Definition: universal quantifier

The phrase "for every" (or its equivalents) is called a *universal quantifier*. The phrase "there exists" (or its equivalents) is called an **existential quantifier**. The symbol $\forall$ is used to denote a universal quantifier, and the symbol $\exists$ is used to denote an existential quantifier.

Using this notation, the statement "For each real number x, $x^2 > 0$" could be written in symbolic form as: $(\forall x \in \mathbb{R})(x^2 > 0)$. The following is an example of a statement involving an existential quantifier.

There exists an integer x such that $3x - 2 = 0$.

This could be written in symbolic form as

$$(\exists x \in \mathbb{Z})(3x - 2 = 0).$$

This statement is false because there are no integers that are solutions of the linear equation $3x - 2 = 0$. Table 2.4 summarizes the facts about the two types of quantifiers.

A statement involving	Often has the form	The statement is true provided that
A universal quantifier: $(\forall x, P(x))$	"For every x, $P(x)$," where $P(x)$ is a predicate.	Every value of x in the universal set makes $P(x)$ true.
An existential quantifier: $(\exists x, P(x))$	"There exists an x such that $P(x)$," where $P(x)$ is a predicate.	There is at least one value of x in the universal set that makes $P(x)$ true.

Table 2.4: Properties of Quantifiers

In effect, the table indicates that the universally quantified statement is true provided that the truth set of the predicate equals the universal set, and the existentially quantified statement is true provided that the truth set of the predicate contains at least one element.

Each of the following sentences is a statement or an open sentence. Assume that the universal set for each variable in these sentences is the set of all real numbers. If a sentence is an open sentence (predicate), determine its truth set. If a sentence is a statement, determine whether it is true or false.

1. $(\forall a \in \mathbb{R})(a + 0 = a)$.
2. $3x - 5 = 9$.
3. $\sqrt{x} \in \mathbb{R}$.
4. $sin(2x) = 2(sinx)(cosx)$.
5. $(\forall x \in \mathbb{R})(sin(2x) = 2(sinx)(cosx))$.
6. $(\exists x \in \mathbb{R})(x^2 + 1 = 0)$.
7. $(\forall x \in \mathbb{R})(x^3 \geq x^2)$.
8. $x^2 + 1 = 0$.
9. If $x^2 \geq 1$, then $x \geq 1$.
10. $(\forall x \in \mathbb{R})$ (If $x^2 \geq 1$, then $x \geq 1$).

Preview Activity 2 (Attempting to Negate Quantified Statements)

1. Consider the following statement written in symbolic form:
   $(\forall x \in \mathbb{Z})$ (x is a multiple of 2).

   (a) Write this statement as an English sentence.
   (b) Is the statement true or false? Why?
   (c) How would you write the negation of this statement as an English sentence?
   (d) If possible, write your negation of this statement from part(2) symbolically (using a quantifier).
2. Consider the following statement written in symbolic form:
   $(\exists x \in \mathbb{Z})$ $(x^3 > 0)$.

   (a) Write this statement as an English sentence.
   (b) Is the statement true or false? Why?
   (c) How would you write the negation of this statement as an English sentence?
   (d) If possible, write your negation of this statement from part(2) symbolically (using a quantifier).

We introduced the concepts of open sentences and quantifiers in Section 2.3

Forms of Quantified Statements in English

There are many ways to write statements involving quantifiers in English. In some cases, the quantifiers are not apparent, and this often happens with conditional statements. The following examples illustrate these points. Each example contains a quantified statement written in symbolic form followed by several ways to write the statement in English.

1. $(\forall x \in \mathbb{R})$ $(x^2 > 0)$.

   - For each real number x, $x^2 > 0$.
   - The square of every real number is greater than 0.
   - The square of a real number is greater than 0.
   - If $x \in \mathbb{R}$, then $x^2 > 0$.

   In the second to the last example, the quantifier is not stated explicitly. Care must be taken when reading this because it really does say the same thing as the previous examples. The last example illustrates the fact that conditional statements often contain a “hidden” universal quantifier.

   If the universal set is $\mathbb{R}$, then the truth set of the open sentence $x^2 > 0$ is the set of all nonzero real numbers. That is, the truth set is

   $\{x \in \mathbb{R} | x \neq 0\}$

   So the preceding statements are false. For the conditional statement, the example using $x = 0$ produces a true hypothesis and a false conclusion. This is a **counterexample** that shows that the statement with a universal quantifier is false.
2. $(\exists x \in \mathbb{R})$ $(x^2 = 5)$.

   - There exists a real number x such that $x^2 = 5$.
   - $x^2 = 5$ for some real number x.
   - There is a real number whose square equals 5.

   The second example is usually not used since it is not considered good writing practice to start a sentence with a mathematical symbol.
   If the universal set is $\mathbb{R}$, then the truth set of the predicate "$x^2 = 5$" is $\{-sqrt5, sqrt5\}$. So these are all true statements.

Negations of Quantified Statements

In Preview Activity $2.4.1$, we wrote negations of some quantified statements. This is a very important mathematical activity. As we will see in future sections, it is sometimes just as important to be able to describe when some object does not satisfy a certain property as it is to describe when the object satisfies the property. Our next task is to learn how to write negations of quantified statements in a useful English form.

We first look at the negation of a statement involving a universal quantifier. The general form for such a statement can be written as $(\forall x \in U)\,(P(x))$, where $P(x)$is an open sentence and U is the universal set for the variable x. When we write

$$\neg(\forall x \in U)[P(x)],$$

we are asserting that the statement $\forall x \in U)[P(x)]$ is false. This is equivalent to saying that the truth set of the open sentence $P(x)$ is not the universal set. That is, there exists an element x in the universal set U such that $P(x)$ is false. This in turn means that there exists an element x in U such that $\neg P(x)$ is true, which is equivalent to saying that $(\exists x \in U)[\neg P(x)]$ is true. This explains why the following result is true:

$$\neg(\forall x \in U)[P(x)] \equiv (\exists x \in U)[\neg P(x)]$$

Similarly, when we write

$$\neg(\exists x \in U)[P(x)]$$

we are asserting that the statement $(\exists x \in U)[P(x)]$ is false. This is equivalent to saying that the truth set of the open sentence $P(x)$ is the empty set. That is, there is no element x in the universal set U such that $P(x)$ is true. This in turn means that for each element x in U, $\neg P(x)$ is true, and this is equivalent to saying that $(\forall x \in U)[\neg P(x)]$ is true. This explains why the following result is true:

$$\neg(\exists x \in U)[P(x)] \equiv (\forall x \in U)[\neg P(x)]$$

We summarize these results in the following theorem.

Theorem 2.16.

For any open sentence $P(x)$,

$$\neg(\forall x \in U)[P(x)] \equiv (\exists x \in U)[\neg P(x)], \text{ and}$$
$$\neg(\exists x \in U)[P(x)] \equiv (\forall x \in U)[\neg P(x)]$$

Example 2.17 (Negations of Quantified Statements)

Consider the following statement: $(\forall x \in \mathbb{R})(x^3 \geq x^2)$.

We can write this statement as an English sentence in several ways. Following are two different ways to do so.

- For each real number x, $x^3 \geq x^2$.
- If x is a real number, then x^3 is greater than or equal to x^2.

The second statement shows that in a conditional statement, there is often a hidden universal quantifier. This statement is false since there are real numbers x for which x^3 is not greater than or equal to x^2. For example, we could use $x = -1$ or $x = \frac{1}{2}$. This means that the negation must be true. We can form the negation as follows:

$$\neg(\forall x \in \mathbb{R})(x^3 \geq x^2) \equiv (\exists x \in \mathbb{R})\neg(x^3 \geq x^2)\ .$$

In most cases, we want to write this negation in a way that does not use the negation symbol. In this case, we can now write the open sentence $\neg(x^3 \geq x^2)$ as $(x^3 < x^2)$. (That is, the negation of "is greater than or equal to" is "is less than.") So we obtain the following:

$$\neg(\forall x \in \mathbb{R})(x^3 \geq x^2) \equiv (\exists x \in \mathbb{R})(x^3 < x^2)\ .$$

The statement $(\exists x \in \mathbb{R})(x^3 < x^2)$ could be written in English as follows:

- There exists a real number x such that $x^3 < x^2$.
- There exists an x such that x is a real number and $x^3 < x^2$.

Progress Check 2.18 (Negating Quantified Statements)

For each of the following statements

- Write the statement in the form of an English sentence that does not use the symbols for quantifiers.
- Write the negation of the statement in a symbolic form that does not use the negation symbol.

- Write the negation of the statement in the form of an English sentence that does not use the symbols for quantifiers.

1. $(\forall a \in \mathbb{R})(a+0=a)$.
2. $(\forall x \in \mathbb{R})[sin(2x)=2(sinx)(cosx)]$.
3. $(\forall x \in \mathbb{R})(tan^2x+1=sec^2x)$.
4. $(\exists x \in \mathbb{Q})(x^2-3x-7=0)$.
5. $(\exists x \in \mathbb{R})(x^2+1=0)$.

Answer

Add texts here. Do not delete this text first.

Counterexamples and Negations of Conditional Statements

The real number $x=-1$ in the previous example was used to show that the statement $(\forall x \in \mathbb{R})(x^3 \geq x^2)$ is false. This is called a **counterexample** to the statement. In general, a **counterexample** to a statement of the form $(\forall x)[P(x)]$ is an object a in the universal set U for which $P(a)$ is false. It is an example that proves that $(\forall x)[P(x)]$ is a false statement, and hence its negation, $(\exists x)[\neg P(x)]$, is a true statement.

In the preceding example, we also wrote the universally quantified statement as a conditional statement. The number $x=-1$ is a counterexample for the statement

If x is a real number, then x^3 is greater than or equal to x^2.

So the number -1 is an example that makes the hypothesis of the conditional statement true and the conclusion false. Remember that a conditional statement often contains a "hidden" universal quantifier. Also, recall that in Section 2.2 we saw that the negation of the conditional statement "If P then Q" is the statement "P and not Q." Symbolically, this can be written as follows:

$$\neg(P \rightarrow Q) \equiv P \wedge \neg Q\,.$$

So when we specifically include the universal quantifier, the symbolic form of the negation of a conditional statement is

$$\neg(\forall x \in U)[P(x) \rightarrow Q(x)] \equiv (\exists x \in U)\neg[P(x) \rightarrow Q(x)] \equiv (\exists x \in U)[P(x) \wedge \neg Q(x)]\,.$$

That is,

$$\neg(\forall x \in U)[P(x) \rightarrow Q(x)] \equiv (\exists x \in U)[P(x) \wedge \neg Q(x)].$$

? Progress Check 2.19 (Using Counterexamples)

Use counterexamples to explain why each of the following statements is false.

1. For each integer n, $(n^2+n+1\ )$ is a prime number.
2. For each real number x, if x is positive, then $2x^2 > x$.

Answer

Add texts here. Do not delete this text first.

Quantifiers in Definitions

Definitions of terms in mathematics often involve quantifiers. These definitions are often given in a form that does not use the symbols for quantifiers. Not only is it important to know a definition, it is also important to be able to write a negation of the definition. This will be illustrated with the definition of what it means to say that a natural number is a perfect square.

Definition: perfect square

A natural number n is a *perfect square* provided that there exists a natural number k such that $n=k^2$.

This definition can be written in symbolic form using appropriate quantifiers as follows:

A natural number n is a **perfect square** provided $(\exists k \in \mathbb{N})(n=k^2)$.

We frequently use the following steps to gain a better understanding of a definition.

1. Examples of natural numbers that are perfect squares are 1, 4, 9, and 81 since $1 = 1^2$, $4 = 2^2$, $9 = 3^2$, and $81 = 9^2$.
2. Examples of natural numbers that are not perfect squares are 2, 5, 10, and 50.
3. This definition gives two "conditions." One is that the natural number n is a perfect square and the other is that there exists a natural number k such that $n = k^2$. The definition states that these mean the same thing. So when we say that a natural number n is not a perfect square, we need to negate the condition that there exists a natural number k such that $n = k^2$. We can use the symbolic form to do this.

$$\neg(\exists k \in \mathbb{N})(n = k^2) \equiv (\forall k \in \mathbb{N})(n \neq k^2)$$

Notice that instead of writing $\neg(n = k^2)$, we used the equivalent form of $(n \neq k^2)$. This will be easier to translate into an English sentence. So we can write,

A natural number n is not a perfect square provided taht for every natural number k, $n \neq k^2$.

The preceding method illustrates a good method for trying to understand a new definition. Most textbooks will simply define a concept and leave it to the reader to do the preceding steps. Frequently, it is not sufficient just to read a definition and expect to understand the new term. We must provide examples that satisfy the definition, as well as examples that do not satisfy the definition, and we must be able to write a coherent negation of the definition

? Progress Check 2.20 (Multiples of Three)

Definition

An integer n is a **multiple of 3** provided that there exists an integer k such that $n = 3k$.

1. Write this definition in symbolic form using quantifiers by completing the following:

   An integer n is a multiple of 3 provided that ...
2. Give several examples of integers (including negative integers) that are multiples of 3.
3. Give several examples of integers (including negative integers) that are not multiples of 3.
4. Use the symbolic form of the definition of a multiple of 3 to complete the following sentence: "An integer n is not a multiple of 3 provided that . . . ."
5. Without using the symbols for quantifiers, complete the following sentence: "An integer \(n\0 is not a multiple of 3 provide that . . . ."

Answer

Add texts here. Do not delete this text first.

Statements with More than One Quantifier

When a predicate contains more than one variable, each variable must be quantified to create a statement. For example, assume the universal set is the set of integers, $\mathbb{Z}$, and let $P(x, y)$ be the predicate, "$x + y = 0$." We can create a statement from this predicate in several ways.

1. $(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = 0)$.
   We could read this as," For all integers x and y, $x + y = 0$." This is a false statement since it is possible to find two integers whose sum is not zero $2 + 3 \neq 0$.
2. $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y = 0)$.
   We could read this as, "For every integer x, there exists an integer y such that $x + y = 0$." This is a true statement.
3. $(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = 0)$.
   We could read this as, "There exists an integer x such that for each integer y, $x + y = 0$." This is a false statement since there is no integer whose sum with each integer is zero.
4. $(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y = 0)$.
   We could read this as, "There exist integers x and y such that $x + y = 0$." This is a true statement. For example, $2 + (-2) = 0$

When we negate a statement with more than one quantifier, we consider each quantifier in turn and apply the appropriate part of Theorem 2.16. As an example, we will negate Statement (3) from the preceding list. The statement is

$$(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = 0) \ .$$

We first treat this as a statement in the following form: $(\exists x \in \mathbb{Z})(P(x))$ where $P(x)$ is the predicate $(\forall y \in \mathbb{Z})(x + y = 0)$. Using Theorem 2.16, we have

$$\neg(\exists x \in \mathbb{Z})(P(x)) \equiv (\forall x \in \mathbb{Z})(\neg P(x)).$$

Using Theorem 2.16 again, we obtain the following:

$$\begin{aligned} \neg P(x) &\equiv \neg(\forall y \in \mathbb{Z})(x + y = 0) \\ &\equiv (\exists y \in \mathbb{Z})\neg(x + y = 0) \\ &\equiv (\exists y \in \mathbb{Z})(x + y \neq 0) \ . \end{aligned}$$

Combining these two results, we obtain

$$\neg(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = 0) \equiv (\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y \neq 0) \quad .$$

The results are summarized in the following table.

	Symbolic Form	**English Form**
Statement	$(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = 0)$	There exists an integer x such that for each integer y, $x + y = 0$.
Negation	$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y \neq 0)$	For each integer x, there exists an integer y such that $x + y \neq 0$.

Since the given statement is false, its negation is true.
We can construct a similar table for each of the four statements. The next table shows Statement (2), which is true, and its negation, which is false.

	Symbolic Form	**English Form**
Statement	$(\exists x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = 0)$	For every integer x, there exists an integer y such that $x + y = 0$.
Negation	$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y \neq 0)$	There exists an integer x such that for every integer y, $x + y \neq 0$.

? Progress Check 2.21 (Negating a Statement with Two Quantifiers)

Write the negation of the statement

$$(\forall x \in \mathbb{Z})(\forall y \in \mathbb{Z})(x + y = 0)$$

in symbolic form and as a sentence written in English.

Answer

Add texts here. Do not delete this text first.

Writing Guideline

Try to use English and minimize the use of cumbersome notation. Do not use the special symbols for quantifiers $\forall$ (for all), $\exists$ (there exists), *backepsilon* (such that), or $\therefore$ (therefore) in formal mathematical writing. It is often easier to write and usually easier to read, if the English words are used instead of the symbols. For example, why make the reader interpret

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 0)$$

when it is possible to write

For each real number x, there exists a real number y such that $x + y = 0$, or, more succinctly (if appropriate),

Every real number has an additive inverse.

Exercises for Section 2.4

1. For each of the following, write the statement as an English sentence and then explain why the statement is false.

   (a) $(\exists x \in \mathbb{Q})(x^2 - 3x - 7 = 0)$.
   (b) $(\exists x \in \mathbb{R})(x^2 + 1 = 0)$.
   (c) $(\exists m \in \mathbb{N})(m < 1)$.

2. For each of the following, use a counterexample to show that the statement is false. Then write the negation of the statement in English, without using symbols for quantifiers.

   (a) $(\forall m \in \mathbb{Z})$ (m^2 is even).
   (b) $(\forall x \in \mathbb{R})(x^2 > 0)$.
   (c) For each real number x, $\sqrt{x} \in \mathbb{R}$.
   (d) $(\forall m \in \mathbb{Z})(\frac{m}{3} \in \mathbb{Z})$.
   (e) $(\forall a \in \mathbb{Z})(\sqrt{a^2} = a)$.
   (f) $(\forall x \in \mathbb{R})(tan^2 x + 1 = sec^2 x)$.

3. For each of the following statements
   - Write the statement as an English sentence that does not use the symbols for quantifiers.
   - Write the negation of the statement in symbolic form in which the negation symbol is not used.
   - Write a useful negation of the statement in an English sentence that does not use the symbols for quantifiers.

   (a) $(\exists x \in \mathbb{Q})(x > \sqrt{2})$.
   (b) $(\forall x \in \mathbb{Q})(x^2 - 2 \neq 0)$.
   (c) $(\forall x \in \mathbb{Z})$ (x is even or x is odd).
   (d) $(\exists x \in \mathbb{Q})(\sqrt{2} < x < \sqrt{3})$. **Note**: The sentence "$\sqrt{2} < x < \sqrt{3}$ " is actually a conjunction. It means $\sqrt{2} < x$ and $x < \sqrt{3}$.
   (e) $(\forall x \in \mathbb{Z})$ (If x^2 is odd, then x is odd).
   (f) $(\forall n \in \mathbb{N})$ [If n is a perfect sqare, then $(2^n - 1)$ is not a prime number].
   (g) $(\forall n \in \mathbb{N})$ ($n^2 - n + 41$ is a prime number).
   (h) $(\exists x \in \mathbb{R})(cos(2x) = 2(cosx))$.

4. Write each of the following statements as an English sentence that does not use the symbols for quantifiers.

   (a) $(\exists m \in \mathbb{Z})(\exists n \in \mathbb{Z})(m > n)$
   (b) $(\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})(m > n)$
   (c) $(\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z})(m > n)$
   (d) $(\forall m \in \mathbb{Z})(\forall n \in \mathbb{Z})(m > n)$
   (e) $(\exists m \in \mathbb{Z})(\forall n \in \mathbb{Z})(m^2 > n)$
   (f) $(\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z})(m^2 > n)$

5. Write the negation of each statement in Exercise (4) in symbolic form and as an English sentence that does not use the symbols for quantifiers.

6. Assume that the universal set is $\mathbb{Z}$. Consider the following sentence:

   $(\exists t \in \mathbb{Z})(t \cdot x = 20)$.

   (a) Explain why this sentence is an open sentence and not a statement.
   (b) If 5 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
   (c) If 8 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
   (d) If 2 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
   (e) What is the truth set of the open sentence $(\exists t \in \mathbb{Z})(t \cdot x = 20)$?

7. Assume that the universal set is $\mathbb{R}$. Consider the following sentence:

   $(\exists t \in \mathbb{R})(t \cdot x = 20)$.

(a) Explain why this sentence is an open sentence and not a statement.
(b) If 5 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
(c) If π is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
(d) If 0 is substituted for x, is the resulting sentence a statement? If it is a statement, is the statement true or false?
(e) What is the truth set of the open sentence $(\exists t \in \mathbb{R})(t \cdot x = 20)$?

8. Let $\mathbb{Z}^*$ be the set of all nonzero integers.

   (a) Use a counterexample to explain why the following statement is false:
   For each $x \in \mathbb{Z}^*$, there exists a $y \in \mathbb{Z}^*$ such that $xy = 1$.
   (b) Write the statement in part(a) in symbolic form using appropriate symbols for quantifiers.
   (c) Write the negation of the statement in part (b) in symbolic form using appropriate symbols for quantifiers.
   (d) Write the negation from part(c) in English without usings the symbols for quantifiers.
9. An integer m is said to have the *divides property* provided that for all integers a and b, if m divides ab, then m divides a or m divides b.

   (a) Using the symbols for quantifiers, write what it means to say that the integer m has the divides property.
   (b) Using the symbols for quantifiers, write what it means to say that the integer m does not have the divides property.
   (c) Write an English sentence stating what it means to say that the integer m does not have the divides property.
10. In calculus, we define a function f with domain $\mathbb{R}$ to be **strictly increasing** provided that for all real numbers x and y, $f(x) < f(y)$ whenever $x < y$. Complete each of the following sentences using the appropriate symbols for quantifiers:
    (a) A function f with domain $\mathbb{R}$ is strictly increasing provided that ...
    (b) A function f with domain $\mathbb{R}$ is not strictly increasing provided that ...

    Complete the following sentence in English without using symbols for quantifiers:

    (c) A function f with domain $\mathbb{R}$ is not strictly increasing provided that ...
11. In calculus, we define a function f to be **continuous** at a real number a provided that for every $\varepsilon > 0$, there exists a $\delta > 0$ such that if $|x - a| < \delta$, then $|f(x) - f(a)| < \varepsilon$.

    Note: The symbol ε is the lowercase Greek letter epsilon, and the symbol δ is the lowercase Greek letter delta.

    Complete each of the following sentences using the appropriate symbols for quantifiers:

    (a) A function f is continuous at the real number a provided that ...
    (b) A function f is not continuous at the real number a provided that ...

    Complete the following sentence in English without using symbols for quantifiers:

    (c) A function f is not continuous at the real number a provided that ...
12. The following exercises contain definitions or results from more advanced mathematics courses. Even though we may not understand all of the terms involved, it is still possible to recognize the structure of the given statements and write a meaningful negation of that statement.

    (a) In abstract algebra, an operation $*$ on a set A is called a **commutative operation** provided that for all $x, y \in A$, $x * y = y * x$. Carefully explain what it means to say that an operation $*$ on a set A is not a commutative operation.

    (b) In abstract algebra, a **ring** consists of a nonempty set R and two operations called addition and multiplication. A nonzero element a in a ring R is called a zero divisor provided that there exists a nonzero element b in R such that $ab = 0$. Carefully explain what it means to say that a nonzero element a in a ring R is not a zero divisor.

    (c) A set M of real numbers is called a **neighborhood** of a real number aprovided that there exists a positive real number ϵ such that the open interval $(a - \epsilon, a + \epsilon\ )$ is contained in M. Carefully explain what it means to say that a set M is not a

neighborhood of a real number a.

(d) In advanced calculus, a sequence of real numbers $\{x_1, x_2, ..., x_k, ...\}$ is called a **Cauchy sequence** provided that for each positive real number, there exists a natural number N such that for all $m; n \in \mathbb{N}$, if $m > N$ and $n > N$, then $|x_n - x_m| < \epsilon$. Carefully explain what it means to say that the sequence of real numbers $\{x_1, x_2, ..., x_k, ...\}$ is not a Cauchy sequence.

Explorations and Activities

13. **Prime Numbers.** The following definition of a prime number is very important in many areas of mathematics. We will use this definition at various places in the text. It is introduced now as an example of how to work with a definition in mathematics.

> **Definition**
>
> A natural number p is a **prime number** provided that it is greater than 1 and the only natural numbers that are factors of p are 1 and p. A natural number other than 1 that is not a prime number is a **composite number**. The number 1 is neither prime nor composite.

Using the definition of a prime number, we see that 2, 3, 5, and 7 are prime numbers. Also, 4 is a composite number since $4 = 2 \cdot 2$; 10 is a composite number since $10 = 2 \cdot 5$; and 60 is a composite number since $60 = 4 \cdot 15$.

(a) Give examples of four natural numbers other than 2, 3, 5, and 7 that are prime numbers.
(b) Explain why a natural number p that is greater than 1 is a prime number provided that
For all $d \in \mathbb{N}$, if d is a factor of p, then $d = 1$ or $d = p$.
(c) Give examples of four natural numbers that are composite numbers and explain why they are composite numbers.
(d) Write a useful description of what it means to say that a natural number is a composite number (other than saying that it is not prime).

14. **Upper Bounds for Subsets of** $\mathbb{R}$. Let A be a subset of the real numbers. A number b is called an **upper bound** for the set A provided that for each element x in A, $x \leq b$.

(a) Write this definition in symbolic form by completing the following:
Let A be a subset of the real numbers. A number b is called an upper bound for the set A provided that ...
(b) Give examples of three different upper bounds for the set $A = \{x \in \mathbb{R} | 1 \leq x \leq 3\}$.
(c) Does the set $B = \{x \in \mathbb{R} | x > 0\}$ have an upper bound? Explain.
(d) Give examples of three different real numbers that are not upper bounds for the set $A = \{x \in \mathbb{R} | 1 \leq x \leq 3\}$.
(e) Complete the following in symbolic form: "Let A be a subset of $\mathbb{R}$. A number b is not an upper bound for the set A provided that ..."
(f) Without using the symbols for quantifiers, complete the following sentence: "Let A be a subset of $\mathbb{R}$. A number b is not an upper bound for the set A provided that ..."
(g) Are your examples in Part(14d) consistent with your work in Part(14f)? Explain.

15. **Least Upper Bound for a Subset of** $\mathbb{R}$. In Exercise 14, we introduced the definition of an upper bound for a subset of the real numbers. Assume that we know this definition and that we know what it means to say that a number is not an upper bound for a subset of the real numbers.

Let A be a subset of $\mathbb{R}$. A real number α is the **least upper bound** for A provided that α is an upper bound for A, and if β is an upper bound for A, then $\alpha \leq \beta$.

Note: The symbol α is the lowercase Greek letter alpha, and the symbol β is the lowercase Greek letter beta.

If we define $P(x)$ to be "x is an upper bound for A," then we can write the definition for least upper bound as follows:

A real number α is the **least upper bound** for A provided that
$P(\alpha) \wedge [(\forall \beta \in \mathbb{R})(P(\beta) \rightarrow (\alpha \leq \beta))]$.

(a) Why is a universal quantifier used for the real number β?
(b) Complete the following sentence in symbolic form: “A real number α is not the least upper bound for A provided that ...
(c) Complete the following sentence as an English sentence: "A real number α is not the least upper bound for A provided that ..."

Answer

Add texts here. Do not delete this text first.

SECTION OVERVIEW

2.5: Structures and Languages

2.5.1: Summing Up, Looking Ahead

What we have tried to do in this first chapter is to introduce the concepts of formal languages and formal structures. We hope that you will agree that you have seen many mathematical structures in the past, even though you may not have called them structures at the time. By formalizing what we mean when we say that a formula is true in a structure, we will be able to tie together truth and provability in the next couple of chapters.

You might be at a point where you are about to throw your hands up in disgust and say, "Why does any of this matter? I've been doing mathematics for over ten years without worrying about structures or assignment functions, and I have been able to solve problems and succeed as a mathematician so far." Allow us to assure you that the effort and the almost unreasonable precision that we are imposing on our exposition will have a payoff in later chapters. The major theorems that we wish to prove are theorems about the existence or nonexistence of certain objects. To prove that you cannot express a certain idea in a certain language, we have to *know*, with an amazing amount of exactitude, what a language is and what structures are. Our goals are some theorems that are easy to state incorrectly, so by being precise about what we are saying, we will be able to make (and prove) claims that are truly revolutionary.

Since we will be talking about the existence and nonexistence of proofs, we now must turn our attention to defining (yes, precisely) what sorts of things qualify as proofs. That is the topic of the next chapter.

2.5.2: Naïvely

Let us begin by talking informally about mathematical structures and mathematical languages.

There is no doubt that you have worked with mathematical models in several previous mathematics courses, although in all likelihood it was not pointed out to you at the time. For example, if you have taken a course in linear algebra, you have some experience with $\mathbb{R}^2$, $\mathbb{R}^3$, and $\mathbb{R}^n$ as examples of vector spaces. In high school geometry you learned that the plane is a "model" of Euclid's axioms of geometry. Perhaps you have taken a class in abstract algebra, where you saw several examples of groups: The integers under addition, permutation groups, and the group of invertible $n \times n$ matrices with the operation of matrix multiplication are all examples of groups - they are "models" of the group axioms. All of these are mathematical models, or structures. Different structures are used for different purposes.

Suppose we think about a particular mathematical structure, for example $\mathbb{R}^3$, the collection of ordered triples of real numbers. If we try to do plane Euclidean geometry in $\mathbb{R}^3$, we fail miserably, as (for example) the parallel postulate is false in this structure. On the other hand, if we want to do linear algebra in $\mathbb{R}^3$, all is well and good, as we can think of the points of $\mathbb{R}^3$ as vectors and let the scalars be real numbers. Then the axioms for a real vector space are all true when interpreted in $\mathbb{R}^3$. We will say that $\mathbb{R}^3$ is a model of the axioms for a vector space, whereas it is not a model for Euclid's axioms for geometry.

As you have no doubt noticed, our discussion has introduced two separate types of things to worry about. First, there are the mathematical models, which you can think of as the mathematical worlds, or constructs. Examples of these include $\mathbb{R}^3$, the collection of polynomials of degree 17, the set of 3x2 matrices, and the real line. We have also been talking about the axioms of geometry and vector spaces, and these are something different. Let us discuss those axioms for a moment.

Just for the purposes of illustration, let us look at some of the axioms which state that V is a real vector space. They are listed here both informally and in a more formal language:

Vector addition is commutative: $(\forall u \in V)\,(\forall v \in V)\,u+v=v+u$.

There is a zero vector: $(\exists 0 \in V)\,(\forall v \in V)\,v+0=v$.

One times anything is itself: $(\forall v \in V)\,1v=v$.

Don't worry if the formal language is not familiar to you at this point; it suffices to notice that there *is* a formal language. But do let us point out a few things that you probably accepted without question. The addition sign that is in the first two axioms is not the same plus sign that you were using when you learned to add in first grade. Or rather, it *is* the same sign, but you *interpret* that sign differently. If the vector space under consideration is $\mathbb{R}^3$, you know that as far as the first two axioms up there are concerned, addition is vector addition. Similarly, the 0 in the second axiom is not the real number 0; rather, it is the zero vector. Also, the multiplication in the third axiom that is indicated by the juxtaposition of the 1 and the v is the scalar multiplication of the vector space, not the multiplication of third grade.

So it seems that we have to be able to look at some symbols in a particular formal language and then take those symbols and relate them in some way to a mathematical structure. Different interpretations of the symbols will lead to different conclusions as regards the truth of the formal statement. For example, if we take the commutivity axiom above and work with the space V being $\mathbb{R}^3$ but interpret the sign $+$ as standing for cross product instead of vector addition, we see that the axiom is no longer true, as cross product is not commutative.

These, then, are our next objectives: to introduce formal languages, to give an official definition of a mathematical structure, and to discuss truth in those structures. Beauty will come later.

2.5.3: Languages

We will be constructing a very restricted formal language, and our goal in constructing that language will be to be able to form certain statements about certain kinds of mathematical structures. For our work, it will be necessary to be able to talk about constants, functions, and relations, and so we will need symbols to represent them.

> *Chaff:* Let us emphasize this once more. Right now we are discussing the *syntax* of our language, the marks on the paper. We are not going to worry about the semantics, or meaning, of those marks until later - at least not formally. But it is silly to pretend that the intended meanings do not drive our choice of symbols and the way in which we use them. If we want to discuss left-hemi-semi-demi-rings, our formal language should include the function and relation symbols that mathematicians in this lucrative and exciting field customarily use, not the symbols involved in chess, bridge, or right-hemi-semi-para-fields. It is not our goal to confuse anyone more than is necessary. So you should probably go through the exercise right now of taking a guess at a reasonable language to use if our intended field of discussion was, say, the theory of the natural numbers. See Exercise 1.

Definition 1.2.1. A **first-order language** $\mathcal{L}$ is an infinite collection of distinct symbols, no one of which is properly contained in another, separated into the following categories:

1. *Parentheses: (,).*
2. *Connectives:* $\vee$, $\neg$.
3. *Quantifier:* $\forall$.
4. *Variables, one for each positive integer* n*:* $v_1, v_2, \ldots, v_n, \ldots$. The set of variable symbols will be denoted *Vars.*
5. *Equality symbol:* $=$.
6. *Constant symbols:* Some set of zero or more symbols.
7. *Function symbols:* For each positive integer n, some set of zero or more n-ary function symbols.
8. *Relation symbols:* For each positive integer n, some set of zero or more n-ary relation symbols.

To say that a function symbol is n-ary (or has arity n) means that it is intended to represent a function of n variables. For example, $+$ has arity 2. Similarly, an n-ary relation symbols will be intended to represent a relation on n-tuples of objects. This will be made formal in Definition 1.6.1.

To specify a language, all we have to do is determine which, if any, constant, function, and relation symbols we wish to use. Many authors, by the way, let the equality symbol be optional, or treat the equality symbol as an ordinary binary (i.e. 2-ary) relation symbol. We will assume that each language has the equality symbol, unless specifically noted.

> *Chaff:* We ought to add a word about the phrase "no one of which is properly contained in another", which appears in this definition. We have been quite vague about the meaning of the word *symbol*, but you are supposed to be thinking about marks made on a piece of paper. We will be constructing sequences of symbols and trying to figure out what they mean in the next few sections, and by not letting one symbol be contained in another, we will find our job of interpreting sequences to be much easier.
>
> For example, suppose that our language contained both the constant symbol $\heartsuit$ and the constant symbol $\heartsuit\heartsuit$ (notice that the first symbol is properly contained in the second). If you were reading a sequence of symbols and ran across $\heartsuit\heartsuit$, it would be impossible to decide if this was one symbol or a sequence of two symbols. By not allowing symbols to be contained in other symbols, this type of confusion is avoided, leaving the field open for other types of confusion to take its place.

Example 1.2.2. Suppose that we were taking an abstract algebra course and we wanted to specify the language of groups. A group consists of a set and a binary operation that has certain properties. Among those properties is the existence of an identity element for the operation. Thus, we could decide that our language will contain one constant symbols for the identity element, one binary operation symbol, and no relation symbols. We would get

$$\mathcal{L}_G \text{ is } \{0, +\}, \tag{2.5.3.1}$$

where 0 is the constant symbol and $+$ is a binary function symbol. Or perhaps we would like to write our groups using the operation as multiplication. Then a reasonable choice could be

$$\mathcal{L}_G \text{ is } \{1, ^{-1}, \cdot\}, \tag{2.5.3.2}$$

which includes not only the constant symbol 1 and the binary function symbol $\cdot$, but also a unary (or 1-ary) function symbol $^{-1}$, which is designed to pick out the inverse of an element of the group. As you can see, there is a fair bit of choice involved in designing a language.

Example 1.2.3. The language of set theory is not very complicated at all. We will include one binary relation symbol, $\in$, and that is all:

$$\mathcal{L}_{ST} \text{ is } \{\in\}. \tag{2.5.3.3}$$

The idea is that this symbol will be used to represent the elementhood relation, so the interpretation of the string $x \in y$ will be that the set x is an element of the set y. You might be tempted to add other relation symbols, such as $\subset$, or constant symbols, such as $\emptyset$, but it will be easier to define such symbols in terms of more primitive symbols. Not easier in terms of readability, but easier in terms of proving things about the language.

In general, to specify a language we need to list the constant symbols, the function symbols, and the relation symbols. There can be infinitely many [in fact, uncountably many (cf. the Appendix)] of each. So, here is a specification of a language:

$$\mathcal{L} \text{ is } \{c_1, c_2, \ldots, f_1^{a(f_1)}, f_2^{a(f_2)}, \ldots, R_1^{a(R_1)}, R_2^{a(R_2)}, \ldots\}. \tag{2.5.3.4}$$

Here, the c_i's are the constant symbols, the $f_i^{a(f_i)}$'s are the function symbols, and the $R_i^{a(R_i)}$'s are the relation symbols. The superscripts on the function and relation symbols indicate the arity of the associated symbols, so a is a mapping that assigns a natural number to a string that begins with an f or an R, followed by a subscripted ordinal. Thus, an official function symbol might look like this:

$$f_{17}^{223}, \tag{2.5.3.5}$$

which would say that the function that will be associated with the 17th function symbol is a function of 223 variables. Fortunately, such dreadful detail will rarely be needed. We will usually see only unary or binary function symbols and the arity of each symbol will be stated once. Then the authors will trust that the context will remind the patient reader of each symbol's arity.

Exercises

1. Carefully write out the symbols that you would want to have in a language $\mathcal{L}$ that you intend to use to write statements of elementary algebra. Indicate which of the symbols are constant symbols, and the arity of the function and relation symbols that you choose. Now write out another language, $\mathcal{M}$ (i.e., another list of symbols) with the same number of constant symbols, function symbols, and relation symbols that you would *not* want to use for elementary algebra. Think about the value of good notation.
2. What are good examples of unary (1-ary) functions? Binary functions? Can you find natural examples of relations with arity 1, 2, 3, and 4? As you think about this problem, stay mindful of the difference between the function and the function symbol, between the relation and the relation symbol.
3. In the town of Sneezblatt there are three eating establishments: McBurgers, Chez Fancy, and Sven's Tandoori Palace. Think for a minute about statements that you might want to make about these restaurants, and then write out $\mathcal{L}$, the formal language for your theory of restaurants. Have fun with this, but try to include both function and relation symbols in $\mathcal{L}$. What interpretations are you planning for your symbols?
4. You have been put in charge of drawing up the schedule for a basketball league. This league involves eight teams, each of which must play each of the other seven teams exactly two times: once at home and once on the road. Think of a reasonable language for this situation. What constants would you need? Do you need any relation symbols? Function symbols? It would be nice if your finished schedule did not have any team playing two games on the same day. Can you think of a way to state this using the formal symbols that you have chosen? Can you express the sentence which states that each team plays every other team exactly two times?
5. Let's work out a language for elementary trigonometry. To get you started, let us suggest that you start off with *lots* of constant symbols - one for each real number. It is tempting to use the symbols 7 to stand for the number seven, but this runs into problems. (Do you see why this is illegal? 7, 77, 7/3, ...) Now, what functions would you like to discuss? Think of symbols for them. What are the arities of your function symbols? Do not forget that you need symbols for addition and multiplication! What relation symbols would you like to use?
6. A computer language is another example of a language. For example, the symbol $:=$ might be a binary function symbol, where the interpretation of the instruction

$$x := 7 \tag{2.5.3.6}$$

would be to alter the internal state of the computer by placing the value 7 into the position in memory referenced by the variable x. Think about the function associated with the binary function symbol

$$\text{if } \_\_\_\_\_, \text{ then } \_\_\_\_\_. \tag{2.5.3.7}$$

What are the inputs into this function? What sort of thing does the function do? Look at the statement

$$\text{If } x + y > 3, \text{ then } z := 7. \tag{2.5.3.8}$$

Identify the function symbols, constant symbols, and relation symbols. What are the arities of each function and relation symbol?

7. What would be a good language for the theory of vector spaces? This problem is slightly more difficult, as there are two different varieties of objects, scalars and vectors, and you have to be able to tell them apart. Write out the axioms of vector spaces in your language. Or, better yet, use a language that includes a unary function symbol for each real number so that scalars don't exist as objects at all!
8. It is not actually necessary to include function symbols in the language, since a function is just a special kind of relation. Just to see an example, think about the function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(x) = x^2$. Remembering that a relation on $\mathbb{N} \times \mathbb{N}$ is just a set of ordered pairs of natural numbers, find a relation R on $\mathbb{N} \times \mathbb{N}$ such that (x, y) is an element of R if and only if $y = f(x)$. Convince yourself that you could do the same for any function defined on any domain. What condition must be true if a relation R on $A \times B$ is to be a function mapping A to B?

$$\cdot\left(+\bar{3}\bar{2}\right)\bar{4}, \tag{2.5.4.3}$$

which ought to have the same meaning as $\cdot\bar{5}\bar{4}$, which is $\bar{2}\bar{0}$, just as you suspected.

Rest assured that we will continue to use infix notation, commas, and parentheses as seem warranted to increase the readability (by humans) of this text. So $ft_1t_2\ldots t_n$ will be written $f\left(t_1, t_2, \ldots, t_n\right)$ and $+\bar{3}\bar{2}$ will be written $\bar{3}+\bar{2}$, with the understanding that this is shorthand and that our official version is the version given in Definition 1.3.1.

The terms of $\mathcal{L}$ play the role of the nouns of the language. To make meaningful mathematical statements about some mathematical structure, we will want to be able to make assertions about the objects of the structure. These assertions will be the formulas of $\mathcal{L}$.

Definition 1.3.3. If $\mathcal{L}$ is a first-order language, a **formula of $\mathcal{L}$** is a nonempty finite string ϕ of symbols from $\mathcal{L}$ such that either:

1. $\phi :\equiv = t_1t_2$, where t_1 and t_2 are terms of $\mathcal{L}$, or
2. $\phi :\equiv Rt_1t_2\ldots t_n$, where R is an n-ary relation symbol of $\mathcal{L}$ and $t_1, t_2, \ldots, t_n$ are all terms of $\mathcal{L}$, or
3. $\phi :\equiv (\neg\alpha)$, where α is a formula of $\mathcal{L}$, or
4. $\phi :\equiv (\alpha\vee\beta)$, where α and β are formulas of $\mathcal{L}$, or
5. $\phi :\equiv (\forall v)(\alpha)$, where v is a variable and α is a formula of $\mathcal{L}$.

If a formula ψ contains the subformula $(\forall v)(\alpha)$ [meaning that the string of symbols that constitute the formula $(\forall v)(\alpha)$ is a substring of the string of symbols that make up ψ], we will say that the **scope** of the quantifier $\forall$ is α. Any symbol in α will be said to lie within the scope of the quantifier $\forall$. Notice that a formula ψ can have several different occurrences of the symbol $\forall$, and each occurrence of the quantifier will have its own scope. Also notice that one quantifier can lie within the scope of another.

The **atomic formulas of $\mathcal{L}$** are those formulas that satisfy clause (1) or (2) of Definition 1.3.3.

You have undoubtedly noticed that there are no parentheses or commas in the atomic formulas, and you have probably decided that we will continue to use both commas and infix notation as seems appropriate. You are correct on both counts. So, instead of writing the official version

$$<SSSSS0SS0 \tag{2.5.4.4}$$

in a language containing constant symbol 0, unary function symbol S, and binary relation symbol <, we will write

$$SSSSS0<SS0 \tag{2.5.4.5}$$

or (after some preliminary definitions)

$$\bar{5}<\bar{2} \tag{2.5.4.6}$$

Also notice that we *are* using infix notation for the binary logical connective $\vee$. We hope that this will make your life somewhat easier.

You will be asked in Exercise 8 in Section 1.4 to prove that unique readability holds for formulas as well as terms. We will, in our exposition, use different-size parentheses, different shapes of delimiters, and omit parentheses in order to improve readability without (we hope) introducing confusion on your part.

Notice that a term is not a formula! If the terms are the nouns of the language, the formulas will be the statements. Statements can be either true or false. Nouns cannot. Much confusion can be avoided if you keep this simple dictum in mind.

For example, suppose that you are looking at a string of symbols and you notice that the string does not contain either the symbol = or any other relation symbol from the language. Such a string cannot be a formula, as it makes no claim that can be true or false. The string might be a term, it might be nonsense, but it cannot be a formula.

> *Chaff:* We do hope that you have noticed that we are dealing only with the syntax of our language here. We have not mentioned that the symbol $\neg$ will be used for denial, or that $\vee$ will mean "or", or even that $\forall$ means "for every". Don't worry, they will mean what you think they should mean. Similarly, do not worry about the fact that the definition of a formula left out symbols for conjunctions, implications, and biconditionals. We will get to them in good time.

Exercises

1. Suppose that the language $\mathcal{L}$ consists of two constant symbols, $\diamondsuit$ and $\heartsuit$, a unary relation symbol ¥, a binary function symbol ♭, and a 3-ary function symbol ♯. Write down at least three distinct terms of the language $\mathcal{L}$. Write down a couple of nonterms

2.5.4: Terms and Formulas

Suppose that $\mathcal{L}$ is the language $\{0, +, <\}$, and we are going to use $\mathcal{L}$ to discuss portions of arithmetic. If we were to write down the string of symbols from $\mathcal{L}$,

$$(v_1 + 0) < v_1, \tag{2.5.4.1}$$

and the string

$$v_{17})(\forall + +(((0, \tag{2.5.4.2}$$

you would probably agree that the first string conveyed some meaning, even if that meaning were incorrect, while the second string was meaningless. It is our goal in this section to carefully define which strings of symbols of $\mathcal{L}$ we will use. In other words, we will select the strings that will have meaning.

Now, the point of having a language is to be able to make statements about certain kinds of mathematical systems. Thus, we will want the statements in our language to have the ability to refer to objects in the mathematical structures under consideration. So we will need some of the strings in our language to refer to those objects. Those strings are called the terms of $\mathcal{L}$.

Definition 1.3.1. If $\mathcal{L}$ is a language, a **term of $\mathcal{L}$** is a nonempty finite string t of symbols from $\mathcal{L}$ such that either:

1. t is a variable, or
2. t is a constant symbol, or
3. $t :\equiv ft_1t_2 \dots t_n$, where f is an n-ary function symbol of $\mathcal{L}$ and each of the t_i is a term of $\mathcal{L}$.

A couple of things about this definition need to be pointed out. First, there is the symbol $:\equiv$ in the third clause. The symbol $:\equiv$ is *not* a part of the language $\mathcal{L}$. Rather it is a meta-linguistic symbol that means that the strings of $\mathcal{L}$-symbols on each side of the $:\equiv$ are identical. Probably the best natural way to read clause 3 would be to say that "t is $ft_1t_2 \dots t_n$".

The other thing to notice about Definition 1.3.1 is that this is a definition by recursion, since in the third clause of the definition, t is a tern if it contains substrings that are terms. Since the substrings of t are shorter (contain fewer symbols) than t, and as none of the symbols of $\mathcal{L}$ are made up of other symbols of $\mathcal{L}$, this causes no problems.

Example 1.3.2. Let $\mathcal{L}$ be the language $\{\bar{0}, \bar{1}, \bar{2}, \dots, +, \cdot\}$, with one constant symbol for each natural number and two binary function symbols. Here are some of the terms of $\mathcal{L}$: $7\bar{1}4$, $+\bar{3}\bar{2}$, $\cdot + \bar{3}\bar{2}\bar{4}$. Notice that $\bar{1}\bar{2}\bar{3}$ is not a term of $\mathcal{L}$, but rather is a sequence of three terms in a row.

> *Chaff:* The term $+\bar{3}\bar{2}$ looks pretty annoying at this point, but we will use this sort of notation (called *Polish notation*) for functions rather than the infix notation $(\bar{3} + \bar{2})$ that you are used to. We are not really being odd here: You have certainly seen some functions written in Polish notation: $\sin(x)$ and $f(x, y, z)$ come to mind. We are just being consistent in treating addition in the same way. What makes it difficult is that it is hard to remember that addition really is just another function of two variables. But we are sure that by the end of this book, you will be very comfortable with that idea and with the notation that we are using.

A couple of points are probably worth emphasizing, just this once. Notice that in the application of the function symbols, there are no parentheses and no commas. Also notice that all of our functions are written with the operator on the left. So instead of $\bar{3} + \bar{2}$, we write $+\bar{3}\bar{2}$. The reason for this is for consistency and to make sure that we can parse our expressions.

Let us give an example. Suppose that, in some language or other, we wrote down the string of symbols $\heartsuit ¥ \uparrow \diamondsuit \# \# \int$. Assume that two of our colleagues, Humphrey and Ingrid, were waiting in the hall while we wrote down the string. If Humphrey came into the room and announced that our string was a 3-ary function symbol followed by three terms, whereas Ingrid proclaimed that the string was really a 4-ary relation symbol followed by two terms, this would be rather confusing. It would be *really* confusing if they were both correct! So we need to make sure that the strings that we write down can be interpreted in only one way. This property, called *unique readability*, is addressed in Exercise 7 of Section 1.4.

> *Chaff:* Unique readability is one of those things that, in the opinion of the authors, is important to know, interesting to prove, and boring to read. Thus the proof is placed in (we do not mean "relegated to") the exercises.

Suppose that we look more carefully at the term $\cdot + \bar{3}\bar{2}\bar{4}$. Assume for now that the symbols in this term are supposed to be interpreted in the usual way, so that $\cdot$ means multiply, $+$ means add, and $\bar{3}$ means three. Then if we add some parentheses to the term in order to clarify its meaning, we get

that look like they might be terms and explain why they are not terms. Write a couple of formulas and a couple of nonformulas that look like they ought to be formulas.

2. The fact that we write all of our operations on the left is important for unique readability. Suppose, for example, that we wrote our binary operations in the middle (and did not allow the use of parentheses). If our language included the binary function symbol $\#$, then the term

$$u\#v\#w \tag{2.5.4.7}$$

could be interpreted two ways. This can make a difference: Suppose that the operation associated with the function symbol $\#$ is "subtract". Find three real numbers u, v, and w such that the two different interpretations of $u\#v\#w$ lead to different answers. Any nonassociative binary function will yield another counterexample to unique readability. Can you think of three such functions?

3. The language of number theory is

$$\mathcal{L}_{NT} \text{ is } \{0, S, +, \cdot, E, <\}, \tag{2.5.4.8}$$

where the intended meanings of the symbols are as follows: 0 stands for the number zero, S is the successor function $S(x) = x + 1$, the symbols $+$, $\cdot$, and $<$ mean what you expect, and E stands for exponentiation, so $E(3, 2) = 9$. Assume that $\mathcal{L}_{NT}$-formulas will be interpreted with respect to the nonnegative integers and write an $\mathcal{L}_{NT}$-formula to express the claim that p is a prime number. Can you write the statement of Lagrange's Theorem, which states that every natural number is the sum of four squares?

Write a formula stating that there is no largest prime number. How would we express the Goldbach Conjecture, that every even number greater than two can be expressed as the sum of two primes?

What is the formal statement of the Twin Primes Conjecture, which says that there are infinitely many pairs (x, y) such that x and y are both prime and $y = x + 2$? The Bounded Gap Theorem, proven in 2013, says that there are infinitely many pairs of prime numbers that differ by 70,000,000 or less. Write a formal statement of that theorem.

Use shorthand in your answers to this problem. For example, after you have found the formula which says that p is prime, call the formula $Prime(p)$ and use $Prime(p)$ in your later answers.

4. Suppose that our language has infinitely many constant symbols of the form $',''',''',\ldots$ and no function or relation symbols other than =. Explain why this situation leads to problems by looking at the formula $=''''''$. Where in our definitions do we outlaw this sort of problem?

2.5.5: Induction

You are familiar, no doubt, with proofs by induction. They are the bane of most mathematics students from their first introduction in high school through the college years. It is our goal in this section to discuss the proofs by induction that you know so well, put them in a different light, and then generalize that notion of induction to a setting that will allow us to use induction to prove things about terms and formulas rather than just the natural numbers.

Just to remind you of the general form of a proof by induction on the natural numbers, let us state and prove a familiar theorem, assuming for the moment that the set of natural numbers is $\{1, 2, 3, \ldots\}$.

Theorem 1.4.1. *For every natural number n,*

$$1+2+\cdots+n=\frac{n\,(n+1)}{2}. \tag{2.5.5.1}$$

Proof. If $n=1$, simple computation shows that the equality holds. For the inductive case, fix $k \geq 1$ and assume that

$$1+2+\cdots+k=\frac{k\,(k+1)}{2}. \tag{2.5.5.2}$$

If we add $k+1$ to both sides of this equation, we get

$$1+2+\cdots+k+(k+1)=\frac{k\,(k+1)}{2}+(k+1)\,, \tag{2.5.5.3}$$

and simplifying the right-hand side of this equation shows that

$$1+2+\cdots+(k+1)=\frac{(k+1)\,((k+1)+1)}{2}\,, \tag{2.5.5.4}$$

finishing the inductive step, and the proof.

As you look at the proof of this theorem, you notice that there is a base case, when $n=1$, and an inductive case. In the inductive step of the proof, we prove the implication

If the formula holds for k, then the formula holds for $k+1$.

We prove this implication by assuming the antecedent, that the theorem holds for a (fixed, but unknown) number k, and from that assumption proving the consequent, that the theorem hods for the next number, $k+1$. Notice that this is *not* the same as assuming the theorem that we are trying to prove. The theorem is a universal statement - it claims that a certain formula holds for every natural number.

Looking at this from a slightly different angle, what we have done is to construct a set of numbers with a certain property. If we let S stand for the set of numbers for which our theorem holds, in our proof by induction we show the following facts about S:

1. The number 1 is an element of S. We prove this explicitly in the base case of the proof.
2. If the number k is an element of S, then the number $k+1$ is an element of S. This is the content of the inductive step of the proof.

But now, notice that we know that the collection of natural numbers can be defined as the smallest set such that:

1. The number 1 is a natural number.
2. If k is a natural number, then $k+1$ is a natural number.

So S, the collection of numbers for which the theorem holds, is identical with the set of natural numbers, thus the theorem holds for every natural number n, as needed. (If you caught the slight lie here, just substitute "superset" where appropriate.)

So what makes a proof by induction work is the fact that the natural numbers can be defined recursively. There is a base case, consisting of the smallest natural number ("1 is a natural number"), and there is a recursive case, showing how to construct bigger natural numbers from smaller ones ("If k is a natural number, then $k+1$ is a natural number").

Now, let us look at Definition 1.3.3, the definition of a formula. Notice that the five clauses of the definition can be separated into two groups. The first two clauses, the atomic formulas, are explicitly defined: For example, the first case says that anything that is of the form $=t_1t_2$ is a formula if t_1 and t_2 are terms. These first two clauses form the base case of the definition. The last three

clauses are the recursive case, showing how if α and β are formulas, they can be used to build more complex formulas, such as $(\alpha \vee \beta)$ or $(\forall v)(\alpha)$.

Now since the collection of formulas is defined recursively, we can use an inductive-style proof when we want to prove that something is true about *every* formula. The inductive proof will consist of two parts, a base case and an inductive case. In the base case of the proof we will verify that the theorem is true about every atomic formula - about every string that is known to be a formula from the base case of the definition. In the inductive step of the proof, we assume that the theorem is true about simple formulas (α and β), and use that assumption to prove that the theorem holds a more complicated formula ϕ that is generated by a recursive clause of the definition. This method of proof is called *induction on the complexity of the formula*, or *induction on the structure of the formula*.

There are (at least) two ways to think about the word "simple" in the last paragraph. One way in which a formula α might be simpler than a complicated formula ϕ is if α is a subformula of ϕ. The following theorem, although mildly interesting in its own right, is included here mostly so that you can see an example of a proof by induction in this setting:

Theorem 1.4.2. *Suppose that ϕ is a formula in the language $\mathcal{L}$. Then the number of left parentheses occurring in ϕ is equal to the number of right parentheses occurring in ϕ.*

Proof. We will present this proof in a fair bit of detail, in order to emphasize the proof technique. As you become accustomed to proving theorems by induction on complexity, not so much detail is needed.'

Base Case. We begin our inductive proof with the base case, as you would expect. Our theorem makes an assertion about all formulas, and the simplest formulas are the atomic formulas. They constitute our base case. Suppose that ϕ is an atomic formula. There are two varieties of atomic formulas: Either ϕ begins with an equals sign followed by two terms, or ϕ begins with a relation symbol followed by several terms. As there are no parentheses in any term (we are using the official definition of term, here), there are no parentheses in ϕ. Thus, there are as many left parentheses as right parentheses in ϕ, and we have established the theorem if ϕ is an atomic formula.

Inductive Case. The inductive step of a proof by induction on complexity of a formula takes the following form: Assume that ϕ is a formula by virtue of clause (3), (4), or (5) of Definition 1.3.3. Also assume that the statement of the theorem is true when applied to the formulas α and β. With those assumptions we will prove that the statement of the theorem is true when applied to the formula ϕ. Thus, as every formula is a formula either by virtue of being an atomic formula or by application of clause (3), (4), or (5) of the definition, we will have shown that the statement of the theorem is true when applied to any formula, which has been our goal.

So, assume that α and β are formulas that contain equal numbers of left and right parentheses. Suppose that there are k left parentheses and k right parentheses in α and l left parentheses and l right parentheses in β.

If ϕ is a formula by virtue of clause (3) of the definition, then $\phi :\equiv (\neg\alpha)$. We observe that there are $k+1$ left parentheses and $k+1$ right parentheses in ϕ, and thus ϕ has an equal number of left and right parentheses, as needed.

If ϕ is a formula because of clause (4), then $\phi :\equiv (\alpha \vee \beta)$, and ϕ contains $k+l+1$ left and right parentheses, an equal number of each type.

Finally, if $\phi :\equiv (\forall v)(\alpha)$, then ϕ contains $k+2$ left parentheses and $k+2$ right parentheses, as needed.

This concludes the possibilities for the inductive case of the proof, so we have established that in every formula, the number of left parentheses is equal to the number of right parentheses.

A second way in which we might structure a proof by induction on the structure of the formula is to say that α is simpler than ϕ if the number of connectives/quantifiers in α is less than the number in ϕ. In this case one could argue that the induction argument is really an ordinary induction on the natural numbers. Here is an outline of how such a proof might proceed:

Proof. We argue by induction on the structure of ϕ.

Base Case. Assume ϕ has 0 connectives/quantifiers. This means that ϕ is an atomic formula. {Insert argument establishing the theorem for atomic formulas.}

Inductive Case. Assume that ϕ has $k+1$ connectives/quantifiers. Then either $\phi :\equiv \neg\alpha$, or $\phi :\equiv \alpha \vee \beta$ or $\phi :\equiv (\forall x)\,\alpha$, and we can assume that the theorem holds for *every* formula that has k or fewer connectives/quantifiers. We now argue that the theorem holds for the formula ϕ. {Insert argument for the three inductive cases.}

Between the base case and the inductive case we have established that the theorem holds for ϕ no matter how many connectives/quantifiers the formula ϕ contains, so by induction on the structure of ϕ, we have established that the theorem holds for all formulas ϕ.

This might be a bit confusing on first glance, but the power of this proof technique will become very evident as you work through the following exercises and when we discuss the semantics of our language.

Notice also that the definition of a term (Definition 1.3.1) is also a recursive definition, so we can use induction on the complexity of a term to prove that a theorem holds for every term.

Exercises

1. Prove, by ordinary induction on the natural numbers, that
$$1^2+2^2+\cdots+n^2=\frac{n\,(n+1)\,(2n+1)}{6}. \tag{2.5.5.5}$$
2. Prove, by induction, that the sum of the interior angles in a convex n-gon is $(n-2)\,180^{\circ}$. (A convex n-gon is a polygon with n sides, where the interior angles are all less than 180°.)
3. Prove by induction that if A is a set consisting of n elements, then A has 2^n subsets.
4. Suppose that $\mathcal{L}$ is $\{0, f, g\}$, where 0 is a constant symbol, f is a binary function symbol, and g is a 4-ary function symbol. Use induction on complexity to show that every $\mathcal{L}$-term has an odd number of symbols.
5. If $\mathcal{L}$ is $\{0, <\}$, where 0 is a constant symbol and $<$ is a binary relation symbol, show that the number of symbols in any formula is divisible by 3.
6. If s and t are strings, we say that s is an *initial segment* of t if there is a nonempty string u such that $t :\equiv su$, where su is the string s followed by the string u. For example, $KUMQ$ is an initial segment of $KUMQUAT$ and $+24$ is an initial segment of $+24u-v$. Prove, by induction on the complexity of s, that if s and t are terms, then s is not an initial segment of t. [*Suggestion:* The base case, when s is either a variable or a constant symbol, should be easy. Then suppose that s is an initial segment of t and $s :\equiv ft_1t_2\ldots t_n$, where you know that each t_i is not an initial segment of any other term. Look for a contradiction.]
7. A language is said to satisfy unique readability for terms if, for each term t, t is in exactly one of the following categories:
   (a) Variable
   (b) Constant symbol
   (c) Complex term
   and furthermore, if t is a complex term, then there is a unique function symbol f and a unique sequence of terms $t_1, t_2, \ldots, t_n$ such that $t :\equiv ft_1t_2\ldots t_n$. Prove that our languages satisfy unique readability for terms. [*Suggestion:* You mostly have to worry about uniqueness - for example, suppose that t is c, a constant symbol. How do you know that t is not also a complex term? Suppose that t is $ft_1t_2\ldots t_n$. How do you show that the f and the t_i's are unique? You may find Exercise 6 useful.]
8. To say that a language satisfies unique readability for formulas is to say that every formula ϕ is in exactly one of the following categories:
   (a) Equality (if $\phi :\equiv= t_1t_2$)
   (b) Other atomic (if $\phi :\equiv Rt_1t_2\ldots t_n$ for an n-ary relation symbol R)
   (c) Negation
   (d) Disjunction
   (e) Quantified
   Also, it must be that if ϕ is both $=t_1t_2$ and $=t_3t_4$, then t_1 is identical to t_3 and t_2 is identical to t_4, and similarly for other atomic formulas. Furthermore, if (for example) ϕ is a negation $(\neg\alpha)$, then it must be the case that there is not another formula β such that ϕ is also $(\neg\beta)$, and similarly for disjunctions and quantified formulas. You will want to look at, and use, Exercise 7. You may have to prove an analog of Exercise 6, in which it may be helpful to think about the parentheses in an initial segment of a formula, in order to prove that no formula is an initial segment of another formula.
9. Take the proof of Theorem 1.4.2 and write it out in the way that you would present it as part of a homework assignment. Thus, you should cut out all of the inessential motivation and present only what is needed to make the proof work.

2.5.6: Sentences

Among the formulas in the language $\mathcal{L}$, there are some in which we will be especially interested. These are the sentences of $\mathcal{L}$ - the formulas that can be either true or false in a given mathematical model.

Let us use an example to introduce a language that will be vitally important to us as we work through this book.

Definition 1.5.1. The language $\mathcal{L}_{NT}$ is $\{0, S, +, \cdot, E, <\}$, where 0 is a constant symbol, S is a unary function symbol, $+$, $\cdot$, and E are binary function symbols, and $<$ is a binary relation symbol. This will be referred to as the language of number theory.

> *Chaff:* Although we are not fixing the meanings of these symbols yet, we probably ought to tell you that the standard interpretation of $\mathcal{L}_{NT}$ will use 0, $+$, $\cdot$, and $<$ in the way that you expect. The symbol S will stand for the successor function that maps a number x to the number $x+1$, and E will be used for exponentiation: $E32$ is supposed to be 3^2.

Consider the following two formulas of $\mathcal{L}_{NT}$:

$$\neg(\forall x)[(y<x)\vee(y=x)]. \tag{2.5.6.1}$$

$$(\forall x)(\forall y)[(x<y)\vee(x=y)\vee(y<x)]. \tag{2.5.6.2}$$

(Did you notice that we have begun using an informal presentation of the formulas?)

The second formula should look familiar. It is nothing more than the familiar trichotomy law of $<$, and you would agree that the second formula is a true statement about the collection of natural numbers, where you are interpreting $<$ in the usual way.

The first formula above is different. It "says" that not every x is greater than or equal to y. The truth of that statement is indeterminate: It depends on what natural number y represents. The formula might be true, or it might be false - it all depends on the value of y. So our goal in this section is to separate the formulas of $\mathcal{L}$ into one of two classes: the sentences (like the second example above) and the nonsentences. To begin this task, we must talk about free variables.

Free variables are the variables upon which the truth value of a formula may depend. The variable y is free in the first formula above. To draw an analogy from calculus, if we look at

$$\int_1^x \frac{1}{t}dt, \tag{2.5.6.3}$$

the variable x is free in this expression, as the value of the integral depends on the value of x. The variable t is not free, and in fact it doesn't make any sense to decide on a value for t. The same distinction holds between free and nonfree variables in an $\mathcal{L}$-formula. Let us try to make things a little more precise.

Definition 1.5.2. Suppose that v is a variable and ϕ is a formula. We will say that v **is free in** ϕ if

1. ϕ is atomic and v occurs in (is a symbol in) ϕ, or
2. $\phi :\equiv (\neg\alpha)$ and v is free in α, or
3. $\phi :\equiv (\alpha\vee\beta)$ and v is free in at least on of α or β, or
4. $\phi :\equiv (\forall u)(\alpha)$ and v is not u and v is free in α.

Thus, if we look at the formula

$$\forall v_2\neg(\forall v_3)(v_1 = S(v_2)\vee v_3 = v_2), \tag{2.5.6.4}$$

the variable v_1 is free whereas the variables v_2 and v_3 are not free. A slightly more complicated example is

$$(\forall v_1\forall v_2(v_1+v_2=0))\vee v_1 = S(0). \tag{2.5.6.5}$$

In this formula, v_1 is free whereas v_2 is not free. Especially when a formula is presented informally, you must be careful about the scope of the quantifiers and the placement of parentheses.

We will have occasion to use the informal notation $\forall x\phi(x)$. This will mean that ϕ is a formula and x is among the free variables of ϕ. If we then write $\phi(t)$, where t is an $\mathcal{L}$-term, that will denote the formula obtained by taking ϕ and replacing each occurrence of the variable x with the term t. This will all be defined more formally and more precisely in Definition 1.8.2.

Definition 1.5.3. A **sentence** in a language $\mathcal{L}$ is a formula of $\mathcal{L}$ that contains no free variables.

For example, if a language contained the constant symbols 0, 1, and 2 and the binary function symbol $+$, then the following are sentences: $1+1=2$ and $(\forall x)(x+1=x)$. You are probably convinced that the first of these is true and the second of these is false. In the next two sections we will see that you might be correct. But then again, you might not be.

Exercises

1. For each of the following, find the free variables, if any, and decide if the given formula is a sentence. The language includes a binary function symbol $+$, a binary relation symbol $<$, and constant symbols 0 and 2.
   (a) $(\forall x)(\forall y)(x+y=2)$
   (b) $(x+y<x)\vee(\forall z)(z<0)$
   (c) $((\forall y)(y<x))\vee((\forall x)(x<y))$
2. Explain precisely, using the definition of a free variable, how you know that the variable v_2 is free in the formula
$$(\forall v_1)(\neg(\forall v_5)(v_2=v_1+v_5)). \tag{2.5.6.6}$$
3. In mathematics, we often see statements such as $\sin^2 x+\cos^2 x=1$. Notice that this is not a sentence, as the variable x is free. But we all agree that this statement is true, given the usual interpretations of the symbols. How can we square this with the claim that *sentences* are the formulas that can be either true or false?
4. If we look at the first of our example formulas in this section,
$$\neg(\forall x)[(y<x)\vee(y=x)], \tag{2.5.6.7}$$
   and we interpret the variables as ranging over the natural numbers, you will probably agree that the formula is false if y represents the natural number 0 and true if y represents any other number. (If you aren't happy with 0 being a natural number, then use 1.) On the other hand, if we interpret the variables as ranging over the integers, what can we say about the truth or falsehood of this formula? Can you think of an interpretation for the symbols that would make sense if wy try to apply this formula to the collection of complex numbers?
5. A variable may occur several times in a given formula. For example, the variable v_1 occurs four times in the formula
$$(\forall v_1)[(v_1=v_3)\vee(v_1=Sv_2)\vee(0+v_{17}<v_1-S0)]. \tag{2.5.6.8}$$
   What should it mean for an *occurrence* of a variable to be free? Write a definition that begins: The nth occurrence of a variable v in a formula ϕ is said to be free if .... An occurrence of v in ϕ that is not free is said to be **bound**. Give an example of a formula in a suitable language that contains both free and bound occurrences of a variable v.
6. Look at the formula
$$[(\forall y)(x=y)]\vee[(\forall x)(x<0)]. \tag{2.5.6.9}$$
   If we denote this formula by $\phi(x)$ and t is the term $S0$, find $\phi(t)$. [*Suggestion:* The trick here is to see that there is a bit of a lie in the discussion of $\phi(t)$ in the text. Having completed Exercise 5, we can now say that we only replace the free occurrence of the variable x when we move from $\phi(x)$ to $\phi(t)$.]

2.5.7: Structures

Let us, by way of example, return to the language $\mathcal{L}_{NT}$ of number theory. Recall that $\mathcal{L}_{NT}$ is $\{0, S, +, \cdot, E, <\}$, where 0 is a constant symbol, S is a unary function symbol, $+$, $\cdot$, and E are binary function symbols, and $<$ is a binary relation symbol. We now want to discuss the possible mathematical structures in which we can interpret these symbols, and thus the formulas and sentences of $\mathcal{L}_{NT}$.

"But wait!" cries the incredulous reader. "You just said that this is the language of number theory, so certainly we already know what each of those symbols means."

It is certainly the case that you know *an* interpretation for these symbols. The point of this section is that there are *many* different possible interpretations for these symbols, and we want to be able to specify which of those interpretations we have in mind at any particular moment.

Probably the interpretation you had in mind (what we will call the standard model for number theory) works with the set of natural numbers $\{0, 1, 2, 3, \ldots\}$. The symbol 0 stands for the number 0.

> *Chaff:* Carefully, now! The symbol 0 is the mark on the paper, the numeral. The number 0 is the thing that the numeral 0 represents. The numeral is something that you can see. The number is something that you cannot see.

The symbol S is a unary function symbol, and the function for which that symbol stands is the successor function that maps a number to the next larger natural number. The symbols $+$, $\cdot$, and E represent the functions of addition, multiplication, and exponentiation, and the symbol $<$ will be used for the "less than" relation.

But that is only one of the ways that we might choose to interpret those symbols. Another way to interpret all of those symbols would be to work with the numbers 0 and 1, interpreting the symbol 0 as the number 0, S as the function that maps 0 and 1 and 1 to 0, $+$ as addition mod 2, $\cdot$ as multiplication mod 2, and (just for variety) E as the function with constant value 1. The symbol $<$ can still stand for the relation "less than".

Or, if we were in a slightly more bizarre mood, we could work in a universe consisting of Beethoven, Picasso, and Ernie Banks, interpreting the symbol 0 as Picasso, S as the identity function, $<$ as equality, and each of the binary function symbols as the constant function with output Ernie Banks.

The point is that there is nothing sacred about one mathematical structure as opposed to another. Without determining the structure under consideration, without deciding how we wish to interpret the symbols of the language, we have no way of talking about the truth or falsity of a sentence as trivial as

$$(\forall v_1)\,(v_1 < S\,(v_1))\,. \tag{2.5.7.1}$$

Definition 1.6.1. Fix a language $\mathcal{L}$. An **$\mathcal{L}$-structure $\mathfrak{A}$** is a nonempty set A, called the **universe of $\mathfrak{A}$**, together with:

1. For each constant symbol c of $\mathcal{L}$, an element $c^{\mathfrak{A}}$ of A,
2. For each n-ary function symbol f of $\mathcal{L}$, a function $f^{\mathfrak{A}} : A^n \to A$, and
3. For each n-ary relation symbol R of $\mathcal{L}$, an n-ary relation $R^{\mathfrak{A}}$ on A (i.e., a subset of A^n).

Notice that the domain of the function $f^{\mathfrak{A}}$ is the set A^n, so $f^{\mathfrak{A}}$ is defined for all elements of A^n. Later in the text we will have occasion to discuss partial functions, those whose domain in a proper subset of A^n, but for now our functions are total functions, defined on all of the advertised domain.

> *Chaff:* The letter $\mathfrak{A}$ is a German Frakture capital A. We will also have occasion to use $\mathfrak{A}$'s friends, $\mathfrak{B}$ and $\mathfrak{C}$. $\mathfrak{N}$ will be used for a particular structure involving the natural numbers. The use of this typeface is traditional (which means this is the way we learned it). For your handwritten work, probably using capital script letters will be the best.

Often, we will write a structure as an ordered k-tuple, like this:

$$\mathfrak{A} = \left(A, c_1^{\mathfrak{A}}, c_2^{\mathfrak{A}}, f_1^{\mathfrak{A}}, R_1^{\mathfrak{A}}, R_2^{\mathfrak{A}}\right). \tag{2.5.7.2}$$

As you can see, the notation is starting to get out of hand once again, and we will not hesitate to simplify and abbreviate when we believe that we can do so without confusion. So, when we are working in $\mathcal{L}_{NT}$, we will often talk about the standard structure

$$\mathfrak{N} = (\mathbb{N}, 0, S, +, \cdot, E, <)\,, \tag{2.5.7.3}$$

where the constants, functions, and relations do not get the superscripts they deserve, and the authors trust that you will interpret $\mathbb{N}$ as the collection $\{0, 1, 2, \ldots\}$ of natural numbers, the symbol 0 to stand for the number 0, $+$ to stand for addition, S to stand for the successor function, and so on. By the way, if you are not used to thinking of 0 as a natural number, do not panic. Set theorists see 0 as the most natural of objects, so we tend to include it in $\mathbb{N}$ without thinking about it.

x	$S^{\mathfrak{A}}(x)$
Oberon	Oberon
Titania	Bottom
Puck	Titania
Bottom	Titania

$+^{\mathfrak{A}}$	Oberon	Titania	Puck	Bottom
Oberon	Puck	Puck	Puck	Titania
Titania	Puck	Bottom	Oberon	Titania
Puck	Bottom	Titania	Bottom	Titania
Bottom	Bottom	Bottom	Bottom	Oberon

$\cdot^{\mathfrak{A}}$	Oberon	Titania	Puck	Bottom
Oberon	Oberon	Titania	Puck	Bottom
Titania	Titania	Bottom	Oberon	Titania
Puck	Bottom	Bottom	Oberon	Oberon
Bottom	Titania	Oberon	Puck	Puck

$E^{\mathfrak{A}}$	Oberon	Titania	Puck	Bottom
Oberon	Puck	Puck	Oberon	Oberon
Titania	Titania	Titania	Titania	Titania
Puck	Titania	Bottom	Oberon	Puck
Bottom	Bottom	Puck	Titania	Puck

$<^{\mathfrak{A}}$	Oberon	Titania	Puck	Bottom
Oberon	Yes	No	Yes	Yes
Titania	No	No	Yes	No
Puck	Yes	Yes	Yes	Yes
Bottom	No	No	Yes	No

Table 1.1: *A Midsummer Night's Structure*

Example 1.6.2. The structure $\mathfrak{N}$ that we have just introduced is called the standard $\mathcal{L}_{NT}$-structure. To emphasize that there are other perfectly good $\mathcal{L}_{NT}$-structures, let us construct a different $\mathcal{L}_{NT}$-structure $\mathfrak{A}$ with exactly four elements. The elements of A will be Oberon, Titania, Puck, and Bottom. The constant $0^{\mathfrak{A}}$ will be Bottom. Now we have to construct the functions and relations for our structure. As everything is unary or binary, setting forth tables (as in Table 1.1) seems a reasonable way to proceed. So you can see that in this structure $\mathfrak{A}$ that Titania $+$ Puck $=$ Oberon, while Puck $+$ Titania $=$ Titania. You can also see that 0 (also known as Bottom) is not the additive identity in this structure, and that $<$ is a very strange ordering.

Now the particular functions and relation that we chose were just the functions and relations that jumped into Chris's fingers as he typed up this example, but any such functions would have worked perfectly well to define an $\mathcal{L}_{NT}$-structure. It may well be worth your while to figure out if this $\mathcal{L}_{NT}$-sentence is true (whatever that means) in $\mathfrak{A}$: $SS0 + SS0 < SSSSS0E0 + S0$.

Example 1.6.3. We work in a language with one constant symbol, $\mathfrak{L}$, and one unary function symbol, X. So, to define a model $\mathfrak{A}$, all we need to do is specify a universe, an element of the universe, and a function $X^{\mathfrak{A}}$. Suppose that we let the universe be the collection of all finite strings of 0 or more capital letters from the Roman alphabet. So A includes such strings as: BABY, LOGICISBETTERTHANSIX, ε (the empty string), and DLKFDFAHADS. The constant symbol $\mathfrak{L}$ will be interpreted as the string POTITION, and the function $X^{\mathfrak{A}}$ is the function that adds an X to the beginning of a string. so $X^{\mathfrak{A}}$(YLOPHONE) $=$ XYLOPHONE. Convince yourself that this is a valid, if somewhat odd, $\mathcal{L}$-structure.

To try to be clear about things, notice that we have X, the function symbol, which is an element of the language $\mathcal{L}$. Then there is X, the string of exactly one capital letter of the Roman alphabet, which is one of the elements of the universe. (Did you notice the change in typeface without our pointing it out? You may have a future in publishing!)

Let us look at one of the terms of the language: $X\mathfrak{L}$. In our particular $\mathcal{L}$-structure $\mathfrak{A}$ we will interpret this as

$$X^{\mathfrak{A}}\left(\mathfrak{L}^{\mathfrak{A}}\right) = X^{\mathfrak{A}}\left(\text{POTITION}\right) = \text{XPOTITION}. \tag{2.5.7.4}$$

In a different structure, $\mathfrak{B}$, it is entirely possible that the interpretation of the term $X\mathfrak{L}$ will be HUNNY or AARDVARK or $3\pi/17$. Without knowing the structure, without knowing how to interpret the symbols of the language, we cannot begin to know what object is referred to by a term.

> *Chaff:* All of this stuff about interpreting terms in a structure will be made formal in the next section, so don't panic if it doesn't all make sense right now.

What makes this example confusing, as well as important, is that the function symbol is part of the structure for the language and (modulo a superscript and a change in typeface) the function acts on the elements of the structure in the same way that the function symbol is used in creating $\mathcal{L}$-formulas.

Example 1.6.4. Now, let $\mathcal{L}$ be $\{0, f, g, R\}$, where 0 is a constant symbol, f is a unary function symbol, g is a binary function symbol, and R is a 3-ary relation symbol. We define an $\mathcal{L}$-structure $\mathfrak{B}$ as follows: B, the universe, is the set of all variable-free $\mathcal{L}$-terms. The constant $0^{\mathfrak{B}}$ is the term 0. The functions $f^{\mathfrak{B}}$ and $g^{\mathfrak{B}}$ are defined as in Example 1.6.3, so if t and s are elements of B, (i.e., variable-free terms), then $f^{\mathfrak{B}}(t)$ is ft and $g^{\mathfrak{B}}(t, s)$ is gts.

Let us look at this in a little more detail. Consider 0, the constant symbol, which is an element of $\mathcal{L}$. Since 0 is a constant symbol, it is a term, so 0 is an element of B, the universe of our structure $\mathfrak{B}$. (Alas, there is no change in typeface to help us out this time.) If we want to see what element of the universe is referred to by the constant symbol 0, we see that $0^{\mathfrak{B}} = 0$, so the term 0 refers to the element of the universe 0.

If we look at another term of the language, say $f0$, and we try to find the element of the universe that is denoted by this term, we find that it is

$$f^{\mathfrak{B}}\left(0^{\mathfrak{B}}\right) = f^{\mathfrak{B}}(0) = f0. \tag{2.5.7.5}$$

So the term $f0$ denotes an element of the universe, and that element of the universe is ... $f0$. This is pretty confusing, but all that is going on is that the elements of the universe *are* the syntactic objects of the language.

This sort of structure is called a *Henkin structure*, after Leon Henkin, who introduced them in his PhD dissertation in 1949. These structures will be crucial in our proof of the Completeness Theorem in Chapter 3. The proof of that theorem will involve the construction of a particular mathematical structure, and the structure that we will build will be a Henkin structure.

To finish building our structure $\mathfrak{B}$, we have to define a relation $R^{\mathfrak{B}}$. As R is a 3-ary relation symbol, $R^{\mathfrak{B}}$ is a subset of B^3. We will arbitrarily define

$$R^{\mathfrak{B}} = \{(r, s, t) \in B^3 \mid \text{the number of function symbols in } r \text{ is even}\}. \tag{2.5.7.6}$$

This finishes defining the structure $\mathfrak{B}$. The definition of $R^{\mathfrak{B}}$ given is entirely arbitrary. We invite you to come up with a more interesting or more humorous definition on your own.

Exercises

1. Consider the structure constructed in Example 1.6.2. Find the value of each of the following: $0+0$, $0E0$, $S0 \cdot SS0$. Do you think $0 < 0$ is true in this structure?
2. Suppose that $\mathcal{L}$ is the language $\{0, +, <\}$. Let's work together to describe an $\mathcal{L}$-structure $\mathfrak{A}$. Let the universe A be the set consisting of all of the natural numbers together with Ingrid Bergman and Humphrey Bogart. You decide on the interpretations of the symbols. What is the value of $5+$ Ingrid? Is Bogie < 0?
3. Here is a language consisting of one constant symbol, one 3-ary function symbol, and one binary relation symbol: $\mathcal{L}$ is $\{\flat, \sharp, \natural\}$. Describe an $\mathcal{L}$-model that has as its universe $\mathbb{R}$, the set of real numbers. Describe another $\mathcal{L}$-model that has a finite universe.
4. Write a short paragraph explaining the difference between a language and a structure for a language.
5. Suppose that $\mathfrak{A}$ and $\mathfrak{B}$ are two $\mathcal{L}$-structures. We will say that $\mathfrak{A}$ and $\mathfrak{B}$ are **isomorphic** and write $\mathfrak{A} \cong \mathfrak{B}$ if there is a bijection $i : A \to B$ such that for each constant symbol c of $\mathcal{L}$, $i\left(c^{\mathfrak{A}}\right) = c^{\mathfrak{B}}$, for each n-ary function symbol f and for each $a_1, \ldots, a_n \in A$, $i\left(f^{\mathfrak{A}}(a_1, \ldots, a_n)\right) = f^{\mathfrak{B}}(i(a_1), \ldots i(a_n))$, and for each n-ary relation symbol R in $\mathcal{L}$, $(a_1, \ldots a_n) \in R^{\mathfrak{A}}$ if and only if $(i(a_1), \ldots, i(a_n)) \in R^{\mathfrak{B}}$. The function i is called an **isomorphism**.
   (a) Show that $\cong$ is an equivalence relation. [*Suggestion:* This means that you must show that the relation $\cong$ is reflexive, symmetric, and transitive. To show that $\cong$ is reflexive, you must show that for any structure $\mathfrak{A}$, $\mathfrak{A} \cong \mathfrak{A}$, which means that you must find an isomorphism, a function, mapping A to A that satisfies the conditions above. So the first line of your proof should

be, "Consider this function, with domain A and codomain A : $i\left(x\right)=$ [something brilliant]." Then show that your function i is an isomorphism. Then show, if $\mathfrak{A}\cong\mathfrak{B}$, then $\mathfrak{B}\cong\mathfrak{A}$. Then tackle transitivity. In each case, you must define a particular function and shown that your function is an isomorphism.]
(b) Find a new structure that is isomorphic to the structure given in Example 1.6.2. Prove that the structures are isomorphic.
(c) Find two different structures for a particular language and prove that they are not isomorphic.
(d) Find two different structures for a particular language such that the structures have the same number of elements in their universes but they are still not isomorphic.Prove they are not isomorphic.

6. Take the language of Example 1.6.4 and let C be the set of all $\mathcal{L}$-terms. Create an $\mathcal{L}$-structure $\mathfrak{C}$ by using this universe in such a way that the interpretation of a term t is *not* equal to t.
7. If we take the language $\mathcal{L}_{NT}$, we can create a Henkin structure for that language in the same way as in Example 1.6.4. Do so. Consider the $\mathcal{L}_{NT}$-formula $S0+S0=SS0$. Is this formula "true" (whatever that means) in your structure? Justify your answer.

2.5.8: Truth in a Structure

It is at last time to tie together the syntax and the semantics. We have some formal rules about what constitutes a language, and we can identify the terms, formulas, and sentences of a language. We can also identify $\mathcal{L}$-structures for a given language $\mathcal{L}$. In this section we will decide what it means to say that an $\mathcal{L}$-formula ϕ is *true* in an $\mathcal{L}$-structure $\mathfrak{A}$.

To begin the process of tying together the symbols with the structures, we will introduce assignment functions. These assignment functions will formalize what it means to interpret a term or a formula in a structure.

Definition 1.7.1. If $\mathfrak{A}$ is an $\mathcal{L}$-structure, a **variable assignment function into $\mathfrak{A}$** is a function s that assigns to each variable an element of the universe A. So a variable assignment function into $\mathfrak{A}$ is any function with domain $Vars$ and codomain A.

Variable assignment functions need not be injective or bijective. For example, if we work with $\mathcal{L}_{NT}$ and the standard structure $\mathfrak{N}$, then the function s defined by $s(v_i) = i$ is a variable assignment function, as is the function s' defined by

$$s'(v_i) = \text{ the smallest prime number that does not divide } i. \tag{2.5.8.1}$$

We will have occasion to want to fix the value of the assignment function s for certain variables.

Definition 1.7.2. If s is a variable assignment function into $\mathfrak{A}$ and x is a variable and $a \in A$, then $s[x|a]$ is the variable assignment function into $\mathfrak{A}$ defined as follows:

$$s[x|a] = \begin{cases} s(v) & \text{if } v \text{ is a variable other than } x \\ a & \text{if } v \text{ is the variable } x \end{cases} \tag{2.5.8.2}$$

We call the function $s[x|a]$ an **x-modification of the assignment function s**.

So an x-modification of s is just like s, except that the variable x is assigned to a particular element of the universe.

What we will do next is extend a variable assignment function s to a term assignment function, $\bar{s}$. This function will assign an element of the universe to each term of the language $\mathcal{L}$.

Definition 1.7.3. Suppose that $\mathfrak{A}$ is an $\mathcal{L}$-structure and s is a variable assignment function into $\mathfrak{A}$. The function $\bar{s}$, called the **term assignment function generated by s**, is the function with domain consisting of the set of $\mathcal{L}$-terms and codomain A defined recursively as follows:

1. If t is a variable, $\bar{s}(t) = s(t)$.
2. If t is a constant symbol c, then $\bar{s}(t) = c^{\mathfrak{A}}$.
3. If $t :\equiv f t_1 t_2 \ldots t_n$, then $\bar{s}(t) = f^{\mathfrak{A}}(\bar{s}(t_1), \bar{s}(t_2), \ldots, \bar{s}(t_n))$.

Although we will be primarily interested in truth of sentences, we will first describe truth (or satisfaction) for arbitrary formulas, relative to an assignment function.

Definition 1.7.4. Suppose that $\mathfrak{A}$ is an $\mathcal{L}$-structure, ϕ is an $\mathcal{L}$-formula, and $s : Vars \to A$ is an assignment function. We will say that **$\mathfrak{A}$ satisfies ϕ with assignment s**, and write $\mathfrak{A} \models \phi[s]$, in the following circumstances:

1. If $\phi :\equiv t_1 t_2$ and $\bar{s}(t_1)$ is the same element of the universe A as $\bar{s}(t_2)$, or
2. If $\phi :\equiv R t_1 t_2 \ldots t_n$ and $(\bar{s}(t_1), \bar{s}(t_2), \ldots, \bar{s}(t_n)) \in R^{\mathfrak{A}}$, or
3. If $\phi :\equiv (\neg\alpha)$ and $\mathfrak{A} \not\models \alpha[s]$, (where $\not\models$ means "does not satisfy"), or
4. If $\phi :\equiv (\alpha \vee \beta)$ and $\mathfrak{A} \models \alpha[s]$, or $\mathfrak{A} \models \beta[s]$ (or both), or
5. If $\phi :\equiv (\forall x)(\alpha)$ and, for each element a of A, $\mathfrak{A} \models \alpha[s(x|a)]$.

If Γ is a set of $\mathcal{L}$-formulas, we say that $\mathfrak{A}$ satisfies Γ with assignment s, and write $\mathfrak{A} \models \Gamma[s]$ if for each $\gamma \in \Gamma$, $\mathfrak{A} \models \gamma[s]$.

> *Chaff:* Notice that the symbol $\models$ is *not* part of the language $\mathcal{L}$. Rather, $\models$ is a metalinguistic symbol that we use to talk about formulas in the language and structures for the language.
>
> *Chaff:* Also notice that we have at last tied together the syntax and semantics of our language! The definition above is the place where we formally put the meanings on the symbols that we will use, so that $\vee$ means "or" and $\forall$ means "for all".

Example 1.7.5. Let us work with the empty language, so $\mathcal{L}$ has no constant symbols, no function symbols, and no relation symbols. So an $\mathcal{L}$-structure is simply a nonempty set, and let us consider the $\mathcal{L}$-structure $\mathfrak{A}$, where $A = \{\text{Humphrey}, \text{Ingrid}\}$. Consider the formula $x = y$ and the assignment function s, where $s(x)$ is Humphrey and $s(y)$ is also Humphrey. If we ask

whether $\mathfrak{A} \models x = y\,[s]$, we have to check whether $bars\,(x)$ is the same element of A as $\bar{s}\,(y)$. Since the two objects are identical, the formula is true.

To emphasize this, the formula $x = y$ can be true in some universes with some assignment functions. Although the variables x and y are distinct, the truth or falsity of the formula depends *not* on the variables (which are not equal) but rather, on which elements of the structure the variables denote, the *values* of the variables (which are equal for this example). Of course, there are other assignment functions and other structures that make our formula false. We are sure you can think of some.

To talk about the truth or falsity of a *sentence* in a structure, we will take our definition of satisfaction relative to an assignment function and prove that for sentences, the choice of the assignment function is inconsequential. Then we will say that a sentence σ is true in a structure $\mathfrak{A}$ if and only if $\mathfrak{A} \models \sigma\,[s]$ for any (and therefore all) variable assignment functions s.

> *Chaff:* The next couple of proofs are proofs by induction on the complexity of terms or formulas. You may want to reread the proof of Theorem 1.4.2 if you find these difficult.

Lemma 1.7.6. *Suppose that s_1 and s_2 are variable assignment functions into a structure $\mathfrak{A}$ such that $s_1\,(v) = s_2\,(v)$ for every variable v in the term t. Then $\bar{s_1}\,(t) = \bar{s_2}\,(t)$.*

Proof. We use induction on the complexity of the term t. If t is either a variable or a constant symbol, the result is immediate. If $t :\equiv ft_1t_2 \ldots t_n$, then as $\bar{s_1}\,(t_i) = \bar{s_2}\,(t_i)$ for $1 \leq i \leq n$ by the inductive hypothesis, the definition of $\bar{s_1}\,(t)$ and the definition of $\bar{s_2}\,(t)$ are identical, and thus $\bar{s_1}\,(t) = \bar{s_2}\,(t)$.

Proposition 1.7.7. *Suppose that s_1 and s_2 are variable assignment functions into a structure $\mathfrak{A}$ such that $s_1\,(v) = s_2\,(v)$ for every free variable v in the formula ϕ. Then $mathfrakA \models \phi\,[s_1]$ if and only if $\mathfrak{A} \models \phi\,[s_2]$.*

Proof. We use induction on the complexity of ϕ. If $\phi :\equiv= t_1t_2$, then the free variables of ϕ are exactly the variables that occur in ϕ. Thus Lemma 1.7.6 tells us that $\bar{s_1}\,(t_1) = \bar{s_2}\,(t_1)$ and $\bar{s_1}\,(t_2) = \bar{s_2}\,(t_2)$, meaning that they are the same element of the universe A, so $\mathfrak{A} \models (= t_1t_2)\,[s_1]$ if and only if $\mathfrak{A} \models (= t_1t_2)\,[s_2]$, as needed.

The other base case, if $\phi :\equiv Rt_1t_2 \ldots t_n$, is similar and is left as part of Exercise 6.

To begin the first inductive clause, if $\phi :\equiv \neg\alpha$, notice that the free variables of ϕ are exactly the free variables of α, so s_1 and s_2 agree on the free variables of α. By the inductive hypothesis, $\mathfrak{A} \models \alpha\,[s_1]$ if and only if $\mathfrak{A} \models \alpha\,[s_2]$, and thus (by the definition of satisfaction), $\mathfrak{A} \models \phi\,[s_1]$ if and only if $\mathfrak{A} \models \phi\,[s_2]$. The second inductive clause, if $\phi :\equiv \alpha \vee \beta$, is another part of Exercise 6.

If $\phi :\equiv (\forall x)\,(\alpha)$, we first note that the only variable that might be free in α that is not free in ϕ is x. Thus, if $a \in A$, the assignment functions $s_1\,[x|a]$ and $s_2\,[x|a]$ agree on all of the free variables of α. Therefore, by inductive hypothesis, for each $a \in A$, $\mathfrak{A}$ $= \alpha\,[s_1\,[x|a]]$ if and only if $\mathfrak{A} \models \alpha\,[s_2\,[x|a]]$. So, by Definition 1.7.4, $\mathfrak{A} \models \phi\,[s_1]$ if and only if \(\mathfrak{A} \models \phi \left[s_2 \right]|). This finishes the last inductive clause, and our proof.

Corollary 1.7.8 *If σ is a sentence in the language $\mathcal{L}$ and $\mathfrak{A}$ is an $\mathcal{L}$-structure, either $\mathfrak{A} \models \sigma\,[s]$ for all assignment functions s, or $\mathfrak{A} \models \sigma\,[s]$ for no assignment function s.*

Proof. There *are* no free variables in σ, so if s_1 and s_2 are two assignment functions, they agree on all of the free variables of σ, there just aren't all that many of them. So by Proposition 1.7.7, $\mathfrak{A} \models \sigma\,[s_1]$ if and only if $\mathfrak{A} \models \sigma\,[s_2]$, as needed.

Definition 1.7.9. If ϕ is a formula in the language $\mathcal{L}$ and $\mathfrak{A}$ is an $\mathcal{L}$-structure, we say that $\mathfrak{A}$ is a **model** of ϕ, and write $\mathfrak{A} \models \phi$, if and only if $\mathfrak{A} \models \phi\,[s]$ for every assignment function s. If Φ is a set of $\mathcal{L}$-formulas, we will say that $\mathfrak{A}$ models Φ, and write $\mathfrak{A} \models \Phi$, if and only if $\mathfrak{A} \models \phi$ for each $\phi \in \Phi$.

Notice that if σ is a *sentence*, then $\mathfrak{A} \models \sigma$ if and only if $\mathfrak{A} \models \sigma\,[s]$ for *any* assignment function s. In this case we will say that the sentence σ is **true in $\mathfrak{A}$**.

Example 1.7.10. Let's work in $\mathcal{L}_{NT}$, and let

$$\mathfrak{N} = (\mathbb{N}, 0, S, +, \cdot, E, <) \tag{2.5.8.3}$$

be the standard structure. Let s be the variable assignment function that assigns v_i to the number $2i$. Now let the formula $\phi\,(v_1)$ be $v_1 + v_2 = SSS0$.

To show that $\mathfrak{N} \models \phi\,[s]$, notice that

$$\bar{s}\left(v_1+v_1\right) \text{ is } +^{\mathfrak{N}}\left(\bar{s}\left(v_1\right), \bar{s}\left(v_1\right)\right) \tag{2.5.8.4}$$
$$\text{is } +^{\mathfrak{N}}(2,2) \tag{2.5.8.5}$$
$$\text{is } 4 \tag{2.5.8.6}$$

while

$$\bar{s}\left(SSSS0\right) \text{ is } S^{\mathfrak{N}}\left(S^{\mathfrak{N}}\left(S^{\mathfrak{N}}\left(S^{\mathfrak{N}}\left(0^{\mathfrak{N}}\right)\right)\right)\right) \tag{2.5.8.7}$$
$$\text{is } 4 \tag{2.5.8.8}$$

Now, in the same setting, consider σ, the sentence

$$\left(\forall v_1\right) \neg \left(\forall v_2\right) \neg \left(v_1 = v_2 + v_1\right), \tag{2.5.8.9}$$

which states that everything is even. [That is hard to see unless you know to look for that $\neg\left(\forall v_2\right)\neg$ and to read it as $\left(\exists v_2\right)$. See the last couple of paragraphs of this section.] You know that σ is false in the standard structure, but to show how the formal argument goes, let s be any variable assignment function and notice that

$$\mathfrak{N} \models \sigma\left[s\right] \text{ iff For every } a \in \mathbb{N},\ \mathfrak{N} \models \neg\left(\forall v_2\right) \neg\left(v_1 = v_2 + v_2\right) s\left[v_1|a\right] \tag{2.5.8.10}$$
$$\text{iff For every } a \in \mathbb{N},\ \mathfrak{N} \not\models \left(\forall v_2\right) \neg\left(v_1 = v_2 + v_2\right) s\left[v_1|a\right] \tag{2.5.8.11}$$
$$\text{iff For every } a \in \mathbb{N}, \text{ there is a } b \in \mathbb{N},\ \mathfrak{N} \models v_1 = v_2 + v_2\ s\left[v_1|a\right]\left[v_2|b\right]. \tag{2.5.8.12}$$

Now, if we consider the case when a is the number 3, it is perfectly clear that there is no such b, so we have shown $\mathfrak{N} \not\models \sigma\left[s\right]$. Then, by Definition 1.7.9, we see that the sentence σ is false in the standard structure. As you well knew.

When you were introduced to symbolic logic, you were probably told that there were five connectives. In the mathematics that you have learned recently, you have been using two quantifiers. We hope you have noticed that we have not used all of those symbols in this book, but is now time to make those symbols available. Rather than adding the symbols to our language, however, we will introduce them as abbreviations. This will help us to keep our proofs slightly less complex (as our inductive proofs will have fewer cases) but will still allow us to use the more familiar symbols, at least as shorthand.

Thus, let us agree to use the following abbreviations in constructing $\mathcal{L}$-formulas: We will write $\left(\alpha \wedge \beta\right)$ instead of $\left(\neg\left(\left(\neg\alpha\right) \vee \left(\neg\beta\right)\right)\right)$, $\left(\alpha \rightarrow \beta\right)$ instead of $\left(\left(\neg\alpha\right) \vee \beta\right)$, and $\left(\alpha \leftrightarrow \beta\right)$ instead of $\left(\left(\alpha \rightarrow \beta\right) \wedge \left(\beta \rightarrow \alpha\right)\right)$. We will also introduce our missing existential quantifier as an abbreviation, writing $\left(\exists x\right)\left(\alpha\right)$ instead of $\left(\neg\left(\forall x\right)\left(\neg\alpha\right)\right)$. It is an easy exercise to check that the introduced connectives $\wedge$, $\rightarrow$, and $\leftrightarrow$ behave as you would expect them to. Thus $\mathfrak{A} \models \left(\alpha \wedge \beta\right)\left[s\right]$ if and only if both $\mathfrak{A} \models \alpha\left[s\right]$ and $\mathfrak{A} \models \beta\left[s\right]$. The existential quantifier is only slightly more difficult. See Exercise 7.

Exercises

1. We suggested after Definition 1.5.3 that the truth or falsity of the sentences $1+1=2$ and $\left(\forall x\right)\left(x+1=x\right)$ might not be automatic. Find a structure for the language discussed there that makes the sentence $1+1=2$ true. Find another structure where $1+1=2$ is false. Prove your assertions. Then show that you can find a structure where $\left(\forall x\right)\left(x+1=x\right)$ is true, and another structure where it is false.
2. Let the language $\mathcal{L}$ be $\{S, C\}$, where S is a unary function symbol and $<$ is a binary relation symbol. Let ϕ be the formula $\left(\forall x\right)\left(\exists y\right)\left(Sx < y\right)$.
   (a) Find an $\mathcal{L}$-structure $\mathfrak{A}$ such that $\mathfrak{A} \models \phi$.
   (b) Find an $\mathcal{L}$-structure $\mathfrak{B}$ such that $\mathfrak{B} \models \left(\neg\phi\right)$.
   (c) Prove that your answer to part (a) or part (b) is correct.
   (d) Write an $\mathcal{L}$-sentence that is true in a structure $\mathfrak{A}$ if and only if the universe A of $\mathfrak{A}$ consists of exactly two elements.
3. Consider the language and structure of Example 1.6.4. Write two nontrivial sentences in the language, one of which is true in the structure and one of which (not the denial of the first) is false in the structure. Justify your assertions.
4. Consider the sentence σ: $\left(\forall x\right)\left(\exists y\right)\left[x < y \rightarrow x+1 \neg y\right]$. Find two structures for a suitable language, one of which makes σ true, and the other of which makes σ false.
5. One more bit of shorthand. Assume that the language $\mathcal{L}$ contains the binary relation symbol $\in$, which you are intending to use to mean the elementhood relation (so $p \in q$ will mean that p is an element of q). Often, it is the case that you want to claim that $\phi\left(x\right)$ is true for every element of a set b. Of course, to do this you could write

$$\left(\forall x\right)\left[\left(x \in b\right) \rightarrow \phi\left(x\right)\right]. \tag{2.5.8.13}$$

We will abbreviate this formula as

$$(\forall x \in b)\,(\phi\,(x))\,. \tag{2.5.8.14}$$

Similarly, $(\exists x \in b)\,(\phi\,(x))$ will be an abbreviation for the formula $(\exists x)\,[(x \in b) \wedge \phi\,(x)]$. Notice that this formula has a conjunction where the previous formula had an implication!. We do that just to see if you are paying attention. (Well, if you think about what the abbreviations are supposed to mean, you'll see that the change is necessary. We'll have to do something else just to see if you're paying attention.)
Now suppose that $\mathfrak{A}$ is a structure for the language of set theory. So $\mathcal{L}$ has only this one binary relation symbol, $\in$, which is interpreted as the elementhood relation. Suppose, in addition, that

$$A = \{u, v, w, \{u\}, \{u, v\}, \{u, v, w\}\}. \tag{2.5.8.15}$$

In particular, notice that there is no element x of A such that $x \in x$. Consider the sentence

$$(\forall y \in y)\,(\exists x \in x)\,(x = y)\,. \tag{2.5.8.16}$$

Is this sentence true or false in $\mathfrak{A}$?

6. Fill in the details to complete the proof of Proposition 1.7.7.
7. Show that $\mathfrak{A} \models (\exists x)\,(\alpha)\,[s]$ if and only if there is an element $a \in A$ such that $\mathfrak{A} \models \alpha\,[s\,[x|a]]$.

2.5.9: Substitutions and Substitutability

Suppose you knew that the sentence $\forall x \phi(x)$ was true in a particular structure $\mathfrak{A}$. Then, if c is a constant symbol in the language, you would certainly expect $\phi(c)$ to be true in $\mathfrak{A}$ as well. What we have done is substitute the constant symbol c for the variable x. This seems perfectly reasonable, although there are times when you do have to be careful.

Suppose that $\mathfrak{A} \models \forall x \exists y \neg (x = y)$. This sentence is, in fact, true in any structure $\mathfrak{A}$ such that A has at least two elements. If we then proceed to replace the variable x by the variable u, we get the statement $\exists y \neg (u = y)$, which will still be true in $\mathfrak{A}$, no matter what value we give to the variable u. If, however, we take our original formula and replace x by y, then we find ourselves looking at $\exists y \neg (y = y)$, which will be false in any structure. So by a poor choice of substituting variable, we have changed the truth value of our formula. The rules of substitutability that we will discuss in this section are designed to help us avoid this problem, the problem of attempting to substitute a term inside a quantifier that binds a variable involved in the term.

We begin by defining exactly what we mean when we substitute a term t for a variable x in either a term u or a formula ϕ.

Definition 1.8.1. Suppose that u is a term, x is a variable, and t is a term. We define the term u_t^x (read "u with x replaced by t") as follows:

1. If u is a variable not equal to x, then u_t^x is u.
2. If u is x, then u_t^x is t.
3. If u is a constant symbol, then u_t^x is u.
4. If $u :\equiv f u_1 u_2 \ldots u_n$, where f is an n-ary function symbol and the u_i are terms, then u_t^x is $f (u_1)_t^x (u_2)_t^x \ldots (u_n)_t^x$.

> *Chaff:* In the fourth clause of the definition above and in the first two clauses of the next definition, the parentheses are not really there. However, we believe that no one can look at $u_1 {}_t^x$ and figure out what it is supposed to mean. So the parentheses have been added in the interest of readability.

For example, if we let t be $g(c)$ and we let u be $f(x, y) + h(z, x, g(x))$, then u_t^x is

$$f(g(c), y) + h(z, g(c), g(g(c))). \tag{2.5.9.1}$$

The definition of substitution into a formula is also by recursion:

Definition 1.8.2. Suppose that ϕ is an $\mathcal{L}$-formula, t is a term, and x is a variable. We define the formula ϕ_t^x (read "ϕ with x replaced by t") as follows:

1. If $\phi :\equiv = u_1 u_2$, then ϕ_t^x is $= (u_1)_t^x (u_2)_t^x$.
2. If $\phi :\equiv R u_1 u_2 \ldots u_n$, then ϕ_t^x is $R (u_1)_t^x (u_2)_t^x \ldots (u_n)_t^x$.
3. If $\phi :\equiv \neg(\alpha)$, then ϕ_t^x is $\neg(\alpha_t^x)$.
4. If $\phi :\equiv (\alpha \vee \beta)$, then ϕ_t^x is $(\alpha_t^x \vee \beta_t^x)$.
5. If $\phi :\equiv (\forall y)(\alpha)$, then

$$\phi_t^x = \begin{cases} \phi & \text{if } x \text{ is } y \\ (\forall y)(\alpha_t^x) & \text{otherwise} \end{cases} \tag{2.5.9.2}$$

As an example, suppose that ϕ is the formula

$$P(x, y) \to [(\forall x) Q(g(x), z)) \vee (\forall y)(R(x, h(x))]. \tag{2.5.9.3}$$

Then, if t is the term $g(c)$, we get

$$\phi_t^x \text{ is} P(g(c), y) \to [(\forall x)(Q(g(x), z))) \vee (\forall y)(R(g(c), h(g(c)))]. \tag{2.5.9.4}$$

Having defined what we mean when we substitute a term for a variable, we will now define what it means for a term to be substitutable for a variable in a formula. The idea is that if t is substitutable for a variable in a formula. The idea is that if t is substitutable for x in ϕ, we will not run into the problems discussed at the beginning of this section - we will not substitute a term in such a way that a variable contained in that term is inadvertently bound by a quantifier.

Definition 1.8.3. Suppose that ϕ is an $\mathcal{L}$-formula, t is a term, and x is a variable. We way that **t is substitutable for x in ϕ** if

1. ϕ is atomic, or
2. $\phi :\equiv \neg(\alpha)$ and t is substitutable for x in α, or

3. $\phi :\equiv (\alpha \vee \beta)$ and t is substitutable for x in both α and β, or
4. $\phi :\equiv (\forall y)(\alpha)$ and either
   (a) x is not free in ϕ, or
   (b) y does not occur in t and t is substitutable for x in α

Notice that ϕ_t^x is defined whether or not t is substitutable for x in ϕ. Usually we will not want to do a substitution unless we check for substitutability, but we have the ability to substitute whether or not it is a good idea. In the next chapter, however, you will often see that certain operations are allowed only if t is substitutable for x in ϕ. That restriction is there for good reason, as we will be concerned with preserving the truth of formulas after performing substitutions.

Exercises

1. For each of the following, write out u_t^x:
   (a) $u :\equiv \cos x$, t is $\sin y$.
   (b) $u :\equiv y$, t is Sy.
   (c) $u :\equiv \sharp(x, y, z)$, t is $423 - w$.
2. For each of the following, first write out ϕ_t^x, then decide if t is substitutable for x in ϕ, and then (if you haven't already) use the definition of substitutability to justify your conclusions.
   (a) $\phi :\equiv \forall x\,(x = y \to Sx = Sy)$, t is $S0$.
   (b) $\phi :\equiv \forall y\,(x = y \to Sx = Sy)$, t is Sy.
   (c) $\phi :\equiv x = y \to (\forall x)\,(Sx = Sy)$, t is Sy.
3. Show that if t is variable-free, then t is always substitutable for x in ϕ.
4. Show that x is always substitutable for x in ϕ.
5. Prove that if x is not free in ψ, then ψ_t^x is ψ.
6. You might think that $(\phi_y^x)_x^y$ is ϕ, but a moment's thought will give you an example to show that this doesn't always work. (What if y is free in ϕ?) Find an example that shows that even if y is not free in ϕ, we can still have $(\phi_y^x)_x^y$ different from ϕ. Under what conditions do we know that $(\phi_y^x)_x^y$ is ϕ?
7. Write a computer program (in your favorite language, or in pseudo-code) that accepts as input a formula ϕ, a variable x, and a term t and outputs "yes" or "no" depending on whether or not t is substitutable for x in ϕ.

2.5.10: Logical Implication

At first glance it seems that a large portion of mathematics can be broken down into answering questions of the form: If I know this statement is true, is it necessarily the case that this other statement is true? In this section we will formalize that question.

Definition 1.9.1. Suppose that Δ and Γ are sets of $\mathcal{L}$-formulas. We will say that **Δ logically implies Γ** and write $\Delta \models \Gamma$ if for every $\mathcal{L}$-structure $\mathfrak{A}$, if $\mathfrak{A} \models \Delta$, then $\mathfrak{A} \models \Gamma$.

This definition is a little bit tricky. It says that if Δ is true in $\mathfrak{A}$, then Γ is true in $\mathfrak{A}$. Remember, for Δ to be true in $\mathfrak{A}$, it must be the case that $\mathfrak{A} \models \Delta[s]$ for *every* assignment function s. See Exercise 4.

If $\Gamma = \{\gamma\}$ is a set consisting of a single formula, we will write $\Delta \models \gamma$ rather than the official $\Delta \models \{\gamma\}$.

Definition 1.9.2. An $\mathcal{L}$-formula ϕ is said to be **valid** if $\emptyset \models \phi$, in other words, if ϕ is true in every $\mathcal{L}$-structure with every assignment function s. In this case, we will write $\models \phi$.

> *Chaff:* It doesn't seem like it would be easy to check whether $\Delta \models \Gamma$. To do so directly would mean that we would have to examine every possible $\mathcal{L}$-structure and every possible assignment function \(s\, of which there will be many.
>
> I'm also sure that you've noticed that this double turnstyle symbol, $\models$, is getting a lot of use. Just remember that if there is a structure on the left, $\mathfrak{A} \models \sigma$, we are discussing truth in a single structure. If there is a set of sentences on the left, $\Gamma \models \sigma$, then we are discussing logical implication.

Example 1.9.3. Let $\mathcal{L}$ be the language consisting of a single binary relation symbol, P, and let σ be the sentence $(\exists y \forall x P(x,y)) \rightarrow (\forall x \exists y P(x,y))$. We show that σ is valid.

So let $\mathfrak{A}$ be any $\mathcal{L}$-structure and let $s : Vars \rightarrow A$ be any assignment function. We must show that

$$\mathfrak{A} \models [(\exists y \forall x P(x,y)) \rightarrow (\forall x \exists y P(x,y))][s]. \tag{2.5.10.1}$$

Assume that $\mathfrak{A} \models (\exists y \forall x P(x,y))[s]$, we know that there is an element of the universe, A, such that $\mathfrak{A} \models \forall x P(x,y)[s[y|a]]$. And so, again by the definition of satisfaction, we know that if b is any element of A, $\mathfrak{A} \models P(x,y)[(s[y|a])[x|b]]$. If we chase through the definition of satisfaction (Definition 1.7.4) and of the various assignment functions, this means that for our one fixed a, the ordered pair $(b,a) \in P^{\mathfrak{A}}$ for any choice of $b \in A$.

We have to prove that $\mathfrak{A} \models (\forall x \exists y P(x,y))[s]$. As the statement of interest is universal, we must show that, if c is an arbitrary element of A, $\mathfrak{A} \models \exists y P(x,y)[s[x|c]]$, which means that we must produce an element of the universe, d, such that $\mathfrak{A} \models P(x,y)[(s[x|c])[y|d]]$. Again, from the definition of satisfaction this means that we must find a $d \in A$ such that $(c,d) \in P^{\mathfrak{A}}$. Fortunately, we have such a d in hand, namely a. As we know, $(c,a) \in P^{\mathfrak{A}}$, we have shown $\mathfrak{A} \models (\forall x \exists y P(x,y))[s]$, and we are finished.

Exercises

1. Show that $\{\alpha, \alpha \rightarrow \beta\} \models \beta$ for any formulas α and β. Translate this result into everyday English. Or Norwegian, if you prefer.
2. Show that the formula $x = x$ is valid. Show that the formula $x = y$ is not valid. What can you prove about the formula $\neg x = y$ in terms of validity?
3. Suppose that ϕ is an $\mathcal{L}$-formula and x is a variable. Prove that ϕ is valid if and only if $(\forall x)(\phi)$ is valid. Thus, if ϕ has free variables x, y, and z, ϕ will be valid if and only if $\forall x \forall y \forall z \phi$ is valid. The sentence $\forall x \forall y \forall z \phi$ is called the **universal closure** of ϕ.
4. (a) Assume that $\models (\phi \rightarrow \psi)$. Show that $\phi \models \psi$.
   (b) Suppose that ϕ is $x < y$ and ψ is $z < w$. Show that $\phi \models \psi$ but $\not\models (\phi \rightarrow \psi)$. (The slash through $\models$ means "does not logically imply.")

   [This exercise shows that the two possible ways to define logical equivalence are not equivalent. The strong form of the definition says that ϕ and ψ are logically equivalent if $\models (\phi \rightarrow \psi)$ and $\models (\psi \rightarrow \phi)$. The weak form of the definition states that ϕ and ψ are logically equivalent if $\phi \models \psi$ and $\psi \models \phi$.]

2.S: Logical Reasoning (Summary)

Important Definitions

- Logically equivalent statements, page 43
- Converse of a conditional statement, page 44
- Contrapositive of a conditional statement, page 44
- Equal sets, page 55
- Variable, page 54
- Universal set for a variable, page 54
- Constant, page 54
- Predicate, page 54
- Open sentence, page 54
- Truth set of a predicate, page 58
- Universal quantifier, page 63
- Existential quantifier, page 63
- Empty set, page 60
- Counterexample, page 66 and 69
- Perfect square, page 70
- Prime number, page 78
- Composite number, page 78

Important Theorems and Results

Theorem 2.8. Important Logical Equivalencies. *For statements P, Q, and R,*

De Morgan's Laws $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$
$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$

Conditional Statement $P \to Q \equiv \neg Q \to \neg P$ (contrapostitive)
$P \to Q \equiv \neg P \vee Q$
$\neg(P \to Q) \equiv P \wedge \neg Q$

Biconditional Statement $(P \leftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P)$

Double Negation $\neg(\neg P) \equiv P$

Distributive Laws $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$

Conditionals with Disjunctions $P \to (Q \vee R) \equiv (P \wedge \neg Q) \to R$
$P \vee Q) \to R \equiv (P \to R) \wedge (Q \to R)$

Theorem 2.16. Negations of Quantified Statements. *For any predicate $P(x)$,*

$$\neg(\forall x)[P(x)] \equiv (\exists x)[\neg P(x)], \text{ and}$$
$$\neg(\exists x)[P(x)] \equiv (\forall x)[\neg P(x)]$$

Important Set Theory Notation

Notation	Description	Page
$y \in A$	y is an element of the set A.	55
$z \notin A$	z is not an element of the set A.	55
{ }	The roster method	53
$\{x \in U \mid P(x)\}$	Set builder notation	58

platform; a detailed edit history is available upon request.

- **2.S: Logical Reasoning (Summary)** by Ted Sundstrom is licensed CC BY-NC-SA 3.0. Original source: https://scholarworks.gvsu.edu/books/7.

CHAPTER OVERVIEW

3: Constructing and Writing Proofs in Mathematics

A *proof* in mathematics is a convincing argument that some mathematical statement is true. A proof should contain enough mathematical detail to be convincing to the person(s) to whom the proof is addressed. In essence, a proof is an argument that communicates a mathematical truth to another person (who has the appropriate mathematical background). A proof must use correct, logical reasoning and be based on previously established results. These previous results can be axioms, definitions, or previously proven theorems. These terms are discussed in the sections below.

3.1: Direct Proofs

Preview Activity 1 (Definition of Divides, Divisor, Multiple)

In Section 1.2, we studied the concepts of even integers and odd integers. The definition of an even integer was a formalization of our concept of an even integer as being one this is "divisible by 2," or a "multiple of 2." We could also say that if "2 divides an integer," then that integer is an even integer. We will now extend this idea to integers other than 2. Following is a formal definition of what it means to say that a nonzero integer m divides an integer n.

Definition

A nonzero integer m **divides** an integer n provided that there is an integer q such that $n = m \cdot q$. We also say that m is a **divisor** of n, m is a **factor** of n, and n is a **multiple** of m. The integer 0 is not a divisor of any integer. If a and b are integers and $a \neq 0$, we frequently use the notation $a|b$as a shorthand for "a divides b."

A Note about Notation: Be careful with the notation $a|b$. This does not represent the rational number $\frac{a}{b}$. The notation $a|b$ represents a relationship between the integers a and b and is simply a shorthand for "a divides b."

A Note about Definitions: Technically, a definition in mathematics should almost always be written using "if and only if." It is not clear why, but the convention in mathematics is to replace the phrase "if and only if" with "if" or an equivalent. Perhaps this is a bit of laziness or the "if and only if" phrase can be a bit cumbersome. In this text, we will often use the phrase "provided that" instead.

The definition for "divides" can be written in symbolic form using appropriate quantifiers as follows: A nonzero integer m **divides** an integer n provided that $(\exists q \in \mathbb{Z})(n = m \cdot q)$.

1. Use the definition of divides to explain why 4 divides 32 and to explain why 8 divides -96.
2. Give several examples of two integers where the first integer does not divide the second integer.
3. According to the definition of "divides," does the integer 10 divide the integer 0? That is, is 10 a divisor of 0? Explain.
4. Use the definition of "divides" to complete the following sentence in symbolic form: "The nonzero integer m does not divide the integer n means that ...."
5. Use the definition of "divides" to complete the following sentence without using the symbols for quantifiers: "The nonzero integer m does not divide the integer n. ...."
6. Give three different examples of three integers where the first integer divides the second integer and the second integer divides the third integer.

   As we have seen in Section 1.2, a definition is frequently used when constructing and writing mathematical proofs. Consider the following conjecture:

   > **Conjecture:** Let a, b and c be integers with $a \neq 0$ and $b \neq 0$. If a divides b and b divides c, then a divides c.

7. Explain why the examples you generated in part (6) provide evidence that this conjecture is true.

   In Section 1.2, we also learned how to use a **know-show table** to help organize our thoughts when trying to construct a proof of a statement. If necessary, review the appropriate material in Section 1.2.

8. State precisely what we would assume if we were trying to write a proof of the preceding conjecture.
9. Use the definition of "divides" to make some conclusions based on your assumptions in part (8).
10. State precisely what we would be trying to prove if we were trying to write a proof of the conjecture.
11. Use the definition of divides to write an answer to the question, "How can we prove what we stated in part (10)?

Preview Activity 2 (Calendars and Clocks)

This preview activity is intended to help with understanding the concept of congruence, which will be studied at the end of this section.

1. Suppose that it is currently Tuesday. (a) What day will it be 3 days from now?
   (b) What day will it be 10 days from now?
   (c) What day will it be 17 days from now? What day will it be 24 days from now?
   (d) Find several other natural numbers x such that it will be Friday x days from now.

(e) Create a list (in increasing order) of the numbers 3; 10; 17; 24, and the numbers you generated in Part (1d). Pick any two numbers from this list and subtract one from the other. Repeat this several times.
(f) What do the numbers you obtained in Part (1e) have in common?

2. Suppose that we are using a twelve-hour clock with no distinction between A.M. and P.M. Also, suppose that the current time is 5:00. (a) What time will it be 4 hours from now?
(b) What time will it be 16 hours from now? What time will it be 28 hours from now?
(c) Find several other natural numbers x such that it will be 9:00 x hours from now.
(d) Create a list (in increasing order) of the numbers 4; 16; 28, and the numbers you generated in Part (2c). Pick any two numbers from this list and subtract one from the other. Repeat this several times.
(e) What do the numbers you obtained in Part (2d) have in common?
3. This is a continuation of Part (1). Suppose that it is currently Tuesday.

(a) What day was it 4 days ago?
(b) What day was it 11 days ago? What day was it 18 days ago?
(c) Find several other natural numbers x such that it was Friday x days ago.
(d) Create a list (in increasing order) consisting of the numbers18; 11; 4, the opposites of the numbers you generated in Part (3c) and the positive numbers in the list from Part (1e). Pick any two num- bers from this list and subtract one from the other. Repeat this several times.
(e) What do the numbers you obtained in Part (3d) have in common?

Some Mathematical Terminology

In Section 1.2, we introduced the idea of a direct proof. Since then, we have used some common terminology in mathematics without much explanation. Before we proceed further, we will discuss some frequently used mathematical terms.

A **proof** in mathematics is a convincing argument that some mathematical statement is true. A proof should contain enough mathematical detail to be convincing to the person(s) to whom the proof is addressed. In essence, a proof is an argument that communicates a mathematical truth to another person (who has the appropriate mathematical background). A proof must use correct, logical reasoning and be based on previously established results. These previous results can be axioms, definitions, or previously proven theorems. These terms are discussed below.

Surprising to some is the fact that in mathematics, there are always **undefined terms**. This is because if we tried to define everything, we would end up going in circles. Simply put, we must start somewhere. For example, in Euclidean geometry, the terms “point,” “line,” and “contains” are undefined terms. In this text, we are using our number systems such as the natural numbers and integers as undefined terms. We often assume that these undefined objects satisfy certain properties. These assumed relationships are accepted as true without proof and are called axioms (or postulates). An **axiom** is a mathematical statement that is accepted without proof. Euclidean geometry starts with undefined terms and a set of postulates and axioms. For example, the following statement is an axiom of Euclidean geometry:

Given any two distinct points, there is exactly one line that contains these two points.

> The closure properties of the number systems discussed in Section 1.1 and the properties of the number systems in Table 1.2 on page 18 are being used as axioms in this text.

A **definition** is simply an agreement as to the meaning of a particular term. For example, in this text, we have defined the terms “even integer” and “odd integer.” Definitions are not made at random, but rather, a definition is usually made because a certain property is observed to occur frequently. As a result, it becomes convenient to give this property its own special name. Definitions that have been made can be used in developing mathematical proofs. In fact, most proofs require the use of some definitions.

In dealing with mathematical statements, we frequently use the terms “conjecture,” “theorem,” “proposition,” “lemma,” and “corollary.” A **conjecture** is a statement that we believe is plausible. That is, we think it is true, but we have not yet developed a proof that it is true. A **theorem** is a mathematical statement for which we have a proof. A term that is often considered to be synonymous with “theorem” is proposition.

Often the proof of a theorem can be quite long. In this case, it is often easier to communicate the proof in smaller “pieces.” These supporting pieces are often called lemmas. A **lemma** is a true mathematical statement that was proven mainly to help in the proof of some theorem. Once a given theorem has been proven, it is often the case that other propositions follow immediately from the

fact that the theorem is true. These are called corollaries of the theorem. The term **corollary** is used to refer to a theorem that is easily proven once some other theorem has been proven.

Constructing Mathematical Proofs

To create a proof of a theorem, we must use correct logical reasoning and mathematical statements that we already accept as true. These statements include axioms, definitions, theorems, lemmas, and corollaries.

In Section 1.2, we introduced the use of a **know-show table** to help us organize our work when we are attempting to prove a statement. We also introduced some guidelines for writing mathematical proofs once we have created the proof. These guidelines should be reviewed before proceeding.

Please remember that when we start the process of writing a proof, we are essentially "reporting the news." That is, we have already discovered the proof, and now we need to report it. This reporting often does not describe the process of discovering the news (the investigative portion of the process).

Quite often, the first step is to develop a conjecture. This is often done after working within certain objects for some time. This is what we did in Preview Activity 3.1.1 when we used examples to provide evidence that the following conjecture is true:

> **Conjecture:** Let a, b and c be integers with $a \neq 0$ and $b \neq 0$. If a divides b and b divides c, then a devides c.

Before we try to prove a conjecture, we should make sure we have explored some examples. This simply means to construct some specific examples where the integers a, b, and c satisfy the hypothesis of the conjecture in order to see if they also satisfy the conclusion. We did this for this conjecture in Preview Activity 3.1.1.

We will now start a know-show table for this conjecture.

Step	**Know**	**Reason**
P	$a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $a\|b$ and $b\|c$	Hypothesis
$P1$		
...	...	...
$Q1$		
Q	$a\|c$	
Step	**Show**	**Reason**

The backward question we ask is, "How can we prove that a divides c?" One answer is to use the definition and show that there exists an integer q such that $c = a \cdot q$. This could be step $Q1$ in the know-show table.

We now have to prove that a certain integer q exists, so we ask the question, "How do we prove that this integer exists?" When we are at such a stage in the backward process of a proof, we usually turn to what is known in order to prove that the object exists or to find or construct the object we are trying to prove exists. We often say that we try to "construct" the object or at least prove it exists from the known information. So at this point, we go to the forward part of the proof to try to prove that there exists an integer q such that $c = a \cdot q$.

The forward question we ask is, "What can we conclude from the facts that $a|b$ and $b|c$?" Again, using the definition, we know that there exist integers s and t such that $b = a \cdot s$ and $c = b \cdot t$. This could be step $P1$ in the know-show table.

The key now is to determine how to get from $P1$ to $Q1$. That is, can we use the conclusions that the integers s and t exist in order to prove that the integer q (from the backward process) exists. Using the equation $b = a \cdot s$, we can substitute $a \cdot s$ for b in the second equation, $c = b \cdot t$. This gives

$$\begin{aligned} c &= b \cdot t \\ &= (a \cdot s) \cdot t \\ &= a(s \cdot t) . \end{aligned}$$

The last step used the associative property of multiplication. (See Table 1.2 on page 18.) This shows that c is equal to a times some integer. (This is because $s \cdot t$ is an integer by the closure property for integers.) So although we did not use the letter q, we have arrived at step $Q1$. The completed know-show table follows.

Step	Know	Reason
P	$a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $a \mid b$ and $b \mid c$	Hypothesis
$P1$	$(\exists s \in \mathbb{Z})(b = a \cdot s)$ $(\exists t \in \mathbb{Z})(c = b \cdot t)$	Definition of "Divides"
$P2$	$c = (a \cdot s) \cdot t$	Substitution for b
$P3$	$c = a \cdot (s \cdot t\ )$	Associative property of multiplication
$Q1$	$(\exists q \in \mathbb{Z})(c = a \cdot q)$	Step $P3$ and the closure properties of the integers
Q	$a \mid c$	Definition of "divides"

Notice the similarities between what we did for this proof and many of the proofs about even and odd integers we constructed in Section 1.2. When we try to prove that a certain object exists, we often use what is called the **construction method for a proof**. The appearance of an existential quantifier in the show (or backward) portion of the proof is usually the indicator to go to what is known in order to prove the object exists.

We can now report the news by writing a formal proof.

Theorem 3.1

Let a, b and c be integers with $a \neq 0$ and $b \neq 0$. If a divides b and b divides c, then a divides c.

Proof

We assume that a, b, and c are integers with $a \neq 0$ and $b \neq 0$. We further assume that a divides b and that b divides c. We will prove that a divides c.

Since a divides b and b divides c, there exist an integers s and t such that

$$b = a \cdot s, and \tag{3.1.1}$$

$$c = b \cdot t \tag{3.1.2}$$

We can now substitute the expression for b from equation (1) into equation (2). This gives

$$c = (a \cdot s) \cdot t\ .$$

Using the associate property for multiplication, we can rearrange the right side of the last equation to obtain

$$c = a \cdot (s \cdot t)\ .$$

Because both s and t are integers, and since the integers are closed under multiplication, we know that $s \cdot t \in \mathbb{Z}$. Therefore, the previous equation proves that a divides c. Consequently, we have proven that whenever a, b, and c are integers with $a \neq 0$ and $b \neq 0$ such that a divides b and b divides c, then a divides c.

Writing Guidelines for Equation Numbers

We wrote the proof for Theorem 3.1 according to the guidelines introduced in Section 1.2, but a new element that appeared in this proof was the use of equation numbers. Following are some guidelines that can be used for **equation numbers**.

If it is necessary to refer to an equation later in a proof, that equation should be centered and displayed. It should then be given it a number. The number for the equation should be written in parentheses on the same line as the equation at the right-hand margin as in shown in the following example.

Since x is an odd integer, there exists an integer n such that

$$x = 2n + 1 \tag{3.1.3}$$

.

Later in the proof, there may be a line such as

Then, using the result in equation (1), we obtain . . . .

Notice that we did not number every equation in Theorem 3.1. We should only number those equations we will be referring to later in the proof, and we should only number equations when it is necessary. For example, instead of numbering an equation, it is often better to use a phrase such as, "the previous equation proves that . . . " or "we can rearrange the terms on the right side of the previous equation." Also, note that the word "equation" is not capitalized when we are referring to an equation by number. Although it may be appropriate to use a capital "E," the usual convention in mathematics is not to capitalize.

? Progress Check 3.2 (A Property of Divisors)

1. Give at least four different examples of integers a, b, and c with $a \neq 0$ such that a divides b and a divides c.
2. For each example in Part (1), calculate the sum $b + c$. Does the integer a divide the sum $b + c$?
3. Construct a know-show table for the following proposition: For all integers a, b, and c with $a \neq 0$, if a divides b and a divides c, then a divides $b + c$.

Answer

Add texts here. Do not delete this text first.

Using Counterexamples

In Section 1.2 and so far in this section, our focus has been on proving statements that involve universal quantifiers. However, another important skill for mathematicians is to be able to recognize when a statement is false and then to be able to prove that it is false. For example, suppose we want to know if the following proposition is true or false.

For each integer n, if 5 divides $n^2 - 1$, then 5 divides $n - 1$.

Suppose we start trying to prove this proposition. In the backward process, we would say that in order to prove that 5 divides $n - 1$, we can show that there exists an integer k such that

$$Q_1 : n - 1 = 5k \text{ or } n = 5k + 1 .$$

For the forward process, we could say that since 5 divides (n^2 - 1), we know that there exists an interger m such that

$$P_1 : n^2 - 1 = 5m \text{ or } n^2 = 5m + 1 .$$

The problem is that there is no straightforward way to use P_1 to prove Q_1. At this point, it would be a good idea to try some examples for n and try to find situations in which the hypothesis of the proposition is true. (In fact, this should have been done before we started trying to prove the proposition.) The following table summarizes the results of some of these explorations with values for n.

n	$n^2 - 1$	Does 5 divide $(n^2 - 1)$	$n - 1$	Does 5 divide $(n - 1)$
1	0	yes	0	yes
2	3	no	1	no
3	8	no	2	no
4	15	yes	3	no

We can stop exploring examples now since the last row in the table provides an example where the hypothesis is true and the conclusion is false. Recall from Section 2.4 (see page 69) that a **counterexample** for a statement of the form $\forall x \in U)(P(x))$ is an element a in the universal set for which $P(a)$ is false. So we have actually proved that the negation of the proposition is true.

When using a counterexample to prove a statement is false, we do not use the term "proof" since we reserve a proof for proving a proposition is true. We could summarize our work as follows:

Conjecture. For each integer n, if 5 divides (n^2 - 1), then 5 divides (n - 1).

The integer n = 4 is a counterexample that proves this conjecture is false. Notice that when n = 4, n^2 - 1 = 15 and 5 divides 15. Hence,the hypothesis of the conjecture is true in this case. In addition, n - 1 = 3 and 5 does not divide 3 and so the conclusion

of the conjecture is false in this case. Since this is an example where the hypothesis is true and the conclusion is false, the conjecture is false.

As a general rule of thumb, anytime we are trying to decide if a proposition is true or false, it is a good idea to try some examples first. The examples that are chosen should be ones in which the hypothesis of the proposition is true. If one of these examples makes the conclusion false, then we have found a counterexample and we know the proposition is false. If all of the examples produce a true conclusion, then we have evidence that the proposition is true and can try to write a proof.

? Progress Check 3.3: Using a Counterexample

Use a counterexample to prove the following statement is false.

For all integers a and b, if 5 divides a or 5 divides b, then 5 divides $(5a + b)$.

Answer

Add texts here. Do not delete this text first.

Congruence

What mathematicians call congruence is a concept used to describe cycles in the world of the integers. For example, the day of the week is a cyclic phenomenon in that the day of the week repeats every seven days. The time of the day is a cyclic phenomenon because it repeats every 12 hours if we use a 12-hour clock or every 24 hours if we use a 24-hour clock. We explored these two cyclic phenomena in Preview Activity 3.1.2.

Similar to what we saw in Preview Activity 3.1.2, if it is currently Monday, then it will be Wednesday 2 days from now, 9 days from now, 16 days from now, 23 days from now, and so on. In addition, it was Wednesday 5 days ago, 12 days ago, 19 days ago, and so on. Using negative numbers for time in the past, we generate the following list of numbers:

..., -19, -12, -5, 2, 9, 16, 23, ...

Notice that if we subtract any number in the list above from any other number in that list, we will obtain a multiple of 7. For example,

✓ Example:

16 - 2 = 14 = 7 · 2

(-5) - (9) = -14 = 7 · (-2)

16 - (-12) = 28 = 7 · 4.

Using the concept of congruence, we would say that all the numbers in this list are congruent modulo 7, but we first have to define when two numbers are congruent modulo some natural number n.

Definition

Let $n \in \mathbb{N}$. If a and b are integers, then we say that **a is congruent to b modulo n** provided that n divides $a - b$. A standard notation for this is $a \equiv b \pmod{n}$. This is read as "a is congruent to b modulo n" or "a is congruent to b mod n."

Notice that we can use the definition of divides to say that n divides $a - b$ if and only if there exists an integer k such that $a - b = nk$. So we can write

$$a \equiv b \pmod{n} \text{ means } (\exists k \in \mathbb{Z})(a - b = nk), \text{ or}$$
$$a \equiv b \pmod{n} \text{ means } (\exists k \in \mathbb{Z})(a = b + nk).$$

This means that in order to find integers that are congruent to b modulo n, we only need to add multiples of n to b. For example, to find integers that are congruent to 2 modulo 5, we add multiples of 5 to 2. This gives the following list:

... -13, -8, -3, 2, 7, 12, 17,...

We can also write this using set notation and say that

$$\{a \in \mathbb{Z} | a \equiv 2 \pmod 5\} = \{... -13, -8, -3, 2, 7, 12, 17,...\}$$

? Progress Check 3.4 (Congruence Modulo 8)

1. Determine at least eight different integers that are congruent to 5 modulo 8.
2. Usesetbuildernotationandtherostermethodtospecifythesetofallintegers

   that are congruent to 5 modulo 8.
3. Choose two integers that are congruent to 5 modulo 8 and add them. Then repeat this for at least five other pairs of integers that are congruent to 5 modulo 8.
4. Explain why all of the sums that were obtained in Part (3) are congruent to 2 modulo 8.

Answer

Add texts here. Do not delete this text first.

We will study the concept of congruence modulo n in much more detail later in the text. For now, we will work with the definition of congruence modulo n in the context of proofs. For example, all of the examples used in Progress Check 3.4should provide evidence that the following proposition is true.

Proposition 3.5.

For all integers a and b, if $a \equiv 5 \pmod 8$ and $b \equiv 5 \pmod 8$, then $(a + b) \equiv 2 \pmod 8$.

? Progress Check 3.6 (Proving Proposition 3.5)

We will use “backward questions” and “forward questions” to help construct a proof for Proposition 3.5. So, we might ask, “How do we prove that $(a + b) \equiv 2 \pmod 8$” One way to answer this is to use the definition of congruence and state that$(a + b) \equiv 2 \pmod 8$ provided that 8 divides $(a + b - 2)$.

1. Use the definition of divides to determine a way to prove that 8 divides $(a + b - 2)$.

   We now turn to what we know and ask, "What can we conclude from the assumptions that $a \equiv 5 \pmod 8$ and $b \equiv 5 \pmod 8$." We can again use the definition of congruence and conclude that 8 divides $(a - 5)$ and 8 divides $(b - 5)$.
2. Use the definition of divides to make conclusions based on the facts that 8 divides $(a - 5)$ and 8 divides $(b - 5)$.
3. Solve an equation from part (2) for a and for b.
4. Use the results from part (3) to prove that 8 divides $(a + b - 2)$.
5. Write a proof for Proposition 3.5.

Answer

Add texts here. Do not delete this text first.

Additional Writing Guidelines

We will now be writing many proofs, and it is important to make sure we write according to accepted guidelines so that our proofs may be understood by others. Some writing guidelines were introduced in Chapter 1. The first four writing guidelines given below can be considered general guidelines, and the last three can be considered as technical guidelines specific to writing in mathematics.

1. **Know your audience**. Every writer should have a clear idea of the intended audience for a piece of writing. In that way, the writer can give the right amount of information at the proper level of sophistication to communicate effectively. This is especially true for mathematical writing. For example, if a mathematician is writing a solution to a textbook problem for a solutions manual for instructors, the writing would be brief with many details omitted. However, if the writing was for a students’ solution manual, more details would be included.

2. **Use complete sentences and proper paragraph structure.** Good grammar is an important part of any writing. Therefore, conform to the accepted rules of grammar. Pay careful attention to the structure of sentences. Write proofs using **complete sentences** but avoid run-on sentences. Also, do not forget punctuation, and always use a spell checker when using a word processor.
3. **Keep it simple.** It is often difficult to understand a mathematical argument no matter how well it is written. Do not let your writing help make it more difficult for the reader. Use simple, declarative sentences and short paragraphs, each with a simple point.
4. **Write a first draft of your proof and then revise it**. Remember that a proof is written so that readers are able to read and understand the reasoning in the proof. Be clear and concise. Include details but do not ramble. Do not be satisfied with the first draft of a proof. Read it over and refine it. Just like any worthwhile activity, learning to write mathematics well takes practice and hard work. This can be frustrating. Everyone can be sure that there will be some proofs that are difficult to construct, but remember that proofs are a very important part of mathematics. So work hard and have fun.
5. **Do not use $*$ for multiplication or ^ for exponents.** Leave this type of notation for writing computer code. The use of this notation makes it difficult for humans to read. In addition, avoid using / for division when using a complex fraction.

   For example, it is very difficult to read $(x^3-3x^2+1/2)/(2x/3-7)$; the fraction

$$\frac{x^3-3x^2+\frac{1}{2}}{\frac{2x}{3}-7} \tag{3.1.4}$$

   is much easier to read.
6. **Do not use a mathematical symbol at the beginning of a sentence.** For example, we should not write, “Let n be an integer. n is an odd integer provided that . . . .” Many people find this hard to read and often have to re- read it to understand it. It would be better to write, “An integer n is an odd integer provided that . . . .”
7. **Use English and minimize the use of cumbersome notation.** Do not use the special symbols for quantifiers $\forall$ (for all), $exists$ (there exists), ϵ (such that), or $\therefore$ (therefore) in formal mathematical writing. It is often easier to write, and usually easier to read, if the English words are used instead of the sym- bols. For example, why make the reader interpret

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x+y=0) \tag{3.1.5}$$

   When it is possible to write
   For each real number x, there exists a real number y such that $x+y=0$, or, more succinctly (if appropriate),

   Every real number has an additive inverse.

? Exercise for section 3.1

1. Prove each of the following statements:

   (a) For all integers a, b, and c with $a \neq 0$, if $a|b$ and $a|c$, then $a|(b-c)$.
   (b) For each $n \in \mathbb{Z}$, if n is an odd integer, then n^3 is an odd integer.
   (c) For each integer a, if 4 divides (a - 1), then 4 divides (a^2 - 1).
2. For each of the following, use a counterexample to prove the statement is false.

   (a) For each odd natural number n, if $n>3$, then 3 divides (n^2 - 1).
   (b) For each natural number n, $(3\cdot 2^n+2\cdot 3^n+1\ )$ is a prime number.
   (c) For all real numbers x and y, $\sqrt{x^2+y^2}>2xy$.
   (d) For each integer a, if 4 divides (a^2 - 1), then 4 divides (a - 1).

3. Determine if each of the following statements is true or false. If a statement is true, then write a formal proof of that statement, and if it is false, then provide a counterexample that shows it is false.

   (a) For all integers a, b, and c with $a \neq 0$, if $a|b$, then $a|(bc)$.
   (b) For all integers a and b with $a \neq 0$, if $6|(ab)$, then $6|a$ or $6|b$.
   (c) For all integers a, b and c with $a \neq 0$, if a divides (b - 1) and a divides (c -1), then a divides (bc - 1).
   (d) For each integer n, if 7 divides $(n^2 - 4)$, then 7 divides $(n - 2)$.
   (e) For every integer n, $4n^2 + 7n + 6$ is an odd integer.
   (f) For every odd integer n, $4n^2 + 7n + 6$ is an odd integer
   (g) For all integer a, b, and d with $d \neq 0$, if d divides both $a - b$ and $a + b$, then d divides a.
   (h) For all integer a, b, and c with $a \neq 0$, if $a|(bc)$, then $a|b$ or $a|c$.
4. (a) If x and y are integers and $xy = 1$, explain why $x = 1$ or $x = -1$.
   (b) Is the following proposition true or false?
   For all nonzero integers a and b, if $a|b$ and $b|a$, then $a = \pm b$.
5. Prove the following proposition:

   Let a be an integer. If there exists an integer n such that $a|(4n + 3)$ and $a|(2n + 1)$, then $a = 1$ or $a = -1$.

   Hint: Use the fact that the only divisors of 1 are 1 and -1.
6. Determine if each of the following statements is true or false. If a statement is true, then write a formal proof of that statement, and if it is false, then provide a counterexample that shows it is false. (a) For each integer a, if there exists an integer n such that a divides $(8n + 7)$ and a divides $(4n + 1)$, then a divides 5.
   (a) For each integer a, if there exists an integer n such that a divides $(9n + 5)$ and a divides $(6n + 1)$, then a divides 7.
   (c) For each integer n, if n is odd, then 8 divides $(n^4 + 4n^2 + 11)$.
   (d) For each integer n, if n is odd, then 8 divides $(n^4 + n^2 + 2n)$.
7. Let a be an integer and let $n \in \mathbb{N}$.

   (a) Prove that if $a \equiv 0 \pmod{n}$, then $n|a$.
   (b) Prove that if $n|a$, then $a \equiv 0 \pmod{n}$.
8. Let a and b be integers. Prove that if $a \equiv 2 \pmod 3$ and $b \equiv 2 \pmod 3$, then

   (a) $a + b \equiv 1 \pmod 3$.
   (b) $a \cdot b \equiv 1 \pmod 3$.
9. Let a and b be integers. Prove that if $a \equiv 7 \pmod 8$ and $b \equiv 3 \pmod 8$, then

   (a) $a + b \equiv 2 \pmod 8$.
   (b) $a \cdot b \equiv 5 \pmod 8$.
10. Determine if each of the following propositions is true or false. Justify each conclusion.

    (a) For all integers a and b, if $ab \equiv 0 \pmod 6$, then $a \equiv 0 \pmod 6$ or $b \equiv \pmod 6$.
    (b) For each integer a, if $a \equiv 2 \pmod 8$, then $a^2 \equiv 4 \pmod 8$.
    (c) For each integer a, if $a^2 \equiv 4 \pmod 8$, then $a \equiv 2 \pmod 8$.
11. Let n be a natural number. Prove each of the following:

    (a) For every integer a, $a \equiv a \pmod n$.
    This is called the **reflexive property** of congruence modulo n.
    (b) For every integer a and b, if $a \equiv b \pmod n$, then $b \equiv a \pmod n$.
    This is called the **symmetric property** of congruence modulo n.
    (c) For every integer a, b and \9c\), if $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.
    This is called the **transitive property** of congruence modulo n.

12. Let n be a natural number and let a, b, c, and d be integers. Prove each of the following.

    (a) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a+c) \equiv (b+d) \pmod{n}$.
    (b) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

13. (a) Let a, b, and c be real numbers with $a \neq 0$. Explain how to use a part of the quadratic formula (called the discriminant) to determine if the quadratic equation $ax^2 + bx + c = 0$ has two real number solutions, one real number solution, or no real number solutions. (See Exercise (11) in Section 1.2 for a statement of the quadratic formula.)

    (b) Prove that if a, b, and c are real numbers for which $a > 0$ and $c < 0$, then one solution of the quadratic equation $ax^2 + bx + c = 0$ is a positive real number.

    (c) Prove that if a, b, and c are real numbers, if $a \neq 0$, $b > 0$ and $\frac{b}{2} < \sqrt{ac}$, then the quadratic equation $ax^2 + bx + c = 0$ has no real number solution.

14. Let h and k be real numbers and let r be a positive number. The equation for a circle whose center is at the point (h, k) and whose radius is r is

$$(x-h)^2 + (y-k)^2 = r^2 \tag{3.1.6}$$

    .

    We also know that if a and b are real numbers, then

    - The point (a, b) is inside the circle if $(a-h)^2 + (b-k)^2 < r^2$.
    - The point (a, b) is on the circle if $(a-h)^2 + (b-k)^2 = r^2$.
    - The point (a, b) is outside the circle if $(a-h)^2 + (b-k)^2 > r^2$.

    Prove that all points on or inside the circle whose equation is $(x-1)^2 + (y-2)^2 = 4$ are inside the circle whose equation is $x^2 + y^2 = 26$.

15. Let r be a positive real number. The equation for a circle of radius r whose center is the origin is $x^2 + y^2 = r^2$.

    (a) Use implicit differentiation to determine $\frac{dy}{dx}$.
    (b) Let (a, b) be a point on the circle with $a \neq 0$ and $b \neq 0$. Determine the slope of the line tangent to the circle at the point (a, b).
    (c) Prove that the radius of the circle to the point (a, b) is perpendicular to the line tangent to the circle at the point (a, b).
    Hint: Two lines (neither of which is horizontal) are perpendicular if and only if the products of their slopes is equal to -1.

16. Determine if each of the following statements is true or false. Provide a counterexample for statements that are false and provide a complete proof for those that are true.

    (a) For all real numbers x and y, $\sqrt{xy} \leq \frac{x+y}{2}$.
    (b) For all real numbers x and y, $xy \leq (\frac{x+y}{2})^2$.
    (c) For all nonnegative real numbers x and y, $\sqrt{xy} \leq \frac{x+y}{2}$.

17. Use one of the true in equalities in Exercise(16) to prove the following proposition.

    For each real number a, the value of x that gives the maximum value of $y = x(a-x)$ is $x = \frac{a}{2}$.

18. (a) State the Pythagorean Theorem for right triangles.
    The diagrams in Figure 3.1 will be used for the problems in this exercise.
    (b) In the diagram on the left, x is the length of a side of the equilateral triangle and h is the length of an altitude of the equilateral triangle. The labeling in the diagram shows the fact that the altitude intersects the base of the equilateral triangle at the midpoint of the base. Use the

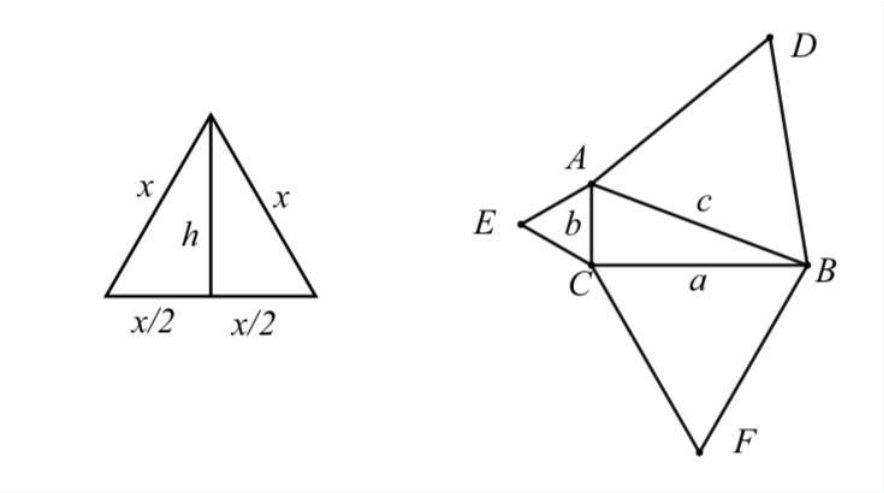


Figure 3.1: Diagrams for Exercise (18)

Pythagorean Theorem to prove that the area of this equilateral triangle is $\frac{\sqrt{3}}{4}x^2$.

(c) In the diagram on the right, $\triangle ABC$ is a right triangle. In addition, there has been an equilateral triangle constructed on each side of this right triangle. Prove that the area of the equilateral triangle on the hypotenuse is equal to the sum of the areas of the equilateral triangles constructed on the other two sides of the right triangle.

19. **Evaluation of proofs**

This type of exercise will appear frequently in the book. In each case, there is a proposed proof of a proposition. However, the proposition may be true or may be false.

• If a proposition is false, the proposed proof is, of course, incorrect. In this situation, you are to find the error in the proof and then provide a counterexample showing that the proposition is false.
• If a proposition is true, the proposed proof may still be incorrect. In this case, you are to determine why the proof is incorrect and then write a correct proof using the writing guidelines that have been presented in this book.
• If a proposition is true and the proof is correct, you are to decide if the proof is well written or not. If it is well written, then you simply must indicate that this is an excellent proof and needs no revision. On the other hand, if the proof is not well written, then you must then revise the proof so by writing it according to the guidelines presented in this text.

(a) **Proposition.** If m is an even integer, then $5m+4$ is an even integer.

Proof. We see that $5m+4=10n+4=2(5n+2)$. Therefore, $5m+4$ is an even integer.

(b) **Proposition.** For all real numbers x and y, if $x \neq y$, $x>0$, and $y>0$, then $\frac{x}{y}+\frac{y}{x}>2$.

Proof. Since x and y are positive real numbers, xy is positive and we can multiply both sides of the inequality by xy to obtain

$$(\frac{x}{y}+\frac{y}{x})\cdot xy > 2\cdot xy \tag{3.1.7}$$

$$x^2+y^2>2xy \tag{3.1.8}$$

.

By combining all terms on the left side of the inequality, we see that $x^2-2xy+y^2>0$ and then by factoring the left side, we obtain $(x-y)^2>0$. Since $x \neq y$, $(x-y)\neq 0$ and so $(x-y)^2>0$. This proves that if $x \neq y$, $x>0$, and $y>0$, any

$y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.

(c) Proposition. For all integers a, b, and c, if $a|(bc)$, then $a|b$ or $a|c$.

Proof. We assume that a, b, and c are integers and that a divides bc. So, there exists an integer k such that $bc = ka$. We now factor k as $k = mn$, where m and n are integers. We then see that

$$bc = mna \tag{3.1.9}$$

.

This means that $b = ma$ or $c = na$ and hence, $a|b$ or $a|c$.

(d) Proposition. For all positive integers a, b, and c, $(a^b)^c = a^{(b^c)}$.
This proposition is false as is shown by the following counterexample: If we let $a = 2$, $b = 3$, and $c = 2$, then

$$(a^b)^c = a^{b^c} \tag{3.1.10}$$

$$(2^3)^2 = 2^{3^2} \tag{3.1.11}$$

$$8^2 = 2^9 \tag{3.1.12}$$

$$64 \neq 512 \tag{3.1.13}$$

Explorations and Activities

20. **Congruence Modulo 6**

(a) Find several integers that are congruent to 5 modulo 6 and then square each of these integers.
(b) For each integer m from Part (20a), determine an integer k so that $0 \leq k < 6$ and $m^2 \equiv k \pmod 6$, then ...
(c) Based on the work in Part (20b), complete the following conjecture:

For each integer m, if $m \equiv 5 \pmod 6$, then ...
(d) Complete a know-show table for the conjecture in Part (20c) or write a proof of the conjecture.

21. **Pythagorean Triples**. Three natural numbers a, b, and c with $a < b < c$ are called a Pythagorean triple provided that $a^2 + b^2 = c^2$. See Exercise (13) on page 29 in Section 1.2. Three natural numbers are called **consecutive natural numbers** if they can be written in the form m, m + 1, and m + 2, where m is a natural number.

(a) Determine all Pythagorean triples consisting of three consecutive natural numbers. (State a theorem and prove it.)
(b) Determine all Pythagorean triples that can be written in the form m, $m + 7$, and $m + 8$, where m is a natural number. State a theorem and prove it.

Answer

Add texts here. Do not delete this text first.

detailed edit history is available upon request.

3.2: More Methods of Proof

Preview Activity 1: Using the Contrapositive

The following statement was proven in Exercise (3c) on page 27 in Section 1.2.

If n is an odd integer, then n^2 is an odd integer.

Now consider the following proposition:

For each integer n, if n^2 is an odd integer, then n is an odd integer.

1. After examining several examples, decide whether you think this proposition is true or false.
2. Try completing the following know-show table for a direct proof of this proposition. The question is, "Can we perform algebraic manipulations to get from the 'know' portion of the table to the 'show' portion of the table?" Be careful with this! Remember that we are working with integers and we want to make sure that we can end up with an integer q as stated in Step $Q1$.

Step	Know	Reason
P	n^2 is an odd integer	Hypothesis
$P1$	$(\forall k \in \mathbb{Z})(n^2 = 2k+1)$	Definition of "odd integer"
...	...	...
$Q1$	$(\forall q \in \mathbb{Z})(n = 2k+1)$	
Q	n is an odd integer.	Definition of "odd integer"
Step	**Show**	**Reason**

Recall that the contrapositive of the conditional statement $P \to Q$ is the conditional statement $\neg Q \to \neg P$. We have seen in Section 2.2 that the contrapositive of a conditional statement is logically equivalent to the conditional statement. (It might be a good idea to review Preview Activity $3.2.2$ from Section 2.2 on page 44.) Consider the following proposition once again:

For each integer n, if n^2 is an odd integer, then n is an odd integer.

3. Write the contrapositive of this conditional statement. Remember that "not odd" means "even."
4. Complete a know-show table for the contrapositive statement from Part(3).
5. By completing the proof in Part (4), have you proven the given proposition? That is, have you proven that if n^2 is an odd integer, then n is an odd integer? Explain.

Preview Activity 2: A Biconditional Statement

1. In Exercise (4a) from Section 2.2, we constructed a truth table to prove that the biconditional statement, $P \leftrightarrow Q$, is logically equivalent to $P \to Q) \wedge (Q \to P$. Complete this exercise if you have not already done so.
2. Suppose that we want to prove a biconditional statement of the form $P \leftrightarrow Q$. Explain a method for completing this proof based on the logical equivalency in part (1).
3. Let n be an integer. Assume that we have completed the proofs of the following two statements:
   - If n is an odd integer, then n2 is an odd integer.
   - If n2 is an odd integer, then n is an odd integer.

(See Exercise (3c) from Section 1.2 and Preview Activity $3.2.1$.) Have we completed the proof of the following proposition?

For each integer n, n is an odd integer if and only if n^2 is an odd integer. Explain.

Review of Direct Proofs

In Sections 1.2 and 3.1, we studied direct proofs of mathematical statements. Most of the statements we prove in mathematics are conditional statements that can be written in the form $P \to Q$. A direct proof of a statement of the form $P \to Q$ is based on the

definition that a conditional statement can only be false when the hypothesis, P, is true and the conclusion, Q, is false. Thus, if the conclusion is true whenever the hypothesis is true, then the conditional statement must be true. So, in a direct proof,

- We start by assuming that P is true.
- From this assumption, we logically deduce that Q is true.

We have used the so-called forward and backward method to discover how to logically deduce Q from the assumption that P is true.

Proof Using the Contrapositive

As we saw in Preview Activity 3.2.1, it is sometimes difficult to construct a direct proof of a conditional statement. This is one reason we studied logical equivalencies in Section 2.2. Knowing that two expressions are logically equivalent tells us that if we prove one, then we have also proven the other. In fact, once we know the truth value of a statement, then we know the truth value of any other statement that is logically equivalent to it.

One of the most useful logical equivalencies in this regard is that a conditional statement $P \to Q$ is logically equivalent to its contrapositive, $\neg Q \to \neg P$. This means that if we prove the contrapositive of the conditional statement, then we have proven the conditional statement. The following are some important points to remember.

- A conditional statement is logically equivalent to its contrapositive.
- Use a direct proof to prove that $\neg Q \to \neg P$ is true.
- Caution: One difficulty with this type of proof is in the formation of correct negations. (We need to be very careful doing this.)
- We might consider using a proof by contrapositive when the statements P and Q are stated as negations.

Writing Guidelines

One of the basic rules of writing mathematical proofs is to keep the reader informed. So when we prove a result using the contrapositive, we indicate this within the first few lines of the proof. For example,

- We will prove this theorem by proving its contrapositive.
- We will prove the contrapositive of this statement.

In addition, make sure the reader knows the status of every assertion that you make. That is, make sure you state whether an assertion is an assumption of the theorem, a previously proven result, a well-known result, or something from the reader's mathematical background. Following is a completed proof of a statement from Preview Activity 3.2.1.

Theorem 3.7

For each integer n, if n^2 is an even integer, then n is an even integer.

Proof

We will prove this result by proving the contrapositive of the statement, which is

For each integer n, if n is an odd integer, then n^2 is an odd integer.

However, in Theorem 1.8 on page 21, we have already proven that if x and y are odd integers, then $x \cdot y$ is an odd integer. So using $x = y = n$, we can conclude that if n is an odd integer, then $n \cdot n$, or n^2, is an odd integer. We have thus proved the contrapositive of the theorem, and consequently, we have proved that if n^2 is an even integer, then n is an even integer.

Using Other Logical Equivalencies

As was noted in Section 2.2, there are several different logical equivalencies. Fortunately, there are only a small number that we often use when trying to write proofs, and many of these are listed in Theorem 2.8 at the end of Section 2.2. We will illustrate the use of one of these logical equivalencies with the following proposition:

For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.

First, notice that the hypothesis and the conclusion of the conditional statement are stated in the form of negations. This suggests that we consider the contrapositive. Care must be taken when we negate the hypothesis since it is a conjunction. We use one of De Morgan's Laws as follows:

$$\neg(a \neq 0 \wedge b \neq 0) \equiv (a = 0) \vee (b = 0). \tag{3.2.1}$$

? Progress Check 3.8 (Using Another Logical Equivalency)

1. In English, write the contrapositive of, "For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$."

   The contrapositive is a conditional statement in the form $X \to (Y \vee Z$. The difficulty is that there is not much we can do with the hypothesis $ab = 0$ since we know nothing else about the real numbers a and b. However, if we knew that a was not equal to zero, then we could multiply both sides of the equation $ab = 0$ by $\frac{1}{a}$. This suggests that we consider using the following logical equivalency based on a result in Theorem 2.8 on page 48:

$$X \to (Y \vee Z) \equiv (X \wedge \neg Y) \to Z. \tag{3.2.2}$$

2. In English, use this logical equivalency, to write a statement that is logically equivalent to the contrapositive from Part (1).

   The logical equivalency in Part (2) makes sense because if we are trying to prove $Y \vee Z$, we only need to prove that at least one of Y or Z is true. So the idea is to prove that if Y is false, then Z must be true.

3. Use the ideas presented in the progress check to complete the proof of the following proposition.

Proposition 3.9.

For all real numbers a and b, if $a \neq$ and $b \neq 0$, then $ab \neq 0$.

Proof

We will prove the contrapositive of this proposition, which is

For all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

This contrapositive, however, is logically equivalent to the following:

For all real numbers a and b, if $ab = 0$ and $a \neq 0$, then $b = 0$.

To prove this, we let a and b be real numbers and assume that $ab = 0$ and$a \neq 0$. We can then multiply both sides of the equation $ab = 0$ by $\frac{1}{a}$. This gives

Now complete the proof.

...

Therefore, $b = 0$. This completes the proof of a statement that is logically equivalent to the contrapositive, and hence, we have proven the proposition.

Answer

Add texts here. Do not delete this text first.

Proofs of Biconditional Statements

In Preview Activity 3.2.2, we used the following logical equivalency:

$$(P \leftrightarrow Q) \equiv (P \to Q) \wedge (Q \to P). \tag{3.2.3}$$

This logical equivalency suggests one method for proving a biconditional statement written in the form "P if and only if Q." This method is to construct separate proofs of the two conditional statements $P \to Q$ and $Q \to P$. For example, since we have now proven each of the following:

- For each integer n, if n is an even integer, then n^2 is an even integer. (Exercise (3c) on page 27 in Section 1.2)
- For each integer n, if n^2 is an even integer, then n is an even integer. (Theorem 3.7)

We can state the following theorem.

Theorem 3.10.

For each integer n, n is an even integer if and only if n^2 is an even integer.

Writing Guidelines

When proving a biconditional statement using the logical equivalency $(P \leftrightarrow Q) \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$, we actually need to prove two conditional statements. The proof of each conditional statement can be considered as one of two parts of the proof of the biconditional statement. Make sure that the start and end of each of these parts is indicated clearly. This is illustrated in the proof of the following proposition.

Proposition 3.11

Let $x \in \mathbb{R}$. The real number x equals 2 if and only if $x^3 - 2x^2 + x = 2$.

Proof

We will prove this biconditional statement by proving the following two conditional statements:

- For each real number x, if x equals 2, then $x^3 - 2x^2 + x = 2$.
- For each real number x, if $x^3 - 2x^2 + x = 2$, then x equals 2.

For the first part, we assume $x = 2$ and prove that $x^3 - 2x^2 + x = 2$. We can do this by substituting $x = 2$ into the expression $x^3 - 2x^2 + x$. This gives

$$x^3 - 2x^2 + x = 2^3 - 2(2^2) + 2 = 8 - 8 + 2 = 2 \tag{3.2.4}$$

This completes the first part of the proof.

For the second part, we assume that $x^3 - 2x^2 + x = 2$ and from this assumption, we will prove that $x = 2$. We will do this by solving this equation for x. To do so, we first rewrite the equation $x^3 - 2x^2 + x = 2$ by subtracting 2 from both sides:

$$x^3 - 2x^2 + x - 2 = 0$$

We can now factor the left side of this equation by factoring an x from the first two terms and then factoring $(x - 2)$ from the resulting two terms. This is shown below.

$$x^3 - 2x^2 + x - 2 = 0$$
$$x^2(x - 2) + x - 2 = 0$$
$$(x - 2)(x^2 + 1) = 0$$

Now, in the real numbers, if a product of two factors is equal to zero, then one of the factors must be zero. So this last equation implies that

$$x - 2 = 0 \text{ or } x^2 + 1 = 0$$

The equation $x^2 + 1 = 0$ has not real numbers solution. So since x is a real number, the only possibility is that $x - 2 = 0$. From this we can conclude that x must be equal to 2.

Since we have now proven both conditional statements, we have proven that $x = 2$ if and only if $x^3 - 2x^2 + x = 2$

Constructive Proofs

We all know how to solve an equation such as $3x + 8 = 23$, where x is a real number. To do so, we first add -8 to both sides of the equation and then divide both sides of the resulting equation by 3. Doing so, we obtain the following result:

If x is a real number and $3x + 8 = 23$, then $x = 5$.

Notice that the process of solving the equation actually does not prove that $x = 5$ is a solution of the equation $3x + 8 = 23$. This process really shows that if there is a solution, then that solution must be $x = 5$. To show that this is a solution, we use the process of substituting 5 for x in the left side of the equation as follows: If $x = 5$,then

$$3x+8=3(5)+8=15+8=23$$

This proves that $x=5$ is a solution of the equation $3x+8=23$. Hence, we have proven that $x=5$ is the only real number solution of $3x+8=23$.

We can use this same process to show that any linear equation has a real number solution. An equation of the form

$$ax+b=c \tag{3.2.5}$$

,

where a, b, and c are real numbers with $a\neq 0$, is called a **linear equation in one variable.**

Proposition 3.12

If a, b, and c are real numbers with $a\neq 0$, then the linear equation $ax+b=c$ has exactly one real number solution, which is $x=\dfrac{c-b}{a}$.

Proof

Assume that a, b, and c are real numbers with $a\neq 0$. We can solve the linear equation $ax+b=c$ by adding $-b$ to both sides of the equation and then dividing both sides of the resulting equation by a (since $a\neq 0$, to obtain

$$x=\frac{c-b}{a}.$$

This shows that if there is a solution, then it must be $x=\dfrac{c-b}{a}$. We also see that if $x=\dfrac{c-b}{a}$, then,

$$ax+b=a(\frac{c-b}{a})+b=(c-b)+b=c$$

Therefore, the linear equation $ax+b=c$ has exactly one real number solution and the solution is $x=\dfrac{c-b}{a}$.

The proof given for Proposition 3.12 is called a **constructive proof**. This is a technique that is often used to prove a so-called **existence theorem.** The objective of an existence theorem is to prove that a certain mathematical object exists. That is, the goal is usually to prove a statement of the form

There exists an x such that $P(x)$.

For a constructive proof of such a proposition, we actually name, describe, or explain how to construct some object in the universe that makes $P(x)$ true. This is what we did in Proposition 3.12 since in the proof, we actually proved that $\dfrac{c-b}{a}$ is a solution of the equation $ax+b=c$. In fact, we proved that this is the only solution of this equation.

Nonconstructive Proofs

Another type of proof that is often used to prove an existence theorem is the so- called **nonconstructive proof**. For this type of proof, we make an argument that an object in the universal set that makes $P(x)$ true must exist but we never construct or name the object that makes $P(x)$ true. The advantage of a constructive proof over a nonconstructive proof is that the constructive proof will yield a procedure or algorithm for obtaining the desired object.

The proof of the **Intermediate Value Theorem** from calculus is an example of a nonconstructive proof. The Intermediate Value Theorem can be stated as follows:

> If f is a continuous function on the closed interval $[a, b]$ and if q is any real number strictly between $f(a)$ and $f(b)$, then there exists a number c in the interval (a, b) such that $f(c)=q$.

The Intermediate Value Theorem can be used to prove that a solution to some equations must exist. This is shown in the next example.

Example 3.13 (Using the Intermediate Value Theorem)

Let x represent a real number. We will use the Intermediate Value Theorem to prove that the equation $x^3 - x + 1 = 0$ has a real number solution.

To investigate solutions of thee quation $x^3 - x + 1 = 0$, we will use the function

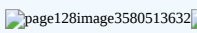
$$f(x) = x^3 - x + 1 = 0$$

Notice that $f(-2)$ = -5 and that $f(0) > 1$. Since $f(-2) < 0$ and $f(0 > 0$, the Intermediate Value Theorem tells us that there is a real number c between -2 and 0 such that $f(c) = 0$. This means that there exists a real number c between -2 and 0 such that

$$c^3 - c + 1 = 0 \ ,$$

and hence c is a real number solution of the equation $x^3 - x + 1 = 0$. This proves that the equation $x^3 - x + 1 = 0$ has at least one real number solution.

Notice that this proof does not tell us how to find the exact value of c. It does, however, suggest a method for approximating the value of c. This can be done by finding smaller and smaller intervals $[a, b]$ such that $f(a)$ and $f(b)$ have opposite signs.




1. Let n be an integer. Prove each of the following:

   (a) If n is even, then n^3 is even.
   (b) If n^3 is even, then n is even.
   (c) The integer n is even if and only if n^3 is an even integer.
   (d) The integer n is odd if and only if n^3 is an odd integer.
2. In Section 3.1, we defined congruence modulo n where n is a natural number. If a and b are integers, we will use the notation $a \not\equiv b \pmod{n}$ to mean that a is not congruent to b modulo n.

   (a) Write the contrapositive of the following conditional statement:
   For all integers a and b, if $a \not\equiv 0 \pmod{6}$ and $b \not\equiv 0 \pmod{6}$, then $ab \not\equiv 0 \pmod{6}$.

   (b) Is this statement true or false? Explain.
3. (a) Write the contrapositive of the following statement:

   For all positive real numbers a and b, if $\sqrt{ab} \neq \dfrac{a+b}{2}$, then $a \neq b$.
   (b) Is this statement true or false? Prove the statement if it is true or provide a counterexample if it is false.
4. Are the following statements true or false? Justify your conclusions.
   (a) For each $a \in \mathbb{Z}$, if $a \equiv 2 \pmod{5}$, then $a^2 \equiv 4 \pmod{5}$.
   (b) For each $a \in \mathbb{Z}$, if $a^2 \equiv 4 \pmod{5}$, then $a \equiv 2 \pmod{5}$.
   (c) For each $a \in \mathbb{Z}$, $a \equiv 2 \pmod{5}$ if and only if $a^2 \equiv 4 \pmod{5}$.
5. Is the following proposition true or false?

   For all integers a and b, if ab is even, then a is even or b is even.

   Justify your conclusion by writing a proof if the proposition is true or by providing a counterexample if it is false.
6. Consider the following proposition: For each integer a, $a \equiv 3 \pmod{7}$ if and only if $(a^2 + 5a)) \equiv 3 \pmod{7}$.

   (a) Write the proposition as the conjunction of two conditional statements.
   (b) Determine if the two conditional statements in Part(a) are true or false. If a conditional statement is true, write a proof, and if it is false, provide a counterexample.
   (c) Is the given proposition true or false? Explain.

7. Consider the following proposition: For each integer a, $a \equiv 2 \pmod 8$ if and only if $(a^2 + 4a) \equiv 4 \pmod 8$.

   (a) Write the proposition as the conjunction of two conditional statements.
   (b) Determine if the two conditional statements in Part(a) are true or false. If a conditional statement is true, write a proof, and if it is false, provide a counterexample.
   (c) Is the given proposition true or false? Explain.
8. For a right triangle, suppose that the hypotenuse has length c feet and the lengths of the sides are a feet and b feet.

   (a) What is a formula for the area of this right triangle? What is an isosceles triangle?
   (b) State the Pythagorean Theorem for right triangles.
   (c) Prove that the right triangle describe above is an isosceles triangle if and only if the area of the right triangle is $\frac{1}{4}c^2$.
9. A real number x is defined to be a **rational number** provided

   there exist integers m and n with $n \neq 0$ such that $x = \frac{m}{n}$.

   A real number that is not a rational number is called an **irrational number**.It is known that if x is a positive rational number, then there exist positive integers m and n with $n \neq 0$ such that $x = \frac{m}{n}$
   Is the following proposition true or false? Explain.
   For each positive real number x, if x is irrational, then $\sqrt{x}$ is irrational.
10. Is the following proposition true or false? Justify your conclusion.

    For each integer n, n is even if and only if 4 divides n^2.
11. Prove that for each integer a, if $a^2 - 1$ is even, then 4 divides $a^2 - 1$.
12. Prove that for all integers a and m, if a and m are the lengths of the sides of a right triangle and $m + 1$ is the length of the hypotenuse, then a is an odd integer.
13. Prove the following proposition:

    If $p, q \in \mathbb{Q}$ with $p < q$, then there exists an $x \in \mathbb{Q}$ with $p < x < q$.
14. Are the following propositions true or false? Justify your conclusion.

    (a) There exist integers x and y such that $4x + 6y = 2$.
    (b) There exist integers x and y such that $6x + 15y = 2$.
    (c) There exist integers x and y such that $6x + 15y = 9$.
15. Prove that there exists a real number x such that $x^3 - 4x^2 = 7$.
16. Let y_1, y_2, y_3, y_4 be real numbers. The **mean**, $\bar{y}$, of these four numbers is defined to be the sum of the four numbers divided by 4, That is,

$$\bar{y} = \frac{y_1 + y_2 + y_3 + y_4}{4}. \tag{3.2.6}$$

    Prove that there exists a y_i with $1 \leq i \leq 4$ such that $y_i \geq \bar{y}$.
    Hint: One way is to let y_{max} be the largest of y_1, y_2, y_3, y_4.
17. Let a and b be natural numbers such that $a^2 = b^3$. Prove each of the propositions in Parts (6a) trough (6d). (The results of Exercise (1) and Theorem 3.10 may be helpful.)

    (a) If a is even, then 4 divides a.
    (b) If 4 divides a, then 4 divides b.
    (c) If 4 divides b, then 8 divides a.
    (d) If a is even, then 8 divides a.
    (e) Given an example of natural numbers a and b such that a is even and $a^2 = b^3$, but b is not divisible by 8.

18. Prove the following proposition:
Let a and b be integers with $a \neq 0$. If a does not divide b, then the equation $ax^3 + bx + (b + a) = 0$ does not have a solution that is a natural number.
Hint: It may be necessary to factor a sum of cubes. Recall that

$$u^3 + v^3 = (u + v)(u^2 - uv + v^2). \tag{3.2.7}$$

19. **Evaluation of Proofs**
See the instructions for Excercise (19) on page 100 from Section 3.1.
(a)

proposition

If m is an odd integer, then $(m + 6)$ is an odd integer.

Proof

For $m + 6$ to be an odd integer, there must exist an integer n such that

$$m + 6 = 2n + 1. \tag{3.2.8}$$

By subtracting 6 from both sides of this equation, we obtain

$$m = 2n - 6 + 1 = 2(n - 3) = 1. \tag{3.2.9}$$

By the closure properties of the integers, $(n - 3)$ is an integer, and hence, the last equation implies that m is an odd integer. This proves that if m is an odd integer, then $m + 6$ is an odd integer.

(b)

proposition

For all integers m and n, if mn is an even integer, then m is even or n is even.

Proof

For either m or n to be even, there exists an integer k such that $m = 2k$ or $n = 2k$. So if we multiply m and n, the product will contain a factor of 2 and, hence, mn will be even.

Explorations and Activities

20. Using a Logical Equivalency. Consider the following proposition:
Proposition. For all integers a and b, if 3 does not divide a and 3 does not divide b, then 3 does not divide the product $a \cdot b$.

(a) Notice that the hypothesis of the proposition is stated as a conjunction of two negations ("3 does not divide a and 3 does not divide b"). Also, the conclusion is stated as the negation of a sentence ("3 does not divide the product $a \cdot b$."). This often indicates that we should consider using a proof of the contrapositive. If we use the symbolic form $(\neg Q \wedge \neg R) \rightarrow \neg P$ as a model for this proposition, what is P, what is Q, and what is R?
(b) Write a symbolic form for the contrapositive of $(\neg Q \wedge \neg R) \rightarrow \neg P$.
(c) Write the contrapositive of the proposition as a conditional statement in English.
We do not yet have all the tools needed to prove the proposition or its contrapositive. However, later in the text, we will learn that the following proposition is true.

Proposition X. Let a be an integer. If 3 does not divide a, then there exist integers x and y such that $3x + ay = 1$.

(d) i. Find integers x and y guaranteed by Proposition X when $a = 5$.
ii. Find integers x and y guaranteed by Proposition X when $a = 2$.

iii. Find integers x and y guaranteed by Proposition X when $a = -2$.

(e) Assume that Proposition X is true and use it to help construct a proof of the contrapositive of the given proposition. In doing so, you will most likely have to use the logical equivalency $P \to (Q \vee R) \equiv (P \wedge \neg Q) \to R$.

Answer

Add texts here. Do not delete this text first.

3.3: Proof by Contradiction

Preview Activity 1 (Proof by Contradiction)

In Section 2.1, we defined a **tautology** to be a compound statement S that is true for all possible combinations of truth values of the component statements that are part of S. We also defined **contradiction** to be a compound statement that is false for all possible combinations of truth values of the component statements that are part of S.

That is, a tautology is necessarily true in all circumstances, and a contradiction is necessarily false in all circumstances.

1. Use truth tables to explain why $P \vee \neg P$ is a tautology and $P \wedge \neg P$ is a contradiction.

   Another method of proof that is frequently used in mathematics is a **proof by contradiction**. This method is based on the fact that a statement X can only be true or false (and not both). The idea is to prove that the statement X is true by showing that it cannot be false. This is done by assuming that X is false and proving that this leads to a contradiction. (The contradiction often has the form $R \wedge \neg R$, where R is some statement.) When this happens, we can conclude that the assumption that the statement X is false is incorrect and hence X cannot be false. Since it cannot be false, then X must be true.
   A logical basis for the contradiction method of proof is the tautology

   $$[\neg X \to C] \to X, \tag{3.3.1}$$

   where X is a statement and C is a contradiction. The following truth table establishes this tautology.

X	C	$\neg X$	$\neg X \to C$	$(\neg X \to C) \to X$
T	F	F	T	T
F	F	T	F	T

   This tautology shows that if $\neg X$ leads to a contradiction, then X must be true. The previous truth table also shows that the statement $\neg X \to C$ is logically equivalent to X. This means that if we have proved that $\neg X$ leads to a contradiction, then we have proved statement X. So if we want to prove a statement X using a proof by contradiction, we assume that $\neg X$ is true and show that this leads to a contradiction.

   When we try to prove the conditional statement, "If P then Q" using a proof by contradiction, we must assume that $P \to Q$ is false and show that this leads to a contradiction.

2. Use a truth table to show that $\neg(P \to Q)$ is logical equivalent to $P \wedge \neg Q$.

   The preceding logical equivalency shows that when we assume that $P \to Q$ is false, we are assuming that P is true and Q is false. If we can prove that this leads to a contradiction, then we have shown that $\neg(P \to Q)$ is false and hence that $P \to Q$ is true.

3. Given a counterexample to show that the following statement is false.

   For each real number x, $\dfrac{1}{x(1-x)} \geq 4$.

4. When a statement is false, it is sometimes possible to add an assumption that will yield a true statement. This is usually done by using a conditional statement. So instead of working with the statement in (3), we will work with a related statement that is obtained by adding an assumption (or assumptions) to the hypothesis.

   For each real number x, if $0 < x < 1$, then $\dfrac{1}{x(1-x)} \geq 4$.

   To begin a proof by contradiction for this statement, we need to assume the negation of the statement. To do this, we need to negate the entire statement, including the quantifier. Recall that the negation of a statement with a universal quantifier is a statement that contains an existential quantifier. (See Theorem 2.16 on page 67). With this in mind, carefully write down all assumptions made at the beginning of a proof by contradiction for this statement.

Preview Activity 2 (Constructing a Proof by Contradiction)

Consider the following proposition:

Proposition. For all real numbers x and y, if $x \neq y$, $x > 0$, and $y > 0$, then $\frac{x}{y} + \frac{y}{x} > 2$.

To start a proof by contradiction, we assume that this statement is false; that is, we assume the negation is true. Because this is a statement with a universal quantifier, we assume that there exist real numbers x and y such that $x \neq y$, $x > 0$, $y > 0$ and that $\frac{x}{y} + \frac{y}{x} \leq 2$. (Notice that the negation of the conditional sentence is a conjunction.)

For this proof by contradiction, we will only work with the know column of a know-show table. This is because we do not have a specific goal. The goal is to obtain some contradiction, but we do not know ahead of time what that contradiction will be. Using our assumptions, we can perform algebraic operations on the inequality

$$\frac{x}{y} + \frac{y}{x} \leq 2 \tag{3.3.2}$$

until we obtain a contradiction.

1. Try the following algebraic operations on the inequality in (2). First, multiply both sides of the inequality by xy, which is a positive real number since $x > 0$ and $y > 0$. Then, subtract $2xy$ from both sides of this inequality and finally, factor the left side of the resulting inequality.
2. Explain why the last inequality you obtained leads to a contradiction.

By obtaining a contradiction, we have proved that the proposition cannot be false, and hence, must be true.

Writing Guidelines: Keep the Reader Informed

A very important piece of information about a proof is the method of proof to be used. So when we are going to prove a result using the contrapositive or a proof by contradiction, we indicate this at the start of the proof.

- We will prove this result by proving the contrapositive of the statement.
- We will prove this statement using a proof by contradiction.
- We will use a proof by contradiction.

We have discussed the logic behind a proof by contradiction in the preview activities for this section. The basic idea for a proof by contradiction of a proposition is to assume the proposition is false and show that this leads to a contradiction. We can then conclude that the proposition cannot be false, and hence, must be true. When we assume a proposition is false, we are, in effect, assuming that its negation is true. This is one reason why it is so important to be able to write negations of propositions quickly and correctly. We will illustrate the process with the proposition discussed in Preview Activity 3.3.1.

Proposition 3.14

For each real number x, if $0 < x < 1$, then $\frac{1}{x(1-x)} \geq 4$

Proof

We will use a proof by contradiction. So we assume that the proposition is false, or that there exists a real number x such that $0 < x < 1$ and

$$\frac{1}{x(1-x)} < 4. \tag{3.3.3}$$

We note that since $0 < x < 1$, we can conclude that $x > 0$ and that $(1-x) > 0$. Hence, $x(1-x) > 0$ and if we multiply both sides of inequality (1) by $x(1-x)$, we obtain

$$1 < 4x(1-x).$$

We can now use algebra to rewrite the last inequality as follows:

$$1 < 4x - 4x^2$$

$$4x^2 - 4x + 1 < 0$$

$$(2x-1)^2 < 0$$

However, $(2x-1)$ is a real number and the last inequality says that a real number squared is less than zero. This is a contradiction since the square of any real number must be greater than or equal to zero. Hence, the proposition cannot be false, and we have proved that for each real number x, if $0 < x < 1$, then $\dfrac{1}{x(1-x)} \geq 4$.

? Progress Check 3.15: Starting a Proof by Contradiction

One of the most important parts of a proof by contradiction is the very first part, which is to state the assumptions that will be used in the proof by contradiction. This usually involves writing a clear negation of the proposition to be proven. Review De Morgan's Laws and the negation of a conditional statement in Section 2.2. (See Theorem 2.8 on page 48.) Also, review Theorem 2.16 (on page 67) and then write a negation of each of the following statements. (Remember that a real number is "not irrational" means that the real number is rational.)

1. For each real number x, if x is irrational, then $\sqrt[3]{x}$ is irrational.
2. For each real number x, $(x+\sqrt{2})$ is irrational or $(-x+\sqrt{2})$ is irrational.
3. For all integers a and b, if 5 divides ab, then 5 divides a or 5 divides b.
4. For all real numbers a and b, if $a > 0$ and $b > 0$, then $\dfrac{2}{a} + \dfrac{2}{b} \neq \dfrac{4}{a+b}$.

Answer

Add texts here. Do not delete this text first.

Important Note

A proof by contradiction is often used to prove a conditional statement $P \to Q$ when a direct proof has not been found and it is relatively easy to form the negation of the proposition. The advantage of a proof by contradiction is that we have an additional assumption with which to work (since we assume not only P but also $\neg Q$). The disadvantage is that there is no well-defined goal to work toward. The goal is simply to obtain some contradiction. There usually is no way of telling beforehand what that contradiction will be, so we have to stay alert for a possible absurdity. Thus, when we set up a know-show table for a proof by contradiction, we really only work with the know portion of the table.

? Progress Check 3.16: Exploration and a Proof by Contradiction

Consider the following proposition:

For each integer n, if $n \equiv 2 \pmod 4$, then $n \not\equiv 3 \pmod 6$.

1. Determine at least five different integers that are congruent to 2 modulo 4, and determine at least five different integers that are congruent to 3 modulo 6. Are there any integers that are in both of these lists?
2. For this proposition, why does it seem reasonable to try a proof by contradiction?
3. For this proposition, state clearly the assumptions that need to be made at the beginning of a proof by contradiction, and then use a proof by contradiction to prove this proposition.

Answer

Add texts here. Do not delete this text first.

Proving that Something Does Not Exist

In mathematics, we sometimes need to prove that something does not exist or that something is not possible. Instead of trying to construct a direct proof, it is sometimes easier to use a proof by contradiction so that we can assume that the something exists. For example, suppose we want to prove the following proposition:

Proposition 3.17.

For all integers x and y, if x and y are odd integers, then there does not exist an integer z such that $x^2 + y^2 = z^2$.

Notice that the conclusion involves trying to prove that an integer with a certain property does not exist. If we use a proof by contradiction, we can assume that such an integer z exists. This gives us more with which to work.

? Progress Check 3.18

Complete the following proof of Proposition 3.17:

Proof. We will use a proof by contradiction. So we assume that there exist integers x and y such that x and y are odd and there exists an integer z such that $x^2 + y^2 = z^2$. Since x and y are odd, there exist integers m and n such that $x = 2m + 1$ and $y = 2n + 1$.

1. Use the assumptions that x and y are odd to prove that $x^2 + y^2$ is even and hence, z^2 is even. (See Theorem 3.7 on page 105.)

   We can now conclude that z is even. (See Theorem 3.7 on page 105.) So there exists an integer k such that $z = 2k$. If we substitute for x, y, and z in the equation $x^2 + y^2 = z^2$, we obtain

   $$(2m + 1)^2 + (2n + 1)^2 = (2k)^2. \tag{3.3.4}$$

2. Use the previous equation to obtain a contradiction. **Hint:** One way is to use algebra to obtain an equation where the left side is an odd integer and the right side is an even integer.

Answer

Add texts here. Do not delete this text first.

Rational and Irrational Numbers

One of the most important ways to classify real numbers is as a rational number or an irrational number. Following is the definition of rational (and irrational) numbers given in Exercise (9) from Section 3.2.

Definitions: Rational and Irrational Number

A real number x is defined to be a **rational number** provided that there exist integers m and n with $n \neq 0$ such that $x = \frac{m}{n}$.

A real number that is not a rational number is called an **irrational number**.

This may seem like a strange distinction because most people are quite familiar with the rational numbers (fractions) but the irrational numbers seem a bit unusual. However, there are many irrational numbers such as $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{2}$, π, and the number e. We are discussing these matters now because we will soon prove that $\sqrt{2}$ is irrational in Theorem 3.20.

We use the symbol $\mathbb{Q}$ to stand for the set of rational numbers. There is no standard symbol for the set of irrational numbers. Perhaps one reason for this is because of the closure properties of the rational numbers. We introduced closure properties in Section 1.1, and the rational numbers $\mathbb{Q}$ are closed under addition, subtraction, multiplication, and division by nonzero rational numbers. This means that if $x, y \in \mathbb{Q}$, then

- $x + y$, xy, and xy are in $\mathbb{Q}$; and
- If $y \neq 0$, then $\frac{x}{y}$ is in $\mathbb{Q}$.

The basic reasons for these facts are that if we add, subtract, multiply, or divide two fractions, the result is a fraction. One reason we do not have a symbol for the irrational numbers is that the irrational numbers are not closed under these operations. For example, we will prove that $\sqrt{2}$ is irrational in Theorem 3.20. We then see that

$$\sqrt{2}\sqrt{2} = 2 \text{ and } \frac{\sqrt{2}}{\sqrt{2}} = 1.$$

which shows that the product of irrational numbers can be rational and the quotient of irrational numbers can be rational.

It is also important to realize that every integer is a rational number since any integer can be written as a fraction. For example, we can write $3 = \frac{3}{1}$. In general, if $n \in \mathbb{Z}$, then $n = \frac{n}{1}$, and hence, $n \in \mathbb{Q}$.

Because the rational numbers are closed under the standard operations and the definition of an irrational number simply says that the number is not rational, we often use a proof by contradiction to prove that a number is irrational. This is illustrated in the next proposition.

Proposition 3.19

For all real numbers x and y, if x is rational and $x \neq 0$ and y is irrational, then $x \cdot y$ is irrational.

Proof

We will use a proof by contradiction. So we assume that there exist real numbers x and y such that x is rational, y is irrational, and $x \cdot y$ is rational. Since $x \neq 0$, we can divide by x, and since the rational numbers are closed under division by nonzero rational numbers, we know that $\frac{1}{x} \in \mathbb{Q}$. We now know that $x \cdot y$ and $\frac{1}{x}$ are rational numbers and since the rational numbers are closed under multiplication, we conclude that

$$\frac{1}{x} \cdot (xy) \in \mathbb{Q} \tag{3.3.5}$$

However, $\frac{1}{x} \cdot (xy) = y$ and hence, y must be a rational number. Since a real number cannot be both rational and irrational, this is a contradiction to the assumption that y is irrational. We have therefore proved that for all real numbers x and y, if x is rational and $x \neq 0$ and y is irrational, then $x \cdot y$ is irrational.

The Square Root of 2 Is an Irrational Number

The proof that the square root of 2 is an irrational number is one of the classic proofs in mathematics, and every mathematics student should know this proof. This is why we will be doing some preliminary work with rational numbers and integers before completing the proof. The theorem we will be proving can be stated as follows:

Theorem 3.20

If r is a real number such that $r^2 = 2$, then r is an irrational number.

This is stated in the form of a conditional statement, but it basically means that $\sqrt{2}$ is irrational (and that $-\sqrt{2}$ is irrational). That is, $\sqrt{2}$ cannot be written as a quotient of integers with the denominator not equal to zero.

In order to complete this proof, we need to be able to work with some basic facts that follow about rational numbers and even integers.

1. Each integer m is a rational number since m can be written as $m = \frac{m}{1}$.
2. Notice that $\frac{2}{3} = \frac{4}{6}$, since

$$\frac{4}{6} = \frac{2 \cdot 2}{3 \cdot 2} = \frac{2}{2} \cdot \frac{2}{3} = \frac{2}{3} \tag{3.3.6}$$

   We can also show that $\frac{15}{12} = \frac{5}{4}$, $\frac{10}{-8} = \frac{-5}{4}$, and $\frac{-30}{-16} = \frac{15}{8}$

   Item (2) was included to illustrate the fact that a rational number can be written as a fraction in "lowest terms" with a positive denominator. This means that any rational number can be written as a quotient $\frac{m}{n}$, where m and n are integers, $n > 0$, and m and n have no common factor greater than 1.
3. If n is an integer and n^2 is even, what can be conclude about n. Refer to theorem 3.7 on page 105.

In a proof by contradiction of a conditional statement $P \to Q$, we assume the negation of this statement or $P \wedge \neg Q$. So in a proof by contradiction of Theorem 3.20, we will assume that r is a real number, $r^2 = 2$, and r is not irrational (that is, r is rational).

Theorem 3.20

If r is a real number such that $r^2 = 2$, then r is an irrational number.

Proof

We will use a proof by contradiction. So we assume that the statement of the theorem is false. That is, we assume that

$$r \text{ is a real number, } r^2 = 2, \text{ and } r \text{ is a rational number.}$$

Since r is a rational number, there exist integers m and n with \(n > 0\0 such that

$$r = \frac{m}{n}$$

and m and n have no common factor greater than 1. We will obtain a contradiction by showing that m and n must both be even. Squaring both sides of the last equation and using the fact that $r^2 = 2$, we obtain

$$2 = \frac{m^2}{n^2}$$

$$m^2 = 2n^2 \tag{3.3.7}$$

Equation (1) implies that m^2 is even, and hence, by Theorem 3.7, m must be an even integer. This means that there exists an integer p such that $m = 2p$. We can now substitute this into equation (1), which gives

$$(2p)^2 = 2n^2$$

$$4p^2 = 2n^2. \tag{3.3.8}$$

We can divide both sides of equation (2) by 2 to obtain $n^2 = 2p^2$. Consequently, n^2 is even and we can once again use Theorem 3.7 to conclude that m is an even integer.

We have now established that both m and n are even. This means that 2 is a common factor of m and n, which contradicts the assumption that m and n have no common factor greater than 1. Consequently, the statement of the theorem cannot be false, and we have proved that if r is a real number such that $r^2 = 2$, then r is an irrational number.

Exercises for Section 3.3

1. This exercise is intended to provide another rationale as to why a proof by contradiction works.

   Suppose that we are trying to prove that a statement P is true. Instead of proving this statement, assume that we prove that the conditional statement "If $\neg P$, then C " is true, where C is some contradiction. Recall that a contradiction is a statement that is always false.

   (a) In symbols, write a statement that is a disjunction and that is logically equivalent to $\neg P \to C$.
   (b) Since we have proven that $\neg P \to C$ is true, then the disjunction in Exercise (1a) must also be true. Use this to explain why the statement P must be true.
   (c) Now explain why P must be true if we prove that the negation of P implies a contradiction.
2. Are the following statements true or false? Justify each conclusion.

   (a) For all integers a and b, if a is even and b is odd, then 4 does not divide $(a^2 + b^2)$.
   (b) For all integers a and b, if a is even and b is odd, then 6 does not divide $(a^2 + b^2)$.
   (c) For all integers a and b, if a is even and b is odd, then 4 does not divide $(a^2 + 2b^2)$.
   (d) For all integers a and b, if a is odd and b is odd, then 4 divides $(a^2 + 3b^2)$.
3. Consider the following statement:
   If r is a real number such that $r^2 = 18$, then r is irrational.

(a) If you were setting up a proof by contradiction for this statement, what would you assume? Carefully write down all conditions that you would assume.
(b) Complete a proof by contradiction for this statement.

4. Prove that the cube root of 2 is an irrational number. That is, prove that if r is a real number such that $r^3 = 2$, then r is an irrational number.
5. Prove the following propositions:

   (a) For all real numbers x and y, if x is rational and y is irrational, then $x + y$ is irrational.
   (b) For all nonzero real numbers x and y, if x is rational and y is irrational, then $\frac{x}{y}$ is irrational.
6. Are the following statements true or false? Justify each conclusion.

   (a) For each positive real number x, if x is irrational, then x^2 is irrational.
   (b) For each positive real number x, if x is irrational, then $\sqrt{x}$ is irrational.
   (c) For every pair of real numbers x and y, if $x + y$ is irrational, then x is irrational and y is irrational.
   (d) For every pair of real numbers x and y, if $x + y$ is irrational, then x is irrational or y is irrational.
7. (a) Give an example that shows that the sum of two irrational numbers can be a rational number.
   (b) Now explain why the following proof that $(\sqrt{2} + \sqrt{5})$ is an irrational number is not a valid proof: Since $\sqrt{2}$ and $\sqrt{5}$ are both irrational numbers, their sum is an irrational number. Therefore, $(\sqrt{2} + \sqrt{5})$ is an irrational number
   Note: You may even assume that we have proven that $\sqrt{5}$ is an irrational number. (We have not proven this.)
   (c) is the real number $\sqrt{2} + \sqrt{5}$ a rational number or an irrational number? Justify your conclusion.
8. (a) Prove that for each reach number x, $(x + \sqrt{2})$ is irrational or $(-x + \sqrt{2})$ is irrational.
   (b) Generalize the proposition in Part(a) for any irrational number (instead of just $\sqrt{2}$) and then prove the new proposition.
9. Is the following statement true or false?
   For all positive real number x and y, $\sqrt{x+y} \leq \sqrt{x} + \sqrt{y}$.
10. Is the following proposition true or false? Justify your conclusion.
    For each real number x, $x(1 - x) \leq \frac{1}{4}$.
11. (a) Is the base 2 logarithm of 32, $log_2 32$, a rational number or an irrational number? Justify your conclusion.
    (b) Is the base 2 logarithm of 3, $log_2 3$, a rational number or an irrational number? Justify your conclusion.
12. In Exercise (15) in Section 3.2, we proved that there exists a real number solution to the equation $x^3 - 4x^2 = 7$. Prove that there is no integer x such that $x^3 - 4x^2 = 7$.
13. Prove each of the following propositions:

    (a) For each real number θ, if $0 < \theta < \frac{\pi}{2}$, then $(sin\theta + cos\theta) > 1$.
    (b) For all real numbers a and b, if $a \neq 0$ and $b \neq 0$, then $\sqrt{a^2 + b^2} \neq a + b$.
    (c) If n is an integer greater than 2, then for all integers m, n does not divide m or $n + m \neq nm$.
    (d) For all numbers a and b, if $a > 0$ and $b > 0$, then

$$\frac{2}{a} + \frac{2}{b} \neq \frac{4}{a+b}. \tag{3.3.9}$$

14. Prove that there do not exist three consecutive natural numbers such that the cube of the largest is equal to the sum of the cubes of the other two.
15. Three natural numbers a, b, and c with $a < b < c$ are called a **Pythagorean** triple provided that $a^2 + b^2 = c^2$. For example, the numbers 3, 4, and 5 form a Pythagorean triple, and the numbers 5, 12, and 13 form a Pythagorean triple.

    (a) Verify that if $a = 20$, $b = 21$, and $c = 29$, then $a^2 + b^2 = c^2$, and hence, 20, 21, and 29 form a Pythagorean triple.
    (b) Determine two other Pythagorean triples. That is, find integers a, b, and c such that $a^2 + b^2 = c^2$.
    (c) Is the following proposition true or false? Justify your conclusion.
    For all integers a, b, and c, if $a^2 + b^2 = c^2$, then a is even or b is even.
16. Consider the following proposition: There are no integers a and b such that $b^2 = 4a + 2$.

    (a) Rewrite this statement in an equivalent form using a universal quantifier by completing the following:

For all integers a and b, ...
(b) Prove the statement in Part (a).

17. Is the following statement true or false? Justify your conclusion.

    For each integer n that is greater than 1, if a is the smallest positive factor of n that is greater than 1, then a is prime.

    See Exercise (13) in Section 2.4 (page 78) for the definition of a prime number and the definition of a composite number.

18. A **magic square** is a square array of natural numbers whose rows, columns, and diagonals all sum to the same number. For example, the following is a 3 by 3 magic square since the sum of 3 numbers in each row is equal to 15, the sum of the 3 numbers in each column is equal to 15, and the sum of the 3 numbers in each diagonal is equal to 15.

8	3	4
1	5	9
6	7	2

    Prove that the following 4 by 4 square cannot be completed to form a magic square.

	1		2
3	4	5	
6	7		8
9		10	

    Hint: Assign each of the six blank cells in the square a name. One possibility is to use a, b, c, d, e, and f.

19. Using only the digits 1 through 9 one time each, is it possible to construct a 3 by 3 magic square with the digit 3 in the center square? That is, is it possible to construct a magic square of the form

a	b	c
d	3	e
f	g	h

    where a, b, c, d, e, f, g, h are all distinct digits, none of which is equal to 3? Either construct such a magic square or prove that it is not possible.

20. **Evaluation of proofs**
    See the instructions for Exercise (19) on page 100 from Section 3.1

proposition

For each real number x, if x is irrational and m is an integer, then mx is irrational.

Proof

We assume that x is a real number and is irrational. This means that for all integers a and b with $b \neq 0$, $x \neq \frac{a}{b}$.

Hence, we may conclude that $mx \neq \frac{ma}{b}$ and, therefore, mx is irrational.

proposition

For all real numbers x and y, if x is irrational and y is rational, then $x + y$ is irrational.

Proof

We will use a proof by contradiction. So we assume that the proposition is false, which means that there exist real numbers x and y where $x \notin \mathbb{Q}$, $y \in \mathbb{Q}$, and $x + y \in \mathbb{Q}$. Since the rational numbers are closed under subtraction

and $x+y$ and y are rational, we see that

$$(x+y)-y \in \mathbb{Q} \tag{3.3.10}$$

.

However, $(x+y)-y=x$, and hence we can conclude that $x \in \mathbb{Q}$. This is a contradiction to the assumption that $x \notin \mathbb{Q}$. Therefore, the proposition is not false, and we have proven that for all real numbers x and y, if x is irrational and y is rational, then $x+y$ is irrational.

proposition

For each real number x, $x(1-x) \leq \frac{1}{4}$.

Proof

A proof by contradiction will be used. So we assume the proposition is false. This means that there exists a real number x such that $x(1-x) > \frac{1}{4}$. If multiply both sides of this inequality by 4, we obtain $4x(1-x) > 1$. However, if we let $x=3$, we then see that

$$\begin{gathered} 4x(1-x) > 1 \\ 4 \cdot 3(1-3) > 1 \\ -12 > 1 \end{gathered}$$

The last inequality is clearly a contradiction and so we have proved the proposition.

Explorations and Activities

21. A Proof by Contradiction. Consider the following proposition:

Proposition. Let a, b, and c be integers. If 3 divides a, 3 divides b, and $c \equiv 1 \pmod 3$, then the equation

$$ax+by=c$$

has not solution in which both x and y are integers.

Proof. A proof by contradiction will be used. So we assume that the statement is false. That is, we assume that there exist integers a, b, and c such that 3 divides both a and b, that $c \equiv 1 \pmod 3$, and that the equation

$$ax+by=c$$

has a solution in which both x and y are integers. So there exist integers m and n such that

$$am+bn=c$$

Hint: Now use the facts that 3 divides a, 3 divides b, and $c \equiv 1 \pmod 3$.

22. Exploring a Quadratic Equation. Consider the following proposition:

Proposition. For all integers m and n, if n is odd, then the equation

$$x^2+2mx+2n=0$$

has no integer solution for x.

(a) What are the solutions of the equation when $m=1$ and $n=1$? That is, what are the solutions of the equation $x^2+2x-2=0$?
(b) What are the solutions of the equation when $m=2$ and $n=3$? That is, what are the solutions of the equation $x^2+4x+2=0$?
(c) Solve the resulting quadratic equation for at least two more examples using values of m and n that satisfy the hypothesis of the proposition.
(d) For this proposition, why does it seem reasonable to try a proof by contradiction?

(e) For this proposition, state clearly the assumptions that need to be made at the beginning of a proof by contradiction.
(f) Use a proof by contradiction to prove this proposition.

Answer

Add texts here. Do not delete this text first.

3.4: Using Cases in Proofs

PREVIEW ACTIVITY 3.4.1: Using a Logical Equivalency

1. Complete a truth table to show that $(P \vee Q) \to R$ is logical equivalent to $(P \to R) \wedge (Q \to R)$.
2. Suppose that you are trying to prove a statement that is written in the form $(P \vee Q) \to R$. Explain why you can complete this proof by writing separate and independent proofs of $P \to R$ and $Q \to R$.
3. Now consider the following proposition:

   Proposition. For all integers x and y, if xy is odd, then x is odd and y is odd.
   Write the contrapositive of this proposition.
4. Now prove that if x is an even integer, then xy is an even integer. Also, prove that if y is an even integer, then xy is an even integer.
5. Use the results proved in part (4) and the explanation in part (2) to explain why we have proved the contrapositive of the proposition in part (3).

Preview Activity 3.4.1: Using Cases in a Proof

The work in Preview Activity 3.4.1 was meant to introduce the idea of using cases in a proof. The method of using cases is often used when the hypothesis of the proposition is a disjunction. This is justified by the logical equivalency

$$[(P \vee Q) \to R] \equiv [(P \to R) \wedge (Q \to R)] \tag{3.4.1}$$

See Theorem 2.8 on page 48 and Exercise (6) on page 50.

In some other situations when we are trying to prove a proposition or a theorem about an element x in some set U, we often run into the problem that there does not seem to be enough information about x to proceed. For example, consider the following proposition:

Proposition 1. If n is an integer, then $n^2 + n$ is an even integer.

If we were trying to write a direct proof of this proposition, the only thing we could assume is that n is an integer. This is not much help. In a situation such as this, we will sometimes use cases to provide additional assumptions for the forward process of the proof. Cases are usually based on some common properties that the element x may or may not possess. The cases must be chosen so that they exhaust all possibilities for the object x in the hypothesis of the original proposition. For Proposition 1, we know that an integer must be even or it must be odd. We can thus use the following two cases for the integer n:

- The integer n is an even integer;
- The integer n is an odd integer.

1. Complete the proof for the following proposition:

   Proposition 2: If n is an even integer, then $n^2 + n$ is an even integer.
   Proof. Let n be an even integer. Then there exists an integer m such that $n = 2m$. Substituting this into the expression $n^2 + n$ yields ...
2. Construct a proof for the following proposition:

   Proposition 3: If n is an odd integer, then $n^2 + n$ is an even integer.
3. Explain why the proofs of Proposition 2 and Proposition 3 can be used to construct a proof of Proposition 1.

Some Common Situations to Use Cases

When using cases in a proof, the main rule is that the cases must be chosen so that they exhaust all possibilities for an object x in the hypothesis of the original proposition. Following are some common uses of cases in proofs.

When the hypothesis is, "n is an integer."	Case 1: n is an even integer. Case 2: n is an odd integer.

When the hypothesis is, "m and n are integers."	Case 1: m and n are even. Case 2: m is even and n is odd. Case 3: m is odd and n is even. Case 4: m and n are both odd.
When the hypothesis is, "x is a real number."	Case 1: x is rational. Case 2: x is irrational.
When the hypothesis is, "x is a real number."	Case 1: $x = 0$ OR Case 1: $x > 0$ Case 2: $x \neq 0$ Case 2: $x = 0$ Case 3: $x < 0$
When the hypothesis is, "a and b are real numbers."	Case 1: $a = b$ OR Case 1: $a > b$ Case 2: $a \neq b$ Case 2: $a = b$ Case 3: $a < b$

Writing Guidelines for a Proof Using Cases

When writing a proof that uses cases, we use all the other writing guidelines. In addition, we make sure that it is clear where each case begins. This can be done by using a new paragraph with a label such as “Case 1,” or it can be done by starting a paragraph with a phrase such as, “In the case where . . . .”

? Progress Check 3.21: Using Cases: n Is Even or n Is Odd

Complete the proof of the following proposition:

Proposition. For each integer n, $n^2 - 5n + 7$ is an odd integer.

Proof. Let n be an integer. We will prove that $n^2 - 5n + 7$ is an odd integer by examining the case where n is even and the case where n is odd.

Case 1. The integer n is even. In this case, there exists an integer m such that $n = 2m$. Therefore, ...

Answer

Add texts here. Do not delete this text first.

As another example of using cases, consider a situation where we know that a and b are real numbers and $ab = 0$. If we want to make a conclusion about b, the temptation might be to divide both sides of the equation by a. However, we can only do this if $a \neq 0$. So, we consider two cases: one when $a = 0$ and the other when $a \neq 0$.

proposition 3.22

For all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

Proof

We let a and b be real numbers and assume that $ab = 0$. We will prove that $a = 0$ or $b = 0$ by considering two cases: (1) $a = 0$, and (2) $a \neq 0$.

In the case where $a = 0$, the conclusion of the proposition is true and so there is nothing to prove.

In the case where $a \neq 0$, we can multiply both sides of the equation $ab = 0$ by $dfrac1a$and obtain

$$\frac{1}{a} \cdot ab = \frac{1}{a} \cdot 0$$

$$b = 0$$

So in both cases, $a = 0$ or $b = 0$, and this proves that for all real numbers a and b, if $ab = 0$, then $a = 0$ or $b = 0$.

Absolute Value

Most students by now have studied the concept of the absolute value of a real number. We use the notation $|x|$ to stand for the absolute value of the real number x. One way to think of the absolute value of x is as the "distance" between x and 0 on the number line. For example,

$$|-5| = 5 \text{ and } |-7| = 7$$

Although this notion of absolute value is convenient for determining the absolute value of a specific number, if we want to prove properties about absolute value, we need a more careful and precise definition.

Definition: absolute value

For $x \in \mathbb{R}$, we define $|x|$, called the **absolute value of x**, by

$$|x| = \begin{cases} x & \text{if } x \geq 0; \\ -x & \text{if } x < 0. \end{cases}$$

Let's first see if this definition is consistent with our intuitive notion of absolute value by looking at two specific examples.

- Since 5 > 0, we see that |5| = 5, which should be no surprise.
- Since -7 < 0, we see that |-7| = -(-7) = 7.

Notice that the definition of the absolute value of x is given in two parts, one for when $x \geq 0$ and the other for when $x < 0$. This means that when attempting to prove something about absolute value, we often uses cases. This will be illustrated in Theorem 3.23.

Theorem 3.23

Let a be a positive real number. For each real number x,

1. $|x| = a$ if and only if $x = a$ or $x = -a$.
2. $|-x| = |x|$.

Proof

The proof of Part (2) is part of Exercise (10). We will prove Part (1).

We let a be a positive real number and let $x \in \mathbb{R}$. We will first prove that if $|x| = a$, then $x = a$ or $x = -a$. So we assume that $|x| = a$. In the case where $x \geq 0$, we see that $|x| = x$, and since $|x| = a$, we can conclude that $x = -a$.

In the case where $x < 0$, we see that $|x| = -x$. Since $|x| = a$, we can conclude that $-x = a$ and hence that $x = -a$. These two cases prove that if $|x| = a$, then $x = a$ or $x = -a$.

We will now prove that if $x = a$ or $x = -a$, then $|x| = a$. We start by assuming that $x = a$ or $x = -a$. Since the hypothesis of this conditional statement is a disjunction, we use two cases. When $x = a$, we see that

$$|x| = |a| = a \text{ since } a > 0.$$

When $x = -a$, we conclude that

$$|x| = |-a| = -(-a) \text{ since } -a < 0.$$

and hence, $|x| = a$. This proves that if $x = a$ or $x = -a$, then $|x| = a$. Because we have proven both conditional statements, we have proven that $|x| = a$ if and only if $x = a$ or $x = -a$.

Progress Check 3.24: Equations Involving Absolute Values

1. What is |4,3| and what is |-π|?
2. Use the properties of absolute value in Proposition 3.23 to help solve the following equations for t, where t is a real number.

   (a) $|t| = 12$.
   (b) $|t + 3| = 5$

(c) $|t-4| = \frac{1}{5}$.
(d) $|3t-4| = 8$.

Answer

Add texts here. Do not delete this text first.

Although solving equations involving absolute values may not seem to have anything to do with writing proofs, the point of Progress Check 3.24 is to emphasize the importance of using cases when dealing with absolute value. The following theorem provides some important properties of absolute value.

Theorem 3.25

Let a be a positive real number. For all real numbers x and y,

1. $|x| < a$ if and only if $-a < x < a$.
2. $|xy| = |x||y|$
3. $|x+y| \leq |x| + |y|$. This is know as the ***Triangle Inequality.***

Proof

We will prove Part (1). The proof of Part (2) is included in Exercise (10), and the proof of Part (3) is Exercise (14). For Part (1), we will prove the biconditional proposition by proving the two associated conditional propositions.

So we let a be a positive real number and let $x \in \mathbb{R}$ and first assume that $|x| < a$. We will use two cases: either $x \geq 0$ or $x < 0$.

- In the case where $x \geq 0$, we know that $|x| = x$ and so the inequality $|x| < a$ implies that $x < a$. However, we also know that $-a < 0$ and that $x > 0$. Therefore, we conclude that $-a < x$ and, hence, $-a < x < a$.
- When $x < 0$, we see that $|x| = -x$. Therefore, the inequality $|x| < a$ implies that $-x < a$, which in turn implies that $-a < x$. In this case, we also know that $x < a$ since x is negative and a is positive. Hence, $-a < x < a$

So in both cases, we have proven that $-a < x < a$ and this proves that if $|x| < a$, then $-a < x < a$. We now assume that $-a < x < a$.

- If $x \geq 0$, then $|x| = x$ and hence, $|x| < a$.
- If $x < 0$, then $|x| = -x$ and so $|x| = -x$. Thus, $-a < -|x|$. By multiplying both sides of the last inequality by -1, we conclude that $|x| < a$.

These two cases prove that if $-a < x < a$, then $|x| < a$. Hence, we have proven that $|x| < a$ if and only if $-a < x < a$.

Exercises for section 3.4

1. In Preview Activity 3.4.2, we proved that if n is an integer, then $n^2 + n$ is an even integer. We define two integers to be **consecutive integers** if one of the integers is one more than the other integer. This means that we can represent consecutive integers as m and $m+1$, where m is some integer.
   Explain why the result proven in Preview Activity 3.4.2 can be used to prove that the product of any two consecutive integers is divisible by 2.
2. Prove that if u is an odd integer, then the equation $x^2 + x - u = 0$ has no solution that is an integer.
3. Prove that if n is an odd integer, then $n = 4k+1$ for some integer k or $n = 4k+3$ for some integer k.
4. Prove the following proposition:

   For each integer a, if $a^2 = a$, then $a = 0$ or $a = 1$.
5. (a) Prove the following proposition:
   For all integers a, b, and d with $d \neq 0$, if d divides a or d divides b, then d divides the product ab.
   Hint: Notice that the hypothesis is a disjunction. So use two cases.

(b) Write the contrapositive of the proposition in Exercise(5a).
(c) Write the converse of the proposition in Exercise (5a). Is the converse true or false? Justify your conclusion.

6. Are the following propositions true or false? Justify all your conclusions. If a biconditional statement is found to be false, you should clearly determine if one of the conditional statements within it is true. In that case, you should state an appropriate theorem for this conditional statement and prove it. (a) For all integers m and n, m and n are consecutive integers if and only if 4 divides $(m^2+n^2-1$.
(b) For all integers m and n, 4 divides (m^2-n^2) if and only if m and n are both even or m and n are both odd.
7. Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.

   For each integer n, if n is odd, then $8|(n^2-1)$.
8. Prove that there are no natural numbers a and n with $n \geq 2$ and $a^2+1=2^n$.
9. Are the following propositions true or false? Justify each conclusions with a counterexample or a proof.

   (a) For all integers a and b with $a \neq 0$, the equation $ax+b=0$ has a rational number solution.
   (b) For all integers a, b, and c, if a, b, and c are odd, then the equation $ax^2+bx+c=0$ has no solution that is a rational number.
   Hint: Do not use the quadratic formula. Use a proof by contradiction and recall that any rational number can be written in the form $\frac{p}{q}$, where p and q are integers, $q>0$, and p and q have no common factor greater than 1.
   (c) For all integers a, b, c, and d, if a, b, c, and d are odd, then the equation $ax^3+bx^2+cx+d=0$ has no solution that is a rational number.
10. (a) Prove Part (2) of Proposition 3.23.
    For each $x \in \mathbb{R}$, $|-x|=|x|$.
    (b) Prove Part (2) of Proposition 3.25.
    For all real numbers x and y, $|xy|=|x||y|$.
11. Let a be a positive real number. In Part (1) of Theorem 3.25, we proved that for each real number x, $|x|<a$ if and only if $-a<x<a$. It is important to realize that the sentence $-a<x<a$ is actually the conjunction of two inequalities. That is, $-a<x<a$ means that $-a<x$ and $x<a$.

    (a) Complete the following statement: For each real number x, $|x| \geq a$ if and only if ....
    (b) Prove that for each real number x, $|x| \leq a$ if and only if $-a \leq x \leq a$
    (c) Complete the following statement: For each real number x, $|x|>a$ if and only if ....
12. Prove each of the following:

    (a) For each nonzero real number x, $|x^{-1}|=\dfrac{1}{|x|}$.
    (b) For all real number x and y, $|x-y| \geq |x|-|y|$.
    Hint: An idea that is often used by mathematicians is to add 0 to an expression "intelligently". In this case, we know that $(-y)+y=0$. Start by adding this "version" of 0 inside the absolute value sign of $|x|$.
    (c) For all real number x and y, $||x|-|y|| \leq |x-y|$.
13. **Evaluation of proofs**
    See the instructions for Exercise (19) on page 100 from Section 3.1.

Theorem 3.4.1

The probabilities assigned to events by a distribution function on a sample space are given by.

Proof

Add proof here and it will automatically be hidden if you have a "AutoNum" template active on the page.

Theorem 3.4.1

The probabilities assigned to events by a distribution function on a sample space are given by.

Proof

Add proof here and it will automatically be hidden if you have a "AutoNum" template active on the page.

Explorations and Activities

14. **Proof of the Triangle Inequality.**

(a) Verify that the triangle inequality is true for several different real numbers x and y. Be sure to have some examples where the real numbers are negative.
(b) Explain why the following proposition is true: For each real number r, $-|r| \leq r \leq |r|$.
(c) Now let x and y be real numbers. Apply the result in Part (14b) to both x and y. Then add the corresponding parts of the two inequalities to obtain another inequality. Use this to prove that $|x+y| \leq |x| + |y|$.

Answer

Add texts here. Do not delete this text first.

3.5: The Division Algorithm and Congruence

Preview Activity 1: Quotients and Remainders

1. Let $a = 27$ and $b = 4$. We will now determine several pairs of integers q and r so that $27 = 4q + r$. For example, if $q = 2$ and $r = 19$, we obtain $4 \cdot 2 + 19 = 27$. The following table is set up for various values of q. For each q, determine the value of r so that $4q + r = 27$.

q	1	2	3	4	5	6	7	8	9	10
r		19						-5		
$4q + r$	27	27	27	27	27	27	27	27	27	27

2. What is the smallest positive value for r that you obtained in your examples from Part (1)?

   Division is not considered an operation on the set of integers since the quotient of two integers need not be an integer. However, we have all divided one integer by another and obtained a quotient and a remainder. For example, if we divide 113 by 5, we obtain a quotient of 22 and a remainder of 3. We can write this as $\frac{113}{5} = 22 + \frac{3}{5}$. If we multiply both sides of this equation by 5 and then use the distributive property to "clear the parentheses," we obtain

   $$5 \cdot \frac{113}{5} = 5(22 + \frac{3}{5})$$
   $$113 = 5 \cdot 22 + 3$$

   This is the equation that we use when working in the integers since it involves only multiplication and addition of integers.
3. What are the quotient and the remainder when we divide 27 by 4? How is this related to your answer for Part (2)?
4. Repeat part (1) using $a = -17$ and $b = 5$. So the object is to find integers q and r so that $-17 = 5q + r$. Do this by completing the following table.

q	-7	-6	-5	-4	-3	-2	-1
r	18					-7	
$5q + r$	-17	-17	-17	-17	-17	-17	-17

5. The convention we will follow is that the remainder will be the smallest positive integer r for which $-17 = 5q + r$ and the quotient will be the corresponding value of q. Using this convention, what is the quotient and what is the remainder when -17 is divided by 5?

Preview Activity 2: Some Work with Congruence Modulo n

1. Let n be a natural number and let a and b be integers.

   (a) Write the definition of "a is congruent to b modulo n," which is written $a \equiv b \pmod{n}$.

   (b) Use the definition of "divides" to complete the following:
   When we write $a \equiv b \pmod{n}$, we may conclude that there exists an integer k such that ....

   We will now explore what happens when we multiply several pairs of integers where the first one is congruent to 3 modulo 6 and the second is congruent to 5 modulo 6. We can use set builder notation and the roster method to specify the set A of all integers that are congruent to 2 modulo 6 as follows:

   $$A = \{a \in \mathbb{Z} | a \equiv 3 \ (mod\ 6)\} = \{\ldots -15, -9, -3, 3, 9, 15, 21, \ldots\} \quad (3.5.1)$$

2. Use the roster method to specify the set B of all integers that are congruent to 5 modulo 6.

   $$B = \{b \in \mathbb{Z} | b \equiv 5 \ (mod\ 6)\} = \ldots \quad (3.5.2)$$

Notice that $15 \in A$ and $11 \in B$ and that $15+11=26$. Also notice that $26 \equiv 2 \pmod 6$ and that 2 is the smallest positive integer that is congruent to 26 (mod 6).

3. Now choose at least four other pairs of integers a and b where $a \in A$ and $b \in B$. For each pair, calculate $(a+b)$ and then determine the smallest positive integer r for which $(a+b) \equiv r \pmod 6$. **Note**: The integer r will satisfy the inequalities $0 \leq r < 6$.
4. Prove that for all integers a and b, if $a \equiv 3 \pmod 6$ and $b \equiv 5 \pmod 6$, then $(a+b) \equiv 2 \pmod 6$.

The Division Algorithm

Preview Activity 3.5.1 was an introduction to a mathematical result known as the Division Algorithm. One of the purposes of this preview activity was to illustrate that we have already worked with this result, perhaps without knowing its name. For example, when we divide 337 by 6, we often write

$$\frac{337}{6} = 56 + \frac{1}{6}.$$

When we multiply both sides of this equation by 6, we get

$$337 = 6 \cdot 56 + 1$$

When we are working within the system of integers, the second equation is preferred over the first since the second one uses only integers and the operations of addition and multiplication, and the integers are closed under addition and multiplication. Following is a complete statement of the Division Algorithm.

The Division Algorithm

For all integers a and b with $b > 0$, there exist unique integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < b$$

Some Comments about the Division Algorithm

1. The Division Algorithm can be proven, but we have not yet studied the methods that are usually used to do so. In this text, we will treat the Division Algorithm as an axiom of the integers. The work in Preview Activity 3.5.1 provides some rationale that this is a reasonable axiom.
2. The statement of the Division Algorithm contains the new phrase, “there exist unique integers q and r such that ....” This means that there is only one pair of integers q and r that satisfy both the conditions $a = bq + r$ and $0 \leq r < b$. As we saw in Preview Activity 3.5.1, there are several different ways to write the integer a in the form $a = bq + r$. However, there is only one way to do this and satisfy the additional condition that $0 \leq r < b$.
3. In light of the previous comment, when we speak of **the quotient** and **the remainder** when we “divide an integer a by the positive integer b,” we will always mean the quotient (q) and the remainder (r) guaranteed by the Division Algorithm. So the remainder r is the least nonnegative integer such that there exists an integer (quotient) q with $a = bq + r$.
4. If $a < 0$, then we must be careful when writing the result of the Division Algorithm. For example, in parts (4) and (5) of Preview Activity 3.5.1, with $a = -17$ and $b = 5$, we obtained $-17 = 5 \cdot (-4) + 3$, and so the quotient is -4 and the remainder is 3. Notice that this is different than the result from a calculator, which would be $\frac{-17}{5} = -3.4$. But this means

$$\frac{-17}{5} = -(3 + \frac{4}{10}) = -3 - \frac{2}{5}. \tag{3.5.3}$$

If we multiply both sides of this equation by 5, we obtain

$$-17 = 5(-3) + (-2). \tag{3.5.4}$$

This is not the result guaranteed by the Division Algorithm since the value of 2 does not satisfy the result of being greater than or equal to 0 and less than 5.

5. One way to look at the Division Algorithm is that the integer a is either going to be a multiple of b, or it will lie between two multiples of b. Suppose that a is not a multiple of b and that it lies between the multiples $b \cdot q$ and $b(q+1)$, where q is some

integer. This is shown on the number line in Figure 3.2.

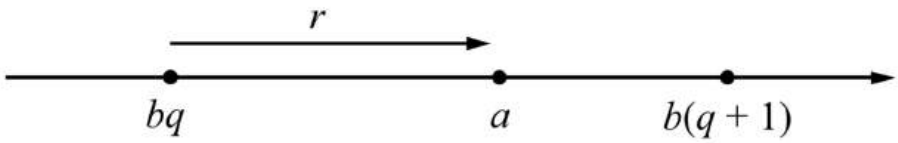


Figure 3.2: Remainder for the Division Algorithm

6. If r represents the distance from $b \cdot q$ to a, then

$$r = a - b \cdot q, or \tag{3.5.5}$$
$$a = b \cdot q + r. \tag{3.5.6}$$

From the diagram, also notice that r is less than the distance between $b \cdot q$ and $b(q+1)$. Algebraically, this distance is

$$b(q+1) - b \cdot q = b \cdot q + b - b \cdot q \tag{3.5.7}$$
$$= b. \tag{3.5.8}$$

Thus, in the case where a is not a multiple of b, we get $0 < r < b$.

7. We have been implicitly using the fact that an integer cannot be both even and odd. There are several ways to understand this fact, but one way is through the Division Algorithm. When we classify an integer as even or odd, we are doing so on the basis of the remainder (according to the Division Algorithm) when the integer is "divided" by 2. If $a \in \mathbb{Z}$, then by the Division Algorithm there exist unique integers q and r such that

$a = 2q + r$ and $0 \leq r < 2$.

This means that the remainder, r, can only be zero or one (and not both). When $r = 0$, the integer is even, and when $r = 1$, the integer is odd.

? Progress Check 3.26: Using the Division Algorithm

1. What are the possible remainders (according to the Division Algorithm) when an integer is
   a. (a) Divided by 4?
   b. (b) Divided by 9?
2. For each of the following, find the quotient and remainder (guaranteed by the Division Algorithm) and then summarize the results by writing an equation of the form $a = bq + r$, where $0 \leq r < b$.
   a. When 17 is divided by 3.
   b. When -17 is divided by 3.
   c. When 73 is divided by 7.
   d. When -73 is divided by 7.
   e. When 436 is divided by 27.
   f. When 539 is divided by 110.

Answer

Add texts here. Do not delete this text first.

Using Cases Determined by the Division Algorithm

The Division Algorithm can sometimes be used to construct cases that can be used to prove a statement that is true for all integers. We have done this when we divided the integers into the even integers and the odd integers since even integers have a remainder of 0 when divided by 2 and odd integers have a remainder o 1 when divided by 2.

Sometimes it is more useful to divide the integer a by an integer other than 2. For example, if a is divided by 3, there are three possible remainders: 0, 1, and 2. If a is divided by 4, there are four possible remainders: 0, 1, 2, and 3. The remainders form the basis for the cases.

If the hypothesis of a proposition is that "n is an integer," then we can use the Division Algorithm to claim that there are unique integers q and r such that

$$n = 3q + r \text{ and } 0 \leq r < 3$$

We can then divide the proof into the following three cases: (1) $r = 0$; (2) $r = 1$; and (3) $r = 2$. This is done in Proposition 3.27.

Proposition 3.27

If n is an integer, then 3 divides $n^3 - n$.

Proof

Let n be an integer. We will show that 3 divides $n^3 - n$ by examining the three cases for the remainder when n is divided by 3. By the Division Algorithm, there exist unique integers q and r such that

$$n = 3q + r \text{ , and } 0 \leq r < 3 \text{ .}$$

This means that we can consider the following three cases:(1) $r = 0$; (2) $r = 1$; and (3) $r = 2$.

In the case where $r = 0$, we have $n = 3q$. By substituting this into the expression $n^3 - n$, we get

$$\begin{aligned} n^3 - n &= (3q)^3 - (3q) && (3.5.9)\\ &= 27q^3 - 3q && (3.5.10)\\ &= 3(9q^3 - q). && (3.5.11) \end{aligned}$$

Since $(9q^3 - q)$ is an integer, the last equation proves that $3|(n^3 - n)$.

In the second case, $r = 1$ and $n = 3q + 1$. When we substitute this into $(n^3 - n)$, we obtain

$$\begin{aligned} n^3 - n &= (3q+1)^3 - (3q+1) && (3.5.12)\\ &= (27q^3 27q^2 + 27q + 1) - (3q + 1) && (3.5.13)\\ &= 27q^3 + 27q^2 + 6q && (3.5.14)\\ &= 3(9q^3 + 9q^2 + 2q). && (3.5.15) \end{aligned}$$

Since $(9q^3 + 9q^2 + 2q)$ is an integer, the last equation proves that $3|(n^3 - n)$.

The last case is when $r = 2$. The details for this case are part of Exercise (1). Once this case is completed, we will have proved that 3 divides $n^3 - n$ in all three cases. Hence, we may conclude that if n is an integer, then 3 divides $n^3 - n$.

Properties of Congruence

Most of the work we have done so far has involved using definitions to help prove results. We will continue to prove some results but we will now prove some theorems about congruence (Theorem 3.28 and Theorem 3.30) that we will then use to help prove other results.

Let $n \in \mathbb{N}$. Recall that if a and b are integers, then we say that a is congruent to b modulo n provided that n divides $a - b$, and we write $a \equiv b \pmod{n}$. (See Section 3.1.) We are now going to prove some properties of congruence that are direct consequences of the definition. One of these properties was suggested by the work in Preview Activity 3.5.2 and is Part (1) of the next theorem.

Theorem 3.28: Properties of Congruence Modulo n

Let n be a natural number and let a, b, c, and d be integers. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

1. $a + c) \equiv (b + d) \pmod{n}$.
2. $ac \equiv bd \pmod{n}$.
3. For each $m \in \mathbb{N}$, $a^m \equiv b^m \pmod{n}$.

Proof

We will prove Parts (2) and (3). The proof of Part (1) is Progress Check 3.29. Let n be a natural number and let a, b, c, and d be integers. Assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. This means that n divides $a-b$ and that n divides $c-d$. Hence, there exist integers k and q such that $a-b=nk$ and $c-d=nq$. We can then write $a=b+nk$ and $c=d+nq$ and obtain

$$\begin{aligned} ac &= (b+nk)(d+nq) && (3.5.16)\\ &= bd+bnq+dnk+n^2kq && (3.5.17)\\ &= bd+n(bq+dk+nkq). && (3.5.18) \end{aligned}$$

by subtracting bd from both sides of the last equation, we see that

$$ac-bd=n(bq+dk+nkq). \quad (3.5.19)$$

Since $bq+dk+nkq$ is an integer, this proves that $n|(ac-bd)$, and hence we can conclude that $ac \equiv bd \pmod{n}$. This completes the proof of Part (2).

Part (2) basically means that if we have two congruences, we can multiply the corresponding sides of these congruences to obtain another congruence. We have assumed that $a \equiv ??b \pmod{n}$ and so we write this twice as follows:

$$\begin{aligned} a &\equiv b(mod\, n),\ and && (3.5.20)\\ a &\equiv b(mod\, n). && (3.5.21) \end{aligned}$$

If we now use the result in Part (2) and multiply the corresponding sides of these two congruences, we obtain $a^2 \equiv b^2 \pmod{n}$. We can then use this congruence and the congruence $a \equiv b \pmod{n}$ and the result in Part (2) to conclude that

$$a^2 \cdot b \equiv b^2 \cdot b(mod\, n), \quad (3.5.22)$$

or that $a^3 \equiv b^3 \pmod{n}$. We can say that we can continue with this process to prove Part (3), but this is not considered to be a formal proof of this result. To construct a formal proof for this, we could use a proof by mathematical induction. This will be studied in Chapter 4. See Exercise (13) in Section 4.1.

? Progress Check 3.29: Proving Part (1) of Theorem 3.28

Prove part (1) of Theorem 3.28.

Answer

Add texts here. Do not delete this text first.

Exercise (11) in Section 3.1 gave three important properties of congruence modulo n. Because of their importance, these properties are stated and proved in Theorem 3.30. Please remember that textbook proofs are usually written in final form of "reporting the news." Before reading these proofs, it might be instructive to first try to construct a know-show table for each proof.

Theorem 3.30: Properties of Congruence Modulo n

Let $n \in \mathbb{N}$, and let a, b, and c be integers.

1. For every integer a, $a \equiv a \pmod{n}$.
   This is called the ***reflexive property*** of congruence modulo n.
2. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
   This is called ***symmetric property*** of congruence modulo n.
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
   This is called ***transitive property*** of congruence modulo n.

Proof

We will prove the reflexive property and the transitive property. The proof of the symmetric property is Exercise (3).

Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. We will show that $a \equiv a \pmod{n}$. Notice that

$$a-a=0=n\cdot 0. \tag{3.5.23}$$

This proves that n divides $a-a$ and hence, by the definition of congruence modulo n, we have proven that $a\equiv a \pmod{n}$.

To prove the transitive property, we let $n\in\mathbb{N}$, and let a, b, and c be integers. We assume that $a\equiv b \pmod{n}$ and $b\equiv c \pmod{n}$. We will use the definition of congruence modulo n to prove that $a\equiv c \pmod{n}$. Since $a\equiv b \pmod{n}$ and $b\equiv c \pmod{n}$, we know that $n|(a-b)$ and $n|(b-c)$. Hence, there exist integers k and q such that

$$a-b=nk \tag{3.5.24}$$
$$b-c=nq. \tag{3.5.25}$$

by adding the corresponding sides of these two equations, we obtain

$$(a-b)+(b-c)=nk+nq. \tag{3.5.26}$$

If we simplify the left side of the last equation and factor the right side, we get

$$a-c=n(k+q). \tag{3.5.27}$$

By the closure property of the integers, $(k+q)\in\mathbb{Z}$, and so this equation proves that $n|(a-c)$ and hence that $a\equiv c \pmod{n}$. This completes the proof of the transitive property of congruence modulo n.

Using Cases Based on Congruence Modulo n

Notice that the set of all integers that are congruent to 2 modulo 7 is

$$\{n\in\mathbb{Z}|n\equiv 2\ (mod\ 7)\}=\{\dots,-19,-12,-5,2,9,16,23,\dots\} \tag{3.5.28}$$

If we divide any integer in this set by 7 and write the result according to the Division Algorithm, we will get a remainder of 2. For example,

$$2=7\cdot 0+2 \tag{3.5.29}$$
$$9=7\cdot 1+2 \tag{3.5.30}$$
$$16=7\cdot 2+2 \tag{3.5.31}$$
$$23=7\cdot 3+2 \tag{3.5.32}$$
$$-5=7(-1)+2 \tag{3.5.33}$$
$$-12=7(-2)+2 \tag{3.5.34}$$
$$-19=7(-3)+2 \tag{3.5.35}$$

Is this a coincidence or is this always true? Let's look at the general case. For this, let n be a natural number and let $a\in\mathbb{Z}$. By the Division Algorithm, there exist unique integers q and r such that

$$a=nq+r \text{ and } 0\le r<n.$$

By subtracting r from both sides of the equation $a=nq+r$, we obtain

$$a-r=nq.$$

But this implies that $n|(a-r)$ and hence that $a\equiv r \pmod{n}$. We have proven the following result.

Theorem 3.31

Let $n\in\mathbb{N}$ and let $a\in mathbbZ$. If $a=nq+r$ and $0\le r<n$ for some integers q and r, then $a\equiv r \pmod{n}$.

This theorem says that an integer is congruent (mod n) to its remainder when it is divided by n. Since this remainder is unique and since the only possible remainders for division by n are 0, 1, 2,..., $n1$, we can state the following result.

Corollary 3.32

If $n \in \mathbb{N}$, then each integer is congruent, modulo n, to precisely one of the integers 0, 1, 2, ..., $n-1$. That is, for each integer a, there exists a unique integer r such that

$$a \equiv r \pmod{n} \text{ and } 0 \leq r < n.$$

Corollary 3.32 can be used to set up cases for an integer in a proof. If $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, then we can consider n cases for a. The integer a could be congruent to 0,1, 2, ..., or $n-1$ modulo n. For example, if we assume that 5 does not divide an integer a, then we know a is not congruent to 0 modulo 5, and hence, that a must be congruent to 1, 2, 3, or 4 modulo 5. We can use these as 4 cases within a proof. For example, suppose we wish to determine the values of a^2 modulo 5 for integers that are not congruent to 0 modulo 5. We begin by squaring some integers that are not congruent to 0 modulo 5. We see that

$$1^2 = 1 \quad and \quad 1 \equiv 1\ (mod\ 5). \tag{3.5.36}$$
$$3^2 = 9 \quad and \quad 9 \equiv 4\ (mod\ 5). \tag{3.5.37}$$
$$6^2 = 36 \quad and \quad 36 \equiv 1\ (mod\ 5). \tag{3.5.38}$$
$$8^2 = 64 \quad and \quad 64 \equiv 4\ (mod\ 5). \tag{3.5.39}$$
$$9^2 = 81 \quad and \quad 81 \equiv 1\ (mod\ 5). \tag{3.5.40}$$

These explorations indicate that the following proposition is true and we will now outline a method to prove it.

Proposition 3.33.

For each integer a, if $a \not\equiv 0 \pmod 5$, then $a^2 \equiv 1 \pmod 5$ or \(a^2 \equiv 4) (mod 5).

Proof

We will prove this proposition using cases for a based on congruence modulo 5. In doing so, we will use the results in Theorem 3.28 and Theorem 3.30. Because the hypothesis is $a \not\equiv 0 \pmod 5$, we can use four cases, which are: (1)$a \equiv 1 \pmod 5$, (2)$a \equiv 2 \pmod 5$, (3)$a \equiv 3 \pmod 5$, and (4)\(a \equiv 4) (mod 5). Following are proofs for the first and fourth cases.

Case 1. ($a \equiv 1 \pmod 5$). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 1^2 \pmod 5 \text{ or } a^2 \equiv 1 \pmod 5.$$

This proves that if $a \equiv 1 \pmod 5$, then $a^{\equiv}1 \pmod 5$.

Case 4. ($a \equiv 4 \pmod 5$). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 4^2 \pmod 5 \text{ or } a^2 \equiv 16 \pmod 5.$$

We also know that $16 \equiv 1 \pmod 5$. So we have $a^2 \equiv 16 \pmod 5$ and $16 \equiv 1 \pmod 5$, and we can now use the transitive property of congruence (Theorem 3.30) to conclude that $a^2 \equiv 1 \pmod 5$. This proves that if $a \equiv 4 \pmod 5$, then $a^2 \equiv 1 \pmod 5$.

Progress Check 3.34 (Using Properties of Congruence)

Complete a proof of Proposition 3.33 by completing proofs for the other two cases.

Note: It is possible to prove Proposition 3.33 using only the definition of congruence instead of using the properties that we have proved about congruence. However, such a proof would involve a good deal of algebra. One of the advantages of using the properties is that it avoids the use of complicated algebra in which it is easy to make mistakes.

Answer

Add texts here. Do not delete this text first.

In the proof of Proposition 3.33, we used four cases. Sometimes it may seem a bit overwhelming when confronted with a proof that requires several cases. For example, if we want to prove something about some integers modulo 6, we may have to use six cases.

However, there are sometimes additional assumptions (or conclusions) that can help reduce the number of cases that must be considered. This will be illustrated in the next progress check.

Progress Check 3.35: Using Cases Modulo 6

Suppose we want to determine the possible values for a^2 modulo 6 for odd integers that are not multiples of 3. Before beginning to use congruence arithmetic (as in the proof of Proposition 3.33) in each of the possible six cases, we can show that some of the cases are not possible under these assumptions. (In some sense, we use a short proof by contradiction for these cases.) So assume that a is an odd integer. Then:

- If $a \equiv 0 \pmod 6$, then there exists an integer k such that $a = 6k$. But then $a = 2(3k)$ and hence, a is even. Since we assumed that a is odd, this case is not possible.
- If $a \equiv 2 \pmod 6$, then there exists an integer k such that $a = 6k + 2$. But then $a = 2(3k + 1)$ and hence, a is even. Since we assumed that a is odd, this case is not possible.

1. Prove that if a is an odd integer, then a cannot be congruent to 4 modulo 6.
2. Prove that if a is an integer and 3 does not divide a, then a cannot be congruent to 3 modulo 6.
3. So if a is an odd integer that is not a multiple of 3, then a must be congruent to 1 or 5 modulo 6. Use these two cases to prove the following proposition:

Answer

Add texts here. Do not delete this text first.

Proposition 3.36.

For each integer a, if a is an odd integer that is not multiple of 3, then $a^2 \equiv 1 \pmod 6$.

Exercises for Section 3.5

1. Complete the details for the proof of Case 3 of Proposition 3.27.
2. Extending the idea in Exercise (1) of Section 3.4, we can represent three consecutive integers as m, $m + 1$, and $m + 2$, where m is an integer.

   (a) Explain why we can also represent three consecutive integers as $k - 1$, k, and $k + 1$, where k is an integer.
   (b) Explain why Proposition 3.27 proves that the product of any three consecutive integers is divisible by 3.
   (c) Prove that the product of three consecutive integers is divisible by 6.
3. Prove the symmetric property of congruence stated in Theorem 3.30.
4. (a) Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$. Explain why n divides a if and only if $a \equiv 0 \pmod n$.
   (b) Let $a \in \mathbb{Z}$. Explain why if $a \not\equiv 0 \pmod 3$, then $a \equiv 1 \pmod 3$ or $a \equiv 2 \pmod 3$.
   (c) Is the following proposition true or false? Justify your conclusion.
   For each $a \in \mathbb{Z}$, $a \not\equiv 0 \pmod 3$ if and only if $a^2 \equiv 1 \pmod 3$.
5. (a) Use cases based on congruence modulo 3 and properties of congruence to prove that for each integer n, $n^3 \equiv n \pmod 3$.
   (b) Explain why the result in Part (a) proves that for each integer n, 3 divides $n^3 - n$. Compare this to the proof of the same result in Proposition 3.27.
6. Prove that for each natural number n, $\sqrt{3n + 2}$ is not a natural number.
7. Prove the following proposition by proving its contrapositive. (**Hint**: Use case analysis. There are several cases.

   For all integers a and b, if $ab \equiv 0 \pmod 3$, then $a \equiv 0 \pmod 3$ or $b \equiv 0 \pmod 3$.
8. (a) Explain why the following proposition is equivalent to the proposition in Exercise (7).
   For all integers a and b, if $3|ab$, then $3|a$ or $3|b$.
   (b) Prove that for each integer a, if 3 divides a^2, then 3 divides a.

9. (a) Prove that the real number $\sqrt{3}$ is an irrational number. That is, prove that
If r is a positive real number such that $r^2 = 3$, then r is irrational.
(b) Prove that the real number $\sqrt{12}$ is an irrational number.
10. (a) Use the result in Proposition 3.33 to help prove that the integer m = 5, 344, 580, 232, 468, 953, 153 is not a perfect square. Recall that an integer n is a perfect square provided that there exists an integer k such that $n = k^2$. **Hint**: Use a proof by contradiction.
(b) Is the integer n = 782, 456, 231, 189, 002, 288, 438 a perfect square? Justify your conclusion.
11. (a) Use the result in Proposition 3.33 to help prove that for each integer a, if 5 divides a^2, then 5 divides a.
(b) Prove that the real number $\sqrt{5}$ is an irrational number.
12. (a) Prove that for each integer a, if $a \not\equiv 0 \pmod 7$, then $a^2 \not\equiv 0 \pmod 7$.
(b) Prove that for each integer a, if 7 divides a^2, then 7 divides a.
(c) Prove that the real number $\sqrt{7}$ is an irrational number.
13. (a) If an integer has a remainder of 6 when it is divided by 7, is it possible to determine the remainder of the square of that integer when it is divided by 7? If so, determine the remainder and prove that your answer is correct.
(b) If an integer has a remainder of 11 when it is divided by 12, is it possible to determine the remainder of the square of that integer when it is divided by 12? If so, determine the remainder and prove that your answer is correct.
(c) Let n be a natural number greater than 2. If an integer has a remainder of $n-1$ when it is divided by n, is it possible to determine the remainder of the square of that integer when it is divided by n? If so, determine the remainder and prove that your answer is correct.
14. Let n be a natural number greater than 4 and let a be an integer that has a remainder of $n-2$ when it is divided by n. Make whatever conclusions you can about the remainder of a^2 when it is divided by n. Justify all conclusions.
15. Is the following proposition true or false? Justify your conclusion with a proof or a counterexample.
For each natural number n, if 3 does not divide (n^2+2), then n is not a prime number or $n = 3$.
16. (a) Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.
For each integer n, if n is odd then $n^2 \equiv 1 \pmod 8$.
(b) Compare this proposition to the proposition in Exercise (7) from Section 3.4. Are these two propositions equivalent? Explain.
(c) Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.
For each integer n, if n is odd and n is not a multiple of 3, then $n^2 \equiv 1 \pmod{24}$.
17. Prove the following proposition:
For all integers a and b, if 3 divides (a^2+b^2), then 3 divides a and 3 divides b.
18. Is the following proposition true or false? Justify your conclusion with a counterexample or a proof.
For each integer a, 3 divides a^3+23a.
19. Are the following statements true or false? Either prove the statement is true or provide a counterexample to show it is false.

(a) For all integer a and b, if $a \cdot b \equiv 0 \pmod 6$, then $a \equiv 0 \pmod 6$ or $b \equiv 0 \pmod 6$.
(b) For all integer a and b, if $a \cdot b \equiv 0 \pmod 8$, then $a \equiv 0 \pmod 8$ or $b \equiv 0 \pmod 8$.
(c) For all integer a and b, if $a \cdot b \equiv 1 \pmod 6$, then $a \equiv 1 \pmod 6$ or $b \equiv 1 \pmod 6$.
(d) For all integer a and b, if $ab \equiv 7 \pmod 6$, then either $a \equiv 1 \pmod{12}$ or $b \equiv 7 \pmod{12}$.
20. (a) Determine several pairs of integers a and b such that $a \equiv b \pmod 5$. For each such pair, calculate $4a+b$, $3a+2b$, and $7a+3b$. Are each of the resulting integers congruent to 0 modulo 5?
(b) Prove or disprove the following proposition:
Let m and n be integers such that $(m+n) \equiv 0 \pmod 5$ and let $a, b \in \mathbb{Z}$. If $a \equiv b \pmod 5$, then $(ma+nb) \equiv 0 \pmod 5$.
21. **Evaluation of proofs**
See the instructions for Exercise (19) on page 100 from Section 3.1.
(a)

Proposition

For all integers a and b, if $(a+2b) \equiv 0 \pmod 3$, then $(2a+b) \equiv 0 \pmod 3$.

Proof

We assume $a, b \in \mathbb{Z}$ and $(a+2b) \equiv 0 \pmod 3$. This means that 3 divides $a+2b$ and, hence, there exists an integer m such that $a+2b = 3m$. Hence, $a = 3m-2b$. For $(2a+b) \equiv 0 \pmod 3$, there exists an integer x such that $2a+b = 3x$. Hence,

$$2(3m-2b)+b = 3x \tag{3.5.41}$$
$$6m-3b = 3x \tag{3.5.42}$$
$$3(2m-b) = 3x \tag{3.5.43}$$
$$2m-b = x \tag{3.5.44}$$

Since $(2m-b)$ is an integer, this proves that 3 divides $(2a+b)$ and hence, $(2a+b) \equiv 0 \pmod 3$

(b)

Proposition.

For each integer m, 5 divides (m^5-m).

Proof

Let $m \in \mathbb{Z}$. We will prove that 5 divides (m^5-m) by proving that divides $(m^5-m) \equiv 0 \pmod 5$. We will use cases.

For the first case, if $m \equiv 0 \pmod 5$, then $m^5 \equiv 0 \pmod 5$ and, hence, ((m^5 - m) \equiv 0\) (mod 5).

For the second case, if $m \equiv 1 \pmod 5$, then $m^5 \equiv 1 \pmod 5$ and, hence, ((m^5 - m) \equiv (1 - 1)\) (mod 5), which means that ((m^5 - m) \equiv 0\) (mod 5).

For the third case, if $m \equiv 2 \pmod 5$, then $m^5 \equiv 32 \pmod 5$ and, hence, ((m^5 - m) \equiv (32 - 2)\) (mod 5), which means that ((m^5 - m) \equiv 0\) (mod 5).

Explorations and Activities

22. **Using a Contradiction to Prove a Case Is Not Possible.** Explore the statements in Parts (a) and (b) by considering several examples where the hypothesis is true.

(a) If an integer a is divisible by both 4 and 6, then it divisible by 24.
(b) If an integer a is divisible by both 2 and 3, then it divisible by 6.
(c) What can you conclude from the examples in Part (a)?
(d) What can you conclude from the examples in Part (b)?

The proof of the following proposition based on Part (b) uses cases. In this proof, however, we use cases and a proof by contradiction to prove that a certain integer cannot be odd. Hence, it must be even. Complete the proof of the proposition.

Proposition. Let $a \in \mathbb{Z}$. If 2 divides a and 3 divides a, then 6 divides a.

Proof : Let $a \in \mathbb{Z}$ and assume that 2 divides a and 3 divides a. We will prove that 6 divides a. Since 3 divides a, there exists an integer n such that

$$a = 3n. \tag{3.5.45}$$

The integer n is either even or it is odd. We will show that it must be even by obtaining a contradiction if it assumed to be odd. So, assume that n is odd. (Now complete the proof.)

23. **The Last Two Digits of a Large Integer.**
Notice that 7, 381, 272 $\equiv$ 72 (mod 100) since 7, 381, 272 - 72 = 7, 381, 200, which is divisible by 100. In general, if we start with an integer whose decimal representation has more than two digits and subtract the integer formed by the last two digits, the result will be an integer whose last two digits are 00. This result will be divisible by 100. Hence, any integer with

more than 2 digits is congruent modulo 100 to the integer formed by its last two digits.

(a) Start by squaring both sides of the congruence $3^4 \equiv 81 \pmod{100}$ to prove that $3^8 \equiv 61 \pmod{100}$ and then prove that $3^{16} \equiv 21 \pmod{100}$. What does this tell you about the last two digits in the decimal representation of 3^{16}?
(b) Use the two congruences in Part (23a) and laws of exponents to determine r where $3^{20} \equiv r \pmod{100}$ and $r \in \mathbb{Z}$ with $0 \leq r < 100$. What does this tell you about the last two digits in the decimal representation of 3^{20}?
(c) Determine the last two digits in the decimal representation of 3^{400}.
(d) Determine the last two digits in the decimal representation of 4^{804}.
Hint: One way is to determine the "mod 100 values", for 4^2, 4^4, 4^8, 4^{16}, 4^{32}, 4^{64}, and so on. Then use these values and laws of exponents to determine r, where $4^{804} \equiv r \pmod{100}$ and $r \in \mathbb{Z}$ with $0 \leq r < 100$.
(e) Determine the last two digits in the decimal representation of 3^{3356}.
(f) Determine the last two digits in the decimal representation of 7^{403}.

Answer

Add texts here. Do not delete this text first.

3.6: Review of Proof Methods

This section is different from others in the text. It is meant primarily as a review of the proof methods studied in Chapter 3. So the first part of the section will be a description of some of the main proof techniques introduced in Chapter 3. The most important part of this section is the set of exercises since these exercises will provide an opportunity to use the proof techniques that we have studied so far.

We will now give descriptions of three of the most common methods used to prove a conditional statement.

Direct Proof of a Conditional Statement $(P \to Q)$

- **When is it indicated?** This type of proof is often used when the hypothesis and the conclusion are both stated in a "positive" manner. That is, no negations are evident in the hypothesis and conclusion. That is, no negations are evident in the hypothesis and conclusion.
- **Description of the process.** Assume that P is true and use this to conclude that Q is true. That is, we use the forward-backward method and work forward from P and backward from Q.
- **Why the process makes sense.** We know that the conditional statement $P \to Q$ is automatically true when the hypothesis is false. Therefore, because our goal is to prove that $P \to Q$ is true, there is nothing to do in the case that P is false. Consequently, we may assume that P is true. Then, in order for $P \to Q$ to be true, the conclusion Q must also be true. (When P is true, but Q is false, $P \to Q$ is false.) Thus, we must use our assumption that P is true to show that Q is also true.

Proof of a Conditional Statement $(P \to Q)$ Using the Contrapositive

- **When is it indicated?** This type of proof is often used when both the hypothesis and the conclusion are stated in the form of negations. This often works well if the conclusion contains the operator "or"; that is, if the conclusion is in the form of a disjunction. In this case, the negation will be a conjunction.
- **Description of the process.** We prove the logically equivalent statement $\neg Q \to \neg P$. The forward-backward method is used to prove $\neg Q \to \neg P$. That is, we work forward from $\neg Q$ and backward from $\neg P$.
- **Why the process makes sense.** When we prove $\neg Q \to \neg P$, we are also proving $P \to Q$ because these two statements are logically equivalent. When we prove the contrapositive of $P \to Q$, we are doing a direct proof of $\neg Q \to \neg P$. So we assume $\neg Q$ because, when doing a direct proof, we assume the hypothesis, and $\neg Q$ is the hypothesis of the contrapositive. We must show $\neg P$ because it is the conclusion of the contrapositive.

Proof of $P \to Q$ Using a Proof by Contradiction

- When is it indicated? This type of proof is often used when the conclusion is stated in the form of a negation, but the hypothesis is not. This often works well if the conclusion contains the operator "or"; that is, if the conclusion is in the form of a disjunction. In this case, the negation will be a conjunction.
- Description of the process. Assume P and $\neg Q$ and work forward from these two assumptions until a contradiction is obtained.
- Why the process makes sense. The statement $P \to Q$ is either true or false. In a proof by contradiction, we show that it is true by eliminating the only other possibility (that it is false). We show that $P \to Q$ cannot be false by assuming it is false and reaching a contradiction. Since we assume that $P \to Q$ is false, and the only way for a conditional statement to be false is for its hypothesis to be true and its conclusion to be false, we assume that P is true and that Q is false (or, equivalently, that $\neg Q$ is true). When we reach a contradiction, we know that our original assumption that $P \to Q$ is false is incorrect. Hence, $P \to Q$ cannot be false, and so it must be true.

Other Methods of Proof

The methods of proof that were just described are three of the most common types of proof. However, we have seen other methods of proof and these are described below.

Proofs that Use a Logical Equivalency

As was indicated in Section 3.2, we can sometimes use of a logical equivalency to help prove a statement. For example, in order to prove a statement of the form

$$P \to (Q \vee R), \tag{3.6.1}$$

it is sometimes possible to use the logical equivalency

$$[P \to (Q \vee R)] \equiv [(P \wedge \neg Q) \to R]. \tag{3.6.2}$$

We would then prove the statement

$$[(P \wedge \neg Q) \rightarrow R]. \tag{3.6.3}$$

Most often, this would use a direct proof for statement (3.6.1) but other methods could also be used. Because of the logical equivalency, by proving statement (3.6.3), we have also proven the statement (3.6.1).

Proofs that Use Cases

When we are trying to prove a proposition or a theorem, we often run into the problem that there does not seem to be enough information to proceed. In this situation, we will sometimes use cases to provide additional assumptions for the forward process of the proof. When this is done, the original proposition is divided into a number of separate cases that are proven independently of each other. The cases must be chosen so that they exhaust all possibilities for the hypothesis of the original proposition. This method of case analysis is justified by the logical equivalency

$$(P \vee Q) \rightarrow R \equiv (P \rightarrow R) \wedge (Q \rightarrow R). \tag{3.6.4}$$

which was established in Preview Activity 3.6.1 in Section 3.4.

Constructive Proof

This is a technique that is often used to prove a so-called existence theorem. The objective of an existence theorem is to prove that a certain mathematical object exists. That is, the goal is usually to prove a statement of the form

There exists an x such that $P(x)$.

For a constructive proof of such a proposition, we actually name, describe, or explain how to construct some object in the universe that makes $P(x)$ true.

Nonconstructive Proof

This is another type of proof that is often used to prove an existence theorem is the so-called **nonconstructive proof**. For this type of proof, we make an argument that an object in the universal set that makes $P(x)$ true must exist but we never construct or name the object that makes $P(x)$ true.

? Exercises for Section 3.6

1. Let h and k be real numbers and let r be a positive number. The equation for a circle whose center is at the point (h, k) and whose radius is r is

$$(x-h)^2 + (y-k)^2 = r^2. \tag{3.6.5}$$

We also know that if a and b are real numbers, then

- The point (a, b) is inside the circle if $(a-h)^2 + (b-k)^2 < r^2$.
- The point (a, b) is on the circle if $(a-h)^2 + (b-k)^2 = r^2$.
- The point (a, b) is outside the circle if $(a-h)^2 + (b-k)^2 > r^2$.

Prove that all points on or inside the circle whose equation is $(x-1)^2 + (y-2)^2 = 4$ are inside the circle whose equation is $x^2 + y^2 = 26$.

2. Let r be a positive real number. The equation for a circle of radius r whose center is the origin is $x^2 + y^2 = r^2$.

(a) Use implicit differentiation to determine $\dfrac{dy}{dx}$.
(b) Let (a, b) be a point on the circle with $a \neq 0$ and $b \neq 0$. Determine the slope of the line tangent to the circle at the point (a, b).
(c) Prove that the radius of the circle to the point (a, b) is perpendicular to the line tangent to the circle at the point (a, b).
Hint: Two lines (neither of which is horizontal) are perpendicular if and only if the products of their slopes is equal to 1.

3. Are the following statements true or false? Justify your conclusions.

   (a) For each integer a, if 3 does not divide a, then 3 divides $2a^2+1$.
   (b) For each integer a, if 3 divides $2a^2+1$, then 3 does not divide a.
   (c) For each integer a, 3 does not divide a if and only if 3 divides $2a^2+1$.
4. Prove that for each real number x and each irrational number q, $x+q$ is irrational or $x-q$ is irrational.
5. Prove that there exist irrational numbers u and v such that uv is a rational number.

   Hint: We have proved that $\sqrt{2}$ is irrational. For the real number $q=\sqrt{2}^{\sqrt{2}}$, either q is rational or q is irrational. Use this disjunction to set up two cases.
6. Let a and b be natural numbers such that $a^2=b^3$. Prove each of the propositions in Parts (6a) through (6d). (The results of Exercise (1) and Theorem 3.10 from Section 3.2 may be helpful.)

   (a) If a is even, then 4 divides a.
   (b) If 4 divides a, then 4 divides b.
   (c) If 4 divides b, then 8 divides a.
   (d) If a is even, then 8 divides a.
   (e) Give an example of natural numbers a and b such that a is even and $a^2=b^3$, but b is not divisible by 8.
7. Prove the following proposition:
   Let a and b be integers with $a \leq 0$. If a does not divide b, then the equation $ax^3+bx+(b+a)=0$ does not have a solution that is a natural number.
   Hint: It may be necessary to factor a sum of cubes. Recall that

$$u^3+v^3=(u+v)(u^2-uv+v^2). \tag{3.6.6}$$

8. Recall that a **Pythagorean triple** consists of three natural numbers a, b, and c such that $a<b<c$ and $a^2+b^2=c^2$. Are the following propositions true or false? Justify your conclusions.

   (a) For all $a, b, c \in \mathbb{N}$ such that $a<b<c$, if a, b, and c form a Pythagorean triple, then 3 divides a or 3 divides b.
   (b) For all $a, b, c \in \mathbb{N}$ such that $a<b<c$, if a, b, and c form a Pythagorean triple, then 5 divides a or 5 divides b or 5 divides c.
9. (a) Prove that there exists a Pythagorean triple a, b, and c, where $a=5$ and b and c are consecutive natural numbers.
   (b) Prove that there exists a Pythagorean triple a, b, and c, where $a=7$ and b and c are consecutive natural numbers.
   (c) Let m be an odd natural number that is greater than 1. Prove that there exists a Pythagorean triple a, b, and c, where $a=m$ and b and c are consecutive natural numbers.
10. One of the most famous unsolved problems in mathematics is a conjecture made by Christian Goldbach in a letter to Leonhard Euler in 1742. The conjecture made in this letter is now known as **Goldbach's Conjecture**. The conjecture is as follows:
    Every even integer greater than 2 can be expressed as the sum of two (not necessarily distinct) prime numbers.
    Currently, it is not known if this conjecture is true or false.

    (a) Write 50, 142, and 150 as a sum of two prime numbers
    (b)Prove the following:
    If Goldbach's Conjecture is true, then every integer greater than 5 can be written as a sum of three prime numbers.
    (c)Prove the following:
    If Goldbach's Conjecture is true, then every odd integer greater than 7 can be written as a sum of three odd prime numbers.
11. Two prime numbers that differ by 2 are called **twin primes**. For example, 3 and 5 are twin primes, 5 and 7 are twin primes, and 11 and 13 are twin primes. Determine at least two other pairs of twin primes. Is the following proposition true or false? Justify your conclusion.

    For all natural numbers p and q if p and q are twin primes other than 3 and 5, then $pq+1$ is a perfect square and 36 divides $pq+1$.

12. Are the following statements true or false? Justify your conclusions.

    (a) For all integers a and b, $(a+b)^2 \equiv (a^2+b^2)(mod\ 2)$.
    (b) For all integers a and b, $(a+b)^3 \equiv (a^3+b^3)(mod\ 3)$.
    (c) For all integers a and b, $(a+b)^4 \equiv (a^4+b^4)(mod\ 4)$.
    (d) For all integers a and b, $(a+b)^5 \equiv (a^5+b^5)(mod\ 5)$.

    If any of the statements above are false, write a new statement of the following form that is true (and prove that it is true):

    For all integers a and b, $(a+b)^n \equiv (a^n + something + b^n)(mod n)$.

13. Let a, b, c, and d be real numbers with $a \neq 0$ and let $f(x) = ax^3 + bx^2 + cx + d$.

    (a) Determine the derivative and second derivative of the cubic function f.

    (b) Prove that the cubic function f has at most two critical points and has exactly one inflection point.

Explorations and Activities

14. **A Special Case of Fermat's Last Theorem**. We have already seen examples of **Pythagorean triples**, which are natural numbers a, b, and c where $a^2 + b^2 = c^2$. For example, 3, 4, and 5 form a Pythagorean triple as do 5, 12, and 13. One of the famous mathematicians of the 17th century was Pierre de Fermat (1601 – 1665). Fermat made an assertion that for each natural number n with $n \geq 3$, there are no integers a, b, and c for which $a^n + b^n = c^n$. This assertion was discovered in a margin of one of Fermat's books after his death, but Fermat provided no proof. He did, however, state that he had discovered truly remarkable proof but the margin did not contain enough room for the proof.

    This assertion became known as **Fermat's Last Theorem** but it more prop- erly should have been called Fermat's Last Conjecture. Despite the efforts of mathematicians, this "theorem" remained unproved until Andrew Wiles, a British mathematician, first announced a proof in June of 1993. However, it was soon recognized that this proof had a serious gap, but a widely accepted version of the proof was published by Wiles in 1995. Wiles' proof uses many concepts and techniques that were unknown at the time of Fermat. We cannot discuss the proof here, but we will explore and prove the following proposition, which is a (very) special case of Fermat's Last Theorem.

    Proposition. There do not exist prime numbers a, b,and c such that

    $$a^3 + b3 = c3 \tag{3.6.7}$$

    .

    Although Fermat's Last Theorem implies this proposition is true, we will use a proof by contradiction to prove this proposition. For a proof by contradiction, we assume that

    there exist prime numbers a, b, and c such that $a^3 + b^3 = c^3$.

    Since 2 is the only even prime number, we will use the following cases: (1) $a = b = 2$; (2) a and b are both odd; and (3) one of a and b is odd and the other one is 2.

    (a) Show that the case where $a = b = 2$ leads to a contradiction and hence, this case is not possible.
    (b) Show that the case where a and b are both odd leads to a contradiction and hence, this case is not possible.
    (c) We now know that one of a or b must be equal to 2. So we assume that $b = 2$ and that a is an odd prime. Substitute $b = 2$ into the equation $b^3 = c^3 - a^3$ and then factor the expression $c^3 - a^3$. Use this to obtain a contradiction.
    (d) Write a complete proof of the proposition.

Answer

Add texts here. Do not delete this text first.

platform; a detailed edit history is available upon request.

- **3.6: Review of Proof Methods** by Ted Sundstrom is licensed CC BY-NC-SA 3.0. Original source: https://scholarworks.gvsu.edu/books/7.

3.S: Constructing and Writing Proofs in Mathematics (Summary)

Important Definitions

- Divides,divisor,page82
- Factor, multiple, page 82
- Proof, page 85
- Undefined term, page 85
- Axiom, page 85
- Definition,page86
- Conjecture, page 86
- Theorem, page 86
- Proposition,page 86
- Lemma, page 86
- Corollary, page 86
- Congruence modulo n, page 92
- Tautology,page 40
- Contradiction,page 40
- Absolutevalue,page 135

Important Theorems and Results about Even and Odd Integers

- **Exercise (1), Section 1.2**
  If m is an even integer, then $m+1$ is an odd integer.
  If m is an odd integer, then $m+1$ is an even integer.
- **Exercise (2), Section 1.2**
  If x is an even integer and y is an even integer, then $x+y$ is an even integer.
  If x is an even integer and y is an odd integer, then $x+y$ is an odd integer.
  If x is an odd integer and y is an odd integer, then $x+y$ is an even integer.
- **Exercise (3), Section 1.2.** *If x is an even integer and y is an integer, then $x \cdot y$ is an even integer.*
- **Theorem1.8.** *If x is an odd integer and y is an odd integer, then $x \cdot y$ is an odd integer.*
- **Theorem 3.7**. *The integer n is an even integer if and only if n^2 is an even integer.*
  Preview Activity $3.S.2$ in Section 3.2. *The integer n is an odd integer if and only if n^2 is an odd integer.*

Important Theorems and Results about Divisors

- **Theorem 3.1.** *For all integers a, b, and c with $a \neq 0$, if $a|b$ and $b|c$, then $a|c$.*
- **Exercise (3), Section 3.1**. *For all integers a, b, and c with $a \neq 0$,*
  If $a|b$ and $a|c$, then $a|(b+c)$.
  If $a|b$ and $a|c$, then $a|(b-c)$.
- **Exercise (3a), Section 3.1.** *For all integers a, b, and c with $a \neq 0$, if $a|b$, then $a|(bc)$.*
- **Exercise (4), Section 3.1.** *For all nonzero integers a and b, if $a|b$ and $b|a$, then $a = \pm b$.*

The Division Algorithm

Let a and b be integers with $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < b.$$

Important Theorems and Results about Congruence

- **Theorem 3.28.** *Let $a, b, c \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then*

  $(a+c) \equiv (b+d) \pmod{n}$.

  $ac \equiv bd \pmod{n}$.
  For each $m \in \mathbb{N}$, $a^m \equiv b^m \pmod{n}$.

- **Theorem 3.30.** *For all integers a, b, and c,*
  Reflexive Property. $a \equiv a \pmod{n}$.
  Symmetric Property. *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$.
  Transitive Property. *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$.
- **Theorem 3.31.** *Let* $a \in \mathbb{Z}$ *and let* $n \in \mathbb{N}$. *If* $a = nq + r$ *and* $0 \leq r < n$ *for some integers q and r, then* $a \equiv r \pmod{n}$.
- **Corollary 3.32.** *Each integer is congruent, modulo* n, *to precisely one of the integers 0, 1, 2, ...,* $n - 1$. *That is, for each integer* a, *there exists a unique integer* r *such that*

$$a \equiv r \pmod{n} \text{ and } 0 \leq r < n.$$

CHAPTER OVERVIEW

4: Mathematical Induction (with Sequences)

Mathematical induction is a mathematical proof technique that is used to prove that a property $P(n)$ holds for every natural number n, i.e. for n = 0, 1, 2, 3, and so on.

Thumbnail: Mathematical induction can be informally illustrated by reference to the sequential effect of falling dominoes. Image used wtih permission (CC BY-SA 3.0; Pokipsy76).

4.1: The Principle of Mathematical Induction

Preview Activity 4.1.1: Exploring Statements of the Form $(\forall n \in \mathbb{N})(P(n))$

One of the most fundamental sets in mathematics is the set of natural numbers $\mathbb{N}$. In this section, we will learn a new proof technique, called mathematical induction, that is often used to prove statements of the form $(\forall n \in \mathbb{N})(P(n))$. In Section 4.2, we will learn how to extend this method to statements of the form $(\forall n \in T)(P(n))$, where T is a certain type of subset of the integers $\mathbb{Z}$.

For each natural number n, let $P(n)$ be the following open sentence:

$$4 \text{ divides } (5^n - 1).$$

1. Does this open sentence become a true statement when $n = 1$? That is, is 1 in the truth set of $P(n)$?
2. Does this open sentence become a true statement when $n = 2$? That is, is 2 in the truth set of $P(n)$?
3. Choose at least four more natural numbers and determine whether the open sentence is true or false for each of your choices.

All of the examples that were used should provide evidence that the following proposition is true:

$$\text{For each natural number } n, 4 \text{ divides } (5^n - 1).$$

We should keep in mind that no matter how many examples we try, we cannot prove this proposition with a list of examples because we can never check if 4 divides $(5^n - 1)$ for every natural number n. Mathematical induction will provide a method for proving this proposition.

For another example, for each natural number n, we now let $Q(n)$ be the following open sentence:

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{4.1.1}$$

The expression on the left side of the previous equation is the sum of the squares of the first n natural numbers. So when $n = 1$, the left side of equation (4.1.1) is 1^2. When $n = 2$, the left side of equation (4.1.1) is $1^2 + 2^2$.

4. Does $Q(n)$ become a true statement when

   - $n = 1$? (Is 1 in the truth set of $Q(n)$?
   - $n = 2$? (Is 1 in the truth set of $Q(n)$?
   - $n = 3$? (Is 1 in the truth set of $Q(n)$?

5. Choose at least four more natural numbers and determine whether the open sentence is true or false for each of your choices. A table with the columns n, $1^2 + 2^2 + \ldots + n^2$, and $\frac{n(n+1)(2n+1)}{6}$ may help you organize your work.

All of the examples we have explored, should indicate the following proposition is true:

For each natural number n, \(1^2 + 2^2 + ... + n^2 = \dfrac{n(n + 1)(2n + 1)}{6}.\]

In this section, we will learn how to use mathematical induction to prove this statement.

Preview Activity 4.1.1: A Property of the Natural Numbers

Intuitively, the natural numbers begin with the number 1, and then there is 2, then 3, then 4, and so on. Does this process of "starting with 1" and "adding 1 repeatedly" result in all the natural numbers? We will use the concept of an inductive set to explore this idea in this activity.

Definition

A set T that is a subset of $\mathbb{Z}$ is an **inductive set** provided that for each integer k, if $k \in T$, then $k + 1 \in T$.

1. Carefully explain what it means to say that a subset T of the integers $\mathbb{Z}$ is not an inductive set. This description should use an existential quantifier.
2. Use the definition of an inductive set to determine which of the following sets are inductive sets and which are not. Do not worry about formal proofs, but if a set is not inductive, be sure to provide a specific counterexample that proves it is not inductive.

   (a) $A = \{1, 2, 3, \ldots, 20\}$
   (b) The set of natural numbers, $\mathbb{N}$
   (c) $B = \{n \in \mathbb{N} | n \geq 5\}$
   (d) $S = \{n \in \mathbb{Z} | n \geq -3\}$
   (e) $R = \{n \in \mathbb{Z} | n \leq 100\}$
   (f) The set of integers, $\mathbb{Z}$
   (g) The set of odd natural numbers.
3. This part will explore one of the underlying mathematical ideas for a proof by induction. Assume that $T \subseteq \mathbb{N}$ and assume that $1 \in T$ and that T is an inductive set. Use the definition of an inductive set to answer each of the following:

   (a) Is $2 \in T$? Explain.
   (b) Is $3 \in T$? Explain.
   (c) Is $4 \in T$? Explain.
   (d) Is $100 \in T$? Explain.
   (e) Do you think that $T = \mathbb{N}$? Explain.

Inductive Sets

The two open sentences in Preview Activity 4.1.1 appeared to be true for all values of n in the set of natural numbers, $\mathbb{N}$. That is, the examples in this preview activity provided evidence that the following two statements are true.

- For each natural number n, 4 divides $(5^n - 1)$.
- For each natural number n, $1^2 + 2^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

One way of proving statements of this form uses the concept of an inductive set introduced in Preview Activity 4.1.2. The idea is to prove that if one natural number makes the open sentence true, then the next one also makes the open sentence true. This is how we handle the phrase "and so on" when dealing with the natural numbers. In Preview Activity 4.1.2, we saw that the number systems $\mathbb{N}$ and $\mathbb{Z}$ and other sets are inductive. What we are trying to do is somehow distinguish $\mathbb{N}$ from the other inductive sets. The way to do this was suggested in Part (3) of Preview Activity 4.1.2. Although we will not prove it, the following statement should seem true.

Statement 1: For each subset T of $\mathbb{N}$, if $1 \in T$ and T is inductive, then $T = \mathbb{N}$.

Notice that the integers, $\mathbb{Z}$, and the set $S = \{n \in \mathbb{Z} | n \geq -3\}$ both contain 1 and both are inductive, but they both contain numbers other than natural numbers. For example, the following statement is false:

Statement 2: For each subset T of $\mathbb{Z}$, if $1 \in T$ and T is inductive, then $T = \mathbb{Z}$.

The set $S = \{n \in \mathbb{Z} | n \geq -3\} = \{-3, -2, -1, 0, 1, 2, 3, \ldots\}$ is a counterexample that shows that this statement is false.

? Progress Check 4.1 (Inductive Sets)

Suppose that T is an inductive subset of the integers. Which of the following statements are true, which are false, and for which ones is it not possible to tell?

1. $1 \in T$ and $5 \in T$.
2. If $1 \in T$, then $5 \in T$.
3. If $5 \notin T$, then $2 \notin T$.
4. For each integer k, if $k \in T$, then $k + 7 \in T$.
5. For each integer k, $k \notin T$ or $k + 1 \in T$.
6. There exists an integer k such that $k \in T$ and $k + 1 \notin T$.

7. For each integer k, if $k+1 \in T$, then $k \in T$.
8. For each integer k, if $k+1 \notin T$, then $k \notin T$.

Answer

Add texts here. Do not delete this text first.

The Principle of Mathematical Induction

Although we proved that Statement (2) is false, in this text, we will not prove that Statement (1) is true. One reason for this is that we really do not have a formal definition of the natural numbers. However, we should be convinced that Statement (1) is true. We resolve this by making Statement (1) an axiom for the natural numbers so that this becomes one of the defining characteristics of the natural numbers.

The Principle of Mathematical Induction

If T is a subset of $\mathbb{N}$ such that

1. $1 \in T$, and
2. For every $k \in \mathbb{N}$, if $k \in T$, then $(k+1) \in T$.

Then $T = \mathbb{N}$.

Using the Principle of Mathematical Induction

The primary use of the Principle of Mathematical Induction is to prove statements of the form

$$(\forall n \in \mathbb{N})(P(n)).$$

where $P(n)$ is some open sentence. Recall that a universally quantified statement like the preceding one is true if and only if the truth set T of the open sentence $P(n)$ is the set $\mathbb{N}$. So our goal is to prove that $T = \mathbb{N}$, which is the conclusion of the Principle of Mathematical Induction. To verify the hypothesis of the Principle of Mathematical Induction, we must

1. Prove that $1 \in T$. That is, prove that $P(1)$ is true.
2. Prove that if $k \in T$, then $(k+1) \in T$. That is, prove that if $P(k)$ is true, then $P(k+1)$ is true.

The first step is called the **basis step** or the **initial step**, and the second step is called the **inductive step**. This means that a proof by mathematical induction will have the following form:

Procedure for a Proof by Mathematical Induction

To prove: $(\forall n \in \mathbb{N})(P(n))$

Basis step: Prove $P(1)$.\

Inductive step: Prove that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

We can then conclude that $P(n)$ is true for all $n \in \mathbb{N}$

Note that in the inductive step, we want to prove that the conditional statement "for each $k \in \mathbb{N}$, if $P(k)$ then $P(k+1)$" is true. So we will start the inductive step by assuming that $P(k)$ is true. This assumption is called the **inductive assumption** or the **inductive hypothesis**.

The key to constructing a proof by induction is to discover how $P(k+1)$ is related to $P(k)$ for an arbitrary natural number k. For example, in Preview Activity 4.1.1, one of the open sentences $P(n)$ was

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Sometimes it helps to look at some specific examples such as $P(2)$ and $P(3)$. The idea is not just to do the computations, but to see how the statements are related. This can sometimes be done by writing the details instead of immediately doing computations.

$$P(2) \quad is \quad 1^2+2^2 = \frac{2\cdot 3\cdot 5}{6} \tag{4.1.2}$$

$$P(3) \quad is \quad 1^2+2^2+3^2 = \frac{3\cdot 4\cdot 7}{6} \tag{4.1.3}$$

In this case, the key is the left side of each equation. The left side of $P(3)$ is obtained from the left side of $P(2)$ by adding one term, which is 3^2. This suggests that we might be able to obtain the equation for $P(3)$ by adding 3^2 to both sides of the equation $P(2)$. Now for the general case, if $k \in \mathbb{N}$, we look at $P(k+1)$ and compare it to $P(k)$.

$$P(k) \quad is \quad 1^2+2^2+\ldots+k^2 = \frac{k(k+1)(2k+1)}{6} \tag{4.1.4}$$

$$P(k+1) \quad is \quad 1^2+2^2+\ldots+(k+1)^2 = \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6} \tag{4.1.5}$$

The key is to look at the left side of the equation for $P(k+1)$ and realize what this notation means. It means that we are adding the squares of the first $k+1$ natural numbers. This means that we can write

$$1^2+2^2+\ldots+(k+1)^2 = 1^2+2^2+\ldots+k^2+(k+1)^2.$$

This shows us that the left side of the equation for $P(k+1)$ can be obtained from the left side of the equation for $P(k)$ by adding $(k+1)^2$. This is the motivation for proving the inductive step in the following proof.

Proposition 4.2.

For each natural number n,

$$1^2+2^2+\ldots+n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof

We will use a proof by mathematical induction. For each natural number n, we let $P(n)$ be

$$1^2+2^2+\ldots+n^2 = \frac{n(n+1)(2n+1)}{6}.$$

We first prove that $P(1)$ is true. Notice that $\frac{1(1+1)(2\cdot 1+1)}{6} = 1$. This shows that

\(1^2 = \dfrac{1(1 + 1)(2 \cdot 1 + 1}{6},

which proves that $P(1)$ is true.

For the inductive step, we prove that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number and assume that $P(k)$ is true. That is, assume that

$$1^2+2^2+\ldots+k^2 = \frac{k(k+1)(2k+1)}{6}. \tag{4.1.6}$$

The goal now is to prove that $P(k+1)$ is true. That is, it must be proved that

$$1^2+2^2+\ldots+k^2+(k+1)^2 = \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6} \tag{4.1.7}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}. \tag{4.1.8}$$

To do this, we add $(k+1)^2$ to both sides of equation (1) and algebraically rewrite the right side of the resulting equation. This gives

$$1^2+2^2+\ldots+k^2+(k+1)^2 = \frac{k(k+1)(2k+1)}{6}+(k+1)^2 \tag{4.1.9}$$

$$= \frac{k(k+1)(2k+1)+6(k+1)^2}{6} \tag{4.1.10}$$

$$= \frac{(k+1)[k(2k+1)+6(k+1)]}{6} \tag{4.1.11}$$

$$= \frac{(k+1)(2k^2+7k+6)}{6} \tag{4.1.12}$$

$$= \frac{(k+1)(k+2)(2k+3)+6(k+1)^2}{6} \tag{4.1.13}$$

Comparing this result to equation (2), we see that if $P(k)$ is true, then $P(k+1)$ is true. Hence, the inductive step has been established, and by the Principle of Mathematical Induction, we have proved that for each natural number n, $1^2+2^2+\ldots+n^2 = \frac{n(n+1)(2n+1)}{6}$.

Writing Guideline

The proof of Proposition 4.2 shows a standard way to write an induction proof. When writing a proof by mathematical induction, we should follow the guideline that we always keep the reader informed. This means that at the beginning of the proof, we should state that a proof by induction will be used. We should then clearly define the open sentence (P(n)\) that will be used in the proof.

Summation Notation

The result in Proposition 4.2 could be written using summation notation as follows:

$$\text{For each natural number } n, \sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

In this case, we use j for the index for the summation, and the notation $\sum_{j=1}^{n} j^2$ tells us to add all the values of j^2 for j from 1 to n, inclusive. That is,

$$\sum_{j=1}^{n} j^2 = 1^2+2^2+\ldots+n^2.$$

So in the proof of Proposition 4.2, we would let $P(n)$ be $\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$, and we would use the fact that for each natural number k,

$$\sum_{j=1}^{k+1} j^2 = (\sum_{j=1}^{k} j^2)+(k+1)^2.$$

? Progress Check 4.3 (An Example of a Proof by Induction)

1. Calculate $1+2+3+\ldots+n$ and $\frac{n(n+1)}{2}$ for several natural numbers n. What do you observe?
2. Use mathematical induction to prove that $1+2+3+\ldots+n = \frac{n(n+1)}{2}$. To do this, let $P(n)$ be the open sentence, "$1+2+3+\ldots+n = \frac{n(n+1)}{2}$." For the basis step, notice that the equation $1 = \frac{1(1+1)}{2}$ shows that $P(1)$ is true. Now let k be a natural number and assume that $P(k)$ is true. That is, assume that

$$1+2+3+\ldots+k = \frac{k(k+1)}{2}, \tag{4.1.14}$$

and complete the proof.

Answer

Add texts here. Do not delete this text first.

Some Comments about Mathematical Induction

1. The basis step is an essential part of a proof by induction. See Exercise (19) for an example that shows that the basis step is needed in a proof by induction.
2. Exercise (20) provides an example that shows the inductive step is also an essential part of a proof by mathematical induction.
3. It is important to remember that the inductive step in an induction proof is a proof of a conditional statement. Although we did not explicitly use the forward-backward process in the inductive step for Proposition 4.2, it was implicitly used in the discussion prior to Proposition 4.2. The key question was, "How does knowing the sum of the first k squares help us find the sum of the first $(k+1)$ squares?"
4. When proving the inductive step in a proof by induction, the key question is,

   How does knowing $P(k)$ help us prove $P(k+1)$?

   In Proposition 4.2, we were able to see that the way to answer this question was to add a certain expression to both sides of the equation given in $P(k)$. Sometimes the relationship between $P(k)$ and $P(k+1)$ is not as easy to see. For example, in Preview Activity 4.1.1, we explored the following proposition:

   For each natural number n, 4 divides (5^n-1).

   This means that the open sentence, $P(n)$, is "4 divides (5^n-1)." So in the inductive step, we assume $k \in \mathbb{N}$ and that 4 divides (5^k-1). This means that there exists an integer m such that

   $$5^k - 1 = 4m. \tag{4.1.15}$$

   In the backward process, the goal is to prove that 4 divides $(5^{k+1}-1)$. This can accomplished if we can prove that there exists an integer s such that

   $$5^{k+1} - 1 = 4s. \tag{4.1.16}$$

   We now need to see if there is anything in equation (4.1.15) that can be used in equation (4.1.16). The key is to find something in the equation $5^k - 1 = 4m$ that is related to something similar in the equation $5^{k+1} - 1 = 4s$ In this case, we notice that

   $$5^{k+1} = 5 \cdot 5^k. \tag{4.1.17}$$

   So if we can solve $5^k - 1 = 4m$ for 5^k, we could make a substitution for 5^k. This is done in the proof of the following proposition.

Proposition 4.4.

For every natural number n, 4 divides (5^n-1).

Proof

(Proof by Mathematical Induction) For each natural number n, let $P(n)$ be "4 divides (5^n-1)" We first prove that $P(1)$ is true. Notice that when $n=1$, $5^n-1=4$. Since 4 divides 4, $P(1)$ is true.

For the inductive step, we prove that for all $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number and assume that $P(k)$ is true. That is, assume that

$$4 \text{ divides } (5^k-1).$$

This means that there exists an integer m such that

$$5^k - 1 = 4m.$$

Thus,

$$5^k = 4m + 1. \tag{4.1.18}$$

In order to prove that $P(k+1)$ is true, we must show that 4 divides $(5^{k+1} - 1)$. Since $5^{k+1} = 5 \cdot 5^k$, we can write

$$5^{k+1} - 1 = 5 \cdot 5^k - 1. \tag{4.1.19}$$

We now substitute the expression for 5k from equation (4.1.18) into equation (4.1.19). This gives

$$\begin{aligned} 5^{k+1} - 1 &= 5 \cdot 5^k - 1 \\ &= 5(4m+1) - 1 \\ &= (20m+5) - 1 \\ &= 20m + 4 \\ &= 4(5m+1) \end{aligned} \tag{4.1.20}$$

Since $(5m+1)$ is an integer, equation (4.1.20) shows that 4 divides $(5^{k+1} - 1)$. Therefore, if $P(k)$ is true, then $P(k+1)$ is true and the inductive step has been established. Thus, by the principle of Mathematical Induction, for every natural number n, 4 divides $(5^n - 1)$.

Proposition 4.4 was stated in terms of "divides." We can use congruence to state a proposition that is equivalent to Proposition 4.4. The idea is that the sentence, 4 divides $(5^n - 1)$ means that $5^n \equiv 1 \pmod 4$. So the following proposition is equivalent to Proposition 4.4.

Proposition 4.5.

For every natural number n, $5^n \equiv 1 \pmod 4$.

Since we have proved Proposition 4.4, we have in effect proved Proposition 4.5. However, we could have proved Proposition 4.5 first by using the results in Theorem 3.28 on page 147. This will be done in the next progress check.

? Progress Check 4.6 (Proof of Proposition 4.5) .

To prove Proposition 4.5, we let $P(n)$ be $5^n \equiv 1 \pmod 4$ and notice that $P(1)$ is true since $5 \equiv 1 \pmod 4$. For the inductive step, let k be a natural number and assume that $P(k)$ is true. That is, assume that $5^n \equiv 1 \pmod 4$.

1. What must be proved in order to prove that $P(k+1)$ is true?
2. Since $5^{k+1} = 5 \cdot 5^k$, multiply both sides of the congruence $5^k \equiv 1 \pmod 4$ by 5. The results in Theorem 3.28 on page 147 justify this step.
3. Now complete the proof that for each $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true and complete the induction proof of Proposition 4.5.

It might be nice to compare the proofs of Propositions 4.4 and 4.5 and decide which one is easier to understand.

Answer

Add texts here. Do not delete this text first.

? Exercises for Section 4.1

1. Which of the following sets are inductive sets? Explain.

   (a) $\mathbb{Z}$
   (b) $\{x \in \mathbb{N} | x \geq 4\}$
   (c) $\{x \in \mathbb{Z} | x \leq 10\}$
   (d) {1, 2, 3, ..., 500}

2. (a) Can a finite, nonempty set be inductive? Explain.
   (b) Is the empty set inductive? Explain.
3. Use mathematical induction to prove each of the following:

   (a) For each natural number n, $2+5+8+\cdots+(3n-1)=\dfrac{n(3n+1)}{2}$.
   (b) For each natural number n, $1+5+9+\cdots+(4n-3)=n(2n-1)$.
   (c) For each natural number n, $1^3+2^3+3^3+\cdots+n^3=[\dfrac{n(n+1)}{2}]^2$.
4. Based on the results in Progress Check 4.3 and Exercise (3c), if $n\in\mathbb{N}$, is there any conclusion that can be made about the relationship between the sum $(1^3+2^3+3^3+\ldots+n^3)$ and the sum $(1+2+3+\cdots+n)$?
5. Instead of using induction, we can sometimes use previously proven results about a summation to obtain results about a different summation.

   (a) Use the result in Progress Check4.3 to prove the following proposition:

$$\text{For each natural number } n, 3+6+9+\ldots+3n=\frac{3n(n+1)}{2}. \tag{4.1.21}$$

   (b) Subtract n from each side of the equation in Part (a). On the left side of this equation, explain why this can be done by subtracting 1 from each term in the summation.
   (c) Algebraically simplify the right side of the equation in Part (b) to obtain a formula for the sum $2+5+8+\ldots(3n-1)$. Compare this to Exercise (3a).
6. (a) Calculate $1+3+5+\cdots+(2n-1)$ for several nuatural numbers n.
   (b) Based on your work in exercise (6a), if $n\in\mathbb{N}$, make a conjecture about the value of the sum $1+3+5+\cdots+(2n-1)=\sum_{j=1}^{n}(2j-1)$.
   (c) Use mathematical induction to prove your conjecture in Exercise (6b).
7. In Section 3.1, we defined congruence modulo n for a natural number n, and in Section 3.5, we used the Division Algorithm to prove that each integer is congruent, modulo n, to precisely one of the integers 0, 1, 2, \cdot\cdot\cdot, $n-1$ (Corollary 3.32).

   (a) Find the value of r so that $4\equiv r \pmod 3$ and $r\in\{0,1,2\}$.
   (b) Find the value of r so that $4^2\equiv r \pmod 3$ and $r\in\{0,1,2\}$.
   (c) Find the value of r so that $4^3\equiv r \pmod 3$ and $r\in\{0,1,2\}$.
   (d) For two other values of n, find the value of r so that $4^n\equiv r \pmod 3$ and $r\in\{0,1,2\}$.
   (e) If $n\in\mathbb{N}$ make a conjecture concerning the value of r where $4^n\equiv r \pmod 3$ and $r\in\{0,1,2\}$. This conjecture should be written as a self-contained proposition including an appropriate quantifier.
   (f) Use mathematical induction to prove your conjecture.
8. Use mathematical induction to prove each of the following:

   (a) For each natural number n, 3 divides (4^n-1).
   (b) For each natural number n, 6 divides (n^3-n).
9. In Exercise (7), we proved that for each natural number n, $4^n\equiv 1 \pmod 3$. Explain how this result is related to the proposition in Exercise (8a).
10. Use mathematical induction to prove that for each natural number n, 3 divides n^3+23n. Compare this proof to the proof from Exercise (18) in Section 3.5.
11. (a) Calculate the value of 5^n-2^n for $n=1, n=2, n=3, n=4, n=5$ and $n=6$.
    (b) Based on your work in Part (a), make a conjecture about the values of 5^n-2^n for each natural number n.
    (c) Use mathematical induction to prove your conjecture in Part (b).
12. Let x and y be integers. Prove that for each natural number n, $(x-y)$ divides (x^n-y^n). Explain why your conjecture in Exercise (11) is a special case of this result.
13. Prove Part (3) of Theorem 3.28 from Section 3.4. Let $n\in\mathbb{N}$ and let a and b be integers. For each $m\in\mathbb{N}$, if $a\equiv b \pmod n$, then $a^m\equiv b^m \pmod n$.

14. Use mathematical induction to prove that the sum of the cubes of any three consecutive natural numbers is a multiple of 9.
15. Let a be a real number. We will explore the derivatives of the function $f(x) = e^{ax}$. By using the chain rule, we see that

$$\frac{d}{dx}(e^{ax}) = ae^{ax}. \tag{4.1.22}$$

Recall that the second derivative of a function is the derivative of the derivative function. Similarly, the third derivative is the derivative of the second derivative.

(a) What is $\frac{d^2}{dx^2}(e^{ax})$, the second derivative of e^{ax}?
(b) What is $\frac{d^3}{dx^3}(e^{ax})$, the third derivative of e^{ax}?
(c) Let n be a natural number. Make a conjecture about the nth derivatives of the function $f(x) = e^{ax}$. That is, what is $\frac{d^n}{dx^n}(e^{ax})$? This conjecture should be written as a self-contained proposition including an appropriate quantifier.
(d) Use mathematical induction to prove that your conjecture.
16. In calculus, it can be shown that

$$\begin{aligned} \int sin^2 x dx &= \frac{x}{2} - \frac{1}{2} sinxcosx + c \text{ and} \\ \int cos^2 x dx &= \frac{x}{2} + \frac{1}{2} sinxcosx + c. \end{aligned} \tag{4.1.23}$$

Using integration by parts, it is also possible to prove that for each natural number n,

$$\begin{aligned} \int sin^n x dx &= -\frac{1}{n} sin^{n-1} x cosx + \frac{n-1}{n} \int sin^{n-2} x dx \text{ and} \\ \int cos^n x dx &= \frac{1}{n} cos^{n-1} x sinx + \frac{n-1}{n} \int cos^{n-2} x dx. \end{aligned} \tag{4.1.24}$$

(a) Determine the values of

$$\int_0^{\pi/2} sin^2 x dx \text{ and } \int_0^{\pi/2} sin^4 x dx. \tag{4.1.25}$$

(b) Use mathematical induction to prove that for each natural number n

$$\begin{aligned} \int_0^{\pi/2} sin^{2n} x dx &= \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n)} \frac{\pi}{2} \text{ and} \\ \int_0^{\pi/2} sin^{2n+1} x dx &= \frac{2 \cdot 4 \cdot 6 \cdots (2n)}{1 \cdot 3 \cdot 5 \cdots (2n+1).} \end{aligned} \tag{4.1.26}$$

These are known as the ***Wallis sine formulas***.
(c) Use mathematical induction to prove that

$$\begin{aligned} \int_0^{\pi/2} cos^{2n} x dx &= \frac{1 \cdot 3 \cdot 5 \cdots (2n-1)}{2 \cdot 4 \cdot 6 \cdots (2n)} \frac{\pi}{2} \text{ and} \\ \int_0^{\pi/2} cos^{2n+1} x dx &= \frac{2 \cdot 4 \cdot 6 \cdots (2n)}{1 \cdot 3 \cdot 5 \cdots (2n+1).} \end{aligned} \tag{4.1.27}$$

These are known as the ***Wallis cosine formulas***.

17. (a) Why is it not possible to use mathematical induction to prove a proposition of the form

$$(\forall x \in \mathbb{Q})(P(x)), \tag{4.1.28}$$

where $P(x)$ is some predicate?
(b) Why is it not possible to use mathematical induction to prove a proposition of the form
For each real number x with $x \geq 1$, $P(x)$,
where \(P(x) is some predicate?

18. **Evaluation of proofs**
See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

For each natural number n, $1+4+7+\cdots+(3n-2)=\dfrac{n(3n-1)}{2}$.

Proof

We will prove this proposition using mathematical induction. So we let $P(n)$ be the open sentence

$$1+4+7+\cdots+(3n-2).$$

Using $n=1$, we see taht $3n-2=1$ and hence, $P(1)$ is true.

We now assume taht $P(k)$ is true. That is,

$$1+4+7+\cdots+(3k-2)=\frac{k(3k-1)}{2}.$$

We then see that

$$\begin{aligned} 1+4+7+\cdots+(3k-2)+(3(k+1)-2) &= \frac{(k+1)(3k+2)}{2} \\ \frac{k(3k-1)}{2}+(3k+1) &= \frac{(k+1)(3k+2)}{2} \\ \frac{(3k^2-k)+(6k+2)}{2} &= \frac{3k^2+5k+2}{2} \\ \frac{3k^2+5k+2}{2} &= \frac{3k^2+5k+2}{2}. \end{aligned} \tag{4.1.29}$$

We have thus proved that $P(k+1)$ is true, and hence, we have proved the proposition.

(b)

For each natural number n, $1+4+7+\cdots+(3n-2)=\dfrac{n(3n-1)}{2}$.

Proof

We will prove this proposition using mathematical induction. So we let

$$P(n)=1+4+7+\cdots+(3n-2) \quad .$$

Using $n=1$, we see that $P(1)=1$ and hence, $P(1)$ is true.

We now assume that $P(k)$ is true. That is,

$$1+4+7+\cdots+(3k-2)=\frac{k(3k-1)}{2}.$$

We then see that

$$\begin{aligned} P(k+1) &= 1+4+7+\cdots+(3k-2)+(3(k+1)-2) \\ &= \frac{k(3k-2)}{2}+3(k+1)-2 \\ &= \frac{3k^2-k+6k+6-4}{2} \\ &= \frac{3k^2+5k+2}{2} \\ &= \frac{(k+1)(3k+2)}{2}. \end{aligned} \tag{4.1.30}$$

we have thus proved that $P(k+1)$ is true, and hence, we have proved the proposition.

(c)

All dogs are the same breed.

Proof

We will prove this proposition using mathematical induction. For each natural number n, we let $P(n)$ be

Any set of n dogs consists entirely of dogs of the same breed.

We will prove that for each natural number n, $P(n)$ is true, which will prove that all dogs are the same breed. A set with only one dog consists entirely of dogs of the same breed and, hence, $P(1)$ is true.

So we let k be a natural number and assume that $P(k)$ is true, that is, that every set of k dogs consists of dogs of the same breed. Now consider a set D of $k+1$ dogs, where

$$D = \{d_1, d_2, \ldots, d_k, d_{k+1}\}.$$

If we remove the dog d_1 from the set D, we then have a set D_1 of k dogs, and using the assumption that $P(k)$ is true, these dogs must all be of the same breed. Similarly, if we remove d_{k+1} from the set D, we again have a set D_2 of k dogs, and these dogs must all be of the same breed. Since $D = D_1 \cup D_2$, we have proved that all of the dogs in D must be of the same breed.

This proves that if $P(k)$ is true, then $P(k+1)$ is true and, hence, by mathematical induction, we have proved that for each natural number n, any set of n dogs consists entirely of dogs of the same breed.

Explorations and Activities

19. **The Importance of the Basis Step**. Most of the work done in constructing a proof by induction is usually in proving the inductive step. This was certainly the case in Proposition 4.2. However, the basis step is an essential part of the proof. Without it, the proof is incomplete. To see this, let $P(n)$ be

$$1+2+\cdots+n = \frac{n^2+n+1}{2}. \tag{4.1.31}$$

(a) Let $k \in \mathbb{N}$. Complete the following proof that if $P(k)$ is true, then $P(k+1)$ is true.
Let $k \in mathbbN$. Assume that $P(k)$ is true. That is, assume that

$$1+2+\cdots+k = \frac{k^2+k+1}{2}. \tag{4.1.32}$$

The goal is to prove that $P(k+1)$ is true. That is, we need to prove that

$$1+2+\cdots+k+(k+1) = \frac{(k+1)^2+(k+1)+1}{2}. \tag{4.1.33}$$

To do this, we add $k+1$ to both sides of equation (4.1.32). This gives

$$\begin{aligned} 1+2+\cdots+k+(k+1) &= \frac{k^2+k+1}{2}+(k+1) \\ &= \cdots. \end{aligned} \tag{4.1.34}$$

(b) Is $P(1)$ true? Is $P(2)$ true? What about $P(3)$ and $P(4)$? Explain how this shows that the basis step is an essential part of a proof by induction.

20. **Regions of a Circle.** Place n equally spaced points on a circle and connect each pair of points with the chord of the circle determined by that pair of points. See Figure 4.1.

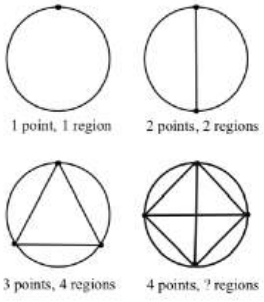


Figure 4.1: Regions of Circles

Count the number of distinct regions within each circle. For example, with three points on the circle, there are four distinct regions. Organize your data in a table with two columns: “Number of Points on the Circle” and “Number of Distinct Regions in the Circle.”

(a) How many regions are there when there are four equally spaced points on the circle?
(b) Based on the work so far, make a conjecture about how many distinct regions would you get with five equally spaced points.
(c) Based on the work so far, make a conjecture about how many distinct regions would you get with six equally spaced points.
(d) Figure 4.2 shows the figures associated with Parts (b) and (c). Count the number of regions in each case. Are your conjectures correct or incorrect?
(e) Explain why this activity shows that the inductive step is an essential part of a proof by mathematical induction.

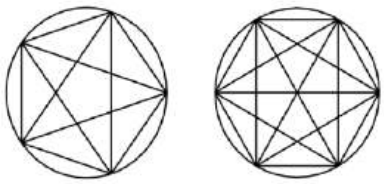


Figure 4.2: Regions of Circles

Answer

Add texts here. Do not delete this text first.

4.2: Other Forms of Mathematical Induction

Preview Activity 4.2.1: Exploring a Proposition about Factorials

Definition

If n is a natural number, we define n *factorial*, denoted by $n!$, to be the product of the first n natural numbers. In addition, we define $0!$ to be equal to 1.

Using this definition, we see that

$$\begin{aligned} 0! &= 1 & 3! &= 1\cdot 2\cdot 3 = 6 \\ 1! &= 1 & 4! &= 1\cdot 2\cdot 3\cdot 4 = 24 \\ 2! &= 1\cdot 2 = 2 & 5! &= 1\cdot 2\cdot 3\cdot 4\cdot 5 = 120. \end{aligned} \tag{4.2.1}$$

In general, we write $n! = 1\cdot 2\cdot 3\cdots(n-1)\cdot n$ or $n! = n\cdot(n-1)\cdots 2\cdot 1$. Notice that for any natural number n, $n! = n\cdot(n-1)!$.

1. Compute the values of 2^n and $n!$ for each natural number n with $1 \le n \le 7$.

Now let $P(n)$ be the open sentence, "$n! > 2^n$."

2. Which of the statements $P(1)$ through $P(1)$ are true?

3. Based on the evidence so far, does the following proposition appear to be true or false? For each natural number n with $n \ge 4$, $n! > 2^n$.

Let k be a natural number with $k \ge 4$. Suppose that we want to prove that if $P(k)$ is true, then $P(k+1)$ is true. (This could be the inductive step in an induction proof.) To do this, we would be assuming that $k! > 2^k$ and would need to prove that $(k+1)! > 2^{k+1}$. Notice that if we multiply both sides of the inequality $k! > 2^k$ by $(k+1)$, we obtain

$$(k+1)\cdot k! > (k+1)2^k. \tag{4.2.2}$$

4. In the inequality in (4.2.2), explain why $(k+1)\cdot k! = (k+1)!$.

5. Now look at the right side of the inequality in (4.2.2). Since we are assuming that $k \ge 4$, we can conclude that $(k+1) > 2$. Use this to help explain why $(k+1)2^k > 2^{k+1}$.

6. Now use the inequality in (4.2.2) and the work in steps (4) and (5) to explain why $(k+1)! > 2^{k+1}$.

PREVIEW ACTIVITY 4.2.1: Prime Factors of a Natural Number

Recall that a natural number p is a **prime number** provided that it is greater than 1 and the only natural numbers that divide p are 1 and p. A natural number other than 1 that is not a prime number is a **composite number**. The number 1 is neither prime nor composite.

1. Give examples of four natural numbers that are prime and four natural numbers that are composite.
2. Write each of the natural numbers 20, 40, 50, and 150 as a product of prime numbers.
3. Do you think that any composite number can be written as a product of prime numbers?
4. Write a useful description of what it means to say that a natural number is a composite number (other than saying that it is not prime).
5. Based on your work in Part (2), do you think it would be possible to use induction to prove that any composite number can be written as a product of prime numbers?

The Domino Theory

Mathematical induction is frequently used to prove statements of the form

$$(\forall n \in \mathbb{N})(P(n)). \tag{4.2.3}$$

where $P(n)$ is an open sentence. This means that we are proving that every statement in the following infinite list is true.

$$P(1), P(2), P(3), \ldots \tag{4.2.4}$$

The inductive step in a proof by induction is to prove that if one statement in this infinite list of statements is true, then the next statement in the list must be true. Now imagine that each statement in Equation ??? is a domino in a chain of dominoes. When we prove the inductive step, we are proving that if one domino is knocked over, then it will knock over the next one in the chain. Even if the dominoes are set up so that when one falls, the next one will fall, no dominoes will fall unless we start by knocking one over. This is why we need the basis step in an induction proof. The basis step guarantees that we knock over the first domino. The inductive step, then, guarantees that all dominoes after the first one will also fall.

Now think about what would happen if instead of knocking over the first domino, we knock over the sixth domino. If we also prove the inductive step, then we would know that every domino after the sixth domino would also fall. This is the idea of the *Extended Principle of Mathematical Induction*. It is not necessary for the basis step to be the proof that $P(1)$ is true. We can make the basis step be the proof that $P(M)$ is true, where M is some natural number. The Extended Principle of Mathematical Induction can be generalized somewhat by allowing M to be any integer. We are still only concerned with those integers that are greater than or equal to M.

The Extended Principle of Mathematical Induction

Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

1. $M \in T$, and
2. For every $k \in \mathbb{Z}$ with $k \geq M$, if $k \in T$, then $(k+1) \in T$,

Then T contains all integers greater than or equal to M. That is $\{n \in \mathbb{Z} | n \geq M\} \subseteq T$.

Using the Extended Principle of Mathematical Induction

The primary use of the Principle of Mathematical Induction is to prove statements of the form

$$(\forall n \in \mathbb{Z}, \text{ with} n \geq M)(P(n)).$$

where M is an integer and $P(n)$ is some open sentence. (In most induction proofs, we will use a value of M that is greater than or equal to zero.) So our goal is to prove that the truth set T of the predicate $P(n)$ contains all integers greater than or equal to M. So to verify the hypothesis of the Extended Principle of Mathematical Induction, we must

1. Prove that $M \in T$, That is, prove that $P(M)$ is true.
2. Prove that for every $k \in \mathbb{Z}$ with $k \geq M$, if $k \in T$, then $(k+1) \in T$ .Thatis, prove that if $P(k)$ is true, then $P(k+1)$ is true.

As before, the first step is called the **basis step** or the **initial step**, and the second step is called the **inductive step**. This means that a proof using the Extended Principle of Mathematical Induction will have the following form:

Using the Extended Principle of Mathematical Induction

Let M be an integer. To prove: $(\forall n \in \mathbb{Z}, \text{ with} n \geq M)(P(n))$.

Basis step: Prove $P(M)$.

Inductive step: Prove that for every $k \in \mathbb{Z}$ with $k \geq M$, if $P(k)$ is true, then $P(k+1)$ is true.

We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}, \text{ with} n \geq M)(P(n))$.

This is basically the same procedure as the one for using the Principle of Mathematical Induction. The only difference is that the basis step uses an integer M other than 1. For this reason, when we write a proof that uses the Extended Principle of Mathematical Induction, we often simply say we are going to use a proof by mathematical induction. We will use the work from Preview Activity 4.2.1 to illustrate such a proof.

Proposition 4.7

For each natural number n with $n \geq 4$, $n! > 2^n$.

Proof

We will use a proof by mathematical induction. For this proof, we let

$$P(n) \text{ be "} n! > 2^n \text{."}$$

We first prove that $P(4)$ is true. Using $n = 4$, we see that $4! = 24$ and $2^4 = 16$. This means that $4! > 2^4$ and, hence, $P(4)$ is true.

For the inductive step, we prove that for all $k \in \mathbb{N}$ with $k \geq 4$, if $P(k)$ is true, then $P(k+1)$ is true. So let k be a natural number greater than or equal to 4, and assume that $P(k)$ is true. That is, assume that

$$k! > 2^k. \tag{4.2.5}$$

The goal is to prove that $P(k+1)$ is true or that $(k+1)! > 2^{k+1}$. Multiplying both sides of inequality (4.2.5) by $k+1$ gives

$$\begin{aligned} (k+1) \cdot k! &> (k+1) \cdot 2^k, \text{ or} \\ (k+1)! &> (k+1) \cdot 2^k. \end{aligned} \tag{4.2.6}$$

Now $k \geq 4$. Thus, $k+1 > 2$, and hence $(k+1) \cdot 2^k > 2 \cdot 2^k$. This means that

$$(k+1) \cdot 2^k > 2^{k+1}. \tag{4.2.7}$$

Inequalities (4.2.6) and (4.2.7) show that

$$(k+1)! > 2^{k+1}.$$

and this proves that if $P(k)$ is true, then $P(k+1)$ is true. Thus, the inductive step has been established, and so by the Extended Principle of Mathematical Induction, $n! > 2^n$ for each natural number n with $n \geq 4$.

? Progress Check 4.8: Formulating Conjectures

Formulate a conjecture (with an appropriate quantifier) that can be used as an an- swer to each of the following questions.

1. For which natural numbers n is 3^n greater than $1 + 2^n$?
2. For which natural numbers n is 2^n greater than \((n + 1)^2)?
3. For which natural numbers n is $(1 + \frac{1}{n})^n$ less than n?

Answer

Add texts here. Do not delete this text first.

The Second Principle of Mathematical Induction

Let $P(n)$ be

$$n \text{ is a prime number or } n \text{ is a product of prime numbers.}$$

(This is related to the work in Preview Activity 4.2.2.)

Suppose we would like to use induction to prove that $P(n)$ is true for all natural numbers greater than 1. We have seen that the idea of the inductive step in a proof by induction is to prove that if one statement in an infinite list of statements is true, then the next statement must also be true. The problem here is that when we factor a composite number, we do not get to the previous case. For example, if assume that P.39/ is true and we want to prove that $P(40)$ is true, we could factor 40 as $40 = 2 \cdot 20$. However, the assumption that $P(39)$ is true does not help us prove that $P(40)$ is true.

This work is intended to show the need for another principle of induction. In the inductive step of a proof by induction, we assume one statement is true and prove the next one is true. The idea of this new principle is to assume that all of the previous statements are true and use this assumption to prove the next statement is true. This is stated formally in terms of subsets of natural numbers in the Second Principle of Mathematical Induction. Rather than stating this principle in two versions, we will state the extended version of the Second Principle. In many cases, we will use $M = 1$ or $M = 0$.

The Second Principle of Mathematical Induction

Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

1. $M \in T$, and
2. For every $k \in \mathbb{Z}$ with $k \geq M$, if $\{M, M+1, \ldots, k\} \subseteq T$, then $(k+1) \in T$.

Then T contains all integers greater than or equal to M. That is $\{n \in \mathbb{Z} | n \geq M\} \subseteq T$.

Using the Second Principle of Mathematical Induction

The primary use of mathematical induction is to prove statements of the form

$$(\forall n \in \mathbb{Z},\ \text{with} n \geq M)(P(n)),$$

where M is an integer and $P(n)$ is some predicate. So our goal is to prove that the truth set T of the predicate $P(n)$ contains all integers greater than or equal to M. To use the Second Principle of Mathematical Induction, we must

1. Prove that $M \in T$, That is, prove that $P(M)$ is true.
2. Prove that for every $k \in \mathbb{N}$, if $k \geq M$ and $\{M, M+1, \ldots, k\} \subseteq T$, then $(k+1) \in T$. That is, prove that if $P(M)$, $P(M+1)$, ..., $P(k)$ are true, then $P(k+1)$ is true.

As before, the first step is called the **basis step** or the **initial step**, and the second step is called the **inductive step**. This means that a proof using the Second Principle of Mathematical Induction will have the following form:

Using the Second Principle of Mathematical Induction

Let M be an integer. To prove: $\forall n \in \mathbb{Z} \text{with} n \geq M)(P(n))$

Basis step: Prove $P(M)$.

Inductive step: Let $k \in \mathbb{Z}$ with $k \geq M$. Prove that if $P(M)$, $P(M+1)$, ..., $P(k)$ are true, then $P(k+1)$ is true.

We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq M$.

We will use this procedure to prove the proposition suggested in Preview Activity 4.2.2.

Theorem 4.9

Each natural number greater than 1 is either a prime number or is a product of prime numbers.

Proof

We will use the Second Principle of Mathematical Induction. We let $P(n)$ be

$$n \text{ is either a prime number or } n \text{ is a product of prime numbers.}$$

For the basis step, $P(2)$ is true since 2 is a prime number.

To prove the inductive step, we let k be a natural number with $k \geq 2$. We assume that $P(2)$, $P(3)$, ..., $P(k)$ are true. That is, we assume that each of the natural numbers 2, 3, ..., k is a prime number or a product of prime numbers. The goal is to prove that $P(k+1)$ is true or that $(k+1)$ is a prime number or a product of prime numbers.

Case 1: If $(k+1)$ is a prime number, then $P(k+1)$ is true.

Case 2: If $(k+1)$ is not a prime number, then $(k+1)$ can be factored into a product of natural numbers with each one being less than $(k+1)$. That is, there exist natural numbers a and b with

$$k+1 = a \cdot b, \quad \text{and } 1 < a \leq k \quad \text{and } 1 < b \leq k.$$

Using the inductive assumption, this means that $P(a)$ and $P(b)$ are both true. Consequently, a and b are prime numbers or are products of prime numbers. Since $k+1 = a \cdot b$, we conclude that $(k+1)$ is a product of prime numbers. That is, we conclude that $P(k+1)$ is true. This proves the inductive step.

Hence, by the Second Principle of Mathematical Induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geq 2$, and this means that each natural number greater than 1 is either a prime number or is a product of prime numbers.

We will conclude this section with a progress check that is really more of an activity. We do this rather than including the activity at the end of the exercises since this activity illustrates a use of the Second Principle of Mathematical Induction in which it is convenient to have the basis step consist of the proof of more than one statement.

? Progress Check 4.10 (Using the Second Principle of Induction)

Consider the following question:

For which natural numbers n do there exist nonnegative integers x and $y$such that $n = 3x + 5y$?

To help answer this question, we will let $\mathbb{Z}^* = \{x \in \mathbb{Z} | x \geq 0\}$, and let $P(n)$ be

There exist $x, y \in \mathbb{Z}^*$ such that $n = 3x + 5y$.

Notice that $P(1)$ is false since if both x and y are zero, then $3x + 5y = 0$ and if either $x > 0$ or $y > 0$, then $3x + 5y \geq 3$. Also notice that $P(6)$ is true since $6 = 3 \cdot 2 + 5 \cdot 0$ and $P(8)$ is true since $8 = 3 \cdot 1 + 5 \cdot 1$.

1. Explain why $P(2)$, $P(4)$, and $P(7)$ are false and why $P(3)$ and $P(5)$ are true.
2. Explain why $P(9)$, $P(10)$, $P(11)$, and $P(12)$ are true.

We could continue trying to determine other values of n for which $P(n)$ is true. However, let us see if we can use the work in part (2) to determine if $P(13)$ is true. Notice that $13 = 3 + 10$ and we know that $P(10)$ is true. We should be able to use this to prove that $P(13)$ is true. This is formalized in the next part.

3. Let $k \in \mathbb{N}$. Prove that if $P(8)$, $P(9)$, ..., $P(k)$ are true, then $P(k+1)$ is true. **Hint:** $k+1 = 3 + (k-2)$.

4. Prove the following proposition using mathematical induction. Use the Sec- ond Principle of Induction and have the basis step be a proof that $P(8)$, $P(9)$, and $P(10)$ are true. (The inductive step is part (3).)

Proposition 4.11.

For each $n \in \mathbb{N}$ with $n \geq 8$, there exist nonnegative integers x and y such that $n = 3x + 5y$.

Answer

Add texts here. Do not delete this text first.

? Exercises for Section 4.2

1. Use mathematical induction to prove each of the following:

   (a) For each natural number n with $n \geq 2$, $3^n > 1 + 2^n$.
   (b) For each natural number n with $n \geq 6$, $2^n > (n+1)^2$.
   (c) For each natural number n with $n \geq 3$, $(1 + \frac{1}{n})^n < n$.

2. For each natural number n with $n^2 < 2^n$? Justify your conclusion.
3. For each natural number n with $n! > 3^n$? Justify your conclusion.
4. (a) Verify that $(1 - \frac{1}{4}) = \frac{3}{4}$ and that $(1 - \frac{1}{4})(1 - \frac{1}{9}) = \frac{4}{6}$.
   (b) Verify that $(1 - \frac{1}{4})(1 - \frac{1}{9})(1 - \frac{1}{16}) = \frac{5}{8}$ and that $(1 - \frac{1}{4})(1 - \frac{1}{9})(1 - \frac{1}{16})(1 - \frac{1}{25}) = \frac{6}{10}$.
   (c) For $n \in \mathbb{N}$ with $n \geq 2$, make a conjecture about a formula for the product $(1 - \frac{1}{4})(1 - \frac{1}{9})(1 - \frac{1}{16}) \cdots (1 - \frac{1}{n^2})$.

(d) Based on your work in Parts (4a) and (4b), state a. proposition and then use the Extended Principle of Mathematical Induction to prove your proposition.

5. Is the following proposition true or false? Justify your conclusion.
   For each nonnegative integer n, $8^n|(4n)!$:
6. Let $y = lnx$.

   (a) Determine $\frac{dy}{dx}$, $\frac{d^2y}{dx^2}$, $\frac{d^3y}{dx^3}$, and $\frac{d^4y}{dx^4}$.

   (b) Let n be a natural number. Formulate a conjecture for a formula for $\frac{d^ny}{dx^n}$. Then use mathematical induction to prove your conjecture.
7. For which natural numbers n do there exist nonnegative integers x and y such that $n = 4x + 5y$? Justify your conclusion.
8. Can each natural number greater than or equal to 4 be written as the sum of at least two natural numbers, each of which is a 2 or a 3? Justify your conclusion. For example, $7 = 2+2+3$, and $17 = 2+2+2+2+3+3+3$.
9. Can each natural number greater than or equal to 6 be written as the sum of at least two natural numbers, each of which is a 2 or a 5? Justify your conclusion. For example, $6 = 2+2+2$, $9 = 2+2+5$, and $17 = 2+5+5+5$.
10. Use mathematical induction to prove the following proposition:

    Let x be a real number with $x > 0$. Then for each natural number n with $n \geq 2$, $(1+x)^n > 1+nx$.

    Explain where the assumption that $x > 0$ was used in the proof.
11. Prove that for each odd natural number n with $n \geq 3$,

$$(1+\frac{1}{2})(1-\frac{1}{3})(1+\frac{1}{4})\cdots(1+\frac{(-1)^n}{n}) = 1. \tag{4.2.8}$$

12. Prove that for each natural number n,

    any set. with n elements has $\frac{n(n-1)}{2}$ two-element subsets.
13. Prove or disprove each of the following propositions:

    (a) For each $n \in \mathbb{N}$, $\frac{1}{1\cdot 2}.+\frac{1}{2\cdot 3}+\cdots+\frac{1}{n(n+1)} = \frac{n}{n+1}$.

    (b) For each natural number n with $n \geq 3$,

$$\frac{1}{3\cdot 4}+\frac{1}{4\cdot 5}+\cdots+\frac{1}{n(n+1)} = \frac{n-2}{3n+3} \tag{4.2.9}$$

    .

    (c) For each $n \in \mathbb{N}$, $1\cdot 2+2\cdot 3+3\cdot 4+\cdots+n(n+1) = \frac{n(n+1)(n+2)}{3}$.
14. Is the following proposition true or false? Justify your conclusion.

    For each natural number n, $(\frac{n^3}{3}+\frac{n^2}{2}+\frac{7n}{6})$ is a natural number.
15. Is the following proposition true or false? Justify your conclusion.

    For each natural number n, $(\frac{n^5}{5}+\frac{n^4}{2}+\frac{n^3}{3}-\frac{n}{30})$ is an integer.
16. (a) Prove that if $n \in \mathbb{N}$, then there exists an odd natural number m and a nonnegative integer k such that $n = 2^km$.
    (b) For each $n \in \mathbb{N}$, prove that there is only one way to write n in the form described in Part (a). To do this, assume that $n = 2^km$ and $n = 2^qp$ where m and p are odd natural numbers and k and q are nonnegative integers. Then prove that $k = q$ and $m = p$.
17. Evaluation of proofs
    See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

For each natural number n with $n \geq 2$, $2^n > 1+n$.

Proof

We let k be a natural number and assume that $2^k > 1+k$. Multiplying both sides of this inequality by 2, we see that $2^{k+1} > 2+2k$. However, $2+2k > 2+k$ and, hence,

$$2^{k+1} > 1+(k+1) \ .$$

By mathematical induction, we conclude that $2^n > 1+n$.

(b)

Each natural number greater than or equal to 6 can be written as the sum of natural numbers, each of which is a 2 or a 5.

Proof

We will use a proof by induction. For each natural number n, we let $P(n)$ be, "There exist nonnegative integers x and y such that $n = 2x+5y$." Since

$$\begin{aligned} 6 &= 3\cdot 2+0\cdot 5 \qquad & 7 &= 2+5 \\ 8 &= 4\cdot 2+0\cdot 5 \qquad & 9 &= 2\cdot 2+1\cdot 5 \end{aligned} \tag{4.2.10}$$

We see that $P(6)$, $P(7)$, $P(8)$, and $P(9)$ are true.

We now suppose that for some natural number k with $k \geq 10$ that $P(6)$, $P(7)$, ... $P(k)$ are true. Now

$$k+1 = (k-4)+5.$$

Since $k \geq 10$, we see that $k-4 \geq 6$ and, hence, $P(k-4)$ is true. So $k-4 = 2x+5y$ and, hence,

$$\begin{aligned} k+1 &= (2x+5y)+5 \\ &= 2x+5(y+1). \end{aligned} \tag{4.2.11}$$

This proves that $P(k+1)$ is true, and hence, by the Second Principle of Mathematical Induction, we have proved that for each natural number n with $n \geq 6$, there exist nonnegative integers x and y such that $n = 2x+5y$.

Explorations and Activities

18. **The Sum of the Angles of a Convex Quadrilateral.** There is a famous theorem in Euclidean geometry that states that the sum of the interior angles of a triangle is 180°.

    (a) Use the theorem about triangles to determine the sum of the angles of a convex quadrilateral. **Hint:** Draw a convex quadrilateral and draw a diagonal.
    (b) Use the result in Part (1) to determine the sum of the angles of a convex pentagon.
    (c) Use the result in Part (2) to determine the sum of the angles of a convex hexagon.
    (d) Let n be a natural number with $n \geq 3$. Make a conjecture about the sum of the angles of a convex polygon with n sides and use mathematical induction to prove your conjecture.
19. **De Moivre's Theorem**. One of the most interesting results in trigonometry is De Moivre's Theorem, which relates the complex number i to the trigonometric functions. Recall that the number i is the complex number whose square is 1, that is, $i^2 = -1$. One version of the theorem can be stated as follows:
    If x is a real number, then for each nonnegative integer n.

$$[cosx+i(sinx)]^n = cos(nx)+i(sin(nx)). \tag{4.2.12}$$

This theorem is named after Abraham de Moivre (1667 – 1754), a French mathematician.

(a) The proof of De Moivre's Theorem requires the use of the trigonometric identities for the sine and cosine of the sum of two angles. Use the Internet or a book to find identities for $sin(\alpha+\beta)$ and $cos(\alpha+\beta)$.
(b) To get a sense of how things work, expand $[cosx+i(sinx)]^2$ and write the result in the form $a+bi$. Then use the identities from part (1) to prove that $[cosx+i(sinx)]^2 = cos(2x)+i(sin(2x))$.

20. (c) Use mathematical induction to prove De Moivre's Theorem.

Answer

Add texts here. Do not delete this text first.

4.3: Induction and Recursion

Preview Activity 4.3.1: Recursively Defined Sequences

In a proof by mathematical induction, we "start with a first step" and then prove that we can always go from one step to the next step. We can use this same idea to define a sequence as well. We can think of a **sequence** as an infinite list of numbers that are indexed by the natural numbers (or some infinite subset of $\mathbb{N} \cup \{0\}$). We often write a sequence in the following form:

$$a_1, a_2, \ldots, a_n, \ldots$$

The number a_n is called the n^{th} term of the sequence. One way to define a sequence is to give a specific formula for the n^{th} term of the sequence such as $a_n = \frac{1}{n}$.

Another way to define a sequence is to give a specific definition of the first term (or the first few terms) and then state, in general terms, how to determine a_{n+1} in terms of n and the first n terms $a_1, a_2, \ldots, a_n$. This process is known as **definition by recursion** and is also called a **recursive definition**. The specific definition of the first term is called the **initial condition**, and the general definition of a_{n+1} in terms of n and the first n terms $a_1, a_2, \ldots, a_n$ is called the recurrence relation. (When more than one term is defined explicitly, we say that these are the initial conditions.) For example, we can define a sequence recursively as follows:

$b_1 = 16$, and for each $n \in \mathbb{N}$, $b_{n+1} = \frac{1}{2} b_n$.

Using $n = 1$ and then $n = 2$, we then see that

$$\begin{aligned} b_2 &= \frac{1}{2} b_1 & b_3 &= \frac{1}{2} b_2 \\ &= \frac{1}{2} \cdot 16 & &= \frac{1}{2} \cdot 8 \\ &= 8 & &= 4 \end{aligned} \tag{4.3.1}$$

1. Calculate b_4 through b_{10}. What seems to be happening to the values of b_n as n gets larger?
2. Define a sequence recursively as follows:

   $T_1 = 16$, and for each $n \in \mathbb{N}$, $T_{n+1} = 16 + \frac{1}{2} T_n$.

   Then $T_2 = 16 + \frac{1}{2} T_1 = 16 + 8 = 24$. Caluculate T_3 through T_{10}. What seems to be happening to the values of T_n as n gets larger?

The sequences in Parts (1) and (2) can be generalized as follows: Let a and r be real numbers. Define two sequences recursively as follows:

$a_1 = a$, and for each $n \in \mathbb{N}$, $a_{n+1} = r \cdot a_n$.

$S_1 = a$, and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$.

3. Determine formulas (in terms of a and r) for a_2 through a_6. What do you think an is equal to (in terms of a, r, and n)?
4. Determine formulas (in terms of a and r) for S_2 through S_6. What do you think an is equal to (in terms of a, r, and n)?

In Preview Activity 4.3.1 in Section 4.2, for each natural number n, we defined $n!$, read n **factorial**, as the product of the first n natural numbers. We also defined $0!$ to be equal to 1. Now recursively define a sequence of numbers a_0, a_1, a_2, ... as follows:

$a_0 = 1$, and
for each nonnegative integer n, $a_{n+1} = (n+1) \cdot a_n$.

Using $n = 0$, we see that this implies that $a_1 = 1 \cdot a_0 = 1 \cdot 1 = 1$, Then using $n = 1$, we see that

$$a_2 = 2a_1 = 2 \cdot 1 = 2. \tag{4.3.2}$$

5. Calculate a_3, a_4, a_5 and a_6.
6. Do you think that it is possible to calculate a_{20} and a_{100}? Explain.
7. Do you think it is possible to calculate a_n for any natural number n? Explain.
8. Compare the values of a_0, a_1, a_2, a_3, a_4, a_5, and a_6 with those of 0!, 1!, 2!, 3!, 4!, 5!, and 6!. What do you observe? We will use mathematical induction to prove a result about this sequence in Exercise (1).

Preview Activity 4.3.1: The Fibonacci Numbers

The Fibonacci numbers are a sequence of natural numbers f_1, f_2, f_3, ..., f_n, ... defined recursively as follows:

- $f_1 = 1$ and $f_2 = 1$, and
- For each natural number n, $f_{n+2} = f_{n+1} + f_n$.

In words, the recursion formula states that for any natural number n with $n \geq 3$, the n^{th} Fibonacci number is the sum of the two previous Fibonacci numbers. So we see that

$$\begin{aligned} f_3 &= f_2 + f_1 = 1 + 1 = 2, \\ f_4 &= f_3 + f_2 = 2 + 1 = 3, \text{ and} \\ f_5 &= f_4 + f_3 = 3 + 2 = 5, \end{aligned} \tag{4.3.3}$$

1. Calculate f_6 through f_{20}.
2. Which of the Fibonacci numbers f_1 through f_{20} are even? Which are multiples of 3?
3. For $n = 2$, $n = 3$, $n = 4$, and $n = 5$, how is the sum of the first $(n-1)$ Fibonacci numbers related to the $(n+1)^{st}$ Fibonacci number?
4. Record any other observations about the values of the Fibonacci numbers or any patterns that you observe in the sequence of Fibonacci numbers. If necessary, compute more Fibonacci numbers.

The Fibonacci Numbers

The Fibonacci numbers form a famous sequence in mathematics that was investigated by Leonardo of Pisa (1170 – 1250), who is better known as Fibonacci. Fibonacci introduced this sequence to the Western world as a solution of the following problem:

> *Suppose that a pair of adult rabbits (one male, one female) produces a pair of rabbits (one male, one female) each month. Also, suppose that newborn rabbits become adults in two months and produce another pair of rabbits. Starting with one adult pair of rabbits, how many pairs of rabbits will be produced each month for one year?*

Since we start with one adult pair, there will be one pair produced the first month, and since there is still only one adult pair, one pair will also be produced in the second month (since the new pair produced in the first month is not yet mature). In the third month, two pairs will be produced, one by the original pair and one by the pair which was produced in the first month. In the fourth month, three pairs will be produced, and in the fifth month, five pairs will be produced.

The basic rule is that in a given month after the first two months, the number of adult pairs is the number of adult pairs one month ago plus the number of pairs born two months ago. This is summarized in Table 4.1, where the number of pairs produced is equal to the number of adult pairs, and the number of adult pairs follows the Fibonacci sequence of numbers that we developed in Preview Activity 4.3.2.

Table 4.1: Fibonacci Numbers

Months	1	2	3	4	5	6	7	8	9	10
Adult Pairs	1	1	2	3	5	8	13	21	34	55
Newborn Pairs	1	1	2	3	5	8	13	21	34	55
Month-Old Pairs	0	1	1	2	3	5	8	13	21	34

Historically, it is interesting to note that Indian mathematicians were studying these types of numerical sequences well before Fibonacci. In particular, about fifty years before Fibonacci introduced his sequence, Acharya Hemachandra (1089 – 1173)

considered the following problem, which is from the biography of Hemachandra in the *MacTutor History of Mathematics Archive:*

> Suppose we assume that lines are composed of syllables which are either short or long. Suppose also that each long syllable takes twice as long to articulate as a short syllable. A line of length n contains n units where each short syllable is one unit and each long syllable is two units. Clearly a line of length n units takes the same time to articulate regardless of how it is composed. Hemchandra asks: How many different combinations of short and long syllables are possible in a line of length n?

This is an important problem in the Sanskrit language since Sanskrit meters are based on duration rather than on accent as in the English Language. The answer to this question generates a sequence similar to the Fibonacci sequence. Suppose that hn is the number of patterns of syllables of length n. We then see that $h_1 = 1$ and $h_2 = 2$. Now let n be a natural number and consider pattern of length $n+2$. This pattern either ends in a short syllable or a long syllable. If it ends in a short syllable and this syllable is removed, then there is a pattern of length $n+1$, and there are $h_n + 1$ such patterns. Similarly, if it ends in a long syllable and this syllable is removed, then there is a pattern of length n, and there are h_n such patterns. From this, we conclude that

$$h_{n+2} = h_{n+1} + h_n.$$

This actually generates the sequence 1, 2, 3, 5, 8, 13, 21, ... For more information about Hemachandra, see the article *Math for Poets and Drummers* by Rachel Wells Hall in the February 2008 issue of *Math Horizons*.

We will continue to use the Fibonacci sequence in this book. This sequence may not seem all that important or interesting. However, it turns out that this sequence occurs in nature frequently and has applications in computer science. There is even a scholarly journal, *The Fibonacci Quarterly*, devoted to the Fibonacci numbers.

The sequence of Fibonacci numbers is one of the most studied sequences in mathematics, due mainly to the many beautiful patterns it contains. Perhaps one observation you made in Preview Activity $4.3.2$ is that every third Fibonacci number is even. This can be written as a proposition as follows:

For each natural number n, f_{3n} is an even natural number.

As with many propositions associated with definitions by recursion, we can prove this using mathematical induction. The first step is to define the appropriate open sentence. For this, we can let $P(n)$ be, "f_{3n} is an even natural number."

Notice that $P(1)$ is true since $f_{3n} = 2$. We now need to prove the inductive step. To do this, we need to prove that for each $k \in \mathbb{N}$,

if $P(k)$ is true, then $P(k+1)$ is true.

That is, we need to prove that for each $k \in \mathbb{N}$, if f_{3k} is even, then $f_{3(k+1)}$ is even.

So let's analyze this conditional statement using a know-show table.

Step	Know	Reason
P	f_{3k} is even	Inductive hypothesis
$P1$	$(\exists m \in \mathbb{N})(f_{3k} = 2m)$	Definition of "even integer"
...	...	...
$Q1$	$(\exists q \in \mathbb{N})(f_{3(k+1)} = 2q)$	
Q	$f_{3(k+1)}$ is even.	Definition of "even integer"
Step	**Show**	**Reason**

The key question now is, "Is there any relation between $f_{3(k+1)}$ and f_k?" We can use the recursion formula that defines the Fibonacci sequence to find such a relation.

The recurrence relation for the Fibonacci sequence states that a Fibonacci number (except for the first two) is equal to the sum of the two previous Fibonacci numbers. If we write $3(k+1) = 3k+3$, then we get $f_{3(k+1)} = f_{3k+3}$. For f_{3k+3}, the two previous Fibonacci numbers are f_{3k+2} and f_{3k+1}. This means that

$$f_{3k+3} = f_{3k+2} + f_{3k+1}.$$

Using this and continuing to use the Fibonacci relation, we obtain the following:

$$\begin{aligned} f_{3(k+1)} &= f_{3k+3} \\ &= f_{3k+2} + f_{3k+1} \\ &= (f_{3k+1} + f_{3k}) + f_{3k+1}. \end{aligned} \tag{4.3.4}$$

The preceding equation states that $f_{3(k+1)} = 2f_{3k+1} + f_{3k}$. This equation can be used to complete the proof of the induction step.

? Progress Check 4.12 (Every Third Fibonacci Number Is Even)

Complete the proof of Proposition 4.13.

Proposition 4.13.

For each natural number n, the Fibonacci number f_{3n} is an even natural number.

Hint: We have already defined the predicate $P(n)$ to be used in an induction proof and have proved the basis step. Use the information in and after the preceding know-show table to help prove that if f_{3k} is even, then $f_{3(k+1)}$ is even.

Answer

Add texts here. Do not delete this text first.

Geometric Sequences and Geometric Series

Let $a,\ r \in \mathbb{R}$. The following sequence was introduced in Preview Activity 4.3.1.

$$\begin{aligned} \text{Initial condition} &: a_1 = a. \\ \text{Recurrence relation} &: \text{For each } n \in \mathbb{N},\ a_{n+1} = r \cdot a_n. \end{aligned} \tag{4.3.5}$$

This is a recursive definition for a **geometric sequence** with **initial term** a and (common) **ratio** r. The basic idea is that the next term in the sequence is obtained by multiplying the previous term by the ratio r. The work in Preview Activity 4.3.1 suggests that the following proposition is true.

Theorem 4.14

Let $a,\ r \in \mathbb{R}$, If a geometric sequence is defined by $a_1 = a$ and for each $n \in \mathbb{N}$, $a_{n+1} = r \cdot a_n$, then for each $n \in \mathbb{N}$, $a_n = a \cdot r^{n-1}$.

Proof

The proof of this proposition is Exercise (6).

Another sequence that was introduced in Preview Activity 4.3.1 is related to geometric series and is defined as follows:

$$\begin{aligned} \text{Initial condition} &: S_1 = a. \\ \text{Recurrence relation} &: \text{For each } n \in \mathbb{N},\ S_{n+1} = r \cdot S_n. \end{aligned} \tag{4.3.6}$$

For each $n \in \mathbb{N}$, the term S_n is a (finite) **geometric series** with **initial term** a and (common) **ratio** r. The work in Preview Activity 4.3.1 suggests that the following proposition is true.

Theorem 4.15

Let $a,\ r \in \mathbb{R}$. If the sequence $S_1, S_2, \ldots, S_n, \ldots$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a + a \cdot r + a \cdot r^2 + \cdots + a \cdot r^{n-1}$. That is, the geometric series S_n is the sum of the first n terms of the corresponding geometric sequence.

Proof

Add proof here and it will automatically be hidden if you have a "AutoNum" template active on the page.

The proof of Proposition 4.15 is Exercise (7). The recursive definition of a geometric series and Proposition 4.15 give two different ways to look at geometric series. Proposition 4.15 represents a geometric series as the sum of the first nterms of the corresponding geometric sequence. Another way to determine this sum a geometric series is given in Theorem 4.16, which gives a formula for the sum of a geometric series that does not use a summation.

Theorem 4.16

Let $a,\ r \in \mathbb{R}$ and $r \neq 1$. If the sequence $S_1, S_2, \ldots, S_n, \ldots$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a(\frac{1-r^n}{1-r})$.

Proof

The proof of Proposition 4.16 is Exercise (8).

Exercises for Section 4.3

1. For the sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$, assume that $a_0 = 1$ and that for each $n \in \mathbb{N} \cup \{0\}$, $a_{n+1} = (n+1)a_n$. Use mathematical induction to prove that for each $n \in \mathbb{N} \cup \{0\}$, $a_n = n!$.
2. Assume that $f_1, f_2, \ldots, f_n, \ldots$ are the Fibonacci numbers. Prove each of the following:

   (a) For each $n \in \mathbb{N}$, f_{4n} is a multiple of 3.
   (b) For each $n \in \mathbb{N}$, f_{5n} is a multiple of 5.
   (c) For each $n \in \mathbb{N}$, with $n \geq 2$, $f_1 + f_2 + \cdots + f_{n-1} = f_{n+1} - 1$.
   (d) For each $n \in \mathbb{N}$, $f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$.
   (e) For each $n \in \mathbb{N}$, $f_2 + f_4 + \cdots + f_{2n} = f_{2n+1} - 1$.
   (f) For each $n \in \mathbb{N}$, $f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1}$.
   (g) For each $n \in \mathbb{N}$ such that $n \not\equiv 0 \pmod 3$, f_n is an odd integer.
3. Use the result in Part (f) of Exercise (2) to prove that

$$\frac{f_1^2 + f_2^2 + \cdots + f_n^2 + f_{n+1}^2}{f_1^2 + f_2^2 + \cdots + f_n^2} = 1 + \frac{f_{n+1}}{f_n} \tag{4.3.7}$$

4. The quadratic formula can be used to show that $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$ are the two real number solutions of the quadratic equation $x^2 - x - 1 = 0$. Notice that this implies that

$$\begin{aligned} \alpha^2 &= \alpha + 1, \text{ and} \\ \beta^2 &= \beta + 1. \end{aligned} \tag{4.3.8}$$

   It may be surprising to find out that these two irrational numbers are closely related to the Fibonacci numbers.

   (a) Verify that $f_1 = \frac{\alpha^1 - \beta^1}{\alpha - \beta}$ and that $f_2 = \frac{\alpha^2 - \beta^2}{\alpha - \beta}$
   (b) (This part is optional, but it may help with the induction proof in part (c).) Work with the relation $f_3 = f_2 + f_1$ and substitute the expressions for f_1 and f_2 from part (a). Rewrite the expression as a single fraction and then in the numerator use $\alpha^2 + \alpha = \alpha(\alpha + 1)$ and a similar equation involving β. Now prove that $f_3 = \frac{\alpha^3 - \beta^3}{\alpha - \beta}$.
   (c) Use induction to prove that for each natural number n, if $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$, then $f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$. **Note**: This formula for the n^{th} Fibonacci number is known as Binet's formula, named after the French mathematician Jacques Binet (1786 - 1856).
5. Is the following conjecture true or false? Justify your conclusion.

   Conjecture. Let $f_1, f_2, \ldots, f_m, \ldots$ be the sequence of the Fibonacci numbers. For each natural number n, the numbers

$f_n f_{n+3}$, $2f_{n+1}f_{n+2}$, and $(f_{n+1}^2 + f_{n+2}^2)$ form a Pythagorean triple.

6. Prove Proposition 4.14. Let $a,\ r \in \mathbb{R}$, If a geometric sequence is defined by $a_1 = a$ and for each $n \in \mathbb{N}$, $a_{n+1} = r \cdot a_n$, then for each $n \in \mathbb{N}$, $a_n = a \cdot r^{n-1}$.
7. Prove Proposition 4.15. Let $a,\ r \in \mathbb{R}$. If the sequence $S_1, S_2, \ldots, S_n, \ldots$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a + a \cdot r + a \cdot r^2 + \cdots + a \cdot r^{n-1}$. That is, the geometric series S_n is the sum of the first n terms of the corresponding geometric sequence.
8. Prove Proposition 4.16. Let $a,\ r \in \mathbb{R}$ and $r \neq 1$. If the sequence $S_1, S_2, \ldots, S_n, \ldots$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a(\dfrac{1-r^n}{1-r})$.
9. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 2$ and that for each $n \in \mathbb{N}$, $a_{n+1} = a_n + 5$.

   (a) Calculate a_2 through a_6.
   (b) Make a conjecture for a formula for a_n for each n for each $n \in \mathbb{N}$.
   (c) Prove that your conjecture in Exercise (9b) is correct.
10. The sequence in Exercise (9) is an example of an **arithmetic sequence.** An arithmetic sequence is defined recursively as follows:

    Let c and d be real numbers. Define the sequence $a_1, a_2, \ldots, a_n, \ldots$ by $a_1 = c$ and for each $n \in \mathbb{N}$, $a_{n+1} = a_n + d$.

    (a) Determine formulas for a_3 through a_8.
    (b) Make a conjecture for a formula for a_n for each n for each $n \in \mathbb{N}$.
    (c) Prove that your conjecture in Exercise (10b) is correct.
11. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 5$, and that for each $n \in \mathbb{N}$, $a_{n+1} = a_n + 2a_{n-1}$. Prove that for each natural number n, $a_n = 2^n + (-1)^n$.
12. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$ and that for each $n \in \mathbb{N}$, $a_{n+1} = \sqrt{5 + a_n}$.

    (a) Calculate, or approximate, a_2 through a_6.
    (b) Prove that for each $n \in \mathbb{N}$, $a_n < 3$.
13. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 3$, and that for each $n \in \mathbb{N}$, $a_{n+2} = 3a_{n+1} - 2a_n$.

    (a) Calculate a_3 through a_6.
    (b) Make a conjecture for a formula for a_n for each n for each $n \in \mathbb{N}$.
    (c) Prove that your conjecture in Exercise (13b) is correct.
14. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 1$, and that for each $n \in \mathbb{N}$, $a_{n+2} = \dfrac{1}{2}(a_{n+1} + \dfrac{2}{a_n})$.

    (a) Calculate a_3 through a_6.
    (b) Prove that for each $n \in \mathbb{N}$, $1 \leq a_n \leq 2$.
15. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, and for that each natural number n,

$$a_{n+3} = a_{n+2} + a_{n+1} + a_n. \tag{4.3.9}$$

    (a) Compute a_4, a_5, a_6, and a_7.
    (b) Prove that for each natural number n with $n > 1$, $a_n \leq 2^{n-2}$.
16. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, and for each natural number n,

$$a_{n+1} = a_n + n \cdot n!. \tag{4.3.10}$$

    (a) Compute $n!$ for the first 10 natural numbers.
    (b) Compute a_n for the first 10 natural numbers.
    (c) Make a conjecture about a formula for a_n in terms of n that does not involve a summation or a recursion.
    (d) Prove your conjecture in Part (c).

17. For the sequence $a_1, a_2, \ldots, a_n, \ldots$, assume that $a_1 = 1$, $a_2 = 1$, and for each $n \in \mathbb{N}$, $a_{n+2} = a_{n+1} + 3a_n$. Determine which terms in this sequence are divisible by 4 and prove that your answer is correct.
18. The Lucas numbers are a sequence of natural numbers $L_1, L_2, L_3, \ldots, L_n, \ldots$, which are defined recursively as follows:

    bullet $L_1 = 1$ and $L_2 = 3$, and
    bullet For each natural number n, $L_{n+2} = L_{n+1} + L_n$.

    List the first 10 Lucas numbers and the first ten Fibonacci numbers and then prove each of the following propositions. The Second Principle of Mathematical Induction may be needed to prove some of these propositions.

    (a) For each natural number n, $L_n = 2f_{n+1} - f_n$.
    (b) For each $n \in \mathbb{N}$ with $n \geq 2$, $5f_n = L_{n-1} + L_{n+1}$.
    (c) For each $n \in \mathbb{N}$ with $n \geq 3$, $L_n = f_{n+1} - f_{n-2}$.
19. There is a formula for the Lucas number similar to the formula for the Fibonacci numbers in Exercise (4). Let $\alpha = \dfrac{1+\sqrt{5}}{2}$ and $\beta = \dfrac{1-\sqrt{5}}{2}$. Prove that for each $n \in \mathbb{N}$, $L_n = \alpha^n + \beta^n$.
20. Use the result in Exercise (19), previously proven results from Exercise (18), or mathematical induction to prove each of the following results about Lucas numbers and Fibonacci numbers.

    (a) For each $n \in \mathbb{N}$, $L_n = \dfrac{f_{2n}}{f_n}$
    (b) For each $n \in \mathbb{N}$, $f_{n+1} = \dfrac{f_n + L_n}{2}$.
    (c) For each $n \in \mathbb{N}$, $L_{n+1} = \dfrac{L_n + 5f_n}{2}$.
    (d) For each $n \in \mathbb{N}$ with $n \geq 2$, $L_n = f_{n+1} + f_{n-1}$.
21. **Evaluation of proofs**
    See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

Let f_n be the nth Fibonacci number, and let α be the positive solution of the equation $x^2 = x + 1$. So $\alpha = \dfrac{1+\sqrt{5}}{2}$. For each natural number n, $f_n \leq \alpha^{n-1}$.

Proof

We will use a proof by mathematical induction. For each natural number n, we let $P(n)$ be, "$f_n \leq \alpha^{n-1}$."

We first note that $P(1)$ is true since $f_1 = 1$ and$\alpha^0 = 1$. We also notice that $P(2)$ is true since $f_2 = 1$ and, hence, $f_2 \leq \alpha^1$.

We now let k be a natural number with $k \geq 2$ and assume that $P(1)$, $P(2)$, ..., $P(k)$ are all true. We now need to prove that $P(k+1)$ is true or that $f_{k+1} \leq \alpha^k$.

Since $P(k-1)$ and $P(k)$ are true, we know that $f_{k-1} \leq \alpha^{k-2}$ and $f_k \leq \alpha^{k-1}$. Therefore,

\[\begin{array} {rcl} {f_{k + 1}} &= & {f_k + f_{k - 1}} \\ {f_{k + 1}} &\le & {\alpha ^{k - 1} + {\alpha ^{k - 2}} \\ {f_{k + 1}} &\le & {\alpha ^{k - 2} (\alpha + 1).} \end{array}\]

We now use the fact that $\alpha + 1 = \alpha^2$ and the preceding inequality to obtain

$$\begin{aligned} f_{k+1} &\leq \alpha^{k-2}\alpha^2 \\ f_{k+1} &\leq \alpha^k. \end{aligned} \tag{4.3.11}$$

This proves that if $P(1)$, $P(2)$, ..., $P(k)$ are true, then $P(k+1)$ is true. Hence, by the Second Principle of Mathematical Induction, we conclude that or each natural number n, $f_n \leq \alpha^{n-1}$.

Explorations and Activities

22. **Compound Interest.** Assume that R dollars is deposited in an account that has an interest rate of i for each compounding period. A compounding period is some specified time period such as a month or a year.
For each integer n with $n \leq 0$, let Vn be the amount of money in an account at the end of the nth compounding period. Then

$$\begin{aligned} V_1 &= R + i \cdot R \\ &= R(1+i) \end{aligned} \qquad \begin{aligned} V_2 &= V_1 + i \cdot V_1 \\ &= (1+i)V_1 \\ &= (1+i)^2 R. \end{aligned} \tag{4.3.12}$$

(a) Explain why $V_3 = V_2 + i \cdot V_2$. Then use the formula for V2 to determine a formula for V_3 in terms of i and R.
(b) Determine a recurrence relation for V_{n+1} in terms of i and V_n.
(c) Write the recurrence relation in Part (22b) so that it is in the form of a recurrence relation for a geometric sequence. What is the initial term of the geometric sequence and what is the common ratio?
(d) Use Proposition 4.14 to determine a formula for V_n in terms of I, R, and n.

23. **The Future Value of an Ordinary Annuity.** For an **ordinary annuity**, R dollars is deposited in an account at the end of each compounding period. It is assumed that the interest rate, i, per compounding period for the account remains constant.

Let S_t represent the amount in the account at the end of the tth compounding period. S_t is frequently called the future value of the ordinary annuity.

So $S_1 = R$. To determine the amount after two months, we first note that the amount after one month will gain interest and grow to $(1+i)S_1$. In addition, a new deposit of R dollars will be made at the end of the second month. So

$$S_2 = R + (1+i)S_1 \tag{4.3.13}$$

(a) For each $n \in \mathbb{N}$, use a similar argument to determine a recurrence relation for S_{n+1} in terms of R, i, and S_n.
(b) By recognizing this as a recursion formula for a geometric series, use Proposition 4.16 to determine a formula for S_n in terms of R, i, and n that does not use a summation. Then show that this formula can be written as

$$S_n = R\left(\frac{(1+i)^n - 1}{i}\right). \tag{4.3.14}$$

(c) What is the future value of an ordinary annuity in 20 years if $200 dollars is deposited in an account at the end of each month where the interest rate for the account is 6% per year compounded monthly? What is the amount of interest that has accumulated in this account during the 20 years?

Answer

Add texts here. Do not delete this text first.

4.S: Mathematical Induction (Summary)

Important Definitions

- Inductive set, page 171
- Factorial, page 201
- Recursive definition, page 200
- Fibonacci numbers, page 202
- Geometric sequence, page 206
- Geometric series, page 206

The Various Forms of Mathematical Induction

1. **The Principle of Mathematical Induction**
   If T is a subset of $\mathbb{N}$ such that

   (a) $1 \in T$, and
   (b) For every $k \in \mathbb{N}$, if $k \in T$, then $(k+1) \in T$.

   then $T = \mathbb{N}$
   Procedure for a Proof by Mathematical Induction
   To prove $(\forall n \in \mathbb{N}$(P(n))\)

$$\begin{aligned} \text{Basis step} &: \text{Prove} P(1). \\ \text{Inductive step} &: \text{Prove that for each} k \in \mathbb{N}, \text{if} P(k) \text{is true, then} P(k+1) \text{is true.} \end{aligned} \tag{4.S.1}$$

2. **The Extended Principle of Mathematical Induction**
   Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

   (a) $M \in T$, and
   (b) For every $k \in \mathbb{Z}$ with $k \geq M$, if $k \in T$, then $(k+1) \in T$.

   then T contains all integers greater than or equal to M.
   Using the Extended Principle of Mathematical Induction
   Let M be an intteger. To prove $(\forall n \in \mathbb{Z} \text{with} n \geq M)(P(n))$

$$\begin{aligned} \text{Basis step} &: \text{Prove} P(M). \\ \text{Inductive step} &: \text{Prove that for each} k \in \mathbb{Z} \text{with} k \geq M, \text{if} P(k) \text{is true, then} P(k+1) \text{is true.} \end{aligned} \tag{4.S.2}$$

   We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq M$.
3. The Second Principle of Mathematical Induction
   Let M be an integer. If T is a subset of $\mathbb{Z}$ such that

   (a) $M \in T$, and
   (b) For every $k \in \mathbb{Z}$ with $k \geq M$, if $\{M, M+1, \ldots, k\} \subseteq T$, then $(k+1) \in T$.

   then T contains all integers greater than or equal to M.
   Using the Second Principle of Mathematical Induction
   Let M be an intteger. To prove $(\forall n \in \mathbb{Z} \text{with} n \geq M)(P(n))$

$$\begin{aligned} \text{Basis step} &: \text{Prove} P(M). \\ \text{Inductive step} &: \text{Let} k \in \mathbb{Z} \text{with} k \geq M. \text{ Prove that if} P(M), P(M+1), \ldots, P(k) \text{are true, then} P(k+1) \text{is true.} \end{aligned} \tag{4.S.3}$$

   We can then conclude that $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq M$.

Important Results

- **Theorem 4.9.** *Each natural number greater than 1 is either a prime number or is a product of prime numbers.*
- **Theorem 4.14**. Let $a, r \in \mathbb{R}$. If a geometric sequence is defined by $a_1 = a$ and for each $n \in \mathbb{N}$, $a_{n+1} = r \cdot a_n$, then for each $n \in \mathbb{N}$, $a_n = a \cdot r^{n-1}$.

- **Theorem 4.15.** Let $a, r \in \mathbb{R}$. If the sequence $S_1, S_2, \ldots, S_n, \ldots$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a + a \cdot r + a \cdot r^2 + \cdots + a \cdot r^{n-1}$. That is, the geometric series S_n is the sum of the first n terms of the corresponding geometric sequence.
- **Theorem 4.16.** Let $a, r \in \mathbb{R}$ and $r \neq 1$. If the sequence $S_1, S_2, \ldots, S_n, \ldots$ is defined by $S_1 = a$ and for each $n \in \mathbb{N}$, $S_{n+1} = a + r \cdot S_n$, then for each $n \in \mathbb{N}$, $S_n = a(\frac{1-r^n}{1-r})$.

Supplementary Notes: Sequences, Definitions

Investigate!

What comes next:

$$1,\ 11,\ 21,\ 1211,\ 111221,\ 312211,\ \ldots$$

A *sequence* is simply an ordered list of numbers. For example, here is a sequence: 0, 1, 2, 3, 4, 5, …. This is different from the set $\mathbb{N}$ because, while the sequence is a complete list of every element in the set of natural numbers, in the sequence we very much care what order the numbers come in. For this reason, when we use variables to represent terms in a sequence they will look like this:

$$a_0, a_1, a_2, a_3, \ldots$$

To refer to the *entire* sequence at once, we will write $(a_n)_{n\in\mathbb{N}}$ or $(a_n)_{n\geq 0}$, or sometimes if we are being sloppy, just (a_n) (in which case we assume we start the sequence with a_0).

We might replace the a with another letter, and sometimes we omit a_0, starting with a_1, in which case we would use $(a_n)_{n\geq 1}$ to refer to the sequence as a whole. The numbers in the subscripts are called *indices* (the plural of *index*).

While we often just think of sequences as an ordered list of numbers, they really are a type of function. Specifically, the sequence $(a_n)_{n\geq 0}$ is a function with domain $\mathbb{N}$ where a_n is the image of the natural number n. Later we will manipulate sequences in much the same way you have manipulated functions in algebra or calculus. We can shift a sequence up or down, add two sequences, or ask for the rate of change of a sequence. These are done exactly as you would for functions.

That said, while keeping the rigorous mathematical definition in mind is helpful, we often describe sequences by writing out the first few terms.

Example $SupplementaryNotes.1$

Can you find the next term in the following sequences?

1. $7, 7, 7, 7, 7, \ldots$
2. $3, -3, 3, -3, 3, \ldots$
3. $1, 5, 2, 10, 3, 15, \ldots$
4. $1, 2, 4, 8, 16, 32, \ldots$
5. $1, 4, 9, 16, 25, 36, \ldots$
6. $1, 2, 3, 5, 8, 13, 21, \ldots$
7. $1, 3, 6, 10, 15, 21, \ldots$
8. $2, 3, 5, 7, 11, 13, \ldots$
9. $3, 2, 1, 0, -1, \ldots$
10. $1, 1, 2, 6, \ldots$

Solution

No you cannot. You might guess that the next terms are:

1. 7
2. -3
3. 4
4. 64
5. 49
6. 34
7. 28
8. 17
9. -2
10. 24

In fact, those are the next terms of the sequences I had in mind when I made up the example, but there is no way to be sure they are correct.

Still, we will often do this. Given the first few terms of a sequence, we can ask what the pattern in the sequence suggests the next terms are.

Given that no number of initial terms in a sequence is enough to say for certain which sequence we are dealing with, we need to find another way to specify a sequence. We consider two ways to do this:

Closed formula

A *closed formula* for a sequence $(a_n)_{n\in\mathbb{N}}$ is a formula for a_n using a fixed finite number of operations on n. This is what you normally think of as a formula in n, just like if you were defining a function in terms of n (because that is exactly what you are doing).

Recursive definition

A *recursive definition* (sometimes called an *inductive definition*) for a sequence $(a_n)_{n\in\mathbb{N}}$ consists of a *recurrence relation*: an equation relating a term of the sequence to previous terms (terms with smaller index) and an *initial condition*: a list of a few terms of the sequence (one less than the number of terms in the recurrence relation).

It is easier to understand what is going on here with an example:

Example $SupplementaryNotes.2$

Here are a few closed formulas for sequences:

- $a_n = n^2$.
- $a_n = \dfrac{n(n+1)}{2}$.
- $a_n = \dfrac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1+\sqrt{5}}{2}\right)^{-n}}{5}$.

Note in each case, if you are given n, you can calculate a_n directly: just plug in n. For example, to find a_3 in the second sequence, just compute $a_3 = \frac{3(3+1)}{2} = 6$.

Here are a few recursive definitions for sequences:

- $a_n = 2a_{n-1}$ with $a_0 = 1$.
- $a_n = 2a_{n-1}$ with $a_0 = 27$.
- $a_n = a_{n-1} + a_{n-2}$ with $a_0 = 0$ and $a_1 = 1$.

In these cases, if you are given n, you cannot calculate a_n directly, you first need to find a_{n-1} (or a_{n-1} and a_{n-2}). In the second sequence, to find a_3 you would take $2a_2$, but to find $a_2 = 2a_1$ we would need to know $a_1 = 2a_0$. We do know this, so we could trace back through these equations to find $a_1 = 54$, $a_2 = 108$ and finally $a_3 = 216$.

Investigate!

You have a large collection of 1×1 squares and 1×2 dominoes. You want to arrange these to make a 1×15 strip. How many ways can you do this?

1. Start by collecting data. How many length 1×1 strips can you make? How many 1×2 strips? How many 1×3 strips? And so on.
2. How are the 1×3 and 1×4 strips related to the 1×5 strips?
3. How many 1×15 strips can you make?
4. What if I asked you to find the number of 1×1000 strips? Would the method you used to calculate the number fo 1×15 strips be helpful?

You might wonder why we would bother with recursive definitions for sequences. After all, it is harder to find a_n with a recursive definition than with a closed formula. This is true, but it is also harder to find a closed formula for a sequence than it is to find a recursive definition. So to find a useful closed formula, we might first find the recursive definition, then use that to find the closed formula.

This is not to say that recursive definitions aren't useful in finding a_n. You can always calculate a_n given a recursive definition, it might just take a while.

Example $SupplementaryNotes.3$

Find a_6 in the sequence defined by $a_n = 2a_{n-1} - a_{n-2}$ with $a_0 = 3$ and $a_1 = 4$.

Solution

We know that $a_6 = 2a_5 - a_4$. So to find a_6 we need to find a_5 and a_4. Well

$$a_5 = 2a_4 - a_3 \qquad \text{and} \qquad a_4 = 2a_3 - a_2,$$

so if we can only find a_3 and a_2 we would be set. Of course

$$a_3 = 2a_2 - a_1 \qquad \text{and} \qquad a_2 = 2a_1 - a_0,$$

so we only need to find a_1 and a_0. But we are given these. Thus

$$\begin{aligned} a_0 &= 3 \\ a_1 &= 4 \\ a_2 &= 2\cdot 4 - 3 = 5 \\ a_3 &= 2\cdot 5 - 4 = 6 \\ a_4 &= 2\cdot 6 - 5 = 7 \\ a_5 &= 2\cdot 7 - 6 = 8 \\ a_6 &= 2\cdot 8 - 7 = 9. \end{aligned}$$

Note that now we can guess a closed formula for the nth term of the sequence: $a_n = n+3$. To be sure this will always work, we could plug in this formula into the recurrence relation:

$$\begin{aligned} 2a_{n-1} - a_{n-2} &= 2((n-1)+3) - ((n-2)+3) \\ &= 2n + 4 - n - 1 \\ &= n + 3 \\ &= a_n. \end{aligned}$$

That is not quite enough though, since there can be multiple closed formulas that satisfy the same recurrence relation; we must also check that our closed formula agrees on the initial terms of the sequence. Since $a_0 = 0 + 3 = 3$ and $a_1 = 1 + 3 = 4$ are the correct initial conditions, we can now conclude we have the correct closed formula.

Finding closed formulas, or even recursive definitions, for sequences is not trivial. There is no one method for doing this. Just like in evaluating integrals or solving differential equations, it is useful to have a bag of tricks you can apply, but sometimes there is no easy answer.

One useful method is to relate a given sequence to another sequence for which we already know the closed formula.

Example $SupplementaryNotes.4$

Use the formulas $T_n = \frac{n(n+1)}{2}$ and $a_n = 2^n$ to find closed formulas for the following sequences.

1. (b_n): $1, 2, 4, 7, 11, 16, 22, \ldots$.
2. (c_n): $3, 5, 9, 17, 33, \ldots$.
3. (d_n): $0, 2, 6, 12, 20, 30, 42, \ldots$.
4. (e_n): $3, 6, 10, 15, 21, 28, \ldots$.
5. (f_n): $0, 1, 3, 7, 15, 31, \ldots$.

6. (g_n) $3, 6, 12, 24, 48, \ldots$.
7. (h_n): $6, 10, 18, 34, 66, \ldots$.
8. (j_n): $15, 33, 57, 87, 123, \ldots$.

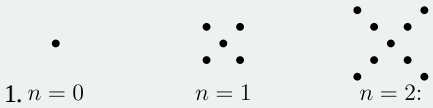
Solution

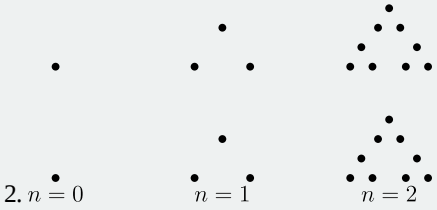
1. Before you say this is impossible, what we are asking for is simply to find a closed formula which agrees with all of the initial terms of the sequences. Of course there is no way to read into the mind of the person who wrote the numbers down, but we can at least do this.
2. The first few terms of $(T_n)_{n\geq 0}$ are $0, 1, 3, 6, 10, 15, 21, \ldots$ (these are called the *triangular numbers*). The first few terms of $(a_n)_{n\geq 0}$ are $1, 2, 4, 8, 16, \ldots$. Let's try to find formulas for the given sequences:
3. $(1, 2, 4, 7, 11, 16, 22, \ldots)$. Note that if subtract 1 from each term, we get the sequence (T_n). So we have $b_n = T_n + 1$. Therefore a closed formula is $b_n = \frac{n(n+1)}{2} + 1$. A quick check of the first few n confirms we have it right.
4. $(3, 5, 9, 17, 33, \ldots)$. Each term in this sequence is one more than a power of 2, so we might guess the closed formula is $c_n = a_n + 1 = 2^n + 1$. If we try this though, we get $c_0 2^0 + 1 = 2$ and $c_1 = 2^1 + 1 = 3$. We are off because the indices are shifted. What we really want is $c_n = a_{n+1} + 1$ giving $c_n = 2^{n+1} + 1$.
5. $(0, 2, 6, 12, 20, 30, 42, \ldots)$. Notice that all these terms are even. What happens if we factor out a 2? We get (T_n)! More precisely, we find that $d_n/2 = T_n$, so this sequence has closed formula $d_n = n(n+1)$.
6. $(3, 6, 10, 15, 21, 28, \ldots)$. These are all triangular numbers. However, we are starting with 3 as our initial term instead of as our third term. So if we could plug in 2 instead of 0 into the formula for T_n, we would be set. Therefore the closed formula is $e_n = \frac{(n+2)(n+3)}{2}$ (where $n+3$ came from $(n+2)+1$). Thinking about sequences as functions, we are doing a horizontal shift by 2: $e_n = T_{n+2}$ which would cause the graph to shift 2 units to the left.
7. $(0, 1, 3, 7, 15, 31, \ldots)$. Try adding 1 to each term and we get powers of 2. You might guess this because each term is a little more than twice the previous term (the powers of 2 are *exactly* twice the previous term). Closed formula: $f_n = 2^n - 1$.
8. $(3, 6, 12, 24, 48, \ldots)$. These numbers are also doubling each time, but are also all multiples of 3. Dividing each by 3 gives 1, 2, 4, 8, …. Aha. We get the closed formula $g_n = 3 \cdot 2^n$.
9. $(6, 10, 18, 34, 66, \ldots)$. To get from one term to the next, we almost double each term. So maybe we can relate this back to 2^n. Yes, each term is 2 more than a power of 2. So we get $h_n = 2^{n+2} + 2$ (the $n+2$ is because the first term is 2 more than 2^2, not 2^0). Alternatively, we could have related this sequence to the second sequence in this example: starting with 3, 5, 9, 17, … we see that this sequence is twice the terms from that sequence. That sequence had closed formula $c_n = 2^{n+1} + 1$. Our sequence here would be twice this, so $h_n = 2(2^n + 1)$, which is the same as we got before.
10. $(15, 33, 57, 87, 123, \ldots)$. Try dividing each term by 3. That gives the sequence $5, 11, 19, 29, 41, \ldots$. Now add 1: $6, 12, 20, 30, 42, \ldots$, which is (d_n) in this example, except starting with 6 instead of 0. So let's start with the formula $d_n = n(n+1)$. To start with the 6, we shift: $(n+2)(n+3)$. But this is one too many, so subtract 1: $(n+2)(n+3) - 1$. That gives us our sequence, but divided by 3. So we want $j_n = 3((n+2)(n+3) - 1)$.

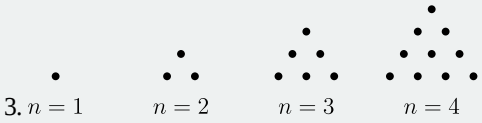
Supplementary Notes: Sequences, Arithmetic and Geometric

Investigate!

For the patterns of dots below, draw the next pattern in the sequence. Then give a recursive definition and a closed formula for the number of dots in the nth pattern.

1. 

2. 

3. 

We now turn to the question of finding closed formulas for particular types of sequences.

Arithmetic Sequences

If the terms of a sequence differ by a constant, we say the sequence is *arithmetic*. If the initial term (a_0) of the sequence is a and the *common difference* is d, then we have,

Recursive definition: $a_n = a_{n-1} + d$ with $a_0 = a$.

Closed formula: $a_n = a + dn$.

How do we know this? For the recursive definition, we need to specify a_0. Then we need to express a_n in terms of a_{n-1}. If we call the first term a, then $a_0 = a$. For the recurrence relation, by the definition of an arithmetic sequence, the difference between successive terms is some constant, say d. So $a_n - a_{n-1} = d$, or in other words,

$$a_0 = a \qquad a_n = a_{n-1} + d.$$

To find a closed formula, first write out the sequence in general:

$$\begin{aligned} a_0 &= a \\ a_1 &= a_0 + d = a + d \\ a_2 &= a_1 + d = a + d + d = a + 2d \\ a_3 &= a_2 + d = a + 2d + d = a + 3d \\ &\vdots \end{aligned}$$

We see that to find the nth term, we need to start with a and then add d a bunch of times. In fact, add it n times. Thus $a_n = a + dn$.

Example $SupplementaryNotes.1$

Find recursive definitions and closed formulas for the sequences below. Assume the first term listed is a_0.

1. $2, 5, 8, 11, 14, \ldots$.
2. $50, 43, 36, 29, \ldots$.

Solution

First we should check that these sequences really are arithmetic by taking differences of successive terms. Doing so will reveal the common difference d.

1. $5-2=3,\ 8-5=3,$ etc. To get from each term to the next, we add three, so $d=3$. The recursive definition is therefore $a_n=a_{n-1}+3$ with $a_0=2$. The closed formula is $a_n=2+3n$.
2. Here the common difference is -7, since we add -7 to 50 to get 43, and so on. Thus we have a recursive definition of $a_n=a_{n-1}-7$ with $a_0=50$. The closed formula is $a_n=50-7n$.

What about sequences like \(2, 6, 18, 54, \ldots\text{?}\) This is not arithmetic because the difference between terms is not constant. However, the *ratio* between successive terms is constant. We call such sequences *geometric*.

The recursive definition for the geometric sequence with initial term a and common ratio r is $a_n=a_n\cdot r; a_0=a$. To get the next term we multiply the previous term by r. We can find the closed formula like we did for the arithmetic progression. Write

$$\begin{aligned} a_0 &= a \\ a_1 &= a_0\cdot r \\ a_2 &= a_1\cdot r=a_0\cdot r\cdot r=a_0\cdot r^2 \\ &\vdots \end{aligned}$$

We must multiply the first term a by r a number of times, n times to be precise. We get $a_n=a\cdot r^n$.

Geometric Sequences

A sequence is called *geometric* if the ratio between successive terms is constant. Suppose the initial term a_0 is a and the *common ratio* is r. Then we have,

- Recursive definition: $a_n=ra_{n-1}$ with $a_0=a$.
- Closed formula: $a_n=a\cdot r^n$.

Example $SupplementaryNotes.3$

Find the recursive and closed formula for the sequences below. Again, the first term listed is a_0.

1. $3,6,12,24,48,\ldots$
2. $27,9,3,1,1/3,\ldots$

Solution

Again, we should first check that these sequences really are geometric, this time by dividing each term by its previous term. Assuming this ratio is constant, we will have found r.

1. $6/3=2, 12/6=2, 24/12=2$,etc. Yes, to get from any term to the next, we multiply by $r=2$. So the recursive definition is $a_n=2a_{n-1}$ with $a_0=3$. The closed formula is $a_n=3\cdot 2^n$.
2. The common ratio is $r=1/3$. So the sequence has recursive definition $a_n=\frac{1}{3}a_{n-1}$ with $a_0=27$ and closed formula $a_n=27\cdot\frac{1}{3}^n$.

In the examples and formulas above, we assumed that the *initial* term was a_0. If your sequence starts with a_1, you can easily find the term that would have been a_0 and use that in the formula. For example, if we want a formula for the sequence \(2, 5, 8,\ldots\) and insist that $2=a_1$, then we can find $a_0=-1$ (since the sequence is arithmetic with common difference 3, we have $a_0+3=a_1$). Then the closed formula will be $a_n=-1+3n$.

If you look at other textbooks or online, you might find that their closed formulas for arithmetic and geometric sequences differ from ours. Specifically, you might find the formulas $a_n=a+(n-1)d$ (arithmetic) and $a_n=a\cdot r^{n-1}$ (geometric). Which is correct? Both! In our case, we take a to be a_0. If instead we had a_1 as our initial term, we would get the (slightly more complicated) formulas you find elsewhere.

Sums of Arithmetic and Geometric Sequences

Investigate!

Your neighborhood grocery store has a candy machine full of Skittles.

1. Suppose that the candy machine currently holds exactly 650 Skittles, and every time someone inserts a quarter, exactly 7 Skittles come out of the machine.
   a. How many Skittles will be left in the machine after 20 quarters have been inserted?
   b. Will there ever be exactly zero Skittles left in the machine? Explain.
2. What if the candy machine gives 7 Skittles to the first customer who put in a quarter, 10 to the second, 13 to the third, 16 to the fourth, etc. How many Skittles has the machine given out after 20 quarters are put into the machine?
3. Now, what if the machine gives 4 Skittles to the first customer, 7 to the second, 12 to the third, 19 to the fourth, etc. How many Skittles has the machine given out after 20 quarters are put into the machine?

Look at the sequence $(T_n)_{n\geq 1}$ which starts $1, 3, 6, 10, 15, \ldots$.These are called the *triangular numbers* since they represent the number of dots in an equilateral triangle (think of how you arrange 10 bowling pins: a row of 4 plus a row of 3 plus a row of 2 and a row of 1).

Is this sequence arithmetic? No, since $3-1=2$ and $6-3=3\neq 2,$ so there is no common difference. Is the sequence geometric? No. $3/1=3$ but $6/3=2$, so there is no common ratio. What to do?

Notice that the differences between terms form an arithmetic sequence: $2, 3, 4, 5, 6, \ldots$.This says that the nth term of the sequence $1, 3, 6, 10, 15, \ldots$is the *sum* of the first n terms in the sequence $1, 2, 3, 4, 5, \ldots$.We say that the first sequence is the *sequence of partial sums* of the second sequence (partial sums because we are not taking the sum of all infinitely many terms). If we know how to add up the terms of an arithmetic sequence, we could use this to find a closed formula for a sequence whose differences are the terms of that arithmetic sequence.

This should become clearer if we write the triangular numbers like this:

$$\begin{aligned} 1 &= 1 \\ 3 &= 1+2 \\ 6 &= 1+2+3 \\ 10 &= 1+2+3+4 \\ \vdots &\quad \vdots \\ T_n &= 1+2+3+\cdots+n. \end{aligned}$$

Consider how we could find the sum of the first 100 positive integers (that is, T_{100}). Instead of adding them in order, we regroup and add $1+100=101$. The next pair to combine is $2+99=101$. Then $3+98=101$. Keep going. This gives 50 pairs which each add up to 101, so $T_{100}=101\cdot 50=5050$.[1] This insight is usually attributed to Carl Friedrich Gauss, one of the greatest mathematicians of all time, who discovered it as a child when his unpleasant elementary teacher thought he would keep the class busy by requiring them to compute the lengthy sum.

In general, using this same sort of regrouping, we find that $T_n=\frac{n(n+1)}{2}$. Incidentally, this is exactly the same as $\binom{n+1}{2}$, which makes sense if you think of the triangular numbers as counting the number of handshakes that take place at a party with $n+1$ people: the first person shakes n hands, the next shakes an additional $n-1$ hands and so on.

The point of all of this is that some sequences, while not arithmetic or geometric, can be interpreted as the sequence of partial sums of arithmetic and geometric sequences. Luckily there are methods we can use to compute these sums quickly.

Summing Arithmetic Sequences: Reverse and Add

Here is a technique that allows us to quickly find the sum of an arithmetic sequence.

Example $Supplementary Notes. 4$

Find the sum: $2+5+8+11+14+\cdots+470$.

Solution

The idea is to mimic how we found the formula for triangular numbers. If we add the first and last terms, we get 472. The second term and second-to-last term also add up to 472. To keep track of everything, we might express this as follows. Call the sum S. Then,

$S=$	2	$+$	5	$+$	8	$+\cdots+$	467	$+$	470
$+\quad S=$	470	$+$	467	$+$	464	$+\cdots+$	5	$+$	2
$2S=$	472	$+$	472	$+$	472	$+\cdots+$	472	$+$	472

To find $2S$ then we add 472 to itself a number of times. What number? We need to decide how many terms (*summands*) are in the sum. Since the terms form an arithmetic sequence, the nth term in the sum (counting 2 as the 0th term) can be expressed as $2+3n$. If $2+3n=470$ then $n=156$. So n ranges from 0 to 156, giving 157 terms in the sum. This is the number of 472's in the sum for $2S$. Thus

$$2S=157\cdot 472=74104$$

It is now easy to find S:

$$S=74104/2=37052$$

This will work for any sum of *arithmetic* sequences. Call the sum S. Reverse and add. This produces a single number added to itself many times. Find the number of times. Multiply. Divide by 2. Done.

Example $Supplementary Notes. 5$

Find a closed formula for $6+10+14+\cdots+(4n-2)$.

Solution

Again, we have a sum of an arithmetic sequence. We need to know how many terms are in the sequence. Clearly each term in the sequence has the form $4k-2$ (as evidenced by the last term). For which values of k though? To get 6, $k=2$. To get $4n-2$ take $k=n$. So to find the number of terms, we need to know how many integers are in the range $2,3,\ldots,n$. The answer is $n-1$. (There are n numbers from 1 to n, so one less if we start with 2.)

Now reverse and add:

$S=$	6	$+$	10	$+\cdots+$	$4n-6$	$+$	$4n-2$
$+\quad S=$	$4n-2$	$+$	$4n-6$	$+\cdots+$	10	$+$	6
$2S=$	$4n+4$	$+$	$4n+4$	$+\cdots+$	$4n+4$	$+$	$4n+4$

Since there are $n-2$ terms, we get

$$2S=(n-2)(4n+4) \qquad \text{so} \qquad S=\frac{(n-2)(4n+4)}{2}$$

Besides finding sums, we can use this technique to find closed formulas for sequences we recognize as sequences of partial sums.

Example $Supplementary Notes. 6$

Use partial sums to find a closed formula for $(a_n)_{n\geq 0}$ which starts $2,3,7,14,24,37,\ldots\ldots$

Solution

First, if you look at the differences between terms, you get a sequence of differences: $1, 4, 7, 10, 13, \ldots$, which is an arithmetic sequence. Written another way:

$$\begin{aligned} a_0 &= 2 \\ a_1 &= 2+1 \\ a_2 &= 2+1+4 \\ a_3 &= 2+1+4+7 \end{aligned}$$

and so on. We can write the general term of (a_n) in terms of the arithmetic sequence as follows:

$$a_n = 2+1+4+7+10+\cdots+(1+3(n-1))$$

(we use $1+3(n-1)$ instead of $1+3n$ to get the indices to line up correctly; for a_3 we add up to 7, which is $1+3(3-1)$).

We can reverse and add, but the initial 2 does not fit our pattern. This just means we need to keep the 2 out of the reverse part:

$a_n =$	2	$+$	1	$+$	4	$+\cdots+$	$1+3(n-1)$
$+\, a_n =$	2	$+$	$1+3(n-1)$	$+$	$1+3(n-2)$	$+\cdots+$	1
$2a_n =$	4	$+$	$2+3(n-1)$	$+$	$2+3(n-1)$	$+\cdots+$	$2+3(n-1)$

Not counting the first term (the 4) there are n summands of $2+3(n-1) = 3n-1$ so the right-hand side becomes $2+(3n-1)n$.

Finally, solving for a_n we get

$$a_n = \frac{4+(3n-1)n}{2}.$$

Just to be sure, we check $a_0 = \frac{4}{2} = 2$, $a_1 = \frac{4+2}{2} = 3$, etc. We have the correct closed formula.

Summing Geometric Sequences: Multiply, Shift and Subtract

To find the sum of a geometric sequence, we cannot just reverse and add. Do you see why? The reason we got the same term added to itself many times is because there was a constant difference. So as we added that difference in one direction, we subtracted the difference going the other way, leaving a constant total. For geometric sums, we have a different technique.

Example $SupplementaryNotes.7$

What is $3+6+12+24+\cdots+12288$?

Solution

Multiply each term by 2, the common ratio. You get $2S = 6+12+24+\cdots+24576$. Now subtract: $2S - S = -3+24576 = 24573$. Since $2S - S = S$, we have our answer.

To better see what happened in the above example, try writing it this way:

$S =$	$3+$	$6+12+24+\cdots+12288$	
$-\, 2S =$		$6+12+24+\cdots+12288$	$+24576$
$-S =$	$3+$	$0+0+0+\cdots+0$	-24576

Then divide both sides by -1 and we have the same result for S. The idea is, by multiplying the sum by the common ratio, each term becomes the next term. We shift over the sum to get the subtraction to mostly cancel out, leaving just the first term and new last term.

Example *SupplementaryNotes.* 8

Find a closed formula for $S(n) = 2 + 10 + 50 + \cdots + 2 \cdot 5^n$.

Solution

The common ratio is 5. So we have

S	$= 2 + 10 + 50 + \cdots + 2 \cdot 5^n$
$-\ 5S$	$= \quad 10 + 50 + \cdots + 2 \cdot 5^n + 2 \cdot 5^{n+1}$
$-4S$	$= 2 - 2 \cdot 5^{n+1}$

Thus $S = \dfrac{2 - 2 \cdot 5^{n+1}}{-4}$

Even though this might seem like a new technique, you have probably used it before.

Example *SupplementaryNotes.* 9

Express $0.464646\ldots$ as a fraction.

Solution

Let $N = 0.46464646\ldots$ Consider $0.01N$. We get:

	$N =$	$0.4646464\ldots$
$-$	$0.01N =$	$0.00464646\ldots$
	$0.99N =$	0.46

So $N = \frac{46}{99}$. What have we done? We viewed the repeating decimal $0.464646\ldots$ as a sum of the geometric sequence $0.46, 0.0046, 0.000046, \ldots$ The common ratio is 0.01. The only real difference is that we are now computing an *infinite* geometric sum, we do not have the extra "last" term to consider. Really, this is the result of taking a limit as you would in calculus when you compute *infinite* geometric sums.

$\sum$ and $\prod$ notation

To simplify writing out sums, we will use notation like $\sum_{k=1}^{n} a_k$. This means add up the a_k's where k changes from 1 to n.

Example *SupplementaryNotes.* 10

Use $\sum$ notation to rewrite the sums:

1. $1 + 2 + 3 + 4 + \cdots + 100$
2. $1 + 2 + 4 + 8 + \cdots + 2^{50}$
3. $6 + 10 + 14 + \cdots + (4n - 2)$.

Solution

$\sum_{k=1}^{100} k \quad \sum_{k=0}^{50} 2^k \quad \sum_{k=2}^{n} (4k - 2)$

If we want to multiply the a_k instead, we would write $\prod_{k=1}^{n} a_k$. For example, $\prod_{k=1}^{n} k = n!$.

Supplementary Notes: Recurrence Relations

Investigate!

Consider the recurrence relation

$$a_n = 5a_{n-1} - 6a_{n-2}.$$

1. What sequence do you get if the initial conditions are $a_0 = 1,\ a_1 = 2$? Give a closed formula for this sequence.
2. What sequence do you get if the initial conditions are $a_0 = 1,\ a_1 = 3$? Give a closed formula.
3. What if $a_0 = 2$ and $a_1 = 5$? Find a closed formula.

We have seen that it is often easier to find recursive definitions than closed formulas. Lucky for us, there are a few techniques for converting recursive definitions to closed formulas. Doing so is called *solving a recurrence relation*. Recall that the recurrence relation is a recursive definition without the initial conditions. For example, the recurrence relation for the Fibonacci sequence is $F_n = F_{n-1} + F_{n-2}$. (This, together with the initial conditions $F_0 = 0$ and $F_1 = 1$ give the entire recursive *definition* for the sequence.)

Example $SupplementaryNotes.1$

Find a recurrence relation and initial conditions for $1, 5, 17, 53, 161, 485 \ldots$.

Solution

Finding the recurrence relation would be easier if we had some context for the problem (like the Tower of Hanoi, for example). Alas, we have only the sequence. Remember, the recurrence relation tells you how to get from previous terms to future terms. What is going on here? We could look at the differences between terms: $4, 12, 36, 108, \ldots$ Notice that these are growing by a factor of 3. Is the original sequence as well? $1 \cdot 3 = 3,\ 5 \cdot 3 = 15,\ 17 \cdot 3 = 51$ and so on. It appears that we always end up with 2 less than the next term. Aha!

So $a_n = 3a_{n-1} + 2$ is our recurrence relation and the initial condition is $a_0 = 1$.

We are going to try to *solve* these recurrence relations. By this we mean something very similar to solving differential equations: we want to find a function of n (a closed formula) which satisfies the recurrence relation, as well as the initial condition.[2] Recurrence relations are sometimes called difference equations since they can describe the difference between terms and this highlights the relation to differential equations further. Just like for differential equations, finding a solution might be tricky, but checking that the solution is correct is easy.

Example $SupplementaryNotes.2$

Check that $a_n = 2^n + 1$ is a solution to the recurrence relation $a_n = 2a_{n-1} - 1$ with $a_1 = 3$.

Solution

First, it is easy to check the initial condition: a_1 should be $2^1 + 1$ according to our closed formula. Indeed, $2^1 + 1 = 3$, which is what we want. To check that our proposed solution satisfies the recurrence relation, try plugging it in.

$$\begin{aligned} 2a_{n-1} - 1 &= 2(2^{n-1} + 1) - 1 \\ &= 2^n + 2 - 1 \\ &= 2^n + 1 \\ &= a_n. \end{aligned}$$

That's what our recurrence relation says! We have a solution.

Sometimes we can be clever and solve a recurrence relation by inspection. We generate the sequence using the recurrence relation and keep track of what we are doing so that we can see how to jump to finding just the a_n term. Here are two examples of how you might do that.

Telescoping refers to the phenomenon when many terms in a large sum cancel out - so the sum "telescopes." For example:

$$(2-1)+(3-2)+(4-3)+\cdots+(100-99)+(101-100)=-1+101$$

because every third term looks like: $2+-2=0,$ and then $3+-3=0$ and so on.

We can use this behavior to solve recurrence relations. Here is an example.

Example $SupplementaryNotes.3$

Solve the recurrence relation $a_n=a_{n-1}+n$ with initial term $a_0=4.$

Solution

To get a feel for the recurrence relation, write out the first few terms of the sequence: $4,5,7,10,14,19,\ldots$ Look at the difference between terms. $a_1-a_0=1$ and $a_2-a_1=2$ and so on. The key thing here is that the difference between terms is n. We can write this explicitly: $a_n-a_{n-1}=n.$ Of course, we could have arrived at this conclusion directly from the recurrence relation by subtracting a_{n-1} from both sides.

Now use this equation over and over again, changing n each time:

$$\begin{aligned} a_1-a_0 &= 1 \\ a_2-a_1 &= 2 \\ a_3-a_2 &= 3 \\ \vdots &\quad \vdots \\ a_n-a_{n-1} &= n. \end{aligned}$$

Add all these equations together. On the right-hand side, we get the sum $1+2+3+\cdots+n.$ We already know this can be simplified to $\frac{n(n+1)}{2}$. What happens on the left-hand side? We get

$$(a_1-a_0)+(a_2-a_1)+(a_3-a_2)+\cdots(a_{n-1}-a_{n-2})+(a_n-a_{n-1}).$$

This sum telescopes. We are left with only the $-a_0$ from the first equation and the a_n from the last equation. Putting this all together we have $-a_0+a_n=\frac{n(n+1)}{2}$ or $a_n=\frac{n(n+1)}{2}+a_0.$ But we know that $a_0=4.$ So the solution to the recurrence relation, subject to the initial condition is

$$a_n=\frac{n(n+1)}{2}+4.$$

(Now that we know that, we should notice that the sequence is the result of adding 4 to each of the triangular numbers.)

The above example shows a way to solve recurrence relations of the form $a_n=a_{n-1}+f(n)$ where $\sum_{k=1}^{n} f(k)$ has a known closed formula. If you rewrite the recurrence relation as $a_n-a_{n-1}=f(n),$ and then add up all the different equations with n ranging between 1 and n, the left-hand side will always give you a_n-a_0. The right-hand side will be $\sum_{k=1}^{n} f(k)$, which is why we need to know the closed formula for that sum.

However, telescoping will not help us with a recursion such as $a_n=3a_{n-1}+2$ since the left-hand side will not telescope. You will have $-3a_{n-1}$'s but only one a_{n-1}. However, we can still be clever if we use *iteration*.

We have already seen an example of iteration when we found the closed formula for arithmetic and geometric sequences. The idea is, we *iterate* the process of finding the next term, starting with the known initial condition, up until we have a_n. Then we simplify. In the arithmetic sequence example, we simplified by multiplying d by the number of times we add it to a when we get to a_n, to get from $a_n=a+d+d+d+\cdots+d$ to $a_n=a+dn$.

To see how this works, let's go through the same example we used for telescoping, but this time use iteration.

Example $SupplementaryNotes.4$

Use iteration to solve the recurrence relation $a_n = a_{n-1} + n$ with $a_0 = 4$.

Answer

Again, start by writing down the recurrence relation when $n = 1$. This time, don't subtract the a_{n-1} terms to the other side:

$$a_1 = a_0 + 1.$$

Now $a_2 = a_1 + 2$, but we know what a_1 is. By substitution, we get

$$a_2 = (a_0 + 1) + 2.$$

Now go to $a_3 = a_2 + 3$, using our known value of a_2:

$$a_3 = ((a_0 + 1) + 2) + 3.$$

We notice a pattern. Each time, we take the previous term and add the current index. So

$$a_n = ((((a_0 + 1) + 2) + 3) + \cdots + n - 1) + n.$$

Regrouping terms, we notice that a_n is just a_0 plus the sum of the integers from 1 to n. So, since $a_0 = 4$,

$$a_n = 4 + \frac{n(n+1)}{2}.$$

Of course in this case we still needed to know formula for the sum of $1, \ldots, n$. Let's try iteration with a sequence for which telescoping doesn't work.

Example $SupplementaryNotes.5$

Solve the recurrence relation $a_n = 3a_{n-1} + 2$ subject to $a_0 = 1$.

Answer

Again, we iterate the recurrence relation, building up to the index n.

$$\begin{aligned}
a_1 &= 3a_0 + 2 \\
a_2 &= 3(a_1) + 2 = 3(3a_0 + 2) + 2 \\
a_3 &= 3[a_2] + 2 = 3[3(3a_0 + 2) + 2] + 2 \\
&\vdots \quad\quad \vdots \quad\quad\quad \vdots \\
a_n &= 3(a_{n-1}) + 2 = 3(3(3(3 \cdots (3a_0 + 2) + 2) + 2) \cdots + 2) + 2.
\end{aligned}$$

It is difficult to see what is happening here because we have to distribute all those 3's. Let's try again, this time simplifying a bit as we go.

$$\begin{aligned}
a_1 &= 3a_0 + 2 \\
a_2 &= 3(a_1) + 2 = 3(3a_0 + 2) + 2 = 3^2 a_0 + 2 \cdot 3 + 2 \\
a_3 &= 3[a_2] + 2 = 3[3^2 a_0 + 2 \cdot 3 + 2] + 2 = 3^3 a_0 + 2 \cdot 3^2 + 2 \cdot 3 + 2 \\
&\vdots \quad\quad\quad\quad\quad\quad\quad\quad \vdots \\
a_n &= 3(a_{n-1}) + 2 = 3(3^{n-1} a_0 + 2 \cdot 3^{n-2} + \cdots + 2) + 2 \\
&\qquad = 3^n a_0 + 2 \cdot 3^{n-1} + 2 \cdot 3^{n-2} + \cdots + 2 \cdot 3 + 2.
\end{aligned}$$

Now we simplify. $a_0 = 1$, so we have $3^n + \langle \text{stuff} \rangle$. Note that all the other terms have a 2 in them. In fact, we have a geometric sum with first term 2 and common ratio 3. We have seen how to simplify $2 + 2 \cdot 3 + 2 \cdot 3^2 + \cdots + 2 \cdot 3^{n-1}$. We get $\frac{2 - 2 \cdot 3^n}{-2}$ which simplifies to $3^n - 1$. Putting this together with the first 3^n term gives our closed formula:

$$a_n = 2 \cdot 3^n - 1.$$

Iteration can be messy, but when the recurrence relation only refers to one previous term (and maybe some function of n) it can work well. However, trying to iterate a recurrence relation such as $a_n = 2a_{n-1} + 3a_{n-2}$ will be way too complicated. We would need to keep track of two sets of previous terms, each of which were expressed by two previous terms, and so on. The length of the formula would grow exponentially (double each time, in fact). Luckily there happens to be a method for solving recurrence relations which works very well on relations like this.

The Characteristic Root Technique

Suppose we want to solve a recurrence relation expressed as a combination of the two previous terms, such as $a_n = a_{n-1} + 6a_{n-2}$. In other words, we want to find a function of n which satisfies $a_n - a_{n-1} - 6a_{n-2} = 0$. Now iteration is too complicated, but think just for a second what would happen if we *did* iterate. In each step, we would, among other things, multiply a previous iteration by 6. So our closed formula would include 6 multiplied some number of times. Thus it is reasonable to guess the solution will contain parts that look geometric. Perhaps the solution will take the form r^n for some constant r.

The nice thing is, we know how to check whether a formula is actually a solution to a recurrence relation: plug it in. What happens if we plug in r^n into the recursion above? We get

$$r^n - r^{n-1} - 6r^{n-2} = 0.$$

Now solve for r:

$$r^{n-2}(r^2 - r - 6) = 0,$$

so by factoring, $r = -2$ or $r = 3$ (or $r = 0$, although this does not help us). This tells us that $a_n = (-2)^n$ is a solution to the recurrence relation, as is $a_n = 3^n$. Which one is correct? They both are, unless we specify initial conditions. Notice we could also have $a_n = (-2)^n + 3^n$. Or $a_n = 7(-2)^n + 4 \cdot 3^n$. In fact, for any a and b, $a_n = a(-2)^n + b3^n$ is a solution (try plugging this into the recurrence relation). To find the values of a and b, use the initial conditions.

This points us in the direction of a more general technique for solving recurrence relations. Notice we will always be able to factor out the r^{n-2} as we did above. So we really only care about the other part. We call this other part the *characteristic equation* for the recurrence relation. We are interested in finding the roots of the characteristic equation, which are called (surprise) the *characteristic roots*.

Characteristic Roots

Given a recurrence relation $a_n + \alpha a_{n-1} + \beta a_{n-2} = 0$, the *characteristic polynomial* is

$$x^2 + \alpha x + \beta$$

giving the *characteristic equation*:

$$x^2 + \alpha x + \beta = 0.$$

If r_1 and r_2 are two distinct roots of the characteristic polynomial (i.e, solutions to the characteristic equation), then the solution to the recurrence relation is

$$a_n = ar_1^n + br_2^n,$$

where a and b are constants determined by the initial conditions.

Example $SupplementaryNotes.6$

Solve the recurrence relation $a_n = 7a_{n-1} - 10a_{n-2}$ with $a_0 = 2$ and $a_1 = 3$.

Solution

Rewrite the recurrence relation $a_n - 7a_{n-1} + 10a_{n-2} = 0$. Now form the characteristic equation:

$$x^2 - 7x + 10 = 0$$

and solve for x:

$$(x - 2)(x - 5) = 0$$

so $x = 2$ and $x = 5$ are the characteristic roots. We therefore know that the solution to the recurrence relation will have the form

$$a_n = a2^n + b5^n.$$

To find a and b, plug in $n = 0$ and $n = 1$ to get a system of two equations with two unknowns:

$$\begin{aligned} 2 &= a2^0 + b5^0 = a + b \\ 3 &= a2^1 + b5^1 = 2a + 5b \end{aligned}$$

Solving this system gives $a = \frac{7}{3}$ and $b = -\frac{1}{3}$ so the solution to the recurrence relation is

$$a_n = \frac{7}{3}2^n - \frac{1}{3}5^n.$$

Perhaps the most famous recurrence relation is $F_n = F_{n-1} + F_{n-2}$, which together with the initial conditions $F_0 = 0$ and $F_1 = 1$ defines the Fibonacci sequence. But notice that this is precisely the type of recurrence relation on which we can use the characteristic root technique. When you do, the only thing that changes is that the characteristic equation does not factor, so you need to use the quadratic formula to find the characteristic roots. In fact, doing so gives the third most famous irrational number, φ, the *golden ratio*.

Before leaving the characteristic root technique, we should think about what might happen when you solve the characteristic equation. We have an example above in which the characteristic polynomial has two distinct roots. These roots can be integers, or perhaps irrational numbers (requiring the quadratic formula to find them). In these cases, we know what the solution to the recurrence relation looks like.

However, it is possible for the characteristic polynomial to only have one root. This can happen if the characteristic polynomial factors as $(x - r)^2$. It is still the case that r^n would be a solution to the recurrence relation, but we won't be able to find solutions for all initial conditions using the general form $a_n = ar_1^n + br_2^n$, since we can't distinguish between r_1^n and r_2^n. We are in luck though:

Characteristic Root Technique for Repeated Roots

Suppose the recurrence relation $a_n = \alpha a_{n-1} + \beta a_{n-2}$ has a characteristic polynomial with only one root r. Then the solution to the recurrence relation is

$$a_n = ar^n + bnr^n$$

where a and b are constants determined by the initial conditions.

Notice the extra n in bnr^n. This allows us to solve for the constants a and b from the initial conditions.

Example $SupplementaryNotes.7$

Solve the recurrence relation $a_n = 6a_{n-1} - 9a_{n-2}$ with initial conditions $a_0 = 1$ and $a_1 = 4$.

Answer

The characteristic polynomial is $x^2 - 6x + 9$. We solve the characteristic equation

$$x^2 - 6x + 9 = 0$$

by factoring:

$$(x - 3)^2 = 0$$

so $x = 3$ is the only characteristic root. Therefore we know that the solution to the recurrence relation has the form

$$a_n = a3^n + bn3^n$$

for some constants a and b. Now use the initial conditions:

$$\begin{aligned} a_0 = 1 \quad &= a3^0 + b \cdot 0 \cdot 3^0 = a \\ a_1 = 4 \quad &= a \cdot 3 + b \cdot 1 \cdot 3 = 3a + 3b. \end{aligned}$$

Since $a = 1,$ we find that $b = \frac{1}{3}.$ Therefore the solution to the recurrence relation is

$$a_n = 3^n + \frac{1}{3} n 3^n.$$

Although we will not consider examples more complicated than these, this characteristic root technique can be applied to much more complicated recurrence relations. For example, $a_n = 2a_{n-1} + a_{n-2} - 3a_{n-3}$ has characteristic polynomial $x^3 - 2x^2 - x + 3.$ Assuming you see how to factor such a degree 3 (or more) polynomial you can easily find the characteristic roots and as such solve the recurrence relation (the solution would look like $a_n = ar_1^n + br_2^n + cr_3^n$ if there were 3 distinct roots). It is also possible to solve recurrence relations of the form $a_n = \alpha a_{n-1} + \beta a_{n-2} + C$ for some constant C. It is also possible (and acceptable) for the characteristic roots to be complex numbers.

CHAPTER OVERVIEW

5: Set Theory

Thumbnail: A Venn diagram illustrating the intersection of two sets. (Public Domain; Cepheus).

5.1: Sets and Operations on Sets

Before beginning this section, it would be a good idea to review sets and set notation, including the *roster method* and *set builder notation*, in Section 2.3.

? PREVIEW ACTIVITY 5.1.1: Set Operations

In Section 2.1, we used logical operators (conjunction, disjunction, negation) to form new statements from existing statements. In a similar manner, there are several ways to create new sets from sets that have already been defined. In fact, we will form these new sets using the logical operators of conjunction (and), disjunction (or), and negation (not). For example, if the universal set is the set of natural numbers N and

$$A = \{1, 2, 3, 4, 5, 6\} \quad \text{and} \quad B = \{1, 3, 5, 7, 9\}, \tag{5.1.1}$$

- The set consisting of all natural numbers that are in A and are in B is the set $\{1, 3, 5\}$;
- The set consisting of all natural numbers that are in A or are in B is the set $\{1, 2, 3, 4, 5, 6, 7, 9\}$ and
- The set consisting of all natural numbers that are in A and are not in B is the set $\{2, 4, 6\}$.

These sets are examples of some of the most common set operations, which are given in the following definitions.

Definition: intersection

Let A and B be subsets of some universal set U. The *intersection* of A and B, written $A \cap B$ and read "A intersect B," is the set of all elements that are in both A and B. That is,

$$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}. \tag{5.1.2}$$

The union of A and B, written $A \cup B$ and read "A union B," is the set of all elements that are in A or in B. That is,

$$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}. \tag{5.1.3}$$

Definition: complement

Let A and B be subsets of some universal set U. The set *difference* of A and B, or *relative complement* of B with respect to A, written $A - B$ and read "A minus B" or "the complement of B with respect to A," is the set of all elements in A that are not in B. That is,

$$A - B = \{x \in U \mid x \in A \text{ and } x \notin B\}. \tag{5.1.4}$$

The *complement* of the set A, written A^c and read "the complement of A," is the set of all elements of U that are not in A. That is,

$$A^c = \{x \in U \mid x \notin A\}. \tag{5.1.5}$$

For the rest of this preview activity, the universal set is $U = \{0, 1, 2, 3, \ldots, 10\}$, and we will use the following subsets of U:

$$A = \{0, 1, 2, 3, 9\} \quad \text{and} \quad B = \{2, 3, 4, 5, 6\}, \tag{5.1.6}$$

So in this case, $A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\} = \{2, 3\}$. Use the roster method to specify each of the following subsets of U.

1. $A \cup B$
2. A^c
3. B^c

We can now use these sets to form even more sets. For example,

$$A \cap B^c = \{0, 1, 2, 3, 9\} \cap \{0, 1, 7, 8, 9, 10\} = \{0, 1, 9\}. \tag{5.1.7}$$

Use the roster method to specify each of the following subsets of U.

4. $A \cup B^c$

5. $A^c \cap B^c$
6. $A^c \cup B^c$
7. $(A \cap B)^c$

Preview Activity 5.1.2: Venn Diagrams for Two Sets

In Preview Activity 5.1.1, we worked with verbal and symbolic definitions of set operations. However, it is also helpful to have a visual representation of sets. *Venn diagrams* are used to represent sets by circles (or some other closed geometric shape) drawn inside a rectangle. The points inside the rectangle represent the universal set U, and the elements of a set are represented by the points inside the circle that represents the set. For example, Figure 5.1.1 is a Venn diagram showing two sets.

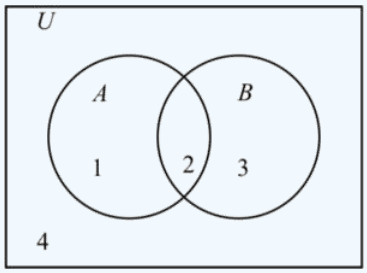


***Figure* 5.1.1** *: Venn Diagram for Two Sets*

In Figure 5.1.1, the elements of A are represented by the points inside the left circle, and the elements of B are represented by the points inside the right circle. The four distinct regions in the diagram are numbered for reference purposes only. (The numbers do not represent elements in a set.) The following table describes the four regions in the diagram.

Region	Elements of U	Set
1	In A and not in B	$A - B$
2	In A and in B	$A \cap B$
3	In B and not in A	$B - A$
4	Not in A and not in B	$A^c \cap B^c$

We can use these regions to represent other sets. For example, the set $A \cup B$ is represented by regions 1, 2, and 3 or the shaded region in Figure 5.1.2.

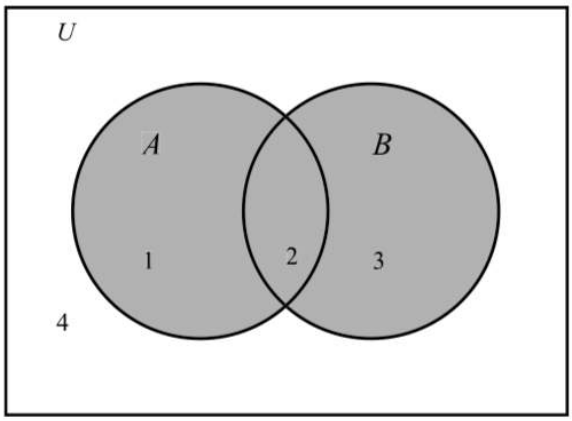


Figure* 5.1.2*: *Venn Diagram for $A \cup B$*

Let A and B be subsets of a universal set U. For each of the following, draw a Venn diagram for two sets and shade the region that represent the specified set. In addition, describe the set using set builder notation.

1. A^c
2. B^c
3. $A^c \cup B$
4. $A^c \cup B^c$
5. $(A \cap B)^c$
6. $(A \cup B) - (A \cap B)$

Set Equality, Subsets, and Proper Subsets

In Section 2.3, we introduced some basic definitions used in set theory, what it means to say that two sets are equal and what it means to say that one set is a subset of another set. We need one more definition.

Definition: proper subset

Let A and B be two sets contained in some universal set U. The set A is a *proper subset* of B provided that $A \subseteq B$ and $A \neq B$. When A is a proper subset of B, we write $A \subset B$.

One reason for the definition of proper subset is that each set is a subset of itself. That is,

$$\text{If } A \text{ is a set, then } A \subseteq A$$

However, sometimes we need to indicate that a set X is a subset of Y but $X \neq Y$. For example, if

$$X = \{1, 2\} \text{ and } Y = \{0, 1, 2, 3\}.$$

then $X \subset Y$. We know that $X \subseteq Y$ since each element of X is an element of Y, but $X \neq Y$ since $0 \in Y$ and $0 \notin X$. (Also, $3 \in Y$ and $3 \notin X$.) Notice that the notations $A \subset B$ and $A \subseteq B$ are used in a manner similar to inequality notation for numbers ($a < b$ and $a \leq b$).

It is often very important to be able to describe precisely what it means to say that one set is not a subset of the other. In the preceding example, Y is not a subset of X since there exists an element of Y (namely, 0) that is not in X.

In general, the subset relation is described with the use of a universal quantifier since $A \subseteq B$ means that for each element x of U, if $x \in A$, then $x \in B$. So when we negate this, we use an existential quantifier as follows:

$$\begin{array}{lll} A \subseteq B & \text{means} & (\forall x \in U)[(x \in A) \to (x \in B)]. \\ A \nsubseteq B & \text{means} & \neg(\forall x \in U)[(x \in A) \to (x \in B)] \\ & & (\exists x \in U)\neg[(x \in A) \to (x \in B)] \\ & & (\exists x \in U)[(x \in A) \wedge (x \notin B)]. \end{array} \tag{5.1.8}$$

So we see that $A \nsubseteq B$ means that there exists an x in U such that $x \in A$ and $x \notin B$.

Notice that if $A = \emptyset$, then the conditional statement, "For each $x \in U$, if $x \in \emptyset$, then $x \in B$" must be true since the hypothesis will always be false. Another way to look at this is to consider the following statement:

$$\emptyset \nsubseteq B \text{ means that there exists an } x \in \emptyset \text{ such that } x \notin B.$$

However, this statement must be false since there does not exist an x in $\emptyset$. Since this is false, we must conclude that $\emptyset \subseteq B$. Although the facts that $\emptyset \subseteq B$ and $B \subseteq B$ may not seem very important, we will use these facts later, and hence we summarize them in Theorem 5.1.

Theorem 5.1

For any set B, $\emptyset \subseteq B$ and $B \subseteq B$.

In Section 2.3, we also defined two sets to be equal when they have precisely the same elements. For example,

$$\{x \in \mathbb{R} \mid x^{=}4\} = \{-2, 2\}.$$

If the two sets A and B are equal, then it must be true that every element of A is an element of B, that is, $A \subseteq B$, and it must be true that every element of B is an element of A, this is, $B \subseteq A$. Conversely, if $A \subseteq B$ and $B \subseteq A$, then A and B must have

precisely the same elements. This gives us the following test for set equality:

Theorem 5.2

Let A and B be subsets of some universal set U. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

Progress Check 5.3: Using Set Notation

Let the universal set be $U = \{1, 2, 3, 4, 5, 6\}$, and let

$$A = \{1, 2, 4\},\ B = \{1, 2, 3, 5\},\ C = \{x \in U \mid x^2 \leq 2\}.$$

In each of the following, fill in the blank with one or more of the symbols $\subset$, $\subseteq$, $=$, $\neq$, $\in$ or $\notin$ so that the resulting statement is true. For each blank, include all symbols that result in a true statement. If none of these symbols makes a true statement, write nothing in the blank.

A	_____	B	$\emptyset$	_____	A
5	_____	B	$\{5\}$	_____	B
A	_____	C	$\{1, 2\}$	_____	C
$\{1, 2\}$	_____	A	$\{4, 2, 1\}$	_____	A
6	_____	A	B	_____	$\emptyset$

Answer

Add texts here. Do not delete this text first.

More about Venn Diagrams

In Preview Activity 5.1.2, we learned how to use Venn diagrams as a visual representation for sets, set operations, and set relationships. In that preview activity, we restricted ourselves to using two sets. We can, of course, include more than two sets in a Venn diagram. Figure 5.1.3 shows a general Venn diagram for three sets (including a shaded region that corresponds to $A \cap C$).

In this diagram, there are eight distinct regions, and each region has a unique reference number. For example, the set A is represented by the combination of regions 1, 2, 4, and 5, whereas the set C is represented by the combination of regions 4, 5, 6, and 7. This means that the set $A \cap C$ is represented by the combination of regions 4 and 5. This is shown as the shaded region in Figure 5.1.3.

Finally, Venn diagrams can also be used to illustrate special relationships be- tween sets. For example, if $A \subseteq B$, then the circle representing A should be completely contained in the circle for B. So if $A \subseteq B$, and we know nothing about

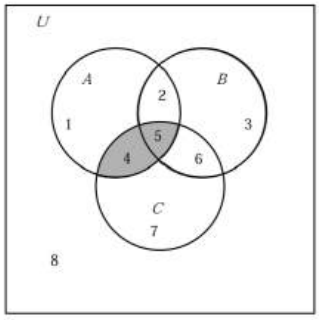


Figure 5.3: Venn Diagram for $A \cap C$

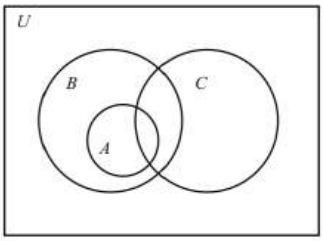


Figure 5.4: Venn Diagram Showing $A \subseteq B$

any relationship between the set C and the sets A and B, we could use the Venn diagram shown in Figure 5.1.4.

? Progress Check 5.4: Using Venn Diagrams

Let A, B, and C be subsets of a universal set U.

1. For each of the following, draw a Venn diagram for three sets and shade the region(s) that represent the specified set.

   (a) $(A \cap B) \cap C$
   (b) $(A \cap B) \cup C$
   (c) $(A^c \cup B)$
   (d) $A^c \cap (B \cup C)$
2. Draw the most general Venn diagram showing $B \subseteq (A \cup C)$.
3. Draw the most general Venn diagram showing $A \subseteq (B^c \cup C)$.

Answer

Add texts here. Do not delete this text first.

The Power Set of a Set

The symbol 2 is used to describe a relationship between an element of the universal set and a subset of the universal set, and the symbol $\subseteq$ is used to describe a relationship between two subsets of the universal set. For example, the number 5 is an integer, and so it is appropriate to write $5 \in \mathbb{Z}$. It is not appropriate, however, to write $5 \subseteq \mathbb{Z}$ since 5 is not a set. It is important to distinguish between 5 and $\{5\}$. The difference is that 5 is an integer and $\{5\}$ is a set consisting of one element. Consequently, it is appropriate to write $\{5\} \subseteq \mathbb{Z}$, but it is not appropriate to write $\{5\} \in \mathbb{Z}$. The distinction between these two symbols (5 and $\{5\}$) is important when we discuss what is called the power set of a given set.

Definition: power set

If A is a subset of a universal set U, then the set whose members are all the subsets of A is called the *power set* of A. We denote the power set of A by $\mathcal{P}(A)$. Symbolically, we write

$$\mathcal{P}(A) = \{X \subseteq U \mid X \subseteq A\}.$$

That is, $X \in \mathcal{P}(A)$ if and only if $X \subseteq A$.

When dealing with the power set of A, we must always remember that $\emptyset \subseteq A$ and $A \subseteq A$. For example, if $A = \{a, b\}$, then the subsets of A are

$$\emptyset, \{a\}, \{b\}, \{a, b\}. \tag{5.1.9}$$

We can write this as

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

Now let $B = \{a, b, c\}$. Notice that $B = A \cup \{c\}$. We can determine the subsets of B by starting with the subsets of A in (5.1.10). We can form the other subsets of B by taking the union of each set in (5.1.10) with the set $\{c\}$. This gives us the following subsets of B.

$$\{c\}, \{a, c\}, \{b, c\}, \{a, b, c\}. \tag{5.1.10}$$

So the subsets of B are those sets in (5.1.10) combined with those sets in (5.1.11). That is, the subsets of B are

$$\emptyset, \{a\}, \{b\}, \{a, b\}, \{c\}, \{a, c\}, \{b, c\}, \{a, b, c\}, \tag{5.1.11}$$

which means that

$$\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{c\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Notice that we could write

$$\{a, c\} \subseteq B \text{ or that } \{a, c\} \in \mathcal{P}(B).$$

Also, notice that A has two elements and A has four subsets, and B has three elements and B has eight subsets. Now, let n be a nonnegative integer. The following result can be proved using mathematical induction. (See Exercise 17).)

Theorem 5.5.

Let n be a nonnegative integer and let T be a subset of some universal set. If the set T has n elements, then the set T has 2^n subsets. That is, $\mathcal{P}(T)$ has 2^n elements.

The Cardinality of a Finite Set

In our discussion of the power set, we were concerned with the number of elements in a set. In fact, the number of elements in a finite set is a distinguishing characteristic of the set, so we give it the following name.

Definition: cardinality

The number of elements in a finite set A is called the *cardinality* of A and is denoted by card(A)

Example

card($\emptyset$) = 0;

card($\{a, b\}$) = 2

card($\mathcal{P}(\{a, b\})$) = 4

Theoretical Note: There is a mathematical way to distinguish between finite and infinite sets, and there is a way to define the cardinality of an infinite set. We will not concern ourselves with this at this time. More about the cardinality of finite and infinite

sets is discussed in Chapter 9.

Standard Number Systems

We can use set notation to specify and help describe our standard number systems. The starting point is the set of **natural numbers**, for which we use the roster method.

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}$$

The **integers** consist of the natural numbers, the negatives of the natural numbers, and zero. If we let $\mathbb{N}^- = \{\dots, -4, -3, -2, -1\}$, then we can use set union and write

$$\mathbb{Z} = \mathbb{N}^- \cup \{0\} \cup \mathbb{N}\,.$$

So we see that $\mathbb{N} \subseteq \mathbb{Z}$, and in fact, $\mathbb{N} \subset \mathbb{Z}$.

We need to use set builder notation for the set $\mathbb{Q}$ of all **rational numbers**, which consists of quotients of integers.

$$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z} \text{and } n \neq 0 \right\}$$

Since any integer n can be written as $n = \dfrac{n}{1}$, we see that $\mathbb{Z} \subseteq \mathbb{Q}$.

We do not yet have the tools to give a complete description of the real numbers. We will simply say that the **real numbers** consist of the rational numbers and the **irrational numbers**. In effect, the irrational numbers are the complement of the set of rational numbers $\mathbb{Q}$ in $\mathbb{R}$. So we can use the notation $\mathbb{Q}^c = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$ and write

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{Q}^c \text{ and } \mathbb{Q} \cap \mathbb{Q}^c = \emptyset\,.$$

A number system that we have not yet discussed is the set of **complex numbers**. The complex numbers, $\mathbb{C}$, consist of all numbers of the form $a + bi$, where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$ (or $i^2 = -1$). That is,

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{and } i = sqrt{-1}\}.$$

We can add and multiply complex numbers as follows: If $a, b, c, d \in \mathbb{R}$, then

$$\begin{aligned} (a+bi)+(c+di) &= (a+c)+(b+d)i, \text{ and} \\ (a+bi)(c+di) &= ac+adi+bci+bdi^2 \\ &= (ac-bd)+(ad+bc)i. \end{aligned} \tag{5.1.12}$$

? Exercises for Section 5.1

1. Assume the universal set is the set of real numbers. Let

   $A = \{-3, -2, 2, 3\}$.
   $B = \{x \in \mathbb{R} \mid x^2 = 4 \text{ or } x^2 = 9\}$,
   $C = \{x \in \mathbb{R} \mid x^2 + 2 = 0\}$,
   $D = \{x \in \mathbb{R} \mid x > 0\}$.

   Respond to each of the following questions. In each case, explain your answer.

   (a) Is the set A equal to the set B?
   (b) Is the set A a subset of the set B?
   (c) Is the set C equal to the set D?
   (d) Is the set C a subset of the set D?
   (e) Is the set A a subset of the set D?
2. (a) Explain why the set $\{a, b\}$ is equal to the set $\{b, a\}$.
   (b) Explain why the set $\{a, b, b, a, c\}$ is equal to the set $\{b, c, a\}$.
3. Assume that the universal set is the set of integers. Let

   $A = \{-3, -2, 2, 3\}$.
   $B = \{x \in \mathbb{Z} \mid x^2 \leq 9\}$,

$C = \{x \in \mathbb{Z} \mid x \geq -3\}$,
$D = \{1, 2, 3, 4\}$,

In each of the following, fill in the blank with one or more of the symbols $\subset$, $\subseteq$, $\not\subseteq$, $=$, $\neq$, $\in$ or $\notin$ so that the resulting statement is true. For each blank, include all symbols that result in a true statement. If none of these symbols makes a true statement, write nothing in the blank.

$$\begin{array}{rcl@{\qquad}rcl} A & \_\_\_\_\_ & B & \emptyset & \_\_\_\_\_ & A \\ 5 & \_\_\_\_\_ & C & \{5\} & \_\_\_\_\_ & C \\ A & \_\_\_\_\_ & C & \{1,2\} & \_\_\_\_\_ & B \\ \{1,2\} & \_\_\_\_\_ & A & \{3,2,1\} & \_\_\_\_\_ & D \\ 4 & \_\_\_\_\_ & B & D & \_\_\_\_\_ & \emptyset \\ \text{card}(A) & \_\_\_\_\_ & \text{card}(D) & \text{card}(A) & \_\_\_\_\_ & \text{card}(B) \\ A & \_\_\_\_\_ & \mathcal{P}(A) & A & \_\_\_\_\_ & \mathcal{P}(B) \end{array} \tag{5.1.13}$$

4. Write all of the proper subset relations that are possible using the sets of numbers $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$.
5. For each statement, write a brief, clear explanation of why the statement is true or why it is false.

   (a) The set $\{a, b\}$ is a subset of $\{a, c, d, e\}$.
   (b) The set $\{-2, 0, 2\}$ is equal to $\{x \in \mathbb{Z} \mid x \text{ is even and } x^2 < 5\}$.
   (c) The empty set $\emptyset$ is a subset of $\{1\}$.
   (d) If $A = \{a, b\}$, then the set $\{a\}$ is a subset of $\mathcal{P}(A)$.
6. Use the definitions of set intersection, set union, and set difference to write useful negations of these definitions. That is, complete each of the following sentences

   (a) $x \notin A \cap B$ if and only if ... .
   (b) $x \notin A \cup B$ if and only if ... .
   (c) $x \notin A - B$ if and only if ... .
7. Let $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, and let

   $A = \{3, 4, 5, 6, 7\}$
   $B = \{1, 5, 7, 9\}$
   $C = \{3, 6, 9\}$
   $D = \{2, 4, 6, 8\}$

   Use the roster method to list all of the elements of each of the following sets.
   (a) $A \cap B$
   (b) $A \cup B$
   (c) $(A \cup B)^c$
   (d) $A^c \cap B^c$
   (e) $(A \cup B) \cap C$
   (f) $A \cap C$
   (g) $B \cap C$
   (h) $(A \cap C) \cup (B \cap C)$
   (i) $B \cap D$
   (j) $(B \cap D)^c$
   (k) $A - D$
   (l) $B - D$
   (m) $(A - D) \cup (B - D)$
   (n) $(A \cup B) - D$
8. Let $U = \mathbb{N}$, and let

   $A = \{x \in \mathbb{N} \mid x \geq 7\}$,

$B = \{x \in \mathbb{N} \mid x \text{ is odd}\}$,
$C = \{x \in \mathbb{N} \mid x \text{ is a multiple of } 3\}$,
$D = \{x \in \mathbb{N} \mid x \text{ is even}\}$,

Use the roster method to list all of the elements of each of the following sets.

(a) $A \cap B$
(b) $A \cup B$
(c) $(A \cup B)^c$
(d) $A^c \cap B^c$
(e) $(A \cup B) \cap C$
(f) $(A \cap C) \cup (B \cap C)$
(g) $B \cap D$
(h) $(B \cap D)^c$
(i) $A - D$
(j) $B - D$
(k) $(A - D) \cup (B - D)$
(l) $(A \cup B) - D$

9. let P, Q, R, and S, be subsets of a universal set U, Assume that $(P - Q) \subseteq (R \cap S)$.

(a) Complete the following sentence:
For each $x \in U$, if $x \in (P - Q)$, then ... .
(b) Write a useful negation of the statement in Part (9a).
(c) Write the contrapositive of the statement in Part (9a).

10. Let U be the universal set. Consider the following statement:

For all A, B, and C that are subsets of U, if $A \subseteq B$, then $B^c \subseteq A^c$.

(a) Identify three conditional statements in the given statement.
(b) Write the contrapositive of this statement.
(c) Write the negation of this statement.

11. Let A, B, and C be subsets of some universal sets U. Draw a Venn diagram for each of the following situations.

(a) $A \subseteq C$
(b) $A \cap B = \emptyset$
(c) $A \nsubseteq B$, $B \nsubseteq A$, $C \subseteq A$, and $C \nsubseteq B$
(d) $A \subseteq B$, $C \subseteq B$, and $A \cap C = \emptyset$

12. Let A, B, and C be subsets of some universal sets U. For each of the following, draw a general Venn diagram for the three sets and then shade the indicated region.

(a) $A \cap B$
(b) $A \cap C$
(c) $(A \cap B) \cup (A \cap C)$
(d) $B \cup C$
(e) $A \cap (B \cup C)$
(f) $(A \cap B) - C$

13. We can extend the idea of consecutive integers (See Exercise (2) in Section 3.5) to represent four consecutive integers as m, $m+1$, $m+2$, and $m+3$, where m is an integer. There are other ways to represent four consecutive integers. For example, if $k \in \mathbb{Z}$, then $k-1$, k, $k+1$, and $k+2$ are four consecutive integers.

(a) Prove that for each $n \in \mathbb{Z}$, n is the sum of four consecutive integers if and only if $n \equiv 2 \pmod 4$.
(b) Use set builder notation or the roster method to specify the set of integers that are the sum of four consecutive integers.

(c) Specify the set of all natural numbers that can be written as the sum of four consecutive natural numbers.
(d) Prove that for each $n \in \mathbb{Z}$, n is the sum of eight consecutive integers if and only if $n \equiv 4 \pmod 8$.
(e) Use set builder notation or the roster method to specify the set of integers that are the sum of eight consecutive integers.
(f) Specify the set of all natural numbers can be written as the sum of eight consecutive natural numbers.

14. One of the properties of real numbers is the so-called **Law of Trichotomy**, which states that if $a, b \in \mathbb{R}$, then exactly one of the following is true:

- $a < b$;
- $a = b$;
- $a > b$.

Is the following proposition concerning sets true or false? Either provide a proof that it is true or a counterexample showing it is false.

If A and B are subsets of some universal set, then exactly one of the following is true:

- $A \subseteq B$;
- $A = B$;
- $B \subseteq A$.

Explorations and Activities

15. **Intervals of Real Numbers.** In previous mathematics courses, we have frequently used subsets of the real numbers called intervals. There are some common names and notations for intervals. These are given in the following table, where it is assumed that a and b are real numbers and $a < b$.

Interval Notation	Set Notation	Name
$(a, b) =$	$\{x \in \mathbb{R} \mid a < x < b\}$	Open interval from a to b
$[a, b] =$	$\{x \in \mathbb{R} \mid a \leq x \leq b\}$	Closed interval from a to b
$[a, b) =$	$\{x \in \mathbb{R} \mid a \leq x < b\}$	Half-open interval
$(a, b] =$	$\{x \in \mathbb{R} \mid a < x \leq b\}$	Half-open interval
$(a, +\infty) =$	$\{x \in \mathbb{R} \mid x > a\}$	Open ray
$(-\infty, b) =$	$\{x \in \mathbb{R} \mid x < b\}$	Open ray
$[a, +\infty) =$	$\{x \in \mathbb{R} \mid x \geq a\}$	Closed ray
$(-\infty, b] =$	$\{x \in \mathbb{R} \mid x \leq b\}$	Closed ray

(a) Is (a, b) a proper subset of $(a, b]$? Explain.
(b) Is $[a, b]$ a subset of $(a, +\infty)$? Explain.
(c) Use interval notation to describe

i. the intersection of the interval $[-3, 7]$ with the interval $(5, 9]$;
ii. the union of the interval $[-3, 7]$ with the interval $(5, 9]$;
iii. the set difference $[-3, 7] - (5, 9]$.

(d) Write the set $\{x \in \mathbb{R} \mid |x| \leq 0.01\}$ using interval notation.
(e) Write the set $\{x \in \mathbb{R} \mid |x| > 2\}$ as the union of two intervals.

16. **More Work with Intervals**. For this exercise, use the interval notation described in Exercise 15.

(a) Determine the intersection and union of $[2, 5]$ and $[-1, +\infty)$.
(b) Determine the intersection and union of $[2, 5]$ and $[3.4, +\infty)$.
(c) Determine the intersection and union of $[2, 5]$ and $[7, +\infty)$.

Now let a, b and c be real numbers with $a < b$.

(d) Explain why the intersection of $[a, b]$ and $[c, +\infty)$ is either a closed interval, a set with one element, or the empty set.
(e)Explain why the union of $[a, b]$ and $[c, +\infty)$ is either a closed ray or the union of a closed interval and a closed ray.

17. **Proof of Theorem 5.5.** To help with the proof by induction of Theorem 5.5, we first prove the following lemma. (The idea for the proof of this lemma was illustrated with the discussion of power set after the definition on page 222.)

Lemma 5.6

Let A and B be subsets of some universal set. If $A = B \cup \{x\}$, where $x \notin B$, then any subset of A is either a subset of B or a set of the form $C \cup \{x\}$, where C is a subset of B.

Proof

Let A and B be subsets of some universal set, and assume that $A = B \cup \{x\}$ where $x \notin B$. Let Y be a subset of A. We need to show that Y is a subset of B or that $Y = C \cup \{x\}$, where C is some subset of B. There are two cases to consider: (1) x is not an element of Y, and (2) x is an element of Y.

Case 1: Assume that $x \notin Y$. Let $y \in Y$. Then. $y \in A$ and $y \neq x$. Since

$$A = B \cup \{x\},$$

this means that y must be in B. Therefore, $Y \subseteq B$.

Case 2: Assume that $x \in Y$. In this case, let $C = Y - \{x\}$. Then every element of C is an element of B. Hence, we can conclude that $C \subseteq B$ and that $Y = C \cup \{x\}$.

Cases (1) and (2) show that if $Y \subseteq A$, then $Y \subseteq B$ or $Y = C \cup \{x\}$, where $C \subseteq B$.

To begin the induction proof of Theorem 5.5, for each nonnegative integer n, we let $P(n)$ be, "If a finite set has exactly n elements, then that set has exactly 2^n subsets."

(a) Verify that $P(0)$ is true. (This is the basis step for the induction proof.)
(b) Verify that $P(1)$ and $P(2)$ are true.
(c) Now assume that k is a nonnegative integer and assume that $P(k)$ is true. That is, assume that if a set has k elements, then that set has 2^k subsets. (This is the inductive assumption for the induction proof.) Let T be a subset of the universal set with $\text{card}(T) = k+1$, and let $x \in T$. Then the set $B = T - \{x\}$ has k elements.

Now use the inductive assumption to determine how many subsets B has. Then use Lemma 5.6 to prove that T has twice as many subsets as B. This should help complete the inductive step for the induction proof.

Answer

Add texts here. Do not delete this text first.

5.2: Proving Set Relationships

Preview Activity 5.2.1: Working with Two Specific Sets

Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers.

1. List at least four different positive elements of S and at least four different negative elements of S. Are all of these integers even?
2. Use the roster method to specify the sets S and T. (See Section 2.3 for a review of the roster method.) Does there appear to be any relationship between these two sets? That is, does it appear that the sets are equal or that one set is a subset of the other set?
3. Use set builder notation to specify the sets S and T. (See Section 2.3 for a review of the set builder notation.)
4. Using appropriate definitions, describe what it means to say that an integer x is a multiple of 6 and what it means to say that an integer y is even.
5. In order to prove that S is a subset of T, we need to prove that for each integer x, if $x \in S$, then $x \in T$.

   Complete the know-show table in Table 5.1 for the proposition that S is a subset of T.

   This table is in the form of a proof method called the **choose-an-element method**. This method is frequently used when we encounter a universal quantifier in a statement in the backward process. (In this case, this is Step $Q1$.) The key is that we have to prove something about all elements in $\mathbb{Z}$. We can then add something to the forward process by choosing an arbitrary element from the set S. (This is done in Step $P1$.) This does not mean that we can choose a specific element of S. Rather, we must give the arbitrary element a name and use only the properties it has by being a member of the set S. In this case, the element is a multiple of 6.

Table 5.1: Know-show table for Preview Activity 5.2.1

Step	Know	Reason
P	S is the set of all integers that are multiples of 6. T is the set of all even. integers.	Hypothesis
$P1$	Let $x \in S$.	Choose an arbitrary element of S.
$P2$	$(\exists m \in \mathbb{Z})(x = 6m)$	Definition of "multiple"
...	...	...
$Q2$	x is an element T.	x is even
$Q1$	$(\forall x \in \mathbb{Z})[(x \in S) \rightarrow (x \in T)]$	Step $P1$ and Step $Q2$
Q	$S \subseteq T$.	Definition of "subset"
Step	**Show**	**Reason**

Preview Activity 5.2.2: Working with Venn Diagrams

1. Draw a Venn diagram for two sets, A and B, with the assumption that A is a subset of B. On this Venn diagram, lightly shade the area corresponding to A^c. Then, determine the region on the Venn diagram that corresponds to B^c. What appears to be the relationship between A^c and B^c? Explain.
2. Draw a general Venn diagram for two sets, A and B. First determine the region that corresponds to the set $A - B$ and then, on the Venn diagram, shade the region corresponding to $A - (A - B)$ and shade the region corresponding to $A \cap B$. What appears to be the relationship between these two sets? Explain.

In this section, we will learn how to prove certain relationships about sets. Two of the most basic types of relationships between sets are the equality relation and the subset relation. So if we are asked a question of the form, “How are the sets A and B related?”, we can answer the question if we can prove that the two sets are equal or that one set is a subset of the other set. There are other ways to answer this, but we will concentrate on these two for now. This is similar to asking a question about how two real

numbers are related. Two real numbers can be related by the fact that they are equal or by the fact that one number is less than the other number.

The Choose-an-Element Method

The method of proof we will use in this section can be called the **choose-an-element method**. This method was introduced in Preview Activity 5.2.1. This method is frequently used when we encounter a universal quantifier in a statement in the backward process. This statement often has the form

For each element with a given property, something happens.

Since most statements with a universal quantifier can be expressed in the form of a conditional statement, this statement could have the following equivalent form:

If an element has a given property, then something happens.

We will illustrate this with the proposition from Preview Activity 5.2.1. This proposition can be stated as follows:

> *Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers. Then S is a subset of T.*

In Preview Activity 5.2.1, we worked on a know-show table for this proposition. The key was that in the backward process, we encountered the following statement:

> Each element of S is an element of T or, more precisely, if $x \in S$, then $x \in T$.

In this case, the "element" is an integer, the "given property" is that it is an element of S, and the "something that happens" is that the element is also an element of T. One way to approach this is to create a list of all elements with the given property and verify that for each one, the "something happens." When the list is short, this may be a reasonable approach. However, as in this case, when the list is infinite (or even just plain long), this approach is not practical.

We overcome this difficulty by using the **choose-an-element method**, where we choose an arbitrary element with the given property. So in this case, we choose an integer x that is a multiple of 6. We cannot use a specific multiple of 6 (such as 12 or 24), but rather the only thing we can assume is that the integer satisfies the property that it is a multiple of 6. This is the key part of this method.

> *Whenever we choose an arbitrary element with a given property, we are not selecting a specific element. Rather, the only thing we can assume about the element is the given property.*

It is important to realize that once we have chosen the arbitrary element, we have added information to the forward process. So in the know-show table for this proposition, we added the statement, "Let $x \in S$" to the forward process. Following is a completed proof of this proposition following the outline of the know-show table from Preview Activity 5.2.1.

Proposition 5.7

Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers. Then S is a subset of T.

Proof

Let S be the set of all integers that are multiples of 6, and let T be the set of all even integers. We will show that S is a subset of T by showing that if an integer x is an element of S, then it is also an element of T.

Let $x \in S$. (**Note**: The use of the word "let" is often an indication that the we are choosing an arbitrary element.) This means that x is a multiple of 6. Therefore, there exists an integer m such that

$$x = 6m.$$

Since $6 = 2 \cdot 3$, this equation can be written in the form

$$x = 2(3m).$$

By closure properties of the integers, 3m is an integer. Hence, this last equation proves that x must be even. Therefore, we have shown that if x is an element of S, then x is an element of T, and hence that $S \subseteq T$.

Having proved that S is a subset of T, we can now ask if S is actually equal to T. The work we did in Preview Activity $5.2.1$ can help us answer this question. In that preview activity, we should have found several elements that are in T but not in S. For example, the integer 2 is in T since 2 is even but $2 \notin S$ since 2 is not a multiple of 6. Therefore, $S \neq T$ and we can also conclude that S is a proper subset of T.

One reason we do this in a "two-step" process is that it is much easier to work with the subset relation than the proper subset relation. The subset relation is de- fined by a conditional statement and most of our work in mathematics deals with proving conditional statements. In addition, the proper subset relation is a conjunction of two statements ($S \subseteq T$ and $S \neq T$) and so it is natural to deal with the two parts of the conjunction separately.

? Progress Check 5.8: Subsets and Set Equality

Let $A = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 9\}$ and let $B = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 3\}$

1. Is the set A a subset of B? Justify your conclusion.
2. Is the set A equal to the set B? Justify your conclusion.

Answer

Add texts here. Do not delete this text first.

? Progress Check 5.9: Using the Choose-an-Element Method

The Venn diagram in Preview Activity $5.2.2$ suggests that the following proposition is true.

Proposition 5.10.

Let A and B be subsets of the universal set U. If $A \subseteq B$, then $B^c \subseteq A^c$.

1. The conclusion of the conditional statement is $B^c \subseteq A^c$. Explain why we should try the choose-an-element method to prove this proposition.
2. Complete the following know-show table for this proposition and explain exactly where the choose-an-element method is used.

Step	Know	Reason
P	$A \subseteq B$	Hypothesis
$P1$	Let $x \in B^c$.	Choose an arbitrary element of B^c.
$P2$	If $x \in A$, then $x \in B$.	Definition of "subset"
...	...	...
$Q1$	If $x \in B^c$, then $x \in A^c$.	
Q	$B^c \subseteq A^c$	Definition of "subset"
Step	**Show**	**Reason**

Answer

Add texts here. Do not delete this text first.

Proving Set Equality

One way to prove that two sets are equal is to use Theorem 5.2 and prove each of the two sets is a subset of the other set. In particular, let A and B be subsets of some universal set. Theorem 5.2 states that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

In Preview Activity $5.2.2$, we created a Venn diagram that indicated that $A - (A - B) = A \cap B$. Following is a proof of this result. Notice where the choose-an-element method is used in each case.

Proposition 5.11.

Let A and B be subsets of some universal set. Then $A-(A-B)=A\cap B$.

Proof

Let A and B be subsets of some universal set. We will prove that $A-(A-B)=A\cap B$ by proving that $A-(A-B)\subseteq A\cap B$ and that $A\cap B\subseteq A-(A-B)$.

First, let $x\in A-(A-B)$. This means that

$$x\in A \text{ and } x\notin (A-B)\,.$$

We know that an element is in $(A-B)$ if and only if it is in A and not in B. Since $x\notin (A-B)$, we conclude that $x\notin A$ or $x\in B$. However, we also know that $x\in A$ and so we conclude that $x\in B$. This proves that

$$x\in A \text{ and } x\in B.$$

This means that $x\in A\cap B$, and hence we have proved that $A-(A-B)\subseteq A\cap B$.

Now we choose $y\in A\cap B$. This means that

$$y\in A \text{ and } y\in B.$$

We note that $y\in (A-B)$ if and only if $y\in A$ and $y\notin B$ and hence, $y\notin (A-B)$ if and only if $y\notin A$ or $y\in B$. Since we have proved that $y\in B$, we conclude that $y\notin (A-B)$, and hence, we have established that $y\in A$ and $y\notin (A-B)$. This proves that if $y\in A\cap B$, then $y\in A-(A-B)$ and hence, $A\cap B\subseteq A-(A-B)$.

Since we have proved that $A-(A-B)\subseteq A\cap B$ and $A\cap B\subseteq A-(A-B)$ we conclude that $A-(A-B)=A\cap B$.

Progress Check 5.12: Set Equality

Prove the following proposition. To do so, prove each set is a subset of the other set by using the choose-an-element method.

Proposition 5.13.

Let A and B be subsets of some universal set. Then $A-B=A\cap B^c$.

Answer

Add texts here. Do not delete this text first.

Disjoint Sets

Earlier in this section, we discussed the concept of set equality and the relation of one set being a subset of another set. There are other possible relationships between two sets; one is that the sets are disjoint. Basically, two sets are disjoint if and only if they have nothing in common. We express this formally in the following definition.

Definition: disjoint

Let A and B be subsets of the universal set U. The sets A and B are said to be *disjoint* provided that $A\cap B=\emptyset$.

For example, the Venn diagram in Figure 5.5 shows two sets A and B with $A\subseteq B$. The shaded region is the region that represents B^c. From the Venn diagram, it appears that $A\cap B^c=\emptyset$. This means that A and B^c are disjoint. The preceding example suggests that the following proposition is true:

$$\text{If } A\subseteq B, \text{ then } A\cap B^c=\emptyset\,.$$

If we would like to prove this proposition, a reasonable "backward question" is, "How do we prove that a set (namely $A\cap B^c$) is equal to the empty set?"

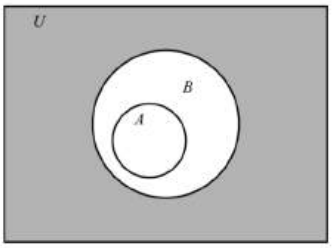


Figure 5.5: Venn Diagram with $A \subseteq B$

This question seems difficult to answer since how do we prove that a set is empty? This is an instance where proving the contrapositive or using a proof by contradiction could be reasonable approaches. To illustrate these methods, let us assume the proposition we are trying to prove is of the following form:

$$\text{If } P, \text{ then } T = \emptyset.$$

If we choose to prove the contrapositive or use a proof by contradiction, we will assume that $T \neq \emptyset$. These methods can be outlined as follows:

- The contrapositive of "If P, then $T = \emptyset$" is, "If $T \neq \emptyset$, then $\neg P$." So in this case, we would assume $T \neq \emptyset$ and try to prove $\neg P$.
- Using a proof by contradiction, we would assume P and assume that $T \neq \emptyset$. From these two assumptions, we would attempt to derive a contradiction.

One advantage of these methods is that when we assume that $T \neq \emptyset$, then we know that there exists an element in the set T. We can then use that element in the rest of the proof. We will prove one of th the conditional statements for Proposition 5.14 by proving its contrapositive. The proof of the other conditional statement associated with Proposition 5.14 is Exercise (10).

Proposition 5.14

Let A and B be subsets of some universal set. Then $A \subseteq B$ if and only if $A \cap B^c = \emptyset$.

Proof

Let A and B be subsets of some universal set. We will first prove that if $A \subseteq B$, then $A \cap B^c = \emptyset$, by proving its contrapositive. That is, we will prove

$$\text{If } A \cap B^c \neq \emptyset \text{ , then } A \nsubseteq B.$$

So assume that $A \cap B^c \neq \emptyset$. We will prove that $A \nsubseteq B$ by proving that there must exist an element x such that $x \in A$ and $x \notin B$.

Since $A \cap B^c \neq \emptyset$, there exists an element x that is in $A \cap B^c$. This means that

$$x \in A \text{ and } x \in B^c.$$

Now the fact that $x \in B^c$ means that $x \notin B$. Hence, we can conclude that

$$x \in A \text{ and } x \notin B.$$

This means that $A \nsubseteq B$, and hence, we have proved that if $A \cap B^c \neq \emptyset$, then $A \nsubseteq B$, and therefore, we have proved that if $A \subseteq B$, then $A \cap B^c = \emptyset$.

The proof that if $A \cap B^c = \emptyset$, then $A \subseteq B$ is Exercise (10).

? Progress Check 5.15: Proving Two Sets Are Disjoint

It has been noted that it is often possible to prove that two sets are disjoint by using a proof by contradiction. In this case, we assume that the two sets are not disjoint and hence, there intersection is not empty. Use this method to prove that the following two sets are disjoint.

$A = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{12}\}$ and $B = \{y \in \mathbb{Z} \mid y \equiv 2 \pmod{8}\}$

Answer

Add texts here. Do not delete this text first.

A Final Comment

We have used the choose-an-element method to prove Propositions 5.7, 5.11, and 5.14. Proofs involving sets that use this method are sometimes referred to **aselement-chasing proofs**. This name is used since the basic method is to choose an arbitrary element from one set and "chase it" until you prove it must be in another set.

? Exercises for Section 5.2

1. Let $A = \{x \in \mathbb{R} \mid x^2 < 4\}$ and let $B = \{x \in \mathbb{R} \mid x < 2\}$

   (a) Is $A \subseteq B$? Justify your conclusion with a proof or a counterexample.
   (b) Is $B \subseteq A$? Justify your conclusion with a proof or a counterexample.
2. Let A, B, and C be subsets of a universal set U.

   (a) Draw a Venn diagram with $A \subseteq B$ and $B \subseteq C$. Does it appear that $A \subseteq C$?
   (b) Prove the following proposition:
   If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.
   Note: This may seem like an obvious result. However, one of the reasons for this exercise is to provide practice at properly writing a proof that one set is a subset of another set. So we should start the proof by assuming that $A \subseteq B$ and $B \subseteq C$. Then we should choose an arbitrary element of A.
3. Let $A = \{x \in \mathbb{Z} \mid x \equiv 7 \pmod 8\}$ and $B = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod 4\}$.

   (a) List at least five different elements of the set A and at least five elements of the set B.
   (b) Is $A \subseteq B$? Justify your conclusion with a proof or a counterexample.
   (c) Is $B \subseteq A$? Justify your conclusion with a proof or a counterexample.
4. Let $C = \{x \in \mathbb{Z} \mid x \equiv 7 \pmod 9\}$ and $D = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\}$.

   (a) List at least five different elements of the set C and at least five elements of the set D.
   (b) Is $C \subseteq D$? Justify your conclusion with a proof or a counterexample.
   (c) Is $D \subseteq C$? Justify your conclusion with a proof or a counterexample.
5. In each case, determine if $A \subseteq B$, $B \subseteq A$, $A = B$, or $A \cap B = \emptyset$ or none of these.

   (a) $A = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 3\}$ and $B = \{y \in \mathbb{Z} \mid 6 \text{ divides } (2y - 4)\}$.
   (b) $A = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod 4\}$ and $B = \{y \in \mathbb{Z} \mid 3 \text{ divides } (y - 2)\}$.
   (c) $A = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 5\}$ and $B = \{x \in \mathbb{Z} \mid y \equiv 7 \pmod{10}\}$
6. To prove the following set equalities, it may be necessary to use some of the properties of positive and negative real numbers. For example, it may be necessary to use the facts that:

   • The product of two real numbers is positive if and only if the two real numbers are either both positive or are both negative.

   • The product of two real numbers is negative if and only if one of the two numbers is positive and the other is negative.

   For example, if $x(x - 2) < 0$, then we can conclude that either (1) $x < 0$ and $x - 2 > 0$ or (2) $x > 0$ and $x - 2 < 0$. However, in the first case, we must have $x < 0$ and $x > 2$, and this is impossible. Therefore, we conclude that $x > 0$ and $x - 2 < 0$, which means that $0 < x < 2$.

   Use the choose-an-element method to prove each of the following:

   (a) $\{x \in \mathbb{R} \mid x^2 - 3x - 10 < 0\} = \{x \in \mathbb{R} \mid -2 < x < 5\}$

(b) $\{x \in \mathbb{R} \mid x^2 - 5x + 6 < 0\} = \{x \in \mathbb{R} \mid 2 < x < 3\}$
(c) $\{x \in \mathbb{R} \mid x^2 \geq 4\} = \{x \in \mathbb{R} \mid x \leq -2\}\ cup\{x \in \mathbb{R} \mid x \geq 2\}$

7. Let A and B be subsets of some universal set U. Prove each of the following:

   (a) $A \cap B \subseteq A$
   (b) $A \subseteq A \cup B$
   (c) $A \cap A = A$
   (d) $A \cup A = A$
   (e) $A \cap \emptyset = \emptyset$
   (f) $A \cup \emptyset = A$
8. Let A and B be subsets of some universal set U. From Proposition 5.10, we know that if $A \subseteq B$, then $B^c \subseteq A^c$. Now prove the following proposition:

   For all sets (A\) and B be subsets of some universal set U, $A \subseteq B$ if and only if $B^c \subseteq A^c$.
9. Is the following proposition true or false? Justify your conclusion with a proof or a counterexample.

   For all sets (A\) and B be subsets of some universal set U, the sets $A \cap B$ and $A - B$ are disjoint.
10. Complete the proof of Proposition 5.14 by proving the following conditional statement:

    Let (A\) and B be subsets of some universal set. If $A \cap B^c = \emptyset$, then $A \subseteq B$.
11. Let A, B, C, and D be subsets of some universal set U. Are the following propositions true or false? Justify your conclusions.

    (a) If $A \subseteq B$ and $C \subseteq D$ and A and C are disjoint, then B and D are disjoint.
    (b) If $A \subseteq B$ and $C \subseteq D$ and B and D are disjoint, then A and C are disjoint.
12. Let A, B, and C be subsets of a universal set U. Prove:

    (a) If $A \subseteq B$, then $A \cap C \subseteq B \cap C$.
    (b) If $A \subseteq B$, then $A \cup C \subseteq B \cup C$.
13. Let A, B, and C be subsets of a universal set U. Are the following propositions true or false? Justify your conclusions.

    (a) If $A \cap C \subseteq B \cap C$, then $A \subseteq B$.
    (b) If $A \cup C \subseteq B \cup C$, then $A \subseteq B$.
    (c) If $A \cup C = B \cup C$, then $A = B$.
    (d) If $A \cap C = B \cup C$, then $A = B$.
    (e) If $A \cup C = B \cup C$ and $A \cap C = B \cap C$, then $A = B$.
14. Prove the following proposition:

    For all sets A, B, and C that are subsets of some universal set, if $A \cap B = A \cap C$ and $A^c \cap B = A^c \cap C$, then $B = C$.
15. Are the following biconditional statements true or false? Justify your conclusion. If a biconditional statement is found to be false, you should clearly determine if one of the conditional statements within it is true and provide a proof of this conditional statement.

    (a) For all subsets A and B of some universal set U, $A \subseteq B$ if and only if $A \cap B^c = \emptyset$.
    (b) For all subsets A and B of some universal set U, $A \subseteq B$ if and only if $A \cup B = B$.
    (c) For all subsets A and B of some universal set U, $A \subseteq B$ if and only if $A \cap B = A$.
    (d) For all subsets A, B, and C of some universal set U, $A \subseteq B \cup C$ if and only if $A \subseteq B$ or $A \subseteq C$.
    (e) For all subsets A, B, and C of some universal set U, $A \subseteq B \cup C$ if and only if $A \subseteq B$ and $A \subseteq C$.
16. Let S, T, X, and Y be subsets of some universal set. Assume that

    (i) $S \cup T \subseteq X \cup Y$; (ii) $S \cap T = \emptyset$; and (iii) $X \subseteq S$.

(a) Using assumption (i), what conclusion(s) can be made if it is known that $a \in T$?
(b) Using assumption (ii), what conclusion(s) can be made if it is known that $a \in T$?
(c) Using all three assumptions, either prove that $T \subseteq Y$ or explain why it is not possible to do so.

17. **Evaluation of Proofs**
See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

Let A, B, and C be subsets of some universal set. If $A \nsubseteq B$ and $B \nsubseteq C$, then $A \nsubseteq C$.

Proof

We assume that A, B, and C be subsets of some universal set and that $A \nsubseteq B$ and $B \nsubseteq C$. This means that there exists an element x in A that is not in B and there exists an element x that is in B and not in C. Therefore, $x \in A$ and $x \notin C$, and we have proved that $A \nsubseteq C$.

(b)

Let A, B, and C be subsets of some universal set. If $A \cap B = A \cap C$, then $B = C$.

Proof

We assume that $A \cap B = A \cap C$ and prove that $B = C$. We will first prove that $B \subseteq C$.

So let $x \in B$. If $x \in A$, then $x \in A \cap B$, and hence, $x \in A \cap C$. From this we can conclude that $x \in C$. If $x \notin A$, then $x \notin A \cap B$, and hence, $x \notin A \cap C$. However, since $x \notin A$, we may conclude that $x \in C$. Therefore, $B \subseteq C$.

The proof that $C \subseteq B$ may be done in a similar manner. Hence, $B = C$.

Let A, B, and C be subsets of some universal set. If $A \nsubseteq B$ and $B \subseteq C$, then $A \nsubseteq C$.

Proof

Assume that $A \nsubseteq B$ and $B \subseteq C$. Since $A \nsubseteq B$, there exists an element x such that $x \in A$ and $x \notin B$. Since $B \subseteq C$, we may conclude that $x \notin C$. Hence, $x \in A$ and $x \notin C$, and we have proved that $A \nsubseteq C$.

Explorations and Activities

18. Using the Choose-an-Element Method in a Different Setting. We have used the choose-an-element method to prove results about sets. This method, however, is a general proof technique and can be used in settings other than set theory. It is often used whenever we encounter a universal quantifier in a statement in the backward process. Consider the following proposition.

Proposition 5.16.

Let a, b and t be integers with $t \neq 0$. If t divides a and t divides b, then for all integers x and y, t divides $(ax + by)$.

(a) Whenever we encounter a new proposition, it is a good idea to explore the proposition by looking at specific examples. For example, let $a = 20$, $b = 12$, and $t = 4$. In this case, $t \mid a$ and $t \mid b$. In each of the following cases, determine the value of $(ax + by)$ and determine if t divides $(ax + by)$.

i. $x = 1, y = 1$.
ii. $x = 1, y = -1$.
iii. $x = 2, y = 2$.
iv. $x = 2, y = -3$.

v. $x = -2$, $y = 3$.
vi. $x = -2$, $y = -5$.

(b) Repeat Part (18a) with $a = 21$, $b = 6$, and $t = 3$.

Notice that the conclusion of the conditional statement in this proposition involves the universal quantifier. So in the backward process, we would have

Q: For all integers x and y, t divides $ax + by$.

The "elements" in this sentence are the integers x and y. In this case, these integers have no "given property" other than that they are integers. The "something that happens" is that t divides $(ax + by)$. This means that in the forward process, we can use the hypothesis of the proposition and choose integers x and y. That is, in the forward process, we could have

P: a, b, and t are integers with $t \neq 0$, t divides a and t divides b.

$P1$: Let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$.

(c) Complete the following proof of Proposition 5.16.

Proof. Let a, b and t be integers with $t \neq 0$, and assume that t divides a and t divides b. We will prove that for all integers x and y, t dibides $(ax + by)$.

So let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$. Since t divides a, there exists an integer m such that ... .

Answer

Add texts here. Do not delete this text first.

5.3: Properties of Set Operations

? PREVIEW ACTIVITY 5.3.1: Exploring a Relationship between Two Sets

Let A and B be subsets of some universal set U.

1. Draw two general Venn diagrams for the sets A and B. On one, shade the region that represents $(A \cup B)^c$, and on the other, shade the region that represents $A^c \cap B^c$. Explain carefully how you determined these regions.
2. Based on the Venn diagrams in Part (1), what appears to be the relationship between the sets ((A \cup B)^c\) and $A^c \cap B^c$?

Some of the properties of set operations are closely related to some of the logical operators we studied in Section 2.1. This is due to the fact that set intersection is defined using a conjunction (and), and set union is defined using a disjunction (or). For example, if A and B are subsets of some universal set U, then an element x is in $A \cup B$ if and only if $x \in A$ or $x \in B$.

3. Use one of De Morgan's Laws (Theorem 2.8 on page 48) to explain carefully what it means to say that an element x is not in $A \cup B$.
4. What does it mean to say that an element x is in A^c? What does it mean to say that an element x is in B^c?
5. Explain carefully what it means to say that an element x is in $A^c \cap B^c$.
6. Compare your response in Part (3) to your response in Part (5). Are they equivalent? Explain.
7. How do you think the sets $(A \cup B)^c$ and $A^c \cap B^c$ are related? Is this consistent with the Venn diagrams from Part (1)?

? PREVIEW ACTIVITY 5.3.2: Proving that Statements Are Equivalent

1. Let X, Y, and Z be statements. Complete a truth table for $[(X \to Y) \wedge (Y \to Z)] \to (X \to Z)$.
2. Assume that P, Q, and R are statements and that we have proven that the following conditional statements are true:

   - If P then $Q (P \to Q)$.
   - If R then $P (R \to P)$.
   - If Q then $R (Q \to R)$.

   Explain why each of the following statements is true.

   (a) P if and only if $Q (P \leftrightarrow Q$.
   (b) Q if and only if $R (Q \leftrightarrow R$.
   (c) R if and only if $P (R \leftrightarrow P$.
   Remember that $X \leftrightarrow Y$ is logically equivalent to $(X \to Y) \wedge (Y \to X)$.

Algebra of Sets – Part 1

This section contains many results concerning the properties of the set operations. We have already proved some of the results. Others will be proved in this section or in the exercises. The primary purpose of this section is to have in one place many of the properties of set operations that we may use in later proofs. These results are part of what is known as the **algebra of sets** or as **set theory**.

Theorem 5.17

Let A, B, and C be subsets of some universal set U. Then

- $A \cap B \subseteq A$ and $A \subseteq A \cup B$.
- If $A \subseteq B$, then $A \cap C \subseteq B \cap C$ and $A \cup C \subseteq B \cup C$.

Proof

The first part of this theorem was included in Exercise (7) from Section 5.2. The second part of the theorem was Exercise (12) from Section 5.2.

The next theorem provides many of the properties of set operations dealing with intersection and union. Many of these results may be intuitively obvious, but to be complete in the development of set theory, we should prove all of them. We choose to prove only some of them and leave some as exercises.

Theorem 5.18: Algebra of Set Operations

Let A, B, and C be subsets of some universal set U. Then all of the following equalities hold.

Proporties of the Empty Set $A \cap \emptyset = \emptyset$ $A \cap U = A$ and the Universal Set $A \cup \emptyset = A$ $A \cup U = U$

Idempotent Laws $A \cap A = A$ $A \cup A = A$

Commutative Laws $A \cap B = B \cap A$ $A \cup B = B \cup A$

Associative Laws $(A \cap B) \cap C = A \cap (B \cap C)$
$(A \cup B) \cup C = A \cup (B \cup C)$

Distributive Laws $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Before proving some of these properties, we note that in Section 5.2, we learned that we can prove that two sets are equal by proving that each one is a subset of the other one. However, we also know that if S and T are both subsets of a universal set U, then

$S = T$ if and only if for each $x \in U$, $x \in S$ if and only if $x \in T$.

We can use this to prove that two sets are equal by choosing an element from one set and chasing the element to the other set through a sequence of "if and only if" statements. We now use this idea to prove one of the commutative laws.

Proof of One of the Commutative Laws in Theorem 5.18

We will prove that $A \cap B = B \cap A$. Let $x \in A \cap B$. Then

$$x \in A \cap B \text{ if and only if } x \in A \text{ and } x \in B. \tag{5.3.1}$$

However, we know that if P and Q are statements, then $PwedgeQ$ is logically equivalent to $Q \wedge P$. Consequently, we can conclude that

$$x \in A \text{ and } x \in B \text{ if and only if } x \in B \text{ and } x \in A. \tag{5.3.2}$$

Now we know that

$$x \in B \text{ and } x \in A \text{ if and only if } x \in B \cap A. \tag{5.3.3}$$

This means that we can use (5.3.1), (5.3.2) and (5.3.3) to conclude that

$$x \in A \cap B \text{ if and only if } x \in B \cap A,$$

and, hence, we have proved that $A \cap B = B \cap A$.

□

Progress Check 5.19: Exploring a Distributive Property

We can use Venn diagrams to explore the more complicated properties in Theorem 5.18, such as the associative and distributive laws. To that end, let A, B, and C be subsets of some universal set U.

1. Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A \cup (B \cap C$, and on the other, shade the region that represents $(A \cup B) \cap (A \cup C)$. Explain carefully how you determined these regions.
2. Based on the Venn diagrams in Part (1), what appears to be the relationship between the sets $A \cup (B \cap C$ and $(A \cup B) \cap (A \cup C)$?

Answer

Add texts here. Do not delete this text first.

Proof of One of the Distributive Laws in Theorem 5.18

We will now prove the distributive law explored in Progress Check 5.19. Notice that we will prove two subset relations, and that for each subset relation, we will begin by choosing an arbitrary element from a set. Also notice how nicely a proof dealing with the union of two sets can be broken into cases.

Proof. Let A, B, and C be subsets of some universal set U. We will prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ by proving that each set is a subset of the other set.

We will first prove that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C$. We let $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$.

So in one case, if $x \in A$, then $x \in A \cup B$ and $x \in A \cup C$. This means that $x \in (A \cup B) \cap (A \cup C)$.

On the other hand, if $x \in B \cap C$, then $x \in B$ and $x \in C$. But $x \in B$ implies that $x \in A \cup B$, and $x \in C$ implies that $x \in A \cup C$. Since x is in both sets, e conclude that $x \in (A \cup B) \cap (A \cup C)$. So in both cases, we see that $x \in (A \cup B) \cap (A \cup C)$, and this proves that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C$.

We next prove that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. So let $y \in (A \cup B) \cap (A \cup C)$. Then, $y \in A \cup B$ and $y \in A \cup C$. We must prove that $y \in A \cup (B \cap C)$. We will consider the two cases where $y \in A$ or $y \notin A$. In the case where $y \in A$, we see that $y \in A \cup (B \cap C)$.

So we consider the case that $y \notin A$. It has been established that $y \in A \cup B$ and $y \in A \cup C$. Since $yinA$ and $y \in A \cup B$, y must be an element of B. Similarly, since $y \notin A$ and $y \in A \cup C$, y must be an element of C. Thus, $y \in B \cap C$ and, hence, $y \in A \cup (B \cap C)$.

In both cases, we have proved that $y \in A \cup (B \cap C)$. This proves that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. The two subset relations establish the equality of the two sets. Thus, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

square

Important Properties of Set Complements

The three main set operations are union, intersection, and complementation. The- orems 5.18 and 5.17 deal with properties of unions and intersections. The next theorem states some basic properties of complements and the important relations dealing with complements of unions and complements of intersections. Two relationships in the next theorem are known as **De Morgan's Laws** for sets and are closely related to De Morgan's Laws for statements.

Theorem 5.20

Let A, B, and C be subsets of some universal set U. Then the following are true:

Basic Properties $(A^c)^c = A$
$A - B = A \cap B^c$

Empty Set and Universal Set $A - \emptyset = A$ and $A - U = \emptyset$
$\emptyset^c = U$ and $U^c = \emptyset$

De Morgan's Laws $(A \cap B)^c = A^c \cup B^c$
$(A \cup B)^c = A^c \cap B^c$

Subsets and Complements $A \subseteq B$ if and only if $B^c \subseteq A^c$

Proof

We will only prove one of De Morgan's Laws, namely, the one that was explored in Preview Activity 5.3.1. The proofs of the other parts are left as exercises. Let A and B be subsets of some universal set U. We will prove that $(A \cup B)^c = A^c \cap B^c$ by proving that an element is in $(A \cup B)^c$ if and only if it is in $A^c \cap B^c$. So let x be in the universal set U. Then

$$x \in (A \cup B)^c \text{ if and only if } x \notin A \cup B. \tag{5.3.4}$$

and

$$x \notin A \cup B \text{ if and only if } x \notin A \text{ and } x \notin B. \tag{5.3.5}$$

Combining (5.3.4) and (5.3.5), we see that

$$x \in (A \cup B)^c \text{ if and only if } x \notin A \text{ and } x \notin B. \tag{5.3.6}$$

In addition, we know that

$$x \notin A \text{ and } x \notin B \text{ if and only if } x \in A^c \text{ and } x \in B^c. \tag{5.3.7}$$

and this is true if and only if $x \in A^c \cap B^c$. So we can use (5.3.6) and (5.3.7) to conclude that

$x \in (A \cup B)^c$ if and only if $x \in A^c \cap B^c$.

and, hence, that $(A \cup B)^c = A^c \cap B^c$.

□

? Progress Check 5.21: Using the Algebra of Sets

1. Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $(A \cup B) - C$, and on the other, shade the region that represents $(A - C) \cup (B - C)$. Explain carefully how you determined these regions and why they indicate that $(A \cup B) - C = (A - C) \cup (B - C)$.

It is possible to prove the relationship suggested in Part (1) by proving that each set is a subset of the other set. However, the results in Theorems 5.18 and 5.20 can be used to prove other results about set operations. When we do this, we say that we are using the algebra of sets to prove the result. For example, we can start by using one of the basic properties in Theorem 5.20 to write

$$A \cup B) - C = (A \cup B) \cap C^c \quad .$$

We can then use one of the commutative properties to write

$$\begin{aligned} (A \cup B) - C &= (A \cup B) \cap C^c \\ &= C^c \cap (A \cup B). \end{aligned} \tag{5.3.8}$$

2. Determine which properties from Theorems 5.18 and 5.20 justify each of the last three steps in the following outline of the proof that $(A \cup B) - C = (A - C) \cup (B - C)$.

$$\begin{aligned} (A \cup B) - C &= (A \cup B) \cap C^c && \text{(Theorem 5.20)} \\ &= C^c \cap (A \cup B) && \text{(Commutative Property)} \\ &= (C^c \cap A) \cup (C^c \cap B) \\ &= (A \cap C^c) \cup (B \cap C^c) \\ &= (A - C) \cup (B - C) \end{aligned} \tag{5.3.9}$$

Note: It is sometimes difficult to use the properties in the theorems when the theorems use the same letters to represent the sets as those being used in the current problem. For example, one of the distributive properties from Theorems 5.18 can be written as follows: For all sets X, Y, and Z that are subsets of a universal set U,

$$(X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Answer

Add texts here. Do not delete this text first.

Proving that Statements Are Equivalent

When we have a list of three statements P , Q, and R such that each statement in the list is equivalent to the other two statements in the list, we say that the three statements are equivalent. This means that each of the statements in the list implies each of the other statements in the list.

The purpose of Preview Activity 5.3.2 was to provide one way to prove that three (or more) statements are equivalent. The basic idea is to prove a sequence of conditional statements so that there is an unbroken chain of conditional statements from each

statement to every other statement. This method of proof will be used in Theorem 5.22.

Theorem 5.22

Let A and B be subsets of some universal set U. The following are equivalent:

1. $A \subseteq B$
2. $A \cap B^c = \emptyset$
3. $A^c \cup B = U$

Proof

To prove that these are equivalent conditions, we will prove that (1) implies (2), that (2) implies (3), and that (3) implies (1).

Let A and B be subsets of some universal set U. We have proved that (1) implies (2) in Proposition 5.14.

To prove that (2) implies (3), we will assume that $A \cap B^c = \emptyset$ and use the fact that $\emptyset^c = U$. We then see that

$(A \cap B^c)^c = \emptyset^c$.

Then, using one of De Morgan's Laws, we obtain

begin{array} {rcl} {A^c \cup (B^c)^c} &= & {U} \\ {A^c \cup B} &= & {U.} \end{array}

This completes the proof that (2) implies (3).

We now need to prove that (3) implies (1). We assume that $A^c \cup B = U$ and will prove that $A \subseteq B$ by proving that every element of A must be in B.

So let $x \in A$. Then we know that $x \notin A^c$. However, $x \in U$ and since $A^c \cup B = U$, we can conclude that $x \in A^c \cup B$. Since $x \notin A^c$, we conclude that $x \in B$. This proves that $A \subseteq B$ and hence that (3) implies (1).

Since we have now proved that (1) implies (2), that (2) implies (3), and that (3) implies (1), we have proved that the three conditions are equivalent.

Exercises for Section 5.3

1. Let A be a subset of some universal set U. Prove each of the following (from Theorem 5.20):

   (a) $(A^c)^c = A$
   (b) $A - \emptyset = A$
   (c) $\emptyset^c = U$
   (d) $U^c = \emptyset$
2. Let A, B, and C be subsets of some universal set U. As part of Theorem 5.18, we proved one of the distributive laws. Prove the other one. That is, prove that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \tag{5.3.10}$$

3. Let A, B, and C be subsets of some universal set U. As part of Theorem 5.20, we proved one of De Morgan's Laws. Prove the other one. That is, prove that

$$(A \cap B)^c = A^c \cup B^c. \tag{5.3.11}$$

4. Let A, B, and C be subsets of some universal set U.

   (a) Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A - (B \cup C)$, and on the other, shade the region that represents $(A - B) \cap (A - C)$. Based on the Venn diagrams, make a conjecture about the relationship between the sets $A - (B \cup C)$ and $(A - B) \cap (A - C)$.
   (b) Use the choose-an-element method to prove the conjecture from Exercise (4a).
   (c) Use the algebra of sets to prove the conjecture from Exercise (4a).

5. Let A, B, and C be subsets of some universal set U.

   (a) Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A-(B\cap C)$, and on the other, shade the region that represents $(A-B)\cup(A-C)$. Based on the Venn diagrams, make a conjecture about the relationship between the sets $A-(B\cap C)$ and $(A-B)\cup(A-C)$.
   (b) Use the choose-an-element method to prove the conjecture from Exercise (5a).
   (c) Use the algebra of sets to prove the conjecture from Exercise (5a).
6. Let A, B, and C be subsets of some universal set U. Prove or disprove each of the following:

   (a) $(A\cap B)-C=(A-C)\cap(B-C)$
   (b) $(A\cup B)-(A\cap B)=(A-B)\cup(B-A)$
7. Let A, B, and C be subsets of some universal set U.

   (a) Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A-(B-C)$, and on the other, shade the region that represents $(A-B)-C$. Based on the Venn diagrams, make a conjecture about the relationship between the sets $A-(B-C)$ and $(A-B)-C$.
   (b) Prove the conjecture from Exercise (7a).
8. Let A, B, and C be subsets of some universal set U.

   (a) Draw two general Venn diagrams for the sets A, B, and C. On one, shade the region that represents $A-(B-C)$, and on the other, shade the region that represents $(A-B)\cup(A-C^c)$. Based on the Venn diagrams, make a conjecture about the relationship between the sets $A-(B-C)$ and $(A-B)\cup(A-C^c)$.
   (b) Prove the conjecture from Exercise (8a).
9. Let A and B be subsets of some universal set U.

   (a) Prove that A and $B-A$ are disjoint sets.
   (b) Prove that $A\cup B=A\cup(B-A)$.
10. Let A and B be subsets of some universal set U.

    (a) Prove that $A-B$ and $A\cap B$ are disjoint sets.
    (b) Prove that $A=(A-B)\cup(A\cap B)$.
11. Let A and B be subsets of some universal set U. Prove or disprove each of the following:

    (a) $A-(A\cap B^c)=A\cap B$
    (b) $(A^c\cup B)^c\cap A=A-B$
    (c) $(A\cup B)-A=B-A$
    (d) $(A\cup B)-B=A-(A\cap B)$
    (e) $(A\cup B)-(A\cap B)=(A-B)\cup(B-A)$
12. **Evaluation of proofs**
    See the instructions for Exercise (19) on page 100 from Section 3.1.

    (a)

    Let A, B, and C be subsets of some universal set U, then $A-(B-C)=A-(B\cup C)$.

    Proof

$$\begin{aligned} A-(B-C) &= (A-B)-(A-C) \\ &= (A\cap B^c)\cap(A\cap C^c) \\ &= A\cap(B^c\cap C^c) \\ &= A\cap(B\cup C)^c \\ &= A-(B\cup C) \end{aligned} \tag{5.3.12}$$

Theorem 5.3.1

Let A, B, and C be subsets of some universal set U, then $A-(B\cup C)=(A-B)\cap(A-C)$.

Proof

We first write $A-(B\cup C)=A\cap(B\cup C)^c$ and then use one of De Morgan's Laws to obtain

$$A-(B\cup C)=A\cap(B^c\cap C^c) \quad .$$

We now use the fact that $A=A\cap A$ and obtain

$$\begin{aligned} A-(B\cup C) &= A\cap A\cap B^c\cap C^c \\ &= (A\cap B^c)\cap(A\cap C^c) \\ &= (A-B)\cap(A-C). \end{aligned} \tag{5.3.13}$$

Explorations and Activities

13. **(Comparison to Properties of the Real Numbers).** The following are some of the basic properties of addition and multiplication of real numbers

Commutative Laws: $a+b=b+a$, for all $a,b\in\mathbb{R}$.
$a\cdot b=b\cdot a$, for all $a,b\in\mathbb{R}$.

Associative Laws: $(a+b)+c=a+(b+c)$, for all $a,b,c\in\mathbb{R}$.
$(a\cdot b)\cdot c=a\cdot(b\cdot c)$, for all $a,b,c\in\mathbb{R}$.

Distributive Law: $a\cdot(b+c)=a\cdot b+a\cdot c$, for all $a,b,c\in\mathbb{R}$.

Additive Identity: For all $a\in\mathbb{R}$, $a+0=a=0+a$.

Multiplicative Identity: For all $a\in\mathbb{R}$, $a\cdot 1=a=1\cdot a$.

Additive Inverses: For all $a\in\mathbb{R}$, $a+(-a)=0=(-a)+a$.

Multiplicative Inverses: For all $a\in\mathbb{R}$ with $a\neq 0$, $a\cdot a^{-1}=1=a^{-1}\cdot a$.

Discuss the similarities and differences among the properties of addition and multiplication of real numbers and the properties of union and intersection of sets.

Answer

Add texts here. Do not delete this text first.

5.4: Cartesian Products

PREVIEW ACTIVITY 5.4.1: An Equation with Two Variables

In Section 2.3, we introduced the concept of the **truth set of an open sentence with one variable**. This was defined to be the set of all elements in the universal set that can be substituted for the variable to make the open sentence a true statement.

In previous mathematics courses, we have also had experience with open sentences with two variables. For example, if we assume that x and y represent real numbers, then the equation

$$2x + 3y = 12$$

is an open sentence with two variables. An element of the truth set of this open sentence (also called a solution of the equation) is an ordered pair (a, b) of real numbers so that when a is substituted for x and b is substituted for y, the open sentence becomes a true statement (a true equation in this case). For example, we see that the ordered pair (6, 0) is in the truth set for this open sentence since

$$2 \cdot 6 + 3 = 12$$

is a true statement. On the other hand, the ordered pair (4, 1) is not in the truth set for this open sentence since

$$2 \cdot 4 + 3 \cdot 1 = 12$$

is a false statement.

Important Note: The order of the of the two numbers in the ordered pair is very important. We are using the convention that the first number is to be substituted for x and the second number is to be substituted for y. With this convention, (3, 2) is a solution of the equation $2x + 3y = 12$, but (2, 3) is not a solution of this equation.

1. List six different elements of the truth set (often called the solution set) of the open sentence with two variables $2x + 3y = 12$.
2. From previous mathematics courses, we know that the graph of the equation $2x + 3y = 12$ is a straight line. Sketch the graph of the equation $2x + 3y = 12$ in the xy-coordinate plane. What does the graph of the equation $2x + 3y = 12$ show?
3. Write a description of the solution set S of the equation $2x + 3y = 12$ using set builder notation.

PREVIEW ACTIVITY 5.4.1: The Cartesian Product of Two Sets

In Preview Activity 5.4.1, we worked with ordered pairs without providing a formal definition of an ordered pair. We instead relied on your previous work with ordered pairs, primarily from graphing equations with two variables. Following is a formal definition of an ordered pair.

Definition: ordered pair

Let A and B be sets. An *ordered pair* (with first element from A and second element from B) is a single pair of objects, denoted by (a, b), with $a \in A$ and $b \in B$ and an implied order. This means that for two ordered pairs to be equal, they must contain exactly the same objects in the same order. That is, if $a, c \in A$ and $b, d \in B$, then

$$(a, b) = (c, d) \text{ if and only if } a = c \text{ and } b = d.$$

The objects in the ordered pair are called the *coordinates* of the ordered pair. In the ordered pair (a, b), a is the *first coordinate* and b is the *second coordinate*.

We will now introduce a new set operation that gives a way of combining elements from two given sets to form ordered pairs. The basic idea is that we will create a set of ordered pairs.

Definition: Cartesian product

If A and B are sets, then the *Cartesian product*, $A \times B$, of A and B is the set of all ordered pairs (x, y) where $x \in A$ and $y \in B$. We use the notation $A \times B$ for the Cartesian product of A and B, and using set builder notation, we can write

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\} .$$

We frequently read $A \times B$ as "A cross B." In the case where the two sets are the same, we will write A^2 for $A \times A$. That is,

$$A^2 = A \times A = \{(a, b) \mid a \in A \text{ and } b \in A\} \quad .$$

Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$.

1. Is the ordered pair (3, a) in the Cartesian product $A \times B$? Explain.
2. Is the ordered pair (3, a) in the Cartesian product $A \times A$? Explain.
3. Is the ordered pair (3, 1) in the Cartesian product $A \times A$? Explain.
4. Using the roster method to specify all the elements of $A \times B$. (Remember that the elements of $A \times B$ will be ordered pairs.
5. Use the roster method to specify all of the elements of the set $A \times A = A^2$.
6. For any sets C and D, explain carefully what it means to say that the ordered pair (x, y) is not in the Cartesian product $C \times D$.

Cartesian Products

When working with Cartesian products, it is important to remember that the Cartesian product of two sets is itself a set. As a set, it consists of a collection of elements. In this case, the elements of a Cartesian product are ordered pairs. We should think of an ordered pair as a single object that consists of two other objects in a specified order. For example,

- If $a \neq 1$, then the ordered pair (1, a) is not equal to the ordered pair (a, 1). That is, (1, a) $\neq$ (a, 1).
- If $A = \{1, 2, 3\}$ and $B = \{a, b\}$, then the ordered pair (3, a) is an element of the set $A \times B$. That is, (3, a) $\in A \times B$.
- If $A = \{1, 2, 3\}$ and $B = \{a, b\}$, then the ordered pair (5, a) is not an element of the set $A \times B$ since $5 \notin A$. That is, $(5, a) \notin A \times B$.

In Section 5.3, we studied certain properties of set union, set intersection, and set complements, which we called the algebra of sets. We will now begin something similar for Cartesian products. We begin by examining some specific examples in Progress Check 5.23 and a little later in Progress Check 5.24.

? progress check 5.23 (relationships between Cartesian products)

Let $A = \{1, 2, 3\}$, $T = \{a, b\}$, and $C = \{a, c\}$. We can then form new sets from all of the set operations we have studied. For example, $B \cap C = \{a\}$, and so

$$A \times (B \cap C) = \{(1, a), (2, a), (3, a)\}.$$

1. Use the roster method to list all of the elements (ordered pairs) in each of the following sets:

   (a) $A \times B$
   (b) $T \times B$
   (c) $A \times C$
   (d) $A \times (B \cap C)$
   (e) $(A \times B) \cap (A \times C)$
   (f) $A \times (B \cup C)$
   (g) $(A \times B) \cup (A \times C)$
   (h) $A \times (B - C)$
   (i) $(A \times B) - (A \times C)$
   (j) $B \times A$
2. List all the relationships between the sets in Part (1) that you observe.

Answer

Add texts here. Do not delete this text first.

The Cartesian Plane

In Preview Activity 5.4.1, we sketched the graph of the equation $2x + 3y = 12$ in the xy-plane. This xy-plane, with which you are familiar, is a representation of the set $\mathbb{R} \times \mathbb{R}$ or $\mathbb{R}^2$. This plane is called the *Cartesian plane*.

The basic idea is that each ordered pair of real numbers corresponds to a point in the plane, and each point in the plane corresponds to an ordered pair of real numbers. This geometric representation of $\mathbb{R}^2$ is an extension of the geometric representation of $\mathbb{R}$ as a straight line whose points correspond to real numbers.

Since the Cartesian product $\mathbb{R}^2$ corresponds to the Cartesian plane, the Cartesian product of two subsets of $\mathbb{R}$ corresponds to a subset of the Cartesian plane. For example, if A is the interval [1, 3], and B is the interval [2, 5], then

$$A \times B = \{(x, y) \in \mathbb{R}^2 \mid 1 \leq x \leq 3 \text{ and } 2 \leq y \leq 5\}.$$

A graph of the set $A \times B$ can then be drawn in the Cartesian plane as shown in Figure 5.6.

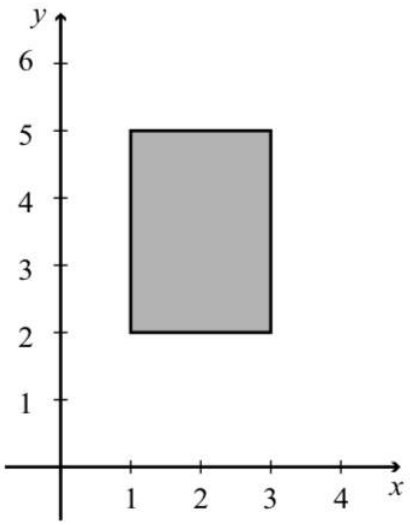


Figure 5.6: Cartesian Product $A \times B$

This illustrates that the graph of a Cartesian product of two intervals of finite length in $\mathbb{R}$ corresponds to the interior of a rectangle and possibly some or all of its boundary. The solid line for the boundary in Figure 5.6 indicates that the boundary is included. In this case, the Cartesian product contained all of the boundary of the rectangle. When the graph does not contain a portion of the boundary, we usually draw that portion of the boundary with a dotted line.

Note: A Caution about Notation. The standard notation for an open interval in $\mathbb{R}$ is the same as the notation for an ordered pair, which is an element of $\mathbb{R} \times \mathbb{R}$. We need to use the context in which the notation is used to determine which interpretation is intended. For example,

- If we write $(sqrt2, 7) \in \mathbb{R} \times \mathbb{R}$, then we are using $(sqrt2, 7)$ to represent an ordered pair of real numbers.
- If we write $(1, 2) \times \{4\}$, then we are interpreting $(1, 2)$ as an open interval. We could write

$$(1, 2) \times \{4\} = \{(x, 4) \mid 1 < x < 2\}.$$

The following progress check explores some of the same ideas explored in Progress Check 5.23 except that intervals of real numbers are used for the sets.

? Progress Check 5.24: Cartesian Products of Intervals

We will use the following intervals that are subsets of $\mathbb{R}$.

$$A = [0, 2]\ T = (1, 2)\ B = [2, 4)\ C = (3, 5]$$

1. Draw a graph of each of the following subsets of the Cartesian plane and write each subset using set builder notation.

   (a) $A \times B$
   (b) $T \times B$
   (c) $A \times C$
   (d) $A \times (B \cap C)$
   (e) $(A \times B) \cap (A \times C)$
   (f) $A \times (B \cup C)$
   (g) $(A \times B) \cup (A \times C)$
   (h) $A \times (B - C)$
   (i) $(A \times B) - (A \times C)$
   (j) $B \times A$
2. List all the relationships between the sets in Part (1) that you observe.

Answer

Add texts here. Do not delete this text first.

One purpose of the work in Progress Checks 5.23 and 5.24 was to indicate the plausibility of many of the results contained in the next theorem.

Theorem 5.25

Let A, B. and C be sets. Then

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
3. $(A \cap B) \times C = (A \times C) \cap (B \times C)$
4. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
5. $A \times (B - C) = (A \times B) - (A \times C)$
6. $(A - B) \times C = (A \times C) - (B \times C)$
7. If $T \subseteq A$, then $T \times B \subseteq A \times B$.
8. If $T \subseteq B$, then $A \times Y \subseteq A \times B$.

We will not prove all these results; rather, we will prove Part (2) of Theorem 5.25 and leave some of the rest to the exercises. In constructing these proofs, we need to keep in mind that Cartesian products are sets, and so we follow many of the same principles to prove set relationships that were introduced in Sections 5.2and 5.3.

The other thing to remember is that the elements of a Cartesian product are ordered pairs. So when we start a proof of a result such as Part (2) of Theorem 5.25, the primary goal is to prove that the two sets are equal. We will do this by proving that each one is a subset of the other one. So if we want to prove that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$, we can start by choosing an arbitrary element of $A \times (B \cup C)$. The goal is then to show that this element must be in $(A \times B) \cup (A \times C)$. When we start by choosing an arbitrary element of $A \times (B \cup C)$, we could give that element a name. For example, we could start by letting

$$u \text{ be an element of } A \times (B \cup C). \tag{5.4.1}$$

We can then use the definition of "ordered pair" to conclude that

$$\text{there exists } x \in A \text{ and there exits } y \in B \cup C \text{ such that } u = (x, y). \tag{5.4.2}$$

In order to prove that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$, we must now show that the ordered pair u from (5.4.1) is in $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$. In order to do this, we can use the definition of set union and prove that

$$u \in (A \times B) \text{ or } u \in (A \times C). \tag{5.4.3}$$

Since $u = (x, y)$, we can prove (5.4.3) by proving that

$$(x \in A \text{ and } y \in B) \text{ or } (x \in A \text{ and } y \in C). \tag{5.4.4}$$

If we look at the sentences in (5.4.2) and (5.4.4), it would seem that we are very close to proving that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$. Following is a proof of Part (2) of Theorem 5.25.

Theorem 5.25 (Part (2)).

Let A, B. and C be sets. Then

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

Proof

Let A, B. and C be sets. We will prove that $A \times (B \cup C)$ is equal to $(A \times B) \cup (A \times C)$ by proving that each set is a subset of the other set.

To prove that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$, we let $u \in A \times (B \cup C)$. Then there exists $x \in A$ and there exists $y \in B \cup C$ such that $u = (x, y)$. Since $y \in B \cup C$, we know that $y \in B$ or $y \in C$.

In the case where $y \in B$, we have $u = (x, y)$, where $x \in A$ and $y \in B$. So in this case, $u \in A \times B$, and hence $u \in (A \times B) \cup (A \times C)$. Similarly, in the case where $y \in C$, we have $u = (x, y)$, where $x \in A$ and $y \in C$. So in this case, $u \in A \times C$ and, hence, $u \in (A \times B) \cup (A \times C)$.

In both cases, $u \in (A \times B) \cup (A \times C)$. Hence, we may conclude that if u is an element of $A \times (B \cup C)$, then $u \in (A \times B) \cup (A \times C)$, and this proves that

$$A \times (B \cup C) \subseteq (A \times B) \cup (A \times C). \tag{5.4.5}$$

We must now prove that $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$. So we let $v \in (A \times B) \cup (A \times C)$. Then $v \in (A \times B)$ or $v \in (A \times C)$.

In the case where $v \in (A \times B)$, we know that there exists $s \in A$ and there exists $t \in B$ such that $v = (s, t)$. But because $t \in C$, we can conclude that $t \in B \cup C$ and, hence, $v \in A \times (B \cup C)$.

In both cases, $v \in A \times (B \cup C)$. Hence, we may conclude that if $v \in (A \times B) \cup (A \times C)$, then $v \in A \times (B \cup C)$, and this proves that

$$(A \times B) \cup (A \times C) \subseteq A \times (B \cup C). \tag{5.4.6}$$

The relationships in (5.4.5) and (5.4.6) prove that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Final Note.

The definition of an ordered pair in Preview Activity 5.4.2 may have seemed like a lengthy definition, but in some areas of mathematics, an even more formal and precise definition of "ordered pair" is needed. This definition is explored in Exercise (10).

Exercises for Section 5.4

1. Let $A = \{1, 2\}$, $B = \{a, b, c, d\}$, and $C = \{1, a, b\}$. Use the roster method to list all of the elements of each of the following sets:

   (a) $A \times B$
   (b) $B \times A$
   (c) $A \times C$
   (d) A^2
   (e) $A \times (B \cap C)$
   (f) $(A \times B) \cap (A \times C)$
   (g) $A \times \emptyset$
   (h) $B \times \{2\}$

2. Sketch a graph of each of the following Cartesian products in the Cartesian plane.

   (a) [0, 2] × [1, 3]
   (b) (0, 2) × (1, 3]
   (c) [2, 3] × {1}
   (d) {1} × [2, 3]
   (e) $\mathbb{R}$ × (2, 4)
   (f) (2, 4) × $\mathbb{R}$
   (g) $\mathbb{R}$ × {-1}
   (h) {-1} × [1, +∞)
3. Prove Theorem 5.25, Part (1): $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
4. Prove Theorem 5.25, Part (4): $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
5. Prove Theorem 5.25, Part (5): $A \times (B - C) = (A \times B) - (A \times C)$.
6. Prove Theorem 5.25, Part (7): If $T \subseteq A$, then $T \times B \subseteq A \times B$.
7. Let $A = \{1\}$, $B = \{2\}$, and $C = \{3\}$.

   (a) Explain why $A \times B \neq B \times A$.
   (b) Explain why $A \times B) \times C \neq A \times (B \times C)$.
8. Let A and B be nonempty sets. Prove that $A \times B = B \times A$ if and only if $A = B$.
9. Is the following proposition true or false? Justify your conclusion.

   Let A, B and C be sets with $A \neq \emptyset$. If $A \times B = A \times C$, then $B = C$. Explain where the assumption that $A \neq \emptyset$ is needed.

Explorations and Activities

10. **(A Set Theoretic Definition of an Ordered Pair)** In elementary mathematics, the notion of an ordered pair introduced at the beginning of this section will suffice. However, if we are interested in a formal development of the Cartesian product of two sets, we need a more precise definition of ordered pair. Following is one way to do this in terms of sets. This definition is credited to Kazimierz Kuratowski (1896 – 1980). Kuratowski was a famous Polish mathematician whose main work was in the areas of topology and set theory. He was appointed the Director of the Polish Academy of Sciences and served in that position for 19 years.

    Let x be an element of the set A, and let y be an element of the set B. The **ordered pair** (x, y) is defined to be the set $\{\{x\}, \{x, y\}\}$ That is,

$$(x, y) = \{\{x\}, \{x, y\}\}. \tag{5.4.7}$$

    (a) Explain how this definition allows us to distinguish between the ordered pairs (3, 5) and (5, 3).

    (b) Let A and B be sets and let $a, c \in A$ and $b, d \in B$. Use this definition of an ordered pair and the concept of set equality to prove that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.

    An ordered triple can be thought of as a single triple of objects, denoted by (a, b, c), with an implied order. This means that in order for two ordered triples to be equal, they must contain exactly the same objects in the same order. That is $(a, b, c) = (p, q, r)$ if and only if $a = p$, $b = q$ and $c = r$.

    (c) Let A, B and C be sets, and let $x \in A$, $y \in B$, and $z \in C$. Write a set theoretic definition of the ordered triple (x, y, z) similar to the set theoretic definition of "ordered pair."

Answer

Add texts here. Do not delete this text first.

5.5: Indexed Families of Sets

Preview Activity 5.5.1: The Union and Intersection of a Family of Sets

In Section 5.3, we discussed various properties of set operations. We will now focus on the associative properties for set union and set intersection. Notice that the definition of "set union" tells us how to form the union of two sets. It is the associative law that allows us to discuss the union of three sets. Using the associate law, if A, B, and C are subsets of some universal set, then we can define $A \cup B \cup C$ to be $(A \cup B) \cup C$ or $A \cup (B \cup C)$. That is,

$$A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C).$$

For this activity, the universal set is N and we will use the following four sets:

$A = \{1, 2, 3, 4, 5\}$

$B = \{2, 3, 4, 5, 6\}$

$C = \{3, 4, 5, 6, 7\}$

$D = \{4, 5, 6, 7, 8\}$

1. Use the roster method to specify the sets $A \cup B \cup C$, $B \cup C \cup D$, $A \cap B \cap C$, and $B \cap C \cap D$.
2. Use the roster method to specify each of the following sets. In each case, be sure to follow the order specified by the parentheses.

   (a) $(A \cup B \cup C) \cup D$
   (b) $A \cup (B \cup C \cup D)$
   (c) $A \cup (B \cup C) \cup D$
   (d) $(A \cup B) \cup (C \cup D)$
   (e) $(A \cap B \cap C) \cap D$
   (f) $A \cap (B \cap C \cap D)$
   (g) $A \cap (B \cap C) \cap D$
   (h) $(A \cap B) \cap (C \cap D)$
3. Based on the work in Part (2), does the placement of the parentheses matter when determining the union (or intersection) of these four sets? Does this make it possible to define $A \cup B \cup C \cup D$ and $A \cap B \cap C \cap D$?

We have already seen that the elements of a set may themselves be sets. For example, the power set of a set T, $\mathcal{P}(T)$, is the set of all subsets of T. The phrase, "a set of sets" sounds confusing, and so we often use the terms ***collection*** and ***family*** when we wish to emphasize that the elements of a given set are themselves sets. We would then say that the power set of T is the family (or collection) of sets that are subsets of T.

One of the purposes of the work we have done so far in this preview activity was to show that it is possible to define the union and intersection of a family of sets.

Definition

Let $\mathcal{C}$ be a family of sets. The **union over** $\mathcal{C}$ is defined as the set of all elements that are in at least one of the sets in $\mathcal{C}$. We write

$$\bigcup_{X \in \mathcal{C}} X = \{x \in U \mid x \in X \text{ for some } X \in \mathcal{C}\}$$

The **intersection over** $\mathcal{C}$ is defined as the set of all elements that are in all of the sets in $\mathcal{C}$. That is,

$$\bigcap_{X \in \mathcal{C}} X = \{x \in U \mid x \in X \text{ for some } X \in \mathcal{C}\}$$

For example, consider the four sets A, B, C, and D used earlier in this preview activity and the sets

$$S = \{5, 6, 7, 8, 9\} \text{ and } T = \{6, 7, 8, 9, 10\}$$

We can then consider the following families of sets: $\mathcal{A} = \{A, B, C, D\}$ and $\mathcal{B} = \{A, B, C, D, S, T\}$

4. Explain why

$\bigcup_{X\in\mathcal{A}} X = A\cup B\cup C\cup D$ and $\bigcap_{X\in\mathcal{A}} X = A\cap B\cap C\cap D$

and use your work in (1), (2), and (3) to determine $\bigcup_{X\in\mathcal{A}} X$ and $\bigcap_{X\in\mathcal{A}} X$.

5. Use the roster method to specify $\bigcup_{X\in\mathcal{B}} X$ and $\bigcap_{X\in\mathcal{B}} X$
6. Use the roster method to specify the sets $(\bigcup_{X\in\mathcal{A}} X)^c$ and $\bigcap_{X\in\mathcal{A}} X^c$. Remember that the universal set is $\mathbb{N}$.

? Preview Activity 5.5.2: An Indexed Family of Sets

We often use subscripts to identify sets. For example, in Preview Activity 5.5.1, instead of using A, B, C, and D as the names of the sets, we could have used A_1, A_2, A_3, and A_4. When we do this, we are using the subscript as an identifying tag, or index, for each set. We can also use this idea to specify an infinite family of sets. For example, for each natural number n, we define

$$C_n = \{n, n+1, n+2, n+3, n+4\}.$$

So if we have a family of sets $\mathcal{C} = \{C_1, C_2, C_3, C_4\}$, we use the notation $\bigcup_{j=1}^{4} C_j$ to mean the same thing as $\bigcup_{x\in\mathcal{C}} X$.

1. Determine $\bigcup_{j=1}^{4} C_j$ and $\bigcap_{j=1}^{4} C_j$

   We can see that with the use of subscripts, we do not even have to define the family of sets $\mathcal{A}$. We can work with the infinite family of sets

   $$\mathcal{C}^* = \{A_n \mid n\in\mathbb{N}\} \tag{5.5.1}$$

   and use the subscripts to indicate which sets to use in a union or an intersection.
2. Use the roster method to specify each of the following pairs of sets. The universal set is $\mathbb{N}$.

   (a) $\bigcup_{j=1}^{6} C_j$ and $\bigcap_{j=1}^{6} C_j$
   (b) $\bigcup_{j=1}^{8} C_j$ and $\bigcap_{j=1}^{8} C_j$
   (c) $\bigcup_{j=4}^{8} C_j$ and $\bigcap_{j=4}^{8} C_j$
   (d) $(\bigcap_{j=1}^{4} C_j)^c$ and $\bigcup_{j=1}^{4} C_j^c$

The Union and Intersection over an Indexed Family of Sets

One of the purposes of the preview activities was to show that we often encounter situations in which more than two sets are involved, and it is possible to define the union and intersection of more than two sets. In Preview Activity 5.5.2, we also saw that it is often convenient to "index" the sets in a family of sets. In particular, if n is a natural number and $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ is a family of n sets, then the union of these n sets, denoted by $A_1\cup A_2\cup\cdots\cup A_n$ or $\bigcup_{j=1}^{n} A_j$, is defined as

$$\bigcup_{j=1}^{n} A_j = \{x\in U \mid x\in A_j, \text{ for some } j \text{ with } 1\le j\le n\}. \tag{5.5.2}$$

We can also defined the intersection of these n sets, denoted by $A_1\cap A_2\cap\cdots\cap A_n$ or $\bigcap_{j=1}^{n} A_j$, as

$$\bigcap_{j=1}^{n} A_j = \{x\in U \mid x\in A_j, \text{ for some } j \text{ with } 1\le j\le n\}. \tag{5.5.3}$$

We can also extend this idea to define the union and intersection of a family that consists of infinitely many sets. So if $\mathcal{B} = \{B_1, B_2, \ldots, B_n, \ldots\}$, then

$\bigcup_{j=1}^{\infty} B_j = \{x\in U \mid x\in B_j, \text{ for some } j \text{ with } j\ge 1\}$, and

$\bigcap_{j=1}^{\infty} B_j = \{x\in U \mid x\in B_j, \text{ for all } j \text{ with } j\ge 1\}$.

Progress Check 5.26 (An Infinite Family of Sets)

For each natural number n, let $A_n = \{1, n, n^2\}$. For example,

$A_1 = \{1\}$, $A_2 = \{1, 2, 4\}$, $A_3 = \{1, 3, 9\}$,

and

$\bigcup_{j=1}^{3} A_j = \{1, 2, 3, 4, 9\}$, $\bigcap_{j=1}^{3} A_j = \{1\}$.

Determine each of the following sets:

1. $\bigcup_{j=1}^{6} A_j$
2. $\bigcap_{j=1}^{6} A_j$
3. $\bigcup_{j=3}^{6} A_j$
4. $\bigcap_{j=3}^{6} A_j$
5. $\bigcup_{j=1}^{\infty} A_j$
6. $\bigcap_{j=1}^{\infty} A_j$

Answer

Add texts here. Do not delete this text first.

In all of the examples we have studied so far, we have used $\mathbb{N}$ or a subset of $\mathbb{N}$ to index or label the sets in a family of sets. We can use other sets to index or label sets in a family of sets. For example, for each real number x, we can define B_x to be the closed interval [x, x + 2]. That is,

$$B_x = \{y \in \mathbb{R} \mid x \leq y \leq x + 2\} \ .$$

So we make the following definition. In this definition,$\wedge$ is the uppercase Greek letter lambda and α is the lowercase Greek letter alpha.

Definition

Let Λ be a nonempty set and suppose that for each $\alpha \in \wedge$, there is a corresponding set A_α. The family of sets $\{A_\alpha \mid \alpha \in \wedge\}$ is called an **indexed family of sets** indexed by $\wedge$. Each $\alpha \in \wedge$ is called an **index** and Λ is called an **indexing set**.

Progress Check 5.27 (Indexed Families of Sets)

In each of the indexed families of sets that we seen so far, if the indices were different, then the sets were different. That is, if Λ is an indexing for the family of sets $\mathcal{A} = \{A_\alpha \mid \alpha \in \wedge\}$, then if $\alpha, \beta \in \wedge$ and $\alpha \neq \beta$, then $A_\alpha \neq A_\beta$. (**Note**: The letter β is the Greek lowercase beta.)

1. Let $\Lambda = \{1, 2, 3, 4\}$, and for each $n \in \Lambda$, let $A_n = \{2n + 6, 16 - 3n\}$, and let $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$. Determine A_1, A_2, A_3, and A_4.
2. Is the following statement true or false for the indexed family $\mathcal{A}$ in (1)?
3. Now let $\Lambda = \mathbb{R}$. For each $x \in \mathbb{R}$, define $B_x = \{0, x^2, x^4\}$. Is the following statement true for the indexed family of set $\mathcal{B} = \{B_x \mid x \in \mathbb{R}\}$?
   For all $x, y \in \mathbb{R}$, if $x \neq y$, then $B_x \neq B_y$.

Answer

Add texts here. Do not delete this text first.

We now restate the definitions of the union and intersection of a family of sets for an indexed family of sets.

Definition

Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. The union over $\mathcal{A}$ is defined as the set of all elements that are in at least one of sets A_α, where $\alpha \in \wedge$. We write

$$\bigcup_{\alpha\in\Lambda} A_\alpha = \{x \in U \mid \text{ there exits an } \alpha \in \Lambda \text{ with } x \in A_\alpha\} \ .$$

The intersection over (\mathcal{A}\) is the set of all elements that are in all of the sets A_α for each $\alpha \in \Lambda$. That is,

$$\bigcap_{\alpha\in\wedge} A_\alpha = \{x \in U \mid \text{ for all } \alpha \in \wedge, x \in A_\alpha\} \ .$$

Example 5.28 (A Family of Sets Indexed by the Positive Real Numbers)

For each positive real numbe α, let A_α be the interval (-1, α]. That is,

$$A_\alpha = \{x \in \mathbb{R} \mid -1 < x \leq \alpha\}.$$

If we let $\mathbb{R}^+$ be the set of positive real numbers, then we have a family of sets indexed by $\mathbb{R}^+$. We will first determine the union of this family of sets. Notice that for each $\alpha \in mathbbR^+$, $\alpha \in A_\alpha$, and if y is a real number with $-1 < y \leq 0$, then $y \in A_\alpha$. Also notice that if $y \in \mathbb{R}$ and $y < -1$, then for each $\alpha \in mathbbR^+$, $y \notin A_\alpha$. With these observations, we conclude that

$$\bigcup_{\alpha\in\mathbb{R}^+} A_\alpha = (-1, \infty) = \{x \in \mathbb{R} \mid -1 < x\}.$$

To determine the intersection of this family, notice that

- if $y \in \mathbb{R}$ and $y < -1$, then for each $\alpha \in \mathbb{R}^+$, $y \notin A_\alpha$;
- if $y \in \mathbb{R}$ and $-1 < y \leq 0$, then $y \in A_\alpha$ for each $\alpha \in mathbbR^+$; and
- if $y \in \mathbb{R}$ and $y > 0$, then of we let $\beta = \frac{y}{2}$, $y > \beta$ and $y \notin A_\beta$.

From these observations, we conclude that

$$\bigcap_{\alpha\in\mathbb{R}^+} A_\alpha = (-1, 0] = \{x \in \mathbb{R} \mid -1 < x \leq 0\}.$$

Progress Check 5.29 (A Continuation of Example 5.28)

Using the family of sets from Example 5.28, for each $\alpha \in mathbbR^+$, we see that

$A_\alpha^c = (-\infty, 1] \cup (\alpha, \infty)$.

Use the results from Example 5.28 to help determine each of the following sets. For each set, use either interval notation or set builder notation.

1. $(\bigcup_{\alpha\in\mathbb{R}^+} A_\alpha)^c$
2. $(\bigcap_{\alpha\in\mathbb{R}^+} A_\alpha)^c$
3. $\bigcap_{\alpha\in\mathbb{R}^+} A_\alpha^c$
4. $\bigcup_{\alpha\in\mathbb{R}^+} A_\alpha^c$

Answer

Add texts here. Do not delete this text first.

Properties of Union and Intersection

In Theorem 5.30, we will prove some properties of set operations for indexed families of sets. Some of these properties are direct extensions of corresponding properties for two sets. For example, we have already proved De Morgan's Laws for two sets in Theorem 5.20. The work in the preview activities and Progress Check 5.29 suggests that we should get similar results using set operations with an indexed family of sets. For example, in Preview Activity 5.5.2, we saw that

$$(\bigcap_{j=1}^4 A_j)^c = \bigcup_{j=1}^4 A_j^c.$$

Theorem 5.30.

Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \wedge\}$ be an indexed family of sets. Then

1. For each $\beta \in \Lambda$, $\bigcap_{\alpha\in\Lambda} A_\alpha \subseteq A_\beta$
2. For each $\beta \in \Lambda$, $A_\beta \subseteq \bigcup_{\alpha\in\Lambda} A_\alpha$
3. $(\bigcap_{\alpha\in\Lambda} A_\alpha)^c = \bigcup_{\alpha\in\Lambda} A_\alpha^c$
4. $(\bigcup_{\alpha\in\Lambda} A_\alpha)^c = \bigcap_{\alpha\in\Lambda} A_\alpha^c$

Parts (3) and (4) are known as ***De Morgan's Laws.***

Proof

We will prove Parts (1) and (3). The proofs of Parts (2) and (4) are included in Exercise (4). So we let Λ be a nonempty indexing set and let $mathcalA = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. To prove Part (1), we let $\beta \in \Lambda$ and note that if $x \in \bigcap_{\alpha\in\Lambda} A_\alpha$, then $x \in A_\alpha$, for all $\alpha \in \Lambda$. Since β is one element in Λ, we may conclude that $x \in A_\beta$. This proves that $\bigcap_{\alpha\in\Lambda} A_\alpha \subseteq A_\beta$.

To prove Part (3), we will prove that each set is a subset of the other set. We first let $x \in (\bigcap_{\alpha\in\Lambda} A_\alpha)^c$. This means that $x \notin (\bigcap_{\alpha\in\Lambda} A_\alpha)$, and this means that

there exists a $\beta \in \Lambda$ such that $x \notin A_\beta$.

Hence, $x \in A_\beta^c$, which implies that $x \in \bigcup_{\alpha\in\Lambda} A_\alpha^c$. Therefore, we have proved that

$$(\bigcap_{\alpha\in\Lambda} A_\alpha)^c \subseteq \bigcup_{\alpha\in\Lambda} A_\alpha^c. \tag{5.5.4}$$

We now let $y \in \bigcup_{\alpha\in\Lambda} A_\alpha^c$. This means that there exists a $\beta \in \Lambda$ such that $y \in A_\beta^c$ or $y \notin A_\beta$. However, since $y \notin A_\beta$, we may conclude that $y \notin \bigcap_{\alpha\in\Lambda} A_\alpha$ and, hence, $y \in (\bigcap_{\alpha\in\Lambda} A_\alpha)^c$. This proves that

$$\bigcup_{\alpha\in\Lambda} A_\alpha^c \subseteq (\bigcap_{\alpha\in\Lambda} A_\alpha)^c. \tag{5.5.5}$$

Using the results in (5.5.4) and (5.5.5), we have proved that $(\bigcap_{\alpha\in\Lambda} A_\alpha)^c = \bigcup_{\alpha\in\Lambda} A_\alpha^c$.

Many of the other properties of set operations are also true for indexed families of sets. Theorem 5.31 states the distributive laws for set operations.

Theorem 5.31.

Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets, and let B be a set. Then

1. $B \cap (\bigcup_{\alpha\in\Lambda} A_\alpha) = \bigcup_{\alpha\in\Lambda} (B \cap A_\alpha)$, and
2. $B \cup (\bigcap_{\alpha\in\Lambda} A_\alpha) = \bigcap_{\alpha\in\Lambda} (B \cup A_\alpha)$.

Proof

The proof of Theorem 5.31 is Exercise (5).

Pairwise Disjoint Families of Sets

In Section 5.2, we defined two sets A and B to be disjoint provided that $A \cap B = \emptyset$. In a similar manner, if Λ is a nonempty indexing set and $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ is an indexed family of sets, we can say that this indexed family of sets is **disjoint** provided that $\bigcap_{\alpha\in\Lambda} A_\alpha = \emptyset$. However, we can use the concept of two disjoint sets to define a somewhat more interesting type of "disjointness" for an indexed family of sets.

Definition

Let Λ be a nonempty indexing set, and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. We say that $\mathcal{A}$ is pair wise disjoint provided that for all α and β in Λ, if $A_\alpha \neq A_\beta$, then $A_\alpha \cap A_\beta = \emptyset$.

Progress Check 5.32 (Disjoint Families of Sets)

Figure 5.7 shows two families of sets,

$$\mathcal{A} = \{A_1, A_2, A_3, A_4\} \text{ and } \mathcal{B} = \{B_1, B_2, B_3, B_4\}.$$

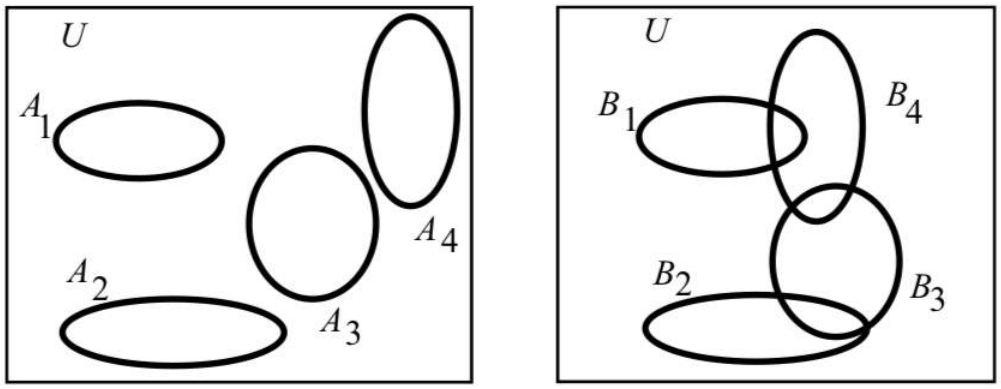


Figure 5.7: Two Families of Indexed Sets

1. Is the family of sets $\mathcal{A}$ a disjoint family of sets? A pairwise disjoint family of sets?
2. Is the family of sets $\mathcal{B}$ a disjoint family of sets? A pairwise disjoint family of sets?

Now let the universal be $\mathbb{R}$. For each $n \in \mathbb{N}$, let $C_n = (n, \infty)$, and let $\mathcal{C} = \{C_n \mid n \in \mathbb{N}\}$.

3. Is the family of sets $\mathcal{C}$ a disjoint family of sets? A pairwise disjoint family of sets?

Answer

Add texts here. Do not delete this text first.

Exercise 5.5.1

1. For each natural number n, let $A_n = \{n, n+1, n+2, n+3\}$. Use the roster method to specify each of the following sets:

   (a) $\bigcap_{j=1}^{3} A_j$
   (b) $\bigcup_{j=1}^{3} A_j$
   (c) $\bigcap_{j=3}^{7} A_j$
   (d) $\bigcup_{j=3}^{7} A_j$
   (e) $A_9 \cap (\bigcup_{j=3}^{7} A_j)$
   (f) $\bigcup_{j=3}^{7} (A_9 \cap A_j)$

2. For each natural number n, let $A_n = \{k \in \mathbb{N} \mid k \geq n\}$. Use the roster method or set builder notation to specify each of the following sets:

   (a) $\bigcap_{j=1}^{5} A_j$
   (b) $(\bigcap_{j=1}^{5} A_j)^c$

(c) $\bigcap_{j=1}^{5} A_j^c$
(d) $\bigcup_{j=1}^{5} A_j^c$
(e) $\bigcup_{j=1}^{5} A_j$
(f) $(\bigcup_{j=1}^{5} A_j)^c$
(g) \(\bigcap_{j \in \mathbb{N}^{} A_j\)
(h) \(\bigcup_{j \in \mathbb{N}^{} A_j\)

3. For each positive real number r, define T_r to be the closed interval $[-r^2, r^2]$. That is

$$T_r = \{x \in \mathbb{R} \mid -r^2 \leq x \leq r^2\}. \tag{5.5.6}$$

Let $\wedge = \{m \in \mathbb{N} \mid 1 \leq m \leq 10\}$. Use either interval notation or set builder notation to specify each of the following sets:

(a) $\bigcup_{k \in \wedge} T_k$
(b) $\bigcap_{k \in \wedge} T_k$
(c) $\bigcup_{r \in \mathbb{R}^+} T_k$
(d) $\bigcap_{r \in \mathbb{R}^+} T_k$
(e) $\bigcup_{r \in \mathbb{N}} T_k$
(f) $\bigcap_{r \in \mathbb{N}} T_k$

4. Prove Parts (2) and (4) of Theorem 5.30. Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets.

(a) For each $\beta \in \Lambda$, $A_\beta \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha$.
(b) $(\bigcup_{\alpha \in \Lambda} A_\alpha)^c = \bigcap_{\alpha \in \Lambda} A_\alpha^c$

5. Prove Theorem 5.31. Let Λ be a nonempty indexing set, let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets, and let B be a set. Then

(a) $B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha) = \bigcup_{\alpha \in \Lambda} (B \cap A_\alpha)$, and
(b) $B \cup (\bigcap_{\alpha \in \Lambda} A_\alpha) = \bigcap_{\alpha \in \Lambda} (B \cup A_\alpha)$.

6. Let Λ and Γ be nonempty indexing sets and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ and $\mathcal{B} = \{B_\beta \mid \beta \in \Gamma\}$ be indexed families of sets. Use the distributive laws in Exercise (5) to:

(a) Write \((\bigcup_{\alpha \in \Lambda}^{} A_{\alpha}) \cap (\bigcup_{\beta \in \Gamma}^{} B_{\beta}) as a union of intersections of two sets.
(b) Write \((\bigcap_{\alpha \in \Lambda}^{} A_{\alpha}) \cup (\bigcap_{\beta \in \Gamma}^{} B_{\beta}) as a union of intersections of two sets.

7. Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. Also, assume that $\Gamma \subseteq \Lambda$ and $\Gamma \neq \emptyset$. (**Note**: The letter Γ is the uppercase Greek letter gamma.) Prove that

(a) $\bigcup_{\alpha \in \Gamma} A_\alpha \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha$
(b) $\bigcap_{\alpha \in \Lambda} A_\alpha \subseteq \bigcap_{\alpha \in \Gamma} A_\alpha$

8. Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets.

(a) Prove that if B is a set such that $B \subseteq A_\alpha$ for every $\alpha \in \Lambda$, then $B \subseteq \bigcap_{\alpha \in \Lambda} A_\alpha$.
(b) Prove that if C is a set such that $A_\alpha \subseteq C$ for every $\alpha \in \Lambda$, then $\bigcap_{\alpha \in \Lambda} A_\alpha \subseteq C$.

9. For each natural number n, let $A_n = \{x \in \mathbb{R} \mid n - 1 < x < n\}$. Prove that $\{A_n \mid n \in \mathbb{N}\}$ is a pairwise disjoint family of sets and that $\bigcup_{n \in \mathbb{N}} A_n = (\mathbb{R}^+ - \mathbb{N})$.

10. For each natural number n, let $A_n = \{k \in \mathbb{N} \mid k \geq n\}$. Determine if the following statements are true or false. Justify each conclusion.

(a) For all $j, k \in \mathbb{N}$, if $j \neq k$, then $A_j \cap A_k \neq \emptyset$.
(b) $\bigcap_{k \in \mathbb{N}} A_k = \emptyset$.

11. Give an example of an indexed family of sets $\{A_n \mid n \in \mathbb{N}\}$ such all three of the following conditions are true:

    (i) For each $m \in \mathbb{N}$, $A_m \subseteq (0,1)$;
    (ii) For each $j, k \in \mathbb{N}$, if $j \neq k$, then $A_j \cap A_k \neq \emptyset$; and
    (iii) $\bigcap_{k\in\mathbb{N}} A_k = \emptyset$.
12. Let Λ be a nonempty indexing set, let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets, and let B be a set. Use the results of Theorem 5.30 and Theorem 5.31 to prove each of the following:

    (a) $(\bigcup_{\alpha\in\Lambda} A_\alpha) - B = \bigcup_{\alpha\in\Lambda}(A_\alpha - B)$
    (b) $(\bigcap_{\alpha\in\Lambda} A_\alpha) - B = \bigcap_{\alpha\in\Lambda}(A_\alpha - B)$
    (c) $B - (\bigcup_{\alpha\in\Lambda} A_\alpha) = \bigcap_{\alpha\in\Lambda} B - (A_\alpha)$
    (d) $B - (\bigcap_{\alpha\in\Lambda} A_\alpha) = \bigcup_{\alpha\in\Lambda} B - (A_\alpha)$

Explorations and Activities

13. An Indexed Family of Subsets of the Cartesian Plane. Let $\mathbb{R}^*$ be the set of nonnegative real numbers, and for each $r \in \mathbb{R}^*$, let

$$\begin{aligned} C_r &= \{(x,y) \in \mathbb{R}\times\mathbb{R} \mid x^2+y^2 = r^2\} \\ D_r &= \{(x,y) \in \mathbb{R}\times\mathbb{R} \mid x^2+y^2 \leq r^2\} \\ T_r &= \{(x,y) \in \mathbb{R}\times\mathbb{R} \mid x^2+y^2 > r^2\} = D_r^c. \end{aligned} \tag{5.5.7}$$

    If $r > 0$, then the set C_r is the circle of radius r with center at the origin as shown in Figure 5.8, and the set D_r is the shaded disk (including the boundary) shown in Figure 5.8.

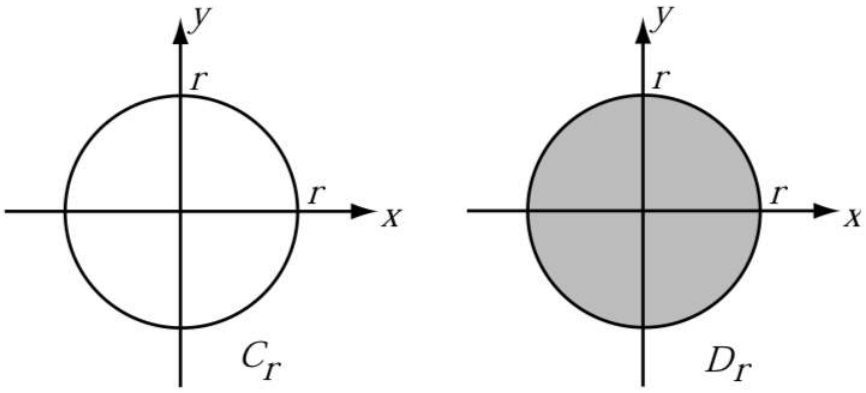


Figure 5.8: Two Sets for Activity 13

    (a) Determine $\bigcup_{r\in\mathbb{R}^*} C_r$ and $\bigcap_{r\in\mathbb{R}^*} C_r$
    (b) Determine $\bigcup_{r\in\mathbb{R}^*} D_r$ and $\bigcap_{r\in\mathbb{R}^*} D_r$
    (c) Determine $\bigcup_{r\in\mathbb{R}^*} T_r$ and $\bigcap_{r\in\mathbb{R}^*} T_r$
    (d) Let $\mathcal{C} = \{C_r \mid r \in \mathbb{R}^*\}$, $\mathcal{D} = \{D_r \mid r \in \mathbb{R}^*\}$, and $\mathcal{T} = \{T_r \mid r \in \mathbb{R}^*\}$. Are any of these indexed families of sets pairwise disjoint? Explain.

    Now let I be the closed interval [0, 2] and let J be the closed interval [1, 2].
    (e) Determine $\bigcup_{r\in I} C_r$, $\bigcap_{r\in I} C_r$, $\bigcup_{r\in J} C_r$, and $\bigcap_{r\in J} C_r$
    (f) Determine $\bigcup_{r\in I} D_r$, $\bigcap_{r\in I} D_r$, $\bigcup_{r\in J} D_r$, and $\bigcap_{r\in J} D_r$
    (g) Determine $(\bigcup_{r\in I} D_r)^c$, $(\bigcap_{r\in I} D_r)^c$, $(\bigcup_{r\in J} D_r)^c$, and $(bigcap_{r\in J} D_r)^c$
    (h) Determine $\bigcup_{r\in I} T_r$, $\bigcap_{r\in I} T_r$, $\bigcup_{r\in J} T_r$, and $\bigcap_{r\in J} T_r$
    (i) Use De Morgan's Laws to explain the relationship between your answers in Parts (13g) and (13h).

Answer

Add texts here. Do not delete this text first.

5.S: Set Theory (Summary)

Important Definitions

- Equal sets, page 55
- Subset, page 55
- Proper subset, page 218
- Power set, page 222
- Cardinality of a finite set, page 223
- Intersection of two sets, page 216
- Union of two sets, page 216
- Set difference, page 216
- Complement of a set, page 216
- Disjoint sets, page 236
- Cartesian product of two sets, pages 256
- Ordered pair, page 256
- Union over a family of sets, page 265
- Intersection over a family of sets, page 265
- Indexing set, page 268
- Indexed family of sets, page 268
- Union over an indexed family of sets, page 269
- Intersection over an indexed family of sets, page 269
- Pairwise disjoint family of sets, page 272

Important Theorems and Results about Sets

- **Theorem 5.5**. Let n be a nonnegative integer and let A be a subset of some universal set. If A is a finite set with n elements, then A has 2^n subsets. That is, if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.
- **Theorem 5.18**. Let A, B, and C be subsets of some universal set U. Then all of the following equalities hold.

  Properties of the Empty Set $A \cap \emptyset = \emptyset \quad A \cap U = A$
  and the Universal Set $A \cup \emptyset = A \quad A \cup U = U$

  Idempotent Laws $A \cap A = A \quad A \cup A = A$

  Commutative Laws. $A \cap B = B \cap A \quad A \cup B = B \cup A$

  Associative Laws $(A \cap B) \cap C = A \cap (B \cap C)$
  $(A \cup B) \cup C = A \cup (B \cup C)$

  Distributive Laws $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- **Theorem 5.20**. Let A and B be subsets of some universal set U. Then the following are true:

$$\begin{array}{ll} \text{Basic Properties} & (A^c)^c = A \\ & A - B = A \cap B^c \\ \text{Empty Set, Universal Set} & A - \emptyset = A \text{ and } A - U = \emptyset \\ & \emptyset^c = U \text{ and } U^c = \emptyset \\ \text{De Morgan's Laws} & (A \cap B)^c = A^c \cup B^c \\ & (A \cup B)^c = A^c \cap B^c \\ \text{Subsets and Complements} & A \subseteq B \text{ if and only if } B^c \subseteq A^c. \end{array} \tag{5.S.1}$$

- **Theorem 5.25**. Let A, B, and C be sets. Then

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
3. $(A \cap B) \times C = (A \times C) \cap (B \times C)$
4. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
5. $A \times (B - C) = (A \times B) - (A \times C)$
6. $(A - B) \times C = (A \times C) - (B \times C)$
7. If $T \subseteq A$, then $T \times B \subseteq A \times B$.
8. If $T \subseteq B$, then $A \times Y \subseteq A \times B$.

- **Theorem 5.30**. Let Λ be a nonempty indexing set and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. Then

  1. For each $\beta \in \Lambda$, $\bigcap_{\alpha \in \Lambda} A_\alpha \subseteq A_\beta$.
  2. For each $\beta \in \Lambda$, $A_\beta \subseteq \bigcap_{\alpha \in \Lambda} A_\alpha$.
  3. $(\bigcap_{\alpha \in \Lambda} A_\alpha)^c = \bigcup_{\alpha \in \Lambda} A_\alpha^c$
  4. $(\bigcup_{\alpha \in \Lambda} A_\alpha)^c = \bigcap_{\alpha \in \Lambda} A_\alpha^c$

  Parts(3) and (4) are known as ***De Morgan's Laws***.
- **Theorem 5.31**. Let Λ be a nonempty indexing set, let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets, and let B be a set. Then

  1. $B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha) = \bigcup_{\alpha \in \Lambda} (B \cap A_\alpha)$, and
  2. $B \cup (\bigcap_{\alpha \in \Lambda} A_\alpha) = \bigcap_{\alpha \in \Lambda} (B \cup A_\alpha)$,

Important Proof Method

The Choose-an-Element Method

The choose-an-element method is frequently used when we encounter a universal quantifier in a statement in the backward process of a proof. This statement often has the form

For each element with a given property, something happens.

In the forward process of the proof, we then we choose an arbitrary element with the given property.

> Whenever we choose an arbitrary element with a given property, we are not selecting a specific element. Rather, the only thing we can assume about the element is the given property.

For more information, see page 232.

CHAPTER OVERVIEW

6: Functions

6.1: Introduction to Functions

Exercise 6.1.1

Preview Activity 1 (Functions from Previous Courses)
One of the most important concepts in modern mathematics is that of a **function**. In previous mathematics courses, we have often thought of a function as some sort of input-output rule that assigns exactly one output to each input. So in this context, a **function** can be thought of as a procedure for associating with each element of some set, called the **domain of the function**, exactly one element of another set, called the **codomain of the function**. This procedure can be considered an input-output-rule. The function takes the input, which is an element of the domain, and produces an output, which is an element of the codomain. In calculus and precalculus, the inputs and outputs were almost always real numbers. So the notationf $f(x) = x^2 sinx$ means the following:

- f is the name of the function.
- $f(x)$ is a real number. It is the output of the function when the input is the real number x. For example,

$$\begin{aligned} f(\frac{\pi}{2}) &= (\frac{\pi}{2})^2 sin(\frac{\pi}{2}) \\ &= \frac{\pi^2}{4} \cdot 1 \\ &= \frac{\pi^2}{4}. \end{aligned} \tag{6.1.1}$$

For this function, it is understood that the domain of the function is the set $\mathbb{R}$ of all real numbers. In this situation, we think of the domain as the set of all possible inputs. That is, the domain is the set of all possible real numbers x for which a real number output can be determined.

This is closely related to the equation $f = x^2 sinx$. With this equation, we frequently think of x as the input and y as the output. In fact, we sometimes write $y = f(x)$. The key to remember is that a function must have exactly one output for each input. When we write an equation such as

$$y = \frac{1}{2}x^3 - 1,$$

we can use this equation to define y as a function of x. This is because when we substitute a real number for x (the input), the equation produces exactly one real number for y (the output). We can give this function a name, such as g, and write

$$y = g(x) = \frac{1}{2}x^3 - 1.$$

However, as written, an equation such as

$$y^2 = x + 3$$

cannot be used to define y as a function of x since there are real numbers that can be substituted for x that will produce more than one possible value of y. For example, if $x = 1$, then $y^2 = 4$, and y could be -2 or 2.

Which of the following equations can be used to define a function with $x \in \mathbb{R}$ as the input and $y \in \mathbb{R}$ as the output?

1. $y = x^2 - 2$
2. $y^2 = x + 3$
3. $y = \frac{1}{2}x^3 - 1$
4. $y = \frac{1}{2}xsinx$
5. $x^2 + y^2 = 4$
6. $y = 2x - 1$
7. $y = dfracxx - 1$

Preview Activity 2 (Some Other Types of Functions)

The domain and codomain of the functions in Preview Activity 6.1.1 is the set $\mathbb{R}$ of all real numbers, or some subset of $\mathbb{R}$. In most of these cases, the way in which the function associates elements of the domain with elements of the codomain is by a rule determined by some mathematical expression. For example, when we say that f is the function such that

$$f(x) = \frac{x}{x-1},$$

then the algebraic rule that determines the output of the function f when the input is x is $\frac{x}{x-1}$. In this case, we would say that the domain of f is the set of all real numbers not equal to 1 since division by zero is not defined.

However, the concept of a function is much more general than this. The domain and codomain of a function can be any set, and the way in which a function associates elements of the domain with elements of the codomain can have many different forms. The input-output rule for a function can be a formula, a graph, a table, a random process, or a verbal description. We will explore two different examples in this preview activity.

1. Let b be the function that assigns to each person his or her birthday (month and day). The domain of the function b is the set of all people and the codomain of b is the set of all days in a leap year (i.e., January 1 through December 31, including February 29).

   (a) Explain why b really is a function. We will call this the **birthday function**.
   (b) In 1995, Andrew Wiles became famous for publishing a proof of Fermat's Last Theorem. (See A. D. Aczel, *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem*, Dell Publishing, New York, 1996.) Andrew Wiles's birthday is April 11, 1953. Translate this fact into functional notation using the "birthday function" b. That is, fill in the spaces for the following question marks:

   $$b(?) = ?. \tag{6.1.2}$$

   (c) Is the following statement true or false? Explain.
   For each day D of the year, there exists a person x such that $b(x) = D$.
   (d) Is the following statement true or false? Explain.
   For any people x and y, if x and y are different people, then $b(x) \neq b(y)$.
2. Let s be the function that associates with each natural number the sum of its distinct natural number divisors. This is called the **sum of the divisors function**. For example, the natural number divisors of 6 are 1, 2, 3, and 6, and so

   $$\begin{aligned} s(6) &= 1+2+3+6 \\ &= 12. \end{aligned} \tag{6.1.3}$$

   (a) Calculate $s(k)$ for each natural number k from 1 through 15.
   (b) Does there exist a natural number n such that $s(n) = 5$? Justify your conclusion.
   (c) Is it possible to find two different natural numbers m and n such that $s(m) = s(n)$? Explain.
   (d) Use your responses in (b) and (c) to determine whether the following statements true or false.
   i. For each $m \in \mathbb{N}$, there exists a natural number n such that $s(n) = m$.
   ii. For all $m, n \in \mathbb{N}$, if $m \neq n$, then $s(m) \neq s(n)$.

The Definition of a Function

The concept of a function is much more general than the idea of a function used in calculus or precalculus. In particular, the domain and codomain do not have to be subsets of $\mathbb{R}$. In addition, the way in which a function associates elements of the domain with elements of the codomain can have many different forms. This input-output rule can be a formula, a graph, a table, a random process, a computer algorithm, or a verbal description. Two such examples were introduced in Preview Activity 6.1.2.

For the **birthday function**, the domain would be the set of all people and the codomain would be the set of all days in a leap year. For the **sum of the divisors function**, the domain is the set $\mathbb{N}$ of natural numbers, and the codomain could also be $\mathbb{N}$. In both of

these cases, the input-output rule was a verbal description of how to assign an element of the codomain to an element of the domain.

We formally define the concept of a function as follows:

Definition

A *function* from a set A to a set B is a rule that associates with each element x of the set A exactly one element of the set B. A function from A to B is also called a *mapping* from A to B.

Function Notation. When we work with a function, we usually give it a name. The name is often a single letter, such as f or g. If f is a function from the set A to be the set B, we will write $f : A \to B$. This is simply shorthand notation for the fact that f is a function from the set A to the set B. In this case, we also say that f maps A to B.

Definition

Let $f : A \to B$. (This is read, "Let f be a function from A to B.") The set A is called the **domain** of the function f, and we write $A = dom(f)$. The set B is called the **codomain** of the function f, and we write $B = codom(f)$.

If $a \in A$, then the element of B that is associated with a is denoted by $f(a)$ and is called the ***image of a under f***. If $f(a) = b$, with $b \in B$, then a is called a **preimage of *b* under *f***.

Some Function Terminology with an Example. When we have a function $f : A \to B$, we often write $y = f(x)$. In this case, we consider x to be an unspecified object that can be chosen from the set A, and we would say that x is the **independent variable** of the function f and y is the **dependent variable** of the function f.

For a specific example, consider the function $g : \mathbb{R} \to \mathbb{R}$, where $g(x)$ is defined by the formula

$$g(x) = x^2 - 2.$$

Note that this is indeed a function since given any input x in the domain, $\mathbb{R}$, there is exactly one output $g(x)$ in the codomain, $\mathbb{R}$. For example,

$$\begin{aligned} g(-2) &= (-2)^2 - 2 = 2, \\ g(5) &= 5^2 - 2 = 23, \\ g(\sqrt{2}) &= (\sqrt{2})^2 - 2 = 0, \\ g(-\sqrt{2}) &= (-\sqrt{2})^2 - 2 = 0. \end{aligned} \tag{6.1.4}$$

So we say that the image of -2 under g is 2, the image of 5 under g is 23, and so on.

Notice in this case that the number 0 in the codomain has two preimages, $-\sqrt{2}$ and $\sqrt{2}$. This does not violate the mathematical definition of a function since the definition only states that each input must produce one and only one output. That is, each element of the domain has exactly one image in the codomain. Nowhere does the definition stipulate that two different inputs must produce different outputs.

Finding the preimages of an element in the codomain can sometimes be difficult. In general, if y is in the codomain, to find its preimages, we need to ask, "For which values of x in the domain will we have $y = g(x)$?" For example, for the function g, to find the preimages of 5, we need to find all x for which $g(x) = 5$. In this case, since $g(x) = x^2 - 2$, we can do this by solving the equation

$$x^2 - 2 = 5.$$

The solutions of this equation are $-\sqrt{7}$ and $\sqrt{7}$. So for the function g, the preimages of 5 are $-\sqrt{7}$ and $\sqrt{7}$. We often use set notation for this and say that the set of preimages of 5 for the function g is $\{-\sqrt{7}, \sqrt{7}\}$.

Also notice that for this function, not every element in the codomain has a preimage. For example, there is no input x such that $g(x) = -3$. This is true since for all real numbers x, $x^2 \geq 0$ and hence $x^2 - 2 \geq -2$. This means that for all x in $\mathbb{R}$, $g(x) \geq -2$.

Finally, note that we introduced the function g with the sentence, "Consider the function $g : \mathbb{R} \to \mathbb{R}$, where $g(x)$ is defined by the formula $g(x) = x^2 - 2$." This is one correct way to do this, but we will frequently shorten this to, "Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2 - 2$ ", or "Let $g : \mathbb{R} \to \mathbb{R}$, where $g(x) = x^2 - 2$."

? Progress Check 6.1 (Images and Preimages)

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 5x$ for all $x \in \mathbb{R}$. and let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(m) = m^2 - 5m$ for all $m \in \mathbb{Z}$.

1. Determine $f(-3)$ and $f(\sqrt{8})$.
2. Determine $g(2)$ and $g(-2)$.
3. Determine the set of all preimage of 6 for the function f.
4. Determine the set of all preimage of 6 for the function g.
5. Determine the set of all preimage of 2 for the function f.
6. Determine the set of all preimage of 2 for the function g.

Answer

Add texts here. Do not delete this text first.

The Codomain and Range of a Function

Besides the domain and codomain, there is another important set associated with a function. The need for this was illustrated in the example of the function g on page 285. For this function, it was noticed that there are elements in the codomain that have no preimage or, equivalently, there are elements in the codomain that are not the image of any element in the domain. The set we are talking about is the subset of the codomain consisting of all images of the elements of the domain of the function, and it is called the range of the function.

Definition

Let $f : A \to B$. The set $\{f(x) \mid x \in A\}$ is called the ***range of the function f*** and is denoted by range (f). The range of f is sometimes called the ***image of the function f*** (or the ***image of A under f***).

The range of $f : A \to B$ could equivalently be defined as follows:

$$\text{range}(f) = \{y \in B \mid y = f(x) \text{ for some } x \in A\} .$$

Notice that this means that range$(f) \subseteq$ codom(f) but does not necessarily mean that range$(f) =$ codom(f). Whether we have this set equality or not depends on the function f. More about this will be explored in Section 6.3.

? Progress Check 6.2 (Codomain and Range)

1. Let b be the function that assigns to each person his or her birthday (month and day).

   (a) What is the domain of this function?
   (b) What is a codomain for this function?
   (c) In Preview Activity 6.1.2, we determined that the following statement is true: For each day D of the year, there exists a person x such that $b(x) = D$. What does this tell us about the range of the function b? Explain.
2. Let s be the function that associates with each natural number the sum of its distinct natural number factors.

   (a) What is the domain of this function?
   (b) What is a codomain for this function?
   (c) In Preview Activity 6.1.2, we determined that the following statement is false:
   For each $m \in \mathbb{N}$, there exists a natural number n such that $s(n) = m$.
   Give an example of a natural number m that shows this statement is false, and explain what this tells us about the range of the function s.

Answer

Add texts here. Do not delete this text first.

The Graph of a Real Function

We will finish this section with methods to visually communicate information about two specific types of functions. The first is the familiar method of graphing functions that was a major part of some previous mathematics courses. For example, consider the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2 - 2x - 1$.

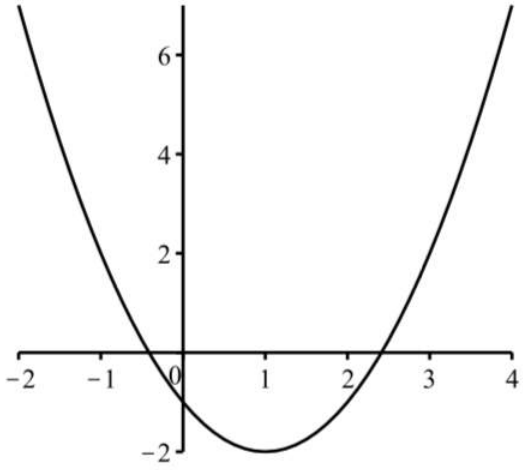


Figure 6.1: Graph of $y = g(x)$, where $g(x) = x^2 - 2x - 1$

Every point on this graph corresponds to an ordered pair (x, y) of real numbers, where $y = g(x) = x^2 - 2x - 1$. Because we use the Cartesian plane when drawing this type of graph, we can only use this type of graph when both the domain and the codomain of the function are subsets of the real numbers $\mathbb{R}$. Such a function is sometimes called a **real function**. The graph of a real function is a visual way to communicate information about the function. For example, the range of g is the set of all y-values that correspond to points on the graph. In this case, the graph of g is a parabola and has a vertex at the point (1, -2). (**Note**: The x-coordinate of the vertex can be found by using calculus and solving the equation $f\prime(x) = 0$.) Since the graph of the function g is a parabola, we know that pattern shown on the left end and the right end of the graph continues and we can conclude that the range of g is the set of all $y \in \mathbb{R}$ such that $y \geq -2$. That is,

$$\text{range}(g) = \{y \in \mathbb{R} \mid y \geq -2\}.$$

? Progress Check 6.3 (Using the Graph of a Real Function)

The graph in Figure 6.2 shows the graph of (slightly more than) two complete periods for a function $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = Asin(Bx)$ for some positive real number constants A and B.

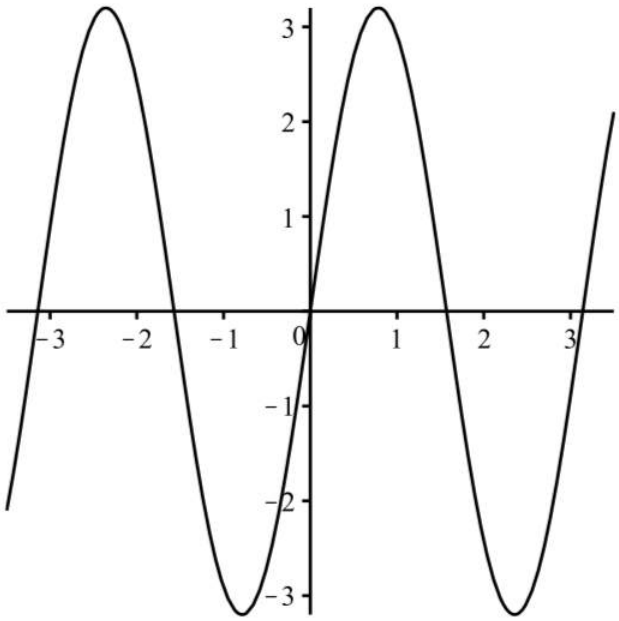


Figure 6.2: Graph of $y = f(x)$

1. We can use the graph to estimate the output for various inputs. This is done by estimating the y-coordinate for the point on the graph with a specified x-coordinate. On the graph, draw vertical lines at $x = -1$ and $x = 2$ and estimate the values of $f(-1)$ and $f(2)$.
2. Similarly, we can estimate inputs of the function that produce a specified output. This is done by estimating the x-coordinates of the points on the graph that have a specified y-coordinate. Draw a horizontal line at $y = 2$ and estimate at least two values of x such that $f(x) = 2$.
3. Use the graph Figure 6.2 to estimate the range of the function f.

Answer

Add texts here. Do not delete this text first.

Arrow Diagrams

Sometimes the domain and codomain of a function are small, finite sets. When this is the case, we can define a function simply by specifying the outputs for each input in the domain. For example, if we let $A = \{1, 2, 3\}$ and let $B = \{a, b\}$, we can define a function $F : A \to B$ by specifying that

$$F(1) = a, F(2) = a, \text{ and } F(3) = b.$$

This is a function since each element of the domain is mapped to exactly one element in B. A convenient way to illustrate or visualize this type of function is with a so-called **arrow diagram** as shown in Figure 6.3. An arrow diagram can

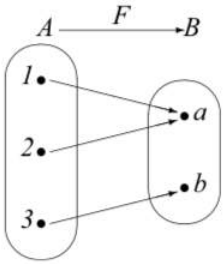


Figure 6.3: Arrow Diagram for a Function

be used when the domain and codomain of the function are finite (and small). We represent the elements of each set with points and then use arrows to show how the elements of the domain are associated with elements of the codomain. For example, the arrow from the point 2 in A to the point a in B represents the fact that $F(2) = a$. In this case, we can use the arrow diagram in Figure 6.3 to conclude that range(F)$= \{a, b\}$.

? Progress Check 6.4 (Working with Arrow Diagrams)

Let $A = \{1, 2, 3, 4\}$ and let $B = \{a, b, c\}$.

1. Which of the arrow diagrams in Figure 6.4 can be used to represent a function from A to B? Explain.
2. For those arrow diagrams that can be used to represent a function from A to B, determine the range of the function.

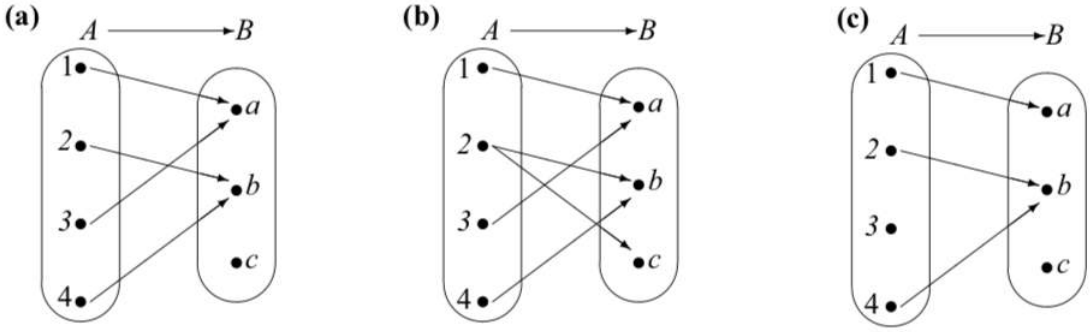


Figure 6.4: Arrow Diagram for a Function

Answer

Add texts here. Do not delete this text first.

? Exercises 6.1

1. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 2x$.

   (a) Evaluate $f(-3)$, $f(-1)$, $f(1)$, and $f(3)$.
   (b) Determine the set of all of the preimages of 0 and the set of all of the preimages of 4.
   (c) Sketch a graph of the function f.
   (d) Determine the range of the function f.

2. Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$, and let $s : \mathbb{R} \to \mathbb{R}^*$ be defined by $s(x) = x^2$.

   (a) Evaluate $s(-3)$, $s(-1)$, $s(1)$, and $s(3)$.
   (b) Determine the set of all of the preimages of 0 and the set of all of the preimages of 2.
   (c) Sketch a graph of the function s.
   (d) Determine the range of the function s.
3. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m) = 3 - m$.

   (a) Evaluate $f(-7)$, $f(-3)$, $f(3)$, and $f(7)$.
   (b) Determine the set of all of the preimages of 5 and the set of all of the preimages of 4.
   (c) Determine the range of the function f.
   (d) This function can be considered a real function since $\mathbb{Z} \subseteq \mathbb{R}$. Sketch a graph of this function. **Note**: The graph will be an infinite set of points that lie on a line. However, it will not be a line since its domain is not $\mathbb{R}$ but is $\mathbb{Z}$.
4. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m) = 2m + 1$.

   (a) Evaluate $f(-7)$, $f(-3)$, $f(3)$, and $f(7)$.
   (b) Determine the set of all of the preimages of 5 and the set of all of the preimages of 4.
   (c) Determine the range of the function f.
   (d) Sketch a graph of the function f. See the comments in Exercise (3d).
5. Recall that a **real function** is a function whose domain and codomain are subsets of the real numbers R. (See page 288.) Most of the functions used in calculus are real functions. Quite often, a real function is given by a formula or a graph with no specific reference to the domain or the codomain. In these cases, the usual convention is to assume that the domain of the real function f is the set of all real numbers x for which $f(x)$ is a real number, and that the codomain is $\mathbb{R}$. For example, if we define the (real) function f by

$$f(x) = \frac{x}{x-2}, \tag{6.1.5}$$

   we would be assuming that the domain is the set of all real numbers that are not equal to 2 and that the codomain in $\mathbb{R}$. Determine the domain and range of each of the following real functions. It might help to use a graphing calculator to plot a graph of the function.

   (a) The function k defined by $k(x) = \sqrt{x-3}$
   (b) The function F defined by $F(x) = ln(2x-1)$
   (c) The function f defined by $f(x) = 3sin(2x)$
   (d) The function g defined by $g(x) = \dfrac{4}{x^2-4}$
   (e) The function G defined by $G(x) = 4cos(\pi x) + 8$
6. **The number of divisors function**. Let d be the function that associates with each natural number the number of its natural number divisors. That is $d : \mathbb{N} \to \mathbb{N}$ where $d(n)$ is the number of natural number divisors of n. For example, $d(6) = 4$ since 1, 2, 3, and 6 are the natural number divisors of 6.

   (a) Calculate $d(k)$ for each natural number k from 1 through 12.
   (b) Does there exist a natural number n such that $d(n) = 1$? What is the set of preimages of the natural number 1.
   (c) Does there exist a natural number n such that $d(n) = 2$? If so, determine the set of all preimages of the natural number 2.
   (d) Is the following statement true or false? Justify your conclusion.
   For all $m, n \in \mathbb{N}$, if $m \neq n$, then $d(m) \neq d(n)$.
   (e) Calculate $d(2^k)$ for $k = 0$ and for each natural number k from 1 through 6.
   (f) Based on your work in Exercise (6e), make a conjecture for a formula for $d(2^n)$ where n is a nonnegative integer. Then explain why your conjecture is correct.
   (g) Is the following statement is true or false?
   For each $n \in \mathbb{N}$, there exists a natural number m such that $d(m) = n$.

7. In Exercise (6), we introduced the **number of divisors function** d. For this function, $d : \mathbb{N} \to \mathbb{N}$, where $d(n)$ is the number of natural number divisors of n.
A function that is related to this function is the so-called **set of divisors function**. This can be defined as a function S that associates with each natural number the set of its distinct natural number factors. For example, $S(6) = \{1, 2, 3, 6\}$ and $S(10) = \{1, 2, 5, 10\}$.

(a) Discuss the function S by carefully stating its domain, codomain, and its rule for determining outputs.
(b) Determine $S(n)$ for at least five different values of n.
(c) Determine $S(n)$ for at least three different prime number values of n.
(d) Does there exist a natural number n such that card$(S(n) = 1)$? Explain. [Recall that card$(S(n))$ is the number of elements in the set $S(n)$.]
(e) Does there exist a natural number n such that card$(S(n) = 2)$? Explain.
(f) Write the output for the function d in terms of the output for the function S. That is, write $d(n)$ in terms of $S(n)$.
(g) Is the following statement true or false? Justify your conclusion.
For all natural numbers m and n, if $m \neq n$, then $S(m) \neq S(n)$.
(h) Is the following statement true or false? Justify your conclusion.
For all sets T that are subsets of $\mathbb{N}$, there exists a natural number n such that $S(n) = T$.

Explorations and Activities

8. Creating Functions with Finite Domains. Let $A = \{a, b, c, d\}$, $B = \{a, b, c\}$. and $C = \{s, t, u, v\}$. In each of the following exercises, draw an arrow diagram to represent your function when it is appropriate.

(a) Create a function $f : A \to C$ whose range is the set C or explain why it is not possible to construct such a function.
(b) Create a function $f : A \to C$ whose range is the set $\{u, v\}$ or explain why it is not possible to construct such a function.
(c) Create a function $f : B \to C$ whose range is the set C or explain why it is not possible to construct such a function.
(d) Create a function $f : A \to C$ whose range is the set $\{u\}$ or explain why it is not possible to construct such a function.
(e) If possible, create a function $f : A \to C$ that satisfies the following condition:
For all $x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.
If it is not possible to create such a function, explain why.
(f) If possible, create a function $f : A \to \{s, t, u\}$ that satisfies the following condition:
For all $x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.
If it is not possible to create such a function, explain why.

Answer

Add texts here. Do not delete this text first.

6.2: More about Functions

In Section 6.1, we have seen many examples of functions. We have also seen various ways to represent functions and to convey information about them. For example, we have seen that the rule for determining outputs of a function can be given by a formula, a graph, or a table of values. We have also seen that sometimes it is more convenient to give a verbal description of the rule for a function. In cases where the domain and codomain are small, finite sets, we used an arrow diagram to convey information about how inputs and outputs are associated without explicitly stating a rule. In this section, we will study some types of functions, some of which we may not have encountered in previous mathematics courses.

? Preview Activity 6.2.1: The Number of Diagonals of a Polygon

A **polygon** is a closed plane figure formed by the joining of three or more straight lines. For example, a triangle is a polygon that has three sides; a **quadrilateral** is a polygon that has four sides and includes squares, rectangles, and parallelograms; a **pentagon** is a polygon that has five sides; and an **octagon** is a polygon that has eight sides. A r**egular polygon** is one that has equal-length sides and congruent interior angles.

A **diagonal of a polygon** is a line segment that connects two nonadjacent vertices of the polygon. In this activity, we will assume that all polygons are **convex polygons** so that, except for the vertices, each diagonal lies inside the polygon. For example, a triangle (3-sided polygon) has no diagonals and a rectangle has two diagonals.

1. How many diagonals does any quadrilateral (4-sided polygon) have?
2. Let $D = \mathbb{N} - \{1, 2\}$. Define $d : D \to \mathbb{N} \cup \{0\}$ so that $d(n)$ is the number of diagonals of a convex polygon with n sides. Determine the values of $d(3)$, $d(4)$, $d(5)$, $d(6)$, $d(7)$, and $d8)$. Arrange the results in the form of a table of values for the function d.
3. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by

$$f(x) = \frac{x(x-3)}{2}. \tag{6.2.1}$$

   Determine the values of $f(0)$, $f(1)$, $f(2)$, $f(3)$, $f(4)$, $f(5)$, $f(6)$, $f(7)$, $f(8)$, and $f9)$. Arrange the results in the form of a table of values for the function f.
4. Compare the functions in Parts (2) and (3). What are the similarities between the two functions and what are the differences? Should these two functions be considered equal functions? Explain.

? Preview Activity 6.2.1: Derivatives

In calculus, we learned how to find the derivatives of certain functions. For example, if $f(x) = x^2(sinx)$, then we can use the product rule to obtain

$$f\prime(x) = 2x(\sin x) + x^2(\cos x). \tag{6.2.2}$$

1. If possible, find the derivative of each of the following functions:

   (a) $f(x) = x^4 - 5x^3 + 3x - 7$
   (b) $g(x) = \cos(5x)$
   (c) $h(x) = \dfrac{\sin x}{x}$
   (d) $k(x) = e^{-x^2}$
   (e) $r(x) = |x|$
2. Is it possible to think of differentiation as a function? Explain. If so, what would be the domain of the function, what could be the codomain of the function, and what is the rule for computing the element of the codomain (output) that is associated with a given element of the domain (input)?

Functions Involving Congruences

Theorem 3.31 and Corollary 3.32 state that an integer is congruent (mod n) to its remainder when it is divided by n. (Recall that we always mean the remainder guaranteed by the Division Algorithm, which is the least nonnegative remainder.) Since this

remainder is unique and since the only possible remainders for division by n are 0, 1, 2, ..., $n-1$, we then know that each integer is congruent, modulo n, to precisely one of the integers 0, 1, 2, ..., $n-1$. So for each natural number n, we will define a new set $\mathbb{Z}_n$ as follows:

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

For example, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. We will now explore a method to define a function from $\mathbb{Z}_6$ to $\mathbb{Z}_6$.

For each $x \in \mathbb{Z}_6$, we can compute $x^2 + 3$ and then determine the value of r in $\mathbb{Z}_6$ so that

$$(x^2 + 3) \equiv r \pmod 6.$$

Since r must be in $\mathbb{Z}_6$, we must have $0 \leq r < 6$. The results are shown in the following table.

Table6 .1: Table of Values Defined by a Congruence

x	r, where $x^2 + 3) \equiv r (\text{mod } 6)$	x	r, where $x^2 + 3) \equiv r (\text{mod } 6)$
0	3	3	0
1	4	4	1
2	1	5	4

The value of x in the first column can be thought of as the input for a function with the value of r in the second column as the corresponding output. Each input produces exactly one output. So we could write

$$f : \mathbb{Z}_6 \to \mathbb{Z}_6 \text{ by } f(x) = r \text{ where } (x^2 + 3) \equiv r \pmod 6.$$

This description and the notation for the outputs of this function are quite cumbersome. So we will use a more concise notation. We will, instead, write

Let $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ by $f(x) = (x^2 + 3) \pmod 6$.

? Progress Check 6.5 (Functions Defined by Congruences)

Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4\}$. Define

$$f : \mathbb{Z}_5 \to \mathbb{Z}_5 \text{ by } f(x) = x^4 \pmod 5, \text{ for each } x \in \mathbb{Z}_5;$$

$$g : \mathbb{Z}_5 \to \mathbb{Z}_5 \text{ by } g(x) = x^5 \pmod 5, \text{ for each } x \in \mathbb{Z}_5;$$

1. Determine $f(0)$, $f(1)$, $f(2)$, $f(3)$, and $f(4)$ and represent the function f with an arrow diagram.
2. Determine $g(0)$, $g(1)$, $g(2)$, $g(3)$, and $g(4)$ and represent the function g with an arrow diagram.

Answer

Add texts here. Do not delete this text first.

Equality of Functions

The idea of equality of functions has been in the background of our discussion of functions, and it is now time to discuss it explicitly. The preliminary work for this discussion was Preview Activity 6.2.1, in which $D = \mathbb{N} - \{1, 2\}$ and there were two functions:

- $d : D \to \mathbb{N} \cup \{0\}$, where $d(n)$ is the number of diagonals of a convex polygon with n sides
- $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = \dfrac{x(x-3)}{2}$, for each real number x.

In Preview Activity 6.2.1, we saw that these two functions produced the same outputs for certain values of the input (independent variable). For example, we can verify that

$$d(3) = f(3) = 0, \; d(4) = f(4) = 2,$$
$$d(5) = f(5) = 5, \text{ and } d(6) = f(6) = 9.$$

Although the functions produce the same outputs for some inputs, these are two different functions.For example, the outputs of the function f are determined by a formula, and the outputs of the function d are determined by a verbal description. This is not

enough, however, to say that these are two different functions. Based on the evidence from Preview Activity 6.2.1, we might make the following conjecture:

$$\text{For } n \geq 3,\ d(n) = \frac{n(n-3)}{2}.$$

Although we have not proved this statement, it is a true statement. (See Exercise 6.) However, we know the function d and the function f are not the same function. For example,

- $f(0) = 0$, but 0 is not in the domain of d;
- $f(\pi) = \frac{\pi(\pi-3)}{2}$, but π is not in the domain of d.

We thus see the importance of considering the domain and codomain of each of the two functions in determining whether the two functions are equal or not. This motivates the following definition.

Definition: equal Functions

Two functions f and g are **equal** provided that

- The domain of f equals the domain of g. That is dom(f) = dom(g)
- The codomain of f equals the codomain of g. That is codom(f) = codom(g)
- For each x in the domain of f (which equals the domain of g), $f(x) = g(x)$.

Progress Check 6.6: Equality of Functions

Let A be a nonempty set. The **identity function on the set A**, denoted by I_A, is the function $I_A : A \to A$ defined by $I_A(x) = x$ for every x in A. That is, for the identity map, the output is always equal to the input.

For this progress check, we will use the functions f and g from Progress Check 6.5. The identity function on the set $\mathbb{Z}_5$ is

$I_{\mathbb{Z}_5} : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $I_{\mathbb{Z}_5}(x) = x \pmod 5$, for each $x \in \mathbb{Z}_5$.

Is the identity function on $\mathbb{Z}_5$ equal to either of the functions f or g from Progress Check 6.5? Explain.

Answer

Add texts here. Do not delete this text first.

Mathematical Processes as Functions

Certain mathematical processes can be thought of as functions. In Preview Activity 6.2.2, we reviewed how to find the derivatives of certain functions, and we considered whether or not we could think of this differentiation process as a function. If we use a differentiable function as the input and consider the derivative of that function to be the output, then we have the makings of a function. Computer algebra systems such as *Maple and Mathematica* have this derivative function as one of their predefined operators.

Following is some *Maple* code (using the Classic Worksheet version of *Maple*) that can be used to find the derivative function of the function given by $f(x) = x^2(sinx)$. The lines that start with the *Maple* prompt, [>, are the lines typed by the user. The centered lines following these show the resulting *Maple* output. The first line defines the function f, and the second line uses the derivative function D to produce the derivative of the function f.

[> f := x → x^2 ∗ sin (x);

$$f := x \to x^2 \sin(x)$$

[> f1 := D(f);

$$f1 := x \to 2x \sin(x) + x^2 \cos(x)$$

We must be careful when determining the domain for the derivative function since there are functions that are not differentiable. To make things reasonably easy, we will let F be the set of all real functions that are differentiable and call this the domain of the derivative function D. We will use the set T of all real functions as the codomain. So our function D is

$$D : F \to T \text{ by } D(f) = f\prime.$$

Progress Check 6.7: Average of a Finite Set of Numbers

Let $A = \{a_1, a_2, \ldots a_n\}$ be a finite set whose elements are the real numbers $a_1, a_2, \ldots a_n$. We define the **average of the set** A to be the real number $\bar{A}$, where

$$\bar{A} = \frac{a_1, a_2, \ldots a_n}{n}.$$

1. Find the average of $A = \{3, 7, -1, 5\}$.
2. Find the average of $B = \{7, -2, 3.8, 4.2, 7.1\}$
3. Find the average of $C = \{\sqrt{2}, \sqrt{3}, \pi - \sqrt{3}\}$.
4. Now let $\mathcal{F}(\mathbb{R})$ be the set of all finite subsets of $\mathbb{R}$. That is, a subset A of $\mathbb{R}$ is in $\mathcal{F}(\mathbb{R})$ if and only if A contains only a finite number of elements. Carefully explain how the process of finding the average of a finite subset of $\mathbb{R}$ can be thought of as a function. In doing this, be sure to specify the domain of the function and the codomain of the function.

Answer

Add texts here. Do not delete this text first.

Sequences as Functions

A sequence can be considered to be an infinite list of objects that are indexed (subscripted) by the natural numbers (or some infinite subset of $\mathbb{N} \cup \{0\}$). Using this idea, we often write a sequence in the following form:

$$a_1, a_2, \ldots, a_n, \ldots.$$

In order to shorten our notation, we will often use the notation $\langle a_n \rangle$ to represent this sequence. Sometimes a formula can be used to represent the terms of a sequence, and we might include this formula as the nth term in the list for a sequence such as in the following example:

$$1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots.$$

In this case, the nth term of the sequence is $\frac{1}{n}$. If we know a formula for the nth term, we often use this formula to represent the sequence. For example, we might say

$$\text{Define the sequence } \langle a_n \rangle \text{ by } a_n = \frac{1}{n} \text{ for each } n \in \mathbb{N}.$$

This shows that this sequence is a function with domain $\mathbb{N}$. If it is understood that the domain is $\mathbb{N}$, we could refer to this as the sequence $\langle \frac{1}{n} \rangle$. Given an element of the domain, we can consider a_n to be the output. In this case, we have used subscript notation to indicate the output rather than the usual function notation. We could just as easily write

$$a(n) = \frac{1}{n} \text{ instead of } a_n = \frac{1}{n}.$$

We make the following formal definition.

Definition: sequence

An (infinite) **sequence** is a function whose domain is $\mathbb{N}$ or some infinite subset of $\mathbb{N} \cup \{0\}$.

Progress Check 6.8 (Sequences)

Find the sixth and tenth terms of each of the following sequences:

1. $\frac{1}{3}, \frac{1}{6}, \frac{1}{9}, \frac{1}{12}, \ldots$
2. $\langle a_n \rangle$, where $a_n = \frac{1}{n^2}$ for each $n \in \mathbb{N}$

3. $\langle (-1)^n \rangle$

Answer

Add texts here. Do not delete this text first.

Functions of Two Variables

In Section 5.4, we learned how to form the Cartesian product of two sets. Recall that a Cartesian product of two sets is a set of ordered pairs. For example, the set $\mathbb{Z} \times \mathbb{Z}$ is the set of all ordered pairs, where each coordinate of an ordered pair is an integer. Since a Cartesian product is a set, it could be used as the domain or codomain of a function. For example, we could use $\mathbb{Z} \times \mathbb{Z}$ as the domain of a function as follows:

$$\text{Let } f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \text{ be defined by } f(m, n) = 2m + n.$$

- Technically, an element of $\mathbb{Z} \times \mathbb{Z}$ is an ordered pair, and so we should write $f((m, n))$ for the out put of the function f when the input is the ordered pair (m, n). However, the double parentheses seem unnecessary in this context and there should be no confusion if we write $f(m, n)$ for the output of the function f when the input is (m, n). So, for example, we simply write

$$\begin{aligned} f(3, 2) &= 2 \cdot 3 + 2 = 8, \text{ and} \\ f(-4, 5) &= 2 \cdot (-4) + 5 = -3. \end{aligned} \tag{6.2.3}$$

- Since the domain of this function is $\mathbb{Z} \times \mathbb{Z}$ and each element of $\mathbb{Z} \times \mathbb{Z}$ is an ordered pair of integers, we frequently call this type of function a **function of two variables.**

Finding the preimages of an element of the codomain for the function f, $\mathbb{Z}$, usually involves solving an equation with two variables. For example, to find the preimages of 0 2 Z, we need to find all ordered pairs $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(m, n) = 0$. This means that we must find all ordered pairs $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that

$$2m + n = 0$$

Three such ordered pairs are (0,0), (1, -2), and (-1, 2). In fact, whenever we choose an integer value for m, we can find a corresponding integer n such that $2m + n = 0$. This means that 0 has infinitely many preimages, and it may be difficult to specify the set of all of the preimages of 0 using the roster method. One way that can be used to specify this set is to use set builder notation and say that the following set consists of all of the preimages of 0:

$$\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid 2m + n = 0\} = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid n = -2m\}.$$

The second formulation for this set was obtained by solving the equation $2m + n = 0$ for n.

? Progress Check 6.9 (Working with a Function of Two Variables)

Let $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $g(m, n) = m^2 - n$ for all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$.

1. Determine $g(0, 3)$, $g(3, -2)$, $g(-3, -2)$, and $g(7, -1)$.
2. Determine the set of all preimages of the integer 0 for the function g. Write your answer using set builder notation.
3. Determine the set of all preimages of the integer 5 for the function g. Write your answer using set builder notation.

Answer

Add texts here. Do not delete this text first.

? Exercise 6.2

1. Let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Define $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $f(x) = x^2 + 4 \pmod 5$ and define $g : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $g(x) = (x + 1)(x + 4) \pmod 5$.

   (a) Calculate $f(0)$, $f(1)$, $f(2)$, $f(3)$, and $f(4)$.
   (b) Calculate $g(0)$, $g(1)$, $g(2)$, $g(3)$, and $g(4)$.
   (c) Is the function f equal to the function g? Explain.

2. Let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Define $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $f(x) = x^2 + 4 \pmod 5$ and define $g : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $g(x) = (x + 1)(x + 4) \pmod 5$.

   (a) Calculate $f(0)$, $f(1)$, $f(2)$, $f(3)$, and $f(4)$.
   (b) Calculate $g(0)$, $g(1)$, $g(2)$, $g(3)$, and $g(4)$.
   (c) Is the function f equal to the function g? Explain.

3. Let $f : (\mathbb{R} - \{0\}) \to \mathbb{R}$ by $f(x) = \dfrac{x^3 + 5x}{x}$ and let $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2 + 5$.

   (a) Calculate $f(2)$, $f(-2)$, $f(3)$, and $f(\sqrt{2})$.
   (b) Calculate $g(0)$, $g(2)$, $g(-2)$, $g(3)$, and $g(\sqrt{2})$.
   (c) Is the function f equal to the function g? Explain.
   (d) Now let $h : (\mathbb{R} - \{0\}) \to \mathbb{R}$ by $h(x) = x^2 + 5$. Is the function f equal to the function h? Explain.

4. Represent each of the following sequences as functions. In each case, state the domain, codomain, and rule for determining the outputs of the function. Also, determine if any of the sequences are equal.

   (a) $1, \dfrac{1}{4}, \dfrac{1}{9}, \dfrac{1}{16}, \ldots$
   (b) $\dfrac{1}{3}, \dfrac{1}{9}, \dfrac{1}{27}, \dfrac{1}{81}, \ldots$
   (c) 1, -1, 1, -1, 1, -1, ...
   (d) cos(0), cos(π), cos(2π), cos(3π), cos(4π), ...

5. Let A and B be two nonempty sets. There are two **projection functions** with domain $A \times B$, the Cartesian product of A and B. One projection function will map an ordered pair to its first coordinate, and the other projection function will map the ordered pair to its second coordinate. So we define
   $p_1 : A \times B \to A$ by $p_1(a, b) = a$ for every $(a, b) \in A \times B$; and
   $p_2 : A \times B \to B$ by $p_2(a, b) = a$ for every $(a, b) \in A \times B$.
   Let $A = \{1, 2\}$ and let $B = \{x, y, z\}$.

   (a) Determine the outputs for all possible inputs for the projection function$p_1 : A \times B \to A$.
   (b) Determine the outputs for all possible inputs for the projection function$p_2 : A \times B \to B$.
   (c) What is the range of these projection functions?
   (d) Is the following statement true or false? Explain.
   For all $(m, n), (u, v) \in A \times B$, if $(m, n) \neq (u, v)$, then
   $p_1(m, n) \neq p_1(u, v)$.

6. Let $D = \mathbb{N} - \{1, 2\}$ and define $d : D \to \mathbb{N} \cup \{0\}$ by $d(n) =$ the number of diagonals of a convex polygon with n sides. In Preview Activity 6.2.1, we showed that for values of n from 3 through 8,

$$d(n) = \frac{n(n-3)}{2}. \tag{6.2.4}$$

   Use mathematical induction to prove that for all $n \in D$,

$$d(n) = \frac{n(n-3)}{2}. \tag{6.2.5}$$

   Hint: To get an idea of how to handle the inductive step, use a pentagon. First, form all the diagonals that can be made from four of the vertices. Then consider how to make new diagonals when the fifth vertex is used. This may generate an idea of how to proceed from a polygon with k sides to a polygon with $k + 1$ sides.

7. Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m, n) = m + 3n$.

   (a) Calculate $f(-3, 4)$ and $f(-2, -7)$.

(b) Determine the set of all the preimages of 4 by using set builder notation to describe the set of all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that $f(m, n) = 4$.

8. Let $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be defined by $g(m, n) = (2m, m - n)$.

   (a) Calculate $g(3, 5)$ and $g(-1, 4)$.
   (b) Determine all the preimages of .0; 0/. That is, find all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that $g(m, n) = (0, 0)$.
   (c) Determine the set of all the preimages of (8, -3).
   (d) Determine the set of all the preimages of (1, 1).
   (e) Is the following proposition true or false? Justify your conclusion.
   For each $(s, t) \in \mathbb{Z} \times \mathbb{Z}$, there exists an $(m, n) \in \mathbb{Z} \times \mathbb{Z}$ such that $g(m, n) = (s, t)$.

9. A **2 by 2 matrix over** $\mathbb{R}$ is a rectangular array of four real numbers arranged in two rows and two columns. We usually write this array inside brackets (or parentheses) as follows:

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{6.2.6}$$

   where a, b, c and d are real numbers. The **determinant** of the 2 by 2 matrix A, denoted by det(A), is defined as det(A) = $ad - bc$.

   (a) Calculate the determinant of each of the following matrices:
   $\begin{bmatrix} 3 & 5 \\ 4 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}$, and $\begin{bmatrix} 3 & -2 \\ 5 & 0 \end{bmatrix}$.
   (b) Let $\mathcal{M}_2(\mathbb{R})$ be the set of all 2 by 2 matrices over $\mathbb{R}$. The mathematical process of finding the determinant of a 2 by 2 matrix over $\mathbb{R}$ can be thought of as a function. Explain carefully how to do so, including a clear statement of the domain and codomain of this function.

10. Using the notation from Exercise (9), let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \tag{6.2.7}$$

   be a 2 by 2 matrix over $\mathbb{R}$. The transpose of the matrix A, denoted by A^T, is the 2 by 2 matrix over $\mathbb{R}$ defined by

$$A^T = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \tag{6.2.8}$$

   (a) Calculate the transpose of each of the following matrices:
   $\begin{bmatrix} 3 & 5 \\ 4 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}$, and $\begin{bmatrix} 3 & -2 \\ 5 & 0 \end{bmatrix}$.
   (b) Let $\mathcal{M}_2(\mathbb{R})$ be the set of all 2 by 2 matrices over $\mathbb{R}$. The mathematical process of finding the determinant of a 2 by 2 matrix over $\mathbb{R}$ can be thought of as a function. Explain carefully how to do so, including a clear statement of the domain and codomain of this function.

Explorations and Activities

11. **Integration as a Function.** In calculus, we learned that if f is real function that is continuous on the closed interval [a, b], then the definite integral $\int_a^b f(x)dx$ is a real number. In fact, one form of the **Fundamental Theorem of Calculus** states that

$$\int_a^b f(x)dx = F(b) - F(a), \tag{6.2.9}$$

where F is any antiderivative of f, that is, where $F\prime = f$.

(a) Let $[a, b]$ be a closed interval of real numbers and let $C[a, b]$ be the set of all real functions that are continuous on $[a, b]$. That is,

$$C[a, b] = \{f : [a, b] \to \mathbb{R} \mid f \text{ is continuous on } [a, b]\}. \tag{6.2.10}$$

i. Explain how the definite integral $\int_a^b f(x)dx$ can be used to define a function I from $C[a, b]$ to $\mathbb{R}$.
ii. Let $[a, b] = [0, 2]$. Calculate $I(f)$, where $f(x) = x^2 + 1$.
iii. Let $[a, b] = [0, 2]$. Calculate $I(g)$, where $g(x) = sin(\pi x)$.

In calculus, we also learned how to determine the indefinite integral $\int f(x)dx$ of a continuous funtion f.

(b) Let $f(x) = x^2 + 1$ and $g(x) = cos(2x)$. Determine $\int f(x)dx$ and $\int g(x)dx$.
(c) Let f be a continuous function on the closed interval [0, 1] and let T be the set of all real functions. Can the process of determining the indefinite integral of a continuous function be used to define a function from $C[0, 1]$ to T? Explain.
(d) Another form of the Fundamental Theorem of Calculus states that if f is continuous on the interval $[a, b]$ and if

$$g(x) = \int_a^x f(t)dt \tag{6.2.11}$$

For each x in $[a, b]$, then $g\prime(x) = f(x)$. That is, g is an antiderivative of f. Explain how this t heorem can be used to define a function from $C[a, b]$ to T, where the output of the function i s an antiderivative of the input. (Recall that T is the set of all real functions.)

Answer

Add texts here. Do not delete this text first.

6.3: Injections, Surjections, and Bijections

Functions are frequently used in mathematics to define and describe certain relationships between sets and other mathematical objects. In addition, functions can be used to impose certain mathematical structures on sets. In this section, we will study special types of functions that are used to describe these relationships that are called injections and surjections. Before defining these types of functions, we will revisit what the definition of a function tells us and explore certain functions with finite domains.

? Preview Activity 6.3.1: Functions with Finite Domains

Let A and B be sets. Given a function $f : A \to B$, we know the following:

- For every $x \in A$, $f(x) \in B$. That is, every element of A is an input for the function f. This could also be stated as follows: For each $x \in A$, there exists a $y \in B$ such that $y = f(x)$.
- For a given $x \in A$, there is exactly one $y \in B$ such that $y = f(x)$.

The definition of a function does not require that different inputs produce different outputs. That is, it is possible to have $x_1, x_2 \in A$ with $x1 \neq x_2$ and $f(x_1) = f(x_2)$. The arrow diagram for the function f in Figure 6.5 illustrates such a function.

Also, the definition of a function does not require that the range of the function must equal the codomain. The range is always a subset of the codomain, but these two sets are not required to be equal. That is, if $g : A \to B$, then it is possible to have a $y \in B$ such that $g(x) \neq y$ for all $x \in A$. The arrow diagram for the function g in Figure 6.5 illustrates such a function.

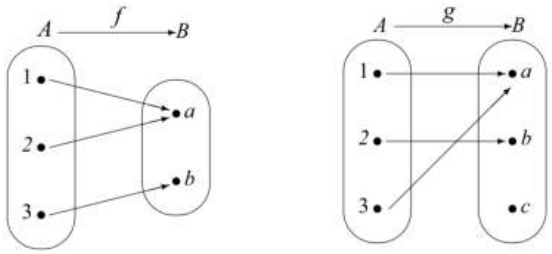


Figure 6.5: Arrow Diagram for Two Functions

Now let $A = \{1, 2, 3\}$, $B = \{a, b, c, d\}$, and $C = \{s, t\}$. Define

$f : A \to B$ by	$g : A \to B$ by	$h : A \to C$ by
$f(1) = a$	$g(1) = a$	$h(1) = s$
$f(2) = b$	$g(2) = b$	$h(2) = t$
$f(3) = c$	$g(3) = a$	$h(3) = s$

1. Which of these functions satisfy the following property for a function F?
   For all $x, y \in \text{dom}(F)$, if $x \neq y$, then $F(x) \neq F(y)$.
2. Which of these functions satisfy the following property for a function F?
   For all $x, y \in \text{dom}(F)$, if $F(x) = F(y)$, then $x = y$.
3. Determine the range of each of these functions.
4. Which of these functions have their range equal to their codomain?
5. Which of the these functions satisfy the following property for a function F?
   For all y in the codomain of F, there exists an $x \in \text{dom}(F\backslash)$ such that $F(x) = y$.

? Preview Activity 6.3.1: Statements Involving Functions

Let A and B be nonempty sets and let $f : A \to B$. In Preview Activity 6.3.1, we determined whether or not certain functions satisfied some specified properties. These properties were written in the form of statements, and we will now examine these statements in more detail.

1. Consider the following statement:
   For all $x, y \in A$, if $x \neq y$, then $f(x) \neq f(y)$.

   (a) Write the contrapositive of this conditional statement.
   (b) Write the negation of this conditional statement.
2. Now consider the statement:
   For all $y \in B$, there exists an $x \in A$ such that $f(x) = y$.
   Write the negation of this statement.
3. Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = 5x + 3$, for all $x \in \mathbb{R}$. Complete the following proofs of the following propositions about the function g.

   Proposition 1. For all $a, b \in \mathbb{R}$, if $g(a) = g(b)$, then $a = b$.
   Proof. We let $a, b \in \mathbb{R}$, and we assume that $g(a) = g(b)$ and will prove that $a = b$. Since $g(a) = g(b)$, we know that

   $$5a + 3 = 5b + 3. \tag{6.3.1}$$

   (Now prove that in this situation, $a = b$.)

   Proposition 2. For all $b \in \mathbb{R}$, there exists an $a \in \mathbb{R}$ such that $g(a) = b$.
   Proof. We let $b \in \mathbb{R}$. We will prove that there exists an $a \in \mathbb{R}$ such that $g(a) = b$ by constructing such an a in $\mathbb{R}$. In order for this to happen, we need $g(a) = 5a + 3 = b$.
   (Now solve the equation for a and then show that for this real number a, $g(a) = b$.)

Injections

In previous sections and in Preview Activity 6.3.1, we have seen examples of functions for which there exist different inputs that produce the same output. Using more formal notation, this means that there are functions $f : A \to B$ for which there exist $x_1, x_2 \in A$ with $x_1 \neq x_2$ and $f(x_1) = f(x_2)$. The work in the preview activities was intended to motivate the following definition.

Definition

Let $f : A \to B$ be a function from the set A to the set B. The function f is called an **injection** provided that

for all $x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$.

When f is an injection, we also say that f is a **one-to-one function**, or that f is an **injective function.**

Notice that the condition that specifies that a function f is an injection is given in the form of a conditional statement. As we shall see, in proofs, it is usually easier to use the contrapositive of this conditional statement. Although we did not define the term then, we have already written the contrapositive for the conditional statement in the definition of an injection in Part (1) of Preview Activity 6.3.2. In that preview activity, we also wrote the negation of the definition of an injection. Following is a summary of this work giving the conditions for f being an injection or not being an injection.

Let $f : A \to B$

"The function f is an injection" means that

- for all $x_1, x_2 \in A$, if $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$; or
- for all $x_1, x_2 \in A$, if $f(x_1) = f(x_2)$, then $x_1 = x_2$.

"The function f is not an injection" means that

- There exist $x_1, x_2 \in A$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.

? Progress Check 6.10 (Working with the Definition of an Injection)

Now that we have defined what it means for a function to be an injection, we can see that in Part (3) of Preview Activity 6.3.2, we proved that the function $g: \mathbb{R} \to \mathbb{R}$ is an injection, where $g(x/) = 5x + 3$ for all $x \in \mathbb{R}$. Use the definition (or its negation) to determine whether or not the following functions are injections.

1. $k : A \to B$, where $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $k(a) = 4$, $k(b) = 1$, and $k(c) = 3$.
2. $f : A \to C$, where $A = \{a, b, c\}$, $C = \{1, 2, 3\}$, and $f(a) = 2$, $f(b) = 3$, and $f(c) = 2$.
3. $F : \mathbb{Z} \to \mathbb{Z}$ defined by $F(m) = 3m + 2$ for all $m \in \mathbb{Z}$
4. $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = x^2 - 3x$ for all $x \in \mathbb{R}$
5. $s : \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $sx) = x^3$ for all $x \in \mathbb{Z}_5$

Answer

Add texts here. Do not delete this text first.

Surjections

In previous sections and in Preview Activity 6.3.1, we have seen that there exist functions $f : A \to B$ for which range$(f) = B$. This means that every element of B is an output of the function f for some input from the set A. Using quantifiers, this means that for every $y \in B$, there exists an $x \in A$ such that $f(x) = y$. One of the objectives of the preview activities was to motivate the following definition.

Definition

Let $f : A \to B$ be a function from the set A to the set B. The function f is called a **surjection** provided that the range of f equals the codomain of f. This means that

for every $y \in B$, there exists an $x \in A$ such that $f(x) = y$.

When f is a surjection, we also say that f is an **onto function** or that f maps A onto B. We also say that f is a **surjective function.**

One of the conditions that specifies that a function f is a surjection is given in the form of a universally quantified statement, which is the primary statement used in proving a function is (or is not) a surjection. Although we did not define the term then, we have already written the negation for the statement defining a surjection in Part (2) of Preview Activity 6.3.2. We now summarize the conditions for f being a surjection or not being a surjection.

Let $f : A \to B$

"The function f is a surjection" means that

- range(f) = codom(f) $= B$; or
- For every $y \in B$, there exsits an $x \in A$ such that $f(x) = y$.

“The function f is not a surjection” means that

- rang(f) \ne codom(f); or
- There exists a $y \in B$ such that for all $x \in A$, $f(x) \neq y$.

One other important type of function is when a function is both an injection and surjection. This type of function is called a bijection.

Definition

A **bijection** is a function that is both an injection and a surjection. If the function f is a bijection, we also say that f is **one-to-one and onto** and that f is a **bijective function.**

? Progress Check 6.11 (Working with the Definition of a Surjection)

Now that we have defined what it means for a function to be a surjection, we can see that in Part (3) of Preview Activity 6.3.2, we proved that the function $g : \mathbb{R} \to \mathbb{R}$ is a surjection, where $g(x) = 5x + 3$ for all $x \in \mathbb{R}$. Determine whether or not the following functions are surjections.

1. $k : A \to B$, where $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, and $k(a) = 4$, $k(b) = 1$, and $k(c) = 3$.
2. $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 3x + 2$ for all $x \in \mathbb{R}$.
3. $F : \mathbb{Z} \to \mathbb{Z}$ defined by $F(m) = 3m + 2$ for all $m \in \mathbb{Z}$.
4. $s : \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $s(x) = x^3$ for all $x \in \mathbb{Z}_5$.

Answer

Add texts here. Do not delete this text first.

The Importance of the Domain and Codomain

The functions in the next two examples will illustrate why the domain and the codomain of a function are just as important as the rule defining the outputs of a function when we need to determine if the function is a surjection.

✓ Example 6.12 (A Function that Is Neither an Injection nor a Surjection)

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 + 1$. Notice that

$$f(2) = 5 \text{ and } f(-2) = 5.$$

This is enough to prove that the function f is not an injection since this shows that there exist two different inputs that produce the same output.

Since $f(x) = x^2 + 1$, we know that $f(x) \geq 1$ for all $x \in \mathbb{R}$. This implies that the function f is not a surjection. For example, -2 is in the codomain of f and $f(x) \neq -2$ for all x in the domain of f.

✓ Example 6.13 (A Function that Is Not an Injection but Is a Surjection)

Let $T = \{y \in \mathbb{R} \mid y \geq 1\}$, and define $F : \mathbb{R} \to T$ by $F(x) = x^2 + 1$. As in Example 6.12, the function F is not an injection since $F(2) = F(-2) = 5$.

Is the function F a surjection? That is, does F map $\mathbb{R}$ onto T? As in Example 6.12, we do know that $F(x) \geq 1$ for all $x \in \mathbb{R}$.

To see if it is a surjection, we must determine if it is true that for every $y \in T$, there exists an $x \in \mathbb{R}$ such that $F(x) = y$. So we choose $y \in T$. The goal is to determine if there exists an $x \in \mathbb{R}$ such that

$$\begin{aligned} F(x) &= y, \text{ or} \\ x^2 + 1 &= y. \end{aligned} \tag{6.3.2}$$

One way to proceed is to work backward and solve the last equation (if possible) for x. Doing so, we get

$x^2 = y - 1$

$x = \sqrt{y-1}$ or $x = -\sqrt{y-1}$.

Now, since $y \in T$, we know that $y \geq 1$ and hence that $y - 1 \geq 0$. This means that $\sqrt{y-1} \in \mathbb{R}$. Hence, if we use $x = \sqrt{y-1}$, then $x \in \mathbb{R}$, and

$$\begin{aligned} F(x) &= F(\sqrt{y-1}) \\ &= (\sqrt{y-1})^2 + 1 \\ &= (y-1) + 1 \\ &= y. \end{aligned} \tag{6.3.3}$$

This proves that F is a surjection since we have shown that for all $y \in T$, there exists an

$x \in \mathbb{R}$ such that $F(x) = y$. Notice that for each $y \in T$, this was a constructive proof of the existence of an $x \in \mathbb{R}$ such that $F(x) = y$.

An Important Lesson.

In Examples 6.12 and 6.13, the same mathematical formula was used to determine the outputs for the functions. However, one function was not a surjection and the other one was a surjection. This illustrates the important fact that whether a function is surjective not only depends on the formula that defines the output of the function but also on the domain and codomain of the function.

The next example will show that whether or not a function is an injection also depends on the domain of the function.

Example 6.14 (A Function that Is a Injection but Is Not a Surjection)

Let $\mathbb{Z}^* = \{x \in \mathbb{Z} \mid x \geq 0\} = \mathbb{N} \cup \{0\}$. Define $g : \mathbb{Z}^* \to \mathbb{N}$ by $g(x) = x^2 + 1$. (Notice that this is the same formula used in Examples 6.12 and 6.13.) Following is a table of values for some inputs for the function g.

x	$g(x)$	x	$g(x)$
0	1	3	10
1	2	4	17
2	5	5	26

Notice that the codomain is $\mathbb{N}$, and the table of values suggests that some natural numbers are not outputs of this function. So it appears that the function g is not a surjection.

To prove that g is not a surjection, pick an element of $\mathbb{N}$ that does not appear to be in the range. We will use 3, and we will use a proof by contradiction to prove that there is no x in the domain ($\mathbb{Z}^*$) such that $g(x) = 3$. So we assume that there exists an $x \in \mathbb{Z}^*$ with $g(x) = 3$. Then

$$\begin{aligned} x^2 + 1 &= 3 \\ x^2 &= 2 \\ x &= \pm\sqrt{2}. \end{aligned} \tag{6.3.4}$$

But this is not possible since $\sqrt{2} \notin \mathbb{Z}^*$. Therefore, there is no $x \in \mathbb{Z}^*$ with $g(x) = 3$. This means that for every $x \in \mathbb{Z}^*$, $g(x) \neq 3$. Therefore, 3 is not in the range of g, and hence g is not a surjection.

The table of values suggests that different inputs produce different outputs, and hence that g is an injection. To prove that g is an injection, assume that $s, t \in \mathbb{Z}^*$ (the domain) with $g(s) = g(t)$. Then

$$\begin{aligned} s^2 + 1 &= t^2 + 1 \\ s^2 &= t^2. \end{aligned} \tag{6.3.5}$$

Since $s, t \in \mathbb{Z}^*$, we know that $s \geq 0$ and $t \geq 0$. So the preceding equation implies that $s = t$. Hence, g is an injection.

An Important Lesson

The functions in the three preceding examples all used the same formula to determine the outputs. The functions in Exam- ples 6.12 and 6.13 are not injections but the function in Example 6.14 is an injection. This illustrates the important fact that whether a function is injective not only depends on the formula that defines the output of the function but also on the domain of the function.

Progress Check 6.15 (The Importance of the Domain and Codomain)

Let $R^+ = \{y \in \mathbb{R} \mid y > 0\}$. Define

\[\begin{array} {rcl} {f} &: & {\mathbb{R} \to \mathbb{R} \text{ by } f(x) = e^{-x}, \text{ for each } x \in \mathbb{R}, \text{ and }} \\ {g} &: & {\mathbb{R} \to \mathbb{R}^{+} \text{ by } g(x) = e^{-x}, \text{ for each } x \in \mathbb{R}.} \end{array}

Determine if each of these functions is an injection or a surjection. Justify your conclusions. **Note**: Before writing proofs, it might be helpful to draw the graph of $y = e^{-x}$. A reasonable graph can be obtained using $-3 \leq x \leq 3$ and $-2 \leq y \leq 10$. Please keep in mind that the graph is does not prove your conclusions, but may help you arrive at the correct conclusions, which will still need proof.

Answer

Add texts here. Do not delete this text first.

Working with a Function of Two Variables

It takes time and practice to become efficient at working with the formal definitions of injection and surjection. As we have seen, all parts of a function are important (the domain, the codomain, and the rule for determining outputs). This is especially true for functions of two variables.

For example, we define $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ by

$$f(a,b) = (2a+b, a-b) \quad \text{for all } (a,b) \in \mathbb{R} \times \mathbb{R}\,.$$

Notice that both the domain and the codomain of this function is the set $\mathbb{R} \times \mathbb{R}$. Thus, the inputs and the outputs of this function are ordered pairs of real numbers. For example,

$$f(1,1) = (3,0) \text{ and } f(-1,2) = (0,-3).$$

To explore wheter or not f is an injection, we assume that $(a,b) \in \mathbb{R} \times \mathbb{R}$, $(c,d) \in \mathbb{R} \times \mathbb{R}$, and $f(a,b) = f(c,d)$. This means that

$$(2a+b, a-b) = (2c+d, c-d) \quad .$$

Since this equation is an equality of ordered pairs, we see that

$$\begin{aligned} 2a+b &= 2c+d, \text{ and} \\ a-b &= c-d. \end{aligned} \tag{6.3.6}$$

By adding the corresponding sides of the two equations in this system, we obtain $3a = 3c$ and hence, $a = c$. Substituting $a = c$ into either equation in the system give us $b = d$. Since $a = c$ and $b = d$, we conclude that

$$(a,b) = (c,d)\,.$$

Hence, we have shown that if $f(a,b) = f(c,d)$, then $(a,b) = (c,d)$. Therefore, f is an injection.

Now, to determine if f is a surjection, we let $(r,s) \in \mathbb{R} \times \mathbb{R}$, where (r,s) is considered to be an arbitrary element of the codomain of the function f . Can we find an ordered pair $(a,b) \in \mathbb{R} \times \mathbb{R}$ such that $f(a,b) = (r,s)$? Working backward, we see that in order to do this, we need

$$(2a+b, a-b) = (r,s).$$

That is, we need

$$2a+b = r \text{ and } a-b = s\,.$$

Solving this system for a and b yields

$$a = \frac{r+s}{3} \text{ and } b = \frac{r-2s}{3}\,.$$

Since $r, s \in \mathbb{R}$, we can conclude that $a \in \mathbb{R}$ and $b \in \mathbb{R}$ and hence that $(a,b) \in \mathbb{R} \times \mathbb{R}$.

We now need to verify that for. these values of a and b, we get $f(a,b) = (r,s)$. So

$$\begin{aligned} f(a,b) &= f\left(\frac{r+s}{3}, \frac{r-2s}{3}\right) \\ &= \left(2\left(\frac{r+s}{3}\right) + \frac{r-2s}{3}, \frac{r+s}{3} - \frac{r-2s}{3}\right) \\ &= \left(\frac{2r+2s+r-2s}{3}, \frac{r+s-r+2s}{3}\right) \\ &= (r,s). \end{aligned} \tag{6.3.7}$$

This proves that for all $(r, s) \in \mathbb{R} \times \mathbb{R}$, there exists $(a, b) \in \mathbb{R} \times \mathbb{R}$ such that $f(a, b) = (r, s)$. Hence, the function f is a surjection. Since f is both an injection and a surjection, it is a bijection.

? Progress Check 6.16 (A Function of Two Variables)

Let $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be defined by $g(x, y) = 2x + y$, for all $(x, y) \in \mathbb{R} \times \mathbb{R}$.

Note: Be careful! One major difference between this function and the previous example is that for the function g, the codomain is $\mathbb{R}$, not $\mathbb{R} \times \mathbb{R}$. It is a good idea to begin by computing several outputs for several inputs (and remember that the inputs are ordered pairs).

1. Notice that the ordered pair $(1, 0) \in \mathbb{R} \times \mathbb{R}$. That is (1, 0) is in the domain of g. Also notice that $g(1, 0) = 2$. Is it possible to find another ordered pair $(a, b) \in \mathbb{R} \times \mathbb{R}$ such that $g(a, b) = 2$?
2. Let $z \in \mathbb{R}$. Then $(0, z) \in \mathbb{R} \times \mathbb{R}$ and so $(0, z) \in \text{dom}(g)$. Now determine $g(0, z)$?
3. Is the function g an injection? Is the function g a surjection? Justify your conclusions.

Answer

Add texts here. Do not delete this text first.

? Exercise 6.3

1. (a) Draw an arrow diagram that represents a function that is an injection but is not a surjection.
   (b) Draw an arrow diagram that represents a function that is an injection and is a surjection.
   (c) Draw an arrow diagram that represents a function that is not an injection and is not a surjection.
   (d) Draw an arrow diagram that represents a function that is not an injection but is a surjection.
   (e) Draw an arrow diagram that represents a function that is not a bijection.
2. Let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ and let $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. For each of the following functions, determine if the function is an injection and determine if the function is a surjection. Justify all conclusions.

   (a) $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $f(x) = x^2 + 4 \pmod 5$, for all $x \in \mathbb{Z}_5$
   (b) $g : \mathbb{Z}_6 \to \mathbb{Z}_6$ by $g(x) = x^2 + 4 \pmod 6$, for all $x \in \mathbb{Z}_6$
   (c) $F : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $F(x) = x^3 + 4 \pmod 5$, for all $x \in \mathbb{Z}_5$
3. For each of the following functions, determine if the function is an injection and determine if the function is a surjection. Justify all conclusions.

   (a) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 3x + 1$, for all $x \in \mathbb{Z}$.
   (b) $F : \mathbb{Q} \to \mathbb{Q}$ defined by $F(x) = 3x + 1$, for all $x \in \mathbb{Q}$.
   (c) $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^3$, for all $x \in \mathbb{R}$.
   (d) $G : \mathbb{Q} \to \mathbb{Q}$ defined by $G(x) = x^3$, for all $x \in \mathbb{Q}$.
   (e) $k : \mathbb{R} \to \mathbb{R}$ defined by $k(x) = e^{-x^2}$, for all $x \in \mathbb{R}$.
   (f) $K : \mathbb{R}^* \to \mathbb{R}$ defined by $K(x) = e^{-x^2}$, for all $x \in \mathbb{R}^*$.
   Note: $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$.
   (g) $K_1 : \mathbb{R}^* \to T$ defined by $K_1(x) = e^{-x^2}$, for all $x \in \mathbb{R}^*$, where $T = \{y \in \mathbb{R} \mid 0 < y \leq 1\}$.
   (h) $h : \mathbb{R} \to \mathbb{R}$ defined by $h(x) = \dfrac{2x}{x^2 + 4}$, for all $x \in \mathbb{R}$.
   (i) $H : \{x \in \mathbb{R} \mid x \geq 0\} \to \{y \in \mathbb{R} \mid 0 \leq y \leq \dfrac{1}{2}\}$ defined by $H(x) = \dfrac{2x}{x^2 + 4}$, for all $x \in \{x \in \mathbb{R} \mid x \geq 0\}$.
4. For each of the following functions, determine if the function is a bijection. Justify all conclusions.

   (a) $F : \mathbb{R} \to \mathbb{R}$ defined by $F(x) = 5x + 3$, for all $x \in \mathbb{R}$.
   (b) $G : \mathbb{Z} \to \mathbb{Z}$ defined by $G(x) = 5x + 3$, for all $x \in \mathbb{Z}$.
   (c) $f : (\mathbb{R} - \{4\}) \to \mathbb{R}$ defined by $f(x) = \dfrac{3x}{x - 4}$, for all $x \in (\mathbb{R} - \{4\})$.
   (d) $g : (\mathbb{R} - \{4\}) \to (\mathbb{R} - \{3\})$ defined by $g(x) = \dfrac{3x}{x - 4}$, for all $x \in (\mathbb{R} - \{4\})$.

5. Let $s : \mathbb{N} \to \mathbb{N}$, where for each $n \in \mathbb{N}$, $s(n)$ is the sum of the distinct natural number divisors of n. This is the **sum of the divisors function** that was introduced in Preview Activity 6.3.2 from Section 6.1. Is s an injection? Is s a surjection? Justify your conclusions.
6. Let $d : \mathbb{N} \to \mathbb{N}$, where $d(n)$ is the number of natural number divisors of n. This is the **number of divisors function** introduced in Exercise (6) from Section 6.1. Is the function d an injection? Is the function d a surjection? Justify your conclusions.
7. In Preview Activity 6.3.2 from Section 6.1 , we introduced the **birthday function**. Is the birthday function an injection? Is it a surjection? Justify your conclusions.
8. (a) Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m, n) = 2m + n$. Is the function f an injection? Is the function f a surjection? Justify your conclusions.
   (b) Let $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined by $g(m, n) = 6m + 3n$. Is the function g an injection? Is the function g a surjection? Justify your conclusions.
9. (a) Let $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ be defined by $f(x, y) = (2x, x + y)$. Is the function f an injection? Is the function f a surjection? Justify your conclusions.
   (b) Let $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be defined by $g(x, y) = (2x, x + y)$. Is the function g an injection? Is the function g a surjection? Justify your conclusions.
10. Let $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x, y) = -x^2y + 3y$, for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Is the function f and injection? Is the function f a surjection? Justify your conclusions.
11. Let $g : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ be the function defined by $g(x, y) = (x^3 + 2)siny$, for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Is the function g and injection? Is the function g a surjection? Justify your conclusions.
12. Let A be a nonempty set. The **identity function on the set A**, denoted by I_A, is the function $I_A : A \to A$ defined by $I_A(x) = x$ for every x in A. Is I_A an injection? Is I_A a surjection? Justify your conclusions.
13. Let A and B be two nonempty sets. Define

$$p_1 : A \times B \to A \text{ by } p_1(a, b) = a \tag{6.3.8}$$

    for every $(a, b) \in A \times B$. That is the **first projection function** introduced in Exercise (5) in Section 6.2.
    (a) Is the function p_1 a surjection? Justify your conclusion.
    (b) If $B = \{b\}$, is the function p_1 an injection? Justify your conclusion.
    (c) Under what condition(s) is the function p_1 not an injection? Make a conjecture and prove it.
14. Define $f : \mathbb{N} \to \mathbb{Z}$ be defined as follows: For each $n \in \mathbb{N}$,

$$f(n) = \frac{1 + (-1)^n(2n - 1)}{4}. \tag{6.3.9}$$

    Is the function f an injection? Is the function f a surjection? Justify your conclusions.

    Suggestions. Start by calculating several outputs for the function before you attempt to write a proof. In exploring whether or not the function is an injection, it might be a good idea to uses cases based on whether the inputs are even or odd. In exploring whether f is a surjection, consider using cases based on whether the output is positive or less than or equal to zero.
15. Let C be the set of all real functions that are continuous on the closed interval [0, 1]. Define the function $A : C \to \mathbb{R}$ as follows: For each $f \in C$.

$$A(f) = \int_0^1 f(x)dx. \tag{6.3.10}$$

    Is the function A an injection? Is it a surjection? Justify your conclusions.
16. Let $A = \{(m, n) \mid m \in \mathbb{Z}, n \in \mathbb{Z}, \text{ and } n \neq 0\}$. Define $f : A \to \mathbb{Q}$ as follows:
    For each $(m, n) \in A$, $f(m, n) = \dfrac{m + n}{n}$.
    (a) Is the function f an injection? Justify your conclusion.
    (b) Is the function f a surjection? Justify your conclusion.

17. **Evaluation of proofs**
See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

Proposition. The function $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ defined by $f(x, y) = (2x + y, x - y)$ is an injection.

Proof

For each (a, b) and (c, d) in $\mathbb{R} \times \mathbb{R}$, if $f(a, b) = f(c, d)$, then

$$(2a + b, a - b) = (2c + d, c - d).$$

We will use systems of equations to prove that $a = c$ and $b = d$.

$$\begin{aligned} 2a + b &= 2c + d \\ a - b &= c - d \\ 3a &= 3c \\ a &= c \end{aligned} \tag{6.3.11}$$

Since $a = c$, we see that

$$(2c + b, c - b) = (2c + d, c - d).$$

So $b = d$. Therefore, we have proved that the function f is an injection.

(b)

Proposition. The function $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ defined by $f(x, y) = (2x + y, x - y)$ is an surjection.

Proof

We need to find an ordered pair such that $f(x, y) = (a, b)$ for each (a, b) in $\mathbb{R} \times \mathbb{R}$. That is, we need $(2x + y, x - y) = (a, b)$, or

$$2x + y = a \text{ and } x - y = b .$$

Treating these two equations as a system of equations and solving for x and y, we find that

$$x = \frac{a + b}{3} \text{ and } y = \frac{a - 2b}{3}.$$

Hence, x and y are real numbers, $(x, y) \in \mathbb{R} \times \mathbb{R}$, and

$$\begin{aligned} f(x, y) &= f(\frac{a + b}{3}, \frac{a - 2b}{3}) \\ &= (2(\frac{a + b}{3}) + \frac{a - 2b}{3}, \frac{a + b}{3} - \frac{a - 2b}{3}) \\ &= (\frac{2a + 2b + a - 2b}{3}, \frac{a + b - a + 2b}{3}) \\ &= (\frac{3a}{3}, \frac{3b}{3}) \\ &= (a, b). \end{aligned} \tag{6.3.12}$$

Therefore, we. have proved that for every $(a, b) \in \mathbb{R} \times \mathbb{R}$, there exists an $(x, y) \in \mathbb{R} \times \mathbb{R}$ such that $f(x, y) = (a, b)$. This proves that the function f is a surjection.

Explorations and Activities

18. **Piecewise Defined Functions**. We often say that a function is a **piecewise defined function** if it has different rules for determining the output for different parts of its domain. For example, we can define a function $f : \mathbb{R} \to \mathbb{R}$ by giving a rule for calculating $f(x)$ when $x \geq 0$ and giving a rule for calculating $f(x)$ when x < 0 as follows:

$$f(x) = \begin{cases} x^2 + 1, & \text{if } x \geq 0; \\ x - 1 & \text{if } x < 0. \end{cases} \tag{6.3.13}$$

(a) Sketch a graph of the function f. Is the function f and injection? Is the function f a surjection? Justify your conclusions.

For each of the following functions, determine if the function is an injection and determine if the function is a surjection. Justify all conclusions.

(b) $g : [0, 1] \to (0, 1)$ by

$$g(x) = \begin{cases} 0.8, & \text{if } x = 0; \\ 0.5x & \text{if } 0 < x < 1; \\ 0.6 & \text{if } x = 1. \end{cases} \tag{6.3.14}$$

(c) $h : \mathbb{Z} \to \{0, 1\}$ by

$$h(x) = \begin{cases} 0, & \text{if } x \text{ is even}; \\ 1, & \text{if } x \text{ is odd}. \end{cases} \tag{6.3.15}$$

19. **Functions Whose Domain is $\mathcal{M}_2(\mathbb{R})$.** Let $\mathcal{M}_2(\mathbb{R})$. represent the set of all 2 by 2 matrices over $\mathbb{R}$.

(a) Defien det: $\mathcal{M}_2(\mathbb{R}) \to \mathbb{R}$ by

$$det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = ad - bc. \tag{6.3.16}$$

This is the **determinant function** introduced in Exercise (9) from Section 6.2. Is the determinant function an injection? Is the determinant function a surjection? Justify your conclusions.

(b) Define tran: $\mathcal{M}_2(\mathbb{R}) \to \mathcal{M}_2(\mathbb{R})$ by

$$tran \begin{bmatrix} a & b \\ c & d \end{bmatrix} = A^T = \begin{bmatrix} a & c \\ b & d \end{bmatrix}. \tag{6.3.17}$$

This is the **transpose function** introduced in Exercise (10) from Section 6.2. Is the transpose function an injection? Is the transpose function a surjection? Justify your conclusions.

(c) Define $F : \mathcal{M}_2(\mathbb{R}) \to \mathbb{R}$ by

$$F \begin{bmatrix} a & b \\ c & d \end{bmatrix} = a^2 + d^2 - b^2 - c^2. \tag{6.3.18}$$

Is the function F an injection? Is the function F a surjection? Justify your conclusions.

Answer

Add texts here. Do not delete this text first.

6.4: Composition of Functions

PREVIEW ACTIVITY 6.4.1: Constructing a New Function

Let $A = \{a, b, c, d\}$, $B = \{p, q, r\}$, and $C = \{s, t, u, v\}$. The arrow diagram in Figure 6.6 shows two functions: $f : A \to B$ and $g : B \to C$. Notice that if $x \in A$, then $f(x) \in B$. Since $f(x) \in B$, we can apply the function g to $f(x)$, and we obtain $g(f(x))$, which is an element of C.

Using this process, determine $g(f(a))$, $g(f(b))$, $g(f(c))$, and $g(f(d))$. Then explain how we can use this information to define a function from A to C.

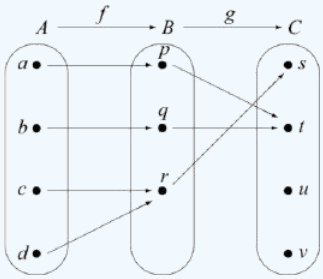


Figure 6.6: Arrow Diagram Showing Two Functions

PREVIEW ACTIVITY 6.4.1: Verbal Descriptions of Functions

The outputs of most real functions we have studied in previous mathematics courses have been determined by mathematical expressions. In many cases, it is possible to use these expressions to give step-by-step verbal descriptions of how to compute the outputs. For example, if

$$f : \mathbb{R} \to \mathbb{R} \text{ is defined by } f(x) = (3x + 2)^3,$$

we could describe how to compute the outputs as follows:

Step	**Verbal Description**	**Symbolic Result**
1	Choose an input.	x
2	Multiply by 3.	$3x$
3	Add 2.	$3x + 2$
4	Cube the result.	$(3x + 3)^3$

Complete step-by-step verbal descriptions for each of the following functions.

1. $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \sqrt{3x^2 + 2}$, for each $x \in \mathbb{R}$.
2. $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = \sin(3x^2 + 2)$, for each $x \in \mathbb{R}$.
3. $h : \mathbb{R} \to \mathbb{R}$ by $h(x) = e^{3x^2+2}$, for each $x \in \mathbb{R}$.
4. $G : \mathbb{R} \to \mathbb{R}$ by $G(x) = \ln(x^4 + 3)$, for each $x \in \mathbb{R}$.
5. $k : \mathbb{R} \to \mathbb{R}$ by $k(x) = \sqrt[3]{\dfrac{\sin(4x + 3)}{x^2 + 1}}$, for each $x \in \mathbb{R}$.

Composition of Functions

There are several ways to combine two existing functions to create a new function. For example, in calculus, we learned how to form the product and quotient of two functions and then how to use the product rule to determine the derivative of a product of two functions and the quotient rule to determine the derivative of the quotient of two functions. The chain rule in calculus was used to determine the derivative of the composition of two functions, and in this section, we will focus only on the composition of two functions. We will then consider some results about the compositions of injections and surjections.

The basic idea of function composition is that when possible, the output of a function f is used as the input of a function g. This can be referred to as "f followed by g" and is called the composition of f and g. In previous mathematics courses, we used this idea to determine a formula for the composition of two real functions.

For example, if

$$f(x) = 3x^2 + 2 \text{ and } g(x) = sinx$$

then we can compute $g(f(x))$ as follows:

$$\begin{aligned} g(f(x)) &= g(3x^2+2) \\ &= sin(3x^2+2). \end{aligned} \tag{6.4.1}$$

In this case, $f(x)$, the output of the function f, was used as the input for the function g. We now give the formal definition of the composition of two functions.

Definition: composite function

Let A, B, and C be nonempty sets, and let $f : A \to B$ and $g : B \to C$ be functions. The *composition* of f and g is the function $g \circ f : A \to C$ defined by

$$(g \circ f)(x) = g(f(x))$$

for all $x \in A$. We often refer to the function $g \circ f$ as a *composite function*.

It is helpful to think of composite function $g \circ f$ as "**f followed by g**". We then refer to f as the **inner function** and g as the **outer function**.

Composition and Arrow Diagrams

The concept of the composition of two functions can be illustrated with arrow diagrams when the domain and codomain of the functions are small, finite sets. Although the term "composition" was not used then, this was done in Preview Activity 6.4.1, and another example is given here.

Let $A = \{a, b, c, d\}$, $B = \{p, q, r\}$, and $C = \{s, t, u, v\}$. The arrow diagram in Figure 6.7 shows two functions: $f : A \to B$ and $g : B \to C$.

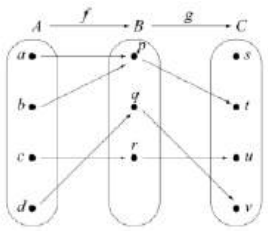


Figure 6.7: Arrow Diagram for Two Functions

If we follow the arrows from the set A to the set C, we will use the outputs of f as inputs of g, and get the arrow diagram from A to C shown in Figure 6.8. This diagram represents the composition of f followed by g.

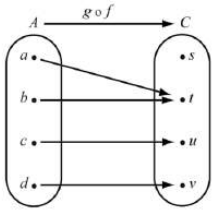


Figure 6.8: Arrow Diagram for $g \circ f : A \to C$

? Progress Check 6.17 (The Composition of Two Functions)

Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$. Define the function f and g as follows:

$f : A \to B$ defined by $f(a) = 2$, $f(b) = 3$, $f(c) = 1$, and $f(d) = 2$.

$g : A \to B$ defined by $g(1) = 3$. $g(2) = 1$, and $g(3) = 2$.

Create arrow diagrams for the function f, g, $g \circ f$, and $g \circ g$.

Answer

Add texts here. Do not delete this text first.

Decomposing Functions

We use the chain rule in calculus to find the derivative of a composite function. The first step in the process is to recognize a given function as a composite function. This can be done in many ways, but the work in Preview Activity 6.4.2 can be used to decompose a function in a way that works well with the chain rule. The use of the terms "inner function" and "outer function" can also be helpful. The idea is that we use the last step in the process to represent the outer function, and the steps prior to that to represent the inner function. So for the function,

$$f : \mathbb{R} \to \mathbb{R} \text{ by } f(x) = (3x + 2)^3,$$

the last step in the verbal description table was to cube the result. This means that we will use the function g (the cubing function) as the outer function and will use the prior steps as the inner function. We will denote the inner function by h. So we let $h : \mathbb{R} \to \mathbb{R}$ by $h(x) = 3x + 2$ and $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^3$. Then

$$\begin{aligned} (g \circ h)(x) &= g(h(x)) \\ &= g(3x + 2) \\ &= (3x + 2)^3 \\ &= f(x). \end{aligned} \tag{6.4.2}$$

We see that $g \circ h = f$ and, hence, we have "decomposed" the function f. It should be noted that there are other ways to write the function f as a composition of two functions, but the way just described is the one that works well with the chain rule. In this case, the chain rule gives

$$\begin{aligned} f\prime(x) &= (g \circ h)\prime(x) \\ &= g\prime(h(x))h\prime(x) \\ &= 3(h(x))^2 \cdot 3 \\ &= g(3x + 2)^2 \end{aligned} \tag{6.4.3}$$

? Progress Check 6.18 (Decomposing Functions

Write each of the following functions as the composition of two functions.

1. $F : \mathbb{R} \to \mathbb{R}$ by $F(x) = (x^2 + 3)^3$
2. $G : \mathbb{R} \to \mathbb{R}$ by $G(x) = In(x^2 + 3)$
3. $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = |x^2 - 3|$
4. $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = cos(\frac{2x - 3}{x^2 + 1})$

Answer

Add texts here. Do not delete this text first.

Theorems about Composite Functions

If $f : A \to B$ and $g : B \to C$, then we can form the composite function $g \circ f : A \to C$. In Section 6.3, we learned about injections and surjections. We now explore what type of function $g \circ f$ will be if the functions f and g are injections (or

surjections).

Progress Check 6.19: Compositions of Injections and Surjections

Although other representations of functions can be used, it will be helpful to use arrow diagrams to represent the functions in this progress check. We will use the following sets:

$$A = \{a, b, c\},\ B = \{p, q, r\},\ C = \{u, v, w, x\}, \text{ and } D = \{u, v\}.$$

1. Draw an arrow diagram for a function $f : A \to B$ that is an injection and an arrow diagram for a function $g : B \to C$ that is an injection. In this case, is the composite function $g \circ f : A \to C$ an injection? Explain.
2. Draw an arrow diagram for a function $f : A \to B$ that is a surjection and an arrow diagram for a function $g : B \to D$ that is a surjection. In this case, is the composite function $g \circ f : A \to D$ a surjection? Explain.
3. Draw an arrow diagram for a function $f : A \to B$ that is a bijection and an arrow diagram for a function $g : B \to A$ that is a bijection. In this case, is the composite function $g \circ f : A \to A$ bijection? Explain.

Answer

Add texts here. Do not delete this text first.

In Progress Check 6.19, we explored some properties of composite functions related to injections, surjections, and bijections. The following theorem contains results that these explorations were intended to illustrate. Some of the proofs will be included in the exercises.

Theorem 6.20.

Let A, B, and C be nonempty sets and assume that $f : A \to B$ and $g : B \to C$.

1. If f and g are both injections, then $(g \circ f) : A \to C$ is an injection.
2. If f and g are both surjections, then $(g \circ f) : A \to C$ is an surjection.
3. If f and g are both bijections, then $(g \circ f) : A \to C$ is an bijection.

Proof

The proof of Part (1) is Exercise (6).

Part (3) is a direct consequence of the first two parts. We will discuss a process for constructing a proof of Part (2). Using the forward-backward process, we first look at the conclusion of the conditional statement in Part (2). The goal is to prove that $g \circ f$ is a surjection. Since $(g \circ f) : A \to C$, this is equivalent to proving that

$$\text{For all } c \in C, \text{ there exists an } a \in A \text{ such that } (g \circ f)(a) = c.$$

Since this statement in the backward process uses a universal quantifier, we will use the choose-an-element method and choose an arbitrary element c in the set C. The goal now is to find an $a \in A$ such that $(g \circ f)(a) = c$.

Now we can look at the hypotheses. In particular, we are assuming that both $f : A \to B$ and $g : B \to C$ are surjections. Since we have chosen $c \in C$, and $g : B \to C$ is a surjection, we know that

$$\text{there exists a } b \in B \text{ such that } g(b) = c.$$

Now, $b \in B$ and $f : A \to B$ is a surjection. Hence

$$\text{there exists an } a \in A \text{ such that } f(a) = b.$$

If we now compute $(g \circ f)(a)$, we will see that

$$(g \circ f)(a) = g(f(a)) = g(b) = c \quad .$$

We can now write the proof as follows:

Proof of Theorem 6.20, Part (2)

Let A, B, and C be nonempty sets and assume that $f : A \to B$ and $g : B \to C$ are both surjections. We will prove that $g \circ f : A \to C$ is a surjection.

Let c be an arbitrary element of C. We will prove there exists an $a \in A$ such that $(g \circ f)(a) = c$. Since $g : B \to C$ is a surjection, we conclude that

$$\text{there exists a } b \in B \text{ such that } g(b) = c.$$

Now, $b \in B$ and $f : A \to B$ is a surjection. Hence

$$\text{there exists an } a \in A \text{ such that } f(a) = b.$$

We now see that

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) \\ &= g(b) \\ &= c. \end{aligned}$$

We have now shown that for every $c \in C$, there exists an $a \in A$ such that $(g \circ f)(a) = c$, and this proves that $g \circ f$ is a surjection.

Theorem 6.20 shows us that if f and g are both special types of functions, then the composition of f followed by g is also that type of function.The next question is, "If the composition of f followed by g is an injection (or surjection), can we make any conclusions about f or g?" A partial answer to this question is provided in Theorem 6.21. This theorem will be investigated and proved in the Explorations and Activities for this section. See Exercise (10).

Theorem 6.21

Let A, B, and C be nonempty sets and assume that $f : A \to B$ and $g : B \to C$.

1. If $g \circ f : A \to C$ is an injection, then $f : A \to B$ is an injection.
2. If $g \circ f : A \to C$ is a surjection, then $f : A \to B$ is a surjection.

Exercise 6.4

1. In our definition of the composition of two functions, f and g, we required that the domain of g be equal to the codomain of f. However, it is sometimes possible to form the composite function $g \circ f$ even though dom$(g) \neq$ codom(f). For example, let

$$\begin{aligned} f : \mathbb{R} \to \mathbb{R} \quad & textbedefinedby \quad f(x) = x^2 + 1, \text{ and let} \\ g : \mathbb{R} - \{0\} \to \mathbb{R} \quad & textbedefinedby \quad g(x) = \frac{1}{x}. \end{aligned} \tag{6.4.4}$$

   (a) Is it possible to determine $(g \circ f)(x)$ for all $x \in \mathbb{R}$? Explain.
   (b) In general, let $f : A \to T$ and $g : B \to C$. Find a condition on the domain of g (other than $B = T$) that results in a meaningful definition of the composite function $g \circ f : A \to C$.
2. Let $h : \mathbb{R} \to \mathbb{R}$ be defined $h(x) = 3x + 2$ and $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^3$. Determine formulas for the composite functions $g \circ h$ and $h \circ g$. Is the function $g \circ h$ equal to the function $h \circ g$? Explain. What does this tell you about the operation of composition of functions?
3. Following are formulas for certain real functions. Write each of these real functions as the composition of two functions. That is, decompose each of the functions.

   (a) $F(x) = cos(e^x)$
   (b) $G(x) = e^{cos(x)}$

(c) $H(x) = \dfrac{1}{sinx}$
(d) $K(x) = cos(e^{-x^2})$

4. The identity function on a set S, denoted by I_S, is defined as follows: $I_S : S \to S$ by $I_s(x) = x$ for each $x \in S$. Let $f : A \to B$.

   (a) For each $x \in A$, determine $(f \circ I_A)(x)$ and use this to prove that $f \circ I_A = f$.
   (b) Prove that $I_B \circ f = f$.
5. (a) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$, let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = sinx$, and let $h : \mathbb{R} \to \mathbb{R}$ be defined by $h(x) = \sqrt[3]{x}$.

   Determine formulas for $[(h \circ g) \circ f](x)$ and $[h \circ (g \circ f)](x)$.

   Does this prove that $(h \circ g) \circ f = h \circ (g \circ f)$ for these particular functions? Explain.

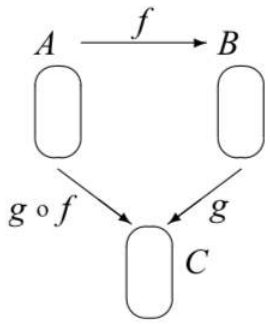
   (b) Now let A, B, and C be sets and let $f : A \to B$, $g : B \to C$, and $h : C \to D$. Prove that $(h \circ g) \circ f = h \circ (g \circ f)$. That is, prove that function composition is an associative operation.
6. Prove Part (1) of Theorem 6.20.
   Let A, B, and C be nonempty sets and let $f : A \to B$ and $g : B \to C$. If f and g are both injections, then $g \circ f$ is an injection.
7. For each of the following, give an example of functions $f : A \to B$ and $g : B \to C$ that satisfy the stated conditions, or explain why no such example exists.

   (a) The function f is a surjection, but the function $g \circ f$ is not a surjection.
   (b) The function f is an injection, but the function $g \circ f$ is not an injection.
   (c) The function g is a surjection, but the function $g \circ f$ is not a surjection.
   (d) The function g is an injection, but the function $g \circ f$ is not an injection.
   (e) The function f is not a surjection, but the function $g \circ f$ is a surjection.
   (f) The function f is not an injection, but the function $g \circ f$ is an injection.
   (g) The function f is not an injection, but the function $g \circ f$ is an injection.
   (h) The function g is not an injection, but the function $g \circ f$ is an injection.
8. Let A be a nonempty set and let $f : A \to A$. For each $n \in \mathbb{N}$, define a funciton $f^n : A \to A$ recursively as follows: $f^1 = f$ and for each $n \in \mathbb{N}$, $f^{n+1} = f \circ f^n$. For example, $f^2 = f \circ f^1 = f \circ f$ and $f^3 = f \circ f^2 = f \circ (f \circ f)$.

   (a) Let $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x + 1$ for each $x \in \mathbb{R}$. For each $n \in \mathbb{N}$ and for each $x \in \mathbb{R}$, determine a formula for $f^n(x)$ and use induction to prove that your formula is correct.
   (b) Let $a, b \in \mathbb{R}$ and let $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = ax + b$ for each $x \in \mathbb{R}$. For each $n \in \mathbb{N}$ and for each $x \in \mathbb{R}$, determine a formula for $f^n(x)$ and use induction to prove that your formula is correct.
   (c) Now let A be a nonempty set and let $f : A \to A$. Use induction to prove that for each $n \in \mathbb{N}$, $f^{n+1} = f^n \circ f$. (**Note:** You will need to use the result in Exercise (5).)

Explorations and Activities

9. **Exploring Composite Functions**. Let A, B, and C be nonempty sets and let $f : A \to B$ and $g : B \to C$. For this activity, it may be useful to draw your arrow diagrams in a triangular arrangement as follows:



It might be helpful to consider examples where the sets are small. Try constructing examples where the set A has 2 elements, the set B has 3 elements, and the set C has 2 elements.

(a) Is it possible to construct an example where $g \circ f$ is an injection, f is an injection, but g is not an injection? Either construct such an example or explain why it is not possible.
(b) Is it possible to construct an example where $g \circ f$ is an injection, g is an injection, but f is not an injection? Either construct such an example or explain why it is not possible.
(c) Is it possible to construct an example where $g \circ f$ is a surjection, f is a surjection, but g is not a surjection? Either construct such an example or explain why it is not possible.
(d) Is it possible to construct an example where $g \circ f$ is a surjection, g is a surjection, but f is not a surjection? Either construct such an example or explain why it is not possible.

10. The Proof of Theorem 6.21. Use the ideas from Exercise (9) to prove Theorem 6.21. Let A, B and C be nonempty sets and let $f : A \to B$ and $g : B \to C$.

(a) If $g \circ f : A \to C$ is an injection, then $f : A \to B$ is an injection.
(b) If $g \circ f : A \to C$ is a surjection, then $g : B \to C$ is a surjection.

Hint: For part (a), start by asking, "What do we have to do to prove that f is an injection? " Start with a similar question for part (b).

Answer

Add texts here. Do not delete this text first.

6.5: Inverse Functions

For this section, we will use the concept of Cartesian product of two sets A and B, denoted by $A \times B$, which is the set of all ordered pairs (x, y) where $x \in A$ and $y \in B$. That is,

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}.$$

See Preview Activity 6.5.2 in Section 5.4 for a more thorough discussion of this concept.

? PREVIEW ACTIVITY 6.5.1: Functions and Sets of Ordered Pairs

When we graph a real function, we plot ordered pairs in the Cartesian plane where the first coordinate is the input of the function and the second coordinate is the output of the function. For example, if $g : \mathbb{R} \to \mathbb{R}$, then every point on the graph of g is an ordered pair (x, y) of real numbers where $y = g(x)$. This shows how we can generate ordered pairs from a function. It happens that we can do this with any function. For example, let

$$A = \{1, 2, 3\} \text{ and } B = \{a, b\}.$$

Define the function $F : A \to B$ by

$$F(1) = a,\ F(2) = b, \text{ and } F(3) = b.$$

We can convert each of these to an ordered pair in $A \times B$ by using the input as the first coordinate and the output as the second coordinate. For example, $F(1) = a$ is converted to $(1, a)$, $F(2) = b$ is converted to $(2, b)$, and $F(3) = b$ is converted to $(3, b)$. So we can think of this function as a set of ordered pairs, which is a subset of $A \times B$, and write

$$F = \{(1, a), (2, b), (3, b)\}.$$

Note: Since F is the name of the function, it is customary to use F as the name for the set of ordered pairs.

1. Let $A = \{1, 2, 3\}$ and let $C = \{a, b, c, d\}$. Define the function $g : A \to C$ by $g(1) = a$, $g(2) = b$, and $g(3) = d$. Write the function g as a set of ordered pairs in $A \times C$.

For another example, if we have a real function, such as: $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2 - 2$, then we can think of g as the following infinite subset of $\mathbb{R} \times \mathbb{R}$:

$$g = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2 - 2\}.$$

We can also write this sometimes write this as $g = \{(x, x^2 - 2) \mid x \in \mathbb{R}\}$.

2. Let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(m) = 3m + 5$, for all $m \in \mathbb{Z}$. Use set builder notation to write the function f as a set of ordered pairs, and then use the roster method to write the function f as a set of ordered pairs.

So any function $f : A \to B$ can be thought of as a set of ordered pairs that is a subset of $A \times B$. This subset is

$$f = \{(a, f(a)) \mid a \in A\} \text{ or } f = \{(a, b) \in A \times B \mid b = f(a)\}.$$

On the other hand, if we started with $A = \{1, 2, 3\}$, $B = \{a, b\}$, and

$$G = \{(1, a), (2, a), (3, b)\} \subseteq A \times B,$$

then we could think of G as a function from A to B with $G(1) = a$, $G(2) = a$, and $G(3) = b$. The idea is to use the first coordinate of each ordered pair as the input, and the second coordinate as the output. However, not every subset of $A \times B$ can be used to define a function from A to B. This is explored in the following questions.

3. Let $f = \{(1, a), (2, a), (3, a), (1, b)\}$. Could this set of ordered pairs be used to define a function from A to B? Explain.
4. Let $g = \{(1, a), (2, a), (3, a)\}$. Could this set of ordered pairs be used to define a function from A to B? Explain.
5. Let $h = \{(1, a), (2, b)\}$. Could this set of ordered pairs be used to define a function from A to B? Explain.

? PREVIEW ACTIVITY 6.5.1: A Composition of Two Specific Functions

Let $A = \{a, b, c, d\}$ and let $B = \{p, q, r, s\}$.

1. Construct an example of a function $f : A \to B$ that is a bijection. Draw an arrow diagram for this function.
2. On your arrow diagram, draw an arrow from each element of B back to its corresponding element in A. Explain why this defines a function from B to A.
3. If the name of the function in Part (2) is g, so that $g : B \to A$, what are $g(p)$, $g(q)$, $g(r)$, and $g(s)$?

4. Construct a table of values for each of the functions $g \circ f : A \to A$ and $f \circ g : B \to B$. What do you observe about these tables of values?

The Ordered Pair Representation of a Function

In Preview Activity 6.5.1, we observed that if we have a function $f : A \to B$, we can generate a set of ordered pairs f that is a subset of $A \times B$ as follows:

$$f = \{(a, f(a) \mid a \in A\} \text{ or } f = \{(a, b) \in A \times B \mid b = f(a)\}.$$

However, we also learned that some sets of ordered pairs cannot be used to define a function. We now wish to explore under what conditions a set of ordered pairs can be used to define a function. Starting with a function $f : A \to B$, since dom(f) = A, we know that

$$\text{For every } a \in A, \text{ there exists a } b \in B \text{ such that } (a, b) \in f. \tag{6.5.1}$$

Specifically, we use $b = f(a)$. This says that every element of A can be used as an input. In addition, to be a function, each input can produce only one output. In terms of ordered pairs, this means that there will never be two ordered pairs (a, b) and (a, c) in the function f where $a \in A$, $b, c \in B$, and $b \neq c$. We can formulate this as a conditional statement as follows:

$$\begin{gathered}\text{For every } a \in A \text{ and every } b, c \in B, \\ \text{if } (a, b) \in f \text{ and } (a, c) \in f, \text{ then } b = c.\end{gathered} \tag{6.5.2}$$

This also means that if we start with a subset f of $A \times B$ that satisfies conditions in Equation 6.5.1 and 6.5.2, then we can consider f to be a function from A to B by using $b = f(a)$ whenever (a, b) is in f. This proves the following theorem.

Theorem 6.22

Let A and B be nonempty sets and let f be a subset of $A \times B$ that satisfies the following two properties:

- For every $a \in A$, there exists $b \in B$ such that $(a, b) \in f$; and
- For every $a \in A$ and every $b, c \in B$, if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

If we use $f(a) = b$ whenever $(a, b) \in f$, then f is a function from A to B.

A Note about Theorem 6.22. The first condition in Theorem 6.22 means that every element of A is an input, and the second condition ensures that every input has exactly one output. Many texts will use Theorem 6.22 as the definition of a function. Many mathematicians believe that this ordered pair representation of a function is the most rigorous definition of a function. It allows us to use set theory to work with and compare functions. For example, equality of functions becomes a question of equality of sets. Therefore, many textbooks will use the ordered pair representation of a function as the definition of a function.

? Progress Check 6.23 (Sets of Ordered Pairs that Are Not Functions)

Let $A = \{1, 2, 3\}$ and let $B = \{a, b\}$. Explain why each of the following subsets of $A \times B$ cannot be used to define a function from A to B.

1. $F = \{(1, a), (2, a)\}$,
2. $G = \{(1, a), (2, b), (3, c), (2, c)\}$.

Answer

Add texts here. Do not delete this text first.

The Inverse of a Function

In previous mathematics courses, we learned that the exponential function (with base e) and the natural logarithm functions are inverses of each other. This was often expressed as follows:

$$\text{For each } x \in R \text{ with } x > 0 \text{ and for each } y \in \mathbb{R}, \ y = \ln x \text{ if and only if } x = e^y.$$

Notice that this means that x is the input and y is the output for the natural logarithm function if and only if y is the input and x is the output for the exponential function. In essence, the inverse function (in this case, the exponential function) reverses the action of the original function (in this case, the natural logarithm function). In terms of ordered pairs (input-output pairs), this means that if (x, y) is

an ordered pair for a function, then (y, x) is an ordered pair for its inverse. This idea of reversing the roles of the first and second coordinates is the basis for our definition of the inverse of a function.

Definition: Inverse of a Function

Let $f : A \to B$ be a function. The inverse of f, denoted by f^{-1}, is the set of ordered pairs $\{(b, a) \in B \times A \mid f(a) = b\}$. That is,

$$f^{-1} = \{(b, a) \in B \times A \mid f(a) = b\} \ .$$

If we use the ordered pair representation for f, we could also write

$$f^{-1} = \{(b, a) \in B \times A \mid (a, b) \in f\} \ .$$

Notice that this definition does not state that f^{-1} is a function. It is simply a subset of $B \times A$. After we study the material in Chapter 7, we will say that this means that f^{-1} is a **relation** from B to A. This fact, however, is not important to us now. We are mainly interested in the following question:

Under what conditions will the inverse of the function $f : A \to B$ be a function from B to A?

Progress Check 6.24: Exploring the Inverse of a Function

Let $A = \{a, b, c\}$, $B = \{a, b, c, d\}$, and $C = \{p, q, r\}$. Define

$f : A \to C$ by	$g : A \to C$ by	$h : B \to C$ by
$f(a) = r$	$g(a) = p$	$h(a) = p$
$f(b) = p$	$g(b) = q$	$h(b) = q$
$f(c) = q$	$g(c) = p$	$h(c) = r$
		$h(d) = q$

1. Draw an arrow diagram for each function.
2. Determine the inverse of each function as a set of ordered pairs.
3. (a) Is f^{-1} a function from C to A? Explain.
   (b) Is g^{-1} a function from C to A? Explain.
   (c) Is h^{-1} a function from C to B? Explain.
4. Draw an arrow diagram for each inverse from Part (3) that is a function. Use your existing arrow diagram from Part (1) to draw this arrow diagram.
5. Make a conjecture about what conditions on a function $F : S \to T$ will ensure that its inverse is a function from T to S.

Answer

Add texts here. Do not delete this text first.

We will now consider a general argument suggested by the explorations in Progress Check 6.24. By definition, if $f : A \to B$ is a function, then f^{-1} is a subset of $B \times A$. However, f^{-1} may or may not be a function from B to A. For example, suppose that $s, t \in A$ with $s \neq t$ and $f(s) = f(t)$. This is represented in Figure 6.9.

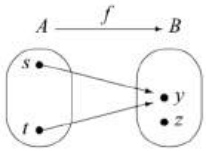


Figure 6.9: The Inverse Is Not a Function

In this case, if we try to reverse the arrows, we will not get a function from B to A. This is because $(y, s) \in f^{-1}$ and $(y, t) \in f^{-1}$ with $s \neq t$. Consequently, f^{-1} is not a function. This suggests that when f is not an injection, then f^{-1} is not a function.

Also, if f is not a surjection, then there exists a $z \in B$ such that $f(a) \neq z$ for all $a \in A$, as in the diagram in Figure 6.9. In other words, there is no ordered pair in f with z as the second coordinate. This means that there would be no ordered pair in f^{-1} with z as a first coordinate. Consequently, f^{-1} cannot be a function from B to A.

This motivates the statement in Theorem 6.25. In the proof of this theorem, we will frequently change back and forth from the input-output representation of a function and the ordered pair representation of a function. The idea is that if $G : S \to T$ is a function, then for $s \in S$ and $t \in T$,

$$G(s) = t \text{ if and only if } (s, t) \in G.$$

When we use the ordered pair representation of a function, we will also use the ordered pair representation of its inverse. In this case, we know that

$$(s, t) \in G \text{ if and only if } (t, s) \in G^{-1}.$$

Theorem 6.25.

Let A and B be nonempty sets and let $f : A \to B$. The inverse of f is a function from B to A if and only if f is a bijection.

Proof

Let A and B be nonempty sets and let $f : A \to B$. We will first assume that f is a bijection and prove that f^{-1} is a function from B to A. To do this, we will show that f^{-1} satisfies the two conditions of Theorem 6.22.

We first choose $b \in B$. Since the function f is a surjection, there exists an $a \in A$ such that $f(a) = b$. This implies that $(a, b) \in f$ and hence that $(b, a) \in f^{-1}$. Thus, each element of B is the first coordinate of an ordered pair in f^{-1}, and hence f^{-1} satisfies the first condition of Theorem 6.22.

To prove that f^{-1} satisfies the second condition of Theorem 6.22, we must show that each element of B is the first coordinate of exactly one ordered pair in f^{-1}. So let $b \in B$, $a_1, a_2 \in A$ and assume that

$$(b, a_1) \in f^{-1} \text{ and } (b, a_2) \in f^{-1}.$$

This means that \((a_1, b) \in f) and \((a_2, b) \in f). We can then conclude that

$$f(a_1) = b \text{ and } f(a_2) = b.$$

But this means that $f(a_1) = f(a_2)$. Since f is a bijection, it is an injection, and we can conclude that $a_1 = a_2$. This proves that b is the first element of only one ordered pair in f^{-1}. Consequently, we have proved that f^{-1} satisfies both conditions of Theorem 6.22 and hence that f^{-1} is a function from B to A.

We now assume that f^{-1} is a function B to A and prove that f is a bijection. First, to prove that f is an injection, we assume that $a_1, a_2 \in A$ and that $f(a_1) = f(a_2)$. We wish to show that $a_1 = a_2$. If we let $b = f(a_1) = f(a_2)$, we can conclude that

\((a_1, b) \in f) and \((a_2, b) \in f).

But this means that

$$(b, a_1) \in f^{-1} \text{ and } (b, a_2) \in f^{-1}.$$

Since we have assumed that f^{-1} is a function, we can conclude that $a_1 = a_2$. Hence, f is an injection.

Now to prove that f is a surjection, we choose $b \in B$ and will show that there exists an $a \in A$ such that $f(a) = b$. Since f^{-1} is a function, b must be the first coordinate of some ordered pair in f^{-1}. Consequently, there exists an $a \in A$ such that

$$(b, a) \in . f^{-1}.$$

Now this implies that $(a, b) \in f$ and hence that $f(a) = b$. This proves that f is a surjection. Since we have also proved that f is an injection, we conclude that f is a bijection.

Inverse Function Notation

In the situation where $f : A \to B$ is a bijection and f^{-1} is a function from B to A, we can write $f^{-1} : B \to A$. In this case, we frequently say that f is an **invertible function**, and we usually do not use the ordered pair representation for either f or f^{-1}. Instead of writing $(a, b) \in f$, we write $f(a) = b$, and instead of writing $(b, a) \in . f^{-1}$, we write $f^{-1}(b) = a$. Using the fact that $(a, b) \in f$ if and only if $(b, a) \in . f^{-1}$, we can now write $f(a) = b$ if and only if $f^{-1}(b) = a$. We summarize this in Theorem 6.26.

Theorem 6.26

Let A and B be nonempty sets and let $f : A \to B$ to be a bijection. Then $f^{-1} : B \to A$ is a function, and for every $a \in A$ and $b \in B$.

$$f(a) = b \text{ if and only if } f^{-1}(b) = a.$$

Example 6.27: Inverse Function Notation

For an example of the use of the notation in Theorem 6.26, let $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$. Define

$$f : \mathbb{R} \to \mathbb{R} \text{ by } f(x) = x^3; \text{ and } g : \mathbb{R} \to \mathbb{R}^+ \text{ by } g(x) = e^x.$$

Notice that $\mathbb{R}^+$ is the codomain of g. We can then say that both f and g are bijections. Consequently, the inverses of these functions are also functions. In fact,

$$f^{-1} : \mathbb{R} \to \mathbb{R} \text{ by } f^{-1}(y) = \sqrt[3]{y}; \text{ and } g^{-1} : \mathbb{R}^+ \to \mathbb{R} \text{ by } g^{-1}(y) = \text{In} y.$$

For each function (and its inverse), we can write the result of Theorem 6.26 as follows:

Theorem 6.26	Translates to:
For $x, y \in \mathbb{R}$, $f(x) = y$ if and only if $f^{-1}(y) = x$.	For $x, y \in \mathbb{R}$, $x^3 = y$ if and only if $\sqrt[3]{y} = x$.
For $x \in \mathbb{R}$, $y \in \mathbb{R}^+$, $g(x) = y$ if and only if $g^{-1}(y) = x$.	For $x \in \mathbb{R}$, $y \in \mathbb{R}^+$, $e^x = y$ if and only if $\ln y = x$.

Theorems about Inverse Functions

The next two results in this section are two important theorems about inverse functions. The first is actually a corollary of Theorem 6.26.

Corollary 6.28.

Let A and B be nonempty sets and let $f : A \to B$ be a bijection. Then

1. For every x in A, $(f^{-1} \circ f)(x) = x$).
2. For every y in B, $(f \circ f^{-1})(y) = y$).

Proof

Let A and B be nonempty sets and assume that $f : A \to B$ is a bijection. So let $x \in A$ and let $f(x) = y$. By Theorem 6.26, we can conclude that $f^{-1}(y) = x$. Therefore,

$$\begin{array} {rcl} (f^{-1} \circ f)(x) &= & f^{-1}(f(x)) \\ & = & f^{-1}(y) \\ & = & x. \end{array}$$

Hence, for each $x \in A$, $(f^{-1} \circ f)(x) = x$).

The proof that for each y in B, $(f \circ f^{-1})(y) = y$) is Exercise (4).

Example 6.27 (continued)

For the cubing function and the cube root function, we have seen that

For $x, y \in \mathbb{R}$, $x^3 = y$ if and only if $\sqrt[3]{y} = x$.

Notice that

- If we substitute $x^3 = y$ into the equation $\sqrt[3]{y} = x$, we obtain $\sqrt[3]{x^3} = x$.
- If we substitute $\sqrt[3]{y} = x$ into the equation $x^3 = y$, we obtain $(\sqrt[3]{y})^3 = y$.

This is an illustration of Corollary 6.28. We can see this by using $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ and $f^{-1} : \mathbb{R} \to \mathbb{R}$ defined by $f^{-1}(y) = \sqrt[3]{y}$. Then $f^{-1} \circ f : \mathbb{R} \to \mathbb{R}$ and $f^{-1} \circ f = I_{\mathbb{R}}$,

\beign{array} {rcl} [(f^{-1} \circ f)(x)} &= & {x} \\ {f^{-1}(f(x))} &= & {x} \\ {f^{-1}(x^3)} &= & {x} \\ {\sqrt[3]{x^3}} &= & {x.} \end{array}

Similarly, the equation $(\sqrt[3]{y})^3 = y$ for each $y \in \mathbb{R}$ can be obtained from the fact that for each $y \in \mathbb{R}$, $(f \circ f^{-1})(y) = y$).

We will now consider the case where $f : A \to B$ and $g : B \to C$ are both bijections. In this case, $f^{-1} : B \to A$ and $g^{-1} : C \to B$. Figure 6.10 can be used to illustrate this situation.

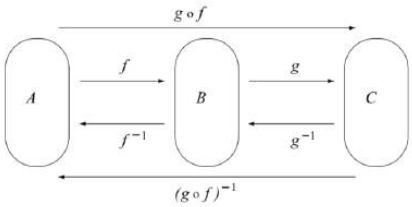


Figure 6.10: Composition of Two Bijections

By Theorem 6.20, $g \circ f : A \to C$ is also a bijection. Hence, by Theorem 6.25, $(g \circ f)^{-1}$ is a function and, in fact, $(g \circ f)^{-1} : C \to A$. Notice that we can also form the composition of g^{-1} followed by f^{-1} to get $f^{-1} \circ g^{-1} : C \to A$. Figure 6.10 helps illustrate the result of the next theorem.

Theorem 6.29.

Let $f : A \to B$ and $g : B \to C$ be bijections. Then $g \circ f$ is a bijection and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof

Let $f : A \to B$ and $g : B \to C$ be bijections. Then $f^{-1} : B \to A$ and $g^{-1} : C \to B$. Hence, $f^{-1} \circ g^{-1} : C \to A$. Also, by Theorem 6.20, $g \circ f : A \to C$ is a bijection, and hence $(g \circ f)^{-1} : C \to A$. We will now prove that for each $z \in C$, $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$.

Let $z \in C$. Since the function g is a surjection, there exists a $y \in B$ such that

$$g(y) = z. \tag{6.5.3}$$

Also, since f is a surjection, there exists an $x \in A$ such that

$$f(x) = y. \tag{6.5.4}$$

Now these two equations can be written in terms of the respective inverse functions as

g^{-1}(z) = y\text[; and}

$$f^{-1}(y) = x. \tag{6.5.5}$$

Using equations (6.5.5) and (6.5.6), we see that

$$\begin{aligned} f^{-1} \circ g^{-1}(z) &= f^{-1}(g^{-1}(z)) \\ &= f^{-1}(y) \\ &= x. \end{aligned} \tag{6.5.6}$$

Using equations (6.5.3) and (6.5.4) again, we see that $(g \circ f)(x) = z$. However, in terms of the inverse function, this means that

$$(g \circ f)^{-1}(z) = x. \tag{6.5.7}$$

Comparing equations (6.5.7) and (6.5.8), we have shown that for all $z \in C$, $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$. This proves that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Exercise 6.5

1. Let $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$.
   (a) Construct an example of a function $f : A \to B$ that is not a bijection. Write the inverse of this function as a set of ordered pairs. Is the inverse of f a function? Explain. If so, draw an arrow diagram for f and f^{-1}.
   (b) Construct an example of a function $g : A \to B$ that is a bijection. Write the inverse of this function as a set of ordered pairs. Is the inverse of g a function? Explain. If so, draw an arrow diagram for g and g^{-1}.
2. Let $S = \{a, b, c, d\}$. Define $f : S \to S$ by defining f to be the following set of ordered pairs.

$$f = \{(a, c), (b, b), (c, d), (d, a)\} \tag{6.5.8}$$

   (a) Draw an arrow diagram to represent the function f. Is the function fa bijection?
   (b) Write the inverse of f as a set of ordered pairs. Is f^{-1} a function? Explain.
   (c) Draw an arrow diagram for f^{-1} using the arrow diagram from Exercise (2a).
   (d) Compute $(f^{-1} \circ f)(x)$ and $(f \circ f^{-1}(x)$ for each x in S. What theorem does this illustrate?
3. Inverse functions can be used to help solve certain equations. The idea is to use an inverse function to undo the function.
   (a) Since the cube root function and the cubing function are inverses of each other, we can often use the cube root function to help solve an equation involving a cube. For example, the main step in solving the equation

$$(2t - 1)^3 = 20 \tag{6.5.9}$$

   is to take the cube root of each side of the equation. This gives
   \[\begin{array} {rcl} {\sqrt[3]{(2t - 1)^3} &= & {\sqrt[3]{20}} \\ {2t - 1} &= &{\sqrt[3]{20}.} \end{array}\]
   Explain how this step in solving the equation is a use of Corollary 6.28.

   (b) A main step in solving the equation \(e^{2t - 1} = 20} is to take the natural logarithm of both sides of this equation. Explain how this step is a use of Corollary 6.28, and then solve the resulting equation to obtain a solution for t in terms of the natural logarithm function.
   (c) How are the methods of solving the equations in Exercise (3a) and Exercise (3b) similar?
4. Prove Part (2) of Corollary 6.28. Let A and B be nonempty sets and let $f : A \to B$ be a bijection. Then for every y in B, $(f \circ f^{-1}(y) = y$.
5. In Progress Check 6.6 on page 298, we defined the identity function on a set. The **identity function on the set T**, denoted by I_T, is the function $I_T : T \to T$ defined by $I_T(t) = t$ for every t in T. Explain how Corollary 6.28 can be stated using the concept of equality of functions and the identity functions on the sets A and B.
6. Let $f : A \to B$ and $g : B \to A$. Let I_A and I_B be the identity functions on the sets A and B, respectively. Prove each of the following:
   (a) If $g \circ f = I_A$, then f is an injection.
   (b) If $g \circ g = I_B$, then f is a surjection.
   (c) If $g \circ f = I_A$ and $g \circ g = I_B$, then f and g are bijections and $g = f^{-1}$.
7. (a) Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = e^{-x^2}$. Is the inverse of f a function? Justify your conclusion.
   (b) Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$. Define $g : \mathbb{R}^* \to (0, 1]$ by $g(x) = e^{-x^2}$. Is the inverse of g a function? Justify your conclusion.
8. (a) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Explain why the inverse of f is not a function.
   (b) Let $\mathbb{R}^* = \{t \in \mathbb{R} \mid t \geq 0\}$. Define $g : \mathbb{R}^* \to \mathbb{R}^*$ by $g(x) = x^2$. Explain why this squaring function (with a restricted domain and codomain) is a bijection.
   (c) Explain how to define the square root function as the inverse of the function in Exercise (8b).
   (d) True or false: $(\sqrt{x})^2 = x$ for all $x \in \mathbb{R}$ such that $x \geq 0$.
   (e) True or false: $\sqrt{x^2} = x$ for all $x \in \mathbb{R}$.
9. Prove the following:
   If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is also a bijection.
10. For each natural number k, let A_k be a set, and for each natural number n, let $f_n : A_n \to A_{n+1}$.
    For example, $f_1 = A_1 \to A_2$, $f_1 = A_1 \to A_2$, $f_2 = A_2 \to A_3$, $f_3 = A_3 \to A_4$, and so on.
    Use mathematical induction to prove that for each natural number n with $n \geq 2$, if f_1, f_2, ..., f_n are all bijections, then $f_n \circ f_{n-1} \circ \cdots \circ f_2 \circ f_1$ is a bijection and

\[(f_n \circ f_{n - 1} \circ \cdot\cdot\cdot \circ f_2 \circ f_1)^{-1} = f_{1}^{-1} \cdot f_{2}^{-1} \cdot \cdot\cdot\cdot \circ f_{n - 1}^{-1} \circ f_{n}^{-1}

Note: This is an extension of Theorem 6.29. In fact, Theorem 6.29 is the basis step of this proof for $n = 2$.

11. $a) Define \(f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 - 4$ for all $x \in \mathbb{R}$. Explain why the inverse of the function f is not a function.
(b) Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$ and let $T = \{y \in \mathbb{R} \mid y \geq -4\}$. Define $F : \mathbb{R}^* \to T$ by $F(x) = x^2 - 4$ for all $x \in \mathbb{R}^*$. Explain why the inverse of the function F is a function and find a formula for $F^{-1}(y)$, where $y \in T$.
12. Let $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
(a) Define $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $f(x) = x^2 + 4 \pmod 5$ for all $x \in \mathbb{Z}_5$. Write the inverse of f as a set of ordered pairs and explain why f^{-1} is not a function.
(b) Define $g : \mathbb{Z}_5 \to \mathbb{Z}_5$ by $g(x) = x^3 + 4 \pmod 5$ for all $x \in \mathbb{Z}_5$. Write the inverse of g as a set of ordered pairs and explain why g^{-1} is not a function.
(c) Is it possible to write a formula for $g^{-1}(y)$, where $y \in \mathbb{Z}_5$? The answer to this question depends on whether or not is possible to define a cube root of elements of $\mathbb{Z}_5$. Recall that for a real number x, we define the cube root of x to the real number y such that $y^3 = x$. That is,

$$y = \sqrt[3]{x} \text{ if and only if } y^3 = x. \tag{6.5.10}$$

Using this idea, is it possible to define the cube root of each number in $\mathbb{Z}_5$? If so, what is $\sqrt[3]{0}$, $\sqrt[3]{1}$, $\sqrt[3]{2}$, $\sqrt[3]{3}$, and $\sqrt[3]{4}$.
(d) Now answer th equestion posed at the beginning of Part (c). If possible, determine a formula for $g^{-1}(y)$ where $g^{-1} : \mathbb{Z}_5 \to \mathbb{Z}_5$.

Explorations and Activities

13. **Constructing an Inverse Function.** If $f : A \to B$ is a bijection, then we know that its inverse is a function. If we are given a formula for the function f, it may be desirable to determine a formula for the function f^{-1}. This can sometimes be done, while at other times it is very difficult or even impossible.
Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x^3 - 7$. A graph of this function would suggest that this function is a bijection.

(a) Prove that the function f is an injection and a surjection.

Let $y \in \mathbb{R}$. One way to prove that f is a surjection is to set $y = f(x)$ and solve for x. If this can be done, then we would know that there exists an $x \in \mathbb{R}$ such that $f(x) = y$. For the function f, we are using x for the input and y for the output. By solving for x in terms of y, we are attempting to write a formula where y is the input and x is the output. This formula represents the inverse function.

(b) Solve the equation $y = 2x^3 - 7$ for x. Use this to write a formula for $f^{-1}(y)$, where $f^{-1} : \mathbb{R} \to \mathbb{R}$.
(c) Use the result of Part (13b) to verify that for each $x \in \mathbb{R}$, $f^{-1}(f(x)) = x$ and for each $y \in \mathbb{R}$, $f(f^{-1}(y)) = y$.

Now let $\mathbb{R}^+ = \{y \in \mathbb{R} \mid y > 0\}$. Define $g : \mathbb{R} \to \mathbb{R}^+$ by $g(x) = e^{2x-1}$.

(d) Set $y = e^{2x-1}$ and solve for x in terms of y.
(e) Use your work in Exercise (13d) to define a function $h : \mathbb{R}^+ \to \mathbb{R}$.
(f) For each $x \in \mathbb{R}$, determine $(h \circ g)(x)$ and for each $y \in \mathbb{R}^+$, determine $(g \circ h)(y)$.
(g) Use Exercise (6) to explain why $h = g^{-1}$.

14. **The Inverse Sine Function.** We have seen that in order to obtain an inverse function, it is sometimes necessary to restrict the domain (or the codomain) of a function.

(a) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = sinx$. Explain why the inverse of the function f is not a function. (A graph may be helpful.)

Notice that if we use the ordered pair representation, then the sine function can be represented as

$$f = \{(x, y) \in \mathbb{R} \to \mathbb{R} \mid y = sinx\}. \tag{6.5.11}$$

If we denote the inverse of the sine function by $\sin^{-1}$, then

$$f^{-1} = \{(y, x) \in \mathbb{R} \to \mathbb{R} \mid y = sinx\}. \tag{6.5.12}$$

Part (14a) proves that f^{-1} is not a function. However, in previous mathematics courses, we frequently used the "inverse sine function." This is not really the inverse of the sine function as defined in Part (14a) but, rather, it is the inverse of the sine function **restricted to the domain** $[-\frac{\pi}{2}, \frac{\pi}{2}]$.

(b) Explain why the function $F : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$ defined by $F(x) = sinx$ is a bijection.

The inverse of the function in Part (14b) is itself a function and is called the inverse sine function (or sometimes the arcsine function).

(c) What is the domain of the inverse sine function? What are the range and codomain of the inverse sine function?

Let us now use $F(x) = \sin(x)$ to represent the restricted sine function in Part (14b). Therefore, $F^{-1}(x) = \sin^{-1}(x)$ can be used to represent the inverse sine function. Observe that

$$F : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1] \text{ and } F^{-1} : [-1, 1] \to [-\frac{\pi}{2}, \frac{\pi}{2}]. \tag{6.5.13}$$

(d) Using this notation, explain why
$\sin^{-1} y = x$ if and only if $[y = \sin x$ and $-\frac{\pi}{2} \leq x \leq \frac{\pi}{2}$];
$\sin(\sin^{-1}(y)) = y$ for all $y \in [-1, 1]$; and
$\sin^{-1}(\sin(x)) = x$ for all $x \in [-\frac{\pi}{2}, \frac{\pi}{2}]$.

Answer

Add texts here. Do not delete this text first.

6.6: Functions Acting on Sets

Preview Activity 1 (Functions and Sets)
Let $S = \{a, b, c, d\}$ and $T = \{s, t, u\}$. Define $f : S \to T$ by

$$f(a) = s \;\; f(b) = t \;\; f(c) = t \;\; f(d) = s$$

1. Let $A = \{a, c\}$ and $B = \{a, d\}$. Notice that A and B are subsets of S. Use the roster method to specify the elements of the following two subsets of T:

   (a) $\{f(x) \mid x \in A\}$
   (b) $\{f(x) \mid x \in B\}$
2. Let $C = \{s, t\}$ and $D = \{s, u\}$. Notice that C and D are subsets of T. Use the roster method to specify the elements of the following two subsets of S:

   (a) $\{x \in S \mid f(x) \in C\}$
   (b) $\{x \in S \mid f(x) \in D\}$

   Now let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2$, for each $x \in \mathbb{R}$.
3. Let $A = \{1, 2, 3, -1\}$. Use the roster method to specify the elements of the set $\{g(x) \mid x \in A\}$.
4. Use the roster method to specify the elements of each of the following sets:

   (a) $\{x \in \mathbb{R} \mid g(x) = 1\}$
   (b) $\{x \in \mathbb{R} \mid g(x) = 9\}$
   (c) $\{x \in \mathbb{R} \mid g(x) = 15\}$
   (d) $\{x \in \mathbb{R} \mid g(x) = -1\}$
5. Let $B = \{1, 9, 15, -1\}$. Use the roster method to specify the elements of the set \{\x \in \mathbb{R}\ |\ g(x) \in B\}\).

Preview Activity 2 (Functions and Intervals)
Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2$, for each $x \in \mathbb{R}$.

1. We will first determine where g maps the closed interval [1, 2]. (Recall that $[1, 2] = \{x \in R \mid 1 \leq x \leq 2\}$.) That is, we will describe, in simpler terms, the set $\{g(x) \mid x \in [1, 2]\}$. This is the set of all images of the real numbers in the closed interval [1, 2].

   (a) Draw a graph of the function g using $-3 \leq x \leq 3$.
   (b) On the graph, draw the vertical lines $x = 1$ and $x = 2$ from the x-axis to the graph. Label the points $P(1, f(1))$ and $Q(2, f(2))$ on the graph.
   (c) Now draw horizontal lines from the points P and Q to the y-axis. Use this information from the graph to describe the set $\{g(x) \mid x \in [1, 2]\}$ in simpler terms. Use interval notation or set builder notation.
2. We will now determine all real numbers that g maps into the closed interval [1, 4]. That is, we will describe the set $\{x \in \mathbb{R} \mid g(x) \in [1, 4]\}$ in simpler terms. This is the set of all preimages of the real numbers in the closed interval [1, 4].
   (a) Draw a graph of the function g using $-3 \leq x \leq 3$.
   (b) On the graph, draw the horizontal lines $y = 1$ and $y = 4$ from they-axis to the graph. Label all points where these two lines intersect the graph.
   (c) Now draw vertical lines from the points in Part (2) to the x-axis, and then use the resulting information to describe the set $\{x \in \mathbb{R} \mid g(x) \in [1, 4]\}$ in simpler terms. (You will need to describe this set as a union of two intervals. Use interval notation or set builder notation.)

Functions Acting on Sets

In our study of functions, we have focused on how a function "maps" individual elements of its domain to the codomain. We also studied the preimage of an individual element in its codomain. For example, if $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = x^2$, for each $x \in \mathbb{R}$, then

- $f(2) = 4$. We say that f maps 2 to 4 or that 4 is the image of 2 under the function f.
- Since $f(2) = 4$ implies that $x = 2$ or $x = -2$, we say that the preimages of 4 are 2 and -2 or that the set of preimages of 4 is {-2, 2}.

For a function $f : S \to T$, the next step is to consider subsets of S or T and what corresponds to them in the other set. We did this in the Preview Activities. We will give some definitions and then revisit the examples in the Preview Activities in light of these definitions. We will first consider the situation where A is a subset of S and consider the set of outputs whose inputs are from A. This will be a subset of T.

Definition

Let $f : S \to T$. If $A \subseteq S$, then the **image of A under f** is the set $f(A)$, where

$$f(A) = \{f(x) \mid x \in A\}.$$

If there is no confusion as to which function is being used, we call $f(A)$ **the image of A.**

We now consider the situation in which C is a subset of T and consider the subset of A consisting of all elements of T whose outputs are in C.

Definition

Let $f : S \to T$. If $C \subseteq T$, then the **preimage of C under f** is the set $f^{-1}(C)$, where

$f^{-1}(C) = \{x \in S \mid f(x) \in C\}$.

If there is no confusion as to which function is being used, we call $f^{-1}(C)$ **the preimage of C**. The preimage of the set C under f is also called the **inverse image of C under f**.

Notice that the set $f^{-1}(C)$ is defined whether or not f^{-1} is a function.

Progress Check 6.30 (Preview Activity 6.6.1 Revisited)

Let $S = \{a, b, c, d\}$ and $T = \{s, t, u\}$. Define $f : S \to T$ by

$$f(a) = s \;\; f(b) = t \;\; f(c) = t \;\; f(d) = s.$$

Let $A = \{a, c\}$, $B = \{a, d\}$, $C = \{s, t\}$, and $D = \{s, u\}$.

Use your work in Preview Activity 6.6.1 to determine each of the following sets:

1. $f(A)$
2. $f(B)$
3. $f^{-1}(C)$
4. $f^{-1}(D)$

Answer

Add texts here. Do not delete this text first.

Example 6.31 (Images and Preimages of Sets)

Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = x^2$, for each $x \in \mathbb{R}$. The following results are based on the examples in Preview Activity 6.6.1 and Preview Activity 6.6.2.

- Let $A = \{1, 2, 3, -1\}$. Then $f(A) = \{1, 4, 9\}$.
- Let $B = \{1, 9, 15, -1\}$. Then $f^{-1}(B) = \{-\sqrt{15}, -3, -1, 1, 3, \sqrt{15}\}$.

The graphs from Preview Activity 6.6.2 illustrate the following results:

- If T is the closed interval [1, 2], then the image of the set T is

$$\begin{aligned} f(T) &= \{f(x) \mid x \in [1,2]\} \\ &= [1,4]. \end{aligned} \tag{6.6.1}$$

- If C is the closed interval [1, 4], then the preimage of the set C is

$$f^{-1}(C) = \{x \in \mathbb{R} \mid f(x) \in [1,4]\} = [-2,-1] \cup [1,2]. \tag{6.6.2}$$

Set Operations and Functions Acting on Sets

We will now consider the following situation: Let S and T be sets and let f be a function from S to T. Also, let A and B be subsets of S and let C and D be subsets of T. In the remainder of this section, we will consider the following situations and answer the questions posed in each case.

- The set $A \cap B$ is a subset of S and so $f(A \cap B$ is a subset of T. In addition, $f(A)$ and $f(B)$ are subsets of T. Hence, $f(A) \cap f(B)$ is a subset of T.

  Is there any relationship between $f(A \cap B$ and $f(A) \cap f(B)$?
- The set $A \cup B$ is a subset of S and so $f(A \cup B$ is a subset of T. In addition, $f(A)$ and $f(B)$ are subsets of T. Hence, $f(A) \cup f(B)$ is a subset of T.

  Is there any relationship between $f(A \cup B$ and $f(A) \cup f(B)$?
- The set $C \cap D$ is a subset of T and so $f^{-1}(C \cap D)$ is a subset of S. In addition, $f^{-1}(C)$ and $f^{-1}(D)$ are subsets of S. Hence, $f^{-1}(C) \cap f^{-1}(D)$ is a subset of S.

  Is there any relationship between the sets $f^{-1}(C \cap D)$ and $f^{-1}(C) \cap f^{-1}(D)$?
- The set $C \cup D$ is a subset of T and so $f^{-1}(C \cup D)$ is a subset of S. In addition, $f^{-1}(C)$ and $f^{-1}(D)$ are subsets of S. Hence, $f^{-1}(C) \cup f^{-1}(D)$ is a subset of S.

  Is there any relationship between the sets $f^{-1}(C \cup D)$ and $f^{-1}(C) \cup f^{-1}(D)$?

These and other questions will be explored in the next progress check.

? Progress check 6.32 (set operations and functions acting on sets)

In Section 6.2, we introduced functions involving congruences. For example, if we let

$$\mathbb{Z}_8 = \{0,1,2,3,4,5,6,7\}.$$

then we can define $f : \mathbb{Z}_8 \to \mathbb{Z}_8$ by $f(x) = r$, where $(x^2+2) \equiv r \pmod 8$ and $r \in \mathbb{Z}_8$. Moreover, we shortened this notation to

$$f(x) = (x^2+2) \pmod 8$$

We will use the following subsets of $\mathbb{Z}_8$:

$$A = \{1,2,4\}\ B = \{3,4,6\}\ C = \{1,2,3\}\ D = \{3,4,5\}$$

1. Verify that $f(0) = 2$, $f(1) = 3$, $f(2) = 6$, and $f(3) = 3$. Then determine $f(4)$, $f(5)$, $f(6)$ and $f(7)$.
2. Determine $f(A)$, $F = f(A = B)$, $f^{-1}(C)$, and $f^{-1}(D)$.
3. For each of the following, determine the two subsets of $\mathbb{Z}_8$ and then determine if there is a relationship between the two sets. For example, $A \cap B = \{4\}$ and since $f(4) = 2$, we see that $f(A \cap B) = \{2\}$.

   (a) $f(A \cap B)$ and $f(A) \cap f(B)$
   (b) $f(A \cup B)$ and $f(A) \cup f(B)$
   (c) $f^{-1}(C \cap D)$ and $f^{-1}(C) \cap f^{-1}(D)$
   (d) $f^{-1}(C \cup D)$ and $f^{-1}(C) \cup f^{-1}(D)$
4. Notice that $f(A)$ is a subset of the codomain, $\mathbb{Z}_8$. Consequently, $f^{-1}(f(A))$ is a subset of the domain, $\mathbb{Z}_8$. Is there any relation between A and $f^{-1}f(A))$ in this case?

5. Notice that $f^{-1}(C)$ is a subset of the codomain, $\mathbb{Z}_8$. Consequently, $f(f^{-1}(f(C))$ is a subset of the domain, $\mathbb{Z}_8$. Is there any relation between C and $f(f^{-1}f(C))$ in this case?

Answer

Add texts here. Do not delete this text first.

Example 6.33 (Set Operations and Functions Acting on Sets)

Define $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 2$ for all $x \in \mathbb{R}$. It will be helpful to use the graph shown in Figure 6.11.

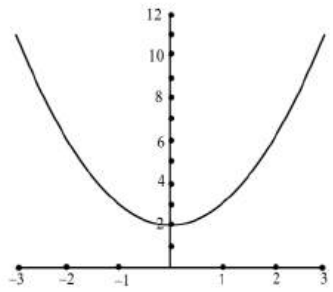


Figure 6.11: Graph for Example 6.33

We will use the following closed intervals:

$$A = [0, 3]\ B = [-2, 1]\ C = [2, 6]\ D = [0, 3].$$

1. Verify that $f(A) = [2, 11]$, $f(B) = [2, 6]$, $f^{-1}(C) = [-2, 2]$, and that $f^{-1}(D) = [-1, 1]$.
2. (a) Explain why $f(A \cap B) = [2, 3]$ and $f(A) \cap f(B) = [2, 6]$. So in this case, $f(A \cap B) \subseteq f(A) \cap f(B)$.
   (b) Explain why $f(A \cup B) = [2, 11]$ and $f(A) \cup f(B) = [2, 11]$. So in this case, $f(A \cup B) \subseteq f(A) \cup f(B)$.
   (c) Explain why $f^{-1}(C \cap D) = [-1, 1]$ and $f^{-1}(C) \cap f^{-1}(D) = [-1, 1]$. So in this case, $f^{-1}(C \cap D) \subseteq f^{-1}(C) \cap f^{-1}(D)$.
   (d) Explain why $f^{-1}(C \cup D) = [-2, 2]$ and $f^{-1}(C) \cap f^{-1}(D) = [-2, 2]$. So in this case, $f^{-1}(C \cup D) \subseteq f^{-1}(C) \cup f^{-1}(D)$.
3. Reacll that $A = [0, 3]$. Notice $f(A) = [2, 11]$ is a subset of the codomain, $\mathbb{R}$. Explain why $f^{-1}(f(A)) = [-3, 3]$. Since $f^{-1}f(A))$ is a subset of the domain, $\mathbb{R}$, we see that in this case, $A \subseteq f^{-1}(f(A))$.
4. Reacll that $C = [2, 6]$. Notice $f^{-1}(C) = [-2, 2]$ is a subset of the codomain, $\mathbb{R}$. Explain why $f(f^{-1}f(C)) = [2, 6]$. Since $f^{-1}f(C))$ is a subset of the domain, $\mathbb{R}$, we see that in this case, $f(f^{-1}(C)) = C$.

The examples in Progress Check 6.32 and Example 6.33 were meant to illustrate general results about how functions act on sets. In particular, we investigated how the action of a function on sets interacts with the set operations of intersection and union. We will now state the theorems that these examples were meant to illustrate. Some of the proofs will be left as exercises.

Theorem 6.34.

Let $f : S \to T$ be a function and let A and B be subsets of S. Then

1. $f(A \cap B$ \subseteq f(A) \cap f(B)\)
2. $f(A \cup B$ = f(A) \cup f(B)\)

Proof

We will prove Part (1). The proof of Part (2) is Exercise (5).

Assume that $f : S \to T$ is a function and let A and B be subsets of S. We will prove that $f(A \cap B$ \subseteq f(A) \cap f(B)\) by proving that for all $y \in T$, if $y \in f(A \cap B)$, then $y \in f(A) \cap f(B)$.

We assume that $y \in f(A \cap B)$. This means that there exists an $x \in A \cap B$ such that $f(x) = y$. Since $x \in A \cap B$, we conclude that $x \in A$ and $x \in B$.

- Since $x \in A$ and $f(x) = y$, we conclude that $y \in f(A)$.
- Since $x \in B$ and $f(x) = y$, we conclude that $y \in f(B)$.

Since $x \in f(A)$ and $y \in f(B)$, $y \in f(A) \cap f(B)$. This proves that if $y \in f(A \cap B)$, then $y \in f(A) \cap f(B)$. Hence $f(A \cap B$ \subseteq f(A) \cap f(B)\).

Theorem 6.35

Let $f : S \to T$ be a function and let C and D be subsets of T. Then

1. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$
2. $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$

Proof

We will prove Part (2). The proof of Part (1) is Exercise (6).

Assume that $f : S \to T$ is a function and that C and D are subsets of T. We will prove that $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$ by proving that each set is a subset of the other.

We start by letting x be an element of $f^{-1}(C \cup D)$. This means that $f(x)$ is an element of $C \cup D$. Hence,

$$f(x) \in C \text{ or } f(x) \in D$$

In the case where $f(x) \in C$, we conclude that $x \in f^{-1}(C)$, and hence that $x \in f^{-1}(C) \cup f^{-1}(D)$. In the case where $f(x) \in D$, we see that $x \in f^{-1}(D)$, and hence that $x \in f^{-1}(C) \cup f^{-1}(D)$. So in both cases, $x \in f^{-1}(C) \cup f^{-1}(D)$, and we have proved that $f^{-1}(C \cup D) \subseteq f^{-1}(C) \cup f^{-1}(D)$

We now let $t \in f^{-1}(C) \cup f^{-1}(D)$. This means that

$$t \in f^{-1}(C) \text{ or } t \in f^{-1}(D)$$

- In the case where $t \in f^{-1}(C)$, we conclude that $f(t) \in C$ and hence that $f(t) \in C \cup D$. This means that $t \in f^{-1}(C \cup D)$.
- Similarly, when $t \in f^{-1}(D)$, it follows that $f(t) \in D$ and hence that $f(t) \in C \cup D$. This means that $t \in f^{-1}(C \cup D)$.

These two cases prove that if $t \in f^{-1}(C) \cup f^{-1}(D)$, then $t \in f^{-1}(C \cup D)$. Therefore, $f^{-1}(C) \cup f^{-1}(D) \subseteq f^{-1}(C \cup D)$.

Since we have now proved that each of the two sets is a subset of the other set, we can conclude that $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

Theorem 6.36.

Let $f : S \to T$ be a function and let A be a subset of S and let C be a subset of T. Then

1. $A \subseteq f^{-1}(f(A))$
2. $f(f^{-1}(C)) \subseteq C$

Proof

We will prove Part (1). The proof of Part (2) is Exercise (7).

To prove Part (1), we will prove that for all $a \in S$, if $a \in A$, then $a \in f^{-1}(f(A))$. So let $a \in A$. Then, by definition, $f(a) \in f(A)$. We know that $f(A) \subseteq T$, and so $f^{-1}(f(A)) \subseteq S$. Notice that

$$f^{-1}(f(A)) = \{x \in S \mid f(x) \in f(A)\}.$$

Since $f(a) \in f(A)$, we use this to conclude that $a \in f^{-1}(f(A)). This proves that if \(a \in A$, then $a \in f^{-1}(f(A))$, and hence that $A \in f^{-1}(f(A))$

Exercise 6.6

1. Let $f : S \to T$. let A and B be subsets of S, and let C and D be subsets of T. For $x \in S$ and $y \in T$, carefully explain what it means to say that

   (a) $y \in f(A \cap B)$
   (b) $y \in f(A \cup B)$
   (c) $y \in f(A) \cap f(B)$
   (d) $y \in f(A) \cup f(B)$
   (e) $x \in f^{-1}(C \cap D)$
   (f) $x \in f^{-1}(C \cup D)$
   (g) $x \in f^{-1}(C) \cap f^{-1}(D)$
   (h) $x \in f^{-1}(C) \cup f^{-1}(D)$
2. Let $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = -2x + 1$. Let

   $A = [2, 5]$ $B = [-1, 3]$ $C = [-2, 3]$ $D = [1, 4]$.

   Find each of the following:

   (a) $f(A)$
   (b) $f^{-1}(f(A))$
   (c) $f^{-1}(C)$
   (d) $f(f^{-1}(C))$
   (e) $f(A \cap B)$
   (f) $f(A) \cap f(B)$
   (g) $f^{-1}(C \cap D)$
   (h) $f^{-1}(C) \cap f^{-1}(D)$
3. Let $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $g(m, n) = 2^m 3^n$, let $A = \{1, 2, 3\}$, and let $C = \{1, 4, 6, 9, 12, 16, 18\}$ Find

   (a) $g(A \times A)$
   (b) $g^{-1}(C)$
   (c) $g^{-1}(g(A \times A))$
   (d) $g(g^{-1}(C))$
4. (a) Let $S = \{1, 2, 3, 4\}$. Define $F : S \to \mathbb{N}$ by $F(x) = x^2$ for each $x \in s$. What is the range of the function F and what is $F(S)$? How do these two sets compare?

   Now let A and B be sets and let $f : A \to B$ be an arbitrary function from A to B.

   (b) Explain why $f(A) = \text{range}(f)$.
   (c) Define a function $g : A \to f(A)$ by $g(x) = f(x)$ for all x in A. Prove that the function g is a surjection.
5. Prove Part (2) of Theorem 6.34.
   Let $f : S \to T$ be a function and let A and B be subsets of S. Then $f(A \cup B) = f(A) \cup f(B)$.
6. Prove Part (1) of Theorem 6.35.
   Let $f : S \to T$ be a function and let C and D be subsets of T. Then $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
7. Prove Part (2) of Theorem 6.36.
   Let $f : S \to T$ be a function and let $C \subseteq T$. Then $f(f^{-1}(C)) \subseteq C$.
8. Let $f : S \to T$ and let A and B be subsets of S. Prove or disprove each of the following:

   (a) If $A \subseteq B$, then $f(A) \subseteq f(B)$.
   (b) If $f(A) \subseteq f(B)$, then $A \subseteq B$.
9. Let $f : S \to T$ and let C and D be subsets of T. Prove or disprove each of the following:

   (a) If $C \subseteq D$, then $f^{-1}(C) \subseteq f^{-1}(D)$.

(b) If $f^{-1}(C) \subseteq f^{-1}(D)$, then $C \subseteq D$.

10. Prove or disprove:
    If $f : S \to T$ is a function and A and B are subsets of S, then
    $f(A) \cap f(B) \subseteq f(A \cap B)$.
    Note: Part (1) of Theorem 6.34 states that $f(A \cap B) \subseteq f(A) \cap f(B)$.
11. If $f : S \to T$ is a function, let $A \subseteq S$, and let $C \subseteq T$.
    (a) Part (1) of Theorem 6.36 states that $A \subseteq f^{-1}(f(A))$. Give an example where $f^{-1}(f(A))\backslash \text{notsubseteq} A$.
    (b) Part (2) of Theorem 6.36 states that $f(f^{-1}(C)) \subseteq C$. Give an example where $C\backslash \text{notsubseteq} f(f^{-1}(C))$.
12. Is the following proposition true or false? Justify your conclusion with a proof or a counterexample.
    If $f : S \to T$ is an injection and $A \subseteq S$, then $f^{-1}(f(A)) = A$.
13. Is the following proposition true or false? Justify your conclusion with a proof or a counterexample.
    If $f : S \to T$ is an injection and $C \subseteq T$, then $f^{-1}(f(C)) = C$.
14. Let (f: S \to T\). Prove that $f(A \cap B) = f(A) \cap f(B)$ for all subsets A and B of S if and only if f is an injection.

Answer

Add texts here. Do not delete this text first.

6.S: Functions (Summary)

Important Definitions

- Function, page 284
- Domain of a function, page 285
- Codomain of a function,page285
- Image of x under f, page 285
- preimage of y under f, page 285
- Independent variable, page 285
- Dependent variable, page 285
- Range of a function, page 287
- Image of a function, page 287
- Equal functions, page 298
- Sequence, page 301
- Injection, page 310
- One-to-one function, page 310
- Surjection, page 311
- Onto function, page 311
- Bijection, page 312
- One-to-one and onto, page 312
- Composition of f and g, page 325
- Composite function, page 325
- f followed by g, page 325
- Inverse of a function, page 338
- Image of a set under a function, page 351
- preimage of a set under a function, page 351

Important Theorems and Results about Functions

- Theorem 6.20. Let A, B and C be nonempty sets and let $f : A \to B$ and $g : B \to C$.

  1. If f and g are both injections, then $g \circ f$ is an injection.
  2. If f and g are both surjections, then $g \circ f$ is a surjection.
  3. If f and g are both bijections, then $g \circ f$ is a bijection.
- Theorem 6.21. Let A, B and C be nonempty sets and let $f : A \to B$ and $g : B \to C$.

  1. If $g \circ f : A \to C$ is an injection, then $f : A \to B$ is an injeciton.
  2. If $g \circ f : A \to C$ is a surjection, then $g : B \to C$ is a surjeciton.
- Theorem 6.22. Let A and B be nonempty sets and let f be a subset of $A \times B$ that satisfies the following two properties:

  • For every $a \in A$, there exists $b \in B$ such that $(a, b) \in f$; and
  • For every $a \in A$ and every $b, c \in B$, if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

  If we use $f(a) = b$ whenever $(a, b) \in f$, then f is a function from A to B.
- Theorem 6.25. Let A and B be nonempty sets and let $f : A \to B$. The inverse of f is a function from B to A if and only if f is a bijection.
- Theorem 6.26. Let A and B be nonempty sets and let $f : A \to B$ be a bijection. Then $f^{-1} : B \to A$ is a function, and for every $a \in A$ and $b \in B$,
  $f(a) = b$ if and only if $f^{-1}(b) = a$.
- Corollary 6.28. Let A and B be nonempty sets and let $f : A \to B$ be a bijection. Then

  1. For every x in A, $(f^{-1} \circ f)(x) = x$.
  2. For every y in B, $(f \circ f^{-1}(y) = y$.

- Theorem 6.29. Let $f : A \to B$ and $g : B \to C$ be bijections. Then $g \circ f$ is a bijection and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
- Theorem 6.34. Let $f : S \to T$ be a function and let A and B be subsets of S. Then

  1. $f(A \cap B) \subseteq f(A) \cap f(B)$
  2. $f(A \cup B) = f(A) \cup f(B)$
- Theorem 6.35. Let $f : S \to T$ be a function and let C and D be subsets of T. Then

  1. $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$
  2. $f^{-1}(C \cup D) = f^{-1}(C) \cap f^{-1}(D)$
- Theorem 6.36. Let $f : S \to T$ be a function and let $A \backslash (beasubsetof \backslash (S$ and let C be a subset of T. Then

  1. $A \subseteq f^{-1}(f(A))$
  2. $f(f^{-1}(C) \subseteq C$

CHAPTER OVERVIEW

7: Equivalence Relations

In Section 6.1, we introduced the formal definition of a function from one set to another set. The notion of a function can be thought of as one way of relating the elements of one set with those of another set (or the same set). A function is a special type of *relation* in the sense that each element of the first set, the domain, is "related" to exactly one element of the second set, the codomain. This idea of relating the elements of one set to those of another set using ordered pairs is not restricted to functions. For example, we may say that one integer, a , is related to another integer, b , provided that a is congruent to b modulo 3. Notice that this relation of congruence modulo 3 provides a way of relating one integer to another integer. However, in this case, an integer a is related to more than one other integer.

7.1: Relations

PREVIEW ACTIVITY 7.1.1: The United States of America

Recall from Section 5.4 that the **Cartesian product** of two sets A and B, written $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$. That is, $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$.

Let A be the set of all states in the United States and let

$$R = \{(x, y) \in A \times A \mid x \text{ and } y \text{ have a land border in common}\} .$$

For example, since California and Oregon have a land border, we can say that (California, Oregon) $\in R$ and (Oregon, California) $\in R$. Also, since California and Michigan do not share a land border, (California, Michigan) $\notin R$ and (Michigan, California) $\notin R$.

1. Use the roster method to specify the elements in each of the following sets:

   (a) $B = \{y \in A \mid (\text{Michigan}, y) \in R\}$
   (b) $C = \{x \in A \mid (x, \text{Michigan}) \in R\}$
   (c) $D = \{y \in A \mid (\text{Wisconsin}, y) \in R\}$
2. Find two different examples of two ordered pairs (x, y) and (y, z) such that $(x, y) \in R$, $(y, z) \in R$, but $(x, z) \notin R$, or explain why no such example exists. Based on this, is the following conditional statement true or false?

   For all $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.
3. Is the following conditional statement true or false? Explain.

   For all $x, y \in A$, if $(x, y) \in R$ then $(y, x) \in R$.

PREVIEW ACTIVITY 7.1.2: The Solution Set of an Equation with Two Variables

In Section 2.3, we introduced the concept of the **truth set of an open sentence with one variable.** This was defined to be the set of all elements in the universal set that can be substituted for the variable to make the open sentence a true proposition. Assume that x and y represent real numbers. Then the equation

$$4x^2 + y^2 = 16$$

is an open sentence with two variables. An element of the truth set of this open sentence (also called a solution of the equation) is an ordered pair (a, b) of real numbers so that when a is substituted for x and b is substituted for y, the predicate becomes a true statement (a true equation in this case). We can use set builder notation to describe the truth set S of this equation with two variables as follows:

$$S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 4x^2 + y^2 = 16\}.$$

When a set is a truth set of an open sentence that is an equation, we also call the set the **solution set** of the equation.

1. List four different elements of the set S.
2. The graph of the equation $4x^2 + y^2 = 16$ in the xy-coordinate plane is an ellipse. Draw the graph and explain why this graph is a representation of the truth set (solutions set) of the equation $4x^2 + y^2 = 16$.
3. Describe each of the following sets as an interval of real numbers:

   (a) $A = \{x \in \mathbb{R} \mid \text{there exists a } y \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$.
   (b) $B = \{y \in \mathbb{R} \mid \text{there exists an } x \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$.

Introduction to Relations

In Section 6.1, we introduced the formal definition of a function from one set to another set. The notion of a function can be thought of as one way of relating the elements of one set with those of another set (or the same set). A function is a special type of

relation in the sense that each element of the first set, the domain, is "related" to exactly one element of the second set, the codomain.

This idea of relating the elements of one set to those of another set using ordered pairs is not restricted to functions. For example, we may say that one integer, a, is related to another integer, b, provided that a is congruent to b modulo 3. Notice that this relation of congruence modulo 3 provides a way of relating one integer to another integer. However, in this case, an integer a is related to more than one other integer. For example, since

$$5 \equiv 5 \pmod 3,\ 5 \equiv 2 \pmod 3, \text{ and } 5 \equiv -1 \pmod 3,$$

we can say that 5 is related to 3, 5 is related to 2, and 5 is related to -1. Notice that, as with functions, each relation of the form $a \equiv b \pmod 3$ involves two integersa and b and hence involves an ordered pair (a, b), which is an element of $\mathbb{Z} \times \mathbb{Z}$.

Definition: relations

Let A and B be sets. A **relation R from the set A to the set B** is a subset of $A \times B$. That is, R is a collection of ordered pairs where the first coordinate of each ordered pair is an element of A, and the second coordinate of each ordered pair is an element of B.

A relation from the set A to the set A is called a **relation on the set A**. So a relation on the set A is a subset of $A \times A$.

In Section 6.1, we defined the domain and range of a function. We make similar definitions for a relation.

Definition: Domain and Range

If R is a relation from the set A to the set B, then the subset of A consisting of all the first coordinates of the ordered pairs in R is called the *domain* of R. The subset of B consisting of all the second coordinates of the ordered pairs in R is called the *range* of R.

We use the notation dom(R) for the domain of R and range(R) for the range of R. So using set builder notation,

$$\text{dom}(R) = \{u \in A \mid (u, y) \in R \text{ for at least one } y \in B\}$$

$$\text{range}(R) = \{v \in B \mid (x, v) \in R \text{ for at least one } x \in A\} \ .$$

Example 7.1: Domain and Range

A relation was studied in each of the Preview Activities for this section. For Preview Activity 2, the set $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 4x^2 + y^2 = 16\}$ is a subset of $\mathbb{R} \times \mathbb{R}$ and, hence, S is a relation on $\mathbb{R}$. In Problem (3) of Preview Activity 7.1.2, we actually determined the domain and range of this relation.

$$\text{dom}(S) = A = \{x \in \mathbb{R} \mid \text{there exists a } y \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$$

$$\text{range}(S) = B = \{y \in \mathbb{R} \mid \text{there exists an } x \in \mathbb{R} \text{ such that } 4x^2 + y^2 = 16\}$$

So from the results in Preview Activity 7.1.2, we can say that the domain of the relation S is the closed interval [-2, 2] and the range of S is the closed interval [-4, 4].

Progress Check 7.2: Examples of Relations

1. Let $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 64\}$.

   (a) Explain why T is a relation on $\mathbb{R}$.
   (b) Find all values of x such that $(x, 4) \in T$. Find all values of x such that $(x, 9) \in T$.
   (c) What is the domain of the relation T? What is the range of T?
   (d) Since T is a relation on $\mathbb{R}$, its elements can be graphed in the coordinate plane. Describe the graph of the relation T.
2. From Preview Activity 7.1.1, A is the set of all states in the United States, and

$$R = \{(x, y) \in A \times A \mid x \text{ and } y \text{ have a border in common}\}. \quad (7.1.1)$$

(a) Explain why R is a relation on A.
(b) What is the domain of the relation R? What is the range of the relation R?
(c) Are the following statements true or false? Justify your conclusions.
i. For all $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.
ii. For all $x, y, z \in A$, if $(x, y) \in R$ and $(y, x) \in R$, then $(x, z) \in R$.

Answer

Add texts here. Do not delete this text first.

Some Standard Mathematical Relations

There are many different relations in mathematics. For example, two real numbers can be considered to be related if one number is less than the other number. We call this the "less than" relation on $\mathbb{R}$. If $x, y \in \mathbb{R}$ and x is less than y, we often write $x < y$. As a set of ordered pairs, this relation is $R_<$, where

\{R_{<} = \{(x, y) \in \mathbb{R} \times \mathbb{R}\ |\ x < y\}\).

With many mathematical relations, we do not write the relation as a set of ordered pairs even though, technically, it is a set of ordered pairs. Table 7.1 describes some standard mathematical relations.

Name	Open Sentence	Relation as a Set of Ordered Pairs
The "less than" relation on $\mathbb{R}$	$x < y$	$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$
The "equality" relation on $\mathbb{R}$	$x = y$	$\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$
The "divides" relation on $\mathbb{Z}$	$m \mid n$	$\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}$
The "subset" relation on $\mathcal{P}(U)$	$S \subseteq T$	$\{(S, T) \in P(U) \times P(U) \mid S \subseteq T\}$
The "element of" relation from U to $\mathcal{P}(U)$	$x \in S$	$\{(x, S) \in U \times P(U) \mid x \in S\}$
The "congruence modulo n" relation on $\mathbb{Z}$	$a \equiv b \pmod n$	$\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \pmod n\}$

Table 7.1: Standard Mathematical Relations

Notation for Relations

The mathematical relations in Table 7.1 all used a relation symbol between the two elements that form the ordered pair in $A \times B$. For this reason, we often do the same thing for a general relation from the set A to the set B. So if R is a relation from A to B, and $x \in A$ and $y \in B$, we use the notation

$$\begin{array}{ll} x\ R\ y & \text{to mean} \quad (x, y) \in R; \text{ and} \\ x\ \not{R}\ y & \text{to mean} \quad (x, y) \notin R. \end{array}$$

In some cases, we will even use a generic relation symbol for defining a new relation or speaking about relations in a general context. Perhaps the most commonly use symbol is "~", read "tilde" or "squiggle" or "is related to." When we do this, we will write

$$\begin{array}{rll} x & y & \text{means the same thing as} \quad (x, y) \in R; \text{ and} \\ x & \sim y & \text{means the same thing as} \quad (x, y) \notin R. \end{array} \tag{7.1.2}$$

? Progress Check 7.3: The Divides Relation

Whenever we have spoken about one integer dividing another integer, we have worked with the "divides" relation on $\mathbb{Z}$. In particular, we can write

$$D = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}.$$

In this case, we have a specific notation for "divides," and we write

$m \mid n$ if and only if $(m, n) \in D$.

1. What is the domain of the "divides" relation? What is the range of the "divides" relation?
2. Are the following statements true or false? Explain.

   (a) For every nonzero integer a, $a \mid a$.
   (b) For all nonzero integers a and b, if $a \mid b$, then $b \mid a$.
   (c) For all nonzero integers a, b, and c,if $a \mid b$ and $b \mid c$, then $a \mid c$.

Answer

Add texts here. Do not delete this text first.

Functions as Relations

If we have a function $f : A \to B$, we can generate a set of ordered pairs f that is a subset of $A \times B$ as follows:

$$f = \{(a, f(a)) \mid a \in A\} \text{ or } f = \{(a, b) \in A \times B \mid b = f(a)\}.$$

This means that f is a relation from A to B. Since, dom$(f) = A$, we know that

(1) For every $a \in A$, there exists $a, b \in B$ such that $(a, b) \in f$.

When $(a, b) \in f$., we write $b = f(a)$. In addition, to be a function, each input can produce only one output. In terms of ordered pairs, this means that there will never be two ordered pairs (a, b) and $a, c)$ in the function f, where $a \in A$, $b, c \in B$, and $b = c$. We can formulate this as a conditional statement as follows:

(2) For every $a \in A$ and every $b, c \in B$, if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

This means that a function f from A to B is a relation from A to B that satisfies conditions (1) and (2). (See Theorem 6.22 in Section 6.5.) Not every relation, however, will be a function. For example, consider the relation T in Progress Check 7.2.

? Progress Check 7.4: A Set of Ordered Pairs

Let $F = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$. The set F can then be considered to be relation on $\mathbb{R}$ since it is a subset of $\mathbb{R} \times \mathbb{R}$.

1. List five different ordered pairs that are in the set F.
2. Use the roster method to specify the elements of each of the following the sets:

   (a) $A = \{x \in \mathbb{R} \mid (x, 4) \in F\}$
   (b) $B = \{x \in \mathbb{R} \mid (x, 10) \in F\}$
   (c) $C = \{y \in \mathbb{R} \mid (5, y) \in F\}$
   (d) $D = \{y \in \mathbb{R} \mid (-3, y) \in F\}$
3. Since each real number x produces only one value of y for which $y = x^2$, the set F can be used to define a function from the set $\mathbb{R}$ to $\mathbb{R}$. Draw a graph of this function.

Answer

Add texts here. Do not delete this text first.

Visual Representations of Relations

In Progress Check 7.4, we were able to draw a graph of a relation as a way to visualize the relation. In this case, the relation was a function from $\mathbb{R}$ to $\mathbb{R}$. In addition, in Progress Check 7.2, we were also able to use a graph to represent a relation. In this case, the graph of the relation $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 64\}$ is a circle of radius 8 whose center is at the origin.

When R is a relation from a subset of the real numbers $\mathbb{R}$ to a subset of $\mathbb{R}$, we can often use a graph to provide a visual representation of the relation. This is especially true if the relation is defined by an equation or even an inequality. For example, if

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geq x^2\},$$

then we can use the following graph as a way to visualize the points in the plane that are also in this relation.

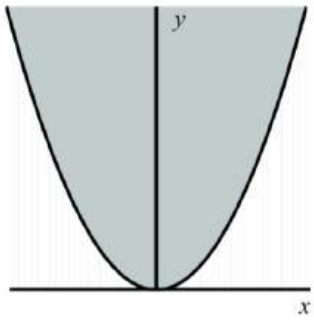


Figure 7.1: Graph of $y \geq x^2$

The points (x, y) in the relation R are the points on the graph of $y = x^2$ or are in the shaded region. This because for these points, $y \geq x^2$. One of the shortcomings of this type of graph is that the graph of the equation and the shaded region are actually unbounded and so we can never show the entire graph of this relation. However, it does allow us to see that the points in this relation are either on the parabola defined by the equation $y = x^2$ or are "inside" the parabola.

When the domain or range of a relation is infinite, we cannot provide a visualization of the entire relation. However, if A is a (small) finite set, a relation R on A can be specified by simply listing all the ordered pairs in R. For example, if $A = \{1, 2, 3, 4\}$, then

$$R = \{(1, 1), (4, 4), (1, 3), (3, 2), (1, 2), (2, 1)\}$$

is a relation on A. A convenient way to represent such a relation is to draw a point in the plane for each of the elements of A and then for each $(x, y) \in R$ (or $x\ R\ y$), we draw an arrow starting at the point x and pointing to the point y. If $(x, x) \in R$ (or $x\ R\ x$), we draw a loop at the point x. The resulting diagram is called a **directed graph** or a **digraph**. The diagram in Figure 7.2 is a digraph for the relation R.

In a directed graph, the points are called the **vertices**. So each element of A corresponds to a **vertex**. The arrows, including the loops, are called the **directed edges** of the directed graph. We will make use of these directed graphs in the next section when we study equivalence relations.

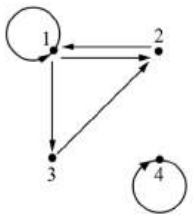


Figure 7.2: Directed Graph for a Relation

? Progress Check 7.5: The Directed Graph of a Relation

Let $A = \{1, 2, 3, 4, 5, 6\}$. Draw a directed graph for the following two relations on the set A. For each relation, it may be helpful to arrange the vertices of A as shown in Figure 7.3.

$R = \{(x, y) \in A \times A \mid x \text{ divides } y\}$, $T = \{(x, y) \in A \times A \mid x + y \text{ is even}\}$.

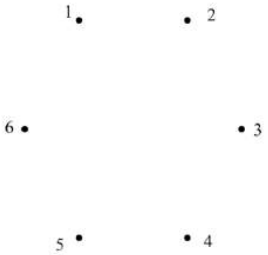


Figure 7.3: Vertices for A

Answer

Add texts here. Do not delete this text first.

Exercise 7.1

1. Let $A = \{a, b, c\}$, $B = \{p, q, r\}$, and let R be the set of ordered pairs defined by $R = \{(a, p), (b, q), (c, p), (a, q)\}$.

   (a) Use the roster method to list all the elements of $A \times B$. Explain why $A \times B$ can be considered to be a relation from A to B.
   (b) Explain why R is a relation from A to B.
   (c) What is the domain of R? What is the range of R?
2. Let $A = \{a, b, c\}$ and let $R = \{(a, a), (a, c), (b, b), (b, c), (c, a), (c, b)\}$ (so R is a relation on A). Are the following statements true or false? Explain.

   (a) For each $x \in A$, $x \, R \, x$.
   (b) For every $x, y \in A$, if $x \, R \, y$, then $y \, R \, x$.
   (c) For every $x, y, z \in A$, if $x \, R \, y$ and $y \, R \, z$, then $x \, R \, z$.
   (d) R is a function from A to A.
3. Let A be the set of all females citizens of the United States. Let D be the relation on A defined by

$$D = \{(x, y) \in A \times A \mid x \text{ is a daughter of } y\}. \tag{7.1.3}$$

   That is, $x \, D \, y$ means that x is a daughter of y.

   (a) Describe those elements of A that are in the domain of D.
   (b) Describe those elements of A that are in the range of D.
   (c) Is the relation D a function from A to A? Explain.
4. Let U be a nonempty set, and let R be the "subset relation" on $\mathcal{P}(U)$. That is,

$$R = \{(S, T) \in \mathcal{P}(U) \times \mathcal{P}(U) \mid S \subseteq T\}. \tag{7.1.4}$$

   (a) Write the open sentence $(S, T) \in R$ using standard subset notation.
   (b) What is the domain of this subset relation, R?
   (c) What is the range of this subset relation, R?
   (d) Is R a function from $\mathcal{P}(U)$ to $\mathcal{P}(U)$? Explain.
5. Let U be a nonempty set, and let R be the "element of" relation from U to $\mathcal{P}(U)$. That is,

$$R = \{(x, S) \in U \times \mathcal{P}(U) \mid x \in S\}. \tag{7.1.5}$$

(a) What is the domain of this “element of” relation, R?
(b) What is the range of this "element of" relation, R?
(c) Is R a function from U to $\mathcal{P}(U)$? Explain.

6. Let $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 100\}$.

   (a) Determine the set of all values of x such that $(x, 6) \in S$, and determine the set of all values of x such that $(x, 9) \in S$.
   (b) Determine the domain and range of the relation S and write each set using set builder notation.
   (c) Is the relation S a function from $\mathbb{R}$ to $\mathbb{R}$? Explain.
   (d) Since S is a relation on $\mathbb{R}$, its elements can be graphed in the coordinate plane. Describe the graph of the relation S. Is the graph consistent with your answers in Exercises (6a) through (6c)? Explain.
7. Repeat Exercise(6) using the relation on $\mathbb{R}$ defined by

$$S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = \sqrt{100 - x^2}\}. \tag{7.1.6}$$

   What is the connection between this relation and the relation in Exercise (6)?
8. Determine the domain and range of each of the following relations on $\mathbb{R}$ and sketch the graph of each relation.

   (a) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 10\}$
   (b) $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y^2 = x + 10\}$
   (c) $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| + |y| = 10\}$
   (d) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 = y^2\}$
9. Let R be the relation on $\mathbb{Z}$, where for all $a, b \in \mathbb{Z}$, $a\, R\, b$ if and only if $|a - b| \leq 2$.

   (a) Use set builder notation to describe the relation R as a set of ordered pairs.
   (b) Determine the domain and range of the relation R.
   (c) Use the roster method to specify these to fall integers x such that $x\, R\, 5$ and the set of all integers x such that $5\, R\, x$.
   (d) If possible, find integers x and y such that $x\, R\, 8$, $8\, R\, y$, but $x \not R\, y$.
   (e) If $a \in \mathbb{Z}$, use the roster method to specify the set of all $x \in \mathbb{Z}$ such that $x\, R\, a$.
10. Let $R_< = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$. This means that $R_<$ is the "less than" relation on $\mathbb{R}$.

    (a) What is the domain of the relation $R_<$?
    (b) What is the range of the relation $R_<$?
    (c) Is the relation $R_<$ a function from $\mathbb{R}$ to $\mathbb{R}$? Explain.

    Note: Remember that a relation is a set. Consequently, we can talk about one relation being a subset of another relation. Another thing to remember is that the elements of a relation are ordered pairs.

Explorations and Activities

11. **The Inverse of a Relation**. In Section 6.5, we introduced the **inverse of a function**. If A and B are nonempty sets and if $f : A \to B$ is a function, then the inverse of f, denoted by f^{-1}, is defined as

$$\begin{aligned} f^{-1} &= \{(b, a) \in B \times A \mid f(a) = b\} \\ &= \{(b, a) \in B \times A \mid (a, b) \in f\}. \end{aligned} \tag{7.1.7}$$

    Now that we know about relations, we see that f^{-1} is always a relation from B to A. The concept of the inverse of a function is actually a special case of the more general concept of the inverse of a relation, which we now define.

Definition

Let R be a relation from the set A to the set B. The inverse of R, written R^{-1} and read "R inverse," is the relation from B to A defined by

$$\begin{aligned} R^{-1} &= \{(y,x) \in B \times A \mid (x,y) \in R\}, \text{ or} \\ R^{-1} &= \{(y,x) \in B \times A \mid x \; R \, y\}. \end{aligned} \tag{7.1.8}$$

That is, R^{-1} is the subset of $B \times A$ consisting of all ordered pairs (y,x) such that $x \; R \, y$.

For example, let D be the "divides" relation on $\mathbb{Z}$. See Progress Check 7.3. So

$$D = \{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}. \tag{7.1.9}$$

This means that we can write $m \mid n$ if and only if $(m,n) \in D$. So, in this case,

$$\begin{aligned} D^{-1} &= \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid (m,n) \in D\} \\ &= \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid m \text{ divides } n\}. \end{aligned} \tag{7.1.10}$$

Now, if we would like to focus on the first coordinate instead of the second coordinate in D^{-1}, we know that "m divides n" means the same thing as "n is a multiple of m." Hence,

$$D^{-1} = \{(n,m) \in \mathbb{Z} \times \mathbb{Z} \mid n \text{ is a multiple of } m\}. \tag{7.1.11}$$

We can say that the inverse of the "divides" relation on $\mathbb{Z}$ is the "is a multiple of" relation on $\mathbb{Z}$.
Theorem 7.6, which follows, contains some elementary facts about inverse.

Theorem 7.6.

Let R be a relation from the set A to the set B. Then

- The domain of R^{-1} is the range of R. That is, dom(R^{-1}) = range(R).
- The range of R^{-1} is the domain of R. That is, range(R^{-1}) = dom(R).
- The inverse of R^{-1} is R. That is, $(R^{-1})^{-1} = R$.

To prove the first part of Theorem 7.6, observe that the goal is to prove that two sets are equal,

$$\text{dom}(R^{-1}) = \text{range}(R)$$

One way to do this is to prove that each is a subset of the other. To prove that dom(R^{-1}) $\subseteq$ range(R), we can start by choosing an arbitrary element of dom(R^{-1}). So let $y \in$ dom(R^{-1}). The goal now is to prove that $y \in$ range(R). What does it mean to say that $y \in$ dom(R^{-1})? It means that there exists an $x \in A$ such that

$$(y,x) \in R^{-1}.$$

Now what does it mean to say that $(y,x) \in R^{-1}$? It means that $(x,y) \in R$. What does this tell us about y?

Complete the proof of the first part of Theorem 7.6. Then, complete the proofs of the other two parts of Theorem 7.6.

Proof

Add proof here and it will automatically be hidden

Answer

Add texts here. Do not delete this text first.

7.2: Equivalence Relations

Preview Activity 7.2.1: Properties of Relations

In previous mathematics courses, we have worked with the equality relation. For example, let R be the relation on $\mathbb{Z}$ defined as follows: For all $a, b \in \mathbb{Z}$, $a \, R \, b$ if and only if $a = b$. We know this equality relation on $\mathbb{Z}$ has the following properties:

- For each $a \in \mathbb{Z}$, $a = b$ and so $a \, R \, a$.
- For all $a, b \in \mathbb{Z}$, if $a = b$, then $b = a$. That is, if $a \, R \, b$, then $b \, R \, a$.
- For all $a, b, c \in \mathbb{Z}$, if $a = b$ and $b = c$, then $a = c$. That is, if $a \, R \, b$ and $b \, R \, c$, then $a \, R \, c$.

In mathematics, when something satisfies certain properties, we often ask if other things satisfy the same properties. Before investigating this, we will give names to these properties.

Definition

Let A be nonempty set and let R be a relation on A.

- The relation R is **reflexive on A** provided that for each $x \in A$, $x \, R \, x$ or, equivalently, $(x, x) \in R$.
- The relation R is **symmetric** provided that for every $x, y \in A$, if $x \, R \, y$, then $y \, R \, x$ or, equivalently, for every $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.
- The relation R is **transitive** provided that for every $x, y, z \in A$, if $x \, R \, y$ and $y \, R \, z$, then $x \, R \, z$ or, equivalently, for every $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

Before exploring examples, for each of these properties, it is a good idea to understand what it means to say that a relation does not satisfy the property. So let A be a nonempty set and let R be a relation on A.

1. Carefully explain what it means to say that the relation R is not reflexive on the set A.
2. Carefully explain what it means to say that the relation R is not symmetric.
3. Carefully explain what it means to say that the relation R is not transitive.
   To illustrate these properties, we let $A = \{1, 2, 3, 4\}$ and define the relations R and T on A as follows:

$$\begin{aligned} R &= \{(1,1), (2,2), (3,3), (4,4), (1,3), (3,2)\} \\ T &= \{(1,1), (1,4), (2,4), (4,1), (4,2)\} \end{aligned} \tag{7.2.1}$$

4. Draw a directed graph for the relation R. Then explain why the relation R is reflexive on A, is not symmetric, and is not transitive.
5. Draw a directed graph for the relation T. Is the relation T reflexive on A? Is the relation T symmetric? Is the relation T transitive? Explain.

Preview Activity 7.2.2: Review of Congruence Modulo n

1. Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. On page 92 of Section 3.1, we defined what it means to say that a is congruent to b modulo n. Write this definition and state two different conditions that are equivalent to the definition.
2. Explain why congruence modulo n is a relation on $\mathbb{Z}$.
3. Carefully review Theorem 3.30 and the proofs given on page 148 of Section 3.5. In terms of the properties of relations introduced in Preview Activity 7.2.1, what does this theorem say about the relation of congruence modulo non the integers?
4. Write a complete statement of Theorem 3.31 on page 150 and Corollary 3.32.
5. Write a proof of the symmetric property for congruence modulo n. That is, prove the following:

Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

Directed Graphs and Properties of Relations

In Section 7.1, we used directed graphs, or digraphs, to represent relations on finite sets. Three properties of relations were introduced in Preview Activity 7.2.1 and will be repeated in the following descriptions of how these properties can be visualized

on a directed graph.

Let A be a nonempty set and let R be a relation on A.

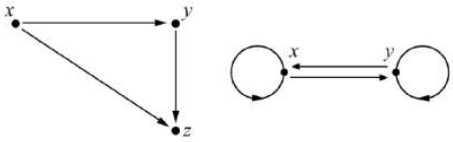
- The relation R is **reflexive on A** provided that for each $x \in A$, $x \; R \; x$ or, equivalently, $.(x, x) \in R$. This means that if a reflexive relation is represented on a digraph, there would have to be a loop at each vertex, as is shown in the following figure.

- The relation R is **symmetric** provided that for every $x, y \in A$, if $x \; R \; y$, then $y \; R \; x$ or, equivalently, for every $x, y \in A$, if $(x, y) \in R$, then $(y, x) \in R$.

  This means that if a symmetric relation is represented on a digraph, then anytime there is a directed edge from one vertex to a second vertex, there would be a directed edge from the second vertex to the first vertex, as is shown in the following figure.

- The relation R is **transitive** provided that for every $x, y, z \in A$, if $x \; R \; y$ and $y \; R \; z$, then $x \; R \; z$ or, equivalently, for every $x, y, z \in A$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$. So if a transitive relation is represented by a digraph, then anytime there is a directed edge from a vertex x to a vertex y and a directed edge from y to a vertex z, there would be a directed edge from x to z.

  In addition, if a transitive relation is represented by a digraph, then anytime there is a directed edge from a vertex x to a vertex y and a directed edge from y to the vertex x, there would be loops at x and y. These two situations are illustrated as follows:



? Progress Check 7.7: Properties of Relations

Let $A = \{a, b, c, d\}$ and let R be the following relation on A:

$$R = \{(a, a), (b, b), (a, c), (c, a), (b, d), (d, b)\}.$$

Draw a directed graph for the relation R and then determine if the relation R is reflexive on A, if the relation R is symmetric, and if the relation R is transitive.

Answer

Add texts here. Do not delete this text first.

Definition of an Equivalence Relation

In mathematics, as in real life, it is often convenient to think of two different things as being essentially the same. For example, when you go to a store to buy a cold soft drink, the cans of soft drinks in the cooler are often sorted by brand and type of soft drink. The Coca Colas are grouped together, the Pepsi Colas are grouped together, the Dr. Peppers are grouped together, and so on. When we choose a particular can of one type of soft drink, we are assuming that all the cans are essentially the same. Even though the specific cans of one type of soft drink are physically different, it makes no difference which can we choose. In doing this, we are saying that the cans of one type of soft drink are equivalent, and we are using the mathematical notion of an equivalence relation.

An equivalence relation on a set is a relation with a certain combination of properties that allow us to sort the elements of the set into certain classes. In this section, we will focus on the properties that define an equivalence relation, and in the next section, we will see how these properties allow us to sort or partition the elements of the set into certain classes.

Definition: equivalence relation

Let A be a nonempty set. A relation $\sim$ on the set A is an **equivalence relation** provided that $\sim$ is reflexive, symmetric, and transitive. For $a, b \in A$, if $\sim$ is an equivalence relation on A and $a \sim b$, we say that $\boldsymbol{a}$ **is equivalent to** $\boldsymbol{b}$.

Most of the examples we have studied so far have involved a relation on a small finite set. For these examples, it was convenient to use a directed graph to represent the relation. It is now time to look at some other type of examples, which may prove to be more interesting. In these examples, keep in mind that there is a subtle difference between the reflexive property and the other two properties. The reflexive property states that some ordered pairs actually belong to the relation R, or some elements of A are related. The reflexive property has a universal quantifier and, hence, we must prove that for all $x \in A$, $x \, R \, x$. Symmetry and transitivity, on the other hand, are defined by conditional sentences. We often use a direct proof for these properties, and so we start by assuming the hypothesis and then showing that the conclusion must follow from the hypothesis.

Example 7.8: A Relation that Is Not an Equivalence Relation

Let M be the relation on $\mathbb{Z}$ defined as follows:

$$\text{For } a, b \in \mathbb{Z}, \; a \; M \; b \text{ if and only if } a \text{ is a multiple of } b.$$

So $a \; M \; b$ if and only if there exists a $k \in \mathbb{Z}$ such that $a = bk$.

- The relation M is reflexive on $\mathbb{Z}$ since for each $x \in \mathbb{Z}$, $x = x \cdot 1$ and, hence, $x \; M \; x$.
- Notice that $4 \; M \; 2$, but $2 \; M \; 4$. So there exist integers x and y such that $x \; M \; y$ but $y \; M \; x$. Hence, the relation M is not symmetric.
- Now assume that $x \; M \; y$ and $y \; M \; z$. Then there exist integers p and q such that

$$x = yp \text{ and } y = zq. \tag{7.2.2}$$

  Using the second equation to make a substitution in the first equation, we see that $x = z(pq)$. Since $pq \in \mathbb{Z}$, we have shown that x is a multiple of z and hence $x \; M \; z$. Therefore, M is a transitive relation.

The relation M is reflexive on $\mathbb{Z}$ and is transitive, but since M is not symmetric, it is not an equivalence relation on $\mathbb{Z}$.

Solution

Add text here.

Progress check 7.9 (a relation that is an equivalence relation)

Define the relation $\sim$ on $\mathbb{Q}$ as follows: For all $a, b \in Q$, $a \sim b$ if and only if $a - b \in \mathbb{Z}$. For example:

- $\frac{3}{4} \sim \frac{7}{4}$ since $\frac{3}{4} - \frac{7}{4} = -1$ and $-1 \in \mathbb{Z}$.
- $\frac{3}{4} \nsim \frac{1}{2}$ since $\frac{3}{4} - \frac{1}{2} = \frac{1}{4}$ and $\frac{1}{4} \notin \mathbb{Z}$.

To prove that $\sim$ is reflexive on $\mathbb{Q}$, we note that for all $q \in \mathbb{Q}$, $a - a = 0$. Since $0 \in \mathbb{Z}$, we conclude that $a \sim a$. Now prove that the relation $\sim$ is symmetric and transitive, and hence, that $\sim$ is an equivalence relation on $\mathbb{Q}$.

Answer

Add texts here. Do not delete this text first.

Congruence Modulo n

One of the important equivalence relations we will study in detail is that of congruence modulo n. We reviewed this relation in Preview Activity 7.2.2.

Theorem 3.30 tells us that congruence modulo n is an equivalence relation on $\mathbb{Z}$. Recall that by the Division Algorithm, if $a \in \mathbb{Z}$, then there exist unique integers q and r such that

$$a = nq + r \text{ and } 0 \leq r < n.$$

Theorem 3.31 and Corollary 3.32 then tell us that $a \equiv r \pmod{n}$. That is, a is congruent modulo n to its remainder r when it is divided by n. When we use the term "remainder" in this context, we always mean the remainder r with $0 \leq r < n$ that is guaranteed by the Division Algorithm. We can use this idea to prove the following theorem.

Theorem 7.10

Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.

Proof

Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. We will first prove that if a and b have the same remainder when divided by n, then $a \equiv b \pmod{n}$. So assume that a and bhave the same remainder when divided by n, and let r be this common remainder. Then, by Theorem 3.31,

$$a \equiv r \pmod{n} \text{ and } b \equiv r \pmod{n}.$$

Since congruence modulo n is an equivalence relation, it is a symmetric relation. Hence, since $b \equiv r \pmod{n}$, we can conclude that $r \equiv b \pmod{n}$. Combining this with the fact that $a \equiv r \pmod{n}$, we now have

$$a \equiv r \pmod{n} \text{ and } r \equiv b \pmod{n}$$

We can now use the transitive property to conclude that $a \equiv b \pmod{n}$. This proves that if a and b have the same remainder when divided by n, then $a \equiv b \pmod{n}$.

We will now prove that if $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n. Assume that $a \equiv b \pmod{n}$, and let r be the least nonnegative remainder when b is divided by n. Then $0 \leq r < n$ and, by Theorem 3.31,

$$b \equiv r \pmod{n}.$$

Now, using the facts that $a \equiv b \pmod{n}$ and $b \equiv r \pmod{n}$, we can use the transitive property to conclude that

$$a \equiv r \pmod{n}$$

This means that there exists an integer q such that $a - r = nq$ or that

$a = nq + r$.

Since we already know that $0 \leq r < n$, the last equation tells us that r is the least nonnegative remainder when a is divided by n. Hence we have proven that if $a \equiv b \pmod{n}$, then a and b have the same remainder when divided by n.

Examples of Other Equivalence Relations

1. The relation $\sim$ on $\mathbb{Q}$ from Progress Check 7.9 is an equivalence relation.
2. Let A be a nonempty set. The **equality relation on A** is an equivalence relation. This relation is also called the **identity relation on A** and is denoted by I_A, where
$$I_A = \{(x, x) \mid x \in A\}. \tag{7.2.3}$$
3. Define the relation $\sim$ on $\mathbb{R}$ as follows:
For $a, b \in \mathbb{R}$, $a \sim b$ if and only if there exists an integer k such that $a - b = 2k\pi$.

   We will prove that the relation ~ is an equivalence relation on $\mathbb{R}$. The relation $\sim$ is reflexive on $\mathbb{R}$ since for each $a \in \mathbb{R}$, $a - a = 0 = 2 \cdot 0 \cdot \pi$.
   Now, let $a, b \in \mathbb{R}$ and assume that $a \sim b$. We will prove that $b \sim a$. Since $a \sim b$, there exists an integer k such that
$$a - b = 2k\pi. \tag{7.2.4}$$

   By multiplying both side of this equation by -1, we obtain
$$\begin{aligned} (-1)(a - b) &= (-1)(2k\pi) \\ b - a &= 2(-k)\pi. \end{aligned} \tag{7.2.5}$$

Since $-k \in \mathbb{Z}$, the last equation proves that $b \sim a$. Hence, we have proven that if $a \sim b$, then $b \sim a$ and, therefore, the relation $\sim$ is symmetric.

To prove transitivity, let $a, b, c \in \mathbb{R}$ and assume that $a \sim b$ and $b \sim c$. We will prove that $a \sim c$. Now, there exist integers k and n such that

$$a - b = 2k\pi \text{ and } b - c = 2n\pi. \tag{7.2.6}$$

By adding the corresponding sides of these two equations, we see that

$$\begin{aligned} (a-b)+(b-c) &= 2k\pi + 2n\pi \\ a - c &= 2(k+n)\pi. \end{aligned} \tag{7.2.7}$$

By the closure properties of the integers, $k+n \in \mathbb{Z}$. So this proves that $a \sim c$ and, hence the relation $\sim$ is transitive.

We have now proven that $\sim$ is an equivalence relation on $\mathbb{R}$. This equivalence relation is important in trigonometry. If $a \sim b$, then there exists an integer k such that $a - b = 2k\pi$ and, hence, $a = b + k(2\pi)$. Since the sine and cosine functions are periodic with a period of 2π, we see that

$$\begin{aligned} sin\, a &= sin(b + k(2\pi)) = sin\, b, \text{ and} \\ cos\, a &= cos(b + k(2\pi)) = cos\, b. \end{aligned} \tag{7.2.8}$$

Therefore, when $a \sim b$, each of the trigonometric functions have the same value at a and b.

4. For an example from Euclidean geometry, we define a relation P on the set $\mathcal{L}$ of all lines in the plane as follows:

   For$l_1, l_2 \in \mathcal{L}$, $l_1\ P\ l_2$ if and only if l_1 is parallel to l_2 or $l_1 = l_2$.

   We added the second condition to the definition of P to ensure that P is reflexive on $\mathcal{L}$. Theorems from Euclidean geometry tell us that if l_1 is parallel to l_2, then l_2 is parallel to l_1, and if l_1 is parallel to l_2 and l_2 is parallel to l_3, then l_1 is parallel to l_3. (Drawing pictures will help visualize these properties.) This tells us that the relation P is reflexive, symmetric, and transitive and, hence, an equivalence relation on $\mathcal{L}$.

? Progress Check 7.11: Another Equivalence Relation

Let U be a finite, nonempty set and let $\mathcal{P}(U)$ be the power set of U. Recall that $\mathcal{P}(U)$ consists of all subsets of U. (See page 222.) Define the relation $\approx$ on $\mathcal{P}(U)$ as follows:

For $A, B \in P(U)$, $A \approx B$ if and only if card(A) = card(B).

For the definition of the cardinality of a finite set, see page 223. This relation states that two subsets of U are equivalent provided that they have the same number of elements. Prove that $\approx$ is an equivalence relation on

Answer

Add texts here. Do not delete this text first.

? Exercise 7.2

1. Let $A = \{a, b\}$ and let $R = \{(a, b)\}$. Is R an equivalence relation on A? If not, is R reflexive, symmetric, or transitive? Justify all conclusions.
2. Let $A = \{a, b, c\}$. For each of the following, draw a directed graph that represents a relation with the specified properties.

   (a) A relation on A that is symmetric but not transitive
   (b) A relation on A that is transitive but not symmetric
   (c) A relation on A that is symmetric and transitive but not reflexive on A

(d) A relation on A that is not reflexive on A, is not symmetric, and is not transitive
(e) A relation on A, other than the identity relation, that is an equivalence relation on A

3. Let $A = \{1, 2, 3, 4, 5\}$. The identity relation on A is

$$I_A = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}. \tag{7.2.9}$$

Determine an equivalence relation on A that is different from I_A or explain why this is not possible.

4. Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| + |y| = 4\}$. Then R is a relation on $\mathbb{R}$. Is R an equivalence relation on $\mathbb{R}$? If not, is R reflexive, symmetric, or transitive? Justify all conclusions.
5. A relation R is defined on $\mathbb{Z}$ as follows: For all a, b in $\mathbb{Z}$, $a\, R\, b$ if and only if $|a - b| \leq 3$. Is R an equivalence relation on $\mathbb{R}$? If not, is R reflexive, symmetric, or transitive. Justify all conclusions.
6. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 4$ for each $x \in \mathbb{R}$. Define a relation $\sim$ on $\mathbb{R}$ as follows:
For $a, b \in \mathbb{R}$, $a \sim b$ if and only if $f(a) = f(b)$.
(a) Is the relation an equivalence relation on $\mathbb{R}$?Justify your conclusion.
(b) Determine all real numbers in the set $C = \{x \in R \mid x \sim 5\}$.
7. Repeat Exercise (6) using the function $f : \mathbb{R} \to \mathbb{R}$ that is defined by $f(x) = x^2 - 3x - 7$ for each $x \in \mathbb{R}$.
8. (a) Repeat Exercise (6a) using the function $f : \mathbb{R} \to \mathbb{R}$ that is defined by $f(x) = sin\, x$ for each $x \in \mathbb{R}$.
(b) Determine all real numbers in the set $C = \{x \in \mathbb{R} \mid x \sim \pi\}$.
9. Define the relation $\sim$ on $\mathbb{Q}$ as follows: For $a, b \in \mathbb{Q}$, $a \sim b$ if and only if $a - b \in \mathbb{Z}$. In progress Check 7.9, we showed that the relation $\sim$ is a equivalence relation on $\mathbb{Q}$.

(a) List four different elements of the set $C = \{x \in \mathbb{Q} \mid x \sim \frac{5}{7}\}$.
(b) Use set builder notation (without using the symbol sim) to specify the set C.
(c) Use the roster method to specify the set C.

10. Let $\sim$ and $\approx$ be relation on $\mathbb{Z}$ defined as follows:

- For $a, b \in Z$, $a \sim b$ if and only if 2 divides $a + b$.
- For $a, b \in Z$, $a \approx b$ if and only if 3 divides $a + b$.

(a) Is $\sim$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?
(b)Is $\approx$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?

11. Let U be a finite, nonempty set and let $\mathcal{P}(U)$ be the power set of U. That is, $\mathcal{P}(U)$ is the set of all subsets of U. Define the relation $\sim$ on $\mathcal{P}(U)$ as follows: For $A, B \in P(U)$, $A \sim B$ if and only if $A \cap B = \emptyset$. That is, the ordered pair (A, B) is in the relaiton $\sim$ if and only if A and B are disjoint.
Is the relation $\sim$ an equivalence relation on $\mathcal{P}(U)$? If not, is it reflexive, symmetric, or transitive? Justify all conclusions.
12. Let U be a nonempty set and let $\mathcal{P}(U)$ be the power set of U. That is, $\mathcal{P}(U)$ is the set of all subsets of U.
For A and B in $\mathcal{P}(U)$, define $A \sim B$ to mean that there exists a bijection $f : A \to B$. Prove that $\sim$ is an equivalence relation on $\mathcal{P}(U)$.
Hint: Use results from Sections 6.4 and 6.5.
13. Let $\sim$ and $\approx$ be relation on $\mathbb{Z}$ defined as follows:

- For $a, b \in Z$, $a \sim b$ if and only if $2a + 3b \equiv 0 \pmod 5$.
- For $a, b \in Z$, $a \approx b$ if and only if $a + 3b \equiv 0 \pmod 5$.

(a) Is $\sim$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?
(b)Is $\approx$ an equivalence relation on $\mathbb{Z}$? If not, is this relation reflexive, symmetric, or transitive?

14. Let $\sim$ and $\approx$ be relation on $\mathbb{R}$ defined as follows:

- For $a, b \in Z$, $a \sim b$ if and only if $xy \geq 0$.
- For $a, b \in Z$, $a \approx b$ if and only if $xy \leq 0$.

(a) Is $\sim$ an equivalence relation on $\mathbb{R}$? If not, is this relation reflexive, symmetric, or transitive?

(b)Is $\approx$ an equivalence relation on $\mathbb{R}$? If not, is this relation reflexive, symmetric, or transitive?

15. Define the relation $\approx$ on $\mathbb{R} \times \mathbb{R}$ as follows: For $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$, $(a, b) \approx (c, d)$ if and only if $a^2 + b^2 = c^2 + d^2$.

(a) Prove that $\approx$ is an equivalence relation on $\mathbb{R} \times \mathbb{R}$.

(b) List four different elements of the set

$$C = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid (x, y) \approx (4, 3)\}. \tag{7.2.10}$$

(c) Give a geometric description of set C.

16. **Evaluation of proofs**

See the instructions for Exercise (19) on page 100 from Section 3.1.

(a)

Proposition. Let R be a relation on a set A. If R is symmetric and transitive, then R is reflexive.

Proof

Let $x, y \in A$. If $x \, R \, y$, then $y \, R \, x$ since R is symmetric. Now, $x \, R \, y$ and $y \, R \, x$, and since R is transitive, we can conclude that $x \, R \, x$. Therefore, R is reflexive.

(b)

Proposition. Let $\sim$ be a relation on $\mathbb{Z}$ where for all $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $(a + 2b) \equiv 0 \pmod 3$. The relation $\sim$ is an equivalence relation on $\mathbb{Z}$.

Proof

Assume $a \sim a$. Then $(a + 2a) \equiv 0 \pmod 3$ since $(3a) \equiv 0 \pmod 3$. Therefore, $\sim$ is reflexive on $\mathbb{Z}$. In addition, if $a \sim b$, then $(a + 2b) \equiv 0 \pmod 3$, and if we multiply both sides of this congruence by 2, we get

$$\begin{aligned} 2(a + 2b) &\equiv 2 \cdot 0 \pmod 3 \\ (2a + 4b) &\equiv 0 \pmod 3 \\ (a + 2b) &\equiv 0 \pmod 3 \\ (b + 2a) &\equiv 0 \pmod 3. \end{aligned} \tag{7.2.11}$$

This means that $b \sim a$ and hence, $\sim$ is symmetric.

We now assume that $(a + 2b) \equiv 0 \pmod 3$ and $(b + 2c) \equiv 0 \pmod 3$.

By adding the corresponding sides of these two congruences, we obtain

$$\begin{aligned} (a + 2b) + (b + 2c) &\equiv 0 + 0 \pmod 3 \\ (a + 3b + 2c) &\equiv 0 \pmod 3 \\ (a + 2c) &\equiv 0 \pmod 3. \end{aligned} \tag{7.2.12}$$

Hence, the relation $\sim$ is transitive and we have proved that $\sim$ is an equivalence relation on $\mathbb{Z}$.

Explorations and Activities

17. **Other Types of Relations.** In this section, we focused on the properties of a relation that are part of the definition of an equivalence relation. However, there are other properties of relations that are of importance. We will study two of these properties in this activity.

A relation R on a set A is a circular relation provided that for all x, y, and z in A, if $x \, R \, y$ and $y \, R \, z$, then $z \, R \, x$.

(a) Carefully explain what it means to say that a relation R on a set A is not circular.

(b) Let $A = \{1, 2, 3\}$. Draw a directed graph of a relation on A that is circular and draw a directed graph of a relation on A that is not circular.
(c) Let $A = \{1, 2, 3\}$. Draw a directed graph of a relation on A that is circular and not transitive and draw a directed graph of a relation on A that is transitive and not circular.

(d) Prove the following proposition:
A relation R on a set A is an equivalence relation if and only if it is reflexive and circular.

A relation R on a set A is an **antisymmetric relation** provided that for all $x, y \in A$, if $x \, R \, y$ and $y \, R \, x$, then $x = y$.

(e) Carefully explain what it means to say that a relation on a set A is not antisymmetric.

(f) Let $A = \{1, 2, 3\}$. Draw a directed graph of a relation on A that is antisymmetric and draw a directed graph of a relation on A that is not antisymmetric.

(g)Are the following propositions true or false? Justify all conclusions.

- If a relation R on a set A is both symmetric and antisymmetric, then R is transitive.
- If a relation R on a set A is both symmetric and antisymmetric, then R is reflexive.

Answer

Add texts here. Do not delete this text first.

7.3: Equivalence Classes

PREVIEW ACTIVITY 7.3.1: Sets Associated with a Relation

As was indicated in Section 7.2, an equivalence relation on a set A is a relation with a certain combination of properties (reflexive, symmetric, and transitive) that allow us to sort the elements of the set into certain classes. This is done by means of certain subsets of A that are associated with the elements of the set A. This will be illustrated with the following example. Let $A = \{a, b, c, d, e\}$, and let R be the relation on the set A defined as follows:

$a\,R\,a$ $b\,R\,b$ $c\,R\,c$ $d\,R\,d$ $e\,R\,e$
$a\,R\,b$ $b\,R\,a$ $b\,R\,e$ $e\,R\,b$
$a\,R\,e$ $e\,R\,a$ $c\,R\,d$ $d\,R\,c$

For each $y \in A$, define the subset $R[y]$ of A as follows:

$$R[y] = \{x \in A \mid x\,R\,y\}.$$

That is, $R[y]$ consists of those elements in A such that $x\,R\,y$. For example, using $y = a$, we see that $a\,R\,a$, $b\,R\,a$, and $e\,R\,a$, and so $R[a] = \{a, b, e\}$.

1. Determine $R[b]$, $R[c]$, $R[d]$ and $R[e]$.
2. Draw a directed graph for the relation R and explain why R is an equivalence relation on A.
3. Which of the sets $R[a]$, $R[b]$, $R[c]$, $R[d]$ and $R[e]$ are equal?
4. Which of the sets $R[a]$, $R[b]$, $R[c]$, $R[d]$ and $R[e]$ are disjoint?

As we will see in this section, the relationships between these sets is typical for an equivalence relation. The following example will show how different this can be for a relation that is not an equivalence relation.

Let $A = \{a, b, c, d\}$, and let S be the relation on the set A defined as follows:

$b\,S\,b$ $c\,S\,c$ $d\,S\,d$ $e\,S\,e$
$a\,S\,b$ $a\,S\,d$ $b\,S\,c$
$c\,S\,d$ $d\,S\,c$

5. Draw a digraph that represents the relation S on A. Explain why S is not an equivalence relation on A.

For each $y \in A$, define the subset $S[y]$ of A as follows:
$$S[y] = \{x \in A \mid x\,S\,y\} = \{x \in A \mid (x, y) \in S\}.$$

For example, using $y = b$, we see that $S[b] = \{a, b\}$ since $(a, b) \in S$ and $(b, b) \in S$. In addition, we see that $S[a] = \emptyset$ since there is no x 2 A such that.x;a/ 2 S.

6. Determine $S[c]$, $S[d]$, and $S[e]$.

7. Which of the sets $S[a]$, $S[b]$, $S[c]$, $S[d]$, and $S[e]$ are equal?

8. Which of the sets $S[b]$, $S[c]$, $S[d]$, and $S[e]$ are disjoint?

PREVIEW ACTIVITY 7.3.2: Congruence Modulo 3

An important equivalence relation that we have studied is congruence modulo n on the integers. We can also define subsets of the integers based on congruence modulo n. We will illustrate this with congruence modulo 3. For example, we can define $C[0]$ to be the set of all integers a that are congruent to 0 modulo 3. That is,

$$C[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\}.$$

Since an integer a is congruent to 0 modulo 3 if an only if 3 divides a, we can use the roster method to specify this set as follows:

$$C[0] = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}.$$

1. Use the roster method to specify each of the following sets:

   (a) The set $C[1]$ of all integers a that are congruent to 1 modulo 3. That is, $C[1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}$.
   (b) The set $C[2]$ of all integers a that are congruent to 2 modulo 3. That is, $C[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}$.
   (c) The set $C[3]$ of all integers a that are congruent to 3 modulo 3. That is, $C[3] = \{a \in \mathbb{Z} \mid a \equiv 3 \pmod 3\}$.
2. Now consider the three sets, $C[0]$, $C[1]$, and $C[2]$.

   (a) Determine the intersection of any two of these sets. That is, determine $C[0] \cap C[1]$, $C[0] \cap C[2]$, and $C[1] \cap C[2]$.
   (b) Let $n = 734$. What is the remainder when n is divided by 3? Which of the three sets, if any, contains $n = 734$?
   (c) Repeat Part (2b) for $n = 79$ and for $n = -79$.
   (d) Do you think that $C[0] \cup C[1] \cup C[2] = \mathbb{Z}$ Explain.
   (e) Is the set $C[3]$ equal to one of the sets $C[0]$, $C[1]$, or $C[2]$?
   (f) We can also define $C[4] = \{a \in \mathbb{Z} \mid a \equiv 4 \pmod 3\}$. Is this set equal to any of the previous sets we have studied in this part? Explain.

The Definition of an Equivalence Class

We have indicated that an equivalence relation on a set is a relation with a certain combination of properties (reflexive, symmetric, and transitive) that allow us to sort the elements of the set into certain classes. We saw this happen in the preview activities. We can now illustrate specifically what this means. For example, in Preview Activity 7.3.2, we used the equivalence relation of congruence modulo 3 on $\mathbb{Z}$ to construct the following three sets:

$$\begin{aligned} C[0] &= \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\}, \\ C[1] &= \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}, \text{ and} \\ C[2] &= \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}. \end{aligned} \tag{7.3.1}$$

The main results that we want to use now are Theorem 3.31 and Corollary 3.32 on page 150. This corollary tells us that for any $a \in \mathbb{Z}$, a is congruent to precisely one of the integers 0, 1, or 2. Consequently, the integer a must be congruent to 0, 1, or 2, and it cannot be congruent to two of these numbers. Thus

1. For each $a \in \mathbb{Z}$, $a \in C[0]$, $a \in C[1]$, or $a \in C[2]$; and
2. $C[0] \cap C[1] = \emptyset$, $C[0] \cap C[2] = \emptyset$, and $C[1] \cap C[2] = \emptyset$.

This means that the relation of congruence modulo 3 sorts the integers into three distinct sets, or classes, and that each pair of these sets have no elements in common. So if we use a rectangle to represent $\mathbb{Z}$, we can divide that rectangle into three smaller rectangles, corresponding to $C[0]$, $C[1]$, and $C[2]$ and we might picture this situation as follows:

The Integers

$C[0]$ consisting of all integers with a remainder of 0 when divided by 3	$C[1]$ consisting of all integers with a remainder of 1 when divided by 3	$C[2]$ consisting of all integers with a remainder of 2 when divided by 3

Each integer is in exactly one of the three sets (C[0]\), $C[1]$, or $C[2]$, and two integers are congruent modulo 3 if and only if they are in the same set. We will see that, in a similar manner, if n is any natural number, then the relation of congruence modulo n can be used to sort the integers into n classes. We will also see that in general, if we have an equivalence relation R on a set A, we can sort the elements of the set A into classes in a similar manner.

Definition

Let $\sim$ be an equivalence relation on a nonempty set A. For each $a \in A$, the equivalence class of a determined by $\sim$ is the subset of A, denoted by $[a]$, consisting of all the elements of A that are equivalent to a. That is,

$$[a] = \{x \in A \mid x \sim a\}.$$

We read $[a]$ as "the equivalence class of a" or as "bracket a."

Notes

1. We use the notation $[a]$ when only one equivalence relation is being used. If there is more than one equivalence relation, then we need to distinguish between the equivalence classes for each relation. We often use something like $[a]_{\sim}$, or if R is the name of the relation, we can use $R[a]$ or $[a]_R$ for the equivalence class of a determined by R. In any case, always remember that when we are working with any equivalence relation on a set A if $a \in A$, then *the equivalence class $[a]$ is a subset of A*.
2. We know that each integer has an equivalence class for the equivalence relation of congruence modulo 3. But as we have seen, there are really only three distinct equivalence classes. Using the notation from the definition, they are:

$[0] = \{a \in \mathbb{Z} \mid a \equiv 0 \pmod 3\}$,
$[1] = \{a \in \mathbb{Z} \mid a \equiv 1 \pmod 3\}$, and
$[2] = \{a \in \mathbb{Z} \mid a \equiv 2 \pmod 3\}$.

? Progress Check 7.12 (Equivalence Classes from Preview Activity 7.3.1)

Without using the terminology at that time, we actually determined the equivalence classes of the equivalence relation R in Preview Activity 7.3.1. What are the distinct equivalence classes for this equivalence relation?

Answer

Add texts here. Do not delete this text first.

Congruence Modulo n and Congruence Classes

In Preview Activity 7.3.2, we used the notation $C[k]$ for the set of all integers that are congruent to k modulo 3. We could have used a similar notation for equivalence classes, and this would have been perfectly acceptable. However, the notation $[a]$ is probably the most common notation for the equivalence class of a. We will now use this same notation when dealing with congruence modulo n when only one congruence relation is under consideration.

Definition: congruence class of a modulo n.

Let $n \in \mathbb{N}$. Congruence modulo n is an equivalence relation on $\mathbb{Z}$. So for $a \in \mathbb{Z}$,

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod n\}.$$

In this case, $[a]$ is called the **congruence class of a modulo n**.

We have seen that congruence modulo 3 divides the integers into three distinct congruence classes. Each congruence class consists of those integers with the same remainder when divided by 3. In a similar manner, if we use congruence modulo 2, we simply divide the integers into two classes. One class will consist of all the integers that have a remainder of 0 when divided by 2, and the other class will consist of all the integers that have a remainder of 1 when divided by 2. That is, congruence modulo 2 simply divides the integers into the even and odd integers.

? Progress Check 7.13: Congruence Modulo 4

Determine all of the distinct congruence classes for the equivalence relation of congruence modulo 4 on the integers. Specify each congruence class using the roster method.

Answer

Add texts here. Do not delete this text first.

Properties of Equivalence Classes

As we have seen, in Preview Activity 7.3.1, the relation R was an equivalence relation. For that preview activity, we used $R[y]$ to denote the equivalence class of $y \in A$, and we observed that these equivalence classes were either equal or disjoint.

However, in Preview Activity 7.3.1, the relation S was not an equivalence relation, and hence we do not use the term “equivalence class” for this relation. We should note, however, that the sets $S[y]$ were not equal and were not disjoint. This exhibits one of the main distinctions between equivalence relations and relations that are not equivalence relations.

In Theorem 7.14, we will prove that if $\sim$ is an equivalence relation on the set A, then we can "sort" the elements of A into distinct equivalence classes. The properties of equivalence classes that we will prove are as follows: (1) Every element of A is in its own equivalence class; (2) two elements are equivalent if and only if their equivalence classes are equal; and (3) two equivalence classes are either identical or they are disjoint.

Theorem 7.14

Let A be a nonempty set and let $\sim$ be an equivalence relation on the set A. Then,

1. For each $a \in A$, $a \in [a]$.
2. For each $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$,
3. For each $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Proof

Let A be a nonempty set and assume that $\sim$ is an equivalence relation on A. To prove the first part of the theorem, let $a \in A$. Since $\sim$ is an equivalence relation on A, it is reflexive on A. Thus, $a \sim a$, and we can conclude that $a \in [a]$.

The second part of this theorem is a biconditional statement. We will prove it by proving two conditional statements. We will first prove that if $a \sim b$, then $[a] = [b]$. So let $a, b \in A$ and assume that $a \sim b$. We will now prove that the two sets $[a]$ and $[b]$ are equal. We will do this by proving that each is a subset of the other.

First, assume that $x \in [a]$. Then, by definition, $x \sim a$. Since we have assumed that $a \sim b$, we can use the transitive property of $\sim$ to conclude that $x \sim b$, and this means that $x \in [b]$. This proves that $[a] \subseteq [b]$.

We now assume that $y \in [b]$. This means that $y \sim b$, and hence by the symmetric property, that $b \sim y$. Again, we are assuming that $a \sim b$. So we have

$$a \sim b \text{ and } b \sim y.$$

We use the transitive property to conclude that $a \sim y$ and then, using the symmetric property, we conclude that $y \sim a$. This proves that $y \in [a]$ and, hence, that $[b] \subseteq [a]$. This means that we can conclude that if $a \sim b$, then $[a] = [b]$.

We must now prove that if $[a] = [b]$, then $a \sim b$. Let $a, b \in A$ and assume that $[a] = [b]$. Using the first part of the theorem, we know that $a \in [a]$ and since the two sets are equal, this tells us that $a \in [b]$. Hence by the definition of $[b]$, we conclude that $a \sim b$. This completes the proof of the second part of the theorem.

For the third part of the theorem, let $a, b \in A$. Since this part of the theorem is a disjunction, we will consider two cases: Either

$$[a] \cap [b] = \emptyset \text{ or } [a] \cap [b] \neq \emptyset.$$

In the case where $[a] \cap [b] = \emptyset$, the first part of the disjunction is true, and hence there is nothing to prove. So we assume that $[a] \cap [b] \neq \emptyset$; and will show that $[a] = [b]$. Since $[a] \cap [b] \neq \emptyset$, there is an element x in A such that

$$a \in [a] \cap [b].$$

This means that $x \in [a]$ and $x \in [b]$. Consequently, $x \in a$ and $x \in b$, and so we can use the first part of the theorem to conclude that $[x] = [a]$ and $[x] = [b]$. Hence, $[a] = [b]$, and we have proven that $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Theorem 7.14 gives the primary properties of equivalence classes. Consequences of these properties will be explored in the exercises. The following table restates the properties in Theorem 7.14 and gives a verbal description of each one.

Formal Statement from Theorem 7.14	Verbal Description
For each $a \in A$, $a \in [a]$.	Every element of A is in its own equivalence class.
For each $a,b \in A$, $a \sim b$ if and only if $[a] = [b]$.	Two elements of A are equivalent if and only if their equivalence classes are equal.
For each $a,b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$	Any two equivalence classes are either equal or they are disjoint. This means that if two equivalence classes are not disjoint then they must be equal.

? Progress Check 7.15: Equivalence Classes

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2 - 4$ for each $x \in \mathbb{R}$. Define a relation $\sim$ on $\mathbb{R}$ as follows:

$$\text{For } a, b \in \mathbb{R},\ a \sim b \text{ if and only if } f(a) = f(b).$$

In Exercise (6) of Section 7.2, we proved that $\sim$ is an equivalence relation on $\mathbb{R}$. Consequently, each real number has an equivalence class. For this equivalence relation,

1. Determine the equivalence classes of 5, -5, 10, -10, π, and $-\pi$.
2. Determine the equivalence class of 0.
3. If $a \in \mathbb{R}$, use the roster method to specify the elements of the equivalence class $[a]$.

Answer

Add texts here. Do not delete this text first.

The results of Theorem 7.14 are consistent with all the equivalence relations studied in the preview activities and in the progress checks. Since this theorem applies to all equivalence relations, it applies to the relation of congruence modulo n on the integers. Because of the importance of this equivalence relation, these results for congruence modulo n are given in the following corollary.

Corollary 7.16.

Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.

1. For each $a \in \mathbb{Z}$, $a \in [a]$.
2. For each $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ if and only if $[a] = [b]$.
3. For each $a, b \in \mathbb{Z}$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

For the equivalence relation of congruence modulo n, Theorem 3.31 and Corollary 3.32 tell us that each integer is congruent to its remainder when divided by n, and that each integer is congruent modulo n to precisely one of one of the integers $0, 1, 2, \ldots, n-1$. This means that each integer is in precisely one of the congruence classes $[0], [1], [2], \ldots, [n-1]$ Hence, Corollary 7.16 gives us the following result

Theorem 7.3.1

Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.

1. $\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n-1]$
2. For $j, k \in \{0, 1, 2, \ldots, n-1\}$, if $j \neq k$, then $[j] \cap [k] = \emptyset$.

Partitions and Equivalence Relations

A partition of a set A is a collection of subsets of A that "breaks up" the set A into disjoint subsets. Technically, each pair of distinct subsets in the collection must be disjoint. We then say that the collection of subsets is **pairwise disjoint.** We introduce the following formal definition.

Definition: partition of A

Let A be a nonempty set, and let $\mathcal{C}$ be a collection of subsets of A. The collection of subsets $\mathcal{C}$ is a **partition of A** provided that

1. For each $V \in \mathcal{C}$, $V \neq \emptyset$.
2. For each $x \in A$, there exists a $V \in \mathcal{C}$ such that $x \in V$.
3. For every $V, W \in \mathcal{C}$, $V = W$ or $V \cap W = \emptyset$.

There is a close relation between partitions and equivalence classes since the equivalence classes of an equivalence relation form a partition of the underlying set, as will be proven in Theorem 7.18. The proof of this theorem relies on the results in Theorem 7.14.

Theorem 7.18

Let $\sim$ be an equivalence relation on the nonempty set A. Then the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ is a partition of the set A.

Proof

Let $\sim$ be an equivalence relation on the nonempty set A, and let $\mathcal{C}$ be the collection of all equivalence classes determined by $\sim$. That is,

$$\mathcal{C} = \{[a] \mid a \in A\}.$$

We will use Theorem 7.14 to prove that $\mathcal{C}$ is a partition of A.

Part (1) of Theorem 7.14 states that for each $a \in A$, $a \in [a]$. In terms of the equivalence classes, this means that each equivalence class is nonempty since each element of A is in its own equivalence class. Consequently, $\mathcal{C}$, the collection of all equivalence classes determined by $\sim$, satisfies the first two conditions of the definition of a partition.

We must now show that the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ satisfies the third condition for being a partition. That is, we need to show that any two equivalence classes are either equal or are disjoint. However, this is exactly the result in Part (3) of Theorem 7.14.

Hence, we have proven that the collection C of all equivalence classes determined by $\sim$ is a partition of the set A.

Note: Theorem 7.18 has shown us that if $\sim$ is an equivalence relation on a nonempty set A, then the collection of the equivalence classes determined by $\sim$ form a partition of the set A.

This process can be reversed. This means that given a partition $\mathcal{C}$ of a nonempty set A, we can define an equivalence relation on A whose equivalence classes are precisely the subsets of A that form the partition. This will be explored in Exercise (12).

Exercise 7.3

1. Let $A = \{a, b, c, d, e\}$ and let $\sim$ be the relation on A that is represented by the directed graph in Figure 7.4.

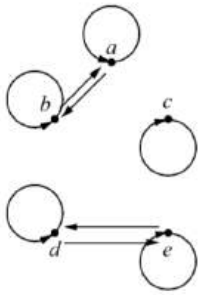


Figure 7.4: Directed Graph for the Relation in Exercise (1)

   Prove that $\sim$ is an equivalence relation on the set A, and determine all of the equivalence classes determined by this equivalence relation.
2. Let $A = \{a, b, c, d, e, f\}$, and assume that $\sim$ is an equivalence relation on A. Also assume that it is known that
   $a \sim b$ $a \nsim c$ $e \sim f$
   $a \sim d$ $a \nsim f$ $e \nsim c$
   Draw a complete directed graph for the equivalence relation $\sim$ on the set A, and then determine all of the equivalence classes for this equivalence relation.
3. Let $A = \{0, 1, 2, 3, \ldots, 999, 1000\}$ Define the relation R on A as follws:
   For $x, y \in A$, $x \; R \; y$ if and only if x and y have the same number of digits.

   Prove that R is an equivalence relation on the set A and determine all of the distinct equivalence classes determined by R.
4. Determine all of the congruence classes for the relation of congruence modulo 5 on the set of integers.

5. Let $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
   (a) Define the relation $\sim$ on $\mathbb{Z}_9$ as follows: for all $a, b \in \mathbb{Z}_9$, $a \sim b$ if and only if $a^2 \equiv b^2 \pmod 9$. Prove that $\sim$ is an equivalence relation on $\mathbb{Z}_9$ and determine all of the distinct equivalence classes of this equivalence relation.
   (b) Define the relation $\approx$ on $\mathbb{Z}_9$ as follows: For all $a, b \in \mathbb{Z}_9$, $a \approx b$ if and only if $a^3 \equiv b^3 \pmod 9$. Prove that $\approx$ is an equivalence relation on $\mathbb{Z}_9$ and determine all of the distinct equivalence classes of this equivalence relation.
6. Define the relation $\sim$ on $\mathbb{Q}$ as follows: For $a, b \in \mathbb{Q}$, $a \sim b$ if and only if $a - b \in \mathbb{Z}$. In Progress Check 7.9 of Section 7.2, we showed that the relation $\sim$ is an equivalence relation on $\mathbb{Q}$. Also, see Exercise (9) in Section 7.2.

   (a) Prove that $[\frac{5}{7} = \{m + \frac{5}{7} \mid m \in \mathbb{Z}\}$.
   (b) If $a \in \mathbb{Z}$, then what is the equivalence class of a?
   (c) If $a \in \mathbb{Z}$, prove that there is a bijection from $[a]$ to $[\frac{5}{7}]$.
7. Define the relation $\sim$ on $\mathbb{R}$ as follows:
   For $x, y \in \mathbb{R}$, $x \sim y$ if and only if $x - y \in \mathbb{Q}$.

   (a) Prove that $\sim$ is an equivalence relation on $\mathbb{R}$.
   (b) List four different real numbers that are in the equivalence class of $\sqrt{2}$.
   (c) If $a \in \mathbb{Q}$, what is the equivalence class of a?
   (d) Prove that $[\sqrt{2}] = \{r + \sqrt{2} \mid r \in \mathbb{Q}\}$.
   (e) If $a \in \mathbb{Q}$, prove that there is a bijection from $[a]$ to $[\sqrt{2}]$.
8. Define the relation $\sim$ on $\mathbb{Z}$ as follows: For $a, b \in \mathbb{Z}$, $a \sim b$ if and only if $(2a + 3b \equiv 0 \pmod 5$. The relation $\sim$ is an equivalence relation on $\mathbb{Z}$. (See Exercise (13) in Section 7.2). Determine all the distinct equivalence classes for this equivalence relation.
9. Let $A = \mathbb{Z} \times (\mathbb{Z} - \{0\})$. That is, $A = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\}$. Define the relation $\approx$ on A as follows:
   For $(a, b), (c, d) \in A$, $(a, b) \approx (c, d)$ if and only if $ad = bc$.

   (a) Prove that $\approx$ is an equivalence relation on A.
   (b) Why was it necessary to include the restriction that $b \neq 0$ in the definition of the set A?
   (c) Determine an equation that gives a relation between a and b if $(a, b) \in A$ and $(a, b) \approx (2, 3)$.
   (d) Determine at least four different elements in [(2, 3)], the equivalence class of (2, 3).
   (e) Use set builder notion to describe [(2, 3)], the equivalence class of (2, 3).
10. For $(a, b)(c, d) \in \mathbb{R} \times \mathbb{R}$, define $(a, b) \sim (c, d)$ if and only if $a^2 + b^2 = c^2 + d^2$. In Exercise (15) of Section 7.2, we proved that $\sim$ is an equivalence relation on $\mathbb{R} \times \mathbb{R}$.

    (a) Determine the equivalence class of (0, 0).
    (b) Use set builder notation (and do not use the symbol $\sim$) to describe the equivalence class of (2, 3) and then give a geometric description of this equivalence class.
    (c) Give a geometric description of a typical equivalence class for this equivalence relation.
    (d) Let $\mathbb{R}^* = \{x \in \mathbb{R} \mid x \geq 0\}$. Prove that there is a one-to-one correspondence (bijection) between $\mathbb{R}^*$ and the set of all equivalence classes for this equivalence relation.
11. Let A be a nonempty set and let $\sim$ be an equivalence relation on A. Prove each of the following:

    (a) For each $a, b \in A$, $a \nsim b$ if and only if $[a] \cap [b] = \emptyset$.
    (b) For each $a, b \in A$, if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$.
    (c) For each $a, b \in A$, if $[a] \cap [b] \neq \emptyset$ then $[a] = [b]$.

Explorations and Activities

12. **A Partition Defines an Equivalence Relation**. Let $A = \{a, b, c, d, e\}$ and let $\mathcal{C} = \{\{a, b, c\}, \{d, e\}\}$.

    (a) Explain why $\mathcal{C}$ is a partition of A.

    Define a relation $\sim$ on A as follows: For $x, y \in A$, $x \sim y$ if and only if there exists a set U in $\mathcal{C}$ such that $x \in U$ and

$y \in U$.

(b) Prove that $\sim$ is an equivalence relation on the set A, and then determine all the equivalence classes for $\sim$. How does the collection of all equivalence classes compare to $\mathcal{C}$?

What we did for the specific partition in Part (12b) can be done for any partition of a set. So to generalize Part (12b), we let A be a nonempty set and let $\mathcal{C}$ be a partition of A. We then define a relation $\sim$ on A as follows:
For $x, y \in A$, $x \sim y$ if and only if there exists a set U in $\mathcal{C}$ such that $x \in U$ and $y \in U$.

(c) Prove that $\sim$ is an equivalence relation on the set A.
(d) Let $a \in A$ and let $U \in \mathcal{C}$ such that $a \in U$. Prove that $[a] = U$.

13. **Equivalence Relations on a Set of Matrices.** The following exercises require a knowledge of elementary linear algebra. We let $\mathcal{M}_{n,n}(\mathbb{R}$ be the set of all n by n matrices with real number entries.

(a) Define a relation $\sim$ on $\mathcal{M}_{n,n}(\mathbb{R}$ as follows: For all $A, B \in \mathcal{M}_{n,n}(\mathbb{R}$, $A \sim B$ if and only if there exists an invertible matrix P in $\mathcal{M}_{n,n}(\mathbb{R}$ such that $B = PAP^{-1}$. Is $\sim$ an equivalence relation on $\mathcal{M}_{n,n}(\mathbb{R}$? Justify your conclusion.
(b) Define a relation R on $\mathcal{M}_{n,n}(\mathbb{R}$ as follows: For all $A, B \in \mathcal{M}_{n,n}(\mathbb{R}$, $A \; R \; B$ if and only if det(A) = det(B). Is R an equivalence relation on $\mathcal{M}_{n,n}(\mathbb{R}$? Justify your conclusion.
(c) Let $\sim$ be an equivalence relation on $\mathbb{R}$. Define a relation $\approx$ on $\mathcal{M}_{n,n}(\mathbb{R}$ as follow: For all $A, B \in \mathcal{M}_{n,n}(\mathbb{R}$, $A \approx B$ if and only if det(A) $\sim$ det(B). Is $\approx$ an equivalence relation on $\mathcal{M}_{n,n}(\mathbb{R}$? Justify your conclusion.

Answer

Add texts here. Do not delete this text first.

7.4: Modular Arithmetic

PREVIEW ACTIVITY7.4.1: Congruence Modulo 6

For this preview activity, we will only use the relation of congruence modulo 6 on the set of integers.

1. Find five different integers a such that $a \equiv 3 \pmod 6$ and find five different integers b such that $b \equiv 4 \pmod 6$. That is, find five different integers in [3], the congruence class of 3 modulo 6 and five different integers in [4], the congruence class of 4 modulo 6.
2. Calculate $s = a + b$ using several values of a in [3] and several values of b in [4] from Part (1). For each sum s that is calculated, find r so that $0 \leq r < 6$ and $s \equiv r \pmod 6$. What do you observe?
3. Calculate $p = a \cdot b$ using several values of a in [3] and several values of b in [4] from Part (1). For each product p that is calculated, find r so that $0 \leq r < 6$ and $p \equiv r \pmod 6$. What do you observe?
4. Calculate $q = a^2$ using several values of a in [3] from Part (1). For each product q that is calculated, find r so that $0 \leq r < 6$ and $q \equiv r \pmod 6$. What do you observe?

PREVIEW ACTIVITY 7.4.2: The Remainder When Dividing by 9

If a and b are integers with b > 0, then from the Division Algorithm, we know that there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < b$.

In this activity, we are interested in the remainder r. Notice that $r = a - bq$. So, given a and b, if we can calculate q, then we can calculate r.

We can use the "int" function on a calculator to calculate q. [The "int" function is the "greatest integer function." If x is a real number, then int(x) is the greatest integer that is less than or equal to x.]

So, in the context of the Division Algorithm, $q = \text{int}(\frac{a}{b})$. Consequently,

$$r = a - b \cdot \text{int}(\frac{a}{b}) \ .$$

If n is a positive integer, we will let $s(n)$ denote the sum of the digits of n. For example, if $n = 731$, then

$$s(731) = 7 + 3 + 1 = 11 \ .$$

For each of the following values of n, calculate

- The remainder when n is divided by 9, and
- The value of $s(n)$ and the remainder when $s(n)$ is divided by 9.

1. $n = 498$
2. $n = 7319$
3. $n = 4672$
4. $n = 9845$
5. $n = 51381$
6. $n = 305877$

What do you observe?

The Integers Modulo n

Let $n \in \mathbb{N}$. Since the relation of congruence modulo n is an equivalence relation on $\mathbb{Z}$, we can discuss its equivalence classes. Recall that in this situation, we refer to the equivalence classes as congruence classes.

Definition: integers modulo n

Let $n \in \mathbb{N}$. The set of congruence classes for the relation of congruence modulo n on $\mathbb{Z}$ is the set of **integers modulo n**, or the set of integers mod n. We will denote this set of congruence classes by $\mathbb{Z}_n$.

Corollary 7.17 tells us that

$$\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n-1] \ .$$

In addition, we know that each integer is congruent to precisely one of the integers 0, 1, 2, ..., $n-1$. This tells us that one way to represent $\mathbb{Z}_n$ is

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots [n-1]\}.$$

Consequently, even though each integer has a congruence class, the set $\mathbb{Z}_n$ has only n distinct congruence classes.

The set of integers $\mathbb{Z}$ is more than a set. We can add and multiply integers. That is, there are the arithmetic operations of addition and multiplication on the set $\mathbb{Z}$, and we know that $\mathbb{Z}$ is closed with respect to these two operations.

One of the basic problems dealt with in modern algebra is to determine if the arithmetic operations on one set "transfer" to a related set. In this case, the related set is $\mathbb{Z}_n$. For example, in the integers modulo 5, $\mathbb{Z}_5$, is it possible to add the congruence classes [4] and [2] as follows?

$$\begin{aligned} [4] \oplus [2] &= [4+2] \\ &= [6] \\ &= [1]. \end{aligned} \tag{7.4.1}$$

We have used the symbol $\oplus$ to denote addition in $\mathbb{Z}_5$ so that we do not confuse it with addition in $\mathbb{Z}$. This looks simple enough, but there is a problem. The congruence classes [4] and [2] are not numbers, they are infinite sets. We have to make sure that we get the same answer no matter what element of [4] we use and no matter what element of [2] we use. For example,

$9 \equiv 4 \pmod 5$ and so [9] = [4]. Also,
$7 \equiv 2 \pmod 5$ and so [7] = [2].

Do we get the same result if we add [9] and [7] in the way we did when we added [4] and [2]? The following computation confirms that we do:

$$\begin{aligned} [9] \oplus [7] &= [9+7] \\ &= [16] \\ &= [1]. \end{aligned} \tag{7.4.2}$$

This is one of the ideas that was explored in Preview Activity 7.4.1. The main difference is that in this preview activity, we used the relation of congruence, and here we are using congruence classes. All of the examples in Preview Activity 7.4.1 should have illustrated the properties of congruence modulo 6 in the following table. The left side shows the properties in terms of the congruence relation and the right side shows the properties in terms of the congruence classes.

If $a \equiv 3 \pmod 6$ and $b \equiv 4 \pmod 6$, then	If $[a] = [3]$ and $[b] = [4]$ in $\mathbb{Z}_6$, then
• $(a+b) \equiv (3+4) \pmod 6$; • $(a \cdot b) \equiv (3 \cdot 4) \pmod 6$.	• $[a+b] = [3+4]$; • $[a \cdot b] = [3 \cdot 4]$.

These are illustrations of general properties that we have already proved in Theorem 3.28. We repeat the statement of the theorem here because it is so important for defining the operations of addition and multiplication in $\mathbb{Z}_n$.

Theorem 3.28

Let n be a natural number and let a, b, c, and d be integers. Then

1. If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $(a+c) \equiv (b+d) \pmod n$.
2. If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$.
3. If $a \equiv b \pmod n$ and $m \in \mathbb{N}$, then $a^m \equiv b^m \pmod n$.

Proof

Add proof here and it will automatically be hidden

Since $x \equiv y \pmod n$ if and only if $[x] = [y]$, we can restate the result of this Theorem 3.28 in terms of congruence classes in $\mathbb{Z}_n$.

Corollary 7.19.

Let n be a natural number and let a, b, c, and d be integers. Then, in $\mathbb{Z}_n$.

1. If $[a] = [b]$ and $[c] = [d]$, then $[a+c] = [b+d]$.
2. If $[a] = [b]$ and $[c] = [d]$, then $[a \cdot c] = [b \cdot d]$.
3. If $[a] = [b]$ and $m \in \mathbb{N}$, then $[a]^m = [b]^m$.

Because of Corollary 7.19, we know that the following formal definition of addition and multiplication of congruence classes in $\mathbb{Z}_n$ is independent of the choice of the elements we choose from each class. We say that these definitions of addition and multiplication are **well defined**.

Definition

Let $n \in \mathbb{N}$. **Addition and multiplication** in $\mathbb{Z}_n$ are defined as follows: For $[a], [c] \in \mathbb{Z}_n$,

$[a] \oplus [c] = [a+c]$ and $[a] \odot [c] = [ac]$.

The term **modular arithmetic** is used to refer to the operations of addition and multiplication of congruence classes in the integers modulo n.

So if $n \in \mathbb{N}$, then we have an addition and multiplication defined on $\mathbb{Z}_n$, the integers modulo n.

Always remember that for each of the equations in the definitions, the operations on the left, $\oplus$ and $\odot$, are the new operations that are being defined. The operations on the right side of the equations ($+$ and $\cdot$) are the known operations of addition and multiplication in $\mathbb{Z}$.

Since $\mathbb{Z}_n$ is a finite set, it is possible to construct addition and multiplication tables for $\mathbb{Z}_n$. In constructing these tables, we follow the convention that all sums and products should be in the form $[r]$, where $0 \leq r < n$. For example, in $\mathbb{Z}_3$, we see that by the definition, $[1] \oplus [2] = [3]$, but since $3 \equiv 0 \pmod 3$, we see that $[3] = [0]$ and so we write

$$[1] \oplus [2] = [3] = [0]$$

Similarly, by definition, $[2] \odot [2] = [4]$, and in $\mathbb{Z}_3$, [4] = [1]. So we write

$$[2] \odot [2] = [4] = [1]$$

The complete addition and multiplication tables for $\mathbb{Z}_3$ are

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

? Progress Check 7.20 (Modular Arithmetic in $\mathbb{Z}_2$, $\mathbb{Z}_5$, and $\mathbb{Z}_6$)

1. Construct addition and multiplication tables for $\mathbb{Z}_2$, the integers modulo 2.
2. Verify that the following addition and multiplication tables for $\mathbb{Z}_5$ are correct.

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

3. Construct complete addition and multiplication tables for $\mathbb{Z}_6$.
4. In the integers, the following statement is true. We sometimes call this the zero product property for the integers.
   For all $a, b \in \mathbb{Z}$, if $a \cdot b = 0$, then $a = 0$ or $b = 0$.
   Write the contrapositive of the conditional statement in this property.
5. Are the following statements true or false? Justify your conclusions.

   (a) For all $[a], [b] \in \mathbb{Z}_5$, if $[a] \odot [b] = [0]$, then $[a] = [0]$ or $[b] = [0]$.

(b) For all $[a], [b] \in \mathbb{Z}_6$, if $[a] \odot [b] = [0]$, then $[a] = [0]$ or $[b] = [0]$.

Answer

Add texts here. Do not delete this text first.

Divisibility Tests

Congruence arithmetic can be used to proof certain divisibility tests. For example, you may have learned that a natural number is divisible by 9 if the sum of its digits is divisible by 9. As an easy example, note that the sum of the digits of 5823 is equal to $5+8+2+3=18$, and we know that 18 is divisible by 9. It can also be verified that 5823 is divisible by 9. (The quotient is 647.) We can actually generalize this property by dealing with remainders when a natural number is divided by 9.

Let $n \in \mathbb{N}$ and let s.n/ denote the sum of the digits of n. For example, if $n = 7319$, then $s(7319) = 7+3+1+9 = 20$. In Preview Activity $7.4.2$, we saw that

$$7319 \equiv 2 \pmod 9 \text{ and } 20 \equiv 2 \pmod 9.$$

In fact, for every example in Preview Activity $7.4.2$, we saw that n and s.n/ were congruent modulo 9 since they both had the same remainder when divided by 9. The concepts of congruence and congruence classes can help prove that this is always true.

We will use the case of $n = 7319$ to illustrate the general process. We must use our standard place value system. By this, we mean that we will write 7319 as follows:

$$7319 = (7 \times 10^3) + (3 \times 10^2) + (1 \times 10^1) + (9 \times 10^0). \tag{7.4.3}$$

The idea is to now use the definition of addition and multiplication in $\mathbb{Z}_9$ to convert equation (7.4.3) to an equation in $\mathbb{Z}_9$. We do this as follows:

$$\begin{aligned} [7319] &= [(7 \times 10^3) + (3 \times 10^2) + (1 \times 10^1) + (9 \times 10^0)] \\ &= [7 \times 10^3] \oplus [3 \times 10^2] \oplus [1 \times 10^1] \oplus [9 \times 10^0] \\ &= ([7] \odot [10^3]) \oplus ([3] \odot [10^2]) \oplus ([1] \odot [10^1]) \oplus ([9] \odot [1]). \end{aligned} \tag{7.4.4}$$

Since $10^3 \equiv 1 \pmod 9$, $10^2 \equiv 1 \pmod 9$ and $10 \equiv 1 \pmod 9$, we can conclude that $[10^3] = [1]$, $[10^2] = [1]$ and $[10] = [1]$. Hence, we can use these facts and equation (7.4.4) to obtain

$$\begin{aligned} [7319] &= ([7] \odot [10^3]) \oplus ([3] \odot [10^2]) \oplus ([1] \odot [10]) \oplus ([9] \odot [1]) \\ &= ([7] \odot [1]) \oplus ([3] \odot [1]) \oplus ([1] \odot [1]) \oplus ([9] \odot [1]) \\ &= [7] \oplus [3] \oplus [1] \oplus [9] \\ &= [7+3+1+9]. \end{aligned} \tag{7.4.5}$$

Equation (7.4.5) tells us that 7319 has the same remainder when divided by 9 as the sum of its digits. It is easy to check that the sum of the digits is 20 and hence has a remainder of 2. This means that when 7319 is divided by 9, the remainder is 2.

To prove that any natural number has the same remainder when divided by 9 as the sum of its digits, it is helpful to introduce notation for the decimal representation of a natural number. The notation we will use is similar to the notation for the number 7319 in equation (7.4.3).

In general, if $n \in \mathbb{N}$, and $n = a_k a_{k-1} \cdots a_1 a_0$ is the decimal representation of n, then

$$n = (a_k \times 10^k) + (a_{k-1} \times 10^{k-1}) + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0).$$

This can also be written using summation notation as follows:

$$n = \textstyle\sum_{j=0}^{k} (a_j \times 10^j).$$

Using congruence classes for congruence modulo 9, we have

$$\begin{aligned} [n] &= [(a_k \times 10^k) + (a_{k-1} \times 10^{k-1}) + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0)] \\ &= [a_k \times 10^k] \oplus [a_{k-1} \times 10^{k-1}] \oplus \cdots \oplus [a_1 \times 10^1] \oplus [a_0 \times 10^0] \\ &= ([a_k] \odot [10^k]) \oplus ([a_{k-1}] \odot [10^{k-1}]) \oplus \cdots \oplus ([a_1] \odot [10^1]) \oplus ([a_0] \odot [10^0]). \end{aligned} \tag{7.4.6}$$

One last detail is needed. It is given in Proposition 7.21. The proof by mathematical induction is Exercise (6).

Proposition 7.21.

If n is a nonnegative integer, then $10^n \equiv 1 \pmod 9$, and hence for the equivalence relation of congruence modulo 9, $[10^n] = [1]$.

If we let $s(n)$ denote the sum of the digits of n, then

$$s(n) = a_k + a_{k-1} + \cdots + a_1 + a_0.$$

Now using equation (7.4.6) and Proposition 7.21, we obtain

\[\begin{array} {rcl} {[n]} &= & {([a_k] \odot [1]) \oplus ([a_{k - 1}] \odot [1]) \oplus \cdot\cdot\cdot \oplus ([a_1] \odot [1]) \oplus ([a_0] \odot [1])} \\ {} &= & {[a_k] \oplus [a_{k - 1}] \oplus \cdot\cdot\cdot \oplus [a_1] \oplus [a_0] \\ {} &= & {[a_k + a_{k-1} + \cdot\cdot\cdot + a_1 + a_0].} \\ {} &= & {[s(n)].} \end{array}\]

This completes the proof of Theorem 7.22.

Theorem 7.22.

Let $n \in \mathbb{N}$ and let $s(n)$ denote the sum of the digits of n. Then

1. $[n] = [s(n)]$, using congruence classes modulo 9.
2. $n \equiv s(n) \pmod 9$
3. $9 \mid n$ if and only if $9 \mid s(n)$.

Part (3) of Theorem 7.22 is called a **divisibility test**. If gives a necessary and sufficient condition for a natural number to be divisible by 9. Other divisibility tests will be explored in the exercises. Most of these divisibility tests can be proved in a manner similar to the proof of the divisibility test for 9.

? Exercise 7.4

1. (a) Complete the addition and multiplication tables for $\mathbb{Z}_4$.
   (b) Complete the addition and multiplication tables for $\mathbb{Z}_7$.
   (c) Complete the addition and multiplication tables for $\mathbb{Z}_8$.
2. The set $\mathbb{Z}_n$ contains n elements. One way to solve an equation in $\mathbb{Z}_n$ is to substitute each of these n elements in the equation to check which ones are solutions. In $\mathbb{Z}_n$, when parentheses are not used, we follow the usual order of operations, which means that multiplications are done first and then additions. Solve each of the following equations:

   (a) $[x]^2 = [1]$ in $\mathbb{Z}_4$
   (b) $[x]^2 = [1]$ in $\mathbb{Z}_8$
   (c) $[x]^4 = [1]$ in $\mathbb{Z}_5$
   (d) $[x]^2 \oplus [3] \odot [x] = [3]$ in $\mathbb{Z}_6$
   (e) $[x]^2 \oplus [1] = [0]$ in $\mathbb{Z}_5$
   (f) $[3] \odot [x] \oplus [2] = [0]$ in $\mathbb{Z}_5$
   (g) $[3] \odot [x] \oplus [2] = [0]$ in $\mathbb{Z}_6$
   (h) $[3] \odot [x] \oplus [2] = [0]$ in $\mathbb{Z}_9$
3. In each case, determine if the statement is true or false.

   (a) For all $[a] \in \mathbb{Z}_6$, if $[a] \neq [0]$, then there exists a $[b] \in \mathbb{Z}_6$ such that $[a] \odot [b] = [1]$.
   (b) For all $[a] \in \mathbb{Z}_5$, if $[a] \neq [0]$, then there exists a $[b] \in \mathbb{Z}_5$ such that $[a] \odot [b] = [1]$.
4. In each case, determine if the statement is true or false.

   (a) For all $[a], [b] \in \mathbb{Z}_6$, if $[a] \neq [0]$ and $[b] \neq [0]$, then $[a] \odot [b] \neq [0]$.
   (b) For all $[a], [b] \in \mathbb{Z}_5$, if $[a] \neq [0]$ and $[b] \neq [0]$, then $[a] \odot [b] \neq [0]$.

5. (a) Prove the following proposition:
   For each $[a] \in \mathbb{Z}_5$, if $[a] \neq [0]$, then $[a]^2 = [1]$ or $[a]^2 = [4]$.
   (b) Does there exist an integer a such that $a^2 = 5, 158, 232, 468, 953, 153$ Use your work in Part (a) to justify your conclusion. Compare to Exercise (10) in Section 3.5.
6. Use mathematical induction to prove Proposition 7.21.
   If n is a nonnegative integer, then $10^n \equiv 1 \pmod 9$, and hence for the equivalence relation of congruence modulo 9, $[10^n] = [1]$.
7. Use mathematical induction to prove that if n is a nonnegative integer, then $10^n \equiv 1 \pmod 3$. Hence, for congruence classes modulo 3, if n is a nonnegative integer, then $[10^n] = [1]$.
8. Let $n \in \mathbb{N}$ and let $s(n)$ denote the sum of the digits of n.So if we write

$$n = (a_k \times 10^k \backslash) + (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.7}$$

   then $s(n) = a_k + a_{k-1} + \cdots + a_1 + a_0$. Use the result in Exercise (7) to help prove each of the following:

   (a) $[n] = [s(n)]$, using congruence classes modulo 3.
   (b) $n \equiv s(n) \pmod 3$.
   (c) $3 \mid n$ if only if $3 \mid s(n)$.
9. Use mathematical induction to prove that if n is an integer and $nge1$, then $10^n \equiv 0 \pmod 5$. Hence, for congruence classes modulo 5, if n is an integer and $n \geq 1$, then $[10^n] = [0]$.
10. Let $n \in \mathbb{N}$ and assume

$$n = (a_k \times 10^k) + (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.8}$$

    Use the result in Exercise (9) to help prove each of the following:

    (a) $[n] = [a_0]$, using congruence classes modulo 5.
    (b) $n \equiv a_0 \pmod 5$.
    (c) $5 \mid n$ if only if $5 \mid a_0$.
11. Use mathematical induction to prove that if n is an integer and $nge2$, then $10^n \equiv 0 \pmod 4$. Hence, for congruence classes modulo 4, if n is an integer and $n \geq 2$, then $[10^n] = [0]$.
12. Let $n \in \mathbb{N}$ and assume

$$n = (a_k \times 10^k) + (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.9}$$

    Use the result in Exercise (11) to help prove each of the following:

    (a) $[n] = [10a_1 + a_0]$, using congruence classes modulo 4.
    (b) $n \equiv (10a_1 + a_0) \pmod 5$.
    (c) $4 \mid n$ if only if $4 \mid (10a_1 + a_0)$.
13. Use mathematical induction to prove that if n is an integer and $nge3$, then $10^n \equiv 0 \pmod 8$. Hence, for congruence classes modulo 8, if n is an integer and $n \geq 3$, then $[10^n] = [0]$.
14. Let $n \in \mathbb{N}$ and assume

$$n = (a_k \times 10^k) + (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.10}$$

    Use the result in Exercise (13) to help develop a divisibility test for 8. Prove that your divisibility test is correct.
15. Use mathematical induction to prove that if n is a nonnegative integer then $10^n \equiv (-1)^n (mod 11)$. Hence, for congruence classes modulo 11, if n is a nonnegative integer, then $[10^n] = [(-1)^n]$.
16. Let $n \in \mathbb{N}$ and assume

$$n = (a_k \times 10^k) + (a_{k-1} \times 10^{k-1} + \cdots + (a_1 \times 10^1) + (a_0 \times 10^0). \tag{7.4.11}$$

Use the result in Exercise (15) to help prove each of the following:

(a) $n \equiv \sum_{j=0}^{k}(-1)^j a_j \pmod{11}$.
(b) $[n] = [\sum_{j=0}^{k}(-1)^j a_j]$, using congruence classes modulo 11.
(c) 11 divides n if and only if 11 divides $\sum_{j=0}^{k}(-1)^j a_j$

17. (a) Prove the following proposition:
For all $[a], [b] \in \mathbb{Z}_3$, if $[a]^2 + [b]^2 = [0]$, then $[a] = 0$ and $[b] = [0]$.
(b) Use Exercise (17a) to prove the following proposition:
Let $a, b \in \mathbb{Z}$. If $(a^2 + b^2) \equiv 0 \pmod{3}$, then $a \equiv 0 \pmod{3}$ and $b \equiv 0 \pmod{3}$.
(c) Use Exercise (17b) to prove the following proposition:
Let $a, b \in \mathbb{Z}$, if 3 divides $(a^2 + b^2)$, then 3 divides a and 3 divides b.
18. Prove the following proposition:
For each $a \in \mathbb{Z}$, if there exist integers b and c such that $a = b^4 + c^4$, then the units digit of a must be 0, 1, 2, 5, 6, or 7.
19. Is the following proposition true or false? Justify your conclusion.
For $n \in \mathbb{Z}$. If n is odd, then $8 \mid (n^2 - 1)$. **Hint**: What are the possible values of $n \pmod 8$?
20. Prove the following proposition:
For $n \in \mathbb{Z}$. If $n \equiv 7 \pmod{8}$, then n is not the sum of three squares. That is, there do not exist natural numbers a, b, and c such that $n = a^2 + b^2 + c^2$.

Explorations and Activities

21. Using Congruence Modulo 4. The set $\mathbb{Z}_n$ is a finite set, and hence one way to prove things about $\mathbb{Z}_n$ is to simply use the n elements in $\mathbb{Z}_n$ as the n cases for a proof using cases. For example, if $n \in \mathbb{Z}$, then in $\mathbb{Z}_4$, $[n] = [0]$, $[n] = [1]$, $[n] = [2]$, or $[n] = [3]$.

(a) Prove that if $n \in \mathbb{Z}$, then in $\mathbb{Z}_4$, $[n]^2 = [0]$ or $[n]^2 = [1]$. Use this to conclude that in $\mathbb{Z}_4$, $[n^2] = [0]$ or $[n^2] = [1]$.
(b) Translate the equations $[n^2] = [0]$ and $[n^2] = [1]$ in $\mathbb{Z}_4$ into congruences modulo 4.
(c) Use a result in Exercise (12) to determine the value of r so that $r \in \mathbb{Z}$, $0 \leq r < 3$, and

$$104\,257\,833\,259 \equiv r \pmod{4}. \tag{7.4.12}$$

That is, $[104\,257\,833\,259] = [r]$in $\mathbb{Z}_4$.
(d) Is the natural number 104 257 833 259 a perfect square? Justify your conclusion.

Answer

Add texts here. Do not delete this text first.

7.S: Equivalence Relations (Summary)

Important Definitions

- Relation from A to B, page 364
- Relation on A, page 364
- Domain of a relation, page 364
- Range of a relation, page 364
- Inverse of a relation, page 373
- Reflexive relation, page 375
- Symmetric relation, page 375
- Transitiverelation,page375
- Equivalence relation, page 378
- Equivalence class, page 391
- Congruence class, page 392
- Partition of a set, page 395
- Integers modulo n, page 402
- Addition in $\mathbb{Z}_n$, page 404
- Multiplication in $\mathbb{Z}_n$, page 404

Important Theorems and Results about Relations, Equivalence Relations, and Equivalence Classes

- **Theorem 7.6.** Let R be a relation from the set A to the set B. Then

  1. The domain of R^{-1} is range of R. That is, dom(R^{-1}) = range(R).
  2. The range of R^{-1} is domain of R. That is, range(R^{-1}) = dom(R).
  3. The inverse of R^{-1} is R. That is, $(R^{-1})^{-1} = R$.
- **Theorem 7.10.** Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n.
- **Theorem 7.14.** Let A be a nonempty set and let $\sim$ be an equivalence relation on A.

  1. For each $a \in A$, $a \in [a]$.
  2. For each $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$.
  3. For each $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.
- **Corollary 7.16.** Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.

  1. For each $a \in \mathbb{Z}$, $a \in [a]$.
  2. For each $a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ if and only if $[a] = [b]$.
  3. For each $a, b \in \mathbb{Z}$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.
- **Corollary 7.17.** Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, let $[a]$ represent the congruence class of a modulo n.

  1. $\mathbb{Z} = [0] \cup [1] \cup [2] \cup \cdots \cup [n-1]$
  2. For $j, k \in \{0, 1, 2, \ldots, n-1\}$, if $j \neq k$, then $[j] \cap [k] = \emptyset$.
- Theorem 7.18. Let $\sim$ be an equivalence relation on the nonempty set A. Then the collection $\mathcal{C}$ of all equivalence classes determined by $\sim$ is a partition of the set A.

CHAPTER OVERVIEW

8: Topics in Number Theory

Thumbnail: Golden spiral. Assuming a square has the side length of 1, the next smaller square is 1/φ wide. Then a width of 1/φ², 1/φ³ and so on. (Public Domain; Jahobr).

8.1: The Greatest Common Divisor

Preview Activity 8.1.1: The Greatest Common Divisor

1. Explain what it means to say that a nonzero integer m divides an integer n. Recall that we use the notation $m \mid n$ to indicate that the nonzero integer m divides the integer n.
2. Let m and n be integers with $m \neq 0$. Explain what it means to say that m does not divide n.

Definition

Let a and b be integers, not both 0. A **common divisor** of a and b is any nonzero integer that divides both a and b. The largest natural number that divides both a and b is called the **greatest common divisor** of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

1. Use the roster method to list the elements of the set that contains all the natural numbers that are divisors of 48.
2. Use the roster method to list the elements of the set that contains all the natural numbers that are divisors of 84.
3. Determine the intersection of the two sets in Parts (3) and (4). This set contains all the natural numbers that are common divisors of 48 and 84.
4. What is the greatest common divisor of 48 and 84?
5. Use the method suggested in Parts (3) through (6) to determine each of the following: gcd (8, -12), gcd (0, 5), gcd (8, 27), and gcd (14, 28).
6. If a and b are integers, make a conjecture about how the common divisors of a and b are related to the greatest common divisor of a and b.

Preview Activity 8.1.2: The GCD and the Division Algorithm

When we speak of the quotient and the remainder when we "divide an integer a by the positive integer b," we will always mean the quotient q and the remainder r guaranteed by the Division Algorithm. (See Section 3.5, page 143.)

1. Each row in the following table contains values for the integers a and b. In this table, the value of r is the remainder (from the Division Algorithm) when a is divided by b. Complete each row in this table by determining $\gcd(a, b)$, r, and $\gcd(b, r)$.

a	b	$\gcd(a, b)$	Remainder r	$\gcd(b, r)$
44	12			
75	21			
50	33			

2. Formulate a conjecture based on the results of the table in Part (1).

The System of Integers

Number theory is a study of the system of integers, which consists of the set of integers, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$and the various properties of this set under the usual operations of addition and multiplication and under the usual ordering relation of "less than." The properties of the integers in Table 8.1 will be considered axioms in this text.

Table 8.1: Axioms for the Integers

	For all integers a, b, and c;
Closure Properties for Addition and Multiplication	$a + b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$
Commutative Properties for Addition and Multiplication	$a + b = b + a$, and $ab = ba$
Associative Properties for Addition and Multiplication	$(a + b) + c = a + (b + c)$ and $(ab)\, c = a\, (bc)$
Distributive Properties of Multiplication over Addition	$a\,(b + c) = (ab + ac)$, and $(b + c)\, a = ba + ca$
Additive and Multiplicative Identity Properties	$a + 0 = 0 + a = a$, and $a \cdot 1 = 1 \cdot a = a$

	For all integers a, b, and c;
Additive Inverse Property	\(a + (-a) = (-a) + a = 0

We will also assume the properties of the integers shown in Table 8.2. These properties can be proven from the properties in Table 8.1. (However, we will not do so here.)

Table 8.2: Properties of the Integers

Zero Property of Multiplication	If $a \in \mathbb{Z}$, then $a \cdot 0 = 0 \cdot a = 0$.
Cancellation Properties of Addition and Multiplication	If $a, b, c \in \mathbb{Z}$, and $a + b = a + c$, then $b = c$. If $a, b, c \in \mathbb{Z}$, $a \neq 0$ and $ac = bc$, then $b = c$.

We have already studied a good deal of number theory in this text in our discussion of proof methods. In particular, we have studied even and odd integers, divisibility of integers, congruence, and the Division Algorithm. See the summary for Chapter 3 for a summary of results concerning even and odd integers as well as results concerning properties of divisors. We reviewed some of these properties and the Division Algorithm in the Preview Activities.

The Greatest Common Divisor

One of the most important concepts in elementary number theory is that of the greatest common divisor of two integers. The definition for the greatest common divisor of two integers (not both zero) was given in Preview Activity 8.1.1.

1. If $a, b \in \mathbb{Z}$ and a and b are not both 0, and if $d \in \mathbb{N}$, then $d =$ gcd (a, b) provided that it satisfies all of the following properties:
   - $d \mid a$ and $d \mid b$. That is, d is a common divisor of a and b.
   - If k is a natural number such that $k \mid a$ and $k \mid b$, then $k \leq d$ .That is, any other common divisor of a and b is less than or equal to d.
2. Consequently, a natural number d is not the greatest common divisor of a and b provided that it does not satisfy at least one of these properties. That is, d is not equal to gcd(a, b) provided that
   - • d does not divide a or d does not divide b; or
   - • There exists a natural number k such that $k \mid a$ and $k \mid b$ and $k > d$.
3. This means that d is not the greatest common divisor of a and b provided that it is not a common divisor of a and b or that there exists a common divisor of a and b that is greater than d.

In the preview activities, we determined the greatest common divisors for several pairs of integers. The process we used was to list all the divisors of both integers, then list all the common divisors of both integers and, finally, from the list of all common divisors, find the greatest (largest) common divisor. This method works reasonably well for small integers but can get quite cumbersome if the integers are large. Before we develop an efficient method for determining the greatest common divisor of two integers, we need to establish some properties of greatest common divisors.

One property was suggested in Preview Activity 8.1.1. If we look at the results in Part (7) of that preview activity, we should observe that any common divisor of a and b will divide gcd(a, b). In fact, the primary goals of the remainder of this section are

1. To find an efficient method for determining gcd(a, b), where a and b are integers.
2. To prove that the natural number gcd(a, b) is the only natural number d that satisfies the following properties:

   - d divides a and d divides b; and
   - if k is a natural number such that $k \mid a$ and $k \mid b$, then $k \mid d$.

The second goal is only slightly different from the definition of the greatest common divisor. The only difference is in the second condition where $k \leq d$ is replaced by $k \mid d$.

We will first consider the case where a and b are integers with $a \neq 0$ and $b > 0$. The proof of the result stated in the second goal contains a method (called the Euclidean Algorithm) for determining the greatest common divisors of the two integers a and b. The main idea of the method is to keep replacing the pair of integers .a; b/ with another pair of integers .b; r/, where $0 \leq r < b$ and gcd.b; r/ D gcd.a; b/. This idea was explored in Preview Activity 8.1.2. Lemma 8.1is a conjecture that could have been formulated in Preview Activity 8.1.2.

Lemma 8.1.

Let c and d be integers, not both equal to zero. If q and r are integers such that $c = d \cdot q + r$, then gcd(c, d) = gcd(d, r).

Proof

Let c and d be integers, not both equal to zero. Assume that q and r are integers such that $c = d \cdot q + r$. For ease of notation, we will let

$$m = \gcd(c, d) \text{ and } n = \gcd(d, r).$$

Now, m divides c and m divides d. Consequently, there exist integers x and y such that $c = mx$ and $d = my$. Hence,

$$\begin{aligned} r &= c - d \cdot q \\ r &= mx - (my)q \\ r &= m(x - yq). \end{aligned} \tag{8.1.1}$$

But this means that m divides r. Since m divides d and m divides r, m is less than or equal to gcd(d, r). Thus, $m \leq n$.

Using a similar argument, we see that n divides d and n divides r. Since $c = d \cdot q + r$, we can prove that n divides c. Hence, n divides c and n divides d. Thus, $n \leq \gcd(c, d)$ or $n \leq m$. We now have $m \leq n$ and $n \leq m$. Hence, $m = n$ and gcd(c, d) = gcd(d, r).

Progress Check 8.2: Illustrations of Lemma 8.1

We completed several examples illustrating Lemma 8.1 in Preview Activity 8.1.2. For another example, let $c = 56$ and $d = 12$. The greatest common divisor of 56 and 12 is 4.

1. According to the Division Algorithm, what is the remainder r when 56 is divided by 12?
2. What is the greatest common divisor of 12 and the remainder r?

The key to finding the greatest common divisor (in more complicated cases) is to use the Division Algorithm again, this time with 12 and r. We now find integers q_2 and r_2 such that

$$12 = r \cdot q_2 + r_2. \tag{8.1.2}$$

3. What is the greatest common divisor of r and r_2?

Answer

Add texts here. Do not delete this text first.

The Euclidean Algorithm

The example in Progress Check 8.2 illustrates the main idea of the **Euclidean Algorithm** for finding gcd(a, b), which is explained in the proof of the following theorem.

Theorem 8.3: Euclidean Algorithm

Let a and b be integers with $a \neq 0$ and $b > 0$. Then gcd(a, b) is the only natural number d such that

(a) d divides a and d divides b, and
(b) if k is an integer that divides both a and b, then k divides d.

Proof

Let a and b be integers with $a \neq 0$ and $b > 0$, and let $d = \gcd(a, b)$. By the Division Algorithm, there exist integers q_1 and r_1 such that

$$a = b \cdot q_1 + r_1, \text{ and } 0 \leq r_1 < b. \tag{8.1.3}$$

If $r_1 = 0$, then equation (8.1.3) implies that b divides a. Hence, $b = d =$ gcd(a, b) and this number satisfies Conditions (a) and (b).

If $r_1 > 0$, then by Lemma 8.1, gcd(a, b) = gcd(b, r_1). We use the Division Algorithm again to obtain integers q_2 and r_2 such that

$$b = r_1 \cdot q_2 + r_2, \text{ and } 0 \leq r_2 < r_1. \tag{8.1.4}$$

If $r_2 = 0$, then equation (8.1.4) implies that r_1 divides b. This means that $r_1 =$ gcd(b, r_1). But we have already seen that gcd(a, b) = gcd(b, r_1). Hence, $r_1 =$ gcd(a, b). In addition, if k is an integer that divides both a and b, then, using equation (8.1.3), we see that $r_1 = a - b \cdot q_1$ and, hence k divides r_1. This shows that $r_1 =$ gcd(a, b) satisfies Conditions (a) and (b).

If $r_2 > 0$, then by Lemma 8.1, gcd(b, r_1) = gcd(r_1, r_2). But we have already seen that gcd(a, b) = gcd(b, r_1). Hence, gcd(a, b) = gcd(r_1, r_2). We now continue to apply the Division Algorithm to produce a sequence of pairs of integers (all of which have the same greatest common divisor). This is summarized in the following table:

Original Pair	Equation from Division	Inequality from Division Algorithm	New Pair
(a,b)	$a = b \cdot q_1 + r_1$	$0 \leq r_1 < b$	(b,r_1)
(b,r_1)	$b = r_1 \cdot q_2 + r_2$	$0 \leq r_2 < r_1$	(r_1,r_2)
(r_1,r_2)	$r_1 = r_2 \cdot q_1 + r_3$	$0 \leq r_3 < r_2$	(r_2,r_3)
(r_2,r_3)	$r_2 = r_3 \cdot q_1 + r_4$	$0 \leq r_4 < r_3$	(r_3,r_4)
(r_3,r_4)	$r_3 = r_4 \cdot q_1 + r_5$	$0 \leq r_5 < r_4$	(r_4,r_5)
...	...	...	...

From the inequalities in the third column of this table, we have a strictly decreasing sequence of nonnegative integers ($b > r_1 > r_2 > r_3 > r_4 \cdots$). Consequently, a term in this sequence must eventually be equal to zero. Let p be the smallest natural number such that $r_{p+1} = 0$. This means that the last two rows in the preceding table will be

Original Pair	**Equation from Division Algorithm**	**Inequality from Division Algorithm**	**New Pair**
(r_{p-2},r_{p-1})	$r_{p-2} = r_{p-1} \cdot q_p + r_p$	$0 \leq r_p < r_{p-1}$	(r_{p-1},r_p)
(r_{p-1},r_p)	$r_{p-1} = r_p \cdot q_{p+1} + 0$		

Remember that this table was constructed by repeated use of Lemma 8.1 and that the greatest common divisor of each pair of integers produced equals gcd(a, b). Also, the last row in the table indicates that r_p divides r_{p-1}. This means that gcd(r_{p-1}, r_p) = r_p and hence $r_p =$ gcd(a, b).

This proves that $r_p =$ gcd(a, b) satisfies Condition (a) of this theorem. Now assume that k is an integer such that k divides a and k divides b. We proceed through the table row by row. First, since $r_1 = a - b \cdot q$, we see that

$$k \text{ must divide } r_1.$$

The second row tells us that $r_2 = b - r_1 \cdot q_2$. Since k divides b and k divides r_1, we conclude that

$$k \text{ divides } r_2.$$

Continuing with each row, we see that k divides each of the remainders $r_1, r_2, r_3, \ldots, r_p$. This means that $r_p =$ gcd(a, b) satisfies Condition (b) of the theorem.

? Progress Check 8.4 (Using the Euclidean Algorithm)

1. Use the Euclidean Algorithm to determine gcd(180, 126). Notice that we have deleted the third column (Inequality from Division Algorithm) from the following table. It is not needed in the computations.

Original Pair	**Equation from Division Algorithm**	**New Pair**

(180, 126)	$180 = 126 \cdot 1 + 54$	(126, 54)
(126, 54)	126 =	

Consequently, gcd(180, 126) = .

2. Use the Euclidean Algorithm to determine gcd(4208, 288).

Original Pair	Equation from Division Algorithm	New Pair
(4208, 288)	$4208 = 288 \cdot 14 + 176$	(288,)

Consequently, gcd(4208, 288) = .

Answer

Add texts here. Do not delete this text first.

Some Remarks about Theorem 8.3

Theorem 8.3 was proven with the assumptions that $a, b \in \mathbb{Z}$ with $a \neq 0$ and $b > 0$. A more general version of this theorem can be proven with $a, b \in \mathbb{Z}$ and $b = 0$. This can be proven using Theorem 8.3 and the results in the following lemma.

Lemma 8.5.

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then

1. gcd(0, b) = $|b|$.
2. If gcd(a, b) = d, then gcd(a, $-b$) = d.

The proofs of these results are in Exercise (4). An application of this result is given in the next example.

Example 8.6 (Using the Euclidean Algorithm)

Let $a = 234$ and $b = -42$. We will use the Euclidean Algorithm to determine gcd(234, 42).

Step	Original Pair	Equation from Division Algorithm	New Pair
1	(234, 42)	$234 = 42 \cdot 5 + 24$	(42, 24)
2	(42, 24)	$42 = 24 \cdot 1 + 18$	(24, 18)
3	(24, 18)	$24 = 18 \cdot 1 + 6$	(18, 6)
4	(18, 6)	$18 = 6 \cdot 3$	

So gcd(234, 42) = 6 and hence gcd(234, -42) = 6.

Writing gcd(a, b) in Terms of a and b

We will use Example 8.6 to illustrate another use of the Euclidean Algorithm. It is possible to use the steps of the Euclidean Algorithm in reverse order to write gcd(a, b) in terms of a and b. We will use these steps in reverse order to find integers m and n such that gcd(234, 42) = 234m + 42n. The idea is to start with the row with the last nonzero remainder and work backward as shown in the following table:

Explanation	Result
First, use the equation in Step 3 to write 6 in terms of 24 and 18.	$6 \quad = \quad 24 - 18 \cdot 1$

Use the equation in Step 2 to write \(18 = 42 - 24 \cdot 1\). Substitute this into the preceding result and simplify.	$\begin{aligned} 6 &= 24 - 18 \cdot 1 \\ &= 24 - (42 - 24 \cdot 1) \\ &= 42 \cdot (-1) + 24 \cdot 2 \end{aligned}$
We now have written 6 in terms of 42 and 24. Use the equation in Step 1 to write $24 = 234 - 42 \cdot 5$. Substitute this into the preceding result and simplify.	$\begin{aligned} 6 &= 42 \cdot (-1) + 24 \cdot 2 \\ &= 42 \cdot (-1) + (234 - 42 \cdot 5) \cdot 2 \\ &= 234 \cdot 2 + 42 \cdot (-11) \end{aligned}$

Hence, we can write

$$\gcd(234, 42) = 234 \cdot 2 + 42 \cdot (-11).$$

(Check this with a calculator.) In this case, we say that we have written gcd(234, 42) as a linear combination of 234 and 42. More generally, we have the following definition.

Definition

Let a and b be integers. A linear combination of a and b is an integer of the form $ax + by$, where x and y are integers.

? Progress Check 8.7 (Writing the gcd as a Linear Combination)

Use the results from Progress Check 8.4 to

1. Write gcd(180, 126) as a linear combination of 180 and 126.
2. Write gcd(4208, 288) as a linear combination of 4208 and 288.

Answer

Add texts here. Do not delete this text first.

The previous example and progress check illustrate the following important result in number theory, which will be used in the next section to help prove some other significant results.

Theorem 8.8

Let a and b be integers, not both 0. Then gcd(a, b) can be written as a linear combination of a and b. That is, there exist integers u and v such that $\gcd(a, b) = au + bv$.

We will not give a formal proof of this theorem. Hopefully, the examples and activities provide evidence for its validity. The idea is to use the steps of the Euclidean Algorithm in reverse order to write gcd(a, b) as a linear combination of a and b. For example, assume the completed table for the Euclidean Algorithm is

Step	Original Pair	Equation from Division Algorithm	New Pair
1	(a,b)	$a = b \cdot q_1 + r_1$	(b,r_1)
2	(b,r_1)	$b = r_1 \cdot q_2 + r_2$	(r_1,r_2)
3	(r_1,r_2)	$r_1 = r_2 \cdot q_3 + r_3$	(r_2,r_3)
4	(r_2,r_3)	$r_2 = r_3 \cdot q_4 + 0$	(r_3,r_4)

We can use Step 3 to write $r_3 = \gcd(a, b)$ as a linear combination of r_1 and r_2. We can then solve the equation in Step 2 for r_2 and use this to write $r_3 = \gcd(a, b)$ as a linear combination of r_1 and b. We can then use the equation in Step 1 to solve for r_1 and use this to write $r_3 = \gcd(a, b)$ as a linear combination of a and b.

In general, if we can write $r_p = \gcd(a, b)$ as a linear combination of a pair in a given row, then we can use the equation in the preceding step to write $r_p = \gcd(a, b)$ as a linear combination of the pair in this preceding row.

The notational details of this induction argument get quite involved. Many mathematicians prefer to prove Theorem 8.8 using a property of the natural numbers called the Well-Ordering Principle. **The Well-Ordering Principle** for the natural numbers states

that any nonempty set of natural numbers must contain a least element. It can be proven that the Well-Ordering Principle is equivalent to the Principle of Mathematical Induction.

Exercise 8.1

1. Find each of the following greatest common divisors by listing all of the common divisors of each pair of integers.

   (a) gcd(21, 28)
   (b) gcd(-21, 28)
   (c) gcd(58, 63)
   (d) gcd(0, 12)
   (e) gcd(110, 215)
   (f) gcd(110, -215)
2. (a) Let $a \in \mathbb{Z}$ and let $k \in \mathbb{Z}$ with $k \neq 0$. Prove that if $k \mid a$ and $k \mid (a+1)$, then $k \mid 1$, and hence $k = \pm 1$.
   (b) Let $a \in \mathbb{Z}$. Find the greatest common divisor of the consecutive integers a and $a+1$. That is, determine gcd(a, $a+1$).
3. (a) Let $a \in \mathbb{Z}$ and let $k \in \mathbb{Z}$ with $k \neq 0$. Prove that if $k \mid a$ and $k \mid (a+2)$, then $k \mid 2$.
   (b) Let $a \in \mathbb{Z}$. Find the greatest common divisor of the common divisor a and $a+2$.
4. Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Prove each of the following:

   (a) gcd(0, b) = $|b|$
   (b) If gcd(a, b) = d, then gcd(a, $-b$) = d. That is, gcd(a, $-b$) = gcd(a, b).
5. For each of the following pairs of integers, use the Euclidean Algorithm to find gcd(a, b) and to write gcd(a, b) as a linear combination of a and b. That is, find integers m and n such that $d = am + bn$.

   (a) $a = 36, b = 60$
   (b) $a = 901, b = 935$
   (c) $a = 72, b = 714$
   (d) $a = 12528, b = 21361$
   (e) $a = -36, b = -60$
   (f) $a = 901, b = -935$
6. (a) Find integers u and v such that $9u + 14v = 1$ or explain why it is not possible to do so. Then find integers x and y such that $9x + 14y = 10$ or explain why it is not possible to do so.
   (b) Find integers x and y such that $9x + 15y = 10$ or explain why it is not possible to do so.
   (c) Find integers x and y such that $9x + 15y = 3162$ or explain why it is not possible to do so.
7. (a) Notice that gcd(11, 17) = 1. Find integers x and y such that $11x + 17y = 1$.
   (b) Let $m, n \in \mathbb{Z}$. Wrtie the sum $\frac{m}{11} + \frac{n}{17}$ as a single fraction.
   (c) Find two rational numbers with denominators of 11 and 17, respectively, whose sum is equal to $\frac{10}{187}$. **Hint**: Write the rational numbers in the form $\frac{m}{11} + \frac{n}{17}$, where $m, n \in \mathbb{Z}$. Then write

   $$\frac{m}{11} + \frac{n}{17} = \frac{10}{187}. \tag{8.1.5}$$

   Use Exercises (7a) and (7b) to determine m and n.
   (d) Find two rational numbers with denominators 17 and 21, respectively, whose sum is equal to $\frac{326}{357}$ or explain why it is not possible to do so.
   (e) Find two rational numbers with denominators 9 and 15, respectively, whose sum is equal to $\frac{10}{225}$ or explain why it is not possible to do so.

Exploration and Activities

8. **Linear Combinations and the Greatest Common Divisor**

(a) Determine the greatest common divisor of 20 and 12?
(b) Let $d = \gcd(20, 12)$. Write d as a linear combination of 20 and 12.
(c) Generate at least six different linear combinations of 20 and 12. Are these linear combinations of 20 and 12 multiples of gcd(20, 12)?
(d) Determine the greatest common divisor of 21 and -6 and then generate at least six different linear combinations of 21 and -6. Are these linear combinations of 21 and -6 multiples of gcd(21, -6)?
(e) The following proposition was first introduced in Exercise (18) on page 243 in Section 5.2. Complete the proof of this proposition if you have not already done so.

Proposition 5.16

Let a, b, and t be integers with $t \neq 0$. If t divides a and t divides b, then for all integers x and y, t divides $ax + by$

Proof: Let a, b and t be integers with $t \neq 0$, and assume that t divides a and t divides b. We will prove that for all integers x and y, t divides $(ax + by)$.
So let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$. Since t divides a, there exists an integer msuch that ...
(f) Now let a and b be integers, not both zero and let $d = \gcd(a, b)$. Theorem 8.8 states that d is a linear combination of a and b. In addition, let S and T be the following sets:

$$S = \{ax + by \mid x, y \in \mathbb{Z}\} \quad \text{and} \quad T = \{kd \mid k \in \mathbb{Z}\}. \tag{8.1.6}$$

That is, S is the set of all linear combinations of a and b, and T is the set of all multiples of the greatest common divisor of a and b. Does the set S equal the set T? If not, is one of these sets a subset of the other set? Justify your conclusions.

Note: In Parts (c) and (d), we were exploring special cases for these two sets.

Answer

Add texts here. Do not delete this text first.

8.2: Prime Numbers and Prime Factorizations

Preview Activity 8.2.1: Exploring Examples where a Divides $b \cdot c$

1. Find at least three different examples of nonzero integers a, b, and c such that $a \mid (bc)$ but a does not divide b and a does not divide c. In each case, compute gcd(a, b) and gcd(a, c).
2. Find at least three different examples of nonzero integers a, b, and c such that gcd(a, b) = 1 and $a \mid (bc)$. In each example, is there any relation between the integers a and c?
3. Formulate a conjecture based on your work in Parts (1) and (2).

Preview Activity 8.2.2: Prime Factorizations

Recall that a natural number p is a **prime number** provided that it is greater than 1 and the only natural numbers that divide p are 1 and p. A natural number other than 1 that is not a prime number is a **composite number**. The number 1 is neither prime nor composite. (See Exercise 13 from Section 2.4 on page 78.)

1. Give examples of four natural numbers that are prime and four natural numbers that are composite.

Theorem 4.9 in Section 4.2 states that every natural number greater than 1 is either a prime number or a product of prime numbers. When a composite number is written as a product of prime numbers, we say that we have obtained a **prime factorization** of that composite number. For example, since $60 = 2^2 \cdot 3 \cdot 5$, we say that $2^2 \cdot 3 \cdot 5$ is a prime factorization of 60.

2. Write the number 40 as a product of prime numbers by first writing $40 = 2 \cdot 20$ and then factoring 20 into a product of primes. Next, write the number 40 as a product of prime numbers by first writing $40 = 5 \cdot 8$ and then factoring 8 into a product of primes.
3. In Part (2), we used two different methods to obtain a prime factorization of 40. Did these methods produce the same prime factorization or different prime factorizations? Explain.
4. Repeat Parts (2) and (3) with 150. First, start with $150 = 3 \cdot 50$, and then start with $150 = 5 \cdot 30$.

Greatest Common Divisors and Linear Combinations

In Section 8.1, we introduced the concept of the greatest common divisor of two integers. We showed how the Euclidean Algorithm can be used to find the greatest common divisor of two integers, a and b, and also showed how to use the results of the Euclidean Algorithm to write the greatest common divisor of a and b as a linear combination of a and b.

In this section, we will use these results to help prove the so-called Fundamental Theorem of Arithmetic, which states that any natural number greater than 1 that is not prime can be written as product of primes in "essentially" only one way. This means that given two prime factorizations, the prime factors are exactly the same, and the only difference may be in the order in which the prime factors are written. We start with more results concerning greatest common divisors. We first prove Proposition 5.16, which was part of Exercise (18) in Section 5.2 and Exercise (8) in Section 8.1.

Theorem 5.16

Let a, b, and t be integers with $t \neq 0$. If t divides a and t divides b, then for all integers x and y, t divides $(ax + by)$.

Proof

Let a, b, and t be integers with $t \neq 0$, and assuem that t divides a and t divides b. We will prove that for all integers x and y, t divides $(ax + by)$.

So let $x \in \mathbb{Z}$ and let $y \in \mathbb{Z}$. Since t divides a, there exists an integer m such that $a = mt$ and since t divides b, there exists an integer n such that $b = nt$. Using substitution and algebra, we then see that

$$\begin{aligned} ax + by &= (mt)x + (nt)y \\ &= t(mx + ny) \end{aligned} \tag{8.2.1}$$

Since $(mx + ny)$ is an integer, the last equation proves that t divides $ax + by$ and this proves that for all integers x and y, t divides $(ax + by)$.

We now let $a, b \in \mathbb{Z}$, not both 0, and let $d = \gcd(a, b)$. Theorem 8.8 states that d can be written as a linear combination of a and b. Now, since $d \mid a$ and $d \mid b$, we can use the result of Proposition 5.16 to conclude that for all $x, y \in \mathbb{Z}$, $d \mid (ax + by)$. This means that d divides every linear combination of a and b. In addition, this means that d must be the smallest positive number that is a linear combination of a and b. We summarize these results in Theorem 8.9.

Theorem 8.9.

Let $a, b \in \mathbb{Z}$, not both 0.

1. The greatest common divisor, d, is a linear combination of a and b. That is, there exist integers m and n such that $d = am + bn$.
2. The greatest common divisor, d, divides every linear combination of a and b. That is, for all $x, y \in \mathbb{Z}$, $d \mid (ax + by)$.
3. The greatest common divisor, d, is the smallest positive number that is a linear combination of a and b.

Relatively Prime Integers

In Preview Activity 8.2.1, we constructed several examples of integers a, b, and c such that $a \mid (bc)$ but a does not divide b and a does not divide c. For each example, we observed that $\gcd(a, b) \neq 1$ and $\gcd(a, c) \neq 1$.

We also constructed several examples where $a \mid (bc)$ and $\gcd(a, b) = 1$. In all of these cases, we noted that a divides c. Integers whose greatest common divisor is equal to 1 are given a special name.

Definition: relatively prime

Two nonzero integers a and b are *relatively prime* provided that $\gcd(a, b) = 1$.

Progress Check 8.10: Relatively Prime Integers

1. Construct at least three different examples where p is a prime number, $a \in \mathbb{Z}$, and $p \mid a$. In each example, what is gcd(a, p)? Based on these examples, formulate a conjecture about gcd(a, p) when $p \mid a$.
2. Construct at least three different examples where p is a prime number, $a \in \mathbb{Z}$, and p does not divide a. In each example, what is gcd(a, p)? Based on these examples, formulate a conjecture about gcd(a, p) when p does not divide a.
3. Give at least three different examples of integers a and b where a is not prime, b is not prime, and $\gcd(a, b) = 1$, or explain why it is not possible to construct such examples.

Answer

Add texts here. Do not delete this text first.

Theorem 8.11.

Let a and b be nonzero integers, and let p be a prime number.

1. If a and b are relatively prime, then there exist integers m and n such that $am + bn = 1$. That is, 1 can be written as linear combination of a of b.
2. If $p \mid a$, then $\gcd(a, p) = p$.
3. If p does not divide a, then $\gcd(a, p) = 1$.

Part (1) of Theorem 8.11 is actually a corollary of Theorem 8.9. Parts (2) and (3) could have been the conjectures you formulated in Progress Check 8.10. The proofs are included in Exercise (1).

Given nonzero integers a and b, we have seen that it is possible to use the Euclidean Algorithm to write their greatest common divisor as a linear combination of a and b. We have also seen that this can sometimes be a tedious, time-consuming process, which is why people have programmed computers to do this. Fortunately, in many proofs of number theory results, we do not actually have to construct this linear combination since simply knowing that it exists can be useful in proving results. This will be illustrated in the proof of Theorem 8.12, which is based on work in Preview Activity 8.2.1.

Theorem 8.12

Let a, b, be nonzero integers and let c be an integer. If a and b are relatively prime and $a \mid (bc)$, then $a \mid c$

The explorations in Preview Activity 8.2.1 were related to this theorem. We will first explore the forward-backward process for the proof. The goal is to prove that $a \mid c$. A standard way to do this is to prove that there exists an integer q such that

$$c = aq. \tag{8.2.2}$$

Since we are given $a \mid (bc)$, there exists an integer k such that

$$bc = ak. \tag{8.2.3}$$

It may seem tempting to divide both sides of Equation ??? by b, but if we do so, we run into problems with the fact that the integers are not closed under division. Instead, we look at the other part of the hypothesis, which is that a and b are relatively prime. This means that $\gcd(a, b) = 1$. How can we use this? This means that a and b have no common factors except for 1. In light of Equation ???, it seems reasonable that any factor of a must also be a factor of c. But how do we formalize this?

One conclusion that we can use is that since $\gcd(a, b) = 1$, by Theorem 8.11, there exist integers m and n such that

$$am + bn = 1. \tag{8.2.4}$$

We may consider solving equation (8.2.4) for b and substituting this into Equation ???. The problem, again, is that in order to solve Equation ??? for b, we need to divide by n.

Before doing anything else, we should look at the goal in Equation ???. We need to introduce c into Equation ???. One way to do this is to multiply both sides of equation (8.2.4) by c. (This keeps us in the system of integers since the integers are closed under multiplication.) This gives

$$\begin{aligned} (am + bn)c &= 1 \cdot c \\ acm + bcn &= c. \end{aligned} \tag{8.2.5}$$

Notice that the left side of Equation ??? contains a term, bcn, that contains bc. This means that we can use Equation ??? and substitute bc D ak in Equation ???. After doing this, we can factor the left side of the equation to prove that $a \mid c$.

? Progress Check 8.13: Completing the Proof of Theorem 8.12

Write a complete proof of Theorem 8.12.

Answer

Add texts here. Do not delete this text first.

Corollary 8.14

1. Let $a, b \in \mathbb{Z}$, and let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.
2. Let p be a prime number, let $n \in \mathbb{N}$, and let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 a_2 \cdots a_n)$, then there exists a natural number k with $1 \leq k \leq n$ such that $p \mid a_k$.

Part (1) of Corollary 8.14 is a corollary of Theorem 8.12. Part (2) is proved using mathematical induction. The basis step is the case where $n = 1$, and Part (1) is the case where $n = 2$. The proofs of these two results are included in Exercises (2) and (3).

Historical Note: Euclid's Lemma

Part (1) of Corollary 8.14 is known as *Euclid's Lemma*. Most people associate geometry with *Euclid's Elements*, but these books also contain many basic results in number theory. Many of the results that are contained in this section appeared in *Euclid's Elements*.

Prime Numbers and Prime Factorizations

We are now ready to prove the Fundamental Theorem of Arithmetic. The first part of this theorem was proved in Theorem 4.9 in Section 4.2. This theorem states that each natural number greater than 1 is either a prime number or is a product of prime numbers. Before we state the Fundamental Theorem of Arithmetic, we will discuss some notational conventions that will help us with the proof. We start with an example.

We will use $n = 120$. Since $5 \mid 120$, we can write $120 = 5 \cdot 24$. In addition, we can factor 24 as $24 = 2 \cdot 2 \cdot 2 \cdot 3$. So we can write

$$\begin{aligned} 120 &= 5 \cdot 24 \\ &= 5(2 \cdot 2 \cdot 2 \cdot 3). \end{aligned} \tag{8.2.6}$$

This is a prime factorization of 120, but it is not the way we usually write this factorization. Most often, we will write the prime number factors in ascending order. So we write

$$120 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \quad \text{or} \quad 120 = 2^3 \cdot 3 \cdot 5 \, .$$

Now, let $n \in \mathbb{N}$. To write the prime factorization of n with the prime factors in ascending order requires that if we write $n = p_1 p_2 \cdots p_r$, where $p_1 p_2 \cdots p_r$ are prime numbers, we will have $p_1 \leq p_2 \leq \cdots \leq p_r$.

Theorem 8.15: The Fundamental Theorem of Arithmetic

1. Each natural number greater than 1 is either a prime number or is a product of prime numbers.
2. let $n \in \mathbb{N}$ with $n > 1$. Assume that

$$n = p_1 p_2 \cdots p_r \text{ and that } n = q_1 q_2 \cdots q_s, \tag{8.2.7}$$

where $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ are prime with $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. Then $r = s$, and for each j from 1 to r, $p_j = qj$.

Proof

The first part of this theorem was proved in Theorem 4.9. We will prove the second part of the theorem by induction on n using the Second Principle of Mathematical Induction. (See Section 4.2.) For each natural number n with $n > 1$, let $P(n)$ be

If $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$, where $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ are primes with $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$, then $r = s$, and for each j from 1 to r, $p_j = qj$.

For the basis step, we notice that since 2 is a prime number, its only factorization is $2 = 1 \cdot 2$. This means that the only equation of the form $n = p_1 p_2 \cdots p_r$, where $p_1 p_2 \cdots p_r$ are prime numbers, is the case where $r = 1$ and $p_1 = 2$.This proves that $P(2)$ is true.

For the inductive step, let $k \in \mathbb{N}$ with $k \geq 2$. We will assume that $P(2), P(3), \ldots, P(k)$ are true. The goal now is to prove that $P(k+1)$ is true. To prove this, we assume that $(k+1)$ has two prime factorizations and then prove that these prime factorizations are the same. So we assume that

$k+1 = p_1 p_2 \cdots p_r$ and that $k+1 = q_1 q_2 \cdots q_s$, wher $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ are prime with $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$.

We must now prove that $r = s$, and for each j from 1 to r, $p_j = q_j$. We can break our proof into two cases: (1) $p_1 \leq q_1$; and (2) $q_1 \leq p_1$. Since one of these must be true, and since the proofs will be similar, we can assume, without loss of generality, that $p_1 \leq q_1$.

Since $k+1 = p_1 p_2 \cdots p_r$, we know that $p_1 \mid (k+1)$, and hence we may conclude that $p_1 \mid (q_1 q_2 \cdots q_s)$. We now use Corollary 8.14 to conclude that there exists a j with $1 \leq j \leq s$ such that $p_1 \mid q_j$. Since p_1 and q_j are primes, we conclude that

$$p_1 = q_j \, .$$

We now use this and the fact that $k+1 = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ to conclude that

$$p_2 \cdots p_r = q_2 \cdots q_s \ .$$

The product in the previous equation is less that $k+1$. Hence, we can apply our induction hypothesis to these factorizations and conclude that $r = s$, and for each j from 2 to r, $p_j = q_j$.

This completes the proof that if $P(2), P(3), \ldots, P(k)$ are true, then $P(k+1)$ is true. Hence, by the Second Principle of Mathematical Induction, we conclude that $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geq 2$. This completes the proof of the theorem.

Note: We often shorten the result of the Fundamental Theorem of Arithmetic by simply saying that each natural number greater than one that is not a prime has a **unique factorization** as a product of primes. This simply means that if $n \in \mathbb{N}$, $n > 1$, and n is not prime, then no matter how we choose to factor n into a product of primes, we will always have the same prime factors. The only difference may be in the order in which we write the prime factors.

Further Results and Conjectures about Prime Numbers

1. **The Number of Prime Numbers**
   Prime numbers have fascinated mathematicians for centuries. For example, we can easily start writing a list of prime numbers in ascending order. Following is a list of the prime numbers less than 100.

   2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

   This list contains the first 25 prime numbers. Does this list ever stop? The question was answered in Euclid's Elements, and the result is stated in Theorem 8.16. The proof of this theorem is considered to be one of the classical proofs by contradiction.

   Theorem 8.16.

   There are infinitely many prime numbers.

   Proof

   We will use a proof by contradiction. We assume that there are only finitely many primes, and let

   $$p_1, p_2, \ldots, p_m$$

   be the list of all the primes. Let

   $$M = p_1 p_2, \ldots, p_m + 1. \tag{8.2.8}$$

   Notice that $M \neq 1$. So M is either a prime number or, by the Fundamental Theorem of Arithmetic, M is a product of prime numbers. In either case, M has a factor that is a prime number. Since we have listed all the prime numbers, this means that there exists a natural number j with $1 \leq j \leq m$ such that $p_j \mid M$. Now, we can rewrite equation (8.2.8) as follows:

   $$1 = M - p_1 p_2 \cdots p_m. \tag{8.2.9}$$

   We have proved $p_j \mid M$, and since p_j is one of the prime factors of $p_1 p_2 \cdots p_m$, we can also conclude that $p_j \mid (p_1 p_2 \cdots p_m)$. Since p_j divides both of the terms on the right side of equation (8.2.9), we can use this equation to conclude that p_j divides 1. This is a contradiction since a prime number is greater than 1 and cannot divide 1. Hence, our assumption that there are only finitely many primes is false, and so there must be infinitely many primes.

2. There are infinitely many primes, but when we write a list of the prime numbers, we can see some long sequences of consecutive natural numbers that contain no prime numbers. For example, there are no prime numbers between 113 and 127. The following theorem shows that there exist arbitrarily long sequences of consecutive natural numbers containing no prime numbers. A guided proof of this theorem is included in Exercise (15).

Theorem 8.17,

For any natural number n, there exist at least n consecutive natural numbers that are composite numbers.

There are many unanswered questions about prime numbers, two of which will now be discussed.

3. By looking at the list of the first 25 prime numbers, we see several cases where consecutive prime numbers differ by 2. Examples are: 3 and 5; 11 and 13; 17 and 19; 29 and 31. Such pairs of prime numbers are said to be **twin primes**. How many twin primes exist? The answer is not known. The **Twin Prime Conjecture** states that there are infinitely many twin primes. As of June 25, 2010, this is still a conjecture as it has not been proved or disproved.

   For some interesting information on prime numbers, visit the Web site *The Prime Pages* (primes.utm.edu/), where there is a link to The Largest Known Primes Web site. According to information at this site as of June 25, 2010, the largest known twin primes are

$$(65516468355 \times 2^{333333} - 1) \text{ and } (65516468355 \times 2^{333333} + 1). \tag{8.2.10}$$

   Each of these prime numbers contains 100355 digits.

4. Given an even natural number, is it possible to write it as a sum of two prime numbers? For example,

   4 = 2 + 2 6 = 3 + 3 8 = 5 + 3
   78 = 37 + 41 90 = 43 + 47 128 = 67 + 71

   One of the most famous unsolved problems in mathematics is a conjecture made by Christian Goldbach in a letter to Leonhard Euler in 1742. The conjecture, now known as **Goldbach's Conjecture**, is as follows:

   Every even integer greater than 2 can be expressed as the sum of two (not necessarily distinct) prime numbers.

   As of June 25, 2010, it is not known if this conjecture is true or false, al- though most mathematicians believe it to be true.

? Exercise 8.2

1. Prove the second and third parts of Theorem 8.11.

   (a) Let a be a nonzero integer, and let p be a prime number. If $p \mid a$, then $\gcd(a, p) = p$.
   (b) Let a be a nonzero integer, and let p be a prime number. If p does not divide a, then $\gcd(a, p) = 1$.
2. Prove the first part of Corollary 8.14.
   Let $a, b \in \mathbb{Z}$, let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$. **Hint**: Consider two cases: (1) $p \mid a$; and (2) p does not divide a.
3. Use mathematical induction to prove the second part of Corollary 8.14.
   Let p be a prime number, let $n \in \mathbb{N}$, and let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 a_2 \cdots a_n)$, then there exists a $k \in \mathbb{N}$ with $1 \leq k \leq n$ such that $p \mid a_k$.
4. (a) Let a and b be nonzero integers. If there exist integers x and y such that $ax + by = 1$, what conclusion can be made about gcd(a, b)? Explain.
   (b) Let a and b be nonzero integers. If there exist integers x and y such that $ax + by = 2$, what conclusion can be made about gcd(a, b)? Explain.
5. (a) Let $a \in \mathbb{Z}$. What is gcd.a; a C 1/? That is, what is the greatest common divisor of two consecutive integers? Justify your conclusion.

   Hint: Exercise (4) might be helpful.

   (b) Let $a \in \mathbb{Z}$. What conclusion can be made about gcd$(a, a + 2)$? That is, what conclusion can be made about the greatest common divisor of two integers that differ by 2? Justify your conclusion.
6. (a) Let $a \in \mathbb{Z}$. What conclusion can be made about gcd$(a, a + 3)$? That is, what conclusion can be made about the greatest common divisor of two integers that differ by 3? Justify your conclusion.
   (b) Let $a \in \mathbb{Z}$. What conclusion can be made about gcd$(a, a + 4)$? That is, what conclusion can be made about the greatest common divisor of two integers that differ by 4? Justify your conclusion.

7. (a) Let $a = 16$ and $b = 28$. Determine the value of $d = \gcd(a, b)$, and then determine the value of $\gcd(\frac{a}{d}, \frac{b}{d})$.
   (b) Repeat Exercise (7a) with $a = 10$ and $b = 45$.
   (c) Let $a, b \in \mathbb{Z}$, not both equal to 0, and let $d = \gcd(a, b)$. Explain why $\frac{a}{d}$ and $\frac{b}{d}$ are integers. Then prove that $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. Hint: Start by writing d as a linear combination of a and b.
   This says that if you divide both a and b by their greatest common divisor, the result will be two relatively prime integers.
8. Are the following propositions true or false? Justify your conclusions.

   (a) For all integers a, b, and c, if $a \mid c$ and $b \mid c$, then $(ab) \mid c$.
   (b) For all integers a, b, and c, if $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$, then $(ab) \mid c$.
9. In Exercise (16) in Section 3.5, it was proved that if n is an odd integer, then $8 \mid (n^2 - 1$ \). (This result was also proved in Exercise (19) in Section 7.4.) Now, prove the following proposition:
   If n is an odd integer and 3 does not divide n, then $24 \mid (n^2 - 1)$.
10. (a) Prove the following proposition:
    For all $a, b, c \in \mathbb{Z}$, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.
    (b) Use mathematical induction to prove the following proposition:
    Let $n \in \mathbb{N}$ and let $a, b_1, b_2, \ldots, b_n \in \mathbb{Z}$. If $\gcd(a, b_i) = 1$ for all $i \in \mathbb{N}$ with $1 \leq i \leq n$, then $\gcd(a, b_1 b_2 \cdots b_n) = 1$.
11. Is the following proposition true or false? Justify your conclusion.
    Fro all integer a, b, and c, if $\gcd(a, b) = 1$ and $c \mid (a + b)$, then $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$.
12. Is the following proposition true or false? Justify your conclusion.
    If $n \in \mathbb{N}$, then $\gcd(5n + 2, 12n + 5) = 1$
13. Let $y \in \mathbb{N}$. Use the Fundamental Theorem of Arithmetic to prove that there exists an odd natural number x and a nonnegative integer k such that $y = 2^k x$.
14. (a) Determine five different primes that are congruent to 3 modulo 4.
    (b) Prove that there are infinitely many primes that are congruent to 3 modulo 4.
15. (a) Let $n \in \mathbb{N}$. Prove that 2 divides $[(n + 1)! + 2]$.
    (b) Let $n \in \mathbb{N}$ with $n \geq 2$. Prove that 3 divides $[(n + 1)! + 3]$.
    (c) Let $n \in \mathbb{N}$. Prove that for each $k \in \mathbb{N}$ with $2 \leq k \leq (n + 1)$, k divides $[(n + 1)! + k]$.
    (d) Use the result of Exercise (15c) to prove that for each $n \in \mathbb{N}$, there exist at least n consecutive composite natural numbers.
16. The Twin Prime Conjecture states that there are infinitely many twin primes, but it is not known if this conjecture is true or false. The answers to the following questions, however, can be determined.

    (a) How many pairs of primes p and q exist where $q - p = 3$? That is, how many pairs of primes are there that differ by 3? Prove that your answer is correct. (One such pair is 2 and 5.)
    (b) How many triplets of primes of the form p, $p + 2$, and $p + 4$ are there? That is, how many triplets of primes exist where each prime is 2 more than the preceding prime? Prove that your answer is correct. Notice that one such triplet is 3, 5, and 7.
    Hint: Try setting up cases using congruence modulo 3.
17. Prove the following proposition:
    Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$, if $\gcd(a, n) = 1$, then for every $b \in \mathbb{Z}$, there exists an $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$.
    Hint: One way is to start by writing 1 as a linear combination of a and n.
18. Prove the following proposition:

    For all natural numbers m and n, if m and n are twin primes other than the pair 3 and 5, then 36 divides $mn + 1$ and $mn + 1$ is a perfect square.

    Hint: Look at several examples of twin primes. What do you notice about the number that is between the two twin primes? Set up cases based on this observation.

Explorations and Activities

19. **Square Roots and Irrational Numbers.** In Chapter 3, we proved that some square roots (such as $\sqrt{2}$ and $\sqrt{3}$) are irrational numbers. In this activity, we will use the Fundamental Theorem of Arithmetic to prove that if a natural number is not a perfect square, then its square root is an irrational number.

(a) Let n be a natural number. Use the Fundamental Theorem of Arithmetic to explain why if n is composite, then there exist prime numbers $p_1, p_2, \ldots, p_r$ and natural numbers $\alpha_1, \alpha_2, \ldots, \alpha_r$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}. \tag{8.2.11}$$

Then,if we use $r = 1$ and $\alpha_1 = 1$ for a prime number, explain why we can write any natural number in the form given in equation (8.2.11).

(b) A natural number b is a perfect square if and only if there exists a natural number a such that $b = a^2$. Explain why 36, 400, and 15876 are perfect squares. Then determine the prime factorization of these perfect squares. What do you notice about these prime factorizations?

(c) Let n be a natural number written in the form given in equation (8.2.11) in part (a). Prove that n is a perfect square if and only if for each natural number k with $1 \leq k \leq r$, α_k is even.

(d) Prove that for all natural numbers n, if n is not a perfect square, then $\sqrt{n}$ is an irrational number. **Hint**: Use a proof by contradiction.

Answer

Add texts here. Do not delete this text first.

8.3: Linear Diophantine Equations

Preview Activity 8.3.1: Integer Solutions for Linear Equations in One Variable

1. Does the linear equation $6x = 42$ have a solutions that is an integer? Explain.
2. Does the linear equation $7x = -21$ have a solution that is an integer? Explain.
3. Does the linear equation $4x = 9$ have a solution that is an integer? Explain.
4. Does the linear equation $-3x = 20$ have a solution that is an integer? Explain.
5. Prove the following theorem:

Theorem 8.18

Let $a, b \in \mathbb{Z}$ with $a \neq 0$.

- If a divides b, then the equation $ax = b$ has exactly one solution that is an integer.
- If a does not divide b, then the equation $ax = b$ has no solution that is an integer.

Preview Activity 8.3.2: Linear Equations in Two Variables

1. Find integers x and y so that $2x + 6y = 25$ or explain why it is not possible to find such a pair of integers.
2. Find integers x and y so that $6x - 9y = 100$ or explain why it is not possible to find such a pair of integers.
3. Notice that $x = 2$ and $y = 1$ is a solution of the equation $3x + 5y = 11$, and that $x = 7$ and $y = -2$ is also a solution of the equation $3x + 5y = 11$.

(a) Find two pairs of integers x and y so that $x > 7$ and $3x + 5y = 11$. (Try to keep the integer values of x as small as possible.)
(b) Find two pairs of integers x and y so that $x < 2$ and $3x + 5y = 11$. (Try to keep the integer values of x as close to 2 as possible.)
(c) Determine formulas (one for x and one for y) that will generate pairs of integers x and y so that $3x + 5y = 11$.
Hint: The two formulas can be written in the form $x = 2 + km$ and $y = 1 + kn$, where k is an arbitrary integer and m and n are specific integers.

4. Notice that $x = 4$ and $y = 0$ is a solution of the equation $4x + 6y = 16$, and that $x = 7$ and $y = -2$ is a solution of the equation $4x + 6y = 16$. (a) Find two pairs of integers x and y so that $x > 7$ and $4x + 6y = 16$. (Try to keep the integer values of x as small as possible.)
   (b) Find two pairs of integers x and y so that $x < 4$ and $4x + 6y = 16$. (Try to keep the integer values of x as close to 4 as possible.)
   (c) Determine formulas (one for x and one for y) that will generate pairs of integers x and y so that $4x + 6y = 16$.
   Hint: The two formulas can be written in the form $x = 4 + km$ and $y = 0 + kn$, where k is an arbitrary integer and m and n are specific integers.

In the two preview activities, we were interested only in integer solutions for certain equations. In such instances, we give the equation a special name.

Definition: Diophantine equation

An equation whose solutions are required to be integers is called a *Diophantine equation.*

Diophantine equations are named in honor of the Greek mathematician Diophantus of Alexandria (circa 300 c.e.). Very little is known about Diophantus' life except that he probably lived in Alexandria in the early part of the fourth centuryc.e. and was probably the first to use letters for unknown quantities in arithmetic problems. His most famous work, Arithmetica, consists of approximately 130 problems and their solutions. Most of these problems involved solutions of equations in various numbers of variables. It is interesting to note that Diophantus did not restrict his solutions to the integers but recognized rational number solutions as well. Today, however, the solutions for a so-called Diophantine equation must be integers.

Definition: linear Diophantine equation in one variable

If a and b are integers with $a \neq 0$, then the equation $ax = b$ is a *linear Diophantine equation in one variable.*

Theorem 8.18 in Preview Activity $8.3.1$ provides us with results that allows us to determine which linear diophantine equations in one variable have solutions and which ones do not have a solution.

A linear Diophantine equation in two variables can be defined in a manner similar to the definition for a linear Diophantine equation in one variable.

Definition: linear Diophantine equation in two variables

Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. The Diophantine equation $ax + by = c$ is called a *linear Diophantine equation in two variables.*

The equations that were investigated in Preview Activity $8.3.2$ were linear Diophantine equations in two variables. The problem of determining all the solutions of a linear Diophantine equation has been completely solved. Before stating the general result, we will provide a few more examples.

Example 8.19: A Linear Diophantine Equation in Two Variables

The following example is similar to the examples studied in Preview Activity $8.3.2$.

We can use substitution to verify that $x = 2$ and $y = -1$ is a solution of the linear Diophantine equation

$$4x + 3y = 5.$$

The following table shows other solutions of this Diophantine equation.

x	y	x	y
2	−1	−1	3
5	−5	−4	7
8	−9	−7	11
11	−13	−10	15

It would be nice to determine the pattern that these solutions exhibit. If we consider the solution $x = 2$ and $y = -1$ to be the "starting point," then we can see that the other solutions are obtained by adding 3 to x and subtracting 4 from y in the previous solution. So we can write these solutions to the equation as

$$x = 2 + 3k \text{ and } y = -1 - 4k,$$

where k is an integer. We can use substitution and algebra to verify that these expressions for x and y give solutions of this equation as follows:

$$\begin{aligned} 4x + 3y &= 4(2 + 3k) + 3(-1 - 4k) \\ &= (8 + 12k) + (-3 - 12k) \\ &= 5. \end{aligned} \tag{8.3.1}$$

We should note that we have not yet proved that these solutions are all of the solutions of the Diophantine equation $4x + 3y = 5$. This will be done later.

If the general form for a linear Diophantine equation is $ax + by = c$, then for this example, $a = 4$ and $b = 3$. Notice that for this equation, we started with one solution and obtained other solutions by adding $b = 3$ to x and subtracting $a = 4$ from y in the previous solution. Also, notice that gcd(3, 4) = 1.

Progress Check 8.20: An Example of a Linear Diophantine Equation

1. Verify that the following table shows some solutions of the linear Diophantine equation $6x + 9y = 12$.

x	y	x	y
2	0	−1	2
5	−2	−4	4
8	−4	−7	6
11	−6	−10	8

2. Follow the pattern in this table to determine formulas for x and y that will generate integer solutions of the equation $6x + 9y = 12$. Verify that the formulas actually produce solutions for the equation $6x + 9y = 12$.

Answer

Add texts here. Do not delete this text first.

? Progress Check 8.21: Revisiting Preview Activity 8.3.2

Do the solutions for the linear Diophantine equations in Preview Activity 8.3.2 show the same type of pattern as the solutions for the linear Diophantine equations in Example 8.19 and Progress Check 8.20? Explain.

Answer

Add texts here. Do not delete this text first.

The solutions for the linear Diophantine equations in Preview Activity 8.3.2, Example 8.19, and Progress Check 8.20 provide examples for the second part of Theorem 8.22.

Theorem 8.22

Let a, b and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$.

1. If d does not divide c, then the linear Diophantine equation $ax + by = c$ has no solution.
2. If d divides c, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if (x_0, y_0) is a particular solution of this equation, then all the solutions of this equation can be written in the form

$$x = x_0 + \frac{b}{d}k \qquad \text{and} \qquad y = y_0 - \frac{a}{d}k, \tag{8.3.2}$$

for some integer k.

Proof

The proof of Part (1) is Exercise (1). For Part (2), we let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$. We also assume that $d \mid c$. Since $d = \gcd(a, b)$, Theorem 8.8 tells us that d is a linear combination of a and b. So there exist integers s and t such that

$$d = as + bt. \tag{8.3.3}$$

Since $d \mid c$, there exists an integer m such that $c = dm$. We can now multiply both sides of equation (8.3.3) by m and obtain

$$\begin{aligned} dm &= (as + bt)m \\ c &= a(sm) + b(tm). \end{aligned} \tag{8.3.4}$$

This means that $x = sm$, $y = tm$ is a solution of $ax + by = c$, and we have proved that the Diophantine equation $ax + by = c$ has at least one solution.

Now let $x = x_0, y = y_0$ be any particular solution of $ax + by = c$, let $k \in \mathbb{Z}$, and let

$$x = x_0 + \frac{b}{d}k \qquad y = y_0 - \frac{a}{d}k. \tag{8.3.5}$$

We now verify that for each $k \in \mathbb{Z}$, the equations in (8.3.4) produce a solution of $ax + by = c$.

$$\begin{aligned} ax + by &= a(x_0 + \frac{b}{d}k) + b(y_0 - \frac{a}{d}k) \\ &= ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k \\ &= ax_0 + by_0 \\ &= c. \end{aligned} \tag{8.3.6}$$

This proves that the Diophantine equation $ax + by = c$ has infinitely many solutions.

We now show that every solution of this equation can be written in the form described in (8.3.4). So suppose that x and y are integers such that $ax + by = c$. Then

$$(ax + by) - (ax_0 + by_0) = c - c = 0,$$

and this equation can be rewritten in the following form:

$$a(x - x_0) = b(y_0 - y). \tag{8.3.7}$$

Dividing both sides of this equation by d, we obtain

$$(\frac{a}{d})(x - x_0) = (\frac{b}{d})(y_0 - y).$$

This implies that

$\frac{a}{d}$ divides $(\frac{b}{d})(y_0 - y)$.

However, by Exercise (7) in Section 8.2, $textgcd(\frac{a}{d}, \frac{b}{d}) = 1$, and so by Theorem 8.12, we can conclude that $\frac{a}{d}$ divides $y_0 - y$. This means that there exists an integer k such that $y_0 - y = \frac{a}{d}k$, and solving for y gives

$$y = y_0 - \frac{a}{d}k.$$

Substituting this value for y in equation (8.3.5) and solving for x yields

$$x = x_0 + \frac{b}{d})k.$$

This proves that every solution of the Diophantine equation $ax + by = c$ can be written in the form prescribed in (8.3.4).

The proof of the following corollary to Theorem 8.22 is Exercise (2)

Theorem 8.3.1

Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$.If a and b are relatively prime, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if x_0, y_0 is a particular solution of this equation, then all the solutions of the equation are given by

$$x = x_0 + bk \;\; y = y_0 - ak$$

where $k \in \mathbb{Z}$

Progress Check 8.24 (Linear Diophantine Equations)

1. Use the Euclidean Algorithm to verify that gcd.63; 336/ D 21. What conclusion can be made about linear Diophantine equation $63x + 336y = 40$ using Theorem 8.22? If this Diophantine equation has solutions, write formulas that will generate the solutions.
2. Use the Euclidean Algorithm to verify that gcd.144; 225/ D 9. What conclusion can be made about linear Diophantine equation $144x + 225y = 27$ using Theorem 8.22? If this Diophantine equation has solutions, write formulas that will generate the solutions.

Answer

Add texts here. Do not delete this text first.

Exercises 8.3

1. Prove Part (1) of Theorem 8.22:

   Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$. If d does not divide c, then the linear Diophantine equation $ax + by = c$ has no solution.

2. Prove Corollary 8.23.

   Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a and b are relatively prime, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if (x_0, y_0) is a particular solution of this equation, then all the solutions of the equation are given by

   $$x = x_0 + bk \qquad y = y_0 - ak, \tag{8.3.8}$$

   where $k \in \mathbb{Z}$.

3. Determine all solutions of the following linear Diophantine equations.

   (a) $9x + 14y = 1$
   (b) $18x + 22y = 4$
   (c) $48x - 18y = 15$
   (d) $12x + 9y = 6$
   (e) $200x + 49y = 10$
   (f) $200x + 54y = 21$
   (g) $10x - 7y = 31$
   (h) $12x + 18y = 6$

4. A certain rare artifact is supposed to weigh exactly 25 grams. Suppose that you have an accurate balance scale and 500 each of 27 gram weights and 50 gram weights. Explain how to use Theorem 8.22 to devise a plan to check the weight of this artifact.

   Hint: Notice that gcd(50, 27) = 1. Start by writing 1 as a linear combination of 50 and 27.

5. On the night of a certain banquet, a caterer offered the choice of two dinners, a steak dinner for $25 and a vegetarian dinner for $16. At the end of the evening, the caterer presented the host with a bill (before tax and tips) for $1461. What is the minimum number of people who could have attended the banquet? What is the maximum number of people who could have attended the banquet?

6. The goal of this exercise is to determine all (integer) solutions of the linear Diophantine equation in three variables $12x_1 + 9x_2 + 16x_3 = 20$.

   (a) First, notice that gcd(12, 9) = 3. Determine formulas that will generate all solutions for the linear Diophantine equation $3y + 16x_3 = 20$.
   (b) Explain why the solutions (for x_1 and x_2) of the Diophantine equation $12x_1 + 9x_2 = 3y$ can be used to geneate solutions for $12x_1 + 9x_2 + 16x_3 = 20$.
   (c) Use the general value for y from Exercise (6a) to determine the solutions of $12x_1 + 9x_2 = 3y$
   (d) Use the results from Exercises (6a) and (6c) to determine formulas that will generate all solutions for the Diophantine equation $12x_1 + 9x_2 + 16x_3 = 20$.
   Note: These formulas will involve two arbitrary integer parameters. Substitute specific values for these integers and then check the resulting solution in the original equation. Repeat this at least three times.
   (e) Check the general solution for $12x_1 + 9x_2 + 16x_3 = 20$ from Exercise (6d).

7. Use the method suggested in Exercise (6) to determine formulas that will generate all solutions of the Diophantine equation $8x_1 + 4x_2 - 6x_3 = 6$. Check the general solution.

8. Explain why the Diophantine equation $24x_1 - 18x_2 + 60x_3 = 21$ has no solution.

9. The purpose of this exercise will be to prove that the nonlinear Diophantine equation $3x^2 - y^2 = -2$ has no solution.

   (a) Explain why if there is a solution of the Diophantine equation $3x^2 - y^2 = -2$, then that solution must also be a solution of the congruence $3x^2 - y^2 \equiv -2 \pmod 3$.
   (b) If there is a solution to the congruence $3x^2 - y^2 \equiv -2 \pmod 3$, explain why there then must be an integer y such that $y^2 \equiv 2 \pmod 3$.
   (c) Use a proof by contradiction to prove that the Diophantine equation $3x^2 - y^2 = -2$ has no solution.
10. Use the method suggested in Exercise (9) to prove that the Diophantine equation $7x^2 + 2 = y^3$ has no solution.

Explorations and Activities

11. **Linear Congruences in One Variable**. Let n be a natural number and let $a, b \in \mathbb{Z}$ with $a \neq 0$. A congruence of the form $ax \equiv b \pmod n$ is called a linear congruence in one variable. This is called a linear congruence since the variable x occurs to the first power.

    A solution of a linear congruence in one variable is defined similarly to the solution of an equation. A solution is an integer that makes the resulting congruence true when the integer is substituted for the variable x. For example,

    • The integer $x = 3$ is a solution for the congruence $2x \equiv 1 \pmod 5$ since $2 \cdot 3 \equiv 1 \pmod 5$ is a true congruence.
    • The integer $x = 7$ is a solution for the congruence $3x \equiv 1 \pmod 6$ since $3 \cdot 7 \equiv 1 \pmod 6$ is not a true congruence.

    (a) Verify that $x = 2$ and $x = 5$ are the only solutions the linear congruence $4x \equiv 2 \pmod 6$ with $0 \leq x < 6$.
    (b) Show that the linear congruence $4x \equiv 3 \pmod 6$ has no solutions with $0 \leq x < 6$.
    (c) Determine all solutions of the linear congruence $3x \equiv 7 \pmod 8$ with $0 \leq x < 8$.

    The following parts of this activity show that we can use the results of Theorem 8.22 to help find all solutions of the linear congruence $6x \equiv 4 \pmod 8$.

    (d) Verify that $x = 2$ and $x = 5$ are the only solutions the linear congruence $6x \equiv 4 \pmod 8$ with $0 \leq x < 8$.
    (e) Use the definition of “congruence” to rewrite the congruence $6x \equiv 4 \pmod 8$ in terms of "divides".
    (f) Use the definition of “divides” to rewrite the result in part (11e) in the form of an equation. (An existential quantifier must be used.)
    (g) Use the results of parts (11d) and (11f) to write an equation that will generate all the solutions of the linear congruence $6x \equiv 4 \pmod 8$.
    Hint: Use Theorem 8.22. This can be used to generate solutions for x and the variable introduced in part (11f). In this case, we are interested only in the solutions for x.

    Now let n be a natural number and let $a, c \in \mathbb{Z}$ with $a \neq 0$. A general linear congruence of the form $ax \equiv c \pmod n$ can be handled in the same way that we handled in $6x \equiv 4 \pmod 8$.

    (h) Use the definition of “congruence” to rewrite $ax \equiv c \pmod n$ in terms of “divides.”
    (i) Use the definition of “divides” to rewrite the result in part (11h) in the form of an equation. (An existential quantifier must be used.)
    (j) Let $d = \gcd(a, n)$. State and prove a theorem about the solutions of the linear congruence $ax \equiv c \pmod n$ in the case where d does not divide c.
    Hint: Use Theorem 8.22.
    (k) Let $d = \gcd(a, n)$. State and prove a theorem about the solutions of the linear congruence $ax \equiv c \pmod n$ in the case where d divides c.

Answer

Add texts here. Do not delete this text first.

8.S: Topics in Number Theory (Summary)

Important Definitions

- Greatest common divisor of two integers, page 414
- Linear combination of two integers, page 423
- Prime number, page 426
- Composite number, page 426
- Prime factorization, page 427
- Relatively prime integers, page 428
- Diophantine equation, page 441
- Linear Diophantine equation in two variables, page 441

Important Theorems and Results about Relations, Equivalence Relations, and Equivalence Classes

- **Theorem 8.3**. Let a and b be integers with $a \neq 0$ and $b > 0$. Then gcd(a, b) is the only natural number d such that

  (a) d divides a,
  (b) d divides b, and
  (c) if k is an integer that divides both a and b, then k divides d.
- **Theorem 8.8.** Let a and b be integers, not both 0. Then gcd(a, b) can be written as a linear combination of a and b. That is, there exist integers u and v such that $\gcd(a, b) = au + bv$.
- **Theorem 8.9.**
  1. The greatest common divisor, d, is a linear combination of a and b. That is, there exist integers m and n such that $d = am + bn$.
  2. The greatest common divisor, d, divides every linear combination of a and b. That is, for all $x, y \in \mathbb{Z}$, $d \mid (ax + by)$.
  3. The greatest common divisor, d, is the smallest positive number that is a linear combination of a and b.
- **Theorem 8.11**. Let a and b be nonzero integers, and let p be a prime number.
  1. If a and b are relatively prime, then there exist integers m and n such that $am + bn = 1$. That is, 1 can be written as linear combination of a and b.
  2. If $p \mid a$,then $\gcd(a, p) = p$.
  3. If p does not divide a, then $\gcd(a, p) = 1$.
- **Theorem 8.12** Let a, b, and c be integers. If a and b are relatively prime and $a \mid (bc)$, then $a \mid c$.
- **Corollary8.14**
  1. Let $a, b \in \mathbb{Z}$, and let p be a prime number. If $p \mid (ab)$, then $p \mid a$ or $p \mid b$.
  2. Let p be a prime number, let $n \in \mathbb{N}$, and let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 a_2 \cdots a_n)$, then there exists a natural number k with $1 \leq k \leq n$ such that $p \mid a_k$.
- **Theorem 8.15, The Fundamental Theorem of Arithmetic**
  1. Each natural number greater than 1 is either a prime number or is a product of prime numbers.
  2. Let $n \in \mathbb{N}$ with $n > 1$. Assume that

  $$n = p_1 p_2 \cdots p_r \text{ and that } n = q_1 q_2 \cdots q_s. \tag{8.S.1}$$

  where $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s$ are primes with $p_1 \leq p_2 \leq \cdots p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. Then $r = s$, and for each j from 1 to r, $p_j = q_j$.
- **Theorem 8.16.** There are infinitely many prime numbers.
- **Theorem 8.22.** Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$, and let $d = \gcd(a, b)$.

  1. If d does not divide c, then the linear Diophantine equation $ax + by = c$ has no solution.

  2. If d divides c, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if (x_0, y_0) is a particular solution of this equation, then all the solutions of the equation are given by

  $$x = x_0 + \frac{b}{d}k \quad \text{and} \quad y = y_0 - \frac{a}{d}k. \tag{8.S.2}$$

where $k \in \mathbb{Z}$.

- **Corollary8.23.** Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If a and b are relatively prime, then the linear Diophantine equation $ax + by = c$ has infinitely many solutions. In addition, if x_0, y_0 is a particular solution of this equation, then all the solutions of the equation are given by

$$x = x_0 + bk \quad \text{and} \quad y = y_0 - ak, \tag{8.S.3}$$

where $k \in \mathbb{Z}$.

CHAPTER OVERVIEW

9: Finite and Infinite Sets

9.1: Finite Sets

Preview Activity 9.1.1: Equivalent Sets, Part 1

1. Let A and B be sets and let f be a function from A to B. ($f : A \to B$). Carefully complete each of the following using appropriate quantifiers: (If necessary, review the material in Section 6.3.)
   a. The function f is an injection provided that...
   b. The function f is not an injection provided that...
   c. The function f is a surjection provided that...
   d. The function f is not a surjection provided that...
   e. The function f is a bijection provided that...

Definitions: equivalent Sets and one-to-one correspondence

Let A and B be sets.

- The set A is **equivalent** to the set B provided that there exists a bijection from the set A onto the set B. In this case, we write $A \approx B$.
- When $A \approx B$, we also say that the set A is in **one-to-one correspondence** with the set B and that the set A has the same **cardinality** as the set B.

Note: When A is not equivalent to B, we write $A \not\approx B$.

2. For each of the following, use the definition of equivalent sets to determine if the first set is equivalent to the second set.
   a. $A = \{1, 2, 3\}$ and $B = \{a, b, c\}$
   b. $C = \{1, 2\}$ and $B = \{a, b, c\}$
   c. $X = \{1, 2, 3, \ldots, 10\}$ and $Y = \{57, 58, 59, \ldots, 66\}$
3. Let D^+ be the set of all odd natural numbers. Prove that the function $f : \mathbb{N} \to D^+$ defined by $f(x) = 2x - 1$, for all $x \in \mathbb{N}$, is a bijection and hence that $N \approx D^+$.
4. Let $\mathbb{R}^+$ be the set of all positive real numbers. Prove that the function $g : \mathbb{R} \to \mathbb{R}^+$ defined by $g(x) = e^x$, for all $x \in \mathbb{R}$ is a bijection and hence, that $\mathbb{R} \approx \mathbb{R}^+$.

Preview Activity 9.1.2: Equivalent Sets, Part 2

1. Review Theorem 6.20 in Section 6.4, Theorem 6.26 in Section 6.5, and Exercise (9) in Section 6.5.
2. Prove each part of the following theorem.

Theorem 9.1.

Let A, B, and C be sets.

a. For each set A, $A \approx A$.
b. For all sets A and B, if $A \approx B$, then $B \approx A$.
c. For all sets A, B and C, if $A \approx B$ and $B \approx C$, then $A \approx C$.

Equivalent Sets

In Preview Activity 9.1.1, we introduced the concept of equivalent sets. The motivation for this definition was to have a formal method for determining whether or not two sets "have the same number of elements." This idea was described in terms of a one-to-one correspondence (a bijection) from one set onto the other set. This idea may seem simple for finite sets, but as we will see, this idea has surprising consequences when we deal with infinite sets. (We will soon provide precise definitions for finite and infinite sets.)

Technical Note

The three properties we proved in Theorem 9.1 in Preview Activity 9.1.2 are very similar to the concepts of reflexive, symmetric, and transitive relations. However, we do not consider equivalence of sets to be an equivalence relation on a set U since an equivalence relation requires an underlying (universal) set U. In this case, our elements would be the sets A, B, and C, and these would then have to subsets of some universal set W (elements of the power set of W). For equivalence of sets, we are not requiring that the sets A, B, and C be subsets of the same universal set. So we do not use the term relation in regards to the equivalence of sets. However, if A and B are sets and $A \approx B$, then we often say that A and B are equivalent sets.

Progress Check 9.2: Examples of Equivalent Sets

We will use the definition of equivalent sets from in Preview Activity 9.1.1 in all parts of this progress check. It is no longer sufficient to say that two sets are equivalent by simply saying that the two sets have the same number of elements.

1. Let $A = \{1, 2, 3, \ldots, 99, 100\}$and let $B = \{351, 352, 353, \ldots, 449, 450\}$Define $f : A \to B$ by $f(x) = x + 350$, for each x in A. Prove that f is a bijection from the set A to the set B and hence, $A \approx B$.
2. Let E be the set of all even integers and let D be the set of all odd integers.
   Prove that $E \approx D$ by proving that $F : E \to D$, where $F(x) = x + 1$, for all $x \in E$, is a bijection.
3. Let (0, 1) be the open interval of real numbers between 0 and 1. Similarly, if $b \in \mathbb{R}$ with $b > 0$, let $0, b$ be the open interval of real numbers between 0 and b.
   Prove that the function $f : (0, 1) \to (0, b)$ by $f(x) = bx$, for all $x \in (0, 1)$, is a bijection and hence $(0, 1) \approx (0, b)$.

Answer

Add texts here. Do not delete this text first.

In Part (3) of Progress Check 9.2, notice that if $b > 1$, then (0, 1) is a proper subset of (0, b) and $(0, 1) \approx (0, b)$. Also, in Part (3) of Preview Activity 9.1.1, we proved that the set D of all odd natural numbers is equivalent to $\mathbb{N}$, and we know that D is a proper subset of $\mathbb{N}$.

These results may seem a bit strange, but they are logical consequences of the definition of equivalent sets. Although we have not defined the terms yet, we will see that one thing that will distinguish an infinite set from a finite set is that an infinite set can be equivalent to one of its proper subsets, whereas a finite set cannot be equivalent to one of its proper subsets.

Finite Sets

In Section 5.1, we defined the **cardinality** of a finite set A, denoted by card(A), to be the number of elements in the set A. Now that we know about functions and bijections, we can define this concept more formally and more rigorously. First, for each $k \in \mathbb{N}$, we define $\mathbb{N}_k$ to be the set of all natural numbers between 1 and k, inclusive. That is,

$$\mathbb{N}_k = \{1, 2, \ldots, k\}.$$

We will use the concept of **equivalent sets** introduced in Preview Activity 9.1.1 to define a finite set.

Definition: finite and infinite sets

- A set A is a **finite set** provided that $A = \emptyset$ or there exists a natural number k such that $A \approx \mathbb{N}_k$.
- A set is an **infinite set** provided that it is not a finite set.
- If $A \approx \mathbb{N}_k$, we say that the set A has **cardinality k** (or **cardinal number k**), and we write card(A) $= k$.

In addition, we say that the empty set has **cardinality 0** (or **cardinal number 0**), and we write $\text{card}(\emptyset) = 0$.

Notice that by this definition, the empty set is a finite set. In addition, for each $k \in \mathbb{N}$, the identity function on $\mathbb{N}_k$ is a bijection and hence, by definition, the set $\mathbb{N}_k$ is a finite set with cardinality k.

Theorem 9.3

Any set equivalent to a finite nonempty set A is a finite set and has the same cardinality as A.

Proof

Suppose that A is a finite nonempty set, B is a set, and $A \approx B$. Since A is a finite set, there exists a $k \in \mathbb{N}$ such that $A \approx \mathbb{N}_k$. We also have assumed that $A \approx B$ and so by part (b) of Theorem 9.1 (in Preview Activity 9.1.2), we can conclude that $B \approx A$. Since $A \approx \mathbb{N}_k$, we can use part (c) of Theorem 9.1 to conclude that $B \approx \mathbb{N}_k$. Thus, B is finite and has the same cardinality as A.

It may seem that we have done a lot of work to prove an "obvious" result in Theorem 9.3. The same may be true of the remaining results in this section, which give further results about finite sets. One of the goals is to make sure that the concept of cardinality for a finite set corresponds to our intuitive notion of the number of elements in the set. Another important goal is to lay the groundwork for a more rigorous and mathematical treatment of infinite sets than we have encountered before. Along the way, we will see the mathematical distinction between finite and infinite sets.

The following two lemmas will be used to prove the theorem that states that every subset of a finite set is finite.

Lemma 9.4

If A is a finite set and $x \notin A$, then $A \cup \{x\}$ is a finite set and $\text{card}(A \cup \{x\}) = \text{card}(A) + 1$.

Proof

Let A is a finite set and assume that $\text{card}(A) = k$, where $k = 0$ or $k \in \mathbb{N}$. Assume $x \notin A$.

If $A = \emptyset$, then $\text{card}(A) = 0$ and $A \cup \{x\} = \{x\}$, which is equivalent to $\mathbb{N}_1$. Thus, $A \cup \{x\}$ is a finite set with cardinality 1, which equals card(A) + 1.

If $A \neq \emptyset$, then $A \approx \mathbb{N}_k$, for some $k \in \mathbb{N}$. This means that $\text{card}(A) = k$, and there exists a bijection $f : A \to \mathbb{N}_k$. We will now use this bijection to define a function $g : A \cup \{x\} \to \mathbb{N}_{k+1}$ and then prove that the function g is a bijection. We define $g : A \cup \{x\} \to \mathbb{N}_{k+1}$ as follows: For each $t \in A \cup \{x\}$,

$$g(t) = \begin{cases} f(t) & \text{if } t \in A \\ k+1 & \text{if } t = x. \end{cases}$$

To prove that g is an injection, we let $x_1, x_2 \in A \cup \{x\}$ and assume $x_1 \neq x_2$.

- If $x_1, x_2 \in A$, then since f is a bijection, $f(x_1) \neq f(x_2)$, and this implies that $g(x_1) \neq g(x_2)$.
- If $x_1 = x$, then since $x_2 \neq x_1$, we conclude that $x_2 \neq x$ and hence $x_2 \in A$. So $g(x_1) = k+1$, and since $f(x_2) \in \mathbb{N}_k$ and $g(x_2) = f(x_2)$, we can conclude that $g(x_1) \neq g(x_2)$.

This proves that the function g is an injection. The proof that g is a surjection is Exercise (1). Since g is a bijection, we conclude that $A \cup \{x\} \approx \mathbb{N}_{k+1}$, and

$$\text{card}(A \cup \{x\}) = k + 1 .$$

Since $\text{card}(A) = k$, we have proved that $\text{card}(A \cup \{x\}) = \text{card}(A) + 1$.

Lemma 9.5

For each natural number m, if $A \subseteq \mathbb{N}_m$, then A is a finite set and $\text{card}(A) \leq m$.

Proof

We will use a proof using induction on m. For each $m \in \mathbb{N}$, let $P(m)$ be, "If $A \subseteq \mathbb{N}_m$, then A is finite and $\text{card}(A) \leq m$".

We first prove that $P(1)$ is true. If $A \subseteq \mathbb{N}_1$, then $A = \emptyset$ or $A = \{1\}$, both of which are finite and have cardinality less than or equal to the cardinality of $\mathbb{N}_1$. This proves that $P(1)$ is true.

For the inductive step, let $k \in \mathbb{N}$ and assume that $P(k)$ is true. That is, assume that if $B \subseteq \mathbb{N}_k$, then B is a finite set and $\text{card}(B) \leq k$. We need to prove that $P(k+1)$ is true.

So assume that A is a subset of $\mathbb{N}_{k+1}$. Then $A - \{k+1\}$ is a subset of $\mathbb{N}_k$. Since $P(k)$ is true, $A - \{k+1\}$ is a finite set and

$$\text{card}(A - \{k+1\}) \leq k \ .$$

There are two cases to consider: Either $k+1 \in A$ or $k+1 \notin A$.

If $k+1 \notin A$, then $A = A - \{k+1\}$. Hence, A is finite and

$$\text{card}(A) \leq k < k+1 \ .$$

If $k+1 \in A$, then $A = (A - \{k+1\}) \cup \{k+1\}$. Hence, by Lemma 9.4, A is a finite set and

$$\text{card}(A) = \text{card}(A - \{k+1\} \quad + 1\backslash).$$

Since $\text{card}(A - \{k+1\}) \leq k$, we can conclude that $\text{card}(A) \leq k+1$.

This means that we have proved the inductive step. Hence, by mathematical induction, for each $m \in \mathbb{N}$, if $A \subset \mathbb{N}_m$, then A is finite and $\text{card}(A) \leq m$.

The preceding two lemmas were proved to aid in the proof of the following theorem.

Theorem 9.6.

If S is a finite set and A is a subset of S, then A is a finite set and $\text{card}(A) \leq \text{card}(S)$.

Proof

Let S be a finite set and assume that A is a subset of S. If $A = \emptyset$, then A is a finite set and $\text{card}(A) \leq \text{card}(S)$. So we assume that $A \neq \emptyset$.

Since S is finite, there exists a bijection $f : S \to \mathbb{N}_k$ for some $k \in \mathbb{N}$. In this case, $\text{card}(S) = k$. We need to show that A is equivalent to a finite set. To do this, we define $g : A \to f(A)$ by

$$g(x) = f(x) \text{ for each } x \in A.$$

Since f is an injection, we conclude that g is an injection. Now let $y \in f(A)$. Then there exists an $a \in A$ such that $f(a) = y$. But by the definition of g, this means that $g(a) = y$, and hence g is a surjection. This proves that g is a bijection.

Hence, we have proved that $A \approx f(A)$. Since $f(A)$ is a subset of $\mathbb{N}_k$, we use Lemma 9.5 to conclude that $f(A)$ is finite and $\text{card}(f(A)) \leq k$. In addition, by Theorem 9.3, A is a finite set and $\text{card}(A) = \text{card}(f(A))$. This proves that A is a finite set and $\text{card}(A) \leq \text{card}(S)$.

Lemma 9.4 implies that adding one element to a finite set increases its cardinality by 1. It is also true that removing one element from a finite nonempty set reduces the cardinality by 1. The proof of Corollary 9.7 is Exercise (4).

corollary 9.7

If A is a finite set and $x \in A$, then $A - \{x\}$ is a finite set and $\text{card}(A - \{x\}) = \text{card}(A) - 1$

The next corollary will be used in the next section to provide a mathematical distinction between finite and infinite sets.

Corollary 9.8

A finite set is not equivalent to any of its proper subsets.

Proof

Let B be a finite set and assume that A is a proper subset of B. Since A is a proper subset of B, there exists an element x in $B - A$. This means that A is a subset of $B - \{x\}$. Hence, by Theorem 9.6,

$$\text{card}(A) \leq \text{card}(B - \{x\}).$$

Also, by Corollary 9.7

$$\text{card}(B - \{x\}) = \text{card}(B) - 1.$$

Hence, we may conclude that $\text{card}(A) \leq \text{card}(B) - 1$ and that

$$\text{card}(A) < \text{card}(B).$$

Theorem 9.3 implies that $B \not\approx A$. This proves that a finite set is not equivalent to any of its proper subsets.

The Pigeonhole Principle

The last property of finite sets that we will consider in this section is often called the **Pigeonhole Principle**. The "pigeonhole" version of this property says, "If m pigeons go into r pigeonholes and $m > r$, then at least one pigeonhole has more than one pigeon."

In this situation, we can think of the set of pigeons as being equivalent to a set P with cardinality m and the set of pigeonholes as being equivalent to a set H with cardinality r. We can then define a function $f : P \to H$ that maps each pigeon to its pigeonhole. The Pigeonhole Principle states that this function is not an injection. (It is not one-to-one since there are at least two pigeons "mapped" to the same pigeonhole.)

Theorem 9.9: The Pigeonhole Principle

Let A and B be finite sets. If $\text{card}(A) > \text{card}(B)$, then any function $f : A \to B$ is not an injection.

Proof

Let A and B be finite sets. We will prove the contrapositive o the theorem, which is, if there exists a function $f : A \to B$ that is an injection, then $\text{card}(A) \leq \text{card}(B)$.

So assume that $f : A \to B$ is an injection. As in Theorem 9.6, we define a function $g : A \to f(A)$ by

$$g(x) = f(x) \text{ for each } x \in A.$$

As we saw in Theorem 9.6, the function g is a bijection. But then $A \approx f(A)$ and $f(A) \subseteq B$. Hence,

$\text{card}(A) = \text{card}(f(x))$ and $\text{card} f((A)) \leq \text{card}(B)$.

Hence, $\text{card} f((A)) \leq \text{card}(B)$, and this proves the contrapositive. Hence, if $\text{card}(A) > \text{card}(B)$, then any function $f : A \to B$ is not an injection.

The Pigeonhole Principle has many applications in the branch of mathematics called "combinatorics." Some of these will be explored in the exercises.

Exercises 9.1

1. Prove that the function $g : A \cup \{x\} \to \mathbb{N}_{k+1}$ in Lemma 9.4 is a surjection.
2. Let A be a subset of some universal set U. Prove that if $x \in U$, then $A \times \{x\} \approx A$.
3. Let E^+ be the set of all even natural numbers. Prove that $\mathbb{N} \approx E^+$.
4. Prove Corollary 9.7.
   If A is a finite set and $x \in A$, then $A - \{x\}$ is a finite set and $\text{card}(A - \{x\}) = \text{card}(A) - 1$
   Hint: One approch is to use the fact that $A = (A - \{x\}) \cup \{x\}$.
5. Let A and B be sets. Prove that

   (a) If A is a finite set, then $A \cap B$ is a finite set.
   (b) If $A \cup B$ is a finite set, then A and B are finite set.
   (c) If $A \cap B$ is an infinite set, then A is an infinite set.
   (d) If A is an infinite set or B is an infinite set, then $A \cup B$ is an infinite set.

6. There are over 7 million people living in New York City. It is also known that the maximum number of hairs on a human head is less than 200,000. Use the Pigeonhole Principle to prove that there are at least two people in the city of New York with the same number of hairs on their heads.
7. Prove the following proposiitons:

   (a) If A, B, C, and D are sets with $A \approx B$ and $C \approx D$, then $A \times C \approx B \times D$.
   (b) If A, B, C, and D are sets with $A \approx B$ and $C \approx D$ and if A and C are disjoint and B and D are disjoint, then $A \cup C \approx B \cup D$.

   Hint: Since $A \approx B$ and $C \approx D$, there exist bijections $f : A \to B$ and $g : C \to D$. To prove that $A \times C \approx B \times D$, prove that $h : A \times C \to B \times D$ is a bijection, where $h(a, c) = (f(a), g(c))$, for all $(a, c) \in A \times C$.
   If $A \cap C = \emptyset$ and $B \cap D = \emptyset$, then to prove that $A \cup C \approx B \cup D$, prove that the following function is a bijection: $k : A \cup C \to B \cup D$, where

$$k(x) = \begin{cases} f(x) & \text{if } t \in A \\ g(x) & \text{if } x \in C. \end{cases} \tag{9.1.1}$$

8. Let $A = \{a, b, c\}$.

   (a) Construct a function $f : \mathbb{N}_5 \to A$ such that f is a surjection.
   (b) Use the function f to construct a function $g : A \to \mathbb{N}_5$ so that $f \circ g = I_A$, where I_A is the identity function on the set A. Is the function g an injection? Explain.
9. This exercise is a generalization of Exercise (8). Let m be a natural number, let A be a set, and assume that $f : \mathbb{N}_m \to A$ is a surjection. Define $g : A \to \mathbb{N}_m$ asfollows:
   For each $x \in A$, $g(x) = j$, where j is the least natural number in $f^{-1}(\{x\})$.
   Prove that $f \circ g = I_A$, where I_A is the identity function on the set A and prove that g is an injection.
10. Let B be a finite, nonempty set and assume that $f : B \to A$ is a surjection. Prove that there exists a function $h : A \to B$ such that $f \circ h = I_A$ and h is an injection.
    Hint: Since B is finite, there exists a natural number m such that $\mathbb{N}_m \approx B$. This means there exists a bijection $k : \mathbb{N}_m \to B$. Now let $h = k \circ g$, where g is the function constructed in Exercise (9).

Explorations and Activities

11. **Using the Pigeonhole Principle.** For this activity, we will consider subsets of $\mathbb{N}_30$ that contain eight elements.

    (a) One such set is $A = \{3, 5, 11, 17, 21, 24, 26, 29\}$Notice that

$$\begin{aligned} \{3, 21, 24, 26\} \subseteq A \quad &\text{and} \quad 3 + 21 + 24 + 26 = 74 \\ \{3, 5, 11, 26, 29\} \subseteq A \quad &\text{and} \quad 3 + 5 + 11 + 26 + 29 = 74 \end{aligned} \tag{9.1.2}$$

    Use this information to find two disjoint subsets of A whose elements have the same sum.
    (b) Let $B = \{3, 5, 9, 12, 15, 18, 21, 24\}$Find two disjoint subsets of B whose elements have the same sum. Note: By convention, if $T = \{a\}$, where $a \in \mathbb{N}$, then the sum of the elements in T is equal to a.
    (c) Now let C be any subset of $\mathbb{N}_{30}$ that contains eight elements.
    i. How many subsets does C have?
    ii. The sum of the elements of the empty set is 0. What is the maximum sum for any subset of $\mathbb{N}_{30}$ that contains eight elements.? Let M be this maximum sum.
    iii. Now define a function $f : \mathcal{P}(C) \to \mathbb{N}_M$ so that for each $X \in \mathcal{P}$, $f(X)$ is equal to the sum of the elements in X.
    Use the Pigeonhole Principle to prove that there exist two subsets of C whose elements have the same sum.
    (d) If the two subsets in part (11(c)iii) are not disjoint, use the idea presented in part (11a) to prove that there exist two disjoint subsets of C whose elements have the same sum.
    (e) Let S be a subset of $\mathbb{N}_{99}$ that contains 10 elements. Use the Pigeonhole Principle to prove that there exist two disjoint subsets of S whose elements have the same sum.

Answer

Add texts here. Do not delete this text first.

9.2: Countable Sets

Preview Activity 9.2.1: Introduction to Infinite Sets

In Section 9.1, we defined a **finite set** to be the empty set or a set A such that $A \approx \mathbb{N}_k$ for some natural number k. We also defined an **infinite set** to be a set that is not finite, but the question now is, "How do we know if a set is infinite?" One way to determine if a set is an infinite set is to use Corollary 9.8, which states that a finite set is not equivalent to any of its subsets. We can write this as a conditional statement as follows:

> If A is a finite set, then A is not equivalent to any of its proper subsets. or more formally as
>
> For each set A, if A is a finite set, then for each proper subset B of A, $A \not\approx B$.

1. Write the contrapositive of the preceding conditional statement. Then explain how this statement can be used to determine if a set is infinite.
2. Let DC be the set of all odd natural numbers. In Preview Activity 9.2.1 from Section 9.1, we proved that $\mathbb{N} \approx D^+$.
   (a) Use this to explain carefully why $\mathbb{N}$ is an infinite set.
   (b) Is D^+ a finite set or an infinite set? Explain carefully how you know.
3. Let b be a positive real number. Let (0, 1) and $(0, b)$ be the open intervals from 0 to 1 and 0 to b, respectively. In Part (3) of Progress Check 9.2 (on page 454), we proved that $(0, 1) \approx (0, b)$.
   (a) Use a value for b where $0 < b < 1$ to explain why (0, 1) is an infinite set.
   (b) Use a value for b where $b > 1$ to explain why $(0, b)$ is an infinite set.

Preview Activity 9.2.2: A Function from $\mathbb{N}$ to $\mathbb{Z}$

In this preview activity, we will define and explore a function $f : \mathbb{N} \to \mathbb{Z}$. We will start by defining $f(n)$ for the first few natural numbers n.

$$\begin{array}{ll} f(1) = 0 & \\ f(2) = 1 & f(3) = -1 \\ f(4) = 2 & f(5) = -2 \\ f(6) = 3 & f(7) = -3 \end{array}$$

Notice that if we list the outputs of f in the order $f(1)$, $f(2)$, $f(3)$, ..., we create the following list of integers: 0, 1, -1, 2, -2, 3, -3, ... We can also illustrate the outputs of this function with the following diagram:

$$\begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots \\ 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & -4 & 5 & \cdots \end{array}$$

Figure 9.1: A Function from $\mathbb{N}$ to $\mathbb{Z}$

1. If the pattern suggested by the function values we have defined continues, what are $f(11)$ and $f(12)$? What is $f(n)$ for n from 13 to 16?
2. If the pattern of outputs continues, does the function f appear to be an injection? Does f appear to be a surjection? (Formal proofs are not required.)

We will now attempt to determine a formula for $f(n)$, where $n \in \mathbb{N}$. We will actually determine two formulas: one for when n is even and one for when n is odd.

3. Look at the pattern of the values of $f(n)$ when n is even. What appears to be a formula for $f(n)$ when n is even?
4. Look at the pattern of the values of $f(n)$ when n is odd. What appears to be a formula for $f(n)$ when n is odd?
5. Use the work in Part (3) and Part (4) to complete the following: Define $f : \mathbb{N} \to \mathbb{Z}$, where

$$f(n) = \begin{cases} ?? & \text{if } n \text{ is even} \\ ?? & \text{if } n \text{ is odd.} \end{cases} \tag{9.2.1}$$

6. Use the formula in Part (5) to (a) Calculate $f(1)$ through $f(10)$. Are these results consistent with the pattern exhibited at the beginning of this preview activity?
   (b) Calculate $f(1000)$ and $f(1001)$.
   (c) Determine the value of n so that $f(n) = 1000$.

In this section, we will describe several infinite sets and define the cardinal number for so-called countable sets. Most of our examples will be subsets of some of our standard numbers systems such as $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$.

Infinite Sets

In Preview Activity $9.2.1$, we saw how to use Corollary 9.8 to prove that a set is infinite. This corollary implies that if A is a finite set, then A is not equivalent to any of its proper subsets. By writing the contrapositive of this conditional statement, we can restate Corollary 9.8 in the following form:

? Corollary 9.8

If a set A is equivalent to one of its proper subsets, then A is infinite.

In Preview Activity $9.2.1$, we used Corollary 9.8 to prove that

- The set of natural numbers, $\mathbb{N}$, is an infinite set.
- The open interval (0, 1) is an infinite set.

Although Corollary 9.8 provides one way to prove that a set is infinite, it is sometimes more convenient to use a proof by contradiction to prove that a set is infinite. The idea is to use results from Section 9.1 about finite sets to help obtain a contradiction. This is illustrated in the next theorem.

Theorem 9.10.

Let A and B be sets.

1. If A is infinite and $A \approx B$, then B is infinite.
2. If A is infinite and $A \subseteq B$, then B is infinite.

Proof

We will prove part (1). The proof of part (2) is exercise (3) on page 473.

To prove part (1), we use a proof by contradiction and assume that A is an infinite set, $A \approx B$, and B is not infinite. That is, B is a finite set. Since $A \approx B$ and B is finite, Theorem 9.3 on page 455 implies that A is a finite set. This is a contradiction to the assumption that A is infinite. We have therefore proved that if A is infinite and $A \approx B$, then B is infinite.

? Progress Check 9.11 (Examples of Infinite Sets)

1. In Preview Activity $9.2.1$, we used Corollary 9.8 to prove that $\mathbb{N}$ is an infinite set. Now use this and Theorem 9.10 to explain why our standard number systems ($\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$) are infinite sets. Also, explain why the set of all positive rational numbers, $\mathbb{Q}^+$, and the set of all positive real numbers, $\mathbb{R}^+$, are infinite sets.
2. Let D^+ be the set of all odd natural numbers. In Part (2) of Preview Activity $9.2.1$, we proved that $D^+ \approx \mathbb{N}$. Use Theorem 9.10 to explain why D^+ is an infinite set.
3. Prove that the set E^+ of all even natural numbers is an infinite set.

Answer

Add texts here. Do not delete this text first.

Countably Infinite Sets

In Section 9.1, we used the set $\mathbb{N}_k$ as the standard set with cardinality k in the sense that a set is finite if and only if it is equivalent to $\mathbb{N}_k$. In a similar manner, we will use some infinite sets as standard sets for certain infinite cardinal numbers. The first set we will use is $\mathbb{N}$.

We will formally define what it means to say the elements of a set can be "counted" using the natural numbers. The elements of a finite set can be "counted" by defining a bijection (one-to-one correspondence) between the set and $\mathbb{N}_k$ for some natural number k. We will be able to "count" the elements of an infinite set if we can define a one-to-one correspondence between the set and $\mathbb{N}$.

Definition

The **cardinality of** $\mathbb{N}$ is denoted by $\aleph_0$. The symbol $\aleph$ is the first letter of the Hebrew alphabet, **aleph**. The subscript 0 is often read as "naught" (or sometimes as "zero" or "null"). So we write

$$\text{card}(\mathbb{N}) = \aleph_0$$

and say that the cardinality of $\mathbb{N}$ is "aleph naught."

Definition

A set A is **countably infinite** provided that $A \approx \mathbb{N}$. In this case, we write

$$\text{card}(A) = \aleph_0$$

A set that is countably infinite is sometimes called a **denumerable** set. A set is **countable** provided that it is finite or countably infinite. An infinite set that is not countably infinite is called an **uncountable set.**

progress check 9.12. (examples of countably infinite sets)

1. In Preview Activity 9.2.1 from Section 9.1, we proved that $\mathbb{N} \approx D^+$, where D^+ is the set of all odd natural numbers. Explain why $\text{card}(D^+) = \aleph_0$.
2. Use a result from Progress Check 9.11 to explain why $\text{card}(E^+) = \aleph_0$.
3. At this point, if we wish to prove a set S is countably infinite, we must find a bijection between the set S and some set that is known to be countably infinite.

   Let S be the set of all natural numbers that are perfect squares. Define a function

   $$f : S \to \mathbb{N} \tag{9.2.2}$$

   that can be used to prove that $S \approx \mathbb{N}$ and, hence, that $\text{card}(S) = \aleph_0$.

Answer

Add texts here. Do not delete this text first.

The fact that the set of integers is a countably infinite set is important enough to be called a theorem. The function we will use to establish that $\mathbb{N} \approx \mathbb{Z}$ was explored in Preview Activity 9.2.2.

Theorem 9.13

The set $\mathbb{Z}$ of integers is countably infinite, and so $\text{card}(\mathbb{Z}) = \aleph_0$

Proof

To prove that $\mathbb{N} \approx \mathbb{Z}$, we will use the following funciton: $f : \mathbb{N} \to \mathbb{Z}$, where

$$f(n) = \begin{cases} \dfrac{n}{2} & \text{if } n \text{ is even} \\ \dfrac{1-n}{2} & \text{if } n \text{ is odd.} \end{cases}$$

From our work in Preview Activity 9.2.2 it appears that if n is an even natural number, then $f(n) > 0$, and if n is an odd natural number, then $f(n) \leq 0$. So it seems reasonable to use cases to prove that f is a surjection and that f is an injection. To prove that f is a surjection, we let $y \in \mathbb{Z}$.

- If $y > 0$, then $2y \in \mathbb{N}$, and

$$f(2y) = \frac{2y}{2} = y. \tag{9.2.3}$$

- If $y \leq 0$, then $-2y \geq 0$ and $1 - 2y$ is an odd natural number. Hence,

$$f(1-2y) = \frac{1-(1-2y)}{2} = \frac{2y}{2} = y. \tag{9.2.4}$$

These two cases prove that if $y \in \mathbb{Z}$, then there exists an $n \in \mathbb{N}$ such that $f(n) = y$. Hence, f is a surjection.

To prove that f is an injection, we let $m, n \in \mathbb{N}$ and assume that $f(m) = f(n)$. First note that if one of m and n is odd and the other is even, then one of $f(m)$ and $f(n)$ is positive and the other is less than or equal to 0. So if $f(m) = f(n)$, then both m and n must be even or both m and n must be odd.

- If both m and n are even, then

$$f(m) = f(n) \text{ implies that } \frac{m}{2} = \frac{n}{2} \tag{9.2.5}$$

  and hence that $m = n$.
- If both m and n are odd, then

$$f(m) = f(n) \text{ implies that } \frac{1-m}{2} = \frac{1-n}{2}. \tag{9.2.6}$$

  From this, we conclude that $1 - m = 1 - n$ and hence that $m = n$. This proves that if $f(m) = f(n)$, then $m = n$ and hence that f is an injection.

Since f is both a surjection and an injection, we see that f is a bijection and, therefore, $\mathbb{N} \approx \mathbb{Z}$. Hence, $\mathbb{Z}$ is countably infinite and $\text{card}(\mathbb{Z}) = \aleph_0$.

The result in Theorem 9.13 can seem a bit surprising. It exhibits one of the distinctions between finite and infinite sets. If we add elements to a finite set, we will increase its size in the sense that the new set will have a greater cardinality than the old set. However, with infinite sets, we can add elements and the new set may still have the same cardinality as the original set. For example, there is a one-to-one correspondence between the elements of the sets $\mathbb{N}$ and $\mathbb{Z}$. We say that these sets have the same cardinality.

Following is a summary of some of the main examples dealing with the cardinality of sets that we have explored.

- The sets $\mathbb{N}_k$, where $k \in \mathbb{N}$, are examples of sets that are countable and finite.
- The sets $\mathbb{N}$, $\mathbb{Z}$, the set of all odd natural numbers, and the set of all even natural numbers are examples of sets that are countable and countably infinite.
- We have not yet proved that any set is uncountable.

The Set of Positive Rational Numbers

If we expect to find an uncountable set in our usual number systems, the rational numbers might be the place to start looking. One of the main differences between the set of rational numbers and the integers is that given any integer m, there is a next integer, namely $m+1$. This is not true for the set of rational numbers. We know that $\mathbb{Q}$ is closed under division (by nonzero rational numbers) and we will see that this property implies that given any two rational numbers, we can also find a rational number between them. In fact, between any two rational numbers, we can find infinitely many rational numbers. It is this property that may lead us to believe that there are “more” rational numbers than there are integers.

The basic idea will be to "go half way" between two rational numbers. For example, if we use $a = \frac{1}{3}$ and $b = \frac{1}{2}$, we can use

$$\frac{a+b}{2} = \frac{1}{2}(\frac{1}{3} + \frac{1}{2}) = \frac{5}{12}$$

as a rational number between a and b. We can then repeat this process to find a rational number between $\frac{5}{12}$ and $\frac{1}{2}$.

So we will now let a and b be any two rational numbers with $a < b$ and let $c_1 = \frac{a+b}{2}$. We then see that

$$\begin{aligned} c_1 - a &= \frac{a+b}{2} - a \\ &= \frac{a+b}{2} - \frac{2a}{2} \\ &= \frac{b-a}{2} \end{aligned} \qquad \begin{aligned} b - c_1 &= b - \frac{a+b}{2} \\ &= \frac{2b}{2} - \frac{a+b}{2} \\ &= \frac{b-a}{2} \end{aligned}$$

Since $b > a$, we see that $b - a > 0$ and so the previous equations show that $c_1 - a > 0$ and $b - c_1 > 0$. We can then conclude that $a < c_1 < b$.

We can now repeat this process by using $c_2 = \frac{c_1 + b}{2}$ and proving that $c_1 < c_2 < b$, In fact, for each natural number, we can define

$$c_{k+1} = \frac{c_k + b}{2}$$

and obtain the result that $a < c_1 < c_2 < \cdots < c_n < \cdots < b$ and this proves that the set $\{c_k \mid k \in \mathbb{N}$ is a countably infinite set where each element is a rational number between a and b. (A formal proof can be completed using mathematical induction. See Exercise ().

This result is true no matter how close together a and b are. For example, we can now conclude that there are infinitely many rational numbers between 0 and $\frac{1}{10000}$ This might suggest that the set $\mathbb{Q}$ of rational numbers is uncountable. Surprisingly, this is not the case. We start with a proof that the set of positive rational numbers is countable.

Theorem 9.14

The set of positive rational numbers is countably infinite.

Proof

We can write all the positive rational numbers in a two-dimensional array as shown in Figure 9.2. The top row in Figure 9.2 represents the numerator of the rational number, and the left column represents the denominator. We follow the arrows in Figure 9.2 to define $f : \mathbb{N} \to \mathbb{Q}^+$. The idea is to start in the upper left corner of the table and move to successive diagonals as follows:

- We start with all fractions in which the sum of the numerator and denominator is 2 (only $\frac{1}{1}$). So $f(1) = \frac{1}{1}$.

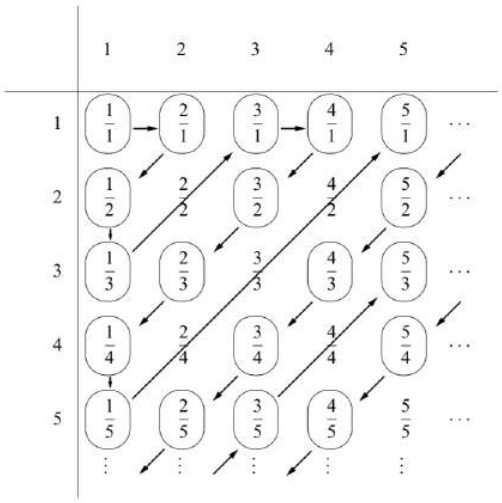


Figure 9.2: Counting the Positive Rational Numbers

- We next use those fractions in which the sum of the numerator and denominator is 3. So $f(2) = \frac{2}{1}$ and $f(3) = \frac{1}{2}$.
- We next use those fractions in which the sum of the numerator and denominator is 4. So $f(4) = \frac{1}{3}$, $f(5) = \frac{3}{1}$. We skipped $\frac{2}{2}$ since $\frac{2}{2} = \frac{1}{1}$. In this way, we will ensure that the function f is a one-to-one function.

We now continue with successive diagonals omitting fractions that are not in lowest terms. This process guarantees that the function f will be an injection and a surjection. Therefore, $\mathbb{N} \approx \mathbb{Q}^+$ and $\text{card}(\mathbb{Q}^+) = \aleph_0$.

Note: For another proof of Theorem 9.14, see exercise (14) on page 475.

Since $\mathbb{Q}^+$ is countable, it seems reasonable to expect that Q is countable. We will explore this soon. On the other hand, at this point, it may also seem reasonable to ask,

"Are there any uncountable sets?"

The answer to this question is yes, but we will wait until the next section to prove that certain sets are uncountable. We still have a few more issues to deal with concerning countable sets.

Countably Infinite Sets

Theorem 9.15.

If A is a countably infinite set, then $A \cup \{x\}$ is a countably infinite set.

Proof

Let A be a countably infinite set. Then there exists a bijection $f : \mathbb{N} \to A$. Since x is either in A or not in A, we can consider two cases.

If $x \in A$, then $A \cup \{x\} = A$ and $A \cup \{x\}$ is countably infinite.

If $x \notin A$, define $g : \mathbb{N} \to A \cup \{x\}$ by

$$g(n) = \begin{cases} x & \text{if } n = 1 \\ f(n-1) & \text{if } n > 1. \end{cases}$$

The proof that the function g is a bijection is Exercise (4). Since g is a bijection, we have proved that $A \cup \{x\} \approx \mathbb{N}$ and hence, $A \cup \{x\}$ is a countably infinite set.

Theorem 9.16.

If A is a countably infinite set and B is a finite set, then $A \cup B$ is a countably infinite set.

Proof

Exercise (5) on page 474.

Theorem 9.16 says that if we add a finite number of elements to a countably infinite set, the resulting set is still countably infinite. In other words, the cardinality of the new set is the same as the cardinality of the original set. Finite sets behave very differently in the sense that if we add elements to a finite set, we will change the cardinality. What may even be more surprising is the result in Theorem 9.17 that states that the union of two countably infinite (disjoint) sets is countably infinite. The proof of this result is similar to the proof that the integers are countably infinite (Theorem 9.13). In fact, if $A = \{a_1, a_2, a_3, \dots\}$ and $B = \{b_1, b_2, b_3, \dots\}$, then we can use the following diagram to help define a bijection from $\mathbb{N}$ to $A \cup B$.

Theorem 9.17

If A and B are disjoint countably infinite sets, then $A \cup B$ is a countably infinite set.

1	2	3	4	5	6	7	8	9	10	$\cdots$
$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\downarrow$	$\cdots$
a_1	b_1	a_2	b_2	a_3	b_3	a_4	b_4	a_5	b_5	$\cdots$

Figure 9.3: A Function from $\mathbb{N}$ to $A \cup B$

Proof

Let A and B be countably infinite sets and let $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$ be bijections. Define $h : \mathbb{N} \to A \cup B$ by

$$h(n) = \begin{cases} f(\frac{n+1}{2}) & \text{if } n \text{ is odd} \\ g(\frac{n}{2}) & \text{if } n \text{ is even.} \end{cases}$$

It is left as Exercise (6) on page 474 to prove that the function h is a bijection.

Since we can write the set of rational numbers Q as the union of the set of nonnegative rational numbers and the set of rational numbers, we can use the results in Theorem 9.14, Theorem 9.15, and Theorem 9.17 to prove the following theorem.

Theorem 9.18.

The set $\mathbb{Q}$ of all rational numbers is countably infinite.

Proof

Exercise (7) on page 474.

In Section 9.1, we proved that any subset of a finite set is finite (Theorem 9.6). A similar result should be expected for countable sets. We first prove that every subset of $\mathbb{N}$ is countable. For an infinite subset B of $\mathbb{N}$, the idea of the proof is to define a function $g : \mathbb{N} \to B$ by removing the elements from B from smallest to the next smallest to the next smallest, and so on. We do this by defining the function g recursively as follows:

- Let $g(1)$ be the smallest natural number in B.
- Remove $g(1)$ from B and let $g(2)$ be the smallest natural number in $B - \{g(1)\}$.
- Remove $g(2)$ and let $g(3)$ be the smallest natural number in $B - \{g(1), g(2)\}$.
- We continue this process. The formal recursive definition of $g : \mathbb{N} \to B$ is included in the proof of Theorem 9.19.

Theorem 9.19.

Every subset of the natural numbers is countable.

Proof

Let B be a subset of $\mathbb{N}$. If B is finte, then B is countable. So we next assume that B is infinite. We will next give a recursive definition of a function $g : \mathbb{N} \to B$ and then prove that g is a bijection.

- Let $g(1)$ be the smallest natural number in B.
- For each $n \in \mathbb{N}$, the set $B - \{g(1), g(2), \ldots, g(n)\}$ is not empty since B is infinte. Define $g(n+1)$ to be the smallest natural number in $B - \{g(1), g(2), \ldots, g(n)\}$.

The proof that the function g is a bijection is Exercise (11) on page 475.

Corollary 9.20.

Every subset of a countable set is countable.

Proof

Exercise (12) on page 475.

Exercise 9.2

1. State whether each of the following is true or false.

   (a) If a set A is countably infinite, then A is infinite.
   (b) If a set A is countably infinite, then A is countable.
   (c) If a set A is uncountable, then A is not countably infinite.
   (d) If $A \approx \mathbb{N}_k$ for some $k \in \mathbb{N}$, then A is not countable.
2. Prove that each of the following sets is countably infinite.

   (a) The set F^+ of all natural numbers that are multiple of 5
   (b) The set F of all integers that are multiples of 5
   (c) $\{\frac{1}{2^k} \mid k \in \mathbb{N}\}$
   (d) \{n \in \mathbb{Z}\ |\ n \ge -10\}\)
   (e) $\mathbb{N} - \{4, 5, 6\}$
   (f) \(\{m \in \mathbb{Z}\ |\ m \equiv 2\text{ (mod 3)}\}\)
3. Prove part (2) of Theorem 9.10.
   Let A and B be sets. If A is infinite and $A \subseteq B$, then B is infinite.
4. Complete the proof of Theorem 9.15 by proving the following:
   Let A be a countably infinite set and $x \notin A$. If $f : \mathbb{N} \to A$ is a bijection, then g is a bijection, where $g : \mathbb{N} \to A \cup \{x\}$ by

$$g(n) = \begin{cases} x & \text{if } n = 1 \\ f(n-1) & \text{if } n > 1. \end{cases} \tag{9.2.7}$$

5. Prove Theorem 9.16.
   If A is a countably infinite set and B is a finite set, then $A \cup B$ is a countably infinite set.

   Hint: Let card$(B) = n$ and use a proof by induction on n. Theorem 9.15 is the basis step.
6. Complete the proof of Theorem 9.17 by proving the following:
   Let A and B be disjoint countably infinite sets and let $f : \mathbb{N} \to A$ and $g : \mathbb{N} \to B$ be bijections. Define $h : \mathbb{N} \to A \cup B$ by

$$h(n) = \begin{cases} f(\frac{n+1}{2}) & \text{if } n \text{ is odd} \\ g(\frac{n}{2}) & \text{if } n \text{ is even.} \end{cases} \tag{9.2.8}$$

Then the function h is a bijection.

7. Prove Theorem 9.18.
   The set $\mathbb{Q}$ of all rational numbers is countable.
   Hint: Use Theorem 9.15 and Theorem 9.17.
8. Prove that if A is countably infinite and B is finite, then $A - B$ is countably infinite.
9. Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as follows: For each $(m, n) \in \mathbb{N} \times \mathbb{N}$,

$$f(m, n) = 2^{m-1}(2n - 1). \tag{9.2.9}$$

   (a) Prove that f is an injection. **Hint:** If $f(m, n) = f(s, t)$, there are three cases to consider: $m > s$, $m < s$, and $m = s$. Use laws of exponents to prove that the first two cases lead to a contradiction.
   (b) Prove that f is a surjection. **Hint**: You may use the fact that if $y \in \mathbb{N}$, then $y = 2^k x$, where x is an odd natural number and k is a nonnegative integer. This is actually a consequence of the Fundamental Theorem of Arithmetic, Theorem 8.15. [See Exercise (13) in Section 8.2.]
   (c) Prove that $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$ and hence that $\text{card}(\mathbb{N} \times \mathbb{N}) = \aleph_0$.
10. Use Exercise (9) to prove that if A and B are countably infinite sets, then $A \times B$ is a countably infinite set.
11. Complete the proof of Theorem 9.19 by proving that the function g defined in the proof is a bijection from $\mathbb{N}$ to B.

    Hint: To prove that g is an injection, it might be easier to prove that for all $r, s \in \mathbb{N}$, if $r \neq s$, then $g(r) \neq g(s)$. To do this, we may assume that $r < s$ since one of the two numbers must be less than the other. Then notice that $g(r) \in \{g(1), g(2), \ldots, g(s-1)\}$.

    To prove that g is a surjection, let $b \in B$ and notice that for some $k \in \mathbb{N}$, there will be k natural numbers in B that are less than b.

12. Prove Corollary 9.20, which states that every subset of a countable set is countable.

    Hint: Let S be a countable set and assume that $A \subseteq S$. There are two cases: A is finite or A is infinite. If A is infinite, let $f : S \to \mathbb{N}$ be a bijection and define $g : A \to f(A)$ by $g(x) = f(x)$, for each $x \in A$.

13. Use Corollary 9.20 to prove that the set of all rational numbers between 0 and 1 is countably infinite.

Explorations and Activities

14. **Another Proof that $\mathbb{Q}^+$ Is Countable.** For this activity, it may be helpful to use the Fundamental Theorem of Arithmetic (see Theorem 8.15 on page 432). Let $\mathbb{Q}^+$ be the set of positive rational numbers. Every positive rational number has a unique representation as a fraction $\frac{m}{n}$, where m and n are relatively prime natural numbers. We will now define a function $f : \mathbb{Q}^+ \to \mathbb{N}$ as follows:

    If $x \in \mathbb{Q}^+$ and $x = \frac{m}{n}$, where $m, n \in \mathbb{N}$, $n \neq 1$ and $\gcd(m, n) = 1$, we write

$$\begin{aligned} m &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \text{ and} \\ n &= q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}, \end{aligned} \tag{9.2.10}$$

    where $p_1, p_2, \ldots, p_r$ are distinct prime numbers, $q_1, q_2, \ldots, q_s$ are distinct prime numbers, and $\alpha_1, \alpha_2, \ldots, \alpha_r$ and $\beta_1, \beta_2, \ldots, \beta_s$ are natural numbers.
    We also write $1 = 2^0$ when $m = 1$. We then define

$$f(x) = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r} q_1^{2\beta_1 - 1} q_2^{2\beta_2 - 1} \cdots q_s^{2\beta_s - 1}. \tag{9.2.11}$$

If $x = \frac{m}{1}$, then we define $f(x) = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r} = m^2$.

(a) Determine $f(\frac{2}{3})$, $f(\frac{5}{6})$, $f(6)$, $f(\frac{12}{25})$, $f(\frac{375}{392})$, and $f(\frac{2^3 \cdot 11^3}{3 \cdot 5^4})$.
(b) If possible, find $x \in \mathbb{Q}^+$ such that $f(x) = 100$.
(c) If possible, find $x \in \mathbb{Q}^+$ such that $f(x) = 12$.
(d) If possible, find $x \in \mathbb{Q}^+$ such that $f(x) = 2^8 \cdot 3^5 \cdot 13 \cdot 17^2$.
(e) Prove that the function f is an injection.
(f) Prove that the function f is a surjection.
(g) What has been proved?

Answer

Add texts here. Do not delete this text first.

9.3: Uncountable Sets

Preview Activity 9.3.1: The Game of Dodge Ball

(From The Heart of Mathematics: *An Invitation to Effective Thinking* by Edward B. Burger and Michael Starbird, Key Publishing Company, ©2000 by Edward B. Burger and Michael Starbird.)

Dodge Ball is a game for two players. It is played on a game board such as the one shown in Figure 9.4. Player One has a 6 by 6 array to complete and Player Two has a 1 by 6 row to complete. Each player has six turns as described next.

- Player One begins by filling in the first horizontal row of his or her table with a sequence of six X's and O's, one in each square in the first row.
- Then Player Two places either an X or an O in the first box of his or her row. At this point, Player One has completed the first row and Player Two has filled in the first box of his or her row with one letter.

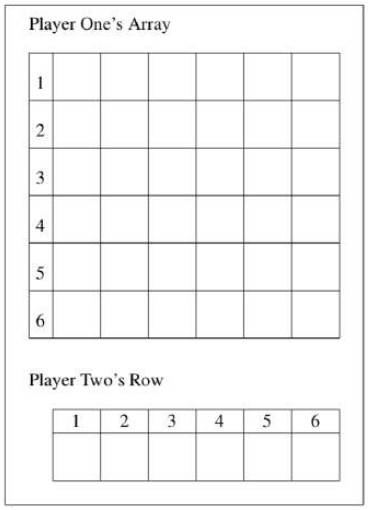


Figure 9.4: Game Board for Dodge Ball

- The game continues with Player One completing a row with six letters (X's and O's), one in each box of the next row followed by Player Two writing one letter (an X or an O) in the next box of his or her row. The game is completed when Player One has completed all six rows and Player Two has completed all six boxes in his or her row.

Winning the Game

- Player One wins if any horizontal row in the 6 by 6 array is identical to the row that Player Two created. (Player One matches Player Two.)
- Player Two wins if Player Two's row of six letters is different than each of the six rows produced by Player One. (Player Two "dodges" Player One.)

There is a winning strategy for one of the two players. This means that there is plan by which one of the two players will always win. Which player has a winning strategy? Carefully describe this winning strategy.

Applying the Winning Strategy to Lists of Real Numbers

Following is a list of real numbers between 0 and 1. Each real number is written as a decimal number.

$$a_1 = 0.1234567890 \quad a_6 = 0.0103492222$$
$$a_2 = 0.3216400000 \quad a_7 = 0.0011223344$$
$$a_3 = 0.4321593333 \quad a_8 = 0.7077700022$$
$$a_4 = 0.9120930092 \quad a_9 = 0.2100000000$$
$$a_5 = 0.0000234102 \quad a_{10} = 0.9870008943$$

Use a method similar to the winning strategy in Cantor's dodge ball to write a real number (in decimal form) between 0 and 1 that is not in this list of 10 numbers.

1. Do you think your method could be used for any list of 10 real numbers between 0 and 1 if the goal is to write a real number between 0 and 1 that is not in the list?
2. Do you think this method could be extended to a list of 20 different real numbers? To a list of 50 different real numbers?
3. Do you think this method could be extended to a list consisting of countably infinite list of real numbers?

? Preview Activity 9.3.2: Functions from a Set to Its Power Set

Let A be a set. In Section 5.1, we defined the power set $\mathcal{P}(A)$ of A to be the set of all subsets of A. This means that

$$X \in \mathcal{P}(A) \text{ if and only if } X \subseteq A.$$

Theorem 5.5 in Section 5.1 states that if a set A has n elements, then A has 2^n subsets or that $\mathcal{P}(A)$ has 2^n elements. Using our current notation for cardinality, this means that

if $\text{card}(A) = n$, then $\text{card}(\mathcal{P}(A) = 2^n$.

(The proof of this theorem was Exercise (17) on page 229.)

We are now going to define and explore some functions from a set A to its power set $\mathcal{P}(A)$. This means that the input of the function will be an element of A and the output of the function will be a subset of A.

1. Let $A = \{1, 2, 3, 4\}$. Define $f : A \to \mathcal{P}(A)$ by
   $f(1) = \{1, 2, 3\}$ $f(3) = \{1, 4\}$
   $f(2) = \{1, 3, 4\}$ $f(4) = \{2, 4\}$.

   (a) Is $1 \in f(1)$? Is $2 \in f(2)$? Is $3 \in f(3)$? Is $4 \in f(4)$?
   (b) Determine $S = \{x \in A \mid x \notin f(x)\}$.
   (c) Notice that $S \in \mathcal{P}(A)$. Does there exist an element t in A such that $f(t) = S$? That is, is $S \in \text{range}(f)$?
2. Let $A = \{1, 2, 3, 4\}$. Define $f : A \to \mathcal{P}(A)$ by

$$f(x) = A - \{x\} \text{ for each } x \in A. \tag{9.3.1}$$

   (a) Determine $f(1)$. Is $1 \in f(1)$?
   (b) Determine $f(2)$. Is $2 \in f(2)$?
   (c) Determine $f(3)$. Is $3 \in f(3)$?
   (d) Determine $f(4)$. Is $4 \in f(4)$?
   (e) Determine $S = \{x \in A \mid x \notin f(x)\}$.
   (f) Notice that $S \in \mathcal{P}(A)$. Does there exist an element t in A such that $f(t) = S$? That is, is $S \in \text{range}(f)$?
3. Define $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ by

$$f(n) - \mathbb{N} - \{n^2, n^2 - 2n\}, \text{ for each} n \in \mathbb{N}. \tag{9.3.2}$$

   (a) Determine $f(1)$, $f(2)$, $f(3)$, and $f(4)$. In each of these cases, determine if $k \in f(k)$.
   (b) Prove that if $n > 3$, then $n \in f(n)$. **Hint**: Prove that if $n > 3$, then $n^2 > n$ and $n^2 - 2n > n$.
   (c) Determine $S = \{x \in \mathbb{N} \mid x \notin f(x)\}$.
   (d) Notice that $S \in \mathcal{P}(\mathbb{N})$. Does there exist an element t in $\mathbb{N}$ such that $f(t) = S$? That is, is $S \in \text{range}(f)$?

We have seen examples of sets that are countably infinite, but we have not yet seen an example of an infinite set that is uncountable. We will do so in this section. The first example of an uncountable set will be the open interval of real numbers (0, 1). The proof that this interval is uncountable uses a method similar to the winning strategy for Player Two in the game of Dodge Ball from Preview Activity 1. Before considering the proof, we need to state an important results about decimal expressions for real numbers.

Decimal Expressions for Real Numbers

In its decimal form, any real number a in the interval (0, 1) can be written as $a = 0.a_1a_2a_3a_4\ldots$, where each a_i is an integer with $0 \leq a_i \leq 9$. For example,

$$\frac{5}{12} = 0.416666...$$

We often abbreviate this as $\frac{5}{12} = 0.41\bar{6}$ to indicate that the 6 is repeated. We can also repeat a block of digits. For example, $\frac{5}{26} = 0.19\overline{230769}$ to indicate that the block 230769 repeats. That is

$$\frac{5}{26} = 0.192307692307692307692...$$

There is only one situation in which a real number can be represented as a decimal in more than one way. A decimal that ends with an infinite string of 9's is equal to one that ends with an infinite string of 0's. For example, 0.3199999... . represents the same real number as 0.3200000... . Geometric series can be used to prove that a decimal that ends with an infinite string of 9's is equal to one that ends with an infinite string of 0's, but we will not do so here.

Definition

A decimal representation of a real number a is in **normalized form** provided that there is no natural number k such that for all natural numbers n with $n > k$, $a_n = 9$. That is, the decimal representation of a is in normalized form if and only if it does not end with an infinite string of 9's.

One reason the normalized form is important is the following theorem (which will not be proved here).

Theorem 9.21

Two decimal numbers in normalized form are equal if and only if they have identical digits in each decimal position.

Uncountable Subsets of $\mathbb{R}$

In the proof that follows, we will use only the normalized form for the decimal representation of a real number in the interval (0, 1).

Theorem 9.22.

The open interval (0, 1) is an uncountable set.

Proof

Since the interval (0, 1) contains the infinite subset$\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$, we can use Theorem 9.10, to conclude that (0, 1) is an infinite set. So (0, 1) is either countably infinite or uncountable. We will prove that (0, 1) is uncountable by proving that any injection from (0, 1) to $\mathbb{N}$ cannot be a surjection, and hence, there is no bijection between (0, 1) and $\mathbb{N}$.

So suppose that the function $f : \mathbb{N} \to (0, 1)$ is an injection. We will show that f cannot be a surjection by showing that there exists an element in (0, 1) that cannot be in the range of f. Writing the images of the elements of $\mathbb{N}$ in normalized form, we can write

$$\begin{aligned}
f(1) &= 0.a_{11}a_{12}a_{13}a_{14}a_{15}\dots \\
f(2) &= 0.a_{21}a_{22}a_{23}a_{24}a_{25}\dots \\
f(3) &= 0.a_{31}a_{32}a_{33}a_{34}a_{35}\dots \\
f(4) &= 0.a_{41}a_{42}a_{43}a_{44}a_{45}\dots \\
f(5) &= 0.a_{51}a_{52}a_{53}a_{54}a_{55}\dots \\
&\dots \\
f(n) &= 0.a_{n1}a_{n2}a_{n3}a_{n4}a_{n5}\dots \\
&\dots
\end{aligned}$$

Notice the use of the double subscripts. The number a_{ij} is the jth digit to the right of the decimal point in the normalized decimal representation of $f(i)$.

We will now construct a real number $b = 0.b_1b_2b_3b_4b_5\dots$ in (0, 1) and in normalized form that is not in this list.

Note: The idea is to start in the upper left corner and move down the diagonal in a manner similar to the winning strategy for Player Two in the game in Preview Activity 1. At each step, we choose a digit that is not equal to the diagonal digit.

Start with a_{11} in $f(1)$. We want to choose b_1 so that $b_1 \neq 0$, $b_1 \neq a_{11}$, and $b_1 \neq 9$. (To ensure that we end up with a decimal that is in normalized form, we make sure that each digit is not equal to 9.) We then repeat this process with a_{22}, a_{33}, a_{44}, a_{55}, and so on. So we let b be the real number $b = 0.b_1b_2b_3b_4b_5\ldots$, where for each $k \in \mathbb{N}$

$$b_k = \begin{cases} 3 & \text{if } a_{kk} \neq 3 \\ 5 & \text{if } a_{kk} = 3. \end{cases}$$

(The choice of 3 and 5 is arbitrary. Other choices of distinct digits will also work.)

Now for each $n \in \mathbb{N}$, $b \neq f(n)$ since b and $f(n)$ are in normalized form and b and $f(n)$ differ in the nth decimal place. This proves that any function from $\mathbb{N}$ to (0, 1) cannot be surjection and hence, there is no bijection from $\mathbb{N}$ to (0, 1). Therefore, (0, 1) is not countably infinite and hence must be an uncountable set.

Progress Check 9.23 (Dodge Ball and Cantor's Diagonal Argument)

The proof of Theorem 9.22 is often referred to as **Cantor's diagonal argument**. It is named after the mathematician Georg Cantor, who first published the proof in 1874. Explain the connection between the winning strategy for Player Two in Dodge Ball (see Preview Activity 1) and the proof of Theorem 9.22 using Cantor's diagonal argument.

Answer

Add texts here. Do not delete this text first.

The open interval (0, 1) is our first example of an uncountable set. The cardinal number of (0, 1) is defined to be c, which stands for **the cardinal number of the continuum**. So the two infinite cardinal numbers we have seen are $\aleph_0$ for countably infinite sets and c.

Definition

A set A is said to have **cardinality** c provided that A is equivalent to (0, 1). In this case, we write $\text{card}(A) = c$ and say that the cardinal number of A is c.

The proof of Theorem 9.24 is included in Progress Check 9.25.

Theorem 9.24.

Let a and b be real numbers with $a < b$. The open interval (a, b) is uncountable and has cardinality c.

Proof

Add proof here and it will automatically be hidden

Progress Check 9.25 (Proof of Theorem 9.24)

1. In Part (3) of Progress Check 9.2, we proved that if $b \in \mathbb{R}$ and $b > 0$, then the open interval (0, 1) is equivalent to the open interval $(0, b)$. Now let a and b be real numbers with $a < b$. Find a function

$$f : (0, 1) \to (a, b) \tag{9.3.3}$$

that is a bijection and conclude that $(0, 1) \approx (a, b)$.
Hint: Find a linear function that passes through the points $(0, a)$ and $(1, b)$. Use this to define the function f. Make sure you prove that this function f is a bijection.
2. Let a, b, c, d be real numbers with $a < b$ and $c < d$. Prove that $(a, b) \approx (c, d)$.

Answer

Add texts here. Do not delete this text first.

Theorem 9.26.

The set of real numbers $\mathbb{R}$ is uncountable and has cardinality c.

Proof

Let $f:(-\frac{\pi}{2},\frac{\pi}{2})\to\mathbb{R}$ be defined by $f(x)=tanx$, for each $x\in\mathbb{R}$. The function f is as bijection and, hence, $(-\frac{\pi}{2},\frac{\pi}{2})\approx\mathbb{R}$. So by Theorem 9.24, $\mathbb{R}$ is uncountable and has cardinality c.

Cantor's Theorem

We have now seen two different infinite cardinal numbers, $\aleph_0$ and c. It can seem surprising that there is more than one infinite cardinal number. A reasonable question at this point is, "Are there any other infinite cardinal numbers?" The astonishing answer is that there are, and in fact, there are infinitely many different infinite cardinal numbers. The basis for this fact is the following theorem, which states that a set is not equivalent to its power set. The proof is due to Georg Cantor (1845–1918), and the idea for this proof was explored in Preview Activity 2. The basic idea of the proof is to prove that any function from a set A to its power set cannot be a surjection.

Theorem 9.27 (Cantor's Theorem).

For every set A, A and $\mathcal{P}(A)$ do not have the same cardinality.

Proof

Let A be a set. If $A=\emptyset$, then $\mathcal{P}(A)=\{\emptyset\}$, which has cardinality 1. Therefore, $\emptyset$ and $\mathcal{P}(\emptyset)$ do not have the same cardinality.

Now suppose that $A\neq\emptyset$, and let $f:A\to\mathcal{P}(A)$. We will show that f cannot be a surjection, and hence there is no bijection from A to $\mathcal{P}(A)$. This will prove that A is not equivalentt to $\mathcal{P}(A)$. Define

$$S=\{x\in A\mid x\notin f(x)\}\ .$$

Assume that there exists a t in A such that $f(t)=S$. Now, either $f\in S$ to $t\notin S$.

- If $t\in S$, then $t\in\{x\in A\mid x\notin f(x)\}$. By the definition of S, this means that $t\notin f(t)$. However, $f(t)=S$ and so we conclude that $t\notin S$. But now we have $t\in S$ and $t\notin S$. This is a contradiction.
- If $t\notin S$, then $t\notin\{x\in A\mid x\notin f(x)\}$. By the definition of S, this means that $t\in f(t)$. However, $f(t)=S$ and so we conclude that $t\in S$. But now we have $t\notin S$ and $t\in S$. This is a contradiction.

So in both cases we have arrived at a contradiction. This means that there does not exist a t in A such that $f(t)=S$. Therefore, any function from A to $\mathcal{P}(A)$ is not a surjection and hence not a bijection. Hence, A and $\mathcal{P}(A)$ do not have the same cardinality.

corollary 9.28.

$\mathcal{P}(\mathbb{N})$ is an infinite set that is not countably infinite.

Proof

Since $\mathcal{P}(\mathbb{N})$ contains the infinite subset $\{\{1\},\{2\},\{3\}\ldots,\}$we can use Theorem 9.10, to conclude that $\mathcal{P}(\mathbb{N})$ is an infinite set. By Cantor's Theorem (Theorem 9.27), $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$ do not have the same cardinality. Therefore, P.N/ is not countable and hence is an uncountable set.

Some Final Comments about Uncountable Sets

1. We have now seen that any open interval of real numbers is uncountable and has cardinality c. In addition, R is uncountable and has cardinality c. Now, Corollary 9.28 tells us that P.N/ is uncountable. A question that can be asked is,

$$\text{“Does } \mathcal{P}(\mathbb{N}) \text{ have the same cardinality as } \mathbb{R}\text{?”} \tag{9.3.4}$$

The answer is yes, although we are not in a position to prove it yet. A proof of this fact uses the following theorem, which is known as the Cantor-Schröder-Bernstein Theorem.

Theorem 9.29. Cantor-Schröder-Bernstein

Let A and B be sets. If there exist injections $f : A \to B$ and $g : B \to A$, then $A \approx B$

In the statement of this theorem, notice that it is not required that the function g be the inverse of the function f. We will not prove the Cantor-Schröder-Bernstein Theorem here. The following items will show some uses of this important theorem.

2. The Cantor-Schröder-Bernstein Theorem can also be used to prove that the closed interval [0, 1] is equivalent to the open interval (0, 1). See Exercise (6) on page 486.
3. Another question that was posed earlier is,

$$\text{“Are there other infinite cardinal numbers other than } \aleph_0 \text{ and } c\text{?”} \tag{9.3.5}$$

Again, the answer is yes, and the basis for this is Cantor’s Theorem (Theorem 9.27). We can start with $\text{card}(\mathbb{N}) = \aleph_0$. We then define the following infinite cardinal numbers:

$$\begin{aligned} &\text{card}(\mathcal{P}(\mathbb{N})) = \alpha_1. && \text{card}(\mathcal{P}(((\mathbb{N})))) = \alpha_1. \\ &\text{card}(\mathcal{P}((\mathbb{N}))) = \alpha_1. && \ldots \end{aligned} \tag{9.3.6}$$

Cantor’s Theorem tells us that these are all different cardinal numbers, and so we are just using the lowercase Greek letter α (alpha) to help give names to these cardinal numbers. In fact, although we will not define it here, there is a way to “order” these cardinal numbers in such a way that

$$\aleph_0 < \alpha_1 < \alpha_2 < \alpha_3 < \cdots. \tag{9.3.7}$$

Keep in mind, however, that even though these are different cardinal numbers, Cantor’s Theorem does not tell us that these are the only cardinal numbers.

4. In Comment (1), we indicated that $\mathcal{P}(\mathbb{N})$ and $\mathbb{R}$ have the same cardinality. Combining this with the notation in Comment (3), this means that

$$\alpha_1 = c. \tag{9.3.8}$$

However, this does not necessarily mean that c is the “next largest” cardinal number after $\aleph_0$. A reasonable question is, “Is there an infinite set with cardinality between $\aleph_0$ and c?” Rewording this in terms of the real number line, the question is, “On the real number line, is there an infinite set of points that is not equivalent to the entire line and also not equivalent to the set of natural numbers?” This question was asked by Cantor, but he was unable to find any such set. He conjectured that no such set exists. That is, he conjectured that c is really the next cardinal number after $\aleph_0$. This conjecture has come to be known as the **Continuum Hypothesis**. Stated somewhat more formally, the Continuum Hypothesis is

$$\text{There is no set } X \text{ such that } \aleph_0 < \text{card}(X) < c. \tag{9.3.9}$$

The question of whether the Continuum Hypothesis is true or false is one of the most famous problems in modern mathematics.

Through the combined work of Kurt Gödel in the 1930s and Paul Cohen in 1963, it has been proved that the Continuum Hypothesis cannot be proved or disproved from the standard axioms of set theory. This means that either the Continuum Hypothesis or its negation can be added to the standard axioms of set theory without creating a contradiction.

Exercise 9.3

1. Use an appropriate bijection to prove that each of the following sets has cardinality c.

   (a) $(0, \infty)$
   (b) (a, ∞), for any $a \in \mathbb{R}$
   (c) $\mathbb{R} - \{0\}$
   (d) $\mathbb{R} - \{a\}$, for any $a \in \mathbb{R}$
2. Is the set of irrational numbers countable or uncountable? Prove that your answer is correct.
3. Prove that if A is uncountable and $A \subseteq B$, then B is uncountable.
4. Do two uncountable sets always have the same cardinality? Justify your conclusion.
5. Let C be the set of all infinite sequences, each of whose entries is the digit 0 or the digit 1. For example,

$$\begin{aligned} (1,0,1,0,1,0,1,0,\dots) &\in C; \\ (0,1,0,1,1,0,1,1,1,0,1,1,1,1,\dots) &\in C; \\ (2,1,0,1,1,0,1,1,1,0,1,1,1,1,\dots) &\notin C. \end{aligned} \tag{9.3.10}$$

   Is the set C a countable set or an uncountable set? Justify your conclusion.
6. The goal of this exercise is to use the Cantor-Schröder-Bernstein Theorem to prove that the cardinality of the closed interval [0, 1]$\diamond\diamond$ is c.

   (a) Find an injection $f : (0, 1) \to [0, 1]$.
   (b) Find an injection $h : [0, 1] \to (-1, 2)$.
   (c) Use the fact that $(-1, 2) \approx (0, 1)$ to prove that there exists an injection $g : [0, 1] \to (0, 1)$. (It is only necessary to prove that the injection g exists. It is not necessary to determine a specific formula for $g(x)$.)
   Note: Instead of doing Part (b) as stated, another approach is to find an injection $k : [0, 1] \to (0, 1)$. Then, it is possible to skip Part (c) and go directly to Part (d).
   (d) Use the Cantor-Schröder-Bernstein Theorem to conclude that $[0, 1] \approx (0, 1)$ and hence that the cardinality of [0, 1] is c.
7. In Exercise (6), we proved that the closed interval [0, 1] is uncountable and has cardinality c. Now let $a, b \in \mathbb{R}$ with $a < b$. Prove that $[a, b] \approx [0, 1]$ and hence that $[a, b]$ is counttable and has cardinality c.
8. Is the set of all finite subsets of $\mathbb{N}$ countable or uncountable? Let F be the set of all finite subsets of $\mathbb{N}$. Determine the cardinality of the set F.

   Consider defining a function $f : F \to \mathbb{N}$ that produces the following.
   • If $A = \{1, 2, 6\}$, then $f(A) = 2^1 3^2 5^6$.
   • If $B = \{3, 6\}$, then $f(B) = 2^3 3^6$.
   • If $C = \{m_1, m_2, m_3, m_4\}$ with $m_1 < m_2 < m_3 < m_4$, then $f(C) = 2^{m_1} 3^{m_2} 5^{m_3} 7^{m_4}$.
   It might be helpful to use the Fundamental Theorem of Arithmetic on page 432and to denote the set of all primes as $P = \{p_1, p_2, p_3, p_4, \dots\}$ with $p_1 > p_2 < p_3 < p_4 \cdots$. Using the sets A, B, and C define above, we could then write $f(A) = p_1^1 p_2^2 p_3^6$, $f(B) = p_1^3 p_2^6$, and $f(C) = p_1^{m_1} p_2^{m_2} p_3^{m_3} p_4^{m_4}$.
9. In Exercise (2), we showed that the set of irrational numbers is uncountable. However, we still do not know the cardinality of the set of irrational numbers. Notice that we can use $\mathbb{Q}^c$ to stand for the set of irrational numbers.

   (a) Construct a function $f : \mathbb{Q}^c \to \mathbb{R}$ that is an injection.

   We know that any real number a can be represented in decimal form as follows:

$$a = A.\, a_1 a_2 a_3 a_4 \cdots a_n \cdots, \tag{9.3.11}$$

   where A is an integer and the decimal part $(0.a_1 a_2 a_3 a_4 \cdots)$ is in normalized form. (See page 480.) We also know that the real number a is an irrational number if and only a has an infinite non-repeating decimal expansion. We now associate with a the real number

$$A.\, a_1 0 a_2 11 a_3 000 a_4 1111 a_5 00000 a_6 111111 \cdots. \tag{9.3.12}$$

Notice that to construct the real number in (9.3.12), we started with the decimal expansion of a, inserted a 0 to the right of the first digit after the decimal point, inserted two 1's to the right of the second digit to the right of the decimal point, inserted three 0's to the right of the third digit to the right of the decimal point, and so on.

(b) Explain why the real number in (9.3.12) is an irrational number.
(c) Use these ideas to construct a function $g : \mathbb{R} \to \mathbb{Q}^c$ that is an injection.
(d) What can we now conclude by using the Cantor-Schröder-Bernstein Theorem?

10. Let J be the unit open interval. That is, $J = \{x \in \mathbb{R} \mid 0 < x < 1\}$ and let $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid 0 < x < 1 \text{ and } 0 < y < 1\}$. We call S the unit open square. We will now define a function f from S to J. Let $(a, b) \in S$ and write the decimal expansions of a and b in normalized form as

$$\begin{aligned} a &= 0.a_1 a_2 a_3 a_4 \cdots a_n \cdots \\ b &= 0.b_1 b_2 b_3 b_4 \cdots b_n \cdots. \end{aligned} \tag{9.3.13}$$

We then define $f(a, b) = 0.a_1 b_1 a_2 b_2 a_3 b_3 a_4 b_4 \cdots a_n b_n \cdots$.

(a) Determine the values of $f(0.3, 0.625)$ $f(\frac{1}{3}, \frac{1}{4})$, and $f(\frac{1}{6}, \frac{5}{6})$.
(b) If possible, find $(x, y) \in S$ such that $f(x, y) = 0.2345$
(c) If possible, find $(x, y) \in S$ such that $f(x, y) = \frac{1}{3}$.
(d) If possible, find $(x, y) \in S$ such that $f(x, y) = \frac{1}{2}$.
(e) Explain why the function $f : S \to J$ is an injection but is not a surjection.
(f) Use the Cantor-Schröder-Bernstein Theorem to prove that the cardinality of the unit open square S is equal to c. If this result seems surprising, you are in good company. In a letter written in 1877 to the mathematician Richard Dedekind describing this result that he had discovered, Georg Cantor wrote, "I see it but I do not believe it."

Explorations and Activities

11. **The Closed Interval [0,1].** In Exercise (6), the Cantor-Schröder-Bernstein Theorem was used to prove that the closed interval [0, 1] has cardinality c. This may seem a bit unsatisfactory since we have not proved the Cantor-Schröder-Bernstein Theorem. In this activity, we will prove that $\text{card}([0, 1]) = c$ by using appropriate bijections.

(a) Let $f : [0, 1] \to [0, 1)$ by

$$f(x) = \begin{cases} \frac{1}{2} & \text{if } x = 0 \\ \frac{1}{n+1} & \text{if } x = \frac{1}{2} \text{ for some } n \in \mathbb{N} \\ x & \text{otherwise.} \end{cases} \tag{9.3.14}$$

i. Determine $f(0)$, $f(1)$, $f(\frac{1}{2})$, $f(\frac{1}{3})$, $f(\frac{1}{4})$, and $f(\frac{1}{5})$.
ii. Sketch a graph of the function f. **Hint**: Start with the graph of $y = x$ for $0 \leq x \leq 1$. Remove the point (1, 1) and replace it with the point (1, $\frac{1}{2}$). Next, remove the point $(\frac{1}{2}, \frac{1}{2})$ and replace it with the point $(\frac{1}{2}, \frac{1}{3})$. Continue this process of removing points on the graph of $y = x$ and replacing them with the points determined from the information in Part (11(a)i). Stop after repeating this four or five times so that pattern of this process becomes apparent.
iii. Explain why the function f is a bijection.
iv. Prove that $[0, 1] \approx [0, 1)$.

(b) Let $g : [0, 1) \to (0, 1)$ by

$$g(x) = \begin{cases} \dfrac{1}{n+1} & \text{if } x = \dfrac{1}{2} \text{ for some } n \in \mathbb{N} \\ x & \text{otherwise.} \end{cases} \tag{9.3.15}$$

i. Follow the procedure suggested in Part (11a) to sketch a graph of g.
ii. Explain why the function g is a bijection.
iii. Prove that $[0, 1) \approx (0, 1)$.
(c) Prove that [0, 1] and [0, 1) are both uncountable and have cardinality c.

Answer

Add texts here. Do not delete this text first.

9.S: Finite and Infinite Sets (Summary)

Important Definitions

- Equivalent sets, page 452
- Sets with the same cardinality, page 452
- Finite set, page 455
- Infinite set, page 455
- Cardinality of a finite set, page 455
- Cardinality of $\mathbb{N}$, page 466
- $\aleph_0$, page 466
- Countably infinite set, page 466
- Denumerable set, page 466
- Uncountable set, page 466

Important Theorems and Results about Finite and Infinite Sets

- **Theorem 9.3.** Any set equivalent to a finite nonempty set A is a finite set and has the same cardinality as A.
- **Theorem 9.6**. If S is a finite set and A is a subset of S, then A is finite and $\text{card}(A) \leq \text{card}(S)$.
- **Corollary 9.8**. A finite set is not equivalent to any of its proper subsets.
- **Theorem 9.9 [The Pigeonhole Principle]**. Let A and B be finite sets. If $\text{card}(A) > \text{card}(B)$, then any function $f : A \to B$ is not an injection.
- **Theorem 9.10**. Let A and B be sets.

  1. If A is infinite and $A \approx B$, then B is infinite.
  2. If A is infinite and $A \subseteq B$,then B is infinite.
- **Theorem 9.13**. The set $\mathbb{Z}$ of integers is countably infinite, and so $\text{card}(\mathbb{Z}) = \aleph_0$.
- **Theorem 9.14**. The set of positive rational numbers is countably infinite.
- **Theorem 9.16**. If A is a countably infinite set and B is a finite set, then $A \cup B$ is a countably infinite set.
- **Theorem 9.17**. If A and B are disjoint countably infinite sets, then $A \cup B$ is a countably infinite set.
- **Theorem 9.18**. The set $\mathbb{Q}$ of all rational numbers is countably infinite.
- **Theorem 9.19**. Every subset of the natural numbers is countable.
- **Corollary 9.20**. Every subset of a countable set is countable.
- **Theorem 9.22**. The open interval (0, 1) is an uncountable set.
- **Theorem 9.24**. Let a and b be real numbers with $a < b$. The open interval (a, b) is uncountable and has cardinality c.
- **Theorem 9.26.** The set of real numbers $\mathbb{R}$ is uncountable and has cardinality c.
- **Theorem 9.27 [Cantor's Theorem]**. For every set A, A and $\mathcal{P}(A)$ do not have the same cardinality.
- **Corollary 9.28.** $\mathcal{P}(\mathbb{N})$ is an infinite set that is not countably infinite.
- **Theorem 9.29 [Cantor-Schr$\ddot{0}$der-Bernstein]**. Let A and B be sets. If there exist injections $f_1 : A \to B$ and $f_2 : B \to A$, then $A \approx B$.

CHAPTER OVERVIEW

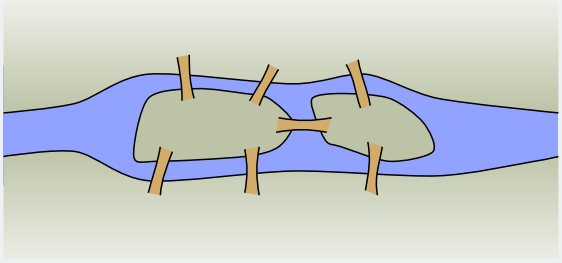
10: Graph Theory

Graph Theory is a relatively new area of mathematics, first studied by the super famous mathematician Leonhard Euler in 1735. Since then it has blossomed in to a powerful tool used in nearly every branch of science and is currently an active area of mathematics research.

10.1: Prelude to Graph Theory

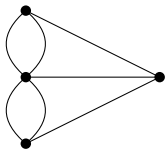
Investigate!

In the time of Euler, in the town of Königsberg in Prussia, there was a river containing two islands. The islands were connected to the banks of the river by seven bridges (as seen below). The bridges were very beautiful, and on their days off, townspeople would spend time walking over the bridges. As time passed, a question arose: was it possible to plan a walk so that you cross each bridge once and only once? Euler was able to answer this question. Are you?



Graph Theory is a relatively new area of mathematics, first studied by the super famous mathematician Leonhard Euler in 1735. Since then it has blossomed in to a powerful tool used in nearly every branch of science and is currently an active area of mathematics research.

The problem above, known as the *Seven Bridges of Königsberg*, is the problem that originally inspired graph theory. Consider a "different" problem: Below is a drawing of four dots connected by some lines. Is it possible to trace over each line once and only once (without lifting up your pencil, starting and ending on a dot)?



There is an obvious connection between these two problems. Any path in the dot and line drawing corresponds exactly to a path over the bridges of Königsberg.

Pictures like the dot and line drawing are called *graphs*. Graphs are made up of a collection of dots called *vertices* and lines connecting those dots called *edges*. When two vertices are connected by an edge, we say they are *adjacent*. The nice thing about looking at graphs instead of pictures of rivers, islands and bridges is that we now have a mathematical object to study. We have distilled the "important" parts of the bridge picture for the purposes of the problem. It does not matter how big the islands are, what the bridges are made out of, if the river contains alligators, etc. All that matters is which land masses are connected to which other land masses, and how many times. This was the great insight that Euler had.

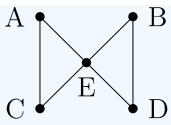
We will return to the question of finding paths through graphs later. But first, here are a few other situations you can represent with graphs:

Example 10.1.1

Al, Bob, Cam, Dan, and Euclid are all members of the social networking website *Facebook*. The site allows members to be "friends" with each other. It turns out that Al and Cam are friends, as are Bob and Dan. Euclid is friends with everyone. Represent this situation with a graph.

Solution

Each person will be represented by a vertex and each friendship will be represented by an edge. That is, two vertices will be adjacent (there will be an edge between them) if and only if the people represented by those vertices are friends. We get the following graph:

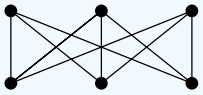


Example 10.1.1

Each of three houses must be connected to each of three utilities. Is it possible to do this without any of the utility lines crossing?

Solution

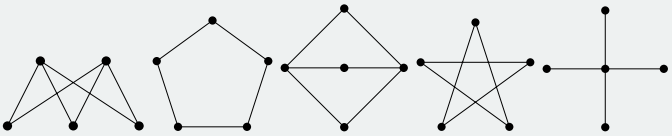
We will answer this question later. For now, notice how we would ask this question in the context of graph theory. We are really asking whether it is possible to redraw the graph below without any edges crossing (except at vertices). Think of the top row as the houses, bottom row as the utilities.



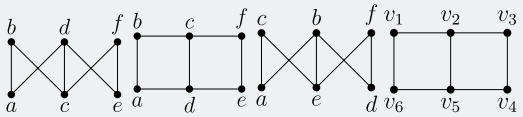
10.2: Definitions

Investigate!

Which (if any) of the graphs below are the same?



The graphs above are unlabeled. Usually we think of a graph as having a specific set of vertices. Which (if any) of the graphs below are the same?



Actually, all the graphs we have seen above are just *drawings* of graphs. A graph is really an abstract mathematical object consisting of two sets V and E where E is a set of 2-element subsets of V. Are the graphs below the same or different?

Graph 1:

- $V = \{a, b, c, d, e\}$,
- $E = \{\{a, b\}, \{a, c\}, \{a, d\}, \{a, e\}, \{b, c\}, \{d, e\}\}$.

Graph 2:

- $V = \{v_1, v_2, v_3, v_4, v_5\}$,
- $E = \{\{v_1, v_3\}, \{v_1, v_5\}, \{v_2, v_4\}, \{v_2, v_5\}, \{v_3, v_5\}, \{v_4, v_5\}\}$.

Before we start studying graphs, we need to agree upon what a graph is. While we almost always think of graphs as pictures (dots connected by lines) this is fairly ambiguous. Do the lines need to be straight? Does it matter how long the lines are or how large the dots are? Can there be two lines connecting the same pair of dots? Can one line connect three dots?

The way we avoid ambiguities in mathematics is to provide concrete and rigorous *definitions*. Crafting good definitions is not easy, but it is incredibly important. The definition is the agreed upon starting point from which all truths in mathematics proceed. Is there a graph with no edges? We have to look at the definition to see if this is possible.

We want our definition to be precise and unambiguous, but it also must agree with our intuition for the objects we are studying. It needs to be useful: we *could* define a graph to be a six legged mammal, but that would not let us solve any problems about bridges. Instead, here is the (now) standard definition of a graph.

Definition

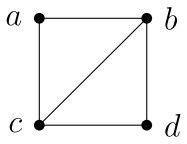
A *graph* is an ordered pair $G = (V, E)$ consisting of a nonempty set V (called the *vertices*) and a set E (called the *edges*) of two-element subsets of V.

Strange. Nowhere in the definition is there talk of dots or lines. From the definition, a graph could be

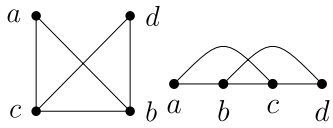
$$(\{a, b, c, d\}, \{\{a, b\}, \{a, c\}, \{b, c\}, \{b, d\}, \{c, d\}\}).$$

Here we have a graph with four vertices (the letters a, b, c, d) and four edges (the pairs $\{a, b\}, \{a, c\}, \{b, c\}, \{b, d\}, \{c, d\}$).

Looking at sets and sets of 2-element sets is difficult to process. That is why we often draw a representation of these sets. We put a dot down for each vertex, and connect two dots with a line precisely when those two vertices are one of the 2-element subsets in our set of edges. Thus one way to draw the graph described above is this:



However we could also have drawn the graph differently. For example either of these:



We should be careful about what it means for two graphs to be "the same." Actually, given our definition, this is easy: Are the vertex sets equal? Are the edge sets equal? We know what it means for sets to be equal, and graphs are nothing but a pair of two special sorts of sets.

Example 10.2.1

Are the graphs below equal?

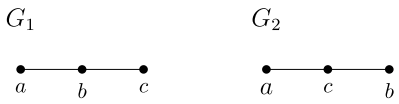
$$G_1 = (\{a,b,c\}, \{\{a,b\},\{b,c\}\}); \qquad G_2 = (\{a,b,c\}, \{\{a,c\},\{c,b\}\})$$

equal?

Solution

No. Here the vertex sets of each graph are equal, which is a good start. Also, both graphs have two edges. In the first graph, we have edges $\{a,b\}$ and $\{b,c\}$, while in the second graph we have edges $\{a,c\}$ and $\{c,b\}$. Now we do have $\{b,c\} = \{c,b\}$,so that is not the problem. The issue is that $\{a,b\} \neq \{a,c\}$.Since the edge sets of the two graphs are not equal (as sets), the graphs are not equal (as graphs).

Even if two graphs are not *equal*, they might be *basically* the same. The graphs in the previous example could be drawn like this:



Graphs that are basically the same (but perhaps not equal) are called *isomorphic*. We will give a precise definition of this term after a quick example:

Example 10.2.2

Consider the graphs:

- $G_1 = \{V_1, E_1\}$ where $V_1 = \{a,b,c\}$ and $E_1 = \{\{a,b\},\{a,c\},\{b,c\}\}$;
- $G_2 = \{V_2, E_2\}$ where $V_2 = \{u,v,w\}$ and $E_2 = \{\{u,v\},\{u,w\},\{v,w\}\}$.

Are these graphs the same?

Solution

The two graphs are NOT equal. It is enough to notice that $V_1 \neq V_2$ since $a \in V_1$ but $a \notin V_2$. However, both of these graphs consist of three vertices with edges connecting every pair of vertices. We can draw them as follows:

Clearly we want to say these graphs are basically the same, so while they are not equal, they will be *isomorphic*. The reason is we can rename the vertices of one graph and get the second graph as the result.

Intuitively, graphs are *isomorphic* if they are basically the same, or better yet, if they are the same except for the names of the vertices. To make the concept of renaming vertices precise, we give the following definitions:

Isomorphic Graphs

An *isomorphism* between two graphs G_1 and G_2 is a bijection $f : V_1 \to V_2$ between the vertices of the graphs such that if $\{a, b\}$ is an edge in G_1 then $\{f(a), f(b)\}$ is an edge in G_2.

Two graphs are *isomorphic* if there is an isomorphism between them. In this case we write $G_1 \cong G_2$.

An isomorphism is simply a function which renames the vertices. It must be a bijection so every vertex gets a new name. These newly named vertices must be connected by edges precisely if they were connected by edges with their old names.

Example 10.2.3

Decide whether the graphs $G_1 = \{V_1, E_1\}$ and $G_2 = \{V_2, E_2\}$ are equal or isomorphic.

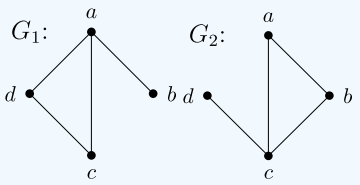
- $V_1 = \{a, b, c, d\}$, $E_1 = \{\{a, b\}, \{a, c\}, \{a, d\}, \{c, d\}\}$
- $V_2 = \{a, b, c, d\}$, $E_2 = \{\{a, b\}, \{a, c\}, \{b, c\}, \{c, d\}\}$

Solution

The graphs are NOT equal, since $\{a, d\} \in E_1$ but $\{a, d\} \notin E_2$. However, since both graphs contain the same number of vertices and same number of edges, they *might* be isomorphic (this is not enough in most cases, but it is a good start).

We can try to build an isomorphism. How about we say $f(a) = b$, $f(b) = c$, $f(c) = d$ and $f(d) = a$. This is definitely a bijection, but to make sure that the function is an isomorphism, we must make sure it *respects the edge relation*. In G_1, vertices a and b are connected by an edge. In G_2, $f(a) = b$ and $f(b) = c$ are connected by an edge. So far, so good, but we must check the other three edges. The edge $\{a, c\}$ in G_1 corresponds to $\{f(a), f(c)\} = \{b, d\}$, but here we have a problem. There is no edge between b and d in G_2. Thus f is NOT an isomorphism.

Not all hope is lost, however. Just because f is not an isomorphism does not mean that there is no isomorphism at all. We can try again. At this point it might be helpful to draw the graphs to see how they should match up.



Alternatively, notice that in G_1, the vertex a is adjacent to every other vertex. In G_2, there is also a vertex with this property: c. So build the bijection $g : V_1 \to V_2$ by defining $g(a) = c$ to start with. Next, where should we send b? In G_1, the vertex b is only adjacent to vertex a. There is exactly one vertex like this in G_2, namely d. So let $g(b) = d$. As for the last two, in this example, we have a free choice: let $g(c) = b$ and $g(d) = a$ (switching these would be fine as well).

We should check that this really is an isomorphism. It is definitely a bijection. We must make sure that the edges are respected. The four edges in G_1 are

$$\{a, b\}, \{a, c\}, \{a, d\}, \{c, d\}$$

Under the proposed isomorphism these become

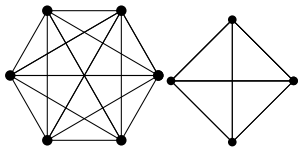
$$\{g(a), g(b)\}, \{g(a), g(c)\}, \{g(a), g(d)\}, \{g(c), g(d)\}$$

$$\{c, d\}, \{c, b\}, \{c, a\}, \{b, a\}$$

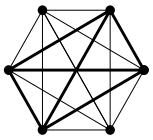
which are precisely the edges in G_2. Thus g is an isomorphism, so $G_1 \cong G_2$

Sometimes we will talk about a graph with a special name (like K_n or the *Peterson graph*) or perhaps draw a graph without any labels. In this case we are really referring to *all* graphs isomorphic to any copy of that particular graph. A collection of isomorphic graphs is often called an *isomorphism class*.[1] This is not unlike geometry, where we might have more than one copy of a particular triangle. There instead of *isomorphic* we say *congruent*.

There are other relationships between graphs that we care about, other than equality and being isomorphic. For example, compare the following pair of graphs:



These are definitely not isomorphic, but notice that the graph on the right looks like it might be part of the graph on the left, especially if we draw it like this:



We would like to say that the smaller graph is a *subgraph* of the larger.

We should give a careful definition of this. In fact, there are two reasonable notions for what a subgroup should mean.

Subgraphs

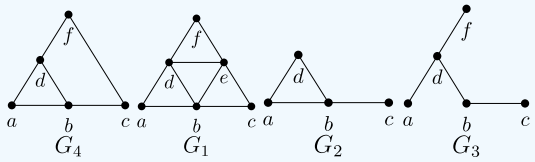
We say that $G_1 = (V_1, E_1)$ is a *subgraph* of $G_2 = (V_2, E_2)$ provided $V_1 \subseteq V_2$ and $E_1 \subseteq E_2$.

We say that $G_1 = (V_1, E_1)$ is an *induced subgraph* of $G_2 = (V_2, E_2)$ provided $V_1 \subseteq V_2$ and E_1 contains all edges of E_2 which are subsets of V_1.

Notice that every induced subgraph is also an ordinary subgraph, but not conversely. Think of a subgraph as the result of deleting some vertices and edges from the larger graph. For the subgraph to be an induced subgraph, we can still delete vertices, but now we only delete those edges that included the deleted vertices.

Example 10.2.4

Consider the graphs:



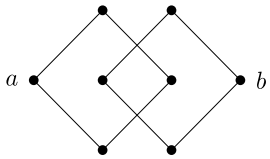
Here both G_2 and G_3 are subgraphs of G_1. But only G_2 is an *induced* subgraph. Every edge in G_1 that connects vertices in G_2 is also an edge in G_2. In G_3, the edge $\{a, b\}$ is in E_1 but not E_3, even though vertices a and b are in V_3.

The graph G_4 is NOT a subgraph of G_1, even though it looks like all we did is remove vertex e. The reason is that in E_4 we have the edge $\{c, f\}$ but this is not an element of E_1, so we don't have the required $E_4 \subseteq E_1$.

Back to some basic graph theory definitions. Notice that all the graphs we have drawn above have the property that no pair of vertices is connected more than once, and no vertex is connected to itself. Graphs like these are sometimes called *simple*, although we will just call them *graphs*. This is because our definition for a graph says that the edges form a set of 2-element subsets of the vertices. Remember that it doesn't make sense to say a set contains an element more than once. So no pair of vertices can be connected by an edge more than once. Also, since each edge must be a set containing two vertices, we cannot have a single vertex connected to itself by an edge.

That said, there are times we want to consider double (or more) edges and single edge loops. For example, the “graph” we drew for the Bridges of Königsberg problem had double edges because there really are two bridges connecting a particular island to the near shore. We will call these objects *multigraphs*. This is a good name: a *multiset* is a set in which we are allowed to include a single element multiple times.

The graphs above are also *connected*: you can get from any vertex to any other vertex by following some path of edges. A graph that is not connected can be thought of as two separate graphs drawn close together. For example, the following graph is NOT connected because there is no path from a to b:



Most of the time, it makes sense to treat non-connected graphs as separate graphs (think of the above graph as two squares), so unless otherwise stated, we will assume all our graphs are connected.

Vertices in a graph do not always have edges between them. If we add all possible edges, then the resulting graph is called *complete*. That is, a graph is complete if every pair of vertices is connected by an edge. Since a graph is determined completely by which vertices are adjacent to which other vertices, there is only one complete graph with a given number of vertices. We give these a special name: K_n is the complete graph on n vertices.

Each vertex in K_n is adjacent to $n-1$ other vertices. We call the number of edges emanating from a given vertex the *degree* of that vertex. So every vertex in K_n has degree $n-1$. How many edges does K_n have? One might think the answer should be $n(n-1)$, since we count $n-1$ edges n times (once for each vertex). However, each edge is incident to 2 vertices, so we counted every edge exactly twice. Thus there are $n(n-1)/2$ edges in K_n. Alternatively, we can say there are $\binom{n}{2}$ edges, since to draw an edge we must choose 2 of the n vertices.

In general, if we know the degrees of all the vertices in a graph, we can find the number of edges. The sum of the degrees of all vertices will always be *twice* the number of edges, since each edge adds to the degree of two vertices. Notice this means that the sum of the degrees of all vertices in any graph must be even!

Example 10.2.5

At a recent math seminar, 9 mathematicians greeted each other by shaking hands. Is it possible that each mathematician shook hands with exactly 7 people at the seminar?

Solution

It seems like this should be possible. Each mathematician chooses one person to not shake hands with. But this cannot happen. We are asking whether a graph with 9 vertices can have each vertex have degree 7. If such a graph existed, the sum of the degrees of the vertices would be $9 \cdot 7 = 63$. This would be twice the number of edges (handshakes) resulting in a graph with 31.5 edges. That is impossible. Thus at least one (in fact an odd number) of the mathematicians must have shaken hands with an *even* number of people at the seminar.

One final definition: we say a graph is *bipartite* if the vertices can be divided into two sets, A and B, with no two vertices in A adjacent and no two vertices in B adjacent. The vertices in A can be adjacent to some or all of the vertices in B. If each vertex in A is adjacent to all the vertices in B, then the graph is a *complete bipartite graph*, and gets a special name: $K_{m,n}$, where $|A| = m$ and $|B| = n$. The graph in the houses and utilities puzzle is $K_{3,3}$.

Named Graphs

Some graphs are used more than others, and get special names.

- K_n: The complete graph on n vertices.
- $K_{m,n}$: The complete bipartite graph with sets of m and n vertices.
- C_n: The cycle on n vertices, just one big loop.
- P_n: The path on n vertices, just one long path.

There are a lot of definitions to keep track of in graph theory. Here is a glossary of the terms we have already used and will soon encounter.

Graph Theory Definitions

- Graph: A collection of vertices, some of which are connected by edges. More precisely, a pair of sets V and E where V is a set of vertices and E is a set of 2-element subsets of V.
- Adjacent: Two vertices are adjacent if they are connected by an edge. Two edges are adjacent if they share a vertex.
- Bipartite graph: A graph for which it is possible to divide the vertices into two disjoint sets such that there are no edges between any two vertices in the same set.
- Complete bipartite graph: A bipartite graph for which every vertex in the first set is adjacent to every vertex in the second set.
- Complete graph: A graph in which every pair of vertices is adjacent.
- Connected: A graph is connected if there is a path from any vertex to any other vertex.
- Chromatic number: The minimum number of colors required in a proper vertex coloring of the graph.
- Cycle: A path (see below) that starts and stops at the same vertex, but contains no other repeated vertices.
- Degree of a vertex: The number of edges incident to a vertex.
- Euler path: A walk which uses each edge exactly once.
- Euler circuit: An Euler path which starts and stops at the same vertex.
- Multigraph: A multigraph is just like a graph but can contain multiple edges between two vertices as well as single edge loops (that is an edge from a vertex to itself).
- Planar: A graph which can be drawn (in the plane) without any edges crossing.
- Subgraph: We say that H is a subgraph of G if every vertex and edge of H is also a vertex or edge of G. We say H is an induced subgraph of G if every vertex of H is a vertex of G and each pair of vertices in H are adjacent in H if and only if they are adjacent in G.
- Tree: A (connected) graph with no cycles. (A non-connected graph with no cycles is called a forest.) The vertices in a tree with degree 1 are called leaves.
- Vertex coloring: An assignment of colors to each of the vertices of a graph. A vertex coloring is proper if adjacent vertices are always colored differently.
- Walk: A sequence of vertices such that consecutive vertices (in the sequence) are adjacent (in the graph). A walk in which no vertex is repeated is called simple

10.3: Planar Graphs

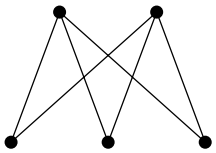
Investigate!

When a connected graph can be drawn without any edges crossing, it is called *planar*. When a planar graph is drawn in this way, it divides the plane into regions called *faces*.

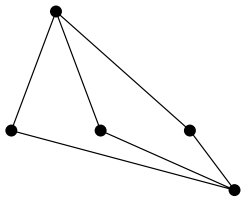
1. Draw, if possible, two different planar graphs with the same number of vertices, edges, and faces.
2. Draw, if possible, two different planar graphs with the same number of vertices and edges, but a different number of faces.

When is it possible to draw a graph so that none of the edges cross? If this *is* possible, we say the graph is *planar* (since you can draw it on the *plane*).

Notice that the definition of planar includes the phrase "it is possible to." This means that even if a graph does not look like it is planar, it still might be. Perhaps you can redraw it in a way in which no edges cross. For example, this is a planar graph:



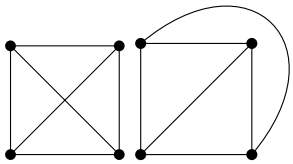
That is because we can redraw it like this:



The graphs are the same, so if one is planar, the other must be too. However, the original drawing of the graph was not a *planar representation* of the graph.

When a planar graph is drawn without edges crossing, the edges and vertices of the graph divide the plane into regions. We will call each region a *face*. The graph above has 3 faces (yes, we *do* include the "outside" region as a face). The number of faces does not change no matter how you draw the graph (as long as you do so without the edges crossing), so it makes sense to ascribe the number of faces as a property of the planar graph.

WARNING: you can only count faces when the graph is drawn in a planar way. For example, consider these two representations of the same graph:



If you try to count faces using the graph on the left, you might say there are 5 faces (including the outside). But drawing the graph with a planar representation shows that in fact there are only 4 faces.

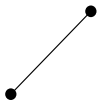
There is a connection between the number of vertices (v), the number of edges (e) and the number of faces (f) in any connected planar graph. This relationship is called Euler's formula.

Definition: Euler's Formula for Planar Graphs

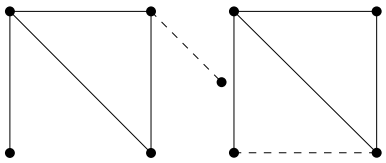
For any (connected) planar graph with v vertices, e edges and f faces, we have

$$v - e + f = 2$$

Why is Euler's formula true? One way to convince yourself of its validity is to draw a planar graph step by step. Start with the graph P_2:



Any connected graph (besides just a single isolated vertex) must contain this subgraph. Now build up to your graph by adding edges and vertices. Each step will consist of either adding a new vertex connected by a new edge to part of your graph (so creating a new “spike”) or by connecting two vertices already in the graph with a new edge (completing a circuit).



What do these “moves” do? When adding the spike, the number of edges increases by 1, the number of vertices increases by one, and the number of faces remains the same. But this means that $v-e+f$ does not change. Completing a circuit adds one edge, adds one face, and keeps the number of vertices the same. So again, $v-e+f$ does not change.

Since we can build any graph using a combination of these two moves, and doing so never changes the quantity $v-e+f$, that quantity will be the same for all graphs. But notice that our starting graph P_2 has $v=2$, $e=1$ and $f=1$, so $v-e+f=2$. This argument is essentially a proof by induction. A good exercise would be to rewrite it as a formal induction proof.

Non-planar Graphs

Investigate!

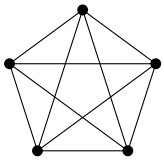
For the complete graphs K_n, we would like to be able to say something about the number of vertices, edges, and (if the graph is planar) faces. Let's first consider K_3:

1. How many vertices does K_3 have? How many edges?
2. If K_3 is planar, how many faces should it have?

Repeat parts (1) and (2) for K_4, K_5, and K_{23}.

What about complete bipartite graphs? How many vertices, edges, and faces (if it were planar) does $K_{7,4}$ have? For which values of m and n are K_n and $K_{m,n}$ planar?

Not all graphs are planar. If there are too many edges and too few vertices, then some of the edges will need to intersect. The first time this happens is in K_5.



If you try to redraw this without edges crossing, you quickly get into trouble. There seems to be one edge too many. In fact, we can prove that no matter how you draw it, K_5 will always have edges crossing.

Theorem 10.3.1

K_5 is not planar.

Proof

The proof is by contradiction. So assume that K_5 is planar. Then the graph must satisfy Euler's formula for planar graphs. K_5 has 5 vertices and 10 edges, so we get

$$5-10+f=2$$

which says that if the graph is drawn without any edges crossing, there would be $f = 7$ faces.

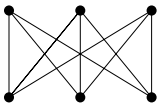
Now consider how many edges surround each face. Each face must be surrounded by at least 3 edges. Let B be the total number of *boundaries* around all the faces in the graph. Thus we have that $B \geq 3f$. But also $B = 2e$, since each edge is used as a boundary exactly twice. Putting this together we get

$$3f \leq 2e$$

But this is impossible, since we have already determined that $f = 7$ and $e = 10$, and $21 \not\leq 20$. This is a contradiction so in fact K_5 is not planar.

□

The other simplest graph which is not planar is $K_{3,3}$



Proving that $K_{3,3}$ is not planar answers the houses and utilities puzzle: it is not possible to connect each of three houses to each of three utilities without the lines crossing.

Theorem 10.3.2

$K_{3,3}$ is not planar.

Proof

Again, we proceed by contradiction. Suppose $K_{3,3}$ were planar. Then by Euler's formula there will be 5 faces, since $v = 6$, $e = 9$, and $6 - 9 + f = 2$.

How many boundaries surround these 5 faces? Let B be this number. Since each edge is used as a boundary twice, we have $B = 2e$. Also, $B \geq 4f$ since each face is surrounded by 4 or more boundaries. We know this is true because $K_{3,3}$ is bipartite, so does not contain any 3-edge cycles. Thus

$$4f \leq 2e.$$

But this would say that $20 \leq 18$, which is clearly false. Thus $K_{3,3}$ is not planar.

□

Note the similarities and differences in these proofs. Both are proofs by contradiction, and both start with using Euler's formula to derive the (supposed) number of faces in the graph. Then we find a relationship between the number of faces and the number of edges based on how many edges surround each face. This is the only difference. In the proof for K_5, we got $3f \leq 2e$ and for $K_{3,3}$ we go $4f \leq 2e$. The coefficient of f is the key. It is the smallest number of edges which could surround any face. If some number of edges surround a face, then these edges form a cycle. So that number is the size of the smallest cycle in the graph.

In general, if we let g be the size of the smallest cycle in a graph (g stands for *girth*, which is the technical term for this) then for any planar graph we have $gf \leq 2e$. When this disagrees with Euler's formula, we know for sure that the graph cannot be planar.

Polyhedra

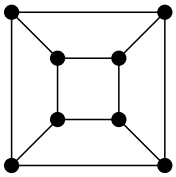
Investigate!

A cube is an example of a convex polyhedron. It contains 6 identical squares for its faces, 8 vertices, and 12 edges. The cube is a *regular polyhedron* (also known as a *Platonic solid*) because each face is an identical regular polygon and each vertex joins an equal number of faces.

There are exactly four other regular polyhedra: the tetrahedron, octahedron, dodecahedron, and icosahedron with 4, 8, 12 and 20 faces respectively. How many vertices and edges do each of these have?

Another area of mathematics where you might have heard the terms “vertex,” “edge,” and “face” is geometry. A *polyhedron* is a geometric solid made up of flat polygonal faces joined at edges and vertices. We are especially interested in *convex* polyhedra, which means that any line segment connecting two points on the interior of the polyhedron must be entirely contained inside the polyhedron.[2] An alternative definition for convex is that the internal angle formed by any two faces must be less than \(180\deg\text{.}\)

Notice that since $8-12+6=2,$ the vertices, edges and faces of a cube satisfy Euler's formula for planar graphs. This is not a coincidence. We can represent a cube as a planar graph by projecting the vertices and edges onto the plane. One such projection looks like this:



In fact, *every* convex polyhedron can be projected onto the plane without edges crossing. Think of placing the polyhedron inside a sphere, with a light at the center of the sphere. The edges and vertices of the polyhedron cast a shadow onto the interior of the sphere. You can then cut a hole in the sphere in the middle of one of the projected faces and “stretch” the sphere to lay down flat on the plane. The face that was punctured becomes the “outside” face of the planar graph.

The point is, we can apply what we know about graphs (in particular planar graphs) to convex polyhedra. Since every convex polyhedron can be represented as a planar graph, we see that Euler's formula for planar graphs holds for all convex polyhedra as well. We also can apply the same sort of reasoning we use for graphs in other contexts to convex polyhedra. For example, we know that there is no convex polyhedron with 11 vertices all of degree 3, as this would make 33/2 edges.

Example 10.3.3

Is there a convex polyhedron consisting of three triangles and six pentagons? What about three triangles, six pentagons and five heptagons (7-sided polygons)?

Solution

How many edges would such polyhedra have? For the first proposed polyhedron, the triangles would contribute a total of 9 edges, and the pentagons would contribute 30. However, this counts each edge twice (as each edge borders exactly two faces), giving 39/2 edges, an impossibility. There is no such polyhedron.

The second polyhedron does not have this obstacle. The extra 35 edges contributed by the heptagons give a total of 74/2 = 37 edges. So far so good. Now how many vertices does this supposed polyhedron have? We can use Euler's formula. There are 14 faces, so we have $v-37+14=2$ or equivalently $v=25$. But now use the vertices to count the edges again. Each vertex must have degree *at least* three (that is, each vertex joins at least three faces since the interior angle of all the polygons must be less that 180°), so the sum of the degrees of vertices is at least 75. Since the sum of the degrees must be exactly twice the number of edges, this says that there are strictly more than 37 edges. Again, there is no such polyhedron.

To conclude this application of planar graphs, consider the regular polyhedra. Above we claimed there are only five. How do we know this is true? We can prove it using graph theory.

Theorem 10.3.3: regular polyhedra

There are exactly five regular polyhedra.

Proof

Recall that a regular polyhedron has all of its faces identical regular polygons, and that each vertex has the same degree. Consider the cases, broken up by what the regular polygon might be.

Case 1: Each face is a triangle. Let f be the number of faces. There are then $3f/2$edges. Using Euler's formula we have $v-3f/2+f=2$ so $v=2+f/2$. Now each vertex has the same degree, say k. So the number of edges is also $kv/2$. Putting this together gives

$$e = \frac{3f}{2} = \frac{k(2+f/2)}{2}$$

which says

$$k = \frac{6f}{4+f}$$

We need k and f to both be positive integers. Note that $\frac{6f}{4+f}$ is an increasing function for positive f, and has a horizontal asymptote at 6. Thus the only possible values for k are 3, 4, and 5. Each of these are possible. To get $k = 3$, we need $f = 4$ (this is the tetrahedron). For $k = 4$ we take $f = 8$ (the octahedron). For $k = 5$ take $f = 20$ (the icosahedron). Thus there are exactly three regular polyhedra with triangles for faces.

Case 2: Each face is a square. Now we have $e = 4f/2 = 2f$. Using Euler's formula we get $v = 2 + f$, and counting edges using the degree k of each vertex gives us

$$e = 2f = \frac{k(2+f)}{2}$$

Solving for k gives

$$k = \frac{4f}{2+f} = \frac{8f}{4+2f}$$

This is again an increasing function, but this time the horizontal asymptote is at $k = 4$, so the only possible value that k could take is 3. This produces 6 faces, and we have a cube. There is only one regular polyhedron with square faces.

Case 3: Each face is a pentagon. We perform the same calculation as above, this time getting $e = 5f/2$ so $v = 2 + 3f/2$. Then

$$e = \frac{5f}{2} = \frac{k(2+3f/2)}{2}$$

so

$$k = \frac{10f}{4+3f}$$

Now the horizontal asymptote is at $\frac{10}{3}$. This is less than 4, so we can only hope of making $k = 3$. We can do so by using 12 pentagons, getting the dodecahedron. This is the only regular polyhedron with pentagons as faces.

Case 4: Each face is an n-gon with $n \geq 6$. Following the same procedure as above, we deduce that

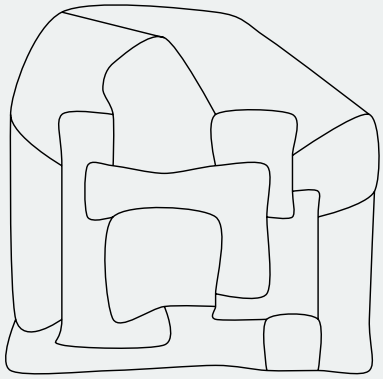
$$k = \frac{2nf}{4+(n-2)f}$$

which will be increasing to a horizontal asymptote of $\frac{2n}{n-2}$. When $n = 6$, this asymptote is at $k = 3$. Any larger value of n will give an even smaller asymptote. Therefore no regular polyhedra exist with faces larger than pentagons. [3] Notice that you can tile the plane with hexagons. This is an infinite planar graph; each vertex has degree 3. These infinitely many hexagons correspond to the limit as \(f \to\infty \) to make \(k = 3\text{.}\)

□

10.4: Coloring

Mapmakers in the fictional land of Euleria have drawn the borders of the various dukedoms of the land. To make the map pretty, they wish to color each region. Adjacent regions must be colored differently, but it is perfectly fine to color two distant regions with the same color. What is the fewest colors the mapmakers can use and still accomplish this task?



Perhaps the most famous graph theory problem is how to color maps.

> *Given any map of countries, states, counties, etc., how many colors are needed to color each region on the map so that neighboring regions are colored differently?*

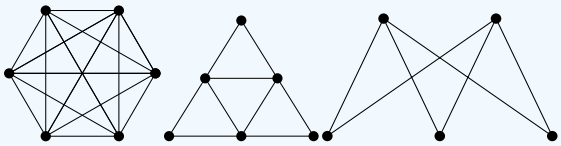
Actual map makers usually use around seven colors. For one thing, they require watery regions to be a specific color, and with a lot of colors it is easier to find a permissible coloring. We want to know whether there is a smaller palette that will work for any map.

How is this related to graph theory? Well, if we place a vertex in the center of each region (say in the capital of each state) and then connect two vertices if their states share a border, we get a graph. Coloring regions on the map corresponds to coloring the vertices of the graph. Since neighboring regions cannot be colored the same, our graph cannot have vertices colored the same when those vertices are adjacent.

In general, given any graph G, a coloring of the vertices is called (not surprisingly) a *vertex coloring*. If the vertex coloring has the property that adjacent vertices are colored differently, then the coloring is called *proper*. Every graph has a proper vertex coloring. For example, you could color every vertex with a different color. But often you can do better. The smallest number of colors needed to get a proper vertex coloring is called the *chromatic number* of the graph, written $\chi(G)$.

Example 10.4.1: chromatic numbers

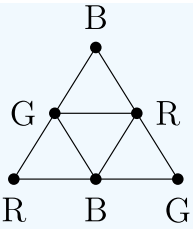
Find the chromatic number of the graphs below.



Solution

The graph on the left is K_6. The only way to properly color the graph is to give every vertex a different color (since every vertex is adjacent to every other vertex). Thus the chromatic number is 6.

The middle graph can be properly colored with just 3 colors (Red, Blue, and Green). For example:



There is no way to color it with just two colors, since there are three vertices mutually adjacent (i.e., a triangle). Thus the chromatic number is 3.

The graph on the right is just $K_{2,3}$. As with all bipartite graphs, this graph has chromatic number 2: color the vertices on the top row red and the vertices on the bottom row blue.

It appears that there is no limit to how large chromatic numbers can get. It should not come as a surprise that K_n has chromatic number n. So how could there possibly be an answer to the original map coloring question? If the chromatic number of graph can be arbitrarily large, then it seems like there would be no upper bound to the number of colors needed for any map. But there is.

The key observation is that while it is true that for any number n, there is a graph with chromatic number n, only some graphs arrive as representations of maps. If you convert a map to a graph, the edges between vertices correspond to borders between the countries. So you should be able to connect vertices in such a way where the edges do not cross. In other words, the graphs representing maps are all *planar*!

So the question is, what is the largest chromatic number of any planar graph? The answer is the best known theorem of graph theory:

Theorem 10.4.1: The Four Color Theorem

If G is a planar graph, then the chromatic number of G is less than or equal to 4. Thus any map can be properly colored with 4 or fewer colors.

We will not prove this theorem. Really. Even though the theorem is easy to state and understand, the proof is not. In fact, there is currently no "easy" known proof of the theorem. The current best proof still requires powerful computers to check an *unavoidable set* of 633 *reducible configurations*. The idea is that every graph must contain one of these reducible configurations (this fact also needs to be checked by a computer) and that reducible configurations can, in fact, be colored in 4 or fewer colors.

Coloring in General

!

The math department plans to offer 10 classes next semester. Some classes cannot run at the same time (perhaps they are taught by the same professor, or are required for seniors).

Class:	Conflicts with:
A	D I
B	D I J
C	E F I
D	A B F
E	H I
F	I
G	J
H	E I J
I	A B C E F H

Class:	Conflicts with:
J	B G H

How many different time slots are needed to teach these classes (and which should be taught at the same time)? More importantly, how could we use graph coloring to answer this question?

Cartography is certainly not the only application of graph coloring. There are plenty of situations in which you might wish partition the objects in question so that related objects are not in the same set. For example, you might wish to store chemicals safely. To avoid explosions, certain pairs of chemicals should not be stored in the same room. By coloring a graph (with vertices representing chemicals and edges representing potential negative interactions), you can determine the smallest number of rooms needed to store the chemicals.

Here is a further example:

Example 10.4.3

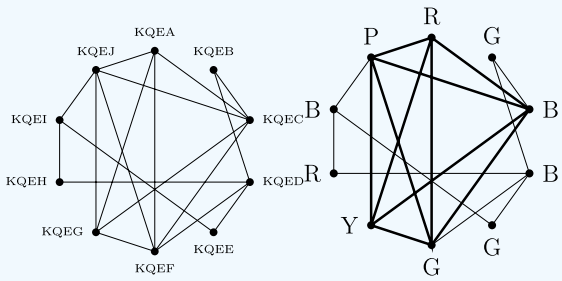
Radio stations broadcast their signal at certain frequencies. However, there are a limited number of frequencies to choose from, so nationwide many stations use the same frequency. This works because the stations are far enough apart that their signals will not interfere; no one radio could pick them up at the same time.

Suppose 10 new radio stations are to be set up in a currently unpopulated (by radio stations) region. The radio stations that are close enough to each other to cause interference are recorded in the table below. What is the fewest number of frequencies the stations could use.

	KQEA	KQEB	KQEC	KQED	KQEE	KQEF	KQEG	KQEH	KQEI	KQEJ
KQEA			X			X	X			X
KQEB			X	X						
KQEC	X					X	X			X
KQED		X			X	X		X		
KQEE				X					X	
KQEF	X		X	X			X			X
KQEG	X		X			X				X
KQEH				X					X	
KQEI					X			X		X
KQEJ	X		X			X	X		X	

Solution

Represent the problem as a graph with vertices as the stations and edges when two stations are close enough to cause interference. We are looking for the chromatic number of the graph. Vertices that are colored identically represent stations that can have the same frequency.



This graph has chromatic number 5. A proper 5-coloring is shown on the right. Notice that the graph contains a copy of the complete graph K_5 so no fewer than 5 colors can be used.

In the example above, the chromatic number was 5, but this is not a counterexample to the Four Color Theorem, since the graph representing the radio stations is not planar. It would be nice to have some quick way to find the chromatic number of a (possibly

non-planar) graph. It turns out nobody knows whether an efficient algorithm for computing chromatic numbers exists.

While we might not be able to find the exact chromatic number of graph easily, we can often give a reasonable range for the chromatic number. In other words, we can give upper and lower bounds for chromatic number.

This is actually not very difficult: for every graph G, the chromatic number of G is at least 1 and at most the number of vertices of G.

What? You want *better* bounds on the chromatic number? Well you are in luck.

A *clique* in a graph is a set of vertices all of which are pairwise adjacent. In other words, a clique of size n is just a copy of the complete graph K_n. We define the *clique number* of a graph to be the largest n for which the graph contains a clique of size n. Any clique of size n cannot be colored with fewer than n colors, so we have a nice lower bound:

Theorem 10.4.2

The chromatic number of a graph G is at least the clique number of G.

There are times when the chromatic number of G is *equal* to the clique number. These graphs have a special name; they are called *perfect*. If you know that a graph is perfect, then finding the chromatic number is simply a matter of searching for the largest clique.[4] There are special classes of graphs which can be proved to be perfect. One such class is the set of *chordal* graphs, which have the property that every cycle in the graph contains a *chord*—an edge between two vertices in of the cycle which are not adjacent in the cycle. However, not all graphs are perfect.

For an upper bound, we can improve on "the number of vertices" by looking to the degrees of vertices. Let $\Delta(G)$ be the largest degree of any vertex in the graph G. One reasonable guess for an upper bound on the chromatic number is $\chi(G) \leq \Delta(G)+1$. Why is this reasonable? Starting with any vertex, it together with all of its neighbors can always be colored in $\Delta(G)+1$ colors, since at most we are talking about $\Delta(G)+1$ vertices in this set. Now fan out! At any point, if you consider an already colored vertex, some of its neighbors might be colored, some might not. But no matter what, that vertex and its neighbors could all be colored distinctly, since there are at most $\Delta(G)$ neighbors, plus the one vertex being considered.

In fact, there are examples of graphs for which $\chi(G) = \Delta(G)+1$. For any n, the complete graph K_n has chromatic number n, but $\Delta(K_n) = n-1$ (since every vertex is adjacent to every *other* vertex). Additionally, any *odd* cycle will have chromatic number 3, but the degree of every vertex in a cycle is 2. It turns out that these are the only two types of examples where we get equality, a result known as Brooks' Theorem.

Theorem 10.4.3: Brooks' Theorem

Any graph G satisfies $\chi(G) \leq \Delta(G)$, unless G is a complete graph or an odd cycle, in which case $\chi(G) = \Delta(G)+1$.

The proof of this theorem is *just* complicated enough that we will not present it here (although you are asked to prove a special case in the exercises). The adventurous reader is encouraged to find a book on graph theory for suggestions on how to prove the theorem.

Coloring Edges

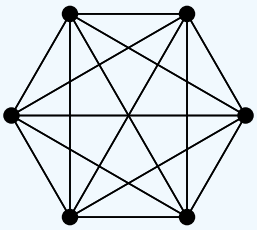
The chromatic number of a graph tells us about coloring vertices, but we could also ask about coloring edges. Just like with vertex coloring, we might insist that edges that are adjacent must be colored differently. Here, we are thinking of two edges as being adjacent if they are incident to the same vertex. The least number of colors required to properly color the edges of a graph G is called the *chromatic index* of G, written $\chi'(G)$.

Example 10.4.3

Six friends decide to spend the afternoon playing chess. Everyone will play everyone else once. They have plenty of chess sets but nobody wants to play more than one game at a time. Games will last an hour (thanks to their handy chess clocks). How many hours will the tournament last?

Solution

Represent each player with a vertex and put an edge between two players if they will play each other. In this case, we get the graph K_6:



We must color the edges; each color represents a different hour. Since different edges incident to the same vertex will be colored differently, no player will be playing two different games (edges) at the same time. Thus we need to know the chromatic index of K_6.

Notice that for sure $\chi'(K_6) \geq 5$, since there is a vertex of degree 5. It turns out 5 colors is enough (go find such a coloring). Therefore the friends will play for 5 hours.

Interestingly, if one of the friends in the above example left, the remaining 5 chess-letes would still need 5 hours: the chromatic index of K_5 is also 5.

In general, what can we say about chromatic index? Certainly $\chi'(G) \geq \Delta(G)$. But how much higher could it be? Only a little higher.

Theorem 10.4.4: Vizing's Theorem

For any graph G, the chromatic index $\chi'(G)$ is either $\Delta(G)$ or $\Delta(G)+1$.

At first this theorem makes it seem like chromatic index might not be very interesting. However, deciding which case a graph is in is not always easy. Graphs for which $\chi'(G) = \Delta(G)$ are called *class 1*, while the others are called *class 2*. Bipartite graphs always satisfy $\chi'(G) = \Delta(G)$, so are class 1 (this was proved by König in 1916, decades before Vizing proved his theorem in 1964). In 1965 Vizing proved that all planar graphs with $\Delta(G) \geq 8$ are of class 1, but this does not hold for all planar graphs with $2 \leq \Delta(G) \leq 5$. Vizing conjectured that all planar graphs with $\Delta(G) = 6$ or $\Delta(G) = 7$ are class 1; the $\Delta(G) = 7$ case was proved in 2001 by Sanders and Zhao; the $\Delta(G) = 6$ case is still open.

There is another interesting way we might consider coloring edges, quite different from what we have discussed so far. What if we colored every edge of a graph either red or blue. Can we do so without, say, creating a *monochromatic* triangle (i.e., an all red or all blue triangle)? Certainly for some graphs the answer is yes. Try doing so for K_4. What about K_5? K_6? How far can we go?

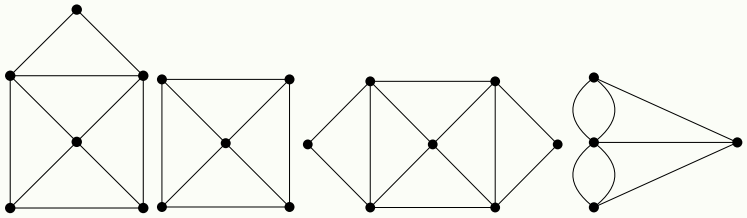
The answer to the above problem is known and is a fun problem to do as an exercise. We could extend the question in a variety of ways. What if we had three colors? What if we were trying to avoid other graphs. The surprising fact is that very little is known about these questions. For example, we know that you need to go up to K_{17} in order to force a monochromatic triangle using three colors, but nobody knows how big you need to go with more colors. Similarly, we know that using two colors K_{18} is the smallest graph that forces a monochromatic copy of K_4, but the best we have to force a monochromatic K_5 is a range, somewhere from K_{43} to K_{49}. If you are interested in these sorts of questions, this area of graph theory is called Ramsey theory. Check it out.

10.5: Euler Paths and Circuits

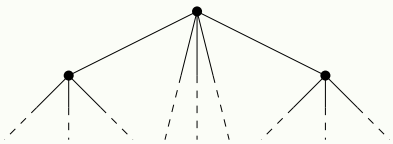
Investigate!

An *Euler path*, in a graph or multigraph, is a walk through the graph which uses every edge exactly once. An *Euler circuit* is an Euler path which starts and stops at the same vertex. Our goal is to find a quick way to check whether a graph (or multigraph) has an Euler path or circuit.

1. Which of the graphs below have Euler paths? Which have Euler circuits?

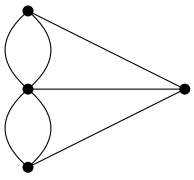


2. List the degrees of each vertex of the graphs above. Is there a connection between degrees and the existence of Euler paths and circuits?
3. Is it possible for a graph with a degree 1 vertex to have an Euler circuit? If so, draw one. If not, explain why not. What about an Euler path?
4. What if every vertex of the graph has degree 2. Is there an Euler path? An Euler circuit? Draw some graphs.
5. Below is *part* of a graph. Even though you can only see some of the vertices, can you deduce whether the graph will have an Euler path or circuit?



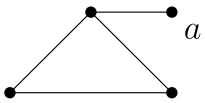
If we start at a vertex and trace along edges to get to other vertices, we create a *walk* through the graph. More precisely, a *walk* in a graph is a sequence of vertices such that every vertex in the sequence is adjacent to the vertices before and after it in the sequence. If the walk travels along every edge exactly once, then the walk is called an *Euler path* (or *Euler walk*). If, in addition, the starting and ending vertices are the same (so you trace along every edge exactly once and end up where you started), then the walk is called an *Euler circuit* (or *Euler tour*). Of course if a graph is not connected, there is no hope of finding such a path or circuit. For the rest of this section, assume all the graphs discussed are connected.

The bridges of Königsberg problem is really a question about the existence of Euler paths. There will be a route that crosses every bridge exactly once if and only if the graph below has an Euler path:



This graph is small enough that we could actually check every possible walk that does not reuse edges, and in doing so convince ourselves that there is no Euler path (let alone an Euler circuit). On small graphs which do have an Euler path, it is usually not difficult to find one. Our goal is to find a quick way to check whether a graph has an Euler path or circuit, even if the graph is quite large.

One way to guarantee that a graph does *not* have an Euler circuit is to include a "spike," a vertex of degree 1.



The vertex a has degree 1, and if you try to make an Euler circuit, you see that you will get stuck at the vertex. It is a dead end. That is, unless you start there. But then there is no way to return, so there is no hope of finding an Euler circuit. There is however an Euler path. It starts at the vertex a, then loops around the triangle. You will end at the vertex of degree 3.

You run into a similar problem whenever you have a vertex of any odd degree. If you start at such a vertex, you will not be able to end there (after traversing every edge exactly once). After using one edge to leave the starting vertex, you will be left with an even number of edges emanating from the vertex. Half of these could be used for returning to the vertex, the other half for leaving. So you return, then leave. Return, then leave. The only way to use up all the edges is to use the last one by leaving the vertex. On the other hand, if you have a vertex with odd degree that you do not start a path at, then you will eventually get stuck at that vertex. The path will use pairs of edges incident to the vertex to arrive and leave again. Eventually all but one of these edges will be used up, leaving only an edge to arrive by, and none to leave again.

What all this says is that if a graph has an Euler path and two vertices with odd degree, then the Euler path must start at one of the odd degree vertices and end at the other. In such a situation, every other vertex *must* have an even degree since we need an equal number of edges to get to those vertices as to leave them. How could we have an Euler circuit? The graph could not have any odd degree vertex as an Euler path would have to start there or end there, but not both. Thus for a graph to have an Euler circuit, all vertices must have even degree.

The converse is also true: if all the vertices of a graph have even degree, then the graph has an Euler circuit, and if there are exactly two vertices with odd degree, the graph has an Euler path. To prove this is a little tricky, but the basic idea is that you will never get stuck because there is an “outbound” edge for every “inbound” edge at every vertex. If you try to make an Euler path and miss some edges, you will always be able to “splice in” a circuit using the edges you previously missed.

Definitions: Euler Paths and Circuits

- A graph has an Euler circuit if and only if the degree of every vertex is even.
- A graph has an Euler path if and only if there are at most two vertices with odd degree.

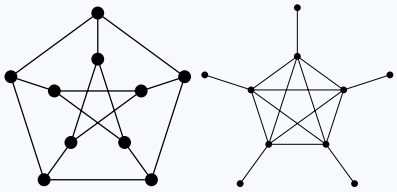
Since the bridges of Königsberg graph has all four vertices with odd degree, there is no Euler path through the graph. Thus there is no way for the townspeople to cross every bridge exactly once.

Hamilton Paths

Suppose you wanted to tour Königsberg in such a way where you visit each land mass (the two islands and both banks) exactly once. This can be done. In graph theory terms, we are asking whether there is a path which visits every vertex exactly once. Such a path is called a *Hamilton path* (or *Hamiltonian path*). We could also consider *Hamilton cycles*, which are Hamliton paths which start and stop at the same vertex.

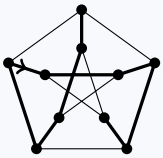
Example 10.5.1

Determine whether the graphs below have a Hamilton path.



Solution

The graph on the left has a Hamilton path (many different ones, actually), as shown here:



The graph on the right does not have a Hamilton path. You would need to visit each of the “outside” vertices, but as soon as you visit one, you get stuck. Note that this graph does not have an Euler path, although there are graphs with Euler paths but

no Hamilton paths.

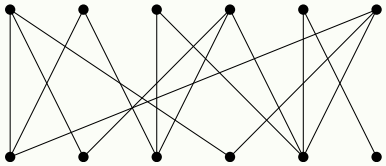
It appears that finding Hamilton paths would be easier because graphs often have more edges than vertices, so there are fewer requirements to be met. However, nobody knows whether this is true. There is no known simple test for whether a graph has a Hamilton path. For small graphs this is not a problem, but as the size of the graph grows, it gets harder and harder to check wither there is a Hamilton path. In fact, this is an example of a question which as far as we know is too difficult for computers to solve; it is an example of a problem which is NP-complete.

10.6: Matching in Bipartite Graphs

Investigate!

Given a bipartite graph, a *matching* is a subset of the edges for which every vertex belongs to exactly one of the edges. Our goal in this activity is to discover some criterion for when a bipartite graph has a matching.

Does the graph below contain a matching? If so, find one.



Not all bipartite graphs have matchings. Draw as many fundamentally different examples of bipartite graphs which do NOT have matchings. Your goal is to find all the possible obstructions to a graph having a perfect matching. Write down the *necessary* conditions for a graph to have a matching (that is, fill in the blank: If a graph has a matching, then). Then ask yourself whether these conditions are sufficient (is it true that if , then the graph has a matching?).

We conclude with one more example of a graph theory problem to illustrate the variety and vastness of the subject.

Suppose you have a bipartite graph G. This will consist of two sets of vertices A and B with some edges connecting some vertices of A to some vertices in B (but of course, no edges between two vertices both in A or both in B). A *matching of* A is a subset of the edges for which each vertex of A belongs to exactly one edge of the subset, and no vertex in B belongs to more than one edge in the subset. In practice we will assume that $|A| = |B|$ (the two sets have the same number of vertices) so this says that every vertex in the graph belongs to exactly one edge in the matching.[5] Note: what we are calling a *matching* is sometimes called a *perfect matching* or *complete matching*. This is because in it interesting to look at non-perfect matchings as well. We will call those *partial* matchings.

Some context might make this easier to understand. Think of the vertices in A as representing students in a class, and the vertices in B as representing presentation topics. We put an edge from a vertex $a \in A$ to a vertex $b \in B$ if student a would like to present on topic b. Of course, some students would want to present on more than one topic, so their vertex would have degree greater than 1. As the teacher, you want to assign each student their own unique topic. Thus you want to find a matching of A: you pick some subset of the edges so that each student gets matched up with exactly one topic, and no topic gets matched to two students.[6] The standard example for matchings used to be the *marriage problem* in which \(A\) consisted of the men in the town, \(B\) the women, and an edge represented a marriage that was agreeable to both parties. A matching then represented a way for the town elders to marry off everyone in the town, no polygamy allowed. We have chosen a more progressive context for the sake of political correctness.

The question is: when does a bipartite graph contain a matching of A? To begin to answer this question, consider what could prevent the graph from containing a matching. This will not necessarily tell us a condition when the graph *does* have a matching, but at least it is a start.

One way G could not have a matching is if there is a vertex in A not adjacent to any vertex in B (so having degree 0). What else? What if two students both like the same one topic, and no others? Then after assigning that one topic to the first student, there is nothing left for the second student to like, so it is very much as if the second student has degree 0. Or what if three students like only two topics between them. Again, after assigning one student a topic, we reduce this down to the previous case of two students liking only one topic. We can continue this way with more and more students.

It should be clear at this point that if there is every a group of n students who as a group like $n-1$ or fewer topics, then no matching is possible. This is true for any value of n, and any group of n students.

To make this more graph-theoretic, say you have a set $S \subseteq A$ of vertices. Define $N(S)$ to be the set of all the *neighbors* of vertices in S. That is, $N(S)$ contains all the vertices (in B) which are adjacent to at least one of the vertices in S. (In the student/topic graph, $N(S)$ is the set of topics liked by the students of S.) Our discussion above can be summarized as follows:

Matching Condition

If a bipartite graph $G = \{A, B\}$ has a matching of A, then

$$|N(S)| \geq |S|$$

for all $S \subseteq A$.

Is the converse true? Suppose G satisfies the matching condition $|N(S)| \geq |S|$ for all $S \subseteq A$ (every set of vertices has at least as many neighbors than vertices in the set). Does that mean that there is a matching? Surprisingly, yes. The obvious necessary condition is also sufficient.[7] This happens often in graph theory. If you can avoid the obvious counterexamples, you often get what you want. This is a theorem first proved by Philip Hall in 1935.[8] There is also an infinite version of the theorem which was proved by Marshal Hall, Jr. The name is a coincidence though as the two Halls are not related.

Hall's Marriage Theorem

Let G be a bipartite graph with sets A and B. Then G has a matching of A if and only if

$$|N(S)| \geq |S|$$

for all $S \subseteq A$.

There are quite a few different proofs of this theorem – a quick internet search will get you started.

In addition to its application to marriage and student presentation topics, matchings have applications all over the place. We conclude with one such example.

Example 10.6.1

Suppose you deal 52 regular playing cards into 13 piles of 4 cards each. Prove that you can always select one card from each pile to get one of each of the 13 card values Ace, 2, 3, …, 10, Jack, Queen, and King.

Solution

Doing this directly would be difficult, but we can use the matching condition to help. Construct a graph G with 13 vertices in the set A, each representing one of the 13 card values, and 13 vertices in the set B, each representing one of the 13 piles. Draw an edge between a vertex $a \in A$ to a vertex $b \in B$ if a card with value a is in the pile b. Notice that we are just looking for a matching of A; each value needs to be found in the piles exactly once.

We will have a matching if the matching condition holds. Given any set of card values (a set $S \subseteq A$) we must show that $|N(S)| \geq |S|$. That is, the number of piles that contain those values is at least the number of different values. But what if it wasn't? Say $|S| = k$. If $|N(S)| < k$, then we would have fewer than $4k$ different cards in those piles (since each pile contains 4 cards). But there are $4k$ cards with the k different values, so at least one of these cards must be in another pile, a contradiction. Thus the matching condition holds, so there is a matching, as required.

10.7: Weighted Graphs and Dijkstra's Algorithm

Investigate!

In the table, the time it takes to travel between various locations by bus in South Bend is given. Incorporate this information in a graph, and then find shortest paths from the airport to every other location.

	Saint Mary's	Holy Cross	Notre Dame	Ranjan's House	Chocolate Cafe	Crooked Ewe	Airport
Saint Mary's	0	3	7	-	-	-	17
Holy Cross		0	6	-	11	-	-
Notre Dame			0	8	-	14	-
Ranjan's House				0	-	15	22
Chocolate Cafe					0	12	15
Crooked Ewe						0	-
Airport							0

Definition

A graph with a number (usually positive) assigned to each edge is called a **weighted graph**. (A graph without weights can be thought of as a weighted graph with all weights equal to 1.) We denote the **weight** between vertices u and v by $w(u,v)$.

In the previous example, the weights represented distances. What else could we represent using weights?

In many situations, we want to find a **shortest path** (or **path of least weight**) between two locations. Dijkstra's algorithm gives us a way to do this.

Dijkstra's algorithm

- Input: a weighted graph, G, with a *source vertex* s
  - for each vertex v in G:
    - $dist(v) := \infty$
    - $prev(v) := undefined$
  - $dist(s) := 0$
  - $Q :=$ set of all vertices in G
  - while Q is not empty:
    - $u :=$ vertex in Q with smallest distance
    - remove u from Q
    - for each neighbor v of u
      - $alt := dist(u) + w(u,v)$
      - if $alt < dist(v)$
        - $dist(v) := alt$
        - $prev(v) := u$
  - return $dist(), prev()$

Remark: If you only want to know the distance from the source to a particular vertex, you can terminate the algorithm when that vertex is removed from Q.

Challenge: Find a big-O estimate for the number of operations (additions and comparisons) used by Dijkstra's algorithm.

Exercise 10.7.1

Saint Mary's once had tunnels connecting various buildings on campus. The tunnels and their lengths are as follows (and definitely not accurate): Regina to McCandless (400 ft), Regina to Student Center (200), McCandless to Student Center (100), McCandless to Angela (500), Student Center to Angela (800), Student Center to Library (1000), Angela to Library (200), Angela to Madeleva (600), Library to Madeleva (300). **Find a shortest path from Regina to Madeleva using Dijkstra's Algorithm.**

Theorem 10.7.2

Dijkstra's Algorithm finds a shortest path between two vertices in a simple undirected weighted graph.

Proof

We will prove the theorem by induction on $|V \setminus Q|$. The first vertex removed from Q is s. In this case $|V \setminus Q| = 1$ and Dijkstra's algorithm tells us that the distance from the source to s (ie from s to itself) is 0. Therefore, the base case is true.

The inductive hypothesis is that for any vertex not in Q, the distance assigned to that vertex by the algorithm is in fact the minimum distance from the source to that vertex.

Let u be the most recent vertex removed from Q. By the inductive hypothesis, the algorithm has provided the minimum distance from the source for every vertex in $V \setminus Q$ besides u.

Suppose by contradiction that a shortest path P from s to u has length less than $dist(u)$. In other words, $length(P) < dist(u)$. Let xy be the first edge along P that isn't in $V \setminus Q$ and let P_x be the sub-path of P from s to x. Then

$$length(P_x) + w(x, y) \leq length(P) ,$$

and by the induction hypothesis

$$dist(x) + w(x, y) \leq length(P) .$$

Since y is adjacent to x, the algorithm recalculates $dist(y)$, so

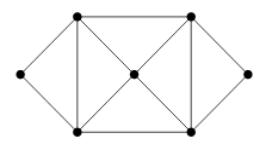
$$dist(y) \leq dist(x) + w(x, y) .$$

Combining these inequalities, we see that $dist(y) < dist(u)$. But the algorithm removed u from Q and not y, so we must have that $dist(u) \leq dist(y)$. This is a contradiction, and the proof is complete.

10.8: Trees

Investigate!

Consider the graph drawn below.

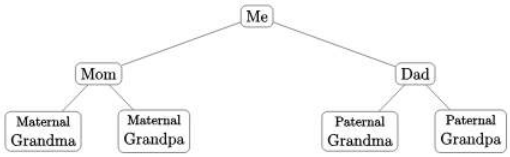


1. Find a subgraph with the smallest number of edges that is still connected and contains all the vertices.
2. Find a subgraph with the largest number of edges that doesn't contain any cycles.
3. What do you notice about the number of edges in your examples above? Is this a coincidence?

Definition

A **tree** is a connected graph with no cycles. (Alternatively, a tree is a connected acyclic graph.)

A **forest** is a graph containing no cycles. Note that this means a connected forest is a tree.



So far so good, but while your grandparents are (probably) not blood-relatives, if we go back far enough, it is likely that they did have *some* common ancestor. If you trace the tree back from you to that common ancestor, then down through your other grandparent, you would have a cycle, and thus the graph would not be a tree.

You might also have seen something called a *decision tree* before (for example when deciding whether a series converges or diverges). Sometimes these too contain cycles, as the decision for one node might lead you back to a previous step.

Both the examples of trees above also have another feature worth mentioning: there is a clear order to the vertices in the tree. In general, there is no reason for a tree to have this added structure, although we can impose such a structure by considering ***rooted trees***, where we simply designate one vertex as the *root*. We will consider such trees in more detail later in this section.

Properties of Trees

We wish to really understand trees. This means we should discover properties of trees; what makes them special and what is special about them.

A tree is an connected graph with no cycles. Is there anything else we can say? It would be nice to have other equivalent conditions for a graph to be a tree. That is, we would like to know whether there are any graph theoretic properties that all trees have, and perhaps even that *only* trees have.

To get a feel for the sorts of things we can say, we will consider three *propositions* about trees. These will also illustrate important proof techniques that apply to graphs in general, and happen to be a little easier for trees.

Our first proposition gives an alternate definition for a tree. That is, it gives necessary and sufficient conditions for a graph to be a tree.

Proposition 10.8.1

A graph T is a tree if and only if between every pair of distinct vertices there is a unique path.

Proof

This is an “if and only if” statement, so we must prove two implications. We start by proving that if T is a tree, then between every pair of distinct vertices there is a unique path.

Assume T is a tree, and let u and v be distinct vertices (if T only has one vertex, then the conclusion is satisfied automatically). We must show two things to show that there is a unique path between u and v: that there is a path, and that there is not more than one path. The first of these is automatic, since T is a tree, it is connected, so there is a path between any pair of vertices.

To show the path is unique, we suppose there are two paths between u and v, and get a contradiction. The two paths might start out the same, but since they are different, there is some first vertex u' after which the two paths diverge. However, since the two paths both end at v, there is some first vertex after u' that they have in common, call it v'. Now consider the two paths from u' to v'. Taken together, these form a cycle, which contradicts our assumption that T is a tree.

Now we consider the converse: if between every pair of distinct vertices of T there is a unique path, then T is a tree. So assume the hypothesis: between every pair of distinct vertices of T there is a unique path. To prove that T is a tree, we must show it is connected and contains no cycles.

The first half of this is easy: T is connected, because there is a path between every pair of vertices. To show that T has no cycles, we assume it does, for the sake of contradiction. Let u and v be two distinct vertices in a cycle of T. Since we can get from u to v by going clockwise or counterclockwise around the cycle, there are two paths from u and v, contradicting our assumption.

We have established both directions so we have completed the proof.

Read the proof above very carefully. Notice that both directions had two parts: the existence of paths, and the uniqueness of paths (which related to the fact there were no cycles). In this case, these two parts were really separate. In fact, if we just considered graphs with no cycles (a forest), then we could still do the parts of the proof that explore the uniqueness of paths between vertices, even if there might not *exist* paths between vertices.

This observation allows us to state the following *corollary*:

Corollary 10.8.2

A graph is a forest if and only if there is at most one path between every pair of vertices.

Proposition 10.8.3

Any tree with at least two vertices has at least two vertices of degree one.

Proof

We give a proof by contradiction. Let T be a tree with at least two vertices, and suppose, contrary to stipulation, that there are not two vertices of degree one.

Let P be a path in T of longest possible length. Let u and v be the endpoints of the path. Since T does not have two vertices of degree one, at least one of these must have degree two or higher. Say that it is u. We know that u is adjacent to a vertex in the path P, but now it must also be adjacent to another vertex, call it u'.

Where is u'? It cannot be a vertex of P, because if it was, there would be two distinct paths from u to u': the edge between them, and the first part of P (up to u'). But u' also cannot be outside of P, for if it was, there would be a path from u' to v that was longer than P, which has longest possible length.

This contradiction proves that there must be at least two vertices of degree one. In fact, we can say a little more: u and v must *both* have degree one.

The proposition is quite useful when proving statements about trees, because we often prove statements about trees by *induction*. To do so, we need to reduce a given tree to a smaller tree (so we can apply the inductive hypothesis). Getting rid of a vertex of degree one is an obvious choice, and now we know there is always one to get rid of.

To illustrate how induction is used on trees, we will consider the relationship between the number of vertices and number of edges in trees. Is there a tree with exactly 7 vertices and 7 edges? Try to draw one? Could a tree with 7 vertices have only 5 edges? There is a good reason that these seem impossible to draw.

Proposition 10.8.4

Let T be a tree with v vertices and e edges. Then $e = v - 1$.

Proof

We will give a proof by induction on the number of vertices in the tree. That is, we will prove that every tree with v vertices has exactly $v - 1$ edges, and then use induction to show this is true for all $v \geq 1$.

For the base case, consider all trees with $v = 1$ vertices. There is only one such tree: the graph with a single isolated vertex. This graph has $e = 0$ edges, so we see that $e = v - 1$ as needed.

Now for the inductive case, fix $k \geq 1$ and assume that all trees with $v = k$ vertices have exactly $e = k - 1$ edges. Now consider an arbitrary tree T with $v = k + 1$ vertices. By Proposition 3, T has a vertex v_0 of degree one. Let T′ be the tree resulting from removing v_0 from T (together with its incident edge). Since we removed a leaf, T′ is still a tree (the unique paths between pairs of vertices in T′ are the same as the unique paths between them in T).

Now T′ has k vertices, so by the inductive hypothesis, has $k - 1$ edges. What can we say about T? Well, it has one more edge than T′, so it has k edges. But this is exactly what we wanted: $v = k + 1$, $e = k$ so indeed $e = v - 1$. This completes the proof.

There is a very important feature of this induction proof that is worth noting. Induction makes sense for proofs about graphs because we can think of graphs as growing into larger graphs. However, this does NOT work. It would not be correct to start with a tree with k vertices, and then add a new vertex and edge to get a tree with $k + 1$ vertices, and note that the number of edges also grew by one. Why is this bad? Because how do you know that *every* tree with $k + 1$ vertices is the result of adding a vertex to your arbitrary starting tree? You don't!

The point is that whenever you give an induction proof that a statement about graphs that holds for all graphs with v vertices, you must start with an arbitrary graph with $v + 1$ vertices, then *reduce* that graph to a graph with v vertices, to which you can apply your inductive hypothesis.

Rooted Trees

So far, we have thought of trees only as a particular kind of graph. However, it is often useful to add additional structure to trees to help solve problems. Data is often structured like a tree. This book, for example, has a tree structure: draw a vertex for the book itself. Then draw vertices for each chapter, connected to the book vertex. Under each chapter, draw a vertex for each section, connecting it to the chapter it belongs to. The graph will not have any cycles; it will be a tree. But a tree with clear hierarchy which is not present if we don't identify the book itself as the “top”.

As soon as one vertex of a tree is designated as the ***root***, then every other vertex on the tree can be characterized by its position relative to the root. This works because between any two vertices in a tree, there is a unique path. So from any vertex, we can travel back to the root in exactly one way. This also allows us to describe how distinct vertices in a rooted tree are related.

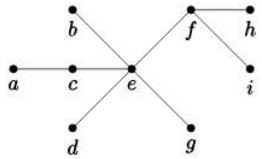
If two vertices are adjacent, then we say one of them is the ***parent*** of the other, which is called the ***child*** of the parent. Of the two, the parent is the vertex that is closer to the root. Thus the root of a tree is a parent, but is not the child of any vertex (and is unique in this respect: all non-root vertices have *exactly one* parent).

Not surprisingly, the child of a child of a vertex is called the ***grandchild*** of the vertex (and it is the ***grandparent***). More in general, we say that a vertex v is a ***descendent*** of a vertex u provided u is a vertex on the path from v to the root. Then we would call u an ***ancestor*** of v.

For most trees (in fact, all except paths with one end the root), there will be pairs of vertices neither of which is a descendant of the other. We might call these cousins or siblings. In fact, vertices u and v are called ***siblings*** provided they have the same parent. Note that siblings are never adjacent (do you see why?).

Example 10.8.5

Consider the tree below.



If we designate vertex f as the root, then e, h, and i are the children of f, and are siblings of each other. Among the other things we can say are that a is a child of c, and a descendant of f. The vertex g is a descendant of f, in fact, is a grandchild of f. Vertices g and d are siblings, since they have the common parent e.

Notice how this changes if we pick a different vertex for the root. If a is the root, then its lone child is c, which also has only one child, namely e. We would then have f the child of ee (instead of the other way around), and f is the descendant of a, instead of the ancestor. f and g are now siblings.

Example 10.8.6

Explain why every tree is a bipartite graph.

Solution

To show that a graph is bipartite, we must divide the vertices into two sets A and B so that no two vertices in the same set are adjacent. Here is an algorithm that does just this.

Designate any vertex as the root. Put this vertex in set A. Now put all of the children of the root in set B. None of these children are adjacent (they are siblings), so we are good so far. Now put into A every child of every vertex in B (i.e., every grandchild of the root). Keep going until all vertices have been assigned one of the sets, alternating between A and B every "generation." That is, a vertex is in set B if and only if it is the child of a vertex in set A.

The key to how we partitioned the tree in the example was to know which vertex to assign to a set next. We chose to visit all vertices in the same generation before any vertices of the next generation. This is usually called a ***breadth first search*** (we say "search" because you often traverse a tree looking for vertices with certain properties).

In contrast, we could also have partitioned the tree in a different order. Start with the root, put it in A. Then look for one child of the root to put in B. Then find a child of that vertex, into A, and then find its child, into B, and so on. When you get to a vertex with no children, retreat to its parent and see if the parent has any other children. So we travel as far from the root as fast as possible, then backtrack until we can move forward again. This is called ***depth first search***.

These algorithmic explanations can serve as a proof that every tree is bipartite, although care needs to be spent to prove that the algorithms are *correct*. Another approach to prove that all trees are bipartite, using induction, is requested in the exercises.

Spanning Trees

One of the advantages of trees is that they give us a few simple ways to travel through the vertices. If a connected graph is not a tree, then we can still use these traversal algorithms if we identify a subgraph that *is* a tree.

First we should consider if this even makes sense. Given any connected graph G ,will there always be a subgraph that is a tree? Well, that is actually too easy: you could just take a single edge of G. If we want to use this subgraph to tell us how to visit all vertices, then we want our subgraph to include all of the vertices. We call such a tree a ***spanning tree***. It turns out that every connected graph has one (and usually many).

Definition

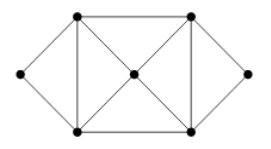
Given a connected graph G, a **spanning tree** of G is a subgraph of G which is a tree and includes all the vertices of G.

How do we know? We can give an algorithm for *finding* a spanning tree! Start with the graph connected graph G. If there is no cycle, then the G is already a tree and we are done. If there is a cycle, let e be any edge in that cycle and consider the new graph $G_1 = G - e$ (i.e., the graph you get by deleting e). This graph is still connected since e belonged to a cycle, there were at least two paths between its incident vertices. Now repeat: if G_1 has no cycles, we are done, otherwise define G_2 to be $G_1 - e_1$, where e_1 is an edge in a cycle in G_1. Keep going. This process must eventually stop, since there are only a finite number of edges to remove. The result will be a tree, and since we never removed any vertex, a *spanning* tree.

This is by no means the only algorithm for finding a spanning tree. You could have started with the empty graph and added edges that belong to G as long as adding them would not create a cycle. You have some choices as to which edges you add first: you could always add an edge adjacent to edges you have already added (after the first one, of course), or add them using some other order. Which spanning tree you end up with depends on these choices.

Example 10.8.7

Find two different spanning trees of this graph.



We will present some algorithms related to trees in the next section.

10.9: Tree Traversal

Definition

An **ordered rooted tree** is a rooted tree in which the children of each internal vertex have an order (generally from left to right).

investigate!

Create an ordered rooted tree for the expression $3(y-z)^2+\frac{4-x}{2}$. Each vertex should either be assigned a number or an operation.

Mathematical expressions can be ambiguous (as many internet memes show), and the ambiguity can be removed by strict adherence to an order of operations or by complete use of parentheses (called **infix notation**). There are other ways of writing expressions; we will also consider **prefix** and **postfix notation**. Each of these ways of writing a mathematical expression can be derived from an ordered rooted tree for that expression.

Tree traversal algorithms

Definition

A **tree traversal algorithm** is a method for systematically visiting every vertex of an ordered rooted tree.

We discuss three such algorithms below.

preorder traversal algorithm

- Input: T, an ordered rooted tree with root r
- Return r
- For each child v of r, from left to right:
  - Traverse subtree of T with root v using preorder

postorder traversal algorithm

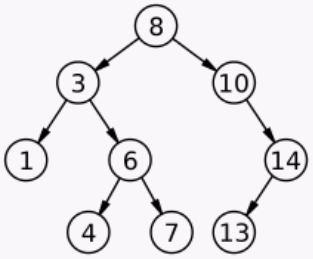
- Input: T, an ordered rooted tree with root r
- For each child v of r, from left to right:
  - Traverse subtree of T with root v using postorder
- Return r

Inorder traversal algorithm

- Input: T, an ordered rooted tree with root r
- If r is a leaf, then return r
- Else, let L be the leftmost child of r
  - Traverse subtree of T with root L using inorder
  - Return r
  - For each child v of r except L from left to right:
    - Traverse subtree of T with root v using inorder

Exercise 10.9.1

Determine the preorder, inorder, and postorder traversals of the ordered rooted tree below.



Answer

Preorder: 8, 3, 1, 6, 4, 7, 10, 14, 13

Inorder: 1, 3, 4, 6, 7, 8, 13, 14, 10

Postorder: 1, 4, 7, 6, 3, 13, 14, 10, 8

In fact, there is a simpler way to determine these traversals. First, draw a closed curve around the rooted tree, hugging both sides of each edge. To get the preorder traversal, simply list each vertex the first time it is passed. For postorder, list the vertices the last time they are passed. For inorder, list leaves the first time they are passed and internal vertices the second time.

Exercise 10.9.2

Determine the **prefix form** and **postfix form** of the mathematical expression above by traversing the ordered rooted tree you created in preorder and postorder, respectively. Use $\uparrow$ to denote exponentiation.

Determine the **infix form** of the expression by traversing the tree in inorder, including all parentheses

To evaluate an expression in prefix form, notice that an operator precedes the numbers it is applied to. Therefore, we can read right to left, and whenever we encounter an operator preceded immediately by two numbers we can perform the operation. Likewise, we can evaluate an expression in postfix form by reading left to right and performing an operation when we encounter an operator immediately preceded by two numbers.

Example 10.9.1

1. Evaluate the following expression written in prefix form: $- + * 4\,3\,5 \,/\, \uparrow 2\,2\,4$.
2. Evaluate the following expression written in postfix form: $8\,6\,1 * - 3 \uparrow 10\,5 \,/\, -$.

Tags recommended by the template: article:topic

10.10: Spanning Tree Algorithms

Definition

Given a connected graph G, a **spanning tree** of G is a subgraph of G which is a tree and includes all the vertices of G.

We also provided the ideas of two algorithms to find a spanning tree in a connected graph.

Start with the graph connected graph G. If there is no cycle, then the G is already a tree and we are done. If there is a cycle, let e be any edge in that cycle and consider the new graph $G_1 = G - e$ (i.e., the graph you get by deleting e). This tree is still connected since e belonged to a cycle, there were at least two paths between its incident vertices. Now repeat: if G_1 has no cycles, we are done, otherwise define G_2 to be $G_1 - e_1$, where e_1 is an edge in a cycle in G_1. Keep going. This process must eventually stop, since there are only a finite number of edges to remove. The result will be a tree, and since we never removed any vertex, a *spanning* tree.

This is by no means the only algorithm for finding a spanning tree. You could have started with the empty graph and added edges that belong to G as long as adding them would not create a cycle. You have some choices as to which edges you add first: you could always add an edge adjacent to edges you have already added (after the first one, of course), or add them using some other order. Which spanning tree you end up with depends on these choices.

We now provide two algorithms that follow this latter idea of starting with an empty graph and adding edges until we have formed a tree.

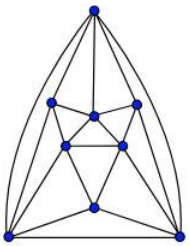
Depth-first search algorithm

- Input G, a connected graph with vertices $v_1, v_2, \ldots, v_n$
- Let $T :=$tree with no edges and only the vertex v_1
- $visit(v_1)$ (i.e. apply the procedure $visit$ to v_1)

VISIT

- Input v, a vertex of a graph G
- For each vertex w adjacent to v and not yet in T
  - add vertex w and edge $\{v, w\}$ to T
  - $visit(w)$

Notice that we can pick our starting vertex arbitrarily and adjacent vertices in any order. Label the vertices in the graph below, pick a starting vertex, and use depth-first search to find a spanning tree of the graph below.



Breadth-first search algorithm

- Input G, a connected graph with vertices $v_1, v_2, \ldots, v_n$
- Let $T :=$tree with no edges and only the vertex v_1
- Let $L :=$empty list
- Put v_1 in L, a list of unprocessed vertices
- While L is not empty
  - remove the first vertex v from L
  - for each neighbor w of v
    - if w is not in L and not in T
      - add w to the end of the list L

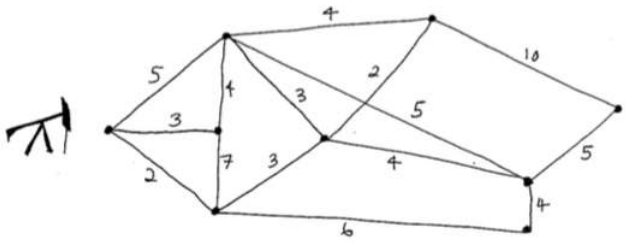
- add w and the edge $\{v, w\}$ to T

Using the same graph, same labels, and same starting vertex, apply the breadth-first search algorithm to find a spanning tree of the graph above.

Find a big-O estimate of the number of steps these algorithms require.

Spanning trees in weighted graphs

In the graph below, there is an oil well located at the left-most vertex, while other vertices represent storage facilities.



1. Suppose the edges represent the possible pipelines we *could* build, and the weight on an edge represents the cost of building that edge (in millions of dollars). Which pipelines should we build so that we can transport oil from the well to each storage facility, but we want to spend as little money as possible? What is the total cost of building these pipelines? Describe an algorithm that could be used to solve this problem.
2. Again, suppose the edges represent the possible pipelines we could build. Now suppose that the weight on each edge represents the time it takes for oil to get through that section of the pipeline (in hours). Which pipelines should we build so that we can transport oil from the well to each storage facility as quickly as possible? Describe an algorithm that could be used to solve this problem.

Definition

A **minimum spanning tree** in a connected weighted graph is a spanning tree with minimum possible total edge weight.

A **shortest path spanning tree from v** in a connected weighted graph is a spanning tree such that the distance from v to any other vertex u is as small as possible.

We present below two common algorithms used to find minimum spanning trees.

Prim's algorithm

- Input: G, a connected weighted graph with n vertices
- Let $T :=$any edge with minimum weight
- for i from 1 to $n-2$
  - let $e :=$an edge of minimum weight among those incident to a vertex in T that will not form a cycle in T if added to it
  - $T := T \cup e$
- Return T

Kruskal's algorithm

- Input: G, a connected weighted graph with n vertices
- Let T be an empty graph
- for i from 1 to $n-1$
  - let $e :=$an edge in G of minimum weight among those that do not form a cycle in T if added to it
  - $T := T \cup e$
- Return T

Notice the difference between the two algorithms. In Prim's edges that are incident to a vertex already in the tree are added, while in Kruskal's the edges that are added need not be incident to a vertex already in the tree.

We now present an algorithm that creates a shortest path spanning tree from a given vertex.

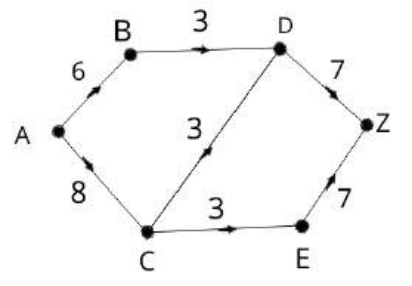
Shortest path spanning tree algorithm

- Input: G, a connected weighted graph with n vertices $v_1, v_2, \ldots, v_n$and with source vertex v_1
- Apply Dijkstra's algorithm (Section 5.7) to G
- Let T be an empty graph
- For i from 2 to n
  - Add edge $e = \{v_i, prev(v_i)\}$ to T
- Return T

10.11: Transportation Networks and Flows

investigate!

At the end of the school day, all the students plan on driving from school (vertex A) to the concert (at vertex Z). The directed edges in the graph below represent one-way roads, and the weight of each edge represents the number of vehicles (in hundreds) that particular road can handle in one hour. What is the greatest number of vehicles that can get from school to the concert in one hour? How many vehicles should take each road?



Definition

A **transportation network** is a connected, weighted, directed graph with the following properties.

1. There is one **source**, a vertex with no incoming edges. [In other language, the vertex has **indegree** 0.]
2. There is one **sink**, a vertex with no outgoing edges. [In other language, the vertex has **outdegree** 0.]
3. Each edge (u, v) is assigned a nonnegative weight C_{uv} called the **capacity** of that edge. [Notice I wrote the edge as an ordered pair rather than a set. This is because each edge has an initial vertex and a terminal vertex, so the order matters.]

Transportation networks can also be used to model oil flowing through a series of pipelines, data flowing through a network of computers, and many other situations.

Definition

Let G be a transportation network with capacity C_{ij} on edge (i, j). A **flow** F on G assigns to each edge (i, j) a nonnegative number F_{ij}, called the **flow on edge (i, j)** with the following properties.

1. $F_{ij} \leq C_{ij}$.
2. For every vertex i other than the source or the sink, $\sum_j F_{ij} = \sum_j F_{ji}$.

What do these two conditions mean in words? The first says that the flow cannot exceed the capacity on an edge. We can see why this condition is necessary - we cannot, for example, send more oil through a pipeline than it can handle. The second says that the flow IN to a vertex must be equal to the flow OUT of that same vertex (except at the source or the sink). Again this condition makes sense: if oil is flowing through a series of pipelines, we should not gain or lose oil between the source of the oil and location to which we are sending it.

To write a flow on a transportation network, give each edge a pair of numbers with the capacity of an edge preceding the flow along that edge: C_{ij}, F_{ij}. Express your solution to the initial example in this section as a flow on a transportation network.

Theorem 10.11.1

For any flow F on a transportation network, the flow out of the source must equal the flow into the sink. In symbols, $\sum_j F_{aj} = \sum_j F_{jz}$.

Proof

This proof is left as an exercise.

Because of the previous theorem, we can make the following definition.

Definition

The **value** of a flow is the total flow out of the sink (or into the source). A **maximal flow** is a flow with greatest possible value.

Definition

A **cut** in a transportation network G is a partition of the vertices of G into two sets S and T so that the source is in S and the sink is in T.

For example $S = \{A, B\}$ and $T = \{C, D, E, Z\}$ is a cut for the transportation network at the beginning of the section.

Definition

The **capacity of the cut S,T** is the sum of the capacities of all edges starting at a vertex in S and ending at a vertex in T. Equivalently, it is the number $\sum_{i \in S, j \in T} C_{ij}$. A **minimal cut** is a cut with the least possible capacity.

The capacity of the previous cut is $3 + 8 = 11$. A minimal cut for the same network is $S = \{A, B, C\}$ and $T = \{D, E, Z\}$. This cut has capacity 9.

It turns out that maximal flows are related to minimal cuts.

Theorem 10.11.2

Let F be a flow on a transportation network G and let S, T be a cut. If $\sum_i F_{ai} = \sum_{i \in S, j \in T} C_{ij}$ (i.e. if the value of the flow is equal to the capacity of the cut), then the flow is maximal and the cut is minimal.

Proof

The proof is omitted.

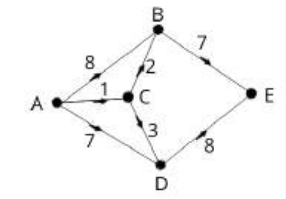
We present below an algorithm that can be used to find a maximal flow in a transportation network. It is given below in sentences rather than in pseudocode for ease of understanding. The basic idea is that we begin with a flow of zero along each edge. We use the algorithm to find a path from the source to the sink along which we can increase the flow. We do so, and then we try again. We keep doing so until we cannot anymore; what we are left with is a maximal flow. The proof that the algorithm produces a maximal flow and a minimum cut are omitted.

Max Flow algorithm

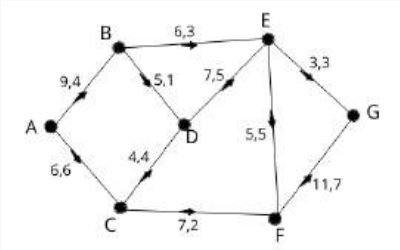
1. Label the source $(source, +, \infty)$.
2. Look at a labeled vertex. Suppose it is called v and has label $(u, \pm, a)$. For each unlabeled vertex w do the following:
    1. If there is an edge from v to w, and the current flow from v to w is below capacity, give w the label $(v, +, b)$ where b is either a or the capacity minus the flow, whichever is smaller.
    2. If there is an edge from w to v and the current flow from w to v is positive, then give w the label $(v, -, b)$ where b is either a or the current flow, whichever is smaller.
    3. Otherwise, don't give w a label.
3. Repeat step 2 until the sink is labeled or you can't label anymore.
    1. If the sink is labeled, increase the flow by the amount in the label on the sink, following the path back to the source. Notice that if you encounter any "-" you need to decrease the flow on that arc. Then start again at step 1 with this new flow.
    2. If the sink isn't labeled you are done. The current flow is maximal. We have also found a minimal cut: the set of labeled vertices is S and the set of unlabeled vertices is T.

Exercise 10.11.3

Use the max flow algorithm to determine a maximal flow, the value of the maximal flow, and a minimal cut for the transportation network below.



Use the max flow algorithm to determine a maximal flow, the value of the maximal flow, and a minimal cut for the transportation network with the given flow below.



10.12: Data Structures for Graphs

In this section, we will describe data structures that are commonly used to represent graphs. In addition we will introduce the basic syntax for graphs in Sage.

10.12.1: Basic Data Structures

List 10.12.1: Data Structures for Graphs

Assume that we have a graph with n vertices that can be indexed by the integers $1, 2, \ldots, n$. Here are three different data structures that can be employed to represent graphs.

a. Adjacency Matrix: As we saw in Chapter 6, the information about edges in a graph can be summarized with an adjacency matrix, G, where $G_{ij} = 1$ if and only if vertex i is connected to vertex j in the graph. Note that this is the same as the adjacency matrix for a relation.
b. Edge Dictionary: For each vertex in our graph, we maintain a list of edges that initiate at that vertex. If G represents the graph's edge information, then we denote by G_i the list of vertices that are terminal vertices of edges initiating at vertex i. The exact syntax that would be used can vary. We will use Sage/Python syntax in our examples.
c. Edge List: Note that in creating either of the first two data structures, we would presume that a list of edges for the graph exists. A simple way to represent the edges is to maintain this list of ordered pairs, or two element sets, depending on whether the graph is intended to be directed or undirected. We will not work with this data structure here, other than in the first example.

Example 10.12.1: A Very Small Example

We consider the representation of the following graph:

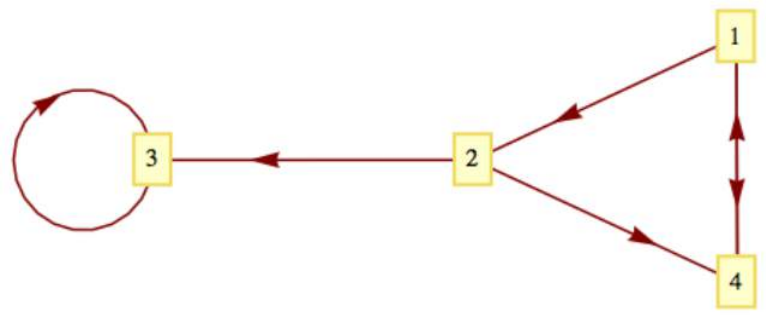


Figure 10.12.1: Graph for a Very Small Example

The adjacency matrix that represents the graph would be

$$G = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The same graph could be represented with the edge dictionary

```
{1:[2,4],2:[3,4],3:[3],4:[1]}
```

.

Notice the general form of each item in the dictionary: `vertex:[list of vertices]` .

Finally, a list of edges `[(1,2),(1,4),(2,3),(2,4),(3,3),(4,1)]` also describes the same graph.

A natural question to ask is: Which data structure should be used in a given situation? For small graphs, it really doesn't make much difference. For larger matrices the edge count would be a consideration. If n is large and the number of edges is relatively small, it might use less memory to maintain an edge dictionary or list of edges instead of building an $n \times n$ matrix. Some software for working with graphs will make the decision for you.

Example 10.12.2: NCAA Basketball

Consider the tournament graph representing a NCAA Division 1 men's (or women's) college basketball season in the United States. There are approximately 350 teams in Division 1. Suppose we constructed the graph with an edge from team A to team B if A beat B at least once in the season; and we label the edge with the number of wins. Since the average team plays around 30 games in a season, most of which will be against other Division I teams, we could expect around $\frac{30 \cdot 350}{2} = 5,250$ edges in the graph. This would be somewhat reduced by games with lower division teams and cases where two or more wins over the same team produces one edge. Since 5,250 is much smaller than $350^2 = 122,500$ entries in an adjacency matrix, an edge dictionary or edge list would be more compact than an adjacency matrix. Even if we were to use software to create an adjacency matrix, many programs will identify the fact that a matrix such as the one in this example would be "sparse" and would leave data in list form and use sparse array methods to work with it.

10.12.2: Graphs

The most common way to define a graph in Sage is to use an edge dictionary. Here is how the graph in Example 10.12.1 is generated and then displayed. Notice that we simply wrap the function `DiGraph()` around the same dictionary expression we identified earlier.

```
G1 = DiGraph( {1 : [4, 2], 2 : [3, 4], 3 : [3], 4 : [1]})
G1.show()
```

You can get the adjacency matrix of a graph with the `adjacency_matrix` method.

```
G1.adjacency_matrix()
```

You can also define a graph based on its adjacency matrix.

```
M = Matrix([[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0],
            [0,0,0,0,1],[1,0,0,0,0]])
DiGraph(M).show()
```

The edge list of any directed graph can be easily retrieved. If you replace `edges` with `edge_iterator`, you can iterate through the edge list. The third coordinate of the items in the edge is the label of the edge, which is `None` in this case.

```
DiGraph(M).edges()
```

Replacing the wrapper `DiGraph()` with `Graph()` creates an undirected graph.

```
G2 = Graph( {1 : [4, 2], 2 : [3, 4], 3 : [3], 4 : [1]})
G2.show()
```

There are many special graphs and graph families that are available in Sage through the `graphs` module. They are referenced with the prefix `graphs.` followed by the name and zero or more parameters inside parentheses. Here are a couple of them, first a complete graph with five vertices.

```
graphs.CompleteGraph(5).show()
```

Here is a wheel graph, named for an obvious pattern of vertices and edges. We assign a name to it first and then show the graph without labeling the vertices.

```
w=graphs.WheelGraph(20)
w.show(vertex_labels=false)
```

There are dozens of graph methods, one of which determines the degree sequence of a graph. In this case, it's the wheel graph above.

```
1 w.degree_sequence()
```

The degree sequence method is defined within the graphs module, but the prefix `graphs.` is not needed because the value of `w` inherits the graphs methods.

10.12.3: Exercises

Exercise 10.12.1

Estimate the number of vertices and edges in each of the following graphs. Would the graph be considered sparse, so that an adjacency matrix would be inefficient?

a. Vertices: Cities of the world that are served by at least one airline. Edges: Pairs of cities that are connected by a regular direct flight.
b. Vertices: ASCII characters. Edges: connect characters that differ in their binary code by exactly two bits.
c. Vertices: All English words. Edges: An edge connects word x to word y if x is a prefix of y.

Answer

a. A rough estimate of the number of vertices in the "world airline graph" would be the number of cities with population greater than or equal to 100,000. This is estimated to be around 4,100. There are many smaller cities that have airports, but some of the metropolitan areas with clusters of large cities are served by only a few airports. 4,000-5,000 is probably a good guess. As for edges, that's a bit more difficult to estimate. It's certainly not a complete graph. Looking at some medium sized airports such as Manchester, NH, the average number of cities that you can go to directly is in the 50-100 range. So a very rough estimate would be $\frac{75 \cdot 4500}{2} = 168,750$. This is far less than $4,500^2$, so an edge list or dictionary of some kind would be more efficient.
b. The number of ASCII characters is 128. Each character would be connected to $\binom{8}{2} = 28$ others and so there are $\frac{128 \cdot 28}{2} = 3,584$ edges. Comparing this to the $128^2 = 16,384$, an array is probably the best choice.
c. The Oxford English Dictionary as approximately a half-million words, although many are obsolete. The number of edges is probably of the same order of magnitude as the number of words, so an edge list or dictionary is probably the best choice.

Exercise 10.12.2

Each edge of a graph is colored with one of the four colors red, blue, yellow, or green. How could you represent the edges in this graph using a variation of the adjacency matrix structure?

Exercise 10.12.3

Directed graphs $G_1, \ldots, G_6$, each with vertex set $\{1, 2, 3, 4, 5\}$ are represented by the matrices below. Which graphs are isomorphic to one another?

$$G_1: \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \quad G_2: \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad G_3: \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \quad G_4: \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$G_5: \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \quad G_6: \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Answer

Each graph is isomorphic to itself. In addition, G_2 and G_4 are isomorphic; and $G_3, G_5,$ and G_6 are isomorphic to one another.

Exercise 10.12.4

The following Sage command verifies that the wheel graph with four vertices is isomorphic to the complete graph with four vertices.

```
graphs.WheelGraph(4).is_isomorphic(graphs.CompleteGraph(4))
```

A list of all graphs in this the `graphs` database is available via tab completion. Type "graphs." and then hit the tab key to see which graphs are available. This can be done using the Sage application or SageMathCloud, but not sage cells. Find some other pairs of isomorphic graphs in the database.

10.E: Graph Theory (Exercises)

5.2: Definitions

1

If 10 people each shake hands with each other, how many handshakes took place? What does this question have to do with graph theory?

Answer

This is asking for the number of edges in K_{10}. Each vertex (person) has degree (shook hands with) 9 (people). So the sum of the degrees is 90. However, the degrees count each edge (handshake) twice, so there are 45 edges in the graph. That is how many handshakes took place.

2

Among a group of 5 people, is it possible for everyone to be friends with exactly 2 of the people in the group? What about 3 of the people in the group?

Answer

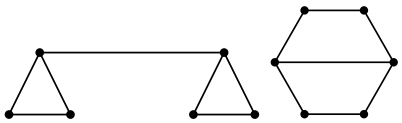
It is possible for everyone to be friends with exactly 2 people. You could arrange the 5 people in a circle and say that everyone is friends with the two people on either side of them (so you get the graph C_5). However, it is not possible for everyone to be friends with 3 people. That would lead to a graph with an odd number of odd degree vertices which is impossible since the sum of the degrees must be even.

3

Is it possible for two *different* (non-isomorphic) graphs to have the same number of vertices and the same number of edges? What if the degrees of the vertices in the two graphs are the same (so both graphs have vertices with degrees 1, 2, 2, 3, and 4, for example)? Draw two such graphs or explain why not.

Answer

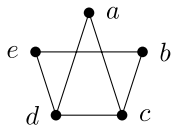
Yes. For example, both graphs below contain 6 vertices, 7 edges, and have degrees (2,2,2,2,3,3).



4

Are the two graphs below equal? Are they isomorphic? If they are isomorphic, give the isomorphism. If not, explain.

- Graph 1: $V = \{a, b, c, d, e\},\ E = \{\{a, b\}, \{a, c\}, \{a, e\}, \{b, d\}, \{b, e\}, \{c, d\}\}$.
- Graph 2:



Answer

The graphs are not equal. For example, graph 1 has an edge $\{a, b\}$ but graph 2 does not have that edge. They are isomorphic. One possible isomorphism is $f : G_1 \to G_2$ defined by $f(a) = d,\ f(b) = c,\ f(c) = e,\ f(d) = b,\ f(e) = a$.

5

Consider the following two graphs:

G_1

- $V_1 = \{a, b, c, d, e, f, g\}$
- $E_1 = \{\{a, b\}, \{a, d\}, \{b, c\}, \{b, d\}, \{b, e\}, \{b, f\}, \{c, g\}, \{d, e\},$
- $\{e, f\}, \{f, g\}\}$.

G_2

- $V_2 = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\},$
- $E_2 = \{\{v_1, v_4\}, \{v_1, v_5\}, \{v_1, v_7\}, \{v_2, v_3\}, \{v_2, v_6\},$
- $\{v_3, v_5\}, \{v_3, v_7\}, \{v_4, v_5\}, \{v_5, v_6\}, \{v_5, v_7\}\}$

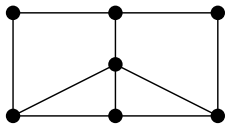
a. Let $f : G_1 \to G_2$ be a function that takes the vertices of Graph 1 to vertices of Graph 2. The function is given by the following table:

x	a	b	c	d	e	f	g
$f(x)$	v_4	v_5	v_1	v_6	v_2	v_3	v_7

Does f define an isomorphism between Graph 1 and Graph 2? Explain.

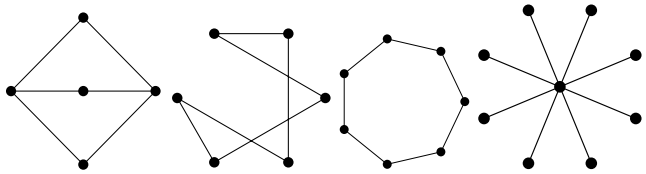
b. Define a new function g (with $g \neq f$) that defines an isomorphism between Graph 1 and Graph 2.

c. Is the graph pictured below isomorphic to Graph 1 and Graph 2? Explain.



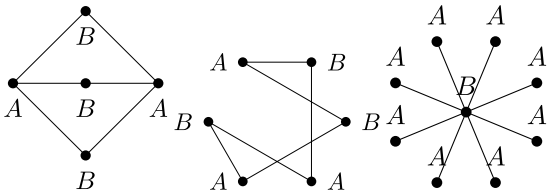
6

Which of the graphs below are bipartite? Justify your answers.



Answer

Three of the graphs are bipartite. The one which is not is C_7 (second from the right). To see that the three graphs are bipartite, we can just give the bipartition into two sets A and B, as labeled below:



The graph C_7 is not bipartite because it is an *odd* cycle. You would want to put every other vertex into the set A, but if you travel clockwise in this fashion, the last vertex will also be put into the set A, leaving two A vertices adjacent (which makes it not a bipartition).

7

For which $n \geq 3$ is the graph C_n bipartite?

8

For each of the following, try to give two *different* unlabeled graphs with the given properties, or explain why doing so is impossible.

a. Two different trees with the same number of vertices and the same number of edges. A tree is a connected graph with no cycles.
b. Two different graphs with 8 vertices all of degree 2.
c. Two different graphs with 5 vertices all of degree 4.
d. Two different graphs with 5 vertices all of degree 3.

Answer

1. For example: 1.

2. This is not possible if we require the graphs to be connected. If not, we could take C_8 as one graph and two copies of C_4 as the other.
3. Not possible. If you have a graph with 5 vertices all of degree 4, then every vertex must be adjacent to every other vertex. This is the graph K_5.
4. This is not possible. In fact, there is not even one graph with this property (such a graph would have $5 \cdot 3/2 = 7.5$ edges).

5.3: Planar Graphs

1

Is it possible for a planar graph to have 6 vertices, 10 edges and 5 faces? Explain.

2

The graph G has 6 vertices with degrees $2, 2, 3, 4, 4, 5$.How many edges does G have? Could G be planar? If so, how many faces would it have. If not, explain.

3

I'm thinking of a polyhedron containing 12 faces. Seven are triangles and four are quadralaterals. The polyhedron has 11 vertices including those around the mystery face. How many sides does the last face have?

Answer

Say the last polyhedron has n edges, and also n vertices. The total number of edges the polyhedron has then is $(7 \cdot 3 + 4 \cdot 4 + n)/2 = (37 + n)/2$. In particular, we know the last face must have an odd number of edges. We also have that $v = 11$. By Euler's formula, we have $11 - (37 + n)/2 + 12 = 2$, and solving for n we get $n = 5$, so the last face is a pentagon.

4

Consider some classic polyhedrons.

a. An *octahedron* is a regular polyhedron made up of 8 equilateral triangles (it sort of looks like two pyramids with their bases glued together). Draw a planar graph representation of an octahedron. How many vertices, edges and faces does an octahedron (and your graph) have?
b. The traditional design of a soccer ball is in fact a (spherical projection of a) truncated icosahedron. This consists of 12 regular pentagons and 20 regular hexagons. No two pentagons are adjacent (so the edges of each pentagon are shared only by hexagons). How many vertices, edges, and faces does a truncated icosahedron have? Explain how you arrived at your answers. Bonus: draw the planar graph representation of the truncated icosahedron.
c. Your “friend” claims that he has constructed a convex polyhedron out of 2 triangles, 2 squares, 6 pentagons and 5 octagons. Prove that your friend is lying. Hint: each vertex of a convex polyhedron must border at least three faces.

5

Prove Euler's formula using induction on the number of edges in the graph.

Answer

Proof

Let $P(n)$ be the statement, "every planar graph containing n edges satisfies $v-n+f=2$. " We will show $P(n)$ is true for all $n \geq 0$. Base case: there is only one graph with zero edges, namely a single isolated vertex. In this case $v=1$, $f=1$ and $e=0$, so Euler's formula holds. Inductive case: Suppose $P(k)$ is true for some arbitrary $k \geq 0$. Now consider an arbitrary graph containing $k+1$ edges (and v vertices and f faces). No matter what this graph looks like, we can remove a single edge to get a graph with k edges which we can apply the inductive hypothesis to. There are two possibilities. First, the edge we remove might be incident to a degree 1 vertex. In this case, also remove that vertex. The smaller graph will now satisfy $v-1-k+f=2$ by the induction hypothesis (removing the edge and vertex did not reduce the number of faces). Adding the edge and vertex back gives $v-(k+1)+f=2$, as required. The second case is that the edge we remove is incident to vertices of degree greater than one. In this case, removing the edge will keep the number of vertices the same but reduce the number of faces by one. So by the inductive hypothesis we will have $v-k+f-1=2$. Adding the edge back will give $v-(k+1)+f=2$ as needed. Therefore, by the principle of mathematical induction, Euler's formula holds for all planar graphs.

6

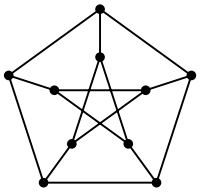
Prove Euler's formula using induction on the number of *vertices* in the graph.

7

Euler's formula ($v-e+f=2$) holds for all *connected* planar graphs. What if a graph is not connected? Suppose a planar graph has two components. What is the value of $v-e+f$ now? What if it has k components?

8

Prove that the *Petersen graph* (below) is not planar.



Answer:

What is the length of the shortest cycle? (This quantity is usually called the *girth* of the graph.)

9

Prove that any planar graph with v vertices and e edges satisfies $e \leq 3v-6$.

Answer

Proof

We know in any planar graph the number of faces f satisfies $3f \leq 2e$ since each face is bounded by at least three edges, but each edge borders two faces. Combine this with Euler's formula:

$$v-e+f=2$$

$$v-e+\frac{2e}{3} \geq 2$$

$$3v-e \geq 6$$

$$3v-6 \geq e.$$

10

Prove that any planar graph must have a vertex of degree 5 or less.

5.4: Coloring

1

What is the smallest number of colors you need to properly color the vertices of $K_{4,5}$? That is, find the chromatic number of the graph.

Answer

2, since the graph is bipartite. One color for the top set of vertices, another color for the bottom set of vertices.

2

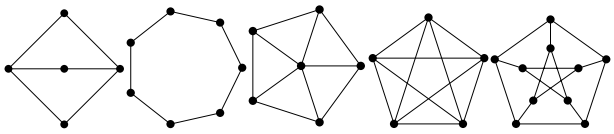
Draw a graph with chromatic number 6 (i.e., which requires 6 colors to properly color the vertices). Could your graph be planar? Explain.

Answer

For example, K_6. If the chromatic number is 6, then the graph is not planar; the 4-color theorem states that all planar graphs can be colored with 4 or fewer colors.

3

Find the chromatic number of each of the following graphs.



4

A group of 10 friends decides to head up to a cabin in the woods (where nothing could possibly go wrong). Unfortunately, a number of these friends have dated each other in the past, and things are still a little awkward. To get the cabin, they need to divide up into some number of cars, and no two people who dated should be in the same car.

a. What is the smallest number of cars you need if all the relationships were strictly heterosexual? Represent an example of such a situation with a graph. What kind of graph do you get?

b. Because a number of these friends dated there are also conflicts between friends of the same gender, listed below. Now what is the smallest number of conflict-free cars they could take to the cabin?

Friend	A	B	C	D	E	F	G	H	I	J
Conflicts with	BEJ	ADG	HJ	BF	AI	DJ	B	CI	EHJ	ACFI

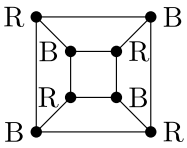
c. What do these questions have to do with coloring?

5

What is the smallest number of colors that can be used to color the vertices of a cube so that no two adjacent vertices are colored identically?

Answer

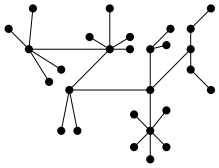
The cube can be represented as a planar graph and colored with two colors as follows:



Since it would be impossible to color the vertices with a single color, we see that the cube has chromatic number 2 (it is bipartite).

6

Prove the chromatic number of any tree is two. Recall, a tree is a connected graph with no cycles.



a. Describe a procedure to color the tree below.
b. The chromatic number of C_n is two when n is even. What goes wrong when n is odd?
c. Prove that your procedure from part (a) always works for any tree.
d. Now, prove using induction that every tree has chromatic number 2.

7

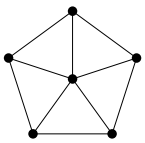
Prove the 6-color theorem: every planar graph has chromatic number 6 or less. Do not assume the 4-color theorem (whose proof is MUCH harder), but you may assume the fact that every planar graph contains a vertex of degree at most 5.

8

Not all graphs are perfect. Give an example of a graph with chromatic number 4 that does not contain a copy of K_4. That is, there should be no 4 vertices all pairwise adjacent.

Answer

The wheel graph below has this property. The outside of the wheel forms an odd cycle, so requires 3 colors, the center of the wheel must be different than all the outside vertices.



9

Prove by induction on vertices that any graph G which contains at least one vertex of degree less than $\Delta(G)$ (the maximal degree of all vertices in G) has chromatic number at most $\Delta(G)$.

10

You have a set of magnetic alphabet letters (one of each of the 26 letters in the alphabet) that you need to put into boxes. For obvious reasons, you don't want to put two consecutive letters in the same box. What is the fewest number of boxes you need (assuming the boxes are able to hold as many letters as they need to)?

Answer

If we drew a graph with each letter representing a vertex, and each edge connecting two letters that were consecutive in the alphabet, we would have a graph containing two vertices of degree 1 (A and Z) and the remaining 24 vertices all of degree 2 (for example, D would be adjacent to both C and E). By Brooks' theorem, this graph has chromatic number at most 2, as that is the maximal degree in the graph and the graph is not a complete graph or odd cycle. Thus only two boxes are needed.

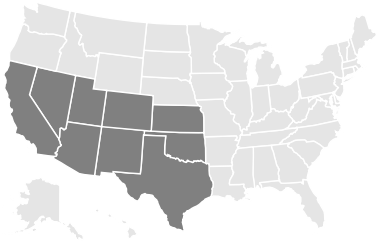
11

Prove that if you color every edge of K_6 either red or blue, you are guaranteed a monochromatic triangle (that is, an all red or an all blue triangle).

5.5: Euler Paths and Circuits

1

You and your friends want to tour the southwest by car. You will visit the nine states below, with the following rather odd rule: you must cross each border between neighboring states exactly once (so, for example, you must cross the Colorado-Utah border exactly once). Can you do it? If so, does it matter where you start your road trip? What fact about graph theory solves this problem?



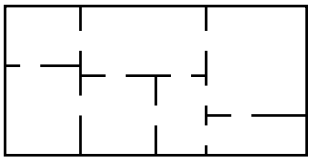
2

Which of the following graphs contain an Euler path? Which contain an Euler circuit?

a. K_4
b. K_5.
c. $K_{5,7}$
d. $K_{2,7}$
e. C_7
f. P_7

3

Edward A. Mouse has just finished his brand new house. The floor plan is shown below:



a. Edward wants to give a tour of his new pad to a lady-mouse-friend. Is it possible for them to walk through every doorway exactly once? If so, in which rooms must they begin and end the tour? Explain.
b. Is it possible to tour the house visiting each room exactly once (not necessarily using every doorway)? Explain.
c. After a few mouse-years, Edward decides to remodel. He would like to add some new doors between the rooms he has. Of course, he cannot add any doors to the exterior of the house. Is it possible for each room to have an odd number of doors? Explain.

4

For which n does the graph K_n contain an Euler circuit? Explain.

Answer

When n is odd, K_n contains an Euler circuit. This is because every vertex has degree $n-1$, so an odd n results in all degrees being even.

5

For which m and n does the graph $K_{m,n}$ contain an Euler path? An Euler circuit? Explain.

Answer

If both m and n are even, then $K_{m,n}$ has an Euler circuit. When both are odd, there is no Euler path or circuit. If one is 2 and the other is odd, then there is an Euler path but not an Euler circuit.

6

For which n does K_n contain a Hamilton path? A Hamilton cycle? Explain.

Answer

All values of n. In particular, K_n contains C_n as a subgroup, which is a cycle that includes every vertex.

7

For which m and n does the graph $K_{m,n}$ contain a Hamilton path? A Hamilton cycle? Explain.

Answer

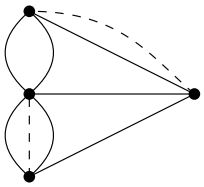
As long as $|m-n| \leq 1,$ the graph $K_{m,n}$ will have a Hamilton path. To have a Hamilton cycle, we must have $m = n$.

8

A bridge builder has come to Königsberg and would like to add bridges so that it *is* possible to travel over every bridge exactly once. How many bridges must be built?

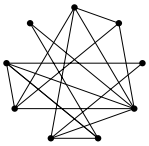
Answer

If we build one bridge, we can have an Euler path. Two bridges must be built for an Euler circuit.



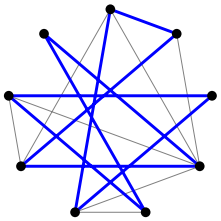
9

Below is a graph representing friendships between a group of students (each vertex is a student and each edge is a friendship). Is it possible for the students to sit around a round table in such a way that every student sits between two friends? What does this question have to do with paths?



Answer

We are looking for a Hamiltonian cycle, and this graph does have one:

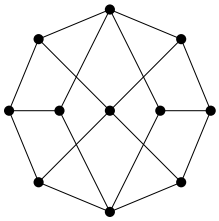


10

a. Suppose a graph has a Hamilton path. What is the maximum number of vertices of degree one the graph can have? Explain why your answer is correct.
b. Find a graph which does not have a Hamilton path even though no vertex has degree one. Explain why your example works.

11

Consider the following graph:

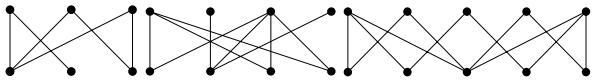


a. Find a Hamilton path. Can your path be extended to a Hamilton cycle?
b. Is the graph bipartite? If so, how many vertices are in each "part"?
c. Use your answer to part (b) to prove that the graph has no Hamilton cycle.
d. Suppose you have a bipartite graph G in which one part has at least two more vertices than the other. Prove that G does not have a Hamilton path.

5.6: Matching in Bipartite Graphs

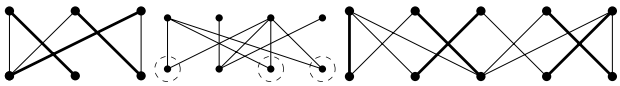
1

Find a matching of the bipartite graphs below or explain why no matching exists.



Answer

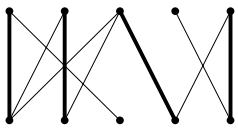
The first and third graphs have a matching, shown in bold (there are other matchings as well). The middle graph does not have a matching. If you look at the three circled vertices, you see that they only have two neighbors, which violates the matching condition $|N(S)| \geq |S|$ (the three circled vertices form the set S).



2

A bipartite graph that doesn't have a matching might still have a *partial matching*. By this we mean a set of *edges* for which no vertex belongs to more than one edge (but possibly belongs to none). Every bipartite graph (with at least one edge) has a partial matching, so we can look for the largest partial matching in a graph.

Your "friend" claims that she has found the largest partial matching for the graph below (her matching is in bold). She explains that no other edge can be added, because all the edges not used in her partial matching are connected to matched vertices. Is she correct?

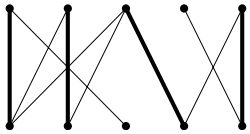


3

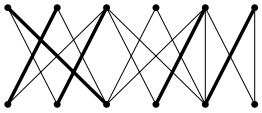
One way you might check to see whether a partial matching is maximal is to construct an *alternating path*. This is a sequence of adjacent edges, which alternate between edges in the matching and edges not in the matching (no edge can be used more than

once). If an alternating path starts and stops with an edge *not* in the matching, then it is called an *augmenting path*.

a. Find the largest possible alternating path for the partial matching of your friend's graph. Is it an augmenting path? How would this help you find a larger matching?

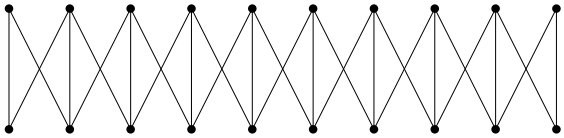


b. Find the largest possible alternating path for the partial matching below. Are there any augmenting paths? Is the partial matching the largest one that exists in the graph?



4

The two richest families in Westeros have decided to enter into an alliance by marriage. The first family has 10 sons, the second has 10 girls. The ages of the kids in the two families match up. To avoid impropriety, the families insist that each child must marry someone either their own age, or someone one position younger or older. In fact, the graph representing agreeable marriages looks like this:



The question: how many different acceptable marriage arrangements which marry off all 20 children are possible?

a. How many marriage arrangements are possible if we insist that there are exactly 6 boys marry girls not their own age?
b. Could you generalize the previous answer to arrive at the total number of marriage arrangements?
c. How do you know you are correct? Try counting in a different way. Look at smaller family sizes and get a sequence.
d. Can you give a recurrence relation that fits the problem?

5

We say that a set of vertices $A \subseteq V$ is a *vertex cover* if every edge of the graph is incident to a vertex in the cover (so a vertex cover covers the *edges*). Since V itself is a vertex cover, every graph has a vertex cover. The interesting question is about finding a *minimal* vertex cover, one that uses the fewest possible number of vertices.

a. Suppose you had a matching of a graph. How can you use that to get a minimal vertex cover? Will your method always work?
b. Suppose you had a minimal vertex cover for a graph. How can you use that to get a partial matching? Will your method always work?
c. What is the relationship between the size of the minimal vertex cover and the size of the maximal partial matching in a graph?

6

For many applications of matchings, it makes sense to use bipartite graphs. You might wonder, however, whether there is a way to find matchings in graphs in general.

a. For which n does the complete graph K_n have a matching?
b. Prove that if a graph has a matching, then $|V|$ is even.
c. Is the converse true? That is, do all graphs with $|V|$ even have a matching?
d. What if we also require the matching condition? Prove or disprove: If a graph with an even number of vertices satisfies $|N(S)| \geq |S|$ for all $S \subseteq V$, then the graph has a matching.

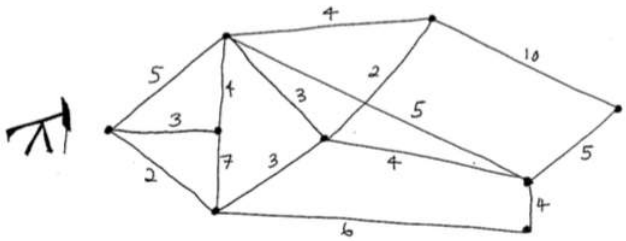
5.7: Weighted Graphs and Dijkstra's Algorithm

1

Find a big-O estimate for the number of operations (additions and comparisons) used by Dijkstra's algorithm.

2

An oil well is located on the left side of the graph below; each other vertex is a storage facility. The edges represent pipes between the well and storage facilities or between two storage facilities. The weights on the edges represent the time it takes for oil to travel from one vertex to another. Using Dijkstra's algorithm find a shortest path and the total time it takes oil to get from the well to the facility on the right side. **Use a table.**



3

Solve the same problem as in #2, but draw several copies of the graph rather than the table when performing Dijkstra's algorithm.

4

A graph G is given by $G=(\{v_1,v_2,v_3,v_4,v_5,v_6\},\{\{v_1,v_2\},\{v_1,v_3\},\{v_2,v_4\},\{v_2,v_5\},\{v_3,v_4\},\{v_4,v_5\},\{v_4,v_6\},\{v_5,v_6\}\})$ Furthermore, the weight on an edge is $w(v_i,v_j)=|i-j|$. Draw the graph, determine a shortest path from v_1 to v_6, and also give the total weight of this path. Use Dijkstra's algorithm (you may make a table or draw multiple copies of the graph).

5.8: Trees

1

Which of the following graphs are trees?

a. $G=(V,E)$ with $V=\{a,b,c,d,e\}$ and $E=\{\{a,b\},\{a,e\},\{b,c\},\{c,d\},\{d,e\}\}$

b. $G=(V,E)$ with $V=\{a,b,c,d,e\}$ and $E=\{\{a,b\},\{b,c\},\{c,d\},\{d,e\}\}$

c. $G=(V,E)$ with $V=\{a,b,c,d,e\}$ and $E=\{\{a,b\},\{a,c\},\{a,d\},\{a,e\}\}$

d. $G=(V,E)$ with $V=\{a,b,c,d,e\}$ and $E=\{\{a,b\},\{a,c\},\{d,e\}\}$

2

For each degree sequence below, decide whether it must always, must never, or could possibly be a degree sequence for a tree. Remember, a degree sequence lists out the degrees (number of edges incident to the vertex) of all the vertices in a graph in non-increasing order.

a. (4,1,1,1,1)

b. (3,3,2,1,1)

c. (2,2,2,1,1)

d. (4,4,3,3,3,2,2,1,1,1,1,1,1,1)

3

For each degree sequence below, decide whether it must always, must never, or could possibly be a degree sequence for a tree. Justify your answers.

a. (3,3,2,2,2)

b. (3,2,2,1,1,1)

c. (3,3,3,1,1,1)

d. (4,4,1,1,1,1,1,1)

4

Suppose you have a graph with v vertices and e edges that satisfies $v = e + 1$. Must the graph be a tree? Prove your answer.

5

Prove that any graph (not necessarily a tree) with v vertices and e edges that satisfies $v > e + 1$ will NOT be connected. [Hint: try a proof by contradiction and consider a spanning tree of the graph.]

6

If a graph G with v vertices and e edges is connected and has $v < e + 1$ must it contain a cycle? Prove your answer. [Hint: use the contrapositive.]

7

We define a ***forest*** to be a graph with no cycles.

a. Explain why this is a good name. That is, explain why a forest is a union of trees.

b. Suppose F is a forest consisting of m trees and v vertices. How many edges does F have? Explain.

c. Prove that any graph G with v vertices and e edges that satisfies $v < e + 1$ must contain a cycle (i.e., not be a forest).

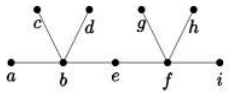
8

Give a proof of the following statement: A graph is a forest if and only if there is at most one path between any pair of vertices. Use proof by contrapositive (and not a proof by contradiction) for both directions.

9

Give a careful proof by induction on the number of vertices, that every tree is bipartite.

10



a. Suppose we designate vertex e as the root. List the children, parents and siblings of each vertex. Does any vertex other than e have grandchildren?

b. Suppose e is *not* chosen as the root. Does our choice of root vertex change the *number* of children e has? The number of grandchildren? How many are there of each?

c. In fact, pick any vertex in the tree and suppose it is not the root. Explain why the number of children of that vertex does not depend on which other vertex is the root.

d. Does the previous part work for other trees? Give an example of a different tree for which it holds. Then either prove that it always holds or give an example of a tree for which it doesn't.

11

Let T be a rooted tree that contains vertices u, v, and w (among possibly others). Prove that if w is a descendant of both u and v, then u is a descendant of v or v is a descendant of u.

12

Unless it is already a tree, a given graph G will have multiple spanning trees. How similar or different must these be?

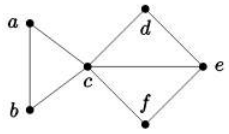
a. Must all spanning trees of a given graph be isomorphic to each other? Explain why or give a counterexample.

b. Must all spanning trees of a given graph have the same number of edges? Explain why or give a counterexample.

c. Must all spanning trees of a graph have the same number of leaves (vertices of degree 1)? Explain why or give a counterexample.

13

Find all spanning trees of the graph below. How many different spanning trees are there? How many different spanning trees are there *up to isomorphism*(that is, if you grouped all the spanning trees by which are isomorphic, how many groups would you have)?



14

Give an example of a graph that has exactly 7 different spanning trees. Note, it acceptable for some or all of these spanning trees to be isomorphic. [Hint: there is an example with 7 edges.)

15

Prove that every connected graph which is not itself a tree must have at last three different (although possibly isomorphic) spanning trees.

16

Consider edges that must be in every spanning tree of a graph. Must every graph have such an edge? Give an example of a graph that has exactly one such edge.

17

An m-ary tree is a rooted tree in which every internal vertex has at most m children. A full m-ary tree is a rooted tree in which every internal vertex has exactly m children. A full m-ary tree with n vertices has how many internal vertices and how many leaves?

5.9.1: Tree traversal

1

Create a rooted ordered tree for the expression $(4+2)^3/((4-1)+(2*3))+4$.

2

Determine the preorder and postorder traversals of this tree.

3

Evaluate the following postfix expression: $6\,2\,3\,-\,+\,2\,3\,1\,*\,+\,-$.

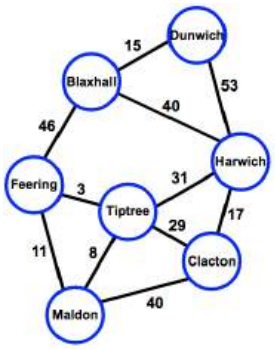
Evaluate the following prefix expression: $\uparrow\,-\,*\,3\,3\,*\,1\,2\,3$.

4

Find a big-O estimate of the time complexity of the preorder, inorder, and postorder traversals.

5.9.2: Spanning tree algorithms

Use the graph below for all 5.9.2 exercises.



1

Use the depth-first search algorithm to find a spanning tree for the graph above. Let v_1 be the vertex labeled "Tiptree" and choose adjacent vertices alphabetically. You can ignore the edge weights.

2

Use the breadth-first search algorithm to find a spanning tree for the graph above, with Tiptree being v_1. Add vertices to L alphabetically.

3

Find a minimum spanning tree using Prim's algorithm. Make sure to keep track of the order in which edges are added to the tree. Then find a minimum spanning tree using Kruskal's algorithm, again keeping track of the order in which edges are added.

4

Find a shortest path spanning tree from Maldon. Make sure to show steps of Dijkstra's algorithm in detail.

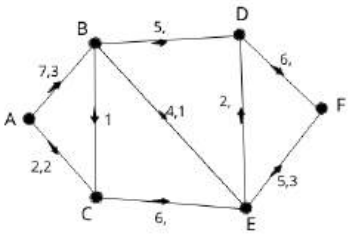
5.9.3: Transportation Networks and Flows

1

A telephone call can be routed from South Bend to Orlando on various routes. The line from South Bend to Indianapolis can carry 40 calls at the same time. Other lines and their capacities are as follows: South Bend to St. Louis (30 calls), South Bend to Memphis (20 calls), Indianapolis to Memphis (15 calls), Indianapolis to Lexington (25 calls), St. Louis to Little Rock (20 calls), Little Rock to Memphis (15 calls), Little Rock to Orlando (10 calls), Memphis to Orlando (25 calls), Lexington to Orlando (15 calls). Draw a transportation network displaying this information.

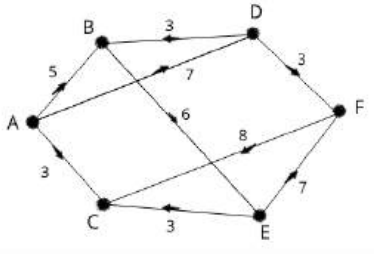
2

Fill in the missing values on the edges so that the result is a flow on the transportation network.



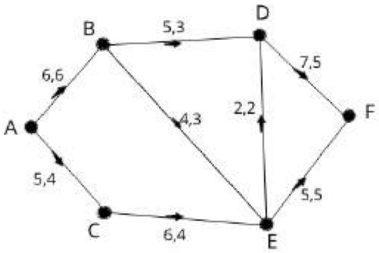
3

Use the max flow algorithm to find a maximal flow and minimum cut on the transportation network below. Determine the value of the flow. Find a minimal cut and give its capacity.



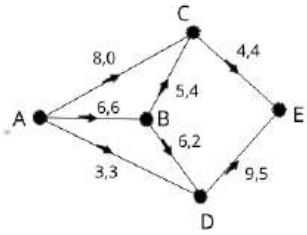
4

Use the max flow algorithm to find a larger flow than the one currently displayed on the transportation network below.



5

Use the max flow algorithm to find a larger flow than the one currently displayed on the transportation network below.



10.S: Graph Theory (Summary)

Hopefully this chapter has given you some sense for the wide variety of graph theory topics as well as why these studies are interesting. There are many more interesting areas to consider and the list is increasing all the time; graph theory is an active area of mathematical research.

One reason graph theory is such a rich area of study is that it deals with such a fundamental concept: any pair of objects can either be related or not related. What the objects are and what "related" means varies on context, and this leads to many applications of graph theory to science and other areas of math. The objects can be countries, and two countries can be related if they share a border. The objects could be land masses which are related if there is a bridge between them. The objects could be websites which are related if there is a link from one to the other. Or we can be completely abstract: the objects are vertices which are related if their is an edge between them.

What question we ask about the graph depends on the application, but often leads to deeper, general and abstract questions worth studying in their own right. Here is a short summary of the types of questions we have considered:

- Can the graph be drawn in the plane without edges crossing? If so, how many regions does this drawing divide the plane into?
- Is it possible to color the vertices of the graph so that related vertices have different colors using a small number of colors? How many colors are needed?
- Is it possible to trace over every edge of a graph exactly once without lifting up your pencil? What other sorts of "paths" might a graph posses?
- Can you find subgraphs with certain properties? For example, when does a (bipartite) graph contain a subgraph in which all vertices are only related to one other vertex?

Not surprisingly, these questions are often related to each other. For example, the chromatic number of a graph cannot be greater than 4 when the graph is planar. Whether the graph has an Euler path depends on how many vertices each vertex is adjacent to (and whether those numbers are always even or not). Even the existence of matchings in bipartite graphs can be proved using paths.

Chapter Review

1

Which (if any) of the graphs below are the same? Which are different? Explain.

Solution

The first and the third graphs are the same (try dragging vertices around to make the pictures match up), but the middle graph is different (which you can see, for example, by noting that the middle graph has only one vertex of degree 2, while the others have two such vertices).

2

Which of the graphs in the previous question contain Euler paths or circuits? Which of the graphs are planar?

Solution

The first (and third) graphs contain an Euler path. All the graphs are planar.

3

Draw a graph which has an Euler circuit but is not planar.

Solution

For example, K_5.

4

Draw a graph which does not have an Euler path and is also not planar.

Solution

For example, $K_{3,3}$.

5

If a graph has 10 vertices and 10 edges and contains an Euler circuit, must it be planar? How many faces would it have?

Solution

Yes. According to Euler's formula it would have 2 faces. It does. The only such graph is C_{10}.

6

Suppose G is a graph with n vertices, each having degree 5.

a. For which values of n does this make sense?
b. For which values of n does the graph have an Euler path?
c. What is the smallest value of n for which the graph might be planar? (tricky)

Solution

a. Only if $n \geq 6$ and is even.
b. None.
c. 12. Such a graph would have $\frac{5n}{2}$ edges. If the graph is planar, then $n - \frac{5n}{2} + f = 2$ so there would be $\frac{4+3n}{2}$ faces. Also, we must have $3f \leq 2e$, since the graph is simple. So we must have $3\left(\frac{4+3n}{2}\right) \leq 5n$. Solving for n gives $n \geq 12$.

7

At a school dance, 6 girls and 4 boys take turns dancing (as couples) with each other.

a. How many couples danced if every girl dances with every boy?
b. How many couples danced if everyone danced with everyone else (regardless of gender)?
c. Explain what graphs can be used to represent these situations.

Solution

a. There were 24 couples: 6 choices for the girl and 4 choices for the boy.
b. There were 45 couples: $\binom{10}{2}$ since we must choose two of the 10 people to dance together.
c. For part (a), we are counting the number of edges in $K_{4,6}$. In part (b) we count the edges of K_{10}.

8

Among a group of n people, is it possible for everyone to be friends with an odd number of people in the group? If so, what can you say about n?

Solution

Yes, as long as n is even. If n were odd, then corresponding graph would have an odd number of odd degree vertices, which is impossible.

9

Your friend has challenged you to create a convex polyhedron containing 9 triangles and 6 pentagons.

a. Is it possible to build such a polyhedron using *only* these shapes? Explain.
b. You decide to also include one heptagon (seven-sided polygon). How many vertices does your new convex polyhedron contain?
c. Assuming you are successful in building your new 16-faced polyhedron, could every vertex be the joining of the same number of faces? Could each vertex join either 3 or 4 faces? If so, how many of each type of vertex would there be?

Solution

a. No. The 9 triangles each contribute 3 edges, and the 6 pentagons contribute 5 edges. This gives a total of 57, which is exactly twice the number of edges, since each edge borders exactly 2 faces. But 57 is odd, so this is impossible.
b. Now adding up all the edges of all the 16 polygons gives a total of 64, meaning there would be 32 edges in the polyhedron. We can then use Euler's formula $v - e + f = 2$ to deduce that there must be 18 vertices.
c. If you add up all the vertices from each polygon separately, we get a total of 64. This is not divisible by 3, so it cannot be that each vertex belongs to exactly 3 faces. Could they all belong to 4 faces? That would mean there were $64/4 = 16$

vertices, but we know from Euler's formula that there must be 18 vertices. We can write $64 = 3x + 4y$ and solve for x and y (as integers). We get that there must be 10 vertices with degree 4 and 8 with degree 3. (Note the number of faces joined at a vertex is equal to its degree in graph theoretic terms.)

10

Is there a convex polyhedron which requires 5 colors to properly color the vertices of the polyhedron? Explain.

Solution

No. Every polyhedron can be represented as a planar graph, and the Four Color Theorem says that every planar graph has chromatic number at most 4.

11

How many edges does the graph $K_{n,n}$ have? For which values of n does the graph contain an Euler circuit? For which values of n is the graph planar?

Solution

$K_{n,n}$ has n^2 edges. The graph will have an Euler circuit when n is even. The graph will be planar only when $n < 3$.

12

The graph G has 6 vertices with degrees $1, 2, 2, 3, 3, 5$.How many edges does G have? If G was planar how many faces would it have? Does G have an Euler path?

Solution

G has 8 edges (since the sum of the degrees is 16). If G is planar, then it will have 4 faces (since $6 - 8 + 4 = 2$). G does not have an Euler path since there are more than 2 vertices of odd degree.

13

What is the smallest number of colors you need to properly color the vertices of K_7. Can you say whether K_7 is planar based on your answer?

Solution

7 colors. Thus K_7 is not planar (by the contrapositive of the Four Color Theorem).

14

What is the smallest number of colors you need to properly color the vertices of $K_{3,4}$? Can you say whether $K_{3,4}$ is planar based on your answer?

Solution

The chromatic number of $K_{3,4}$ is 2, since the graph is bipartite. You cannot say whether the graph is planar based on this coloring (the converse of the Four Color Theorem is not true). In fact, the graph is *not* planar, since it contains $K_{3,3}$ as a subgraph.

15

A dodecahedron is a regular convex polyhedron made up of 12 regular pentagons.

a. Suppose you color each pentagon with one of three colors. Prove that there must be two adjacent pentagons colored identically.
b. What if you use four colors?
c. What if instead of a dodecahedron you colored the faces of a cube?

Solution

For all these questions, we are really coloring the vertices of a graph. You get the graph by first drawing a planar representation of the polyhedron and then taking its planar dual: put a vertex in the center of each face (including the outside) and connect two vertices if their faces share an edge.

a. Since the planar dual of a dodecahedron contains a 5-wheel, it's chromatic number is at least 4. Alternatively, suppose you could color the faces using 3 colors without any two adjacent faces colored the same. Take any face and color it blue. The 5 pentagons bordering this blue pentagon cannot be colored blue. Color the first one red. Its two neighbors (adjacent to the blue pentagon) get colored green. The remaining 2 cannot be blue or green, but also cannot both be red since they are adjacent to each other. Thus a 4th color is needed.
b. The planar dual of the dodecahedron is itself a planar graph. Thus by the 4-color theorem, it can be colored using only 4 colors without two adjacent vertices (corresponding to the faces of the polyhedron) being colored identically.
c. The cube can be properly 3-colored. Color the “top” and “bottom” red, the “front” and “back” blue, and the “left” and “right” green.

16

If a planar graph G with 7 vertices divides the plane into 8 regions, how many edges must G have?

Solution

G has 13 edges, since we need $7-e+8=2$.

17

Consider the graph below:

1. Does the graph have an Euler path or circuit? Explain.
2. Is the graph planar? Explain.
3. Is the graph bipartite? Complete? Complete bipartite?
4. What is the chromatic number of the graph.

Solution

1. The graph does have an Euler path, but not an Euler circuit. There are exactly two vertices with odd degree. The path starts at one and ends at the other.
2. The graph is planar. Even though as it is drawn edges cross, it is easy to redraw it without edges crossing.
3. The graph is not bipartite (there is an odd cycle), nor complete.
4. The chromatic number of the graph is 3.

18

For each part below, say whether the statement is true or false. Explain why the true statements are true, and give counterexamples for the false statements.

a. Every bipartite graph is planar.
b. Every bipartite graph has chromatic number 2.
c. Every bipartite graph has an Euler path.
d. Every vertex of a bipartite graph has even degree.
e. A graph is bipartite if and only if the sum of the degrees of all the vertices is even.

Solution

a. False. For example, $K_{3,3}$ is not planar.
b. True. The graph is bipartite so it is possible to divide the vertices into two groups with no edges between vertices in the same group. Thus we can color all the vertices of one group red and the other group blue.
c. False. $K_{3,3}$ has 6 vertices with degree 3, so contains no Euler path.
d. False. $K_{3,3}$ again.
e. False. The sum of the degrees of all vertices is even for *all* graphs so this property does not imply that the graph is bipartite.

19

Consider the statement “If a graph is planar, then it has an Euler path.”

a. Write the converse of the statement.
b. Write the contrapositive of the statement.

c. Write the negation of the statement.
d. Is it possible for the contrapositive to be false? If it was, what would that tell you?
e. Is the original statement true or false? Prove your answer.
f. Is the converse of the statement true or false? Prove your answer.

Solution

a. If a graph has an Euler path, then it is planar.
b. If a graph does not have an Euler path, then it is not planar.
c. There is a graph which is planar and does not have an Euler path.
d. Yes. In fact, in this case it is because the original statement is false.
e. False. K_4 is planar but does not have an Euler path.
f. False. K_5 has an Euler path but is not planar.

20

Remember that a *tree* is a connected graph with no cycles.

a. Conjecture a relationship between a tree graph's vertices and edges. (For instance, can you have a tree with 5 vertices and 7 edges?)
b. Explain why every tree with at least 3 vertices has a leaf (i.e., a vertex of degree 1).
c. Prove your conjecture from part (a) by induction on the number of vertices. Hint: For the inductive step, you will assume that your conjecture is true for all trees with k vertices, and show it is also true for an arbitrary tree with $k+1$ vertices. Consider what happens when you cut off a leaf and then let it regrow.

CHAPTER OVERVIEW

11: Counting

One of the first things you learn in mathematics is how to count. Now we want to count large collections of things quickly and precisely. For example:

- In a group of 10 people, if everyone shakes hands with everyone else exactly once, how many handshakes took place?
- How many ways can you distribute 1010 girl scout cookies to 77 boy scouts?
- How many anagrams are there of “anagram”?

Before tackling questions like these, let's look at the basics of counting.

11.1: Additive and Multiplicative Principles

Investigate!

1. A restaurant offers 8 appetizers and 14 entrées. How many choices do you have if:
   a. you will eat one dish, either an appetizer or an entrée?
   b. you are extra hungry and want to eat both an appetizer and an entrée?
2. Think about the methods you used to solve question 1. Write down the rules for these methods.
3. Do your rules work? A standard deck of playing cards has 26 red cards and 12 face cards.
   a. How many ways can you select a card which is either red or a face card?
   b. How many ways can you select a card which is both red and a face card?
   c. How many ways can you select two cards so that the first one is red and the second one is a face card?

Consider this rather simple counting problem: at Red Dogs and Donuts, there are 14 varieties of donuts, and 16 types of hot dogs. If you want either a donut or a dog, how many options do you have? This isn't too hard, just add 14 and 16. Will that always work? What is important here?

Additive Principle

The *additive principle* states that if event A can occur in m ways, and event B can occur in n *disjoint* ways, then the event "A or B" can occur in $m+n$ ways.

It is important that the events be *disjoint*: i.e., that there is no way for A and B to both happen at the same time. For example, a standard deck of 52 cards contains 26 red cards and 12 face cards. However, the number of ways to select a card which is either red or a face card is not $26+12=38$. This is because there are 6 cards which are both red and face cards.

Example 11.1.1

How many two letter "words" start with either A or B? (A *word* is just a string of letters; it doesn't have to be English, or even pronounceable.)

Solution

First, how many two letter words start with A? We just need to select the second letter, which can be accomplished in 26 ways. So there are 26 words starting with A. There are also 26 words that start with B. To select a word which starts with either A or B, we can pick the word from the first 26 or the second 26, for a total of 52 words.

The additive principle also works with more than two events. Say, in addition to your 14 choices for donuts and 16 for dogs, you would also consider eating one of 15 waffles? How many choices do you have now? You would have $14+16+15=45$ options.

Example 11.1.2

How many two letter words start with one of the 5 vowels?

Solution

There are 26 two letter words starting with A, another 26 starting with E, and so on. We will have 5 groups of 26. So we add 26 to itself 5 times. Of course it would be easier to just multiply $5 \cdot 26$. We are really using the additive principle again, just using multiplication as a shortcut.

Example 11.1.3

Suppose you are going for some fro-yo. You can pick one of 6 yogurt choices, and one of 4 toppings. How many choices do you have?

Solution

Break your choices up into disjoint events: A are the choices with the first topping, B the choices featuring the second topping, and so on. There are four events; each can occur in 6 ways (one for each yogurt flavor). The events are disjoint, so the total number of choices is $6+6+6+6=24$.

Note that in both of the previous examples, when using the additive principle on a bunch of events all the same size, it is quicker to multiply. This really is the same, and not just because $6+6+6+6=4\cdot 6$. We can first select the topping in 4 ways (that is, we first select which of the disjoint events we will take). For each of those first 4 choices, we now have 6 choices of yogurt. We have:

Multiplicative Principle

The *multiplicative principle* states that if event A can occur in m ways, and each possibility for A allows for exactly n ways for event B, then the event "A and B" can occur in $m\cdot n$ ways.

The multiplicative principle generalizes to more than two events as well.

Example 11.1.4

How many license plates can you make out of three letters followed by three numerical digits?

Solution

Here we have six events: the first letter, the second letter, the third letter, the first digit, the second digit, and the third digit. The first three events can each happen in 26 ways; the last three can each happen in 10 ways. So the total number of license plates will be $26\cdot 26\cdot 26\cdot 10\cdot 10\cdot 10$, using the multiplicative principle.

Does this make sense? Think about how we would pick a license plate. How many choices we would have? First, we need to pick the first letter. There are 26 choices. Now for each of those, there are 26 choices for the second letter: 26 second letters with first letter A, 26 second letters with first letter B, and so on. We add 26 to itself 26 times. Or quicker: there are $26\cdot 26$ choices for the first two letters.

Now for each choice of the first two letters, we have 26 choices for the third letter. That is, 26 third letters for the first two letters AA, 26 choices for the third letter after starting AB, and so on. There are $26\cdot 26$ of these 26 third letter choices, for a total of $(26\cdot 26)\cdot 26$ choices for the first three letters. And for each of these $26\cdot 26\cdot 26$ choices of letters, we have a bunch of choices for the remaining digits.

In fact, there are going to be exactly 1000 choices for the numbers. We can see this because there are 1000 three-digit numbers (000 through 999). This is 10 choices for the first digit, 10 for the second, and 10 for the third. The multiplicative principle says we multiply: $10\cdot 10\cdot 10=1000$.

All together, there were 26^3 choices for the three letters, and 10^3 choices for the numbers, so we have a total of $26^3\cdot 10^3$ choices of license plates.

Careful: "and" doesn't mean "times." For example, how many playing cards are both red and a face card? Not $26\cdot 12$. The answer is 6, and we needed to know something about cards to answer that question.

Another caution: how many ways can you select two cards, so that the first one is a red card and the second one is a face card? This looks more like the multiplicative principle (you are counting two separate events) but the answer is not $26\cdot 12$ here either. The problem is that while there are 26 ways for the first card to be selected, it is not the case that *for each* of those there are 12 ways to select the second card. If the first card was both red and a face card, then there would be only 11 choices for the second card. [1] To solve this problem, you could break it into two cases. First, count how many ways there are to select the two cards when the first card is a red non-face card. Second, count how many ways when the first card is a red face card. Doing so makes the events in each separate case independent, so the multiplicative principle can be applied.

Counting functions

How many functions $f:\{1,2,3,4,5\}\to\{a,b,c,d\}$ are there?

Solution

Remember that a function sends each element of the domain to exactly one element of the codomain. To determine a function, we just need to specify the image of each element in the domain. Where can we send 1? There are 4 choices. Where can we send 2? Again, 4 choices. What we have here is 5 "events" (picking the image of an element in the domain) each of which can happen in 4 ways (the choices for that image). Thus there are $4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 = 4^5$ functions.

This is more than just an example of how we can use the multiplicative principle in a particular counting question. What we have here is a general interpretation of certain applications of the multiplicative principle using rigorously defined mathematical objects: functions. Whenever we have a counting question that asks for the the number of outcomes of a repeated event, we can interpret that as asking for the number of functions from $\{1, 2, \ldots, n\}$(where n is the number of times the event is repeated) to $\{1, 2, \ldots, k\}$(where k is the number of ways that event can occur).

Counting With Sets

Do you believe the additive and multiplicative principles? How would you convince someone they are correct? This is surprisingly difficult. They seem so simple, so obvious. But why do they work?

To make things clearer, and more mathematically rigorous, we will use sets. Do not skip this section! It might seem like we are just trying to give a proof of these principles, but we are doing a lot more. If we understand the additive and multiplicative principles rigorously, we will be better at applying them, and knowing when and when not to apply them at all.

We will look at the additive and multiplicative principles in a slightly different way. Instead of thinking about event A and event B, we want to think of a set A and a set B. The sets will contain all the different ways the event can happen. (It will be helpful to be able to switch back and forth between these two models when checking that we have counted correctly.) Here's what we mean:

Example 11.1.6

Suppose you own 9 shirts and 5 pairs of pants.

1. How many outfits can you make?
2. If today is half-naked-day, and you will wear only a shirt or only a pair of pants, how many choices do you have?

Answer

By now you should agree that the answer to the first question is $9 \cdot 5 = 45$ and the answer to the second question is $9 + 5 = 14$. These are the multiplicative and additive principles. There are two events: picking a shirt and picking a pair of pants. The first event can happen in 9 ways and the second event can happen in 5 ways. To get both a shirt and a pair of pants, you multiply. To get just one article of clothing, you add.

Now look at this using sets. There are two sets, call them S and P. The set S contains all 9 shirts so $|S| = 9$ while $|P| = 5$, since there are 5 elements in the set P (namely your 5 pairs of pants). What are we asking in terms of these sets? Well in question 2, we really want $|S \cup P|$, the number of elements in the union of shirts and pants. This is just $|S| + |P|$ (since there is no overlap; $|S \cap P| = 0$). Question 1 is slightly more complicated. Your first guess might be to find $|S \cap P|$, but this is not right (there is nothing in the intersection). We are not asking for how many clothing items are both a shirt and a pair of pants. Instead, we want one of each. We could think of this as asking how many pairs (x, y) there are, where x is a shirt and y is a pair of pants. As we will soon verify, this number is $|S| \cdot |P|$.

From this example we can see right away how to rephrase our additive principle in terms of sets:

Additive Principle (with sets)

Given two sets A and B, if $A \cap B = \emptyset$ (that is, if there is no element in common to both A and B), then

$$|A \cup B| = |A| + |B| .$$

This hardly needs a proof. To find $A \cup B$, you take everything in A and throw in everything in B. Since there is no element in both sets already, you will have $|A|$ things and add $|B|$ new things to it. This is what adding does! Of course, we can easily extend this to any number of disjoint sets.

From the example above, we see that in order to investigate the multiplicative principle carefully, we need to consider ordered pairs. We should define this carefully:

Cartesian Product

Given sets A and B, we can form the *set* $A \times B = \{(x, y) : x \in A \wedge y \in B\}$ to be the set of all ordered pairs (x, y) where x is an element of A and y is an element of B. We call $A \times B$ the *Cartesian product* of A and B.

Example 11.1.7

Let $A = \{1, 2\}$ and $B = \{3, 4, 5\}$. Find $A \times B$.

Answer

We want to find ordered pairs (a, b) where a can be either 1 or 2 and b can be either 3, 4, or 5. $A \times B$ is the set of all of these pairs:

$$A \times B = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$$

The question is, what is $|A \times B|$? To figure this out, write out $A \times B$. Let $A = \{a_1, a_2, a_3, \ldots, a_m\}$ and $B = \{b_1, b_2, b_3, \ldots, b_n\}$ (so $|A| = m$ and $|B| = n$). The set $A \times B$ contains all pairs with the first half of the pair being some $a_i \in A$ and the second being one of the $b_j \in B$. In other words:

$$\begin{aligned} A \times B = \{ &(a_1, b_1), (a_1, b_2), (a_1, b_3), \ldots (a_1, b_n), \\ &(a_2, b_1), (a_2, b_2), (a_2, b_3), \ldots, (a_2, b_n), \\ &(a_3, b_1), (a_3, b_2), (a_3, b_3), \ldots, (a_3, b_n), \\ &\vdots \\ &(a_m, b_1), (a_m, b_2), (a_m, b_3), \ldots, (a_m, b_n)\}. \end{aligned}$$

Notice what we have done here: we made m rows of n pairs, for a total of $m \cdot n$ pairs.

Each row above is really $\{a_i\} \times B$ for some $a_i \in A$. That is, we fixed the A-element. Broken up this way, we have

$$A \times B = (\{a_1\} \times B) \cup (\{a_2\} \times B) \cup (\{a_3\} \times B) \cup \cdots \cup (\{a_m\} \times B).$$

So $A \times B$ is really the union of m disjoint sets. Each of those sets has n elements in them. The total (using the additive principle) is $n + n + n + \cdots + n = m \cdot n$.

To summarize:

Multiplicative Principle (with sets)

Given two sets A and B, we have $|A \times B| = |A| \cdot |B|$.

Again, we can easily extend this to any number of sets.

Principle of Inclusion/Exclusion

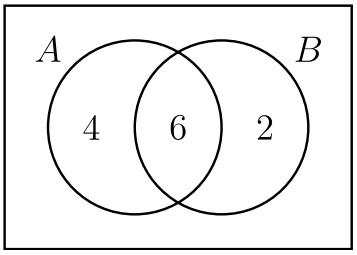
Investigate!

A recent buzz marketing campaign for *Village Inn* surveyed patrons on their pie preferences. People were asked whether they enjoyed (A) Apple, (B) Blueberry or (C) Cherry pie (respondents answered yes or no to each type of pie, and could say yes to more than one type). The following table shows the results of the survey.

Pies enjoyed:	A	B	C	AB	AC	BC	ABC
Number of people:	20	13	26	9	15	7	5

How many of those asked enjoy at least one of the kinds of pie? Also, explain why the answer is not 95.

While we are thinking about sets, consider what happens to the additive principle when the sets are NOT disjoint. Suppose we want to find $|A \cup B|$ and know that $|A| = 10$ and $|B| = 8$. This is not enough information though. We do not know how many of the 8 elements in B are also elements of A. However, if we also know that $|A \cap B| = 6$, then we can say exactly how many elements are in A, and, of those, how many are in B and how many are not (6 of the 10 elements are in B, so 4 are in A but not in B). We could fill in a Venn diagram as follows:



This says there are 6 elements in $A \cap B$, 4 elements in $A \setminus B$ and 2 elements in $B \setminus A$. Now *these* three sets *are* disjoint, so we can use the additive principle to find the number of elements in $A \cup B$. It is $6 + 4 + 2 = 12$.

This will always work, but drawing a Venn diagram is more than we need to do. In fact, it would be nice to relate this problem to the case where A and B are disjoint. Is there one rule we can make that works in either case?

Here is another way to get the answer to the problem above. Start by just adding $|A| + |B|$. This is $10 + 8 = 18$, which would be the answer if $|A \cap B| = 0$. We see that we are off by exactly 6, which just so happens to be $|A \cap B|$. So perhaps we guess,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

This works for this one example. Will it always work? Think about what we are doing here. We want to know how many things are either in A or B (or both). We can throw in everything in A, and everything in B. This would give $|A| + |B|$ many elements. But of course when you actually take the union, you do not repeat elements that are in both. So far we have counted every element in $A \cap B$ exactly twice: once when we put in the elements from A and once when we included the elements from B. We correct by subtracting out the number of elements we have counted twice. So we added them in twice, subtracted once, leaving them counted only one time.

In other words, we have:

Cardinality of a union (2 sets)

For any finite sets A and B,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

We can do something similar with three sets.

Example 11.1.8

An examination in three subjects, Algebra, Biology, and Chemistry, was taken by 41 students. The following table shows how many students failed in each single subject and in their various combinations:

Subject:	A	B	C	AB	AC	BC	ABC
Failed:	12	5	8	2	6	3	1

How many students failed at least one subject?

Solution

The answer is not 37, even though the sum of the numbers above is 37. For example, while 12 students failed Algebra, 2 of those students also failed Biology, 6 also failed Chemestry, and 1 of those failed all three subjects. In fact, that 1 student who failed all three subjects is counted a total of 7 times in the total 37. To clarify things, let us think of the students who failed Algebra as the elements of the set A, and similarly for sets B and C. The one student who failed all three subjects is the lone element of the set $A \cap B \cap C$. Thus, in Venn diagrams:

Now let's fill in the other intersections. We know $A \cap B$ contains 2 elements, but 1 element has already been counted. So we should put a 1 in the region where A and B intersect (but C does not). Similarly, we calculate the cardinality of $(A \cap C) \setminus B$, and $(B \cap C) \setminus A$:

Next, we determine the numbers which should go in the remaining regions, including outside of all three circles. This last number is the number of students who did not fail any subject:

We found 5 goes in the "A only" region because the entire circle for A needed to have a total of 12, and 7 were already accounted for. Similarly, we calculate the "B only" region to contain only 1 student and the "C only" region to contain no students.

Thus the number of students who failed at least one class is 15 (the sum of the numbers in each of the eight disjoint regions). The number of students who passed all three classes is 26: the total number of students, 41, less the 15 who failed at least one class.

Note that we can also answer other questions. For example, now many students failed just Chemistry? None. How many passed Algebra but failed both Biology and Chemistry? This corresponds to the region inside both B and C but outside of A, containing 2 students.

Could we have solved the problem above in an algebraic way? While the additive principle generalizes to any number of sets, when we add a third set here, we must be careful. With two sets, we needed to know the cardinalities of A, B, and $A \cap B$ in order to find the cardinality of $A \cup B$. With three sets we need more information. There are more ways the sets can combine. Not surprisingly then, the formula for cardinality of the union of three non-disjoint sets is more complicated:

Cardinality of a union (3 sets)

For any finite sets A, B, and C,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

To determine how many elements are in at least one of A, B, or C we add up all the elements in each of those sets. However, when we do that, any element in both A and B is counted twice. Also, each element in both A and C is counted twice, as are elements in B and C, so we take each of those out of our sum once. But now what about the elements which are in $A \cap B \cap C$ (in all three sets)? We added them in three times, but also removed them three times. They have not yet been counted. Thus we add those elements back in at the end.

Returning to our example above, we have $|A| = 12$, $|B| = 5$, $|C| = 8$. We also have $|A \cap B| = 2$, $|A \cap C| = 6$, $|B \cap C| = 3$, and $|A \cap B \cap C| = 1$. Therefore:

$$|A \cup B \cup C| = 12 + 5 + 8 - 2 - 6 - 3 + 1 = 15$$

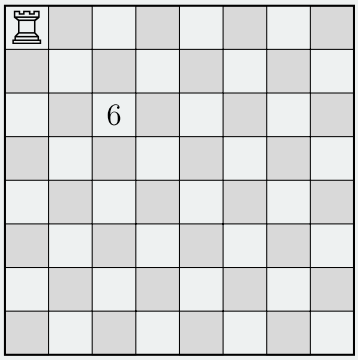
This is what we got when we solved the problem using Venn diagrams.

This process of adding in, then taking out, then adding back in, and so on is called the *Principle of Inclusion/Exclusion*, or simply PIE. We will return to this counting technique later to solve for more complicated problems (involving more than 3 sets).

11.2: Binomial Coefficients

Investigate!

In chess, a rook can move only in straight lines (not diagonally). Fill in each square of the chess board below with the number of different shortest paths the rook, in the upper left corner, can take to get to that square. For example, one square is already filled in. There are six different paths from the rook to the square: DDRR (down down right right), DRDR, DRRD, RDDR, RDRD and RRDD.



Here are some apparently different discrete objects we can count: subsets, bit strings, lattice paths, and binomial coefficients. We will give an example of each type of counting problem (and say what these things even are). As we will see, these counting problems are surprisingly similar.

Subsets

Subsets should be familiar, otherwise read over Section 0.3 again. Suppose we look at the set $A = \{1, 2, 3, 4, 5\}$. How many subsets of A contain exactly 3 elements?

First, a simpler question: How many subsets of A are there total? In other words, what is $|\mathcal{P}(A)|$ (the cardinality of the power set of A)? Think about how we would build a subset. We need to decide, for each of the elements of A, whether or not to include the element in our subset. So we need to decide "yes" or "no" for the element 1. And for each choice we make, we need to decide "yes" or "no" for the element 2. And so on. For each of the 5 elements, we have 2 choices. Therefore the number of subsets is simply $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5$ (by the multiplicative principle).

Of those 32 subsets, how many have 3 elements? This is not obvious. Note that we cannot just use the multiplicative principle. Maybe we want to say we have 2 choices (yes/no) for the first element, 2 choices for the second, 2 choices for the third, and then only 1 choice for the other two. But what if we said "no" to one of the first three elements? Then we would have two choices for the 4th element. What a mess!

Another (bad) idea: we need to pick three elements to be in our subset. There are 5 elements to choose from. So there are 5 choices for the first element, and for each of those 4 choices for the second, and then 3 for the third (last) element. The multiplicative principle would say then that there are a total of $5 \cdot 4 \cdot 3 = 60$ ways to select the 3 element subset. But this cannot be correct ($60 > 32$ for one thing). One of the outcomes we would get from these choices would be the set $\{3, 2, 5\}$,by choosing the element 3 first, then the element 2, then the element 5. Another outcome would be $\{5, 2, 3\}$ by choosing the element 5 first, then the element 2, then the element 3. But these are the same set! We can correct this by dividing: for each set of three elements, there are 6 outcomes counted amoung our 60 (since there are 3 choices for which element we list first, 2 for which we list second, and 1 for which we list last). So we expect there to be 10 3-element subsets of A.

Is this right? Well, we could list out all 10 of them, being very systematic in doing so, to make sure we don't miss any or list any twice. Or we could try to count how many subsets of A *don't* have 3 elements in them. How many have no elements? Just 1 (the empty set). How many have 5? Again, just 1. These are the cases in which we say "no" to all elements, or "yes" to all elements. Okay, what about the subsets which contain a single element? There are 5 of these. We must say "yes" to exactly one element, and there are 5 to choose from. This is also the number of subsets containing 4 elements. Those are the ones for which we must say "no" to exactly one element.

So far we have counted 12 of the 32 subsets. We have not yet counted the subsets with cardinality 2 and with cardinality 3. There are a total of 20 subsets left to split up between these two groups. But the number of each must be the same! If we say "yes" to exactly two elements, that can be accomplished in exactly the same number of ways as the number of ways we can say "no" to exactly two elements. So the number of 2-element subsets is equal to the number of 3-element subsets. Together there are 20 of these subsets, so 10 each.

Number of elements:	0	1	2	3	4	5
Number of subsets:	1	5	10	10	5	1

Bit Strings

"Bit" is short for "binary digit," so a *bit string* is a string of binary digits. The *binary digits* are simply the numbers 0 and 1. All of the following are bit strings:

$$1001 \quad 0 \quad 1111 \quad 1010101010$$

The number of bits (0's or 1's) in the string is the *length* of the string; the strings above have lengths 4, 1, 4, and 10 respectively. We also can ask how many of the bits are 1's. The number of 1's in a bit string is the *weight* of the string; the weights of the above strings are 2, 0, 4, and 5 respectively.

Definition: Bit Strings

- An n-*bit string* is a bit string of length n. That is, it is a string containing n symbols, each of which is a bit, either 0 or 1.
- The *weight* of a bit string is the number of 1's in it.
- $\mathbf{B}^n$ is the *set* of all n-bit strings.
- $\mathbf{B}_k^n$ is the set of all n-bit strings of weight k.

For example, the elements of the set $\mathbf{B}_2^3$ are the bit strings 011, 101, and 110. Those are the only strings containing three bits exactly two of which are 1's.

The counting questions: How many bit strings have length 5? How many of those have weight 3? In other words, we are asking for the cardinalities $|\mathbf{B}^5|$ and $|\mathbf{B}_3^5|$.

To find the number of 5-bit strings is straight forward. We have 5 bits, and each can either be a 0 or a 1. So there are 2 choices for the first bit, 2 choices for the second, and so on. By the multiplicative principle, there are $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32$ such strings.

Finding the number of 5-bit strings of weight 3 is harder. Think about how such a string could start. The first bit must be either a 0 or a 1. In the first case (the string starts with a 0), we must then decide on four more bits. To have a total of three 1's, among those four remaining bits there must be three 1's. To count all of these strings, we must include all 4-bit strings of weight 3. In the second case (the string starts with a 1), we still have four bits to choose, but now only two of them can be 1's, so we should look at all the 4-bit strings of weight 2. So the strings in $\mathbf{B}_3^5$ all have the form $1\mathbf{B}_2^4$ (that is, a 1 followed by a string from $\mathbf{B}_2^4$) or $0\mathbf{B}_3^4$. These two sets are disjoint, so we can use the additive principle:

$$|\mathbf{B}_3^5| = |\mathbf{B}_2^4| + |\mathbf{B}_3^4|.$$

This is an example of a *recurrence relation*. We represented one instance of our counting problem in terms of two simpler instances of the problem. If only we knew the cardinalities of $\mathbf{B}_2^4$ and $\mathbf{B}_3^4$. Repeating the same reasoning,

$$|\mathbf{B}_2^4| = |\mathbf{B}_1^3| + |\mathbf{B}_2^3| \quad \text{and} \quad |\mathbf{B}_3^4| = |\mathbf{B}_2^3| + |\mathbf{B}_3^3|.$$

We can keep going down, but this should be good enough. Both $\mathbf{B}_1^3$ and $\mathbf{B}_2^3$ contain 3 bit strings: we must pick one of the three bits to be a 1 (three ways to do that) or one of the three bits to be a 0 (three ways to do that). Also, $\mathbf{B}_3^3$ contains just one string: 111. Thus $|\mathbf{B}_2^4| = 6$ and $|\mathbf{B}_3^4| = 4$, which puts $\mathbf{B}_3^5$ at a total of 10 strings.

But wait —32 and 10 were the answers to the counting questions about subsets. Coincidence? Not at all. Each bit string can be thought of as a *code* for a subset. For the set $A = \{1, 2, 3, 4, 5\}$, we would use 5-bit strings, one bit for each element of A. Each bit in the string is a 0 if its corresponding element of A is not in the subset, and a 1 if the element of A is in the subset. Remember,

deciding the subset amounted to a sequence of five yes/no votes for the elements of A. Instead of yes, we put a 1; instead of no, we put a 0.

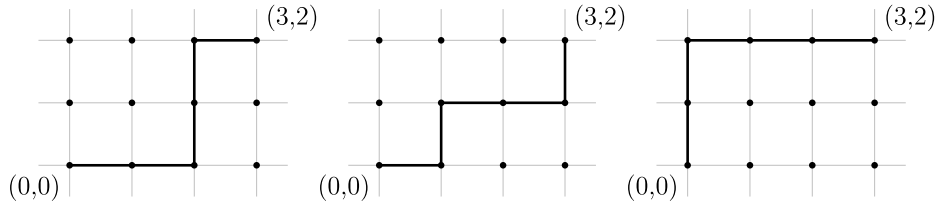
For example, the bit string 11001 represents the subset $\{1,2,5\}$ since the first, second and fifth bits are 1's. The subset $\{3,5\}$ would be coded by the string 00101. What we really have here is a bijection from $\mathcal{P}(A)$ to $\mathbf{B}^5$.

Now for a subset to contain exactly three elements, the corresponding bit string must contain exactly three 1's. In other words, the weight must be 3. Thus counting the number of 3-element subsets of A is the same as counting the number 5-bit strings of weight 3.

Lattice Paths

The *integer lattice* is the set of all points in the Cartesian plane for which both the x and y coordinates are integers. If you like to draw graphs on graph paper, the lattice is the set of all the intersections of the grid lines.

A *lattice path* is one of the shortest possible paths connecting two points on the lattice, moving only horizontally and vertically. For example, here are three possible lattice paths from the points $(0,0)$ to $(3,2)$:

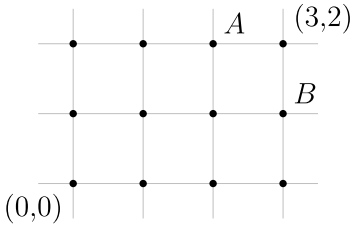


Notice to ensure the path is the *shortest* possible, each move must be either to the right or up. Additionally, in this case, note that no matter what path we take, we must make three steps right and two steps up. No matter what order we make these steps, there will always be 5 steps. Thus each path has *length* 5.

The counting question: how many lattice paths are there between $(0,0)$ and $(3,2)$? We could try to draw all of these, or instead of drawing them, maybe just list which direction we travel on each of the 5 steps. One path might be RRUUR, or maybe UURRR, or perhaps RURRU (those correspond to the three paths drawn above). So how many such strings of R's and U's are there?

Notice that each of these strings must contain 5 symbols. Exactly 3 of them must be R's (since our destination is 3 units to the right). This seems awfully familiar. In fact, what if we used 1's instead of R's and 0's instead of U's? Then we would just have 5-bit strings of weight 3. There are 10 of those, so there are 10 lattice paths from (0,0) to (3,2).

The correspondence between bit strings and lattice paths does not stop there. Here is another way to count lattice paths. Consider the lattice shown below:



Any lattice path from (0,0) to (3,2) must pass through exactly one of A and B. The point A is 4 steps away from (0,0) and two of them are towards the right. The number of lattice paths to A is the same as the number of 4-bit strings of weight 2, namely 6. The point B is 4 steps away from (0,0), but now 3 of them are towards the right. So the number of paths to point B is the same as the number of 4-bit strings of weight 3, namely 4. So the total number of paths to (3,2) is just $6+4$. This is the same way we calculated the number of 5-bit strings of weight 3. The point: the exact same recurrence relation exists for bit strings and for lattice paths.

Binomial Coefficients

Binomial coefficients are the coefficients in the expanded version of a binomial, such as $(x+y)^5$. What happens when we multiply such a binomial out? We will expand $(x+y)^n$ for various values of n. Each of these are done by multiplying everything out (i.e., FOIL-ing) and then collecting like terms.

$$(x+y)^1 = x+y$$
$$(x+y)^2 = x^2+2xy+y^2$$
$$(x+y)^3 = x^3+3x^2y+3xy^2+y^3$$
$$(x+y)^4 = x^4+4x^3y+6x^2y^2+4xy^3+y^4.$$

In fact, there is a quicker way to expand the above binomials. For example, consider the next one, $(x+y)^5$. What we are really doing is multiplying out,

$$(x+y)(x+y)(x+y)(x+y)(x+y).$$

If that looks daunting, go back to the case of $(x+y)^3 = (x+y)(x+y)(x+y)$. Why do we only have one x^3 and y^3 but three x^2y and xy^2 terms? Every time we distribute over an $(x+y)$ we create two copies of what is left, one multiplied by x, the other multiplied by y. To get x^3, we need to pick the "multiplied by x" side every time (we don't have any y's in the term). This will only happen once. On the other hand, to get x^2y we need to select the x side twice and the y side once. In other words, we need to pick one of the three $(x+y)$ terms to "contribute" their y.

Similarly, in the expansion of $(x+y)^5$, there will be only one x^5 term and one y^5 term. This is because to get an x^5, we need to use the x term in each of the copies of the binomial $(x+y)$, and similarly for y^5. What about x^4y? To get terms like this, we need to use four x's and one y, so we need exactly one of the five binomials to contribute a y. There are 5 choices for this, so there are 5 ways to get x^4y, so the coefficient of x^4y is 5. This is also the coefficient for xy^4 for the same (but opposite) reason: there are 5 ways to pick which of the 5 binomials contribute the single x. So far we have

$$(x+y)^5 = x^5+5x^4y+\underline{?}\,x^3y^2+\underline{?}\,x^2y^3+5xy^4+y^5.$$

We still need the coefficients of x^3y^2 and x^2y^3. In both cases, we need to pick exactly 3 of the 5 binomials to contribute one variable, the other two to contribute the other. Wait. This sounds familiar. We have 5 things, each can be one of two things, and we need a total of 3 of one of them. That's just like taking 5 bits and making sure exactly 3 of them are 1's. So the coefficient of x^3y^2 (and also x^2y^3) will be exactly the same as the number of bit strings of length 5 and weight 3, which we found earlier to be 10. So we have:

$$(x+y)^5 = x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5.$$

These numbers we keep seeing over and over again. They are the number of subsets of a particular size, the number of bit strings of a particular weight, the number of lattice paths, and the coefficients of these binomial products. We will call them *binomial coefficients*. We even have a special symbol for them: $\binom{n}{k}$.

Definition: Binomial Coefficients

For each integer $n \geq 0$ and integer k with $0 \leq k \leq n$ there is a number

$$\binom{n}{k}$$

read "n choose k." We have:

- $\binom{n}{k} = |\mathbf{B}_k^n|$, the number of n-bit strings of weight k.
- $\binom{n}{k}$ is the number of subsets of a set of size n each with cardinality k.
- $\binom{n}{k}$ is the number of lattice paths of length n containing k steps to the right.
- $\binom{n}{k}$ is the coefficient of $x^k y^{n-k}$ in the expansion of $(x+y)^n$.
- $\binom{n}{k}$ is the number of ways to select k objects from a total of n objects.

The last bullet point is usually taken as the definition of $\binom{n}{k}$. Out of n objects we must choose k of them, so there are n choose k ways of doing this. Each of our counting problems above can be viewed in this way:

- How many subsets of $\{1,2,3,4,5\}$contain exactly 3 elements? We must choose 3 of the 5 elements to be in our subset. There are $\binom{5}{3}$ ways to do this, so there are $\binom{5}{3}$ such subsets.

- How many bit strings have length 5 and weight 3? We must choose 3 of the 5 bits to be 1's. There are $\binom{5}{3}$ ways to do this, so there are $\binom{5}{3}$ such bit strings.
- How many lattice paths are there from (0,0) to (3,2)? We must choose 3 of the 5 steps to be towards the right. There are $\binom{5}{3}$ ways to do this, so there are $\binom{5}{3}$ such lattice paths.
- What is the coefficient of x^3y^2 in the expansion of $(x+y)^5$? We must choose 3 of the 5 copies of the binomial to contribute an x. There are $\binom{5}{3}$ ways to do this, so the coefficient is $\binom{5}{3}$.

It should be clear that in each case above, we have the right answer. All we had to do is phrase the question correctly and it became obvious that $\binom{5}{3}$ is correct. However, this does not tell us that the answer is in fact 10 in each case. We will eventually find a formula for $\binom{n}{k}$, but for now, look back at how we arrived at the answer 10 in our counting problems above. It all came down to bit strings, and we have a recurrence relation for bit strings:

$$|\mathbf{B}_k^n| = |\mathbf{B}_{k-1}^{n-1}| + |\mathbf{B}_k^{n-1}|.$$

Remember, this is because we can start the bit string with either a 1 or a 0. In both cases, we have $n-1$ more bits to pick. The strings starting with 1 must contain $k-1$ more 1's, while the strings starting with 0 still need k more 1's.

Since $|\mathbf{B}_k^n| = \binom{n}{k}$, the same recurrence relation holds for binomial coefficients:

Recurrence relation for $\binom{n}{k}$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

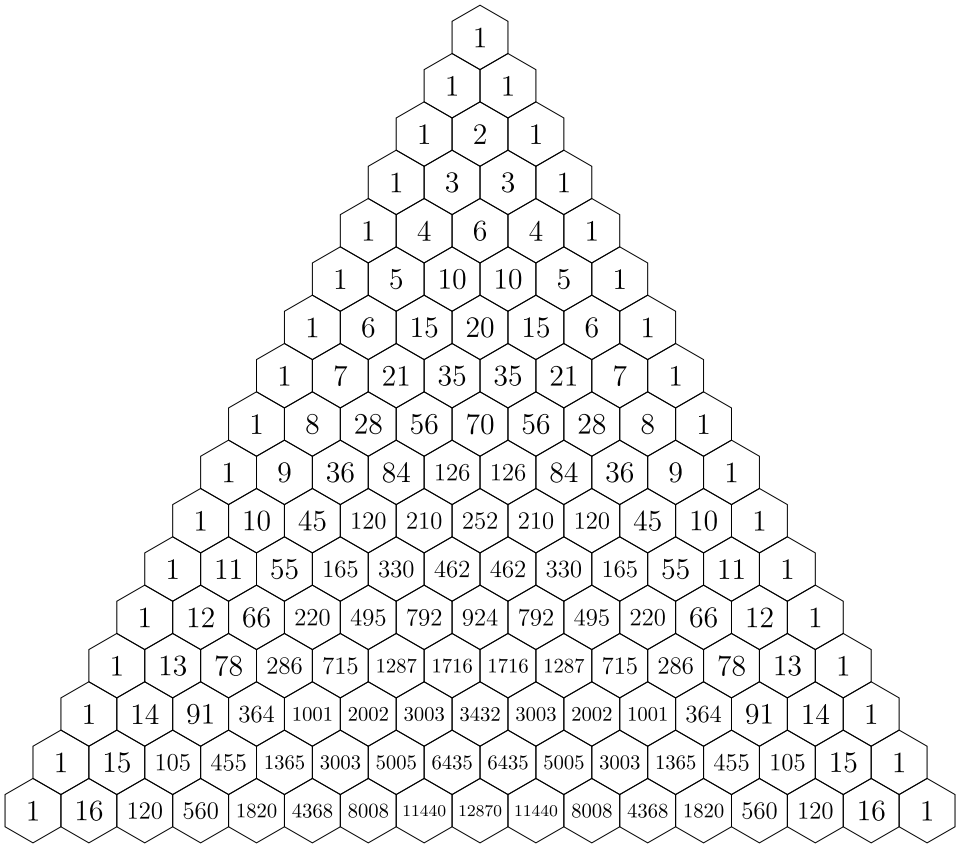
Pascal's Triangle

Let's arrange the binomial coefficients $\binom{n}{k}$ into a triangle like follows:

$$\begin{array}{ccccccccc}
 & & & \binom{0}{0} & & & & & \\
 & & \binom{1}{0} & & \binom{1}{1} & & & & \\
 & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}$$

This can continue as far down as we like. The recurrence relation for $\binom{n}{k}$ tells us that each entry in the triangle is the sum of the two entries above it. The entries on the sides of the triangle are always 1. This is because $\binom{n}{0} = 1$ for all n since there is only one way to pick 0 of n objects and $\binom{n}{n} = 1$ since there is one way to select all n out of n objects. Using the recurrence relation, and the fact that the sides of the triangle are 1's, we can easily replace all the entries above with the correct values of $\binom{n}{k}$. Doing so gives us *Pascal's triangle*.

Pascal's Triangle



We can use Pascal's triangle to calculate binomial coefficients. For example, using the triangle below, we can find $\binom{12}{6} = 924$.

11.3: Combinations and Permutations

Investigate!

You have a bunch of chips which come in five different colors: red, blue, green, purple and yellow.

1. How many different two-chip stacks can you make if the bottom chip must be red or blue? Explain your answer using both the additive and multiplicative principles.
2. How many different three-chip stacks can you make if the bottom chip must be red or blue and the top chip must be green, purple or yellow? How does this problem relate to the previous one?
3. How many different three-chip stacks are there in which no color is repeated? What about four-chip stacks?
4. Suppose you wanted to take three different colored chips and put them in your pocket. How many different choices do you have? What if you wanted four different colored chips? How do these problems relate to the previous one?

A *permutation* is a (possible) rearrangement of objects. For example, there are 6 permutations of the letters *a*, *b*, *c*:

$$abc,\ \ acb,\ \ bac,\ \ bca,\ \ cab,\ \ cba.$$

We know that we have them all listed above —there are 3 choices for which letter we put first, then 2 choices for which letter comes next, which leaves only 1 choice for the last letter. The multiplicative principle says we multiply $3 \cdot 2 \cdot 1$.

Example 11.3.1

How many permutations are there of the letters *a*, *b*, *c*, *d*, *e*, *f*?

Answer

We do NOT want to try to list all of these out. However, if we did, we would need to pick a letter to write down first. There are 6 choices for that letter. For each choice of first letter, there are 5 choices for the second letter (we cannot repeat the first letter; we are rearranging letters and only have one of each), and for each of those, there are 4 choices for the third, 3 choices for the fourth, 2 choices for the fifth and finally only 1 choice for the last letter. So there are $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$ permutations of the 6 letters.

A piece of notation is helpful here: $n!$, read "n factorial", is the product of all positive integers less than or equal to n (for reasons of convenience, we also define 0! to be 1). So the number of permutation of 6 letters, as seen in the previous example is $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$. This generalizes:

Permutations of n elements

There are $n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1$ permutations of n (distinct) elements.

Counting Bijective Functions

How many functions $f : \{1, 2, \ldots, 8\} \to \{1, 2, \ldots, 8\}$are *bijective*?

Solution

Remember what it means for a function to be bijective: each element in the codomain must be the image of exactly one element of the domain. Using two-line notation, we could write one of these bijections as

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 8 & 7 & 6 & 2 & 4 \end{pmatrix}$$

What we are really doing is just rearranging the elements of the codomain, so we are creating a permutation of 8 elements. In fact, "permutation" is another term used to describe bijective functions from a finite set to itself.

If you believe this, then you see the answer must be $8! = 8 \cdot 7 \cdot \cdots \cdot 1 = 40320$. You can see this directly as well: for each element of the domain, we must pick a distinct element of the codomain to map to. There are 8 choices for where to send 1, then 7 choices for where to send 2, and so on. We multiply using the multiplicative principle.

Sometimes we do not want to permute all of the letters/numbers/elements we are given.

Example 11.3.3

How many 4 letter "words" can you make from the letters *a* through *f*, with no repeated letters?

Solution

This is just like the problem of permuting 4 letters, only now we have more choices for each letter. For the first letter, there are 6 choices. For each of those, there are 5 choices for the second letter. Then there are 4 choices for the third letter, and 3 choices for the last letter. The total number of words is \(6\cdot 5\cdot 4 \cdot 3 = 360\text{.}\) This is not \(6!\) because we never multiplied by 2 and 1. We could start with \(6!\) and then cancel the 2 and 1, and thus write \(\frac{6!}{2!}\text{.}\)

In general, we can ask how many permutations exist of k objects choosing those objects from a larger collection of n objects. (In the example above, $k = 4,$ and $n = 6.$) We write this number $P(n, k)$ and sometimes call it a *k-permutation of n elements*. From the example above, we see that to compute $P(n, k)$ we must apply the multiplicative principle to k numbers, starting with n and counting backwards. For example

$$P(10, 4) = 10 \cdot 9 \cdot 8 \cdot 7.$$

Notice again that $P(10, 4)$ starts out looking like $10!,$ but we stop after 7. We can formally account for this "stopping" by dividing away the part of the factorial we do not want:

$$P(10, 4) = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = \frac{10!}{6!}.$$

Careful: The factorial in the denominator is not $4!$ but rather $(10 - 4)!$.

k-permutations of n elements

$P(n, k)$ is the number of k-permutations of n elements, the number of ways to arrange k objects chosen from n distinct objects.

$$P(n, k) = \frac{n!}{(n - k)!}.$$

Note that when $n = k,$ we have $P(n, n) = \frac{n!}{(n-n)!} = n!$ (since we defined $0!$ to be 1). This makes sense —we already know $n!$ gives the number of permutations of all n objects.

Counting injective functions

How many functions $f : \{1, 2, 3\} \to \{1, 2, 3, 4, 5, 6, 7, 8\}$ are *injective*?

Solution

Note that it doesn't make sense to ask for the number of *bijections* here, as there are none (because the codomain is larger than the domain, there are no surjections). But for a function to be injective, we just can't use an element of the codomain more than once.

We need to pick an element from the codomain to be the image of 1. There are 8 choices. Then we need to pick one of the remaining 7 elements to be the image of 2. Finally, one of the remaining 6 elements must be the image of 3. So the total number of functions is $8 \cdot 7 \cdot 6 = P(8, 3)$.

What this demonstrates in general is that the number of injections $f : A \to B,$ where $|A| = k$ and $|B| = n,$ is $P(n, k)$.

Here is another way to find the number of k-permutations of n elements: first select which k elements will be in the permutation, then count how many ways there are to arrange them. Once you have selected the k objects, we know there are $k!$ ways to arrange (permute) them. But how do you select k objects from the n? You have n objects, and you need to *choose* k of them. You can do

that in $\binom{n}{k}$ ways. Then for each choice of those k elements, we can permute *them* in $k!$ ways. Using the multiplicative principle, we get another formula for $P(n,k)$:

$$P(n,k) = \binom{n}{k} \cdot k!.$$

Now since we have a closed formula for $P(n,k)$ already, we can substitute that in:

$$\frac{n!}{(n-k)!} = \binom{n}{k} \cdot k!.$$

If we divide both sides by $k!$ we get a closed formula for $\binom{n}{k}$.

Closed formula for $\binom{n}{k}$

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

We say $P(n,k)$ counts *permutations*, and $\binom{n}{k}$ counts *combinations*. The formulas for each are very similar, there is just an extra $k!$ in the denominator of $\binom{n}{k}$. That extra $k!$ accounts for the fact that $\binom{n}{k}$ does not distinguish between the different orders that the k objects can appear in. We are just selecting (or choosing) the k objects, not arranging them. Perhaps "combination" is a misleading label. We don't mean it like a combination lock (where the order would definitely matter). Perhaps a better metaphor is a combination of flavors — you just need to decide which flavors to combine, not the order in which to combine them.

To further illustrate the connection between combinations and permutations, we close with an example.

Example 11.3.5

You decide to have a dinner party. Even though you are incredibly popular and have 14 different friends, you only have enough chairs to invite 6 of them.

1. How many choices do you have for which 6 friends to invite?
2. What if you need to decide not only which friends to invite but also where to seat them along your long table? How many choices do you have then?

Solution

1. You must simply choose 6 friends from a group of 14. This can be done in $\binom{14}{6}$ ways. We can find this number either by using Pascal's triangle or the closed formula: $\frac{14!}{8!\cdot 6!} = 3003$.
2. Here you must count all the ways you can permute 6 friends chosen from a group of 14. So the answer is $P(14,6)$, which can be calculated as $\frac{14!}{8!} = 2192190$.

Notice that we can think of this counting problem as a question about counting functions: how many injective functions are there from your set of 6 chairs to your set of 14 friends (the functions are injective because you can't have a single chair go to two of your friends).

How are these numbers related? Notice that $P(14,6)$ is much larger than $\binom{14}{6}$. This makes sense. $\binom{14}{6}$ picks 6 friends, but $P(14,6)$ arranges the 6 friends as well as picks them. In fact, we can say exactly how much larger $P(14,6)$ is. In both counting problems we choose 6 out of 14 friends. For the first one, we stop there, at 3003 ways. But for the second counting problem, each of those 3003 choices of 6 friends can be arranged in exactly 6! ways. So now we have $3003 \cdot 6!$ choices and that is exactly 2192190.

Alternatively, look at the first problem another way. We want to select 6 out of 14 friends, but we do not care about the order they are selected in. To select 6 out of 14 friends, we might try this:

$$14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9.$$

This is a reasonable guess, since we have 14 choices for the first guest, then 13 for the second, and so on. But the guess is wrong (in fact, that product is exactly $2192190 = P(14,6)$). It distinguishes between the different orders in which we could

invite the guests. To correct for this, we could divide by the number of different arrangements of the 6 guests (so that all of these would count as just one outcome). There are precisely $6!$ ways to arrange 6 guests, so the correct answer to the first question is

$$\frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9}{6!}.$$

Note that another way to write this is

$$\frac{14!}{8! \cdot 6!}.$$

which is what we had originally.

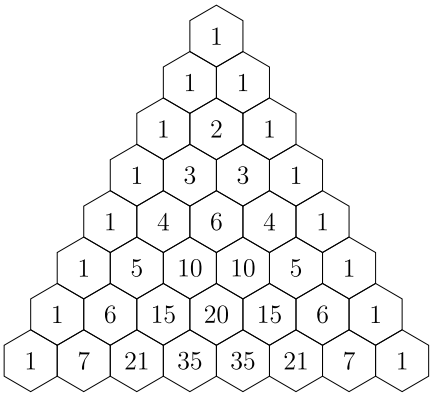
11.4: Combinatorial Proofs

Investigate!

1. The Stanley Cup is decided in a best of 7 tournament between two teams. In how many ways can your team win? Let's answer this question two ways:
   a. How many of the 7 games does your team need to win? How many ways can this happen?
   b. What if the tournament goes all 7 games? So you win the last game. How many ways can the first 6 games go down?
   c. What if the tournament goes just 6 games? How many ways can this happen? What about 5 games? 4 games?
   d. What are the two different ways to compute the number of ways your team can win? Write down an equation involving binomial coefficients (that is, $\binom{n}{k}$'s). What pattern in Pascal's triangle is this an example of?
2. Generalize. What if the rules changed and you played a best of 9 tournament (5 wins required)? What if you played an n game tournament with k wins required to be named champion?

Patterns in Pascal's Triangle

Have a look again at Pascal's triangle. Forget for a moment where it comes from. Just look at it as a mathematical object. What do you notice?



There are lots of patterns hidden away in the triangle, enough to fill a reasonably sized book. Here are just a few of the most obvious ones:

1. The entries on the border of the triangle are all 1.
2. Any entry not on the border is the sum of the two entries above it.
3. The triangle is symmetric. In any row, entries on the left side are mirrored on the right side.
4. The sum of all entries on a given row is a power of 2. (You should check this!)

We would like to state these observations in a more precise way, and then prove that they are correct. Now each entry in Pascal's triangle is in fact a binomial coefficient. The 1 on the very top of the triangle is $\binom{0}{0}$. The next row (which we will call row 1, even though it is not the top-most row) consists of $\binom{1}{0}$ and $\binom{1}{1}$. Row 4 (the row 1, 4, 6, 4, 1) consists of the binomial coefficients

$$\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4}.$$

Given this description of the elements in Pascal's triangle, we can rewrite the above observations as follows:

1. $\binom{n}{0} = 1$ and $\binom{n}{n} = 1$.
2. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
3. $\binom{n}{k} = \binom{n}{n-k}$.
4. $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$.

Each of these is an example of a *binomial identity*: an identity (i.e., equation) involving binomial coefficients.

Our goal is to establish these identities. We wish to prove that they hold for all values of n and k. These proofs can be done in many ways. One option would be to give algebraic proofs, using the formula for $\binom{n}{k}$:

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!}.$$

Here's how you might do that for the second identity above.

Example 11.4.1

Give an algebraic proof for the binomial identity

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Solution

Proof

By the definition of $\binom{n}{k}$, we have

$$\binom{n-1}{k-1} = \frac{(n-1)!}{(n-1-(k-1))!(k-1)!} = \frac{(n-1)!}{(n-k)!(k-1)!}$$

and

$$\binom{n-1}{k} = \frac{(n-1)!}{(n-1-k)!k!}.$$

Thus, starting with the right-hand side of the equation:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-1-k)!\,k!} \\
&= \frac{(n-1)!k}{(n-k)!\,k!} + \frac{(n-1)!(n-k)}{(n-k)!\,k!} \\
&= \frac{(n-1)!(k+n-k)}{(n-k)!\,k!} \\
&= \frac{n!}{(n-k)!\,k!} \\
&= \binom{n}{k}.
\end{aligned}$$

The second line (where the common denominator is found) works because $k(k-1)! = k!$ and $(n-k)(n-k-1)! = (n-k)!$.

□

This is certainly a valid proof, but also is entirely useless. Even if you understand the proof perfectly, it does not tell you *why* the identity is true. A better approach would be to explain what $\binom{n}{k}$ *means* and then say why that is also what $\binom{n-1}{k-1} + \binom{n-1}{k}$ means. Let's see how this works for the four identities we observed above.

Example 11.4.2

Explain why $\binom{n}{0} = 1$ and $\binom{n}{n} = 1$.

Solution

What do these binomial coefficients tell us? Well, $\binom{n}{0}$ gives the number of ways to select 0 objects from a collection of n objects. There is only one way to do this, namely to not select any of the objects. Thus $\binom{n}{0} = 1$. Similarly, $\binom{n}{n}$ gives the

number of ways to select n objects from a collection of n objects. There is only one way to do this: select all n objects. Thus $\binom{n}{n} = 1$.

Alternatively, we know that $\binom{n}{0}$ is the number of n-bit strings with weight 0. There is only one such string, the string of all 0's. So $\binom{n}{0} = 1$. Similarly $\binom{n}{n}$ is the number of n-bit strings with weight n. There is only one string with this property, the string of all 1's.

Another way: $\binom{n}{0}$ gives the number of subsets of a set of size n containing 0 elements. There is only one such subset, the empty set. $\binom{n}{n}$ gives the number of subsets containing n elements. The only such subset is the original set (of all elements).

Example 11.4.3

Explain why $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Solution

The easiest way to see this is to consider bit strings. $\binom{n}{k}$ is the number of bit strings of length n containing k 1's. Of all of these strings, some start with a 1 and the rest start with a 0. First consider all the bit strings which start with a 1. After the 1, there must be $n-1$ more bits (to get the total length up to n) and exactly $k-1$ of them must be 1's (as we already have one, and we need k total). How many strings are there like that? There are exactly $\binom{n-1}{k-1}$ such bit strings, so of all the length n bit strings containing k 1's, $\binom{n-1}{k-1}$ of them start with a 1. Similarly, there are $\binom{n-1}{k}$ which start with a 0 (we still need $n-1$ bits and now k of them must be 1's). Since there are $\binom{n-1}{k}$ bit strings containing $n-1$ bits with k 1's, that is the number of length n bit strings with k 1's which start with a 0. Therefore $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Another way: consider the question, how many ways can you select k pizza toppings from a menu containing n choices? One way to do this is just $\binom{n}{k}$. Another way to answer the same question is to first decide whether or not you want anchovies. If you do want anchovies, you still need to pick $k-1$ toppings, now from just $n-1$ choices. That can be done in $\binom{n-1}{k-1}$ ways. If you do not want anchovies, then you still need to select k toppings from $n-1$ choices (the anchovies are out). You can do that in $\binom{n-1}{k}$ ways. Since the choices with anchovies are disjoint from the choices without anchovies, the total choices are $\binom{n-1}{k-1} + \binom{n-1}{k}$. But wait. We answered the same question in two different ways, so the two answers must be the same. Thus $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

You can also explain (prove) this identity by counting subsets, or even lattice paths.

Example 11.4.4

Prove the binomial identity

$$\binom{n}{k} = \binom{n}{n-k}.$$

Solution

Why is this true? $\binom{n}{k}$ counts the number of ways to select k things from n choices. On the other hand, $\binom{n}{n-k}$ counts the number of ways to select $n-k$ things from n choices. Are these really the same? Well, what if instead of selecting the $n-k$ things you choose to exclude them. How many ways are there to choose $n-k$ things to exclude from n choices. Clearly this is $\binom{n}{n-k}$ as well (it doesn't matter whether you include or exclude the things once you have chosen them). And if you exclude $n-k$ things, then you are including the other k things. So the set of outcomes should be the same.

Let's try the pizza counting example like we did above. How many ways are there to pick k toppings from a list of n choices? On the one hand, the answer is simply $\binom{n}{k}$. Alternatively, you could make a list of all the toppings you don't want. To end up with a pizza containing exactly k toppings, you need to pick $n-k$ toppings to not put on the pizza. You have $\binom{n}{n-k}$ choices for the toppings you don't want. Both of these ways give you a pizza with k toppings, in fact all the ways to get a pizza with k toppings. Thus these two answers must be the same: $\binom{n}{k} = \binom{n}{n-k}$.

You can also prove (explain) this identity using bit strings, subsets, or lattice paths. The bit string argument is nice: $\binom{n}{k}$ counts the number of bit strings of length n with k 1's. This is also the number of bit string of length n with k 0's (just replace each 1 with a 0 and each 0 with a 1). But if a string of length n has k 0's, it must have $n-k$ 1's. And there are exactly $\binom{n}{n-k}$ strings of length n with $n-k$ 1's.

Example 11.4.5

Prove the binomial identity

$$\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}=2^n.$$

Solution

Proof

Let's do a "pizza proof" again. We need to find a question about pizza toppings which has 2^n as the answer. How about this: If a pizza joint offers n toppings, how many pizzas can you build using any number of toppings from no toppings to all toppings, using each topping at most once?

On one hand, the answer is 2^n. For each topping you can say "yes" or "no," so you have two choices for each topping.

On the other hand, divide the possible pizzas into disjoint groups: the pizzas with no toppings, the pizzas with one topping, the pizzas with two toppings, etc. If we want no toppings, there is only one pizza like that (the empty pizza, if you will) but it would be better to think of that number as $\binom{n}{0}$ since we choose 0 of the n toppings. How many pizzas have 1 topping? We need to choose 1 of the n toppings, so $\binom{n}{1}$. We have:

Pizzas with 0 toppings: $\binom{n}{0}$ Pizzas with 1 topping: $\binom{n}{1}$ Pizzas with 2 toppings: $\binom{n}{2}$

The total number of possible pizzas will be the sum of these, which is exactly the left-hand side of the identity we are trying to prove.

Again, we could have proved the identity using subsets, bit strings, or lattice paths (although the lattice path argument is a little tricky).

- $\vdots$
- Pizzas with n toppings: $\binom{n}{n}$.

□

Hopefully this gives some idea of how explanatory proofs of binomial identities can go. It is worth pointing out that more traditional proofs can also be beautiful. [3]Most every binomial identity can be proved using mathematical induction, using the recursive definition for $\binom{n}{k}$. We will discuss induction in Section 2.5. For example, consider the following rather slick proof of the last identity.

Expand the binomial $(x+y)^n$:

$$(x+y)^n=\binom{n}{0}x^n+\binom{n}{1}x^{n-1}y+\binom{n}{2}x^{n-2}y^2+\cdots+\binom{n}{n-1}x\cdot y^n+\binom{n}{n}y^n.$$

Let $x=1$ and $y=1$. We get:

$$(1+1)^n=\binom{n}{0}1^n+\binom{n}{1}1^{n-1}1+\binom{n}{2}1^{n-2}1^2+\cdots+\binom{n}{n-1}1\cdot 1^n+\binom{n}{n}1^n.$$

Of course this simplifies to:

$$(2)^n=\binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n-1}+\binom{n}{n}.$$

Something fun to try: Let $x=1$ and $y=2$. Neat huh?

More Proofs

The explanatory proofs given in the above examples are typically called *combinatorial proofs*. In general, to give a combinatorial proof for a binomial identity, say $A = B$ you do the following:

1. Find a counting problem you will be able to answer in two ways.
2. Explain why one answer to the counting problem is A.
3. Explain why the other answer to the counting problem is B.

Since both A and B are the answers to the same question, we must have $A = B$.

The tricky thing is coming up with the question. This is not always obvious, but it gets easier the more counting problems you solve. You will start to recognize types of answers as the answers to types of questions. More often what will happen is you will be solving a counting problem and happen to think up two different ways of finding the answer. Now you have a binomial identity and the proof is right there. The proof *is* the problem you just solved together with your two solutions.

For example, consider this counting question:

> *How many 10-letter words use exactly four A's, three B's, two C's and one D?*

Let's try to solve this problem. We have 10 spots for letters to go. Four of those need to be A's. We can pick the four A-spots in $\binom{10}{4}$ ways. Now where can we put the B's? Well there are only 6 spots left, we need to pick 3 of them. This can be done in $\binom{6}{3}$ ways. The two C's need to go in two of the 3 remaining spots, so we have $\binom{3}{2}$ ways of doing that. That leaves just one spot of the D, but we could write that 1 choice as $\binom{1}{1}$. Thus the answer is:

$$\binom{10}{4}\binom{6}{3}\binom{3}{2}\binom{1}{1}.$$

But why stop there? We can find the answer another way too. First let's decide where to put the one D: we have 10 spots, we need to choose 1 of them, so this can be done in $\binom{10}{1}$ ways. Next, choose one of the $\binom{9}{2}$ ways to place the two C's. We now have 7 spots left, and three of them need to be filled with B's. There are $\binom{7}{3}$ ways to do this. Finally the A's can be placed in $\binom{4}{4}$ (that is, only one) ways. So another answer to the question is

$$\binom{10}{1}\binom{9}{2}\binom{7}{3}\binom{4}{4}.$$

Interesting. This gives us the binomial identity:

$$\binom{10}{4}\binom{6}{3}\binom{3}{2}\binom{1}{1} = \binom{10}{1}\binom{9}{2}\binom{7}{3}\binom{4}{4}.$$

Here are a couple of other binomial identities with combinatorial proofs.

Example 11.4.6

Prove the identity

$$1n + 2(n-1) + 3(n-2) + \cdots + (n-1)2 + n1 = \binom{n+2}{3}.$$

Solution

To give a combinatorial proof we need to think up a question we can answer in two ways: one way needs to give the left-hand-side of the identity, the other way needs to be the right-hand-side of the identity. Our clue to what question to ask comes from the right-hand side: $\binom{n+2}{3}$ counts the number of ways to select 3 things from a group of $n+2$ things. Let's name those things $1, 2, 3, \ldots, n+2$. In other words, we want to find 3-element subsets of those numbers (since order should not matter, subsets are exactly the right thing to think about). We will have to be a bit clever to explain why the left-hand-side also gives the number of these subsets. Here's the proof.

Proof

Consider the question "How many 3-element subsets are there of the set $\{1,2,3,\ldots,n+2\}$?' We answer this in two ways:

Answer 1: We must select 3 elements from the collection of $n+2$ elements. This can be done in $\binom{n+2}{3}$ ways.

Answer 2: Break this problem up into cases by what the middle number in the subset is. Say each subset is $\{a,b,c\}$ written in increasing order. We count the number of subsets for each distinct value of b. The smallest possible value of b is 2, and the largest is $n+1$.

When $b=2$, there are $1\cdot n$ subsets: 1 choice for a and n choices (3 through $n+2$) for c.

When $b=3$, there are $2\cdot(n-1)$ subsets: 2 choices for a and $n-1$ choices for c.

When $b=4$, there are $3\cdot(n-2)$ subsets: 3 choices for a and $n-2$ choices for c.

And so on. When $b=n+1$, there are n choices for a and only 1 choice for c, so $n\cdot 1$ subsets.

Therefore the total number of subsets is

$$1n+2(n-1)+3(n-2)+\cdots+(n-1)2+n1.$$

Since Answer 1 and Answer 2 are answers to the same question, they must be equal. Therefore

$$1n+2(n-1)+3(n-2)+\cdots+(n-1)2+n1=\binom{n+2}{3}.$$

□

Example 11.4.7

Prove the binomial identity

$$\binom{n}{0}^2+\binom{n}{1}^2+\binom{n}{2}^2+\cdots+\binom{n}{n}^2=\binom{2n}{n}.$$

Solution 1

We will give two different proofs of this fact. The first will be very similar to the previous example (counting subsets). The second proof is a little slicker, using lattice paths.

Proof

Consider the question: "How many pizzas can you make using n toppings when there are $2n$ toppings to choose from?"

Answer 1: There are $2n$ toppings, from which you must choose n. This can be done in $\binom{2n}{n}$ ways.

Answer 2: Divide the toppings into two groups of n toppings (perhaps n meats and n veggies). Any choice of n toppings must include some number from the first group and some number from the second group. Consider each possible number of meat toppings separately:

0 meats: $\binom{n}{0}\binom{n}{n}$, since you need to choose 0 of the n meats and n of the n veggies.

1 meat: $\binom{n}{1}\binom{n}{n-1}$, since you need 1 of n meats so $n-1$ of n veggies.

2 meats: $\binom{n}{2}\binom{n}{n-2}$. Choose 2 meats and the remaining $n-2$ toppings from the n veggies.

And so on. The last case is n meats, which can be done in $\binom{n}{n}\binom{n}{0}$ ways.

Thus the total number of pizzas possible is

$$\binom{n}{0}\binom{n}{n}+\binom{n}{1}\binom{n}{n-1}+\binom{n}{2}\binom{n}{n-2}+\cdots+\binom{n}{n}\binom{n}{0}.$$

This is not quite the left-hand side … yet. Notice that $\binom{n}{n}=\binom{n}{0}$ and $\binom{n}{n-1}=\binom{n}{1}$ and so on, by the identity in Example 1.4.4. Thus we do indeed get

$$\binom{n}{0}^2+\binom{n}{1}^2+\binom{n}{2}^2+\cdots+\binom{n}{n}^2.$$

Since these two answers are answers to the same question, they must be equal, and thus

$$\binom{n}{0}^2+\binom{n}{1}^2+\binom{n}{2}^2+\cdots+\binom{n}{n}^2=\binom{2n}{n}.$$

□

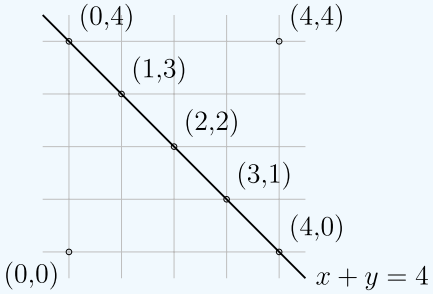
For an alternative proof, we use lattice paths. This is reasonable to consider because the right-hand side of the identity reminds us of the number of paths from $(0,0)$ to (n,n).

Proof

Consider the question: How many lattice paths are there from $(0,0)$ to (n,n)?

Answer 1: We must travel $2n$ steps, and n of them must be in the up direction. Thus there are $\binom{2n}{n}$ paths.

Answer 2: Note that any path from $(0,0)$ to (n,n) must cross the line $x+y=n$. That is, any path must pass through exactly one of the points: $(0,n)$, $(1,n-1)$, $(2,n-2)$, ..., $(n,0)$. For example, this is what happens in the case $n=4$:



How many paths pass through $(0,n)$? To get to that point, you must travel n units, and 0 of them are to the right, so there are $\binom{n}{0}$ ways to get to $(0,n)$. From $(0,n)$ to (n,n) takes n steps, and 0 of them are up. So there are $\binom{n}{0}$ ways to get from $(0,n)$ to (n,n). Therefore there are $\binom{n}{0}\binom{n}{0}$ paths from $(0,0)$ to (n,n) through the point $(0,n)$.

What about through $(1,n-1)$. There are $\binom{n}{1}$ paths to get there (n steps, 1 to the right) and $\binom{n}{1}$ paths to complete the journey to (n,n) (n steps, 1 up). So there are $\binom{n}{1}\binom{n}{1}$ paths from $(0,0)$ to (n,n) through $(1,n-1)$.

In general, to get to (n,n) through the point $(k,n-k)$ we have $\binom{n}{k}$ paths to the midpoint and then $\binom{n}{k}$ paths from the midpoint to (n,n). So there are $\binom{n}{k}\binom{n}{k}$ paths from $(0,0)$ to (n,n) through $(k,n-k)$.

All together then the total paths from $(0,0)$ to (n,n) passing through exactly one of these midpoints is

$$\binom{n}{0}^2+\binom{n}{1}^2+\binom{n}{2}^2+\cdots+\binom{n}{n}^2.$$

Since these two answers are answers to the same question, they must be equal, and thus

$$\binom{n}{0}^2+\binom{n}{1}^2+\binom{n}{2}^2+\cdots+\binom{n}{n}^2=\binom{2n}{n}.$$

□

11.5: Stars and Bars

Investigate!

Suppose you have some number of identical Rubik's cubes to distribute to your friends. Imagine you start with a single row of the cubes.

1. Find the number of different ways you can distribute the cubes provided:
   a. You have 3 cubes to give to 2 people.
   b. You have 4 cubes to give to 2 people.
   c. You have 5 cubes to give to 2 people.
   d. You have 3 cubes to give to 3 people.
   e. You have 4 cubes to give to 3 people.
   f. You have 5 cubes to give to 3 people.
2. Make a conjecture about how many different ways you could distribute 7 cubes to 4 people. Explain.
3. What if each person were required to get *at least one* cube? How would your answers change?

Consider the following counting problem:

You have 7 cookies to give to 4 kids. How many ways can you do this?

Take a moment to think about how you might solve this problem. You may assume that it is acceptable to give a kid no cookies. Also, the cookies are all identical and the order in which you give out the cookies does not matter.

Before solving the problem, here is a wrong answer: You might guess that the answer should be 4^7 because for each of the 7 cookies, there are 4 choices of kids to which you can give the cookie. This is reasonable, but wrong. To see why, consider a few possible outcomes: we could assign the first six cookies to kid A, and the seventh cookie to kid B. Another outcome would assign the first cookie to kid B and the six remaining cookies to kid A. Both outcomes are included in the 4^7 answer. But for our counting problem, both outcomes are really the same – kid A gets six cookies and kid B gets one cookie.

What do outcomes actually look like? How can we represent them? One approach would be to write an outcome as a string of four numbers like this:

$$3112,$$

which represent the outcome in which the first kid gets 3 cookies, the second and third kid each get 1 cookie, and the fourth kid gets 2 cookies. Represented this way, the order in which the numbers occur matters. 1312 is a different outcome, because the first kid gets a one cookie instead of 3. Each number in the string can be any integer between 0 and 7. But the answer is not 7^4. We need the *sum* of the numbers to be 7.

Another way we might represent outcomes is to write a string of seven letters:

$$\text{ABAADCD},$$

which represents that the first cookie goes to kid A, the second cookie goes to kid B, the third and fourth cookies go to kid A, and so on. In fact, this outcome is identical to the previous one—A gets 3 cookies, B and C get 1 each and D gets 2. Each of the seven letters in the string can be any of the 4 possible letters (one for each kid), but the number of such strings is not 4^7, because here order does *not* matter. In fact, another way to write the same outcome is

$$\text{AAABCDD}.$$

This will be the preferred representation of the outcome. Since we can write the letters in any order, we might as well write them in *alphabetical* order for the purposes of counting. So we will write all the A's first, then all the B's, and so on.

Now think about how you could specify such an outcome. All we really need to do is say when to switch from one letter to the next. In terms of cookies, we need to say after how many cookies do we stop giving cookies to the first kid and start giving cookies to the second kid. And then after how many do we switch to the third kid? And after how many do we switch to the fourth? So yet another way to represent an outcome is like this:

$$***|*|*|**$$

Three cookies go to the first kid, then we switch and give one cookie to the second kid, then switch, one to the third kid, switch, two to the fourth kid. Notice that we need 7 stars and 3 bars – one star for each cookie, and one bar for each switch between kids, so one fewer bars than there are kids (we don't need to switch after the last kid – we are done).

Why have we done all of this? Simple: to count the number of ways to distribute 7 cookies to 4 kids, all we need to do is count how many *stars and bars* charts there are. But a *stars and bars chart* is just a string of symbols, some stars and some bars. If instead of stars and bars we would use 0's and 1's, it would just be a bit string. We know how to count those.

Before we get too excited, we should make sure that really *any* string of (in our case) 7 stars and 3 bars corresponds to a different way to distribute cookies to kids. In particular consider a string like this:

$$|***||****$$

Does that correspond to a cookie distribution? Yes. It represents the distribution in which kid A gets 0 cookies (because we switch to kid B before any stars), kid B gets three cookies (three stars before the next bar), kid C gets 0 cookies (no stars before the next bar) and kid D gets the remaining 4 cookies. No matter how the stars and bars are arranged, we can distribute cookies in that way. Also, given any way to distribute cookies, we can represent that with a stars and bars chart. For example, the distribution in which kid A gets 6 cookies and kid B gets 1 cookie has the following chart:

$$******|*||$$

After all that work we are finally ready to count. Each way to distribute cookies corresponds to a stars and bars chart with 7 stars and 3 bars. So there are 10 symbols, and we must choose 3 of them to be bars. Thus:

$$\text{There are } \binom{10}{3} \text{ ways to distribute 7 cookies to 4 kids.}$$

While we are at it, we can also answer a related question: how many ways are there to distribute 7 cookies to 4 kids so that each kid gets at least one cookie? What can you say about the corresponding stars and bars charts? The charts must start and end with at least one star (so that kids A and D) get cookies, and also no two bars can be adjacent (so that kids B and C are not skipped). One way to assure this is to only place bars in the spaces *between* the stars. With 7 stars, there are 6 spots between the stars, so we must choose 3 of those 6 spots to fill with bars. Thus there are $\binom{6}{3}$ ways to distribute 7 cookies to 4 kids giving at least one cookie to each kid.

Another (and more general) way to approach this modified problem is to first give each kid one cookie. Now the remaining 3 cookies can be distributed to the 4 kids without restrictions. So we have 3 stars and 3 bars for a total of 6 symbols, 3 of which must be bars. So again we see that there are $\binom{6}{3}$ ways to distribute the cookies.

Stars and bars can be used in counting problems other than kids and cookies. Here are a few examples:

Example 11.5.1

Your favorite mathematical pizza chain offers 10 toppings. How many pizzas can you make if you are allowed 6 toppings? The order of toppings does not matter but now you are allowed repeats. So one possible pizza is triple sausage, double pineapple, and onions.

Solution

We get 6 toppings (counting possible repeats). Represent each of these toppings as a star. Think of going down the menu one topping at a time: you see anchovies first, and skip to the next, sausage. You say yes to sausage 3 times (use 3 stars), then switch to the next topping on the list. You keep skipping until you get to pineapple, which you say yes to twice. Another switch and you are at onions. You say yes once. Then you keep switching until you get to the last topping, never saying yes again (since you already have said yes 6 times. There are 10 toppings to choose from, so we must switch from considering one topping to the next 9 times. These are the bars.

Now that we are confident that we have the right number of stars and bars, we answer the question simply: there are 6 stars and 9 bars, so 15 symbols. We need to pick 9 of them to be bars, so there number of pizzas possible is

$$\binom{15}{9}.$$

Example 11.5.2

How many 7 digit phone numbers are there in which the digits are non-increasing? That is, every digit is less than or equal to the previous one.

Solution

We need to decide on 7 digits so we will use 7 stars. The bars will represent a switch from each possible single digit number down the next smaller one. So the phone number 866-5221 is represented by the stars and bars chart

$$|*||**|*|||**|*|$$

There are 10 choices for each digit (0-9) so we must switch between choices 9 times. We have 7 stars and 9 bars, so the total number of phone numbers is

$$\binom{16}{9}.$$

Example 11.5.3

How many integer solutions are there to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 13.$$

(An *integer solution* to an equation is a solution in which the unknown must have an integer value.)

1. where $x_i \geq 0$ for each x_i?
2. where $x_i > 0$ for each x_i?
3. where $x_i \geq 2$ for each x_i?

Solution

This problem is just like giving 13 cookies to 5 kids. We need to say how many of the 13 units go to each of the 5 variables. In other words, we have 13 stars and 4 bars (the bars are like the "+" signs in the equation).

1. If x_i can be 0 or greater, we are in the standard case with no restrictions. So 13 stars and 4 bars can be arranged in $\binom{17}{4}$ ways.
2. Now each variable must be at least 1. So give one unit to each variable to satisfy that restriction. Now there are 8 stars left, and still 4 bars, so the number of solutions is $\binom{12}{4}$.
3. Now each variable must be 2 or greater. So before any counting, give each variable 2 units. We now have 3 remaining stars and 4 bars, so there are $\binom{7}{4}$ solutions.

Counting with Functions

Many of the counting problems in this section might at first appear to be examples of counting *functions*. After all, when we try to count the number of ways to distribute cookies to kids, we are assigning each cookie to a kid, just like you assign elements of the domain of a function to elements in the codomain. However, the number of ways to assign 7 cookies to 4 kids is $\binom{10}{7} = 120$, while the number of functions $f : \{1, 2, 3, 4, 5, 6, 7\} \to \{a, b, c, d\}$is $4^7 = 16384$. What is going on here?

When we count functions, we consider the following two functions, for example, to be different:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ a & b & c & c & c & c & c \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ b & a & c & c & c & c & c \end{pmatrix}. \tag{11.5.1}$$

But these two functions would correspond to the *same* cookie distribution: kids a and b each get one cookie, kid c gets the rest (and none for kid d).

The point: elements of the domain are distinguished, cookies are indistinguishable. This is analogous to the distinction between permutations (like counting functions) and combinations (not).

Contributors and Attributions

- Oscar Levin (School of Mathematical Science, University of Northern Colorado)

11.6: Advanced Counting Using PIE

Investigate!

You have 11 identical mini key-lime pies to give to 4 children. However, you don't want any kid to get more than 3 pies. How many ways can you distribute the pies?

1. How many ways are there to distribute the pies without any restriction?
2. Let's get rid of the ways that one or more kid gets too many pies. How many ways are there to distribute the pies if Al gets too many pies? What if Bruce gets too many? Or Cat? Or Dent?
3. What if two kids get too many pies? How many ways can this happen? Does it matter which two kids you pick to overfeed?
4. Is it possible that three kids get too many pies? If so, how many ways can this happen?
5. How should you combine all the numbers you found above to answer the original question?

Suppose now you have 13 pies and 7 children. No child can have more than 2 pies. How many ways can you distribute the pies?

Stars and bars allows us to count the number of ways to distribute 10 cookies to 3 kids and natural number solutions to $x+y+z=11$, for example. A relatively easy modification allows us to put a *lower bound* restriction on these problems: perhaps each kid must get at least two cookies or $x, y, z \geq 2$. This was done by first assigning each kid (or variable) 2 cookies (or units) and then distributing the rest using stars and bars.

What if we wanted an *upper bound* restriction? For example, we might insist that no kid gets more than 4 cookies or that $x, y, z \leq 4$. It turns out this is considerably harder, but still possible. The idea is to count all the distributions and then remove those that violate the condition. In other words, we must count the number of ways to distribute 11 cookies to 3 kids in which *one or more* of the kids gets more than 4 cookies. For any particular kid, this is not a problem; we do this using stars and bars. But how to combine the number of ways for kid A, or B or C? We must use the PIE.

The **Principle of Inclusion/Exclusion (PIE)** gives a method for finding the cardinality of the union of not necessarily disjoint sets. We saw in Subsection how this works with three sets. To find how many things are in *one or more* of the sets A, B, and C, we should just add up the number of things in each of these sets. However, if there is any overlap among the sets, those elements are counted multiple times. So we subtract the things in each intersection of a pair of sets. But doing this removes elements which are in all three sets once too often, so we need to add it back in. In terms of cardinality of sets, we have

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Example 11.6.1:

Three kids, Alberto, Bernadette, and Carlos, decide to share 11 cookies. They wonder how many ways they could split the cookies up provided that none of them receive more than 4 cookies (someone receiving no cookies is for some reason acceptable to these kids).

Solution

Without the "no more than 4" restriction, the answer would be $\binom{13}{2}$, using 11 stars and 2 bars (separating the three kids). Now count the number of ways that one or more of the kids violates the condition, i.e., gets at least 4 cookies.

Let A be the set of outcomes in which Alberto gets more than 4 cookies. Let B be the set of outcomes in which Bernadette gets more than 4 cookies. Let C be the set of outcomes in which Carlos gets more than 4 cookies. We then are looking (for the sake of subtraction) for the size of the set $A \cup B \cup C$. Using PIE, we must find the sizes of $|A|, |B|, |C|, |A \cap B|$ and so on. Here is what we find.

$|A| = \binom{8}{2}$. First give Alberto 5 cookies, then distribute the remaining 6 to the three kids without restrictions, using 6 stars and 2 bars.
$|B| = \binom{8}{2}$. Just like above, only now Bernadette gets 5 cookies at the start.
$|C| = \binom{8}{2}$. Carlos gets 5 cookies first.
$|A \cap B| = \binom{3}{2}$. Give Alberto and Bernadette 5 cookies each, leaving 1 (star) to distribute to the three kids (2 bars).
$|A \cap C| = \binom{3}{2}$. Alberto and Carlos get 5 cookies first.

$|B \cap C| = \binom{3}{2}$. Bernadette and Carlos get 5 cookies first.
$|A \cap B \cap C| = 0$. It is not possible for all three kids to get 4 or more cookies.

Combining all of these we see

$$|A \cup B \cup C| = \binom{8}{2} + \binom{8}{2} + \binom{8}{2} - \binom{3}{2} - \binom{3}{2} - \binom{3}{2} + 0 = 75.$$

Thus the answer to the original question is $\binom{13}{2} - 75 = 78 - 75 = 3$. This makes sense now that we see it. The only way to ensure that no kid gets more than 4 cookies is to give two kids 4 cookies and one kid 3; there are three choices for which kid that should be. We could have found the answer much quicker through this observation, but the point of the example is to illustrate that PIE works!

For four or more sets, we do not write down a formula for PIE. Instead, we just think of the principle: add up all the elements in single sets, then subtract out things you counted twice (elements in the intersection of a *pair* of sets), then add back in elements you removed too often (elements in the intersection of groups of three sets), then take back out elements you added back in too often (elements in the intersection of groups of four sets), then add back in, take back out, add back in, etc. This would be very difficult if it wasn't for the fact that in these problems, all the cardinalities of the single sets are equal, as are all the cardinalities of the intersections of two sets, and that of three sets, and so on. Thus we can group all of these together and multiply by how many different combinations of 1, 2, 3, … sets there are.

Example 11.6.2

How many ways can you distribute 10 cookies to 4 kids so that no kid gets more than 2 cookies?

Solution

There are $\binom{13}{3}$ ways to distribute 10 cookies to 4 kids (using 10 stars and 3 bars). We will subtract all the outcomes in which a kid gets 3 or more cookies. How many outcomes are there like that? We can force kid A to eat 3 or more cookies by giving him 3 cookies before we start. Doing so reduces the problem to one in which we have 7 cookies to give to 4 kids without any restrictions. In that case, we have 7 stars (the 7 remaining cookies) and 3 bars (one less than the number of kids) so we can distribute the cookies in $\binom{10}{3}$ ways. Of course we could choose any one of the 4 kids to give too many cookies, so it would appear that there are $\binom{4}{1}\binom{10}{3}$ ways to distribute the cookies giving too many to one kid. But in fact, we have over counted.

We must get rid of the outcomes in which two kids have too many cookies. There are $\binom{4}{2}$ ways to select 2 kids to give extra cookies. It takes 6 cookies to do this, leaving only 4 cookies. So we have 4 stars and still 3 bars. The remaining 4 cookies can thus be distributed in $\binom{7}{3}$ ways (for each of the $\binom{4}{2}$ choices of which 2 kids to over-feed).

But now we have removed too much. We must add back in all the ways to give too many cookies to three kids. This uses 9 cookies, leaving only 1 to distribute to the 4 kids using stars and bars, which can be done in $\binom{4}{3}$ ways. We must consider this outcome for every possible choice of which three kids we over-feed, and there are $\binom{4}{3}$ ways of selecting that set of 3 kids.

Next we would subtract all the ways to give four kids too many cookies, but in this case, that number is 0.

All together we get that the number of ways to distribute 10 cookies to 4 kids without giving any kid more than 2 cookies is:

$$\binom{13}{3} - \left[\binom{4}{1}\binom{10}{3} - \binom{4}{2}\binom{7}{3} + \binom{4}{3}\binom{4}{3}\right]$$

which is

$$286 - [480 - 210 + 16] = 0.$$

This makes sense: there is NO way to distribute 10 cookies to 4 kids and make sure that nobody gets more than 2. It is

slightly surprising that

$$\binom{13}{3} = \left[\binom{4}{1}\binom{10}{3} - \binom{4}{2}\binom{7}{3} + \binom{4}{3}\binom{4}{3}\right]$$

but since PIE works, this equality must hold.

Just so you don't think that these problems always have easier solutions, consider the following example.

Example 11.6.3

Earlier (Example 1.5.3) we counted the number of solutions to the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 13$$

where $x_i \geq 0$ for each x_i.

How many of those solutions have $0 \leq x_i \leq 3$ for each x_i?

Solution

We must subtract off the number of solutions in which one or more of the variables has a value greater than 3. We will need to use PIE because counting the number of solutions for which each of the five variables separately are greater than 3 counts solutions multiple times. Here is what we get:

- Total solutions: $\binom{17}{4}$.
- Solutions where $x_1 > 3$: $\binom{13}{4}$. Give x_1 4 units first, then distribute the remaining 9 units to the 5 variables.
- Solutions where $x_1 > 3$ and $x_2 > 3$: $\binom{9}{4}$. After you give 4 units to x_1 and another 4 to x_2, you only have 5 units left to distribute.
- Solutions where $x_1 > 3$, $x_2 > 3$ and $x_3 > 3$: $\binom{5}{4}$.
- Solutions where $x_1 > 3$, $x_2 > 3$, $x_3 > 3$, and $x_4 > 3$: 0.

We also need to account for the fact that we could choose any of the five variables in the place of x_1 above (so there will be $\binom{5}{1}$ outcomes like this), any pair of variables in the place of x_1 and x_2 ($\binom{5}{2}$ outcomes) and so on. It is because of this that the double counting occurs, so we need to use PIE. All together we have that the number of solutions with $0 \leq x_i \leq 3$ is

$$\binom{17}{4} - \left[\binom{5}{1}\binom{13}{4} - \binom{5}{2}\binom{9}{4} + \binom{5}{3}\binom{5}{4}\right] = 15.$$

Counting Derangements

Investigate!

For your senior prank, you decide to switch the nameplates on your favorite 5 professors' doors. So that none of them feel left out, you want to make sure that all of the nameplates end up on the wrong door. How many ways can this be accomplished?

The advanced use of PIE has applications beyond stars and bars. A *derangement* of n elements $\{1, 2, 3, \ldots, n\}$ is a permutation in which no element is fixed. For example, there are 6 permutations of the three elements $\{1, 2, 3\}$:

$$123 \;\; 132 \;\; 213 \;\; 231 \;\; 312 \;\; 321.$$

but most of these have one or more elements fixed: 123 has all three elements fixed since all three elements are in their original positions, 132 has the first element fixed (1 is in its original first position), and so on. In fact, the only derangements of three elements are

$$231 \text{ and } 312.$$

If we go up to 4 elements, there are 24 permutations (because we have 4 choices for the first element, 3 choices for the second, 2 choices for the third leaving only 1 choice for the last). How many of these are derangements? If you list out all 24 permutations

and eliminate those which are not derangements, you will be left with just 9 derangements. Let's see how we can get that number using PIE.

Example 11.6.4

How many derangements are there of 4 elements?

Solution

We count all permutations, and subtract those which are not derangements. There are $4! = 24$ permutations of 4 elements. Now for a permutation to not be a derangement, at least one of the 4 elements must be fixed. There are $\binom{4}{1}$ choices for which single element we fix. Once fixed, we need to find a permutation of the other three elements. There are $3!$ permutations on 3 elements. But now we have counted too many non-derangements, so we must subtract those permutations which fix two elements. There are $\binom{4}{2}$ choices for which two elements we fix, and then for each pair, $2!$ permutations of the remaining elements. But this subtracts too many, so add back in permutations which fix 3 elements, all $\binom{4}{3}1!$ of them. Finally subtract the $\binom{4}{4}0!$ permutations (recall $0! = 1$) which fix all four elements. All together we get that the number of derangements of 4 elements is:

$$4! - \left[\binom{4}{1}3! - \binom{4}{2}2! + \binom{4}{3}1! - \binom{4}{4}0!\right] = 24 - 15 = 9.$$

Of course we can use a similar formula to count the derangements of any number of elements. However, the more elements we have, the longer the formula gets. Here is another example:

Example 11.6.5

Five gentlemen attend a party, leaving their hats at the door. At the end of the party, they hastily grab hats on their way out. How many different ways could this happen so that none of the gentlemen leave with their own hat?

Solution

We are counting derangements on 5 elements. There are $5!$ ways for the gentlemen to grab hats in any order—but many of these permutations will result in someone getting their own hat. So we subtract all the ways in which one or more of the men get their own hat. In other words, we subtract the non-derangements. Doing so requires PIE. Thus the answer is:

$$5! - \left[\binom{5}{1}4! - \binom{5}{2}3! + \binom{5}{3}2! - \binom{5}{4}1! + \binom{5}{5}0!\right].$$

Counting Functions

Investigate!

- Consider all functions $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$. How many functions are there all together? How many of those are injective? Remember, a function is an injection if every input goes to a different output.
- Consider all functions $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$. How many of the *injections* have the property that $f(x) \neq x$ for any $x \in \{1, 2, 3, 4, 5\}$? Your friend claims that the answer is:

  $$5! - \left[\binom{5}{1}4! - \binom{5}{2}3! + \binom{5}{3}2! - \binom{5}{4}1! + \binom{5}{5}0!\right].$$

  Explain why this is correct.
- Recall that a *surjection* is a function for which every element of the codomain is in the range. How many of the functions $f : \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ are surjective? Use PIE!

We have seen throughout this chapter that many counting questions can be rephrased as questions about counting functions with certain properties. This is reasonable since many counting questions can be thought of as counting the number of ways to assign elements from one set to elements of another.

Example 11.6.6

You decide to give away your video game collection so to better spend your time studying advance mathematics. How many ways can you do this, provided:

1. You want to distribute your 3 different PS4 games among 5 friends, so that no friend gets more than one game?
2. You want to distribute your 8 different 3DS games among 5 friends?
3. You want to distribute your 8 different SNES games among 5 friends, so that each friend gets at least one game?

In each case, model the counting question as a function counting question.

Solution

We must use the three games (call them 1, 2, 3) as the domain and the 5 friends (a,b,c,d,e) as the codomain (otherwise the function would not be defined for the whole domain when a friend didn't get any game). So how many functions are there with domain $\{1,2,3\}$and codomain $\{a,b,c,d,e\}$?The answer to this is $5^3=125$, since we can assign any of 5 elements to be the image of 1, any of 5 elements to be the image of 2 and any of 5 elements to be the image of 3.

But this is not the correct answer to our counting problem, because one of these functions is $f=\begin{pmatrix}1&2&3\\a&a&a\end{pmatrix}$; one friend can get more than one game. What we really need to do is count *injective* functions. This gives $P(5,3)=60$ functions, which is the answer to our counting question.

Again, we need to use the 8 games as the domain and the 5 friends as the codomain. We are counting all functions, so the number of ways to distribute the games is 5^8.

This question is harder. Use the games as the domain and friends as the codomain (otherwise an element of the domain would have more than one image, which is impossible). To ensure that every friend gets at least one game means that every element of the codomain is in the range. In other words, we are looking for *surjective* functions. How do you count those?

In Example 1.1.5 we saw how to count all functions (using the multiplicative principle) and in Example 1.3.4 we learned how to count injective functions (using permutations). Surjective functions are not as easily counted (unless the size of the domain is smaller than the codomain, in which case there are none).

The idea is to count the functions which are *not* surjective, and then subtract that from the total number of functions. This works very well when the codomain has two elements in it:

Example 11.6.7

How many functions $f:\{1,2,3,4,5\}\to\{a,b\}$are surjective?

Solution

There are 2^5 functions all together, two choices for where to send each of the 5 elements of the domain. Now of these, the functions which are *not* surjective must exclude one or more elements of the codomain from the range. So first, consider functions for which a is not in the range. This can only happen one way: everything gets sent to b. Alternatively, we could exclude b from the range. Then everything gets sent to a, so there is only one function like this. These are the only ways in which a function could not be surjective (no function excludes both a and b from the range) so there are exactly 2^5-2 surjective functions.

When there are three elements in the codomain, there are now three choices for a single element to exclude from the range. Additionally, we could pick pairs of two elements to exclude from the range, and we must make sure we don't over count these. It's PIE time!

Example 11.6.8

How many functions $f:\{1,2,3,4,5\}\to\{a,b,c\}$are surjective?

Solution

Again start with the total number of functions: 3^5 (as each of the five elements of the domain can go to any of three elements of the codomain). Now we count the functions which are *not* surjective.

Start by excluding a from the range. Then we have two choices (b or c) for where to send each of the five elements of the domain. Thus there are 2^5 functions which exclude a from the range. Similarly, there are 2^5 functions which exclude b, and another 2^5 which exclude c. Now have we counted all functions which are not surjective? Yes, but in fact, we have counted some multiple times. For example, the function which sends everything to c was one of the 2^5 functions we counted when we excluded a from the range, and also one of the 2^5 functions we counted when we excluded b from the range. We must subtract out all the functions which specifically exclude two elements from the range. There is 1 function when we exclude a and b (everything goes to c), one function when we exclude a and c, and one function when we exclude b and c.

We are using PIE: to count the functions which are not surjective, we added up the functions which exclude a, b, and c separately, then subtracted the functions which exclude pairs of elements. We would then add back in the functions which exclude groups of three elements, except that there are no such functions. We find that the number of functions which are *not* surjective is

$$2^5+2^5+2^5-1-1-1+0.$$

Perhaps a more descriptive way to write this is

$$\binom{3}{1}2^5-\binom{3}{2}1^5+\binom{3}{3}0^5.$$

since each of the 2^5's was the result of choosing 1 of the 3 elements of the codomain to exclude from the range, each of the three 1^5's was the result of choosing 2 of the 3 elements of the codomain to exclude. Writing 1^5 instead of 1 makes sense too: we have 1 choice of were to send each of the 5 elements of the domain.

Now we can finally count the number of surjective functions:

$$3^5-\left[\binom{3}{1}2^5-\binom{3}{2}1^5\right]=150.$$

You might worry that to count surjective functions when the codomain is larger than 3 elements would be too tedious. We need to use PIE but with more than 3 sets the formula for PIE is very long. However, we have lucked out. As we saw in the example above, the number of functions which exclude a single element from the range is the same no matter which single element is excluded. Similarly, the number of functions which exclude a pair of elements will be the same for every pair. With larger codomains, we will see the same behavior with groups of 3, 4, and more elements excluded. So instead of adding/subtracting each of these, we can simply add or subtract all of them at once, if you know how many there are. This works just like it did in for the other types of counting questions in this section, only now the size of the various combinations of sets is a number raised to a power, as opposed to a binomial coefficient or factorial. Here's what happens with 4 and 5 elements in the codomain.

Example 11.6.9

1. How many functions $f:\{1,2,3,4,5\}\to\{a,b,c,d\}$ are surjective?
2. How many functions $f:\{1,2,3,4,5\}\to\{a,b,c,d,e\}$ are surjective?

Solution

There are 4^5 functions all together; we will subtract the functions which are not surjective. We could exclude any one of the four elements of the codomain, and doing so will leave us with 3^5 functions for each excluded element. This counts too many so we subtract the functions which exclude two of the four elements of the codomain, each pair giving 2^5 functions. But this excludes too many, so we add back in the functions which exclude three of the four elements of the codomain, each triple giving 1^5 function. There are $\binom{4}{1}$ groups of functions excluding a single element, $\binom{4}{2}$ groups of functions excluding a pair of elements, and $\binom{4}{3}$ groups of functions excluding a triple of elements. This means that the number of functions which are *not* surjective is:

$$\binom{4}{1}3^5-\binom{4}{2}2^5+\binom{4}{3}1^5.$$

We can now say that the number of functions which are surjective is:

$$4^5 - \left[\binom{4}{1}3^5 - \binom{4}{2}2^5 + \binom{4}{3}1^5\right].$$

The number of surjective functions is:

$$5^5 - \left[\binom{5}{1}4^5 - \binom{5}{2}3^5 + \binom{5}{3}2^5 - \binom{5}{4}1^5\right].$$

We took the total number of functions 5^5 and subtracted all that were not surjective. There were $\binom{5}{1}$ ways to select a single element from the codomain to exclude from the range, and for each there were 4^5 functions. But this double counts, so we use PIE and subtract functions excluding two elements from the range: there are $\binom{5}{2}$ choices for the two elements to exclude, and for each pair, 3^5 functions. This takes out too many functions, so we add back in functions which exclude 3 elements from the range: $\binom{5}{3}$ choices for which three to exclude, and then 2^5 functions for each choice of elements. Finally we take back out the 1 function which excludes 4 elements for each of the $\binom{5}{4}$ choices of 4 elements.

If you happen to calculate this number precisely, you will get 120 surjections. That happens to also be the value of $5!$. This might seem like an amazing coincidence until you realize that every surjective function $f : X \to Y$ with $|X| = |Y|$ finite must necessarily be a bijection. The number of bijections is always $|X|!$ in this case. What we have here is a *combinatorial proof* of the following identity:

$$n^n - \left[\binom{n}{1}(n-1)^n - \binom{n}{2}(n-2)^n + \cdots + \binom{n}{n-1}1^n\right] = n!.$$

We have seen that counting surjective functions is another nice example of the advanced use of the Principle of Inclusion/Exclusion. Also, counting injective functions turns out to be equivalent to permutations, and counting all functions has a solution akin to those counting problems where order matters but repeats are allowed (like counting the number of words you can make from a given set of letters).

These are not just a few more examples of the techniques we have developed in this chapter. Quite the opposite: everything we have learned in this chapter are examples of *counting functions*!

Example 11.6.10

How many 5-letter words can you make using the eight letters a through h? How many contain no repeated letters?

Solution

By now it should be no surprise that there are 8^5 words, and $P(8,5)$ words without repeated letters. The new piece here is that we are actually counting functions. For the first problem, we are counting all functions from $\{1,2,\ldots,5\}$ to $\{a,b,\ldots,h\}$. The numbers in the domain represent the *position* of the letter in the word, the codomain represents the letter that could be assigned to that position. If we ask for no repeated letters, we are asking for injective functions.

If A and B are *any* sets with $|A| = 5$ and $|B| = 8$, then the number of functions $f : A \to B$ is 8^5 and the number of injections is $P(8,5)$. So if you can represent your counting problem as a function counting problem, most of the work is done.

Example 11.6.11

How many subsets are there of $\{1,2,\ldots,9\}$?How many 9-bit strings are there (of any weight)?

Solution

We saw in Section 1.2 that the answer to both these questions is 2^9, as we can say yes or no (or 0 or 1) to each of the 9 elements in the set (positions in the bit-string). But 2^9 also looks like the answer you get from counting functions. In fact, if you count all functions $f : A \to B$ with $|A| = 9$ and $|B| = 2$, this is exactly what you get.

> This makes sense! Let $A = \{1, 2, \ldots, 9\}$ and $B = \{y, n\}$. We are assigning each element of the set either a yes or a no. Or in the language of bit-strings, we would take the 9 positions in the bit string as our domain and the set $\{0, 1\}$ as the codomain.

So far we have not used a function as a model for binomial coefficients (combinations). Think for a moment about the relationship between combinations and permutations, say specifically $\binom{9}{3}$ and $P(9, 3)$. We *do* have a function model for $P(9, 3)$. This is the number of *injective* functions from a set of size 3 (say $\{1, 2, 3\}$ to a set of size 9 (say $\{1, 2, \ldots, 9\}$) since there are 9 choices for where to send the first element of the domain, then only 8 choices for the second, and 7 choices for the third. For example, the function might look like this:

$$f(1) = 5 \qquad f(2) = 8 \qquad f(3) = 4.$$

This is a different function from:

$$f(1) = 4 \qquad f(2) = 5 \qquad f(3) = 8.$$

Now $P(9, 3)$ counts these as different outcomes correctly, but $\binom{9}{3}$ will count these (among others) as just one outcome. In fact, in terms of functions $\binom{9}{3}$ just counts the number of different ranges possible of injective functions. This should not be a surprise since binomial coefficients counts subsets, and the range is a possible subset of the codomain.[4] A more mathematically sophisticated interpretation of combinations is that we are defining two injective functions to be *equivalent* if they have the same range, and then counting the number of equivalence classes under this notion of equivalence.

While it is possible to interpret combinations as functions, perhaps the better advice is to instead use combinations (or stars and bars) when functions are not quite the right way to interpret the counting question.

11.E: Counting (Exercises)

1.1: Additive and Multiplicative Principles

1

Your wardrobe consists of 5 shirts, 3 pairs of pants, and 17 bow ties. How many different outfits can you make?

Answer

There are 255 outfits. Use the multiplicative principle.

2

For your college interview, you must wear a tie. You own 3 regular (boring) ties and 5 (cool) bow ties.

a. How many choices do you have for your neck-wear?
b. You realize that the interview is for clown college, so you should probably wear both a regular tie and a bow tie. How many choices do you have now?
c. For the rest of your outfit, you have 5 shirts, 4 skirts, 3 pants, and 7 dresses. You want to select either a shirt to wear with a skirt or pants, or just a dress. How many outfits do you have to choose from?

Answer

a. 8 ties. Use the additive principle.
b. 15 ties. Use the multiplicative principle
c. $5 \cdot (4+3)+7=42$ outfits.

3

Your Blu-ray collection consists of 9 comedies and 7 horror movies. Give an example of a question for which the answer is:

a. 16.
b. 63.

Answer

a. For example, 16 is the number of choices you have if you want to watch one movie, either a comedy or horror flick.
b. For example, 63 is the number of choices you have if you will watch two movies, first a comedy and then a horror.

4

We usually write numbers in decimal form (or base 10), meaning numbers are composed using 10 different "digits" $\{0,1,\ldots,9\}$. Sometimes though it is useful to write numbers *hexadecimal* or base 16. Now there are 16 distinct digits that can be used to form numbers: $\{0,1,\ldots,9,\mathrm{A},\mathrm{B},\mathrm{C},\mathrm{D},\mathrm{E},\mathrm{F}\}$.So for example, a 3 digit hexadecimal number might be 2B8.

a. How many 2-digit hexadecimals are there in which the first digit is E or F? Explain your answer in terms of the additive principle (using either events or sets).
b. Explain why your answer to the previous part is correct in terms of the multiplicative principle (using either events or sets). Why do both the additive and multiplicative principles give you the same answer?
c. How many 3-digit hexadecimals start with a letter (A-F) and end with a numeral (0-9)? Explain.
d. How many 3-digit hexadecimals start with a letter (A-F) or end with a numeral (0-9) (or both)? Explain.

5

Suppose you have sets A and B with $|A|=10$ and $|B|=15$.

a. What is the largest possible value for $|A \cap B|$?
b. What is the smallest possible value for $|A \cap B|$?
c. What are the possible values for $|A \cup B|$?

Answer

a. To maximize the number of elements in common between A and B, make $A \subset B$. This would give $|A \cap B|=10$.

b. A and B might have no elements in common, giving $|A \cap B| = 0$.
c. $15 \leq |A \cup B| \leq 25$. In fact, when $|A \cap B| = 0$ then $|A \cup B| = 25$ and when $|A \cap B| = 10$ then $|A \cup B| = 15$.

6

If $|A| = 8$ and $|B| = 5$, what is $|A \cup B| + |A \cap B|$?

Answer

$|A \cup B| + |A \cap B| = 13$. Use PIE: we know $|A \cup B| = 8 + 5 - |A \cap B|$.

7

A group of college students were asked about their TV watching habits. Of those surveyed, 28 students watch *The Walking Dead*, 19 watch *The Blacklist*, and 24 watch *Game of Thrones*. Additionally, 16 watch *The Walking Dead* and *The Blacklist*, 14 watch *The Walking Dead* and *Game of Thrones*, and 10 watch *The Blacklist* and *Game of Thrones*. There are 8 students who watch all three shows. How many students surveyed watched at least one of the shows?

Answer

39 students. Use PIE or a Venn diagram.

8

In a recent survey, 30 students reported whether they liked their potatoes Mashed, French-fried, or Twice-baked. 15 liked them mashed, 20 liked French fries, and 9 liked twice baked potatoes. Additionally, 12 students liked both mashed and fried potatoes, 5 liked French fries and twice baked potatoes, 6 liked mashed and baked, and 3 liked all three styles. How many students *hate* potatoes? Explain why your answer is correct.

9

For how many $n \in \{1, 2, \ldots, 500\}$ is n a multiple of one or more of 5, 6, or 7?

Hint:

To find out how many numbers are divisible by 6 and 7, for example, take $500/42$ and round down.

10

Let A, B, and C be sets.

a. Find $|(A \cup C) \setminus B|$ provided $|A| = 50$, $|B| = 45$, $|C| = 40$, $|A \cap B| = 20$, $|A \cap C| = 15$, $|B \cap C| = 23$, and $|A \cap B \cap C| = 12$.
b. Describe a set in terms of A, B, and C with cardinality 26.

11

Consider all 5 letter "words" made from the letters a through h. (Recall, words are just strings of letters, not necessarily actual English words.)

a. How many of these words are there total?
b. How many of these words contain no repeated letters?
c. How many of these words start with the sub-word "aha"?
d. How many of these words either start with "aha" or end with "bah" or both?
e. How many of the words containing no repeats also do not contain the sub-word "bad"?

Answer

a. $8^5 = 32768$ words, since you select from 8 letters 5 times.
b. $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 6720$ words. After selecting a letter, you have fewer letters to select for the next one.
c. $8 \cdot 8 = 64$ words: you need to select the 4th and 5th letters.
d. $64 + 64 - 0 = 128$ words. There are 64 words which start with "aha" and another 64 words that end with "bah." Perhaps we over counted the words that both start with "aha" and end with "bah", but since the words are only 5 letters long, there are no such words.

e. $(8 \cdot 7 \cdot 6 \cdot 5 \cdot 4) - 3 \cdot (5 \cdot 4) = 6660$ words. All the words minus the bad ones. The taboo word can be in any of three positions (starting with letter 1, 2, or 3) and for each position we must choose the other two letters (from the remaining 5 letters).

12

For how many three digit numbers (100 to 999) is the *sum of the digits* even? (For example, 343 has an even sum of digits: $3+4+3=10$ which is even.) Find the answer and explain why it is correct in at least two *different* ways.

13

The number 735000 factors as $2^3 \cdot 3 \cdot 5^4 \cdot 7^2$. How many divisors does it have? Explain your answer using the multiplicative principle.

1.2: Binomial Coefficients

1

Let $S = \{1, 2, 3, 4, 5, 6\}$

a. How many subsets are there total?
b. How many subsets have $\{2, 3, 5\}$ as a subset?
c. How many subsets contain at least one odd number?
d. How many subsets contain exactly one even number?

Answer

a. $2^6 = 64$ subsets. We need to select yes/no for each of the six elements.
b. $2^3 = 8$ subsets. We need to select yes/no for each of the remaining three elements.
c. $2^6 - 2^3 = 56$ subsets. There are 8 subsets which do not contain any odd numbers (select yes/no for each even number).
d. $3 \cdot 2^3 = 24$ subsets. First pick the even number. Then say yes or no to each of the odd numbers.

2

Let $S = \{1, 2, 3, 4, 5, 6\}$

a. How many subsets are there of cardinality 4?
b. How many subsets of cardinality 4 have $\{2, 3, 5\}$ as a subset?
c. How many subsets of cardinality 4 contain at least one odd number?
d. How many subsets of cardinality 4 contain exactly one even number?

Answer

a. $\binom{6}{4} = 15$ subsets.
b. $\binom{3}{1} = 3$ subsets. We need to select 1 of the 3 remaining elements to be in the subset.
c. $\binom{6}{4} = 15$ subsets. All subsets of cardinality 4 must contain at least one odd number.
d. $\binom{3}{1} = 3$ subsets. Select 1 of the 3 even numbers. The remaining three odd numbers of S must all be in the set.

3

Let $A = \{1, 2, 3, \ldots, 9\}$.

a. How many subsets of A are there? That is, find $|\mathcal{P}(A)|$. Explain.
b. How many subsets of A contain exactly 5 elements? Explain.
c. How many subsets of A contain only even numbers? Explain.
d. How many subsets of A contain an even number of elements? Explain.

4

How many 9-bit strings (that is, bit strings of length 9) are there which:

a. Start with the sub-string 101? Explain.
b. Have weight 5 (i.e., contain exactly five 1's) and start with the sub-string 101? Explain.

c. Either start with 101 or end with 11 (or both)? Explain.
d. Have weight 5 and either start with 101 or end with 11 (or both)? Explain.

5

You break your piggy-bank to discover lots of pennies and nickels. You start arranging these in rows of 6 coins.

a. You find yourself making rows containing an equal number of pennies and nickels. For fun, you decide to lay out every possible such row. How many coins will you need?
b. How many coins would you need to make all possible rows of 6 coins (not necessarily with equal number of pennies and nickels)?

Answer

a. We can think of each row as a 6-bit string of weight 3 (since of the 6 coins, we require 3 to be pennies). Thus there are $\binom{6}{3} = 20$ rows possible. Each row requires 6 coins, so if we want to make all the rows at the same time, we will need 120 coins (60 of each).
b. Now there are $2^6 = 64$ rows possible, which is also $\binom{6}{0} + \binom{6}{1} + \binom{6}{2} + \binom{6}{3} + \binom{6}{4} + \binom{6}{5} + \binom{6}{6}$, if you break them up into rows containing 0, 1, 2, etc. pennies. Thus we need $6 \cdot 64 = 384$ coins (192 of each).

6

How many 10-bit strings contain 6 or more 1's?

Answer

$\binom{10}{6} + \binom{10}{7} + \binom{10}{8} + \binom{10}{9} + \binom{10}{10} = 386$ strings. Count the number of strings with each permissible number of 1's separately, then add them up.

7

How many subsets of $\{0, 1, \ldots, 9\}$ have cardinality 6 or more?

Hint:

Break the question into five cases.

8

What is the coefficient of x^{12} in $(x+2)^{15}$?

Answer

To get an x^{12}, we must pick 12 of the 15 factors to contribute an x, leaving the other 3 to contribute a 2. There are $\binom{15}{12}$ ways to select these 12 factors. So the term containing an x^{12} will be $\binom{15}{12} x^{12} 2^3$. In other words, the coefficient of x^{12} is $\binom{15}{12} 2^3 = 3640$.

9

What is the coefficient of x^9 in the expansion of $(x+1)^{14} + x^3(x+2)^{15}$?

10

How many shortest lattice paths start at (3,3) and

a. end at (10,10)?
b. end at (10,10) and pass through (5,7)?
c. end at (10,10) and avoid (5,7)?

Answer

a. $\binom{14}{7} = 3432$ paths. The paths all have length 14 (7 steps up and 7 steps right), we just select which 7 of those 14 should be up.
b. $\binom{6}{2}\binom{8}{5} = 840$ paths. First travel to (5,7), and then continue on to (10,10).

c. $\binom{14}{7} - \binom{6}{2}\binom{8}{5}$ paths. Remove all the paths that you found in part (b).

11

Gridtown USA, besides having excellent donut shoppes, is known for its precisely laid out grid of streets and avenues. Streets run east-west, and avenues north-south, for the entire stretch of the town, never curving and never interrupted by parks or schools or the like.

Suppose you live on the corner of 1st and 1st and work on the corner of 12th and 12th. Thus you must travel 22 blocks to get to work as quickly as possible.

a. How many different routes can you take to work, assuming you want to get there as quickly as possible?
b. Now suppose you want to stop and get a donut on the way to work, from your favorite donut shoppe on the corner of 8th st and 10th ave. How many routes to work, via the donut shoppe, can you take (again, ensuring the shortest possible route)?
c. Disaster Strikes Gridtown: there is a pothole on 4th avenue between 5th and 6th street. How many routes to work can you take avoiding that unsightly (and dangerous) stretch of road?
d. How many routes are there both avoiding the pothole and visiting the donut shoppe?

12

Suppose you are ordering a large pizza from *D.P. Dough*. You want 3 distinct toppings, chosen from their list of 11 vegetarian toppings.

a. How many choices do you have for your pizza?
b. How many choices do you have for your pizza if you refuse to have pineapple as one of your toppings?
c. How many choices do you have for your pizza if you *insist* on having pineapple as one of your toppings?
d. How do the three questions above relate to each other?

13

Explain why the coefficient of x^5y^3 the same as the coefficient of x^3y^5 in the expansion of $(x+y)^8$?

1.3: Combinations and Permutations

1

A pizza parlor offers 10 toppings.

a. How many 3-topping pizzas could they put on their menu? Assume double toppings are not allowed.
b. How many total pizzas are possible, with between zero and ten toppings (but not double toppings) allowed?
c. The pizza parlor will list the 10 toppings in two equal-sized columns on their menu. How many ways can they arrange the toppings in the left column?

Answer

a. $\binom{10}{3} = 120$ pizzas. We must choose (in no particular order) 3 out of the 10 toppings.
b. $2^{10} = 1024$ pizzas. Say yes or no to each topping.
c. $P(10,5) = 30240$ways. Assign each of the 5 spots in the left column to a unique pizza topping.

2

A combination lock consists of a dial with 40 numbers on it. To open the lock, you turn the dial to the right until you reach a first number, then to the left until you get to second number, then to the right again to the third number. The numbers must be distinct. How many different combinations are possible?

Answer

Despite its name, we are not looking for a combination here. The order in which the three numbers appears matters. There are $P(40,3) = 40 \cdot 39 \cdot 38$ different possibilities for the “combination”. This is assuming you cannot repeat any of the numbers (if you could, the answer would be 40^3).

3

Using the digits 2 through 8, find the number of different 5-digit numbers such that:

a. Digits can be used more than once.
b. Digits cannot be repeated, but can come in any order.
c. Digits cannot be repeated and must be written in increasing order.
d. Which of the above counting questions is a combination and which is a permutation? Explain why this makes sense.

4

How many triangles are there with vertices from the points shown below? Note, we are not allowing degenerate triangles - ones with all three vertices on the same line, but we do allow non-right triangles. Explain why your answer is correct.

Hint:

You need exactly two points on either the x- or y-axis, but don't over-count the right triangles.

5

How many quadrilaterals can you draw using the dots below as vertices (corners)?

Answer

$\binom{7}{2}\binom{7}{2} = 441$ quadrilaterals. We must pick two of the seven dots from the top row and two of the seven dots on the bottom row. However, it does not make a difference which of the two (on each row) we pick first because once these four dots are selected, there is exactly one quadrilateral that they determine.

6

How many of the quadrilaterals possible in the previous problem are:

a. Squares?
b. Rectangles?
c. Parallelograms?
d. Trapezoids?[2] Here, as in calculus, a trapezoid is defined as a quadrilateral with *at least* one pair of parallel sides. In particular, parallelograms are trapezoids.
e. Trapezoids that are not parallelograms?

Answer

a. 5 squares. You need to skip exactly one dot on the top and on the bottom to make the side lengths equal. Once you pick a dot on the top, the other three dots are determined.
b. $\binom{7}{2}$ rectangles. Once you select the two dots on the top, the bottom two are determined.
c. This is tricky since you need to worry about running out of space. One way to count: break into cases by the location of the top left corner. You get $\binom{7}{2} + \left(\binom{7}{2} - 1\right) + \left(\binom{7}{2} - 3\right) + \left(\binom{7}{2} - 6\right) + \left(\binom{7}{2} - 10\right) + \left(\binom{7}{2} - 15\right) = 91$ parallelograms.
d. All of them
e. $\binom{7}{2}\binom{7}{2} - \left[\binom{7}{2} + \left(\binom{7}{2} - 1\right) + \left(\binom{7}{2} - 3\right) + \left(\binom{7}{2} - 6\right) + \left(\binom{7}{2} - 10\right) + \left(\binom{7}{2} - 15\right)\right]$. All of them, except the parallelograms.

7

An *anagram* of a word is just a rearrangement of its letters. How many different anagrams of “uncopyrightable” are there? (This happens to be the longest common English word without any repeated letters.)

8

How many anagrams are there of the word “assesses” that start with the letter “a”?

Answer

After the first letter (a), we must rearrange the remaining 7 letters. There are only two letters (s and e), so this is really just a bit-string question (think of s as 1 and e as 0). Thus there $\binom{7}{2} = 21$ anagrams starting with “a”.

9

How many anagrams are there of “anagram”?

10

On a business retreat, your company of 20 businessmen and businesswomen go golfing.

a. You need to divide up into foursomes (groups of 4 people): a first foursome, a second foursome, and so on. How many ways can you do this?
b. After all your hard work, you realize that in fact, you want each foursome to include one of the five Board members. How many ways can you do this?

Answer

a. $\binom{20}{4}\binom{16}{4}\binom{12}{4}\binom{8}{4}\binom{4}{4}$ ways. Pick 4 out of 20 people to be in the first foursome, then 4 of the remaining 16 for the second foursome, and so on (use the multiplicative principle to combine).
b. $5!\binom{15}{3}\binom{12}{3}\binom{9}{3}\binom{6}{3}\binom{3}{3}$ ways. First determine the tee time of the 5 board members, then select 3 of the 15 non board members to golf with the first board member, then 3 of the remaining 12 to golf with the second, and so on.

11

How many different seating arrangements are possible for King Arthur and his 9 knights around their round table?

Answer

$9!$ (there are 10 people seated around the table, but it does not matter where King Arthur sits, only who sits to his left, two seats to his left, and so on).

12

Consider sets A and B with $|A| = 10$ and $|B| = 17$.

a. How many functions $f : A \to B$ are there?
b. How many functions $f : A \to B$ are injective?

Answer

a. 17^{10} functions. There are 17 choices for the image of each element in the domain.
b. $P(17, 10)$ injective functions. There are 17 choices for image of the first element of the domain, then only 16 choices for the second, and so on.

13

Consider functions $f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4, 5, 6\}$.

a. How many functions are there total?
b. How many functions are injective?
c. How many of the injective functions are *increasing*? To be increasing means that if $a < b$ then $f(a) < f(b)$, or in other words, the outputs get larger as the inputs get larger.

14

We have seen that the formula for $P(n, k)$ is $\dfrac{n!}{(n-k)!}$. Your task here is to explain *why* this is the right formula.

a. Suppose you have 12 chips, each a different color. How many different stacks of 5 chips can you make? Explain your answer and why it is the same as using the formula for $P(12, 5)$.
b. Using the scenario of the 12 chips again, what does $12!$ count? What does $7!$ count? Explain.
c. Explain why it makes sense to divide $12!$ by $7!$ when computing $P(12, 5)$ (in terms of the chips).
d. Does your explanation work for numbers other than 12 and 5? Explain the formula $P(n, k) = \frac{n!}{(n-k)!}$ using the variables n and k.

1.4: Combinatorial Proofs

1

Prove the identity $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ using a question about subsets.

Answer

Proof

Question: How many subsets of size k are there of the set $\{1, 2, \ldots, n\}$?

Answer 1: You must choose k out of n elements to put in the set, which can be done in $\binom{n}{k}$ ways.

Answer 2: First count the number of k-element subsets of $\{1, 2, \ldots, n\}$which contain the number n. We must choose $k-1$ of the $n-1$ other element to include in this set. Thus there are $\binom{n-1}{k-1}$ such subsets. We have not yet counted all the k-element subsets of $\{1, 2, \ldots, n\}$though. In fact, we have missed exactly those subsets which do NOT contain n. To form one of these subsets, we need to choose k of the other $n-1$ elements, so this can be done in $\binom{n-1}{k}$ ways. Thus the answer to the question is $\binom{n-1}{k-1} + \binom{n-1}{k}$.

Since the two answers are both answers tot eh same question, they are equal, establishing the identity $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

□

2

Give a combinatorial proof of the identity $2+2+2 = 3 \cdot 2$.

Answer

Proof

Question: How many 2-letter words start with *a*, *b*, or *c* and end with either *y* or *z*?

Answer 1: There are two words that start with *a*, two that start with *b*, two that start with *c*, for a total of $2+2+2$.

Answer 2: There are three choices for the first letter and two choices for the second letter, for a total of $3 \cdot 2$.

Since the two answers are both answers to the same question, they are equal. Thus $2+2+2 = 3 \cdot 2$.

□

3

Give a combinatorial proof for the identity $1+2+3+\cdots+n = \binom{n+1}{2}$.

Answer

Proof

Question: How many subsets of $A = 1, 2, 3, \ldots, n+1$ contain exactly two elements?

Answer 1: We must choose 2 elements from $n+1$ choices, so there are $\binom{n+1}{2}$ subsets.

Answer 2: We break this question down into cases, based on what the larger of the two elements in the subset is. The larger element can't be 1, since we need at least one element smaller than it.

Larger element is 2: there is 1 choice for the smaller element.

Larger element is 3: there are 2 choices for the smaller element.

Larger element is 4: there are 3 choices for the smaller element.

And so on. When the larger element is $n+1$, there are n choices for the smaller element. Since each two element subset must be in exactly one of these cases, the total number of two element subsets is $1+2+3+\cdots+n$.

Answer 1 and answer 2 are both correct answers to the same question, so they must be equal. Therefore,

$$1+2+3+\cdots+n=\binom{n+1}{2}$$

□

4

A woman is getting married. She has 15 best friends but can only select 6 of them to be her bridesmaids, one of which needs to be her maid of honor. How many ways can she do this?

a. What if she first selects the 6 bridesmaids, and then selects one of them to be the maid of honor?
b. What if she first selects her maid of honor, and then 5 other bridemaids?
c. Explain why $6\binom{15}{6}=15\binom{14}{5}$.

Answer

a. She has $\binom{15}{6}$ ways to select the 6 bridesmaids, and then for each way, has 6 choices for the maid of honor. Thus she has $\binom{15}{6}6$ choices.
b. She has 15 choices for who will be her maid of honor. Then she needs to select 5 of the remaining 14 friends to be bridesmaids, which she can do in $\binom{14}{5}$ ways. Thus she has $15\binom{14}{5}$ choices.
c. We have answered the question (how many wedding parties can the bride choose from) in two ways. The first way gives the left-hand side of the identity and the second way gives the right-hand side of the identity. Therefore the identity holds.

5

Give a combinatorial proof of the identity $\binom{n}{2}\binom{n-2}{k-2}=\binom{n}{k}\binom{k}{2}$.

Answer

Proof

Question: You have a large container filled with ping-pong balls, all with a different number on them. You must select k of the balls, putting two of them in a jar and the others in a box. How many ways can you do this?

Answer 1: First select 2 of the n balls to put in the jar. Then select $k-2$ of the remaining $n-2$ balls to put in the box. The first task can be completed in $\binom{n}{2}$ different ways, the second task in $\binom{n-2}{k-2}$ ways. Thus there are $\binom{n}{2}\binom{n-2}{k-2}$ ways to select the balls.

Answer 2: First select k balls from the n in the container. Then pick 2 of the k balls you picked to put in the jar, placing the remaining $k-2$ in the box. The first task can be completed in $\binom{n}{k}$ ways, the second task in $\binom{k}{2}$ ways. Thus there are $\binom{n}{k}\binom{k}{2}$ ways to select the balls.

Since both answers count the same thing, they must be equal and the identity is established.

□

6

Consider the bit strings in $\mathbf{B}_2^6$ (bit strings of length 6 and weight 2).

a. How many of those bit strings start with 1?
b. How many of those bit strings start with 01?
c. How many of those bit strings start with 001?
d. Are there any other strings we have not counted yet? Which ones, and how many are there?
e. How many bit strings are there total in $\mathbf{B}_2^6$?
f. What binomial identity have you just given a combinatorial proof for?

Answer

a. After the 1, we need to find a 5-bit string with one 1. There are $\binom{5}{1}$ ways to do this.
b. $\binom{4}{1}$ strings (we need to pick 1 of the remaining 4 slots to be the second 1).
c. $\binom{3}{1}$ strings.

d. Yes. We still need strings starting with 0001 (there are $\binom{2}{1}$ of these) and strings starting 00001 (there is only $\binom{1}{1}=1$ of these).
e. $\binom{6}{2}$ strings
f. An example of the Hockey Stick Theorem:

$$\binom{1}{1}+\binom{2}{1}+\binom{3}{1}+\binom{4}{1}+\binom{5}{1}=\binom{6}{2}$$

7

Let's count *ternary* digit strings, that is, strings in which each digit can be 0, 1, or 2.

a. How many ternary digit strings contain exactly n digits?
b. How many ternary digit strings contain exactly n digits and n 2's.
c. How many ternary digit strings contain exactly n digits and $n-1$ 2's. (Hint: where can you put the non-2 digit, and then what could it be?)
d. How many ternary digit strings contain exactly n digits and $n-2$ 2's. (Hint: see previous hint)
e. How many ternary digit strings contain exactly n digits and $n-k$ 2's.
f. How many ternary digit strings contain exactly n digits and no 2's. (Hint: what kind of a string is this?)
g. Use the above parts to give a combinatorial proof for the identity

$$\binom{n}{0}+2\binom{n}{1}+2^2\binom{n}{2}+2^3\binom{n}{3}+\cdots+2^n\binom{n}{n}=3^n.$$

Answer

a. 3^n strings, since there are 3 choices for each of the n digits.
b. 1 string, since all the digits need to be 2's. However, we might write this as $\binom{n}{0}$ strings.
c. There are $\binom{n}{1}$ places to put the non-2 digit. That digit can be either a 0 or a 1, so there are $2\binom{n}{1}$ such strings.
d. We must choose two slots to fill with 0's or 1's. There are $\binom{n}{2}$ ways to do that. Once the slots are picked, we have two choices for the first slot (0 or 1) and two choices for the second slot (0 or 1). So there are a total of $2^2\binom{n}{2}$ such strings.
e. There are $\binom{n}{k}$ ways to pick which slots don't have the 2's. Then those slots can be filled in 2^k ways (0 or 1 for each slot). So there are $2^k\binom{n}{k}$ such strings.
f. These strings contain just 0's and 1's, so they are bit strings. There are 2^n bit strings. But keeping with the pattern above, we might write this as $2^n\binom{n}{n}$ strings.
g. We answer the question of how many length n ternary digit strings there are in two ways. First, each digit can be one of three choices, so the total number of strings is 3^n. On the other hand, we could break the question down into cases by how many of the digits are 2's. If they are all 2's, then there are $\binom{n}{0}$ strings. If all but one is a 2, then there are $2\binom{n}{1}$ strings. If all but 2 of the digits are 2's, then there are $2^2\binom{n}{2}$ strings. We choose 2 of the n digits to be non-2, and then there are 2 choices for each of those digits. And so on for every possible number of 2's in the string. Therefore $\binom{n}{0}+2\binom{n}{1}+2^2\binom{n}{2}+2^3\binom{n}{3}+\cdots+2^n\binom{n}{n}=3^n$.

8

How many ways are there to rearrange the letters in the word “rearrange”? Answer this question in at least two different ways to establish a binomial identity.

Answer

The word contains 9 letters: 3 “r”s, 2 “a”s and 2 “e”s, along with an “n” and a “g”. We could first select the positions for the “r”s in $\binom{9}{3}$ ways, then the “a”s in $\binom{6}{2}$ ways, the “e”s in $\binom{4}{2}$ ways and then select one of the remaining two spots to put the “n” (placing the “g” in the last spot). This gives the answer

$$\binom{9}{3}\binom{6}{2}\binom{4}{2}\binom{2}{1}\binom{1}{1}.$$

Alternatively, we could select the positions of the letters in the opposite order, which would give an answer

$$\binom{9}{1}\binom{8}{1}\binom{7}{2}\binom{5}{2}\binom{3}{3}.$$

(where the 3 “r”s go in the remaining 3 spots). These two expressions are equal:

9

Give a combinatorial proof for the identity $P(n,k)=\binom{n}{k}k!$

Answer

Proof

Question: How many k-letter words can you make using n different letters without repeating any letter?

Answer 1: There are n choices for the first letter, $n-1$ choices for the second letter, $n-2$ choices for the third letter, and so on until $n-(k-1)$ choices for the kth letter (since $k-1$ letters have already been assigned at that point). The product of these numbers can be written $\frac{n!}{(n-k)!}$ which is $P(n,k)$. Therefore there are $P(n,k)$ words.

Answer 2: First pick k letters to be in the word from the n choices. This can be done in $\binom{n}{k}$ ways. Now arrange those letters into a word. There are k choices for the first letter, $k-1$ choices for the second, and so on, for a total of $k!$ arrangements of the k letters. Thus the total number of words is $\binom{n}{k}k!$.

Since the two answers are correct answers to the same question, we have established that $P(n,k)=\binom{n}{k}k!$.

□

10

Establish the identity below using a combinatorial proof.

$$\binom{2}{2}\binom{n}{2}+\binom{3}{2}\binom{n-1}{2}+\binom{4}{2}\binom{n-2}{2}+\cdots+\binom{n}{2}\binom{2}{2}=\binom{n+3}{5}.$$

Answer

Proof

Question: How many 5-element subsets are there of the set $\{1,2,\ldots,n+3\}$.

Answer 1: We choose 5 out of the $n+3$ elements, so $\binom{n+3}{5}$ subsets.

Answer 2: Break this up into cases by what the “middle” (third smallest) element of the 5 element subset is. The smallest this could be is a 3. In that case, we have $\binom{2}{2}$ choices for the numbers below it, and $\binom{n}{2}$ choices for the numbers above it. Alternatively, the middle number could be a 4. In this case there are $\binom{3}{2}$ choices for the bottom two numbers and $\binom{n-1}{2}$ choices for the top two numbers. If the middle number is 5, then there are $\binom{4}{2}$ choices for the bottom two numbers and $\binom{n-2}{2}$ choices for the top two numbers. An so on, all the way up to the largest the middle number could be, which is $n+1$. In that case there are $\binom{n}{2}$ choices for the bottom two numbers and $\binom{2}{2}$ choices for the top number. Thus the number of 5 element subsets is

$$\binom{2}{2}\binom{n}{2}+\binom{3}{2}\binom{n-1}{2}+\binom{4}{2}\binom{n-2}{2}+\cdots+\binom{n}{2}\binom{2}{2}.$$

Since the two answers correctly answer the same question, we have

$$\binom{2}{2}\binom{n}{2}+\binom{3}{2}\binom{n-1}{2}+\binom{4}{2}\binom{n-2}{2}+\cdots+\binom{n}{2}\binom{2}{2}=\binom{n+3}{5}.$$

1.5: Stars and Bars

1

A *multiset* is a collection of objects, just like a set, but can contain an object more than once (the order of the elements still doesn't matter). For example, $\{1,1,2,5,5,7\}$is a multiset of size 6.

a. How many *sets* of size 5 can be made using the 10 numeric digits 0 through 9?

b. How many *multi*sets of size 5 can be made using the 10 numeric digits 0 through 9?

Answer

a. $\binom{10}{5}$ sets. We must select 5 of the 10 digits to put in the set.
b. Use stars and bars: each star represents one of the 5 elements of the set, each bar represents a switch between digits. So there are 5 stars and 9 bars, giving us $\binom{14}{9}$ sets.

2

Each of the counting problems below can be solved with stars and bars. For each, say what outcome the diagram

$$***|*||**|$$

represents, if there are the correct number of stars and bars for the problem. Otherwise, say why the diagram does not represent any outcome, and what a correct diagram would look like.

a. How many ways are there to select a handful of 6 jellybeans from a jar that contains 5 different flavors?
b. How many ways can you distribute 5 identical lollipops to 6 kids?
c. How many 6-letter words can you make using the 5 vowels?
d. How many solutions are there to the equation $x_1+x_2+x_3+x_4=6$.

Answer

a. You take 3 strawberry, 1 lime, 0 licorice, 2 blueberry and 0 bubblegum.
b. This is backwards. We don't want the stars to represent the kids because the kids are not identical, but the stars are. Instead we should use 5 stars (for the lollipops) and use 5 bars to switch between the 6 kids. For example,

$$**||***|||$$

would represent the outcome with the first kid getting 2 lollipops, the third kid getting 3, and the rest of the kids getting none.
c. This is the word AAAEOO.
d. This doesn't represent a solution. Each star should represent one of the 6 units that add up to 6, and the bars should *switch* between the different variables. We have one too many bars. An example of a correct diagram would be

$$*|**||***,$$

representing that $x_1=1$, $x_2=2$, $x_3=0$, and $x_4=3$.

3

After gym class you are tasked with putting the 14 identical dodgeballs away into 5 bins.

a. How many ways can you do this if there are no restrictions?
b. How many ways can you do this if each bin must contain at least one dodgeball?

Answer

a. $\binom{18}{4}$ ways. Each outcome can be represented by a sequence of 14 stars and 4 bars.
b. $\binom{13}{4}$ ways. First put one ball in each bin. This leaves 9 stars and 4 bars.

4

How many integer solutions are there to the equation $x+y+z=8$ for which

a. x, y, and z are all positive?
b. x, y, and z are all non-negative?
c. x, y, and z are all greater than -3.

Answer

a. $\binom{7}{2}$ solutions. After each variable gets 1 star for free, we are left with 5 stars and 2 bars.
b. $\binom{10}{2}$ solutions. We have 8 stars and 2 bars.

c. $\binom{19}{2}$ solutions. This problem is equivalent to finding the number of solutions to $x'+y'+z'=17$ where x', y' and z' are non-negative. (In fact, we really just do a substitution. Let $x=x'-3$, $y=y'-3$ and $z=z'-3$).

5

Using the digits 2 through 8, find the number of different 5-digit numbers such that:

a. Digits cannot be repeated and must be written in increasing order. For example, 23678 is okay, but 32678 is not.
b. Digits *can* be repeated and must be written in *non-decreasing* order. For example, 24448 is okay, but 24484 is not.

Answer

a. There are $\binom{7}{5}$ numbers. We simply choose five of the seven digits and once chosen put them in increasing order.
b. This requires stars and bars. Use a star to represent each of the 5 digits in the number, and use their position relative to the bars to say what numeral fills that spot. So we will have 5 stars and 6 bars, giving $\binom{11}{6}$ numbers.

6

When playing Yahtzee, you roll five regular 6-sided dice. How many different outcomes are possible from a single roll? The order of the dice does not matter.

7

Your friend tells you she has 7 coins in her hand (just pennies, nickels, dimes and quarters). If you guess how many of each kind of coin she has, she will give them to you. If you guess randomly, what is the probability that you will be correct?

8

How many integer solutions to $x_1+x_2+x_3+x_4=25$ are there for which $x_1\geq 1$, $x_2\geq 2$, $x_3\geq 3$ and $x_4\geq 4$?

9

Solve the three counting problems below. Then say why it makes sense that they all have the same answer. That is, say how you can interpret them as each other.

a. How many ways are there to distribute 8 cookies to 3 kids?
b. How many solutions in non-negative integers are there to $x+y+z=8$?
c. How many different packs of 8 crayons can you make using crayons that come in red, blue and yellow?

10

Consider functions $f:\{1,2,3,4,5\}\to\{0,1,2,\ldots,9\}$.

a. How many of these functions are strictly increasing? Explain. (A function is strictly increasing provided if $a<b$, then $f(a)<f(b)$.)
b. How many of the functions are non-decreasing? Explain. (A function is non-decreasing provided if $a<b$, then $f(a)\leq f(b)$.)

11

Conic, your favorite math themed fast food drive-in offers 20 flavors which can be added to your soda. You have enough money to buy a large soda with 4 added flavors. How many different soda concoctions can you order if:

a. You refuse to use any of the flavors more than once?
b. You refuse repeats but care about the order the flavors are added?
c. You allow yourself multiple shots of the same flavor?
d. You allow yourself multiple shots, and care about the order the flavors are added?

Answer

a. $\binom{20}{4}$ sodas (order does not matter and repeats are not allowed).
b. $P(20,4)=20\cdot 19\cdot 18\cdot 17$ sodas (order matters and repeats are not allowed).
c. $\binom{23}{19}$ sodas (order does not matter and repeats are allowed; 4 stars and 19 bars).
d. 20^4 sodas (order matters and repeats are allowed; 20 choices 4 times).

1.6: Advanced Counting Using PIE

1

The dollar menu at your favorite tax-free fast food restaurant has 7 items. You have $10 to spend. How many different meals can you buy if you spend all your money and:

a. Purchase at least one of each item.
b. Possibly skip some items.
c. Don't get more than 2 of any particular item.

Answer a

$\binom{9}{6}$ meals.

Answer b

$\binom{16}{6}$ meals.

Answer c

$\binom{16}{6} - \left[\binom{7}{1}\binom{13}{6} - \binom{7}{2}\binom{10}{6} + \binom{7}{3}\binom{7}{6}\right]$ me als. Use PIE to subtract all the meals in which you get 3 or more of a particular item.

2

After a late night of math studying, you and your friends decide to go to your favorite tax-free fast food Mexican restaurant, *Burrito Chime*. You decide to order off of the dollar menu, which has 7 items. Your group has $16 to spend (and will spend all of it).

a. How many different orders are possible? Explain. (The *order* in which the order is placed does not matter - just which and how many of each item that is ordered.)
b. How many different orders are possible if you want to get at least one of each item? Explain.
c. How many different orders are possible if you don't get more than 4 of any one item? Explain.

3

After another gym class you are tasked with putting the 14 identical dodgeballs away into 5 bins. This time, no bin can hold more than 6 balls. How many ways can you clean up?

Solution

$\binom{18}{4} - \left[\binom{5}{1}\binom{11}{4} - \binom{5}{2}\binom{4}{4}\right]$. Subtract all the distributions for which one or more bins contain 7 or more balls.

4

Consider the equation $x_1 + x_2 + x_3 + x_4 = 15$. How many solutions are there with $2 \leq x_i \leq 5$ for all $i \in \{1, 2, 3, 4\}$?

Solution

The easiest way to solve this is to instead count the solutions to $y_1 + y_2 + y_3 + y_4 = 7$ with $0 \leq y_i \leq 3$. By taking $x_i = y_i + 2$, each solution to this new equation corresponds to exactly one solution to the original equation.

Now all the ways to distribute the 7 units to the four y_i variables can be found using stars and bars, specifically 7 stars and 3 bars, so $\binom{10}{3}$ ways. But this includes the ways that one or more y_i variables can be assigned more than 3 units. So subtract, using PIE. We get

$$\binom{10}{3} - \binom{4}{1}\binom{6}{3}.$$

The $\binom{4}{1}$ counts the number of ways to pick one variable to be over-assigned, the $\binom{6}{3}$ is the number of ways to assign the remaining 3 units to the 4 variables. Note that this is the final answer because it is not possible to have two variables both get 4 units.

5

Suppose you planned on giving 7 gold stars to some of the 13 star students in your class. Each student can receive at most one star. How many ways can you do this? Use PIE, and also an easier method, and compare your results.

6

Based on the previous question, give a combinatorial proof for the identity:

$$\binom{n}{k} = \binom{n+k-1}{k} - \sum_{j=1}^{n} (-1)^{j+1} \binom{n}{j} \binom{n+k-(2j+1)}{k}.$$

7

Illustrate how the counting of derangements works by writing all permutations of $\{1,2,3,4\}$and the crossing out those which are not derangements. Keep track of the permutations you cross out more than once, using PIE.

Solution

The 9 derangements are: 2143, 2341, 2413, 3142, 3412, 3421, 4123, 4312, 4321.

8

How many permutations of $\{1,2,3,4,5\}$leave exactly 1 element fixed?

Solution

First pick one of the five elements to be fixed. For each such choice, derange the remaining four, using the standard advanced PIE formula. We get $\binom{5}{1}\left(4! - \left[\binom{4}{1}3! - \binom{4}{2}2! + \binom{4}{3}1! - \binom{4}{4}0!\right]\right)$ permutations.

9

Ten ladies of a certain age drop off their red hats at the hat check of a museum. As they are leaving, the hat check attendant gives the hats back randomly. In how many ways can exactly six of the ladies receive their own hat (and the other four not)? Explain.

10

The Grinch sneaks into a room with 6 Christmas presents to 6 different people. He proceeds to switch the name-labels on the presents. How many ways could he do this if:

a. No present is allowed to end up with its original label? Explain what each term in your answer represents.
b. Exactly 2 presents keep their original labels? Explain.
c. Exactly 5 presents keep their original labels? Explain.

11

Consider functions $f : \{1,2,3,4\} \to \{a,b,c,d,e,f\}$.How many functions have the property that $f(1) \neq a$ or $f(2) \neq b$, or both?

Solution

There are $5 \cdot 6^3$ functions for which $f(1) \neq a$ and another $5 \cdot 6^3$ functions for which $f(2) \neq b$. There are $5^2 \cdot 6^2$ functions for which both $f(1) \neq a$ and $f(2) \neq b$. So the total number of functions for which $f(1) \neq a$ or $f(2) \neq b$ or both is

$$5 \cdot 6^3 + 5 \cdot 6^3 - 5^2 \cdot 6^2 = 1260.$$

12

Consider sets A and B with $|A| = 10$ and $|B| = 5$. How many functions $f : A \to B$ are surjective?

Solution

$5^{10} - \left[\binom{5}{1}4^{10} - \binom{5}{2}3^{10} + \binom{5}{3}2^{10} - \binom{5}{4}1^{10}\right]$ functions. The 5^{10} is all the functions from A to B. We subtract those that aren't surjective. Pick one of the five elements in B to not have in the range (in $\binom{5}{1}$ ways) and count all those functions (4^{10}). But this overcounts the functions where two elements from B are excluded from the range, so subtract those. And so on, using PIE.

13

Let $A = \{1, 2, 3, 4, 5\}$. How many injective functions $f : A \to A$ have the property that for each $x \in A$, $f(x) \neq x$?

14

Let d_n be the number of derangements of n objects. For example, using the techniques of this section, we find

$$d_3 = 3! - \left(\binom{3}{1} 2! - \binom{3}{2} 1! + \binom{3}{3} 0! \right)$$

We can use the formula for $\binom{n}{k}$ to write this all in terms of factorials. After simplifying, for d_3 we would get

$$d_3 = 3! \left(1 - \frac{1}{1} + \frac{1}{2} - \frac{1}{6} \right)$$

Generalize this to find a nicer formula for d_n. Bonus: For large n, approximately what fraction of all permutations are derangements? Use your knowledge of Taylor series from calculus.

11.S: Counting (Summary)

Investigate!

Suppose you have a huge box of animal crackers containing plenty of each of 10 different animals. For the counting questions below, carefully examine their similarities and differences, and then give an answer. The answers are all one of the following:

$P(10,6)$	$\binom{10}{6}$	10^6	$\binom{15}{9}$.

1. How many animal parades containing 6 crackers can you line up?
2. How many animal parades of 6 crackers can you line up so that the animals appear in alphabetical order?
3. How many ways could you line up 6 different animals in alphabetical order?
4. How many ways could you line up 6 different animals if they can come in any order?
5. How many ways could you give 6 children one animal cracker each?
6. How many ways could you give 6 children one animal cracker each so that no two kids get the same animal?
7. How many ways could you give out 6 giraffes to 10 kids?
8. Write a question about giving animal crackers to kids that has the answer $\binom{10}{6}$.

With all the different counting techniques we have mastered in this last chapter, it might be difficult to know when to apply which technique. Indeed, it is very easy to get mixed up and use the wrong counting method for a given problem. You get better with practice. As you practice you start to notice some trends that can help you distinguish between types of counting problems. Here are some suggestions that you might find helpful when deciding how to tackle a counting problem and checking whether your solution is correct.

- Remember that you are counting the number of items in some *list of outcomes*. Write down part of this list. Write down an element in the middle of the list – how are you deciding whether your element really is in the list. Could you get this element more than once using your proposed answer?
- If generating an element on the list involves selecting something (for example, picking a letter or picking a position to put a letter, etc), can the things you select be repeated? Remember, permutations and combinations select objects from a set *without* repeats.
- Does order matter? Be careful here and be sure you know what your answer really means. We usually say that order matters when you get different outcomes when the same objects are selected in different orders. Combinations and “Stars & Bars” are used when order *does not* matter.
- There are four possibilities when it comes to order and repeats. If order matters and repeats are allowed, the answer will look like n^k. If order matters and repeats are not allowed, we have $P(n,k)$. If order doesn't matter and repeats are allowed, use stars and bars. If order doesn't matter and repeats are not allowed, use $\binom{n}{k}$. But be careful: this only applies when you are selecting things, and you should make sure you know exactly what you are selecting before determining which case you are in.
- Think about how you would represent your counting problem in terms of sets or functions. We know how to count different sorts of sets and different types of functions.
- As we saw with combinatorial proofs, you can often solve a counting problem in more than one way. Do that, and compare your numerical answers. If they don't match, something is amiss.

While we have covered many counting techniques, we have really only scratched the surface of the large subject of *enumerative combinatorics*. There are mathematicians doing original research in this area even as you read this. Counting can be really hard.

In the next chapter, we will approach counting questions from a very different direction, and in doing so, answer infinitely many counting questions at the same time. We will create *sequences* of answers to related questions.

Chapter Review

1

You have 9 presents to give to your 4 kids. How many ways can this be done if:

a. The presents are identical, and each kid gets at least one present?
b. The presents are identical, and some kids might get no presents?
c. The presents are unique, and some kids might get no presents?

d. The presents are unique and each kid gets at least one present?

Answer

a. $\binom{8}{3}$ ways, after giving one present to each kid, you are left with 5 presents (stars) which need to be divide among the 4 kids (giving 3 bars).
b. $\binom{12}{3}$ ways. You have 9 stars and 3 bars.
c. 4^9. You have 4 choices for whom to give each present. This is like making a function from the set of presents to the set of kids.
d. $4^9 - \left[\binom{4}{1}3^9 - \binom{4}{2}2^9 + \binom{4}{3}1^9\right]$ ways. Now the function from the set of presents to the set of kids must be surjective.

2

For each of the following counting problems, say whether the answer is $\binom{10}{4}$, $P(10,4)$, or neither. If you answer is "neither," say what the answer should be instead.

a. How many shortest lattice paths are there from $(0,0)$ to $(10,4)$?
b. If you have 10 bow ties, and you want to select 4 of them for next week, how many choices do you have?
c. Suppose you have 10 bow ties and you will wear one on each of the next 4 days. How many choices do you have?
d. If you want to wear 4 of your 10 bow ties next week (Monday through Sunday), how many ways can this be accomplished?
e. Out of a group of 10 classmates, how many ways can you rank your top 4 friends?
f. If 10 students come to their professor's office but only 4 can fit at a time, how different combinations of 4 students can see the prof first?
g. How many 4 letter words can be made from the first 10 letters of the alphabet?
h. How many ways can you make the word "cake" from the first 10 letters of the alphabet?
i. How many ways are there to distribute 10 apples among 4 children?
j. If you have 10 kids (and live in a shoe) and 4 types of cereal, how many ways can your kids eat breakfast?
k. How many ways can you arrange exactly 4 ones in a string of 10 binary digits?
l. You want to select 4 single digit numbers as your lotto picks. How many choices do you have?
m. 10 kids want ice-cream. You have 4 varieties. How many ways are there to give the kids as much ice-cream as they want?
n. How many 1-1 functions are there from $\{1,2,\ldots,10\}$to $\{a,b,c,d\}$?
o. How many surjective functions are there from $\{1,2,\ldots,10\}$to $\{a,b,c,d\}$?
p. Each of your 10 bow ties match 4 pairs of suspenders. How many outfits can you make?
q. After the party, the 10 kids each choose one of 4 party-favors. How many outcomes?
r. How many 6-elements subsets are there of the set $\{1,2,\ldots,10\}$
s. How many ways can you split up 11 kids into 5 teams?
t. How many solutions are there to $x_1+x_2+\cdots+x_5=6$ where each x_i is non-negative?
u. Your band goes on tour. There are 10 cities within driving distance, but only enough time to play 4 of them. How many choices do you have for the cities on your tour?
v. In how many different ways can you play the 4 cities you choose?
w. Out of the 10 breakfast cereals available, you want to have 4 bowls. How many ways can you do this?
x. There are 10 types of cookies available. You want to make a 4 cookie stack. How many different stacks can you make?
y. From your home at (0,0) you want to go to either the donut shop at (5,4) or the one at (3,6). How many paths could you take?
z. How many 10-digit numbers do not contain a sub-string of 4 repeated digits?

Answer

a. Neither. $\binom{14}{4}$ paths.
b. $\binom{10}{4}$ bow ties. $P(10,4)$,since order is important.
c. Neither. Assuming you will wear each of the 4 ties on just 4 of the 7 days, without repeats: $\binom{10}{4}P(7,4)$.
d. $P(10,4)$. $\binom{10}{4}$.
e. Neither. Since you could repeat letters: 10^4. If no repeats are allowed, it would be $P(10,4)$.
f. Neither. Actually, "k" is the 11th letter of the alphabet, so the answer is 0. If "k" was among the first 10 letters, there would only be 1 way - write it down.
g. Neither. Either $\binom{9}{3}$ (if every kid gets an apple) or $\binom{13}{3}$ (if appleless kids are allowed).

h. Neither. Note that this could not be $\binom{10}{4}$ since the 10 things and 4 things are from different groups. 4^{10}.
i. $\binom{10}{4}$ - don't be fooled by the “arrange” in there - you are picking 4 out of 10 *spots* to put the 1's. $\binom{10}{4}$ (assuming order is irrelevant).
j. Neither. 16^{10} (each kid chooses yes or no to 4 varieties).
k. Neither. 0.
l. Neither. $4^{10} - [\binom{4}{1}3^{10} - \binom{4}{2}2^{10} + \binom{4}{3}1^{10}]$.
m. Neither. $10 \cdot 4$.
n. Neither. 4^{10}.
o. $\binom{10}{4}$ (which is the same as $\binom{10}{6}$).
p. Neither. If all the kids were identical, and you wanted no empty teams, it would be $\binom{10}{4}$. Instead, this will be the same as the number of surjective functions from a set of size 11 to a set of size 5.
q. $\binom{10}{4} \cdot \binom{10}{4}$.
r. Neither. $4!$.
s. Neither. It's $\binom{10}{4}$ if you won't repeat any choices. If repetition is allowed, then this becomes $x_1 + x_2 + \cdots + x_{10} = 4$, which has $\binom{13}{9}$ solutions in non-negative integers.
t. Neither. Since repetition of cookie type is allowed, the answer is 10^4. Without repetition, you would have $P(10, 4)$.
u. $\binom{10}{4}$ since that is equal to $\binom{9}{4} + \binom{9}{3}$.
v. Neither. It will be a complicated (possibly PIE) counting problem.

3

Recall, you own 3 regular ties and 5 bow ties. You realize that it would be okay to wear more than two ties to your clown college interview.

a. You must select some of your ties to wear. Everything is okay, from no ties up to all ties. How many choices do you have?
b. If you want to wear at least one regular tie and one bow tie, but are willing to wear up to all your ties, how many choices do you have for which ties to wear?
c. How many choices do you have if you wear exactly 2 of the 3 regular ties and 3 of the 5 bow ties?
d. Once you have selected 2 regular and 3 bow ties, in how many orders could you put the ties on, assuming you must have one of the three bow ties on top?

Answer

a. $2^8 = 256$ choices. You have two choices for each tie: wear it or don't.
b. You have 7 choices for regular ties (the 8 choices less the “no regular tie” option) and 31 choices for bow ties (32 total minus the “no bow tie” option). Thus total you have $7 \cdot 31 = 217$ choices.
c. $\binom{3}{2}\binom{5}{3} = 30$ choices.
d. Select one of the 3 bow ties to go on top. There are then 4 choices for the next tie, 3 for the tie after that, and so on. Thus $3 \cdot 4! = 72$ choices.

4

Give a counting question where the answer is $8 \cdot 3 \cdot 3 \cdot 5$. Give another question where the answer is $8 + 3 + 3 + 5$.

Answer

You own 8 purple bow ties, 3 red bow ties, 3 blue bow ties and 5 green bow ties. How many ways can you select one of each color bow tie to take with you on a trip? $8 \cdot 3 \cdot 3 \cdot 5$ ways. How many choices do you have for a single bow tie to wear tomorrow? $8 + 3 + 3 + 5$ choices.

5

Consider five digit numbers $\alpha = a_1 a_2 a_3 a_4 a_5$, with each digit from the set $\{1, 2, 3, 4\}$.

a. How many such numbers are there?
b. How many such numbers are there for which the *sum* of the digits is even?
c. How many such numbers contain more even digits than odd digits?

Answer

a. 4^5 numbers.
b. $4^4 \cdot 2$ numbers (choose any digits for the first four digits - then pick either an even or an odd last digit to make the sum even).
c. We need 3 or more even digits. 3 even digits: $\binom{5}{3}2^3 2^2$. 4 even digits: $\binom{5}{4}2^4 2$. 5 even digits: $\binom{5}{5}2^5$. So all together: $\binom{5}{3}2^3 2^2 + \binom{5}{4}2^4 2 + \binom{5}{5}2^5$ numbers.

6

In a recent small survey of airline passengers, 25 said they had flown American in the last year, 30 had flown Jet Blue, and 20 had flown Continental. Of those, 10 reported they had flown on American and Jet Blue, 12 had flown on Jet Blue and Continental, and 7 had flown on American and Continental. 5 passengers had flown on all three airlines.

How many passengers were surveyed? (Assume the results above make up the entire survey.)

Answer

51 passengers.

7

Recall, by 8-bit strings, we mean strings of binary digits, of length 8.

a. How many 8-bit strings are there total?
b. How many 8-bit strings have weight 5?
c. How many subsets of the set $\{a, b, c, d, e, f, g, h\}$ contain exactly 5 elements?
d. Explain why your answers to parts (b) and (c) are the same. Why are these questions equivalent?

Answer

a. 2^8 strings.
b. $\binom{8}{5}$ strings.
c. $\binom{8}{5}$ strings.
d. There is a bijection between subsets and bit strings: a 1 means that element in is the subset, a 0 means that element is not in the subset. To get a subset of an 8 element set we have a 8-bit string. To make sure the subset contains exactly 5 elements, there must be 5 1's, so the weight must be 5.

8

What is the coefficient of x^{10} in the expansion of $(x+1)^{13} + x^2(x+1)^{17}$?

Answer

$\binom{13}{10} + \binom{17}{8}$.

9

How many 8-letter words contain exactly 5 vowels (a,e,i,o,u)? What if repeated letters were not allowed?

Answer

With repeated letters allowed: $\binom{8}{5}5^5 21^3$ words. Without repeats: $\binom{8}{5}5!P(21,3)$words.

10

For each of the following, find the number of shortest lattice paths from $(0,0)$ to $(8,8)$ which:

a. pass through the point $(2,3)$.
b. avoid (do not pass through) the point $(7,5)$.
c. either pass through $(2,3)$ or $(5,7)$ (or both).

Answer

a. $\binom{5}{2}\binom{11}{6}$ paths.
b. $\binom{16}{8} - \binom{12}{7}\binom{4}{1}$ paths.
c. $\binom{5}{2}\binom{11}{6} + \binom{12}{5}\binom{4}{3} - \binom{5}{2}\binom{7}{3}\binom{4}{3}$ paths.

11

You live in Grid-Town on the corner of 2nd and 3rd, and work in a building on the corner of 10th and 13th. How many routes are there which take you from home to work and then back home, but by a different route?

Answer

$\binom{18}{8}\left(\binom{18}{8} - 1\right)$ routes.

12

How many 10-bit strings start with 111 or end with 101 or both?

Answer

$2^7 + 2^7 - 2^4$ strings (using PIE).

13

How many 10-bit strings of weight 6 start with 111 or end with 101 or both?

Answer

$\binom{7}{3} + \binom{7}{4} - \binom{4}{1}$ strings.

14

How many 6 letter words made from the letters a, b, c, d, e, f without repeats do not contain the sub-word "bad" in (a) consecutive letters? or (b) not-necessarily consecutive letters (but in order)?

Answer

(a) $6! - 4 \cdot 3!$ words. (b) $6! - \binom{6}{3}3!$ words.

15

Explain using lattice paths why $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Answer

2^n is the number of lattice paths which have length n, since for each step you can go up or right. Such a path would end along the line $x + y = n$. So you will end at $(0, n)$, or $(1, n-1)$ or $(2, n-2)$ or … or $(n, 0)$. Counting the paths to each of these points separately, give $\binom{n}{0}$, $\binom{n}{1}$, $\binom{n}{2}$, …, $\binom{n}{n}$ (each time choosing which of the n steps to be to the right). These two methods count the same quantity, so are equal.

16

Suppose you have 20 one-dollar bills to give out as prizes to your top 5 discrete math students. How many ways can you do this if:

a. Each of the 5 students gets at least 1 dollar?
b. Some students might get nothing?
c. Each student gets at least 1 dollar but no more than 7 dollars?

Hint

Stars and bars.

Answer

a. $\binom{19}{4}$ ways.
b. $\binom{24}{4}$ ways.

c. $\binom{19}{4} - \left[\binom{5}{1}\binom{12}{4} - \binom{5}{2}\binom{5}{4}\right]$ ways.

17

How many functions $f : \{1, 2, 3, 4, 5\} \to \{a, b, c, d, e\}$ are there satisfying:

a. $f(1) = a$ or $f(2) = b$ (or both)?
b. $f(1) \neq a$ or $f(2) \neq b$ (or both)?
c. $f(1) \neq a$ *and* $f(2) \neq b$, and f is injective?
d. f is surjective, but $f(1) \neq a$, $f(2) \neq b$, $f(3) \neq c$, $f(4) \neq d$ and $f(5) \neq e$?

Answer

a. $5^4 + 5^4 - 5^3$ functions.
b. $4 \cdot 5^4 + 5 \cdot 4 \cdot 5^3 - 4 \cdot 4 \cdot 5^3$ functions.
c. $5! - [4! + 4! - 3!]$ functions. Note we use factorials instead of powers because we are looking for injective functions.
d. Note that being surjective here is the same as being injective, so we can start with all $5!$ injective functions and subtract those which have one or more "fixed point". We get $5! - \left[\binom{5}{1}4! - \binom{5}{2}3! + \binom{5}{3}2! - \binom{5}{4}1! + \binom{5}{5}0!\right]$ functions.

18

How many functions map $\{1, 2, 3, 4, 5, 6\}$ *onto* $\{a, b, c, d\}$ (i.e., how many *surjections* are there)?

Answer

$4^6 - \left[\binom{4}{1}3^6 - \binom{4}{2}2^6 + \binom{4}{3}1^6\right]$.

19

To thank your math professor for doing such an amazing job all semester, you decide to bake Oscar cookies. You know how to make 10 different types of cookies.

a. If you want to give your professor 4 different types of cookies, how many different combinations of cookie type can you select? Explain your answer.
b. To keep things interesting, you decide to make a different number of each type of cookie. If again you want to select 4 cookie types, how many ways can you select the cookie types and decide for which there will be the most, second most, etc. Explain your answer.
c. You change your mind again. This time you decide you will make a total of 12 cookies. Each cookie could be any one of the 10 types of cookies you know how to bake (and it's okay if you leave some types out). How many choices do you have? Explain.
d. You realize that the previous plan did not account for presentation. This time, you once again want to make 12 cookies, each one could be any one of the 10 types of cookies. However, now you plan to shape the cookies into the numerals 1, 2, …, 12 (and probably arrange them to make a giant clock, but you haven't decided on that yet). How many choices do you have for which types of cookies to bake into which numerals? Explain.
e. The only flaw with the last plan is that your professor might not get to sample all 10 different varieties of cookies. How many choices do you have for which types of cookies to make into which numerals, given that each type of cookie should be present at least once? Explain.

Answer

a. $\binom{10}{4}$ combinations. You need to choose 4 of the 10 cookie types. Order doesn't matter.
b. $P(10, 4) = 10 \cdot 9 \cdot 8 \cdot 7$ ways. You are choosing and arranging 4 out of 10 cookies. Order matters now.
c. $\binom{21}{9}$ choices. You must switch between cookie type 9 times as you make your 12 cookies. The cookies are the stars, the switches between cookie types are the bars.
d. 10^{12} choices. You have 10 choices for the "1" cookie, 10 choices for the "2" cookie, and so on.
e. $10^{12} - \left[\binom{10}{1}9^{12} - \binom{10}{2}8^{12} + \cdots - \binom{10}{10}0^{12}\right]$ choices. We must use PIE to remove all the ways in which one or more cookie type is not selected.

20

For which of the parts of the previous problem (Exercise 1.7.19) does it make sense to interpret the counting question as counting some number of functions? Say what the domain and codomain should be, and whether you are counting all functions, injections, surjections, or something else.

Answer

a. You are giving your professor 4 types of cookies coming from 10 different types of cookies. This does not lend itself well to a function interpretation. We *could* say that the domain contains the 4 types you will give your professor and the codomain contains the 10 you can choose from, but then counting injections would be too much (it doesn't matter if you pick type 3 first and type 2 second, or the other way around, just that you pick those two types).
b. We want to consider injective functions from the set $\{$most, second most, second least, least$\}$ to the set of 10 cookie types. We want injections because we cannot pick the same type of cookie to give most and least of (for example).
c. This is not a good problem to interpret as a function. The problem is that the domain would have to be the 12 cookies you bake, but these elements are indistinguishable (there is not a first cookie, second cookie, etc.).
d. The domain should be the 12 shapes, the codomain the 10 types of cookies. Since we can use the same type for different shapes, we are interested in counting all functions here.
e. Here we insist that each type of cookie be given at least once, so now we are asking for the number of surjections of those functions counted in the previous part.

CHAPTER OVERVIEW

12: Boolean Algebra

Figure 12.1: George Boole, 1815 - 1864

George Boole

George Boole *wasn't idle a lot.*
He churned out ideas on the spot,
Making marvellous use of
Inclusive/exclusive
Expressions like AND, OR, and NOT

Andrew Robinson, The Omnificent English Dictionary in Limerick Form

In this chapter we will develop a type of algebraic system, Boolean algebras, that is particularly important to computer scientists, as it is the mathematical foundation of computer design, or switching theory. The similarities of Boolean algebras and the algebra of sets and logic will be discussed, and we will discover properties of finite Boolean algebras.

In order to achieve these goals, we will recall the basic ideas of posets introduced in Chapter 6 and develop the concept of a lattice. The reader should view the development of the topics of this chapter as another example of an algebraic system. Hence, we expect to define first the elements in the system, next the operations on the elements, and then the common properties of the operations in the system.

12.1: Posets Revisited

We recall the definition a partially ordering:

Definition 12.1.1: Partial Ordering

Let $\preceq$ be a relation on a set L. We say that $\preceq$ is a partial ordering on L if it is reflexive, antisymmetric, and transitive. That is:

1. $\preceq$ is reflexive: $a \preceq a \quad \forall a \in L$
2. $\preceq$ is antisymmetric: $a \preceq b$ and $a \neq b \Rightarrow b \npreceq a \quad \forall a, b \in L$
3. $\preceq$ is transitive: $a \preceq b$ and $b \preceq c \Rightarrow a \preceq c \quad \forall a, b, c \in L$

The set together with the relation $(L, \preceq)$ is called a poset.

Example 12.1.1: Some Posets

We recall a few examples of posets:

a. $(\mathbb{R}, \leq)$ is a poset. Notice that our generic symbol for the partial ordering, $\preceq$, is selected to remind us that a partial ordering is similar to "less than or equal to."
b. Let $A = \{a, b\}$. Then $(\mathcal{P}(A), \subseteq)$ is a poset.
c. Let $L = \{1, 2, 3, 6\}$. Then $(L, |)$ is a poset.

The posets we will concentrate on in this chapter will be those which have upper and lower bounds in relation to any pair of elements. Next, we define this concept precisely.

Definition 12.1.2: Lower Bound, Upper Bound

Let $(L, \preceq)$ be a poset, and $a, b \in L$. Then $c \in L$ is a lower bound of a and b if $c \preceq a$ and $c \preceq b$. Also, $d \in L$ is an upper bound of a and b if $a \preceq d$ and $b \preceq d$.

In most of the posets that will interest us, every pair of elements have both upper and lower bounds, though there are posets for which this is not true.

Definition 12.1.3: Greatest Lower Bound

Let $(L, \preceq)$ be a poset. If $a, b \in L$, then $\ell \in L$ is a greatest lower bound of a and b if and only if

- $\ell \preceq a$
- $\ell \preceq b$
- If $\ell' \in L$ such that $\ell' \preceq a$ and $\ell' \preceq b$, then $\ell' \preceq \ell$.

The last condition in the definition of Greatest Lower Bound says that if ℓ' is also a lower bound, then ℓ is "greater" in relation to $\preceq$ than ℓ'. The definition of a least upper bound is a mirror image of a greatest lower bound:

Definition 12.1.4: Least Upper Bound

Let $(L, \preceq)$ be a poset. If $a, b \in L$, then $u \in L$ is a least upper bound of a and b if and only if

- $a \preceq u$
- $b \preceq u$
- If $u' \in L$ such that if $a \preceq u'$ and $b \preceq u'$, then $u \preceq u'$.

Notice that the two definitions above refer to "...a greatest lower bound" and "a least upper bound." Any time you define an object like these you need to have an open mind as to whether more than one such object can exist. In fact, we now can prove that there can't be two greatest lower bounds or two least upper bounds.

Theorem 12.1.1: Uniqueness of Least Upper and Greatest Lower Bounds

Let $(L, \preceq)$ be a poset, and $a, b \in L$. If a greatest lower bound of a and b exists, then it is unique. The same is true of a least upper bound, if it exists.

Proof

Let ℓ and ℓ' be greatest lower bounds of a and b. We will prove that $\ell = \ell'$.

1. ℓ a greatest lower bound of a and $b \Rightarrow \ell$ is a lower bound of a and b.
2. ℓ' a greatest lower bound of a and b and ℓ a lower bound of a and $b \Rightarrow \ell \preceq \ell'$, by the definition of greatest lower bound.
3. ℓ' a greatest lower bound of a and $b \Rightarrow \ell'$ is a lower bound of a and b.
4. ℓ a greatest lower bound of a and b and ℓ' a lower bound of a and $b. \Rightarrow \ell' \preceq \ell$ by the definition of greatest lower bound.
5. $\ell \preceq \ell'$ and $\ell' \preceq \ell \Rightarrow \ell = \ell'$ by the antisymmetry property of a partial ordering.

The proof of the second statement in the theorem is almost identical to the first and is left to the reader.

Definition 12.1.5: Greatest Element, Least Element

Let $(L, \preceq)$ be a poset. $M \in L$ is called the greatest (maximum) element of L if, for all $a \in L$, $a \preceq M$. In addition, $m \in L$ is called the least (minimum) element of L if for all $a \in L$, $m \preceq a$. The greatest and least elements, when they exist, are frequently denoted by **1** and **0** respectively.

Example 12.1.2: Bounds on the Divisors of 105

Consider the partial ordering "divides" on $L = \{1, 3, 5, 7, 15, 21, 35, 105\}$Then $(L, |)$ is a poset. To determine the least upper bound of 3 and 7, we look for all $u \in L$, such that $3|u$ and $7|u$. Certainly, both $u = 21$ and $u = 105$ satisfy these conditions and no other element of L does. Next, since $21|105$,21 is the least upper bound of 3 and 7. Similarly, the least upper bound of 3 and 5 is 15. The greatest element of L is 105 since $a|105$ for all $a \in L$. To find the greatest lower bound of 15 and 35, we first consider all elements g of L such that $g \mid 15$. They are 1, 3, 5, and 15. The elements for which $g \mid 35$ are 1, 5, 7, and 35. From these two lists, we see that $\ell = 5$ and $\ell = 1$ satisfy the required conditions. But since $1|5$, the greatest lower bound is 5. The least element of L is 1 since $1|a$ for all $a \in L$.

Definition 12.1.6: The Set of Divisors of an Integer

For any positive integer n, the divisors of n is the set of integers that divide evenly into n. We denote this set D_n.

For example, the set L of Example $12.1.2$is D_{105}.

Example 12.1.3: The Power Set of a Three Element Set

Consider the poset $(\mathcal{P}(A), \subseteq)$, where $A = \{1, 2, 3\}$. The greatest lower bound of $\{1, 2\}$ and $\{1, 3\}$ is $\ell = \{1\}$. For any other element ℓ' which is a subset of $\{a, b\}$ and $\{a, c\}$ (there is only one; what is it?), $\ell' \subseteq \ell$. The least element of $\mathcal{P}(A)$ is $\emptyset$ and the greatest element is $A = \{a, b, c\}$. The Hasse diagram of this poset is shown in Figure $12.1.1$.

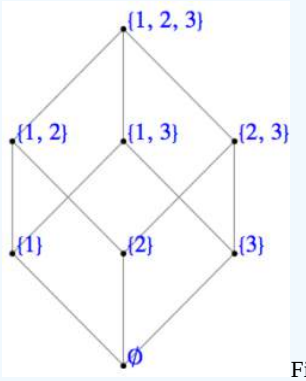


Figure 12.1.1: Power Set of $\{1,\ 2,\ 3\}$

The previous examples and definitions indicate that the least upper bound and greatest lower bound are defined in terms of the partial ordering of the given poset. It is not yet clear whether all posets have the property such every pair of elements always has both a least upper bound and greatest lower bound. Indeed, this is not the case (see Exercise 12.1.1).

12.1.1: Exercises

Exercise 12.1.1

Consider the poset $(D_{30}, |)$, where $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

a. Find all lower bounds of 10 and 15.
b. Find the greatest lower bound of 10 and 15.
c. Find all upper bounds of 10 and 15.
d. Determine the least upper bound of 10 and 15.
e. Draw the Hasse diagram for D_{30} with respect to $|$. Compare this Hasse diagram with that of Example 12.1.3. Note that the two diagrams are structurally the same.

Answer

a. 1, 5
b. 5
c. 30
d. 30
e. See the Sage cell below with the default input displaying a Hasse diagram for D_{12}.

Exercise 12.1.2

List the elements of the sets D_8, D_{50}, and D_{1001}. For each set, draw the Hasse diagram for "divides."

Exercise 12.1.3

Figure 12.1.2 contains Hasse diagrams of posets.

a. Determine the least upper bound and greatest lower bound of all pairs of elements when they exist. Indicate those pairs that do not have a least upper bound (or a greatest lower bound).
b. Find the least and greatest elements when they exist.

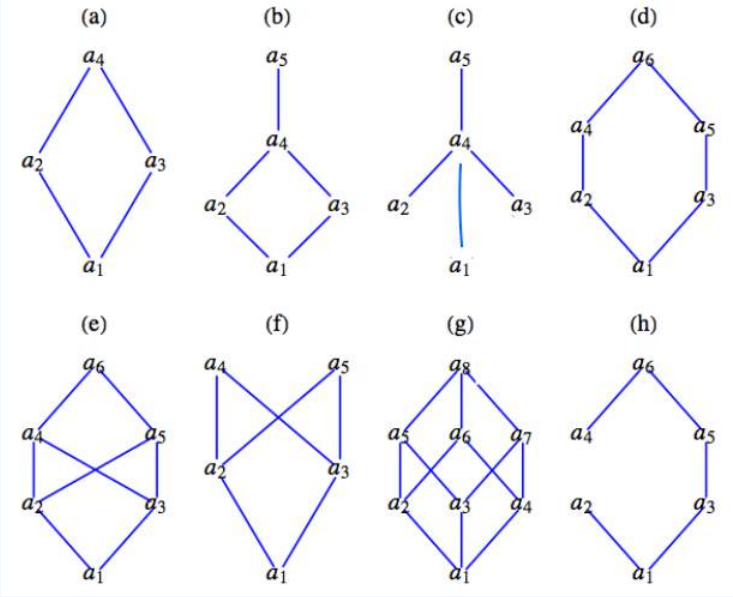


Figure 12.1.2: Figure for Exercise 12.1.3

Answer

- Solution for Hasse diagram (b):
  -

$\vee$	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_2	a_3	a_4	a_5
a_2	a_2	a_2	a_4	a_4	a_5
a_3	a_3	a_4	a_3	a_4	a_5
a_4	a_4	a_4	a_4	a_4	a_5
a_5	a_5	a_5	a_5	a_5	a_5

$\wedge$	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_1	a_1	a_1	a_1
a_2	a_1	a_2	a_1	a_2	a_2
a_3	a_1	a_1	a_3	a_3	a_3
a_4	a_1	a_2	a_3	a_4	a_4
a_5	a_1	a_2	a_3	a_4	a_5

    a_1 is the least element and a_5 is the greatest element.
- Partial solution for Hasse diagram (f):
  - $\text{lub}(a_2, a_3)$ and $\text{lub}(a_4, a_5)$ do not exist.
  - No greatest element exists, but a_1 is the least element.

Exercise 12.1.4

For the poset $(\mathbb{N}, \leq)$, what are the greatest lower bound and least upper bound of two elements a and b? Are there least and/or greatest elements?

Exercise 12.1.5

a. Prove the second part of Theorem 12.1.1, the least upper bound of two elements in a poset is unique, it one exists.
b. Prove that if a poset L has a least element, then that element is unique.

Answer

If 0 and $0'$ are distinct least elements, then

$$\left.\begin{array}{ll} 0 \leq 0' & \text{since } 0 \text{ is a least element} \\ 0' \leq 0 & \text{since } 0' \text{ is a least element} \end{array}\right\} \Rightarrow 0 = 0' \text{ by antisymmetry, a contradiction}$$

Exercise 12.1.6

We naturally order the numbers in $A_m = \{1, 2, \ldots, m\}$ with "less than or equal to," which is a partial ordering. We define an ordering, $\preceq$ on the elements of $A_m \times A_n$ by

$$(a, b) \preceq (a', b') \Leftrightarrow a \leq a' \text{ and } b \leq b'$$

a. Prove that $\preceq$ is a partial ordering on $A_m \times A_n$.
b. Draw the ordering diagrams for $\preceq$ on $A_2 \times A_2,\ A_2 \times A_3,$ and $A_3 \times A_3$.
c. In general, how does one determine the least upper bound and greatest lower bound of two elements of $A_m \times A_n,\ (a, b)$ and (a', b')?
d. Are there least and/or greatest elements in $A_m \times A_n$?

Exercise 12.1.7

Let $\mathcal{P}_0$ be the set of all subsets T of $S = \{1, 2, \ldots, 9\}$ such that the sum of the elements in T is even. (Note that the empty set $\emptyset$ will be included as an element of $\mathcal{P}_0$.) For instance, $\{2, 3, 6, 7\}$is in $\mathcal{P}_0$ because $2 + 3 + 6 + 7$ is even, but $\{1, 3, 5, 6\}$is not in $\mathcal{P}_0$ because $1 + 3 + 5 + 6$ is odd. Consider the poset $(\mathcal{P}_0, \subseteq)$. Let $A = \{1, 2, 3, 6\}$ and $B = \{2, 3, 6, 7\}$ be elements of $\mathcal{P}_0$.

a. Explain why $A \cap B$ is not element of the poset.
b. Use the definitions of the italicized terms and the given partial ordering to complete the following statements:
   i. $R \in \mathcal{P}_0$ is an *upper bound* of A and B if \rule{3cm}{0.01cm}
   ii. $R \in \mathcal{P}_0$ is the *least element* of $\mathcal{P}_0$ if \rule{3cm}{0.01cm}
c. Find three different upper bounds of A and B.
d. Find the least upper bound of A and B. If it doesn't exist, explain why not.

Answer

a. The sum of elements in $A \cap B = \{2,\ 3,\ 6\}$ is odd and disqualifies the set from being an element of the poset.
b. Use the definitions of the italicized terms and the given partial ordering to complete the following statements:
   i. $\ldots A \subseteq R$ and $B \subseteq R$
   ii. $\ldots$ for all $A \in \mathcal{P}_0$, $R \subseteq A$
c. Any set that contains the union of $A \cup B = \{1,\ 2,\ 3,\ 6,\ 7\}$but also contains 3 or 5, but not both will be an upper bound. You can create several by including on not including 4 or 8.
d. The least upper bound doesn't exist. Notice that the union of A and B isn't in $\mathcal{P}_0$. One of the two sets $\{1,\ 2,\ 3,\ 5,\ 6,\ 7\}$ and $\{1,\ 2,\ 3,\ 6,\ 7,\ 9\}$is contained within every upper bound of A and B but neither is contained within the other.

12.2: Lattices

In this section, we restrict our discussion to lattices, those posets for which every pair of elements has both a greatest lower bound and least upper bound. We first introduce some notation.

Definition 12.2.1: Join, Meet

Let $(L, \preceq)$ be a poset, and $a, b \in L$. We define:

- $a \vee b$, read "a join b", as the least upper bound of a and b, if it exists. and
- $a \wedge b$, read "a meet b", as the greatest lower bound of a and b, if it exists.

Since the join and meet produce a unique result in all cases where they exist, by Theorem 13.1.1, we can consider them as binary operations on a set if they always exist. Thus the following definition:

Definition 12.2.2: Lattice

A lattice is a poset $(L, \preceq)$ for which every pair of elements has a greatest lower bound and least upper bound. Since a lattice L is an algebraic system with binary operations $\vee$ and $\wedge$, it is denoted by $[L; \vee, \wedge]$. If we want to make it clear what partial ordering the lattice is based on, we say it is a lattice under $\preceq$.

Example 12.2.1: The Power Set of a Three Element Set

Consider the poset $(\mathcal{P}(A), \subseteq)$ we examined in Example 13.1.3. It isn't too surprising that every pair of sets had a greatest lower bound and least upper bound. Thus, we have a lattice in this case; and $A \vee B = A \cup B$ and $A \wedge B = A \cap B$. The reader is encouraged to write out the operation tables $[\mathcal{P}(A); \cup, \cap]$.

Our first concrete lattice can be generalized to the case of any set A, producing the lattice $[\mathcal{P}(A); \vee, \wedge]$, where the join operation is the set operation of union and the meet operation is the operation intersection; that is, $\vee = \cup$ and $\wedge = \cap$.

It can be shown (see the exercises) that the commutative laws, associative laws, idempotent laws, and absorption laws are all true for any lattice. A concrete example of this is clearly $[\mathcal{P}(A); \cup, \cap]$, since these laws hold in the algebra of sets. This lattice also has distributive property in that join is distributive over meet and meet is distributive over join. However, this is not always the case for lattices in general.

Definition 12.2.3: Distributive Lattice

Let $\mathcal{L} = [L; \vee, \wedge]$ be a lattice under $\preceq$. $\mathcal{L}$ is called a distributive lattice if and only if the distributive laws hold; that is, for all $a, b, c \in L$ we have

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$
$$and$$
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

Example 12.2.2: A Nondistributive Lattice

We now give an example of a lattice where the distributive laws do not hold. Let $L = \{\mathbf{0}, a, b, c, \mathbf{1}\}$. We define the partial ordering $\preceq$ on L by the set

$$\{(\mathbf{0}, \mathbf{0}), (\mathbf{0}, a), (\mathbf{0}, b), (\mathbf{0}, c), (\mathbf{0}, \mathbf{1}), (a, a), (a, \mathbf{1}), (b, b), (b, \mathbf{1}), (c, c), (c, \mathbf{1}), (\mathbf{1}, \mathbf{1})\}$$

The operation tables for $\vee$ and $\wedge$ on L are:

$\vee$	$\mathbf{0}$	a	b	c	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	a	b	c	$\mathbf{1}$
a	a	a	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$
b	b	$\mathbf{1}$	b	$\mathbf{1}$	$\mathbf{1}$
c	c	$\mathbf{1}$	$\mathbf{1}$	c	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$

$\wedge$	$\mathbf{0}$	a	b	c	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
a	$\mathbf{0}$	a	$\mathbf{0}$	$\mathbf{0}$	a
b	$\mathbf{0}$	$\mathbf{0}$	b	$\mathbf{0}$	b
c	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	c	c
$\mathbf{1}$	$\mathbf{0}$	a	b	c	$\mathbf{1}$

Since every pair of elements in L has both a join and a meet, $[L; \vee, \wedge]$ is a lattice (under divides). Is this lattice distributive? We note that: $a \vee (c \wedge b) = a \vee \mathbf{0} = a$ and $(a \vee c) \wedge (a \vee b) = \mathbf{1} \wedge \mathbf{1} = \mathbf{1}$. Therefore, $a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c)$ for some values of $a, b, c \in L$. Thus, this lattice is not distributive.

Our next observation uses the term “sublattice”, which we have not defined at this point, but we would hope that you could anticipate a definition, and we will leave it as an exercises to do so.

It can be shown that a lattice is nondistributive if and only if it contains a sublattice isomorphic to one of the lattices in Figure 12.2.1. The ordering diagram on the right of this figure, produces the ***diamond lattice***, which is precisely the one that is defined in Example 12.2.2 The lattice based on the left hand poset is called the ***pentagon lattice***.

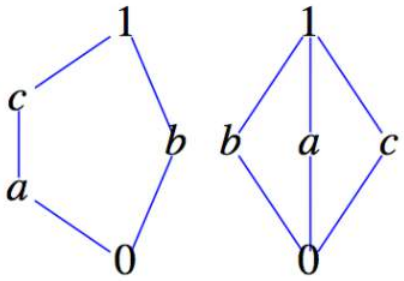


Figure 12.2.1: Nondistributive lattices, the pentagon and diamond lattices

12.2.1: 13.2.1: Exercises

Exercise 12.2.1

Let L be the set of all propositions generated by p and q. What are the meet and join operations in this lattice under implication? What are the maximum and minimum elements?

Exercise 12.2.2

Which of the posets in Exercise 13.1.3 are lattices? Which of the lattices are distributive?

Exercise 12.2.3

a. State the commutative laws, associative laws, idempotent laws, and absorption laws for lattices.
b. Prove laws you stated.

Exercise 12.2.4

Demonstrate that the pentagon lattice is nondistributive.

Exercise 12.2.5

What is a reasonable definition of the term ***sublattice***?

Answer

One reasonable definition would be this: Let $[L; \vee, \wedge]$ be a lattice and let K be a nonempty subset of L. Then K is a sublattice of L if and only if K is closed under both $\vee$ and $\wedge$

Exercise 12.2.6

Let $[L; \vee, \wedge]$ be a lattice based on a partial ordering $\preceq$. Prove that if $a, b, c \in L$,

a. $a \preceq a \vee b$.
b. $a \wedge b \preceq a$.
c. $b \preceq a$ and $c \preceq a \Rightarrow b \vee c \preceq a$.

12.3: Boolean Algebras

In order to define a Boolean algebra, we need the additional concept of complementation. A lattice must have both a greatest element and a least element in order for complementation to take place. The following definition will save us some words in the rest of this section.

Definition 12.3.1: Bounded Lattice

A bounded lattice is a lattice that contains both a least element and a greatest element.

We use the symbols **0** and **1** for the least and greatest elements of a bounded lattice in the remainder of this section.

Definition 12.3.2: The Complement of a Lattice Element

Let $[L; \vee, \wedge]$ be a bounded lattice. If $a \in L$, then a has a complement if there exists $b \in L$ such that

$$a \vee b = \mathbf{1}$$
and
$$a \wedge b = \mathbf{0}$$

Notice that by the commutative laws for lattices, if b complements a, then a complements b.

Definition 12.3.3: Complemented Lattice

Let $\mathcal{L} = [L; \vee, \wedge]$ be a bounded lattice. $\mathcal{L}$ is a complemented lattice if every element of L has a complement in L.

Example 12.3.1: Set Complement is a Complement

In Chapter 1, we defined the complement of a subset of any universe. This turns out to be a concrete example of the general concept we have just defined, but we will reason through why this is the case here. Let $L = \mathcal{P}(A)$, where $A = \{a, b, c\}$. Then $[L; \cup, \cap]$ is a bounded lattice with $0 = \emptyset$ and $1 = A$. To find the complement, if it exists, of $B = \{a, b\} \in L$, for example, we want D such that

$$\{a, b\} \cap D = \emptyset$$
$$and$$
$$\{a, b\} \cup D = A$$

It's not too difficult to see that $D = \{c\}$, since we need to include c to make the first condition true and can't include a or b if the second condition is to be true. Of course this is precisely how we defined A^c in Chapter 1. Since it can be shown that each element of L has a complement (see Exercise 1), $[L; \cup, \cap]$ is a complemented lattice. Note that if A is any set and $L = \mathcal{P}(A)$, then $[L; \cup, \cap]$ is a complemented lattice where the complement of $B \in L$ is $B^c = A - B$.

In Example 12.3.1, we observed that the complement of each element of L is unique. Is this always true in a complemented lattice? The answer is no. Consider the following.

Example 12.3.2: A Lattice for Which Complements are Not Unique

Let $L = \{1, 2, 3, 5, 30\}$ and consider the lattice $[L; \vee, \wedge]$ (under "divides"). The least element of L is 1 and the greatest element is 30. Let us compute the complement of the element $a = 2$. We want to determine $\bar{a}$ such that $2 \wedge \bar{a} = 1$ and $2 \vee \bar{a} = 30$. Certainly, $\bar{a} = 3$ works, but so does $\bar{a} = 5$, so the complement of $a = 2$ in this lattice is not unique. However, $[L; \vee, \wedge]$ is still a complemented lattice since each element does have at least one complement.

Definition 12.3.4: Complementation as an Operation

If a complemented lattice has the property that the complement of every element is unique, then we consider complementation to be a unary operation. The usual notation for the complement of a is $\bar{a}$.

The following theorem gives us an insight into when uniqueness of complements occurs.

Theorem 12.3.1: One Condition for Unique Complements

If $[L; \vee, \wedge]$ is a complemented, distributive lattice, then the complement of each element $a \in L$ is unique.

Proof

Let $a \in L$ and assume to the contrary that a has two complements, namely a_1 and a_2. Then by the definition of complement,

$$\begin{array}{c} a \wedge a_1 = 0 \text{ and } a \vee a_1 = 1, \\ \textit{and} \\ a \wedge a_2 = 0 \text{ and } a \vee a_2 = 1, \end{array} .$$

Then

$$\begin{aligned} a_1 &= a_1 \wedge \mathbf{1} = a_1 \wedge (a \vee a_2) \\ &= (a_1 \wedge a) \vee (a_1 \wedge a_2) \\ &= \mathbf{0} \vee (a_1 \wedge a_2) \\ &= a_1 \wedge a_2 \end{aligned}$$

On the other hand,

$$\begin{aligned} a_2 &= a_2 \wedge \mathbf{1} = a_2 \wedge (a \vee a_1) \\ &= (a_2 \wedge a) \vee (a_2 \wedge a_1) \\ &= \mathbf{0} \vee (a_2 \wedge a_1) \\ &= a_2 \wedge a_1 \\ &= a_1 \wedge a_2 \end{aligned}$$

Hence $a_1 = a_2$, which contradicts the assumption that a has two different complements.

Definition 12.3.5: Boolean Algebra

A Boolean algebra is a lattice that contains a least element and a greatest element and that is both complemented and distributive. The notation $[B; \vee, \wedge, \bar{\ }]$ is used to denote the boolean algebra with operations join, meet and complementation.

Since the complement of each element in a Boolean algebra is unique (by Theorem 12.3.1), complementation is a valid unary operation over the set under discussion, which is why we will list it together with the other two operations to emphasize that we are discussing a set together with three operations. Also, to help emphasize the distinction between lattices and lattices that are Boolean algebras, we will use the letter B as the generic symbol for the set of a Boolean algebra; that is, $[B; \vee, \wedge, \bar{\ }]$ will stand for a general Boolean algebra.

Example 12.3.3: Boolean Algebra of Sets

Let A be any set, and let $B = \mathcal{P}(A)$. Then $[B; \cup, \cap, ^c]$ is a Boolean algebra. Here, ^{c} stands for the complement of an element of B with respect to A, $A - B$.

This is a key example for us since all finite Boolean algebras and many infinite Boolean algebras look like this example for some A. In fact, a glance at the basic Boolean algebra laws in Table 12.3.1, in comparison with the set laws of Chapter 4 and the basic laws of logic of Chapter 3, indicates that all three systems behave the same; that is, they are isomorphic.

Example 12.3.4: Divisors of 30

A somewhat less standard example of a boolean algebra is derived from the lattice of divisors of 30 under the relation "divides". If you examine the ordering diagram for this lattice, you see that it is structurally the same as the boolean algebra of subsets of a three element set. Therefore, the join, meet and complementation operations act the same as union, intersection and set complementation. We might conjecture that the lattice of divisors of any integer will produce a boolean algebra, but it is only the case of certain integers. Try out a few integers to see if you can identify what is necessary to produce a boolean algebra.

Table 12.3.1: Basic Boolean Algebra Laws

Commutative Laws	$a \vee b = b \vee a$	$a \wedge b = b \wedge a$
Associative Laws	$a \vee (b \vee c) = (a \vee b) \vee c$	$a \wedge (b \wedge c) = (a \wedge b) \wedge c$
Distributive Laws	$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
Identity Laws	$a \vee 0 = 0 \vee a = a$	$a \wedge 1 = 1 \wedge a = a$
Complement Laws	$a \vee \bar{a} = 1$	$a \wedge \bar{a} = 0$
Idempotent Laws	$a \vee a = a$	$a \wedge a = a$
Null Laws	$a \vee 1 = 1$	$a \wedge 0 = 0$
Absorption Laws	$a \vee (a \wedge b) = a$	$a \wedge (a \vee b) = a$
DeMorgan's Laws	$\overline{a \vee b} = \bar{a} \wedge \bar{b}$	$\overline{a \wedge b} = \bar{a} \vee \bar{b}$
Involution Law	$\bar{\bar{a}} = a$	

The "pairings" of the boolean algebra laws reminds us of the principle of duality, which we state for a Boolean algebra.

Definition 12.3.6: Principle of Duality for Boolean Algebras

Let $\mathcal{B} = [B; \vee, \wedge, {}^c]$ be a Boolean algebra under $\preceq$, and let S be a true statement for $\mathcal{B}$. If S^* is obtained from S by replacing $\preceq$ with $\succeq$ (this is equivalent to turning the graph upside down), $\vee$ with $\wedge$, $\wedge$ with $\vee$, $\mathbf{0}$ with $\mathbf{1}$, and $\mathbf{1}$ with $\mathbf{0}$, then S^* is also a true statement in $\mathcal{B}$.

12.3.1: Exercises

Exercise 12.3.1

Determine the complement of each element $B \in L$ in Example 12.3.1. Is this lattice a Boolean algebra? Why?

Answer

B	Complement of B
$\emptyset$	A
$\{a\}$	$\{b, c\}$
$\{b\}$	$\{a, c\}$
$\{c\}$	$\{a, b\}$
$\{a, b\}$	$\{c\}$
$\{a, c\}$	$\{b\}$
$\{b, c\}$	$\{a\}$
A	$\emptyset$

This lattice is a Boolean algebra since it is a distributive complemented lattice.

Exercise 12.3.2

a. Determine the complement of each element of D_6 in $[D_6; \vee, \wedge]$.
b. Repeat part a using the lattice in Example 13.2.2.
c. Repeat part a using the lattice in Exercise 13.1.1.
d. Are the lattices in parts a, b, and c Boolean algebras? Why?

Exercise 12.3.3

Determine which of the lattices of Exercise 13.1.3 of Section 13.1 are Boolean algebras.

Answer

a and g.

Exercise 12.3.4

Let $A = \{a, b\}$ and $B = \mathcal{P}(A)$.

a. Prove that $[B; \cup, \cap, {}^c]$ is a Boolean algebra.
b. Write out the operation tables for the Boolean algebra.

Exercise 12.3.5

It can be shown that the following statement, S, holds for any Boolean algebra $[B; \vee, \wedge, -]$: $(a \wedge b) = a$ if and only if $a \leq b$.

a. Write the dual, S^*, of the statement S.
b. Write the statement S and its dual, S^*, in the language of sets.
c. Are the statements in part b true for all sets?
d. Write the statement S and its dual, S^*, in the language of logic.
e. Are the statements in part d true for all propositions?

Answer

a. $S^*: a \vee b = a$ if $a \geq b$
b. The dual of $S: A \cap B = A$ if $A \subseteq B$ is $S^*: A \cup B = A$ if $A \supseteq B$
c. Yes
d. The dual of $S: p \wedge q \Leftrightarrow p$ if $p \Rightarrow q$ is $S^*: p \vee q \Leftrightarrow p$ if $q \Rightarrow p$
e. Yes

Exercise 12.3.6

State the dual of:

a. $a \vee (b \wedge a) = a$.
b. $a \vee \left(\overline{(\bar{b} \vee a) \wedge b}\right) = 1$.
c. $\left(\overline{a \wedge \bar{b}}\right) \wedge b = a \vee b$.

Exercise 12.3.7

Formulate a definition for isomorphic Boolean algebras.

Answer

$[B; \wedge, \vee, -]$ is isomorphic to $[B'; \wedge, \vee, \tilde{}\,]$ if and only if there exists a function $T: B \to B'$ such that

a. T is a bijection;

b. $T(a \wedge b) = T(a) \wedge T(b)$ for all $a, b \in B$
c. $T(a \vee b) = T(a) \vee T(b)$ for all $a, b \in B$
d. $T(\bar{a}) = \tilde{T(a)}$ for all $a \in B$.

Exercise 12.3.8

For what positive integers, n, does the lattice $[D_n, |]$ produce a boolean algebra?

12.4: Atoms of a Boolean Algebra

In this section we will look more closely at something we've hinted at, which is that every finite Boolean algebra is isomorphic to an algebra of sets. We will show that every finite Boolean algebra has 2^n elements for some n with precisely n generators, called atoms.

Consider the Boolean algebra $[B; \vee, \wedge, ^-]$, whose ordering diagram is depicted in Figure $12.4.1$

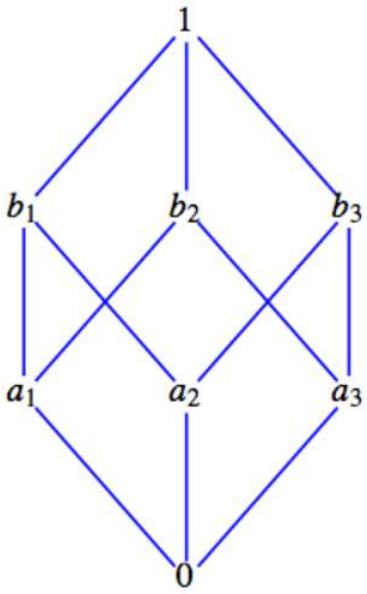


Figure 12.4.1: Illustration of the atom concept

We note that $1 = a_1 \vee a_2 \vee a_3$, $b_1 = a_1 \vee a_2$, $b_2 = a_1 \vee a_3$, and $b_3 = a_2 \vee a_3$; that is, each of the elements above level one can be described completely and uniquely in terms of the elements on level one. The a_i's have uniquely generated the non-least elements of B much like a basis in linear algebra generates the elements in a vector space. We also note that the a_i's are the immediate successors of the minimum element, 0. In any Boolean algebra, the immediate successors of the minimum element are called ***atoms***. For example, let A be any nonempty set. In the Boolean algebra $[\mathcal{P}(A); \cup, \cap, ^c]$ (over $\subseteq$), the singleton sets are the generators, or atoms, of the algebraic structure since each element $\mathcal{P}(A)$ can be described completely and uniquely as the join, or union, of singleton sets.

Definition 12.4.1: Atom

A non-least element a in a Boolean algebra $[B; \vee, \wedge, ^-]$ is called an atom if for every $x \in B$, $x \wedge a = a$ or $x \wedge a = 0$.

The condition that $x \wedge a = a$ tells us that x is a successor of a; that is, $a \preceq x$, as depicted in Figure $12.4.2$(a)

The condition $x \wedge a = 0$ is true only when x and a are "not connected." This occurs when x is another atom or if x is a successor of atoms different from a, as depicted in Figure $12.4.2$(b).

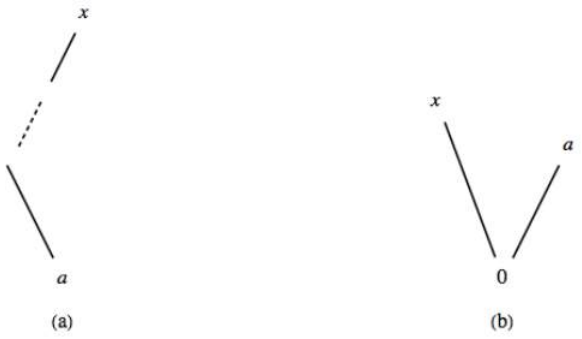


Figure 12.4.2: Conditions for an atom

An alternate definition of an atom is based on the concept of "covering."

Definition 12.4.2: The Covering Relation

Given a Boolean algebra $[B; \vee, \wedge, \bar{\ }]$, let $x, z \in B$. We say that z ***covers*** x iff $x \prec z$ and there does not exist $y \in B$ with $x \prec y \prec z$.

It can be proven that the atoms of Boolean algebra are precisely those elements that cover the zero element.

The set of atoms of the Boolean algebra $[D_{30}; \vee, \wedge, \bar{\ }]$ is $M = \{2, 3, 5\}$. To see that $a = 2$ is an atom, let x be any non-least element of D_{30} and note that one of the two conditions $x \wedge 2 = 2$ or $x \wedge 2 = 1$ holds. Of course, to apply the definition to this Boolean algebra, we must remind ourselves that in this case the 0-element is 1, the operation $\wedge$ is greatest common divisor, and the poset relation is "divides." So if $x = 10$, we have $10 \wedge 2 = 2$ (or $2 \mid 10$), so Condition 1 holds. If $x = 15$, the first condition is not true. (Why?) However, Condition 2, $15 \wedge 2 = 1$, is true. The reader is encouraged to show that 3 and 5 also satisfy the definition of an atom. Next, if we should compute the join (the least common multiple in this case) of all possible combinations of the atoms 2, 3, and 5 to generate all nonzero (non-1 in this case) elements of D_{30}. For example, $2 \vee 3 \vee 5 = 30$ and $2 \vee 5 = 10$. We state this concept formally in the following theorem, which we give without proof.

Theorem 12.4.1

Let $\mathcal{B} = [B; \vee, \wedge, \bar{\ }]$ be any finite Boolean algebra. Let $A = \{a_1, a_2, \ldots, a_n\}$ be the set of all atoms of $\mathcal{B}$. Then every element in B can be expressed uniquely as the join of a subset of A.

The least element in relation to this theorem bears noting. If we consider the empty set of atoms, we would consider the join of elements in the empty set to be the least element. This makes the statement of the theorem above a bit more tidy since we don't need to qualify what elements can be generated from atoms.

We now ask ourselves if we can be more definitive about the structure of different Boolean algebras of a given order. Certainly, the Boolean algebras $[D_{30}; \vee, \wedge, \wedge\ \bar{\ }]$ and $[\mathcal{P}(A); \cup, \cap, {}^c]$ have the same graph (that of Figure 12.4.1), the same number of atoms, and, in all respects, look the same except for the names of the elements and the operations. In fact, when we apply corresponding operations to corresponding elements, we obtain corresponding results. We know from Chapter 11 that this means that the two structures are isomorphic as Boolean algebras. Furthermore, the graphs of these examples are exactly the same as that of Figure 12.4.1, which is an arbitrary Boolean algebra of order $8 = 2^3$.

In these examples of a Boolean algebra of order 8, we note that each had 3 atoms and $2^3 = 8$ number of elements, and all were isomorphic to $[\mathcal{P}(A); \cup, \cap, {}^c]$, where $A = \{a, b, c\}$. This leads us to the following questions:

- Are there any different (nonisomorphic) Boolean algebras of order 8?
- What is the relationship, if any, between finite Boolean algebras and their atoms?
- How many different (nonisomorphic) Boolean algebras are there of order 2? Order 3? Order 4? etc.

The answers to these questions are given in the following theorem and corollaries.

Theorem 12.4.2

Let $\mathcal{B} = [B; \vee, \wedge, -]$ be any finite Boolean algebra, and let A be the set of all atoms of $\mathcal{B}$. Then $[\mathcal{P}(A); \cup, \cap, {}^c]$ is isomorphic to $[B; \vee, \wedge, -]$

Proof

An isomorphism that serves to prove this theorem is $T : \mathcal{P}(A) \to B$ defined by $T(S) = \bigvee_{a \in S} a$, where $T(\emptyset)$ is interpreted as the zero of $\mathcal{B}$. We leave it to the reader to prove that this is indeed an isomorphism.

Corollary 12.4.1

Every finite Boolean algebra $\mathcal{B} = [B; \vee, \wedge, \bar{\ }]$ has 2^n elements for some positive integer n.

Proof

Let A be the set of all atoms of $\mathcal{B}$ and let $|A| = n$. Then there are exactly 2^n elements (subsets) in $\mathcal{P}(A)$, and by Theorem 12.4.2 $[B; \vee, \wedge, \bar{\ }]$ is isomorphic to $[\mathcal{P}(A); \cup, \cap\ {}^c]$ and must also have 2^n elements.

Corollary 12.4.2

All Boolean algebras of order 2^n are isomorphic to one another.

Proof

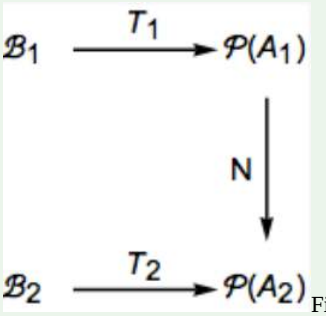


Figure 12.4.1: Isomorphisms to be combined

Every Boolean algebra of order 2^n is isomorphic to $[\mathcal{P}(A); \cup, \cap, {}^c]$ when $|A| = n$. Hence, if $\mathcal{B}_1$ and $\mathcal{B}_2$ each have 2^n elements, they each have n atoms. Suppose their sets of atoms are A_1 and A_2, respectively. We know there are isomorphisms T_1 and T_2, where $T_i : \mathcal{B}_i \to \mathcal{P}(A_i),\ i = 1, 2$. In addition we have an isomorphism, N from $\mathcal{P}(A_1)$ into $\mathcal{P}(A_2)$, which we ask you to prove in Exercise 12.4.9 We can combine these isomorphisms to produce the isomorphism $T_2^{-1} \circ N \circ T_1 : \mathcal{B}_1 \to \mathcal{B}_2,$ which proves the corollary.

The above theorem and corollaries tell us that we can only have finite Boolean algebras of orders $2^1, 2^2, 2^3, \ldots, 2^n$, and that all finite Boolean algebras of any given order are isomorphic. These are powerful tools in determining the structure of finite Boolean algebras. In the next section, we will discuss one of the easiest ways of describing a Boolean algebra of any given order.

12.4.1: Exercises

Exercise 12.4.1

a. Show that $a = 2$ is an atom of the Boolean algebra $[D_{30}; \vee, \wedge, -]$.
b. Repeat part a for the elements 3 and 5 of D_{30}.
c. Verify Theorem 12.4.1 for the Boolean algebra $[D_{30}; \vee, \wedge, -]$.

Answer

a. For $a = 3$ we must show that for each $x \in D_{30}$ one of the following is true: $x \wedge 3 = 3$ or $x \wedge 3 = 1$. We do this through the following table:

x	verification
1	$1 \wedge 3 = 1$
2	$2 \wedge 3 = 1$
3	$3 \wedge 3 = 3$
5	$5 \wedge 3 = 1$
6	$6 \wedge 3 = 3$
10	$20 \wedge 3 = 1$
15	$15 \wedge 3 = 3$
30	$30 \wedge 3 = 3$

For $a = 5$, a similar verification can be performed.
b. $6 = 2 \vee 3$, $10 = 2 \vee 5$, $15 = 3 \vee 5$, and $30 = 2 \vee 3 \vee 5$.

Exercise 12.4.2

Let $A = \{a, b, c\}$.

a. Rewrite the definition of atom for $[\mathcal{P}(A); \cup, \cap, c]$. What does $a \leq x$ mean in this example?
b. Find all atoms of $[\mathcal{P}(A); \cup, \cap, c]$.
c. Verify Theorem 12.4.1 for $[\mathcal{P}(A); c, \cup, \cap]$.

Exercise 12.4.3

Verify Theorem 12.4.2 and its corollaries for the Boolean algebras in Exercises 12.4.1 and 12.4.2 of this section.

Answer

If $B = D_{30}$ 30 then $A = \{2, 3, 5\}$ and D_{30} is isomorphic to $\mathcal{P}(A)$, where

$$\begin{array}{cc} 1 \leftrightarrow \emptyset & 5 \leftrightarrow \{5\} \\ 2 \leftrightarrow \{2\} & 10 \leftrightarrow \{2,5\} \\ 3 \leftrightarrow \{3\} & 15 \leftrightarrow \{3,5\} \\ 6 \leftrightarrow \{2,3\} & 30 \leftrightarrow \{2,3,5\} \end{array} \quad \text{and} \quad \begin{array}{c} \text{Join} \leftrightarrow \text{ Union} \\ \text{Meet} \leftrightarrow \text{ Intersection} \\ \text{Complement} \leftrightarrow \text{ Set Complement} \end{array}$$

Exercise 12.4.4

Give an example of a Boolean algebra of order 16 whose elements are certain subsets of the set $\{1, 2, 3, 4, 5, 6, 7\}$

Exercise 12.4.5

Corollary 12.4.1 implies that there do not exist Boolean algebras of orders 3, 5, 6, 7, 9, etc. (orders different from 2^n). Without this corollary, directly show that we cannot have a Boolean algebra of order 3.

Hint

Assume that $[B; \vee, \wedge, -]$ is a Boolean algebra of order 3 where $B = \{0, x, 1\}$ and show that this cannot happen by investigating the possibilities for its operation tables.

Answer

Assume that $x \neq 0$ or 1 is the third element of a Boolean algebra. Then there is only one possible set of tables for join and meet, all following from required properties of the Boolean algebra.

$\vee$	0	x	1
0	0	x	1
x	x	x	1
1	1	1	1

$\wedge$	0	x	1
0	0	0	0
x	0	x	x
1	0	x	1

Next, to find the complement of x we want y such that $x \wedge y = 0$ and $x \vee y = 1$. No element satisfies both conditions; hence the lattice is not complemented and cannot be a Boolean algebra. The lack of a complement can also be seen from the ordering diagram from which $\wedge$ and $\vee$ must be derived.

Exercise 12.4.6

a. There are many different, yet isomorphic, Boolean algebras with two elements. Describe one such Boolean algebra that is derived from a power set, $\mathcal{P}(A)$, under $\subseteq$. Describe a second that is described from D_n, for some $n \in P$, under "divides."
b. Since the elements of a two-element Boolean algebra must be the greatest and least elements, 1 and 0, the tables for the operations on $\{0, 1\}$ are determined by the Boolean algebra laws. Write out the operation tables for $[\{0, 1\}; \vee, \wedge, -]$.

Exercise 12.4.7

Find a Boolean algebra with a countably infinite number of elements.

Answer

Let X be any countably infinite set, such as the integers. A subset of X is ***cofinite*** if it is finite or its complement is finite. The set of all cofinite subsets of X is:

a. Countably infinite - this might not be obvious, but here is a hint. Assume $X = \{x_0, x_1, x_2, \ldots\}$. For each finite subset A of X, map that set to the integer $\sum_{i=0}^{\infty} \chi_A(x_i)\, 2^i$ You can do a similar thing to sets that have a finite complement, but map them to negative integers. Only one minor adjustment needs to be made to accommodate both the empty set and X.
b. Closed under union
c. Closed under intersection, and
d. Closed under complementation.

Therefore, if $B = \{A \subseteq X : A \text{ is cofinite}\}$, then B is a countable Boolean algebra under the usual set operations.

Exercise 12.4.8

Prove that the direct product of two Boolean algebras is a Boolean algebra.

Hint

"Copy" the corresponding proof for groups in Section 11.6.

Exercise 12.4.9

Prove if two finite sets A_1 and A_2 both have n elements then $[\mathcal{P}(A_1); \cup, \cap, {}^c]$ is isomorphic to $[\mathcal{P}(A_2); \cup, \cap, {}^c]$

Exercise 12.4.10

Prove an element of a Boolean algebra is an atom if and only if it covers the zero element.

12.5: Finite Boolean Algebras as n-tuples of 0's and 1's

From the previous section we know that all finite Boolean algebras are of order 2^n, where n is the number of atoms in the algebra. We can therefore completely describe every finite Boolean algebra by the algebra of power sets. Is there a more convenient, or at least an alternate way, of defining finite Boolean algebras? In Chapter 11 we found that we could produce new groups by taking Cartesian products of previously known groups. We imitate this process for Boolean algebras.

The simplest nontrivial Boolean algebra is the Boolean algebra on the set $B_2 = \{0, 1\}$. The ordering on B_2 is the natural one, $0 \leq 0, 0 \leq 1, 1 \leq 1$. If we treat 0 and 1 as the truth values "false" and "true," respectively, we see that the Boolean operations $\vee(\text{join})$ and $\wedge(\text{meet})$ are nothing more than the logical operation with the same symbols. The Boolean operation, $-$, (complementation) is the logical $\neg$ (negation). In fact, this is why these symbols were chosen as the names of the Boolean operations. The operation tables for $[B_2; \vee, \wedge, -]$ are simply those of "or," "and," and "not," which we repeat here.

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

u	$\bar{u}$
0	1
1	0

By Theorem 13.4.2 and its corollaries, all Boolean algebras of order 2 are isomorphic to this one.

We know that if we form $B_2 \times B_2 = B_2^2$ we obtain the set $\{(0,0),(0,1),(1,0),(1,1)\}$,a set of order 4. We define operations on B_2^2 the natural way, namely componentwise, so that $(0,1) \vee (1,1) = (0 \vee 1, 1 \vee 1) = (1,1)$, $(0,1) \wedge (1,1) = (0 \wedge 1, 1 \wedge 1) = (0,1)$ and $\overline{(0,1)} = (\bar{0}, \bar{1}) = (1,0)$. We claim that B_2^2 is a Boolean algebra under the componentwise operations. Hence, $\left[B_2^2; \vee, \wedge, {}^- \right]$ is a Boolean algebra of order 4. Since all Boolean algebras of order 4 are isomorphic to one other, we have found a simple way of describing all Boolean algebras of order 4.

It is quite clear that we can describe any Boolean algebra of order 8 by considering $B_2 \times B_2 \times B_2 = B_2^3$ and, more generally, any Boolean algebra of order 2^n with $B_2^n = B_2 \times B_2 \times \cdots \times B_2$ (n factors).

12.5.1: Exercises

Exercise 12.5.1

a. Write out the operation tables for $\left[B_2^2; \vee, \wedge, -\right]$.
b. Draw the Hasse diagram for $\left[B_2^2; \vee, \wedge, -\right]$ and compare your results with Figure 6.3.1.
c. Find the atoms of this Boolean algebra.

Answer

a.

$\vee$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,1)$	$(1,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(1,0)$	$(1,1)$
$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$	$(1,1)$

$\wedge$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$
$(1,0)$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,0)$
$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$

u	$\bar{u}$
$(0,0)$	$(1,1)$
$(0,1)$	$(1,0)$
$(1,0)$	$(0,1)$
$(1,1)$	$(0,0)$

b. The graphs are isomorphic.
c. (0, 1) and (1,0)

Exercise 12.5.2

a. Write out the operation tables for $\left[B_2^3; \vee, \wedge, -\right]$.
b. Draw the Hasse diagram for $\left[B_2^3; \vee, \wedge, -\right]$

Exercise 12.5.3

a. List all atoms of B_2^4.
b. Describe the atoms of $B_2^n, n \geq 1$.

Answer

a. $(1,0,0,0),(0,1,0,0),(0,0,1,0)$,and $(0,0,0,1)$are the atoms.
b. The n-tuples of bits with exactly one 1.

Exercise 12.5.4

Theorem 13.4.2 tells us we can think of any finite Boolean algebra in terms of sets. In Chapter 4, we defined minsets Definition 4.3.1 and minset normal form Definition 4.3.2. Rephrase these definitions in the language of Boolean algebra. The generalization of minsets are called ***minterms***.

12.6: Boolean Expressions

In this section, we will use our background from the previous sections and set theory to develop a procedure for simplifying Boolean expressions. This procedure has considerable application to the simplification of circuits in switching theory or logical design.

Definition 12.6.1: Boolean Expression

Let $[B; \vee, \wedge, -]$ be any Boolean algebra, and let $x_1, x_2, \ldots, x_k$ be variables in B; that is, variables that can assume values from B. A Boolean expression generated by $x_1, x_2, \ldots, x_k$ is any valid combination of the x_i and the elements of B with the operations of meet, join, and complementation.

This definition is the analog of the definition of a proposition generated by a set of propositions, presented in Section 3.2.

Each Boolean expression generated by k variables, $e(x_1, \ldots, x_k)$, defines a function $f : B^k \to B$ where $f(a_1, \ldots, a_k) = e(a_1, \ldots, a_k)$. If B is a finite Boolean algebra, then there are a finite number of functions from B^k into B. Those functions that are defined in terms of Boolean expressions are called Boolean functions. As we will see, there is an infinite number of Boolean expressions that define each Boolean function. Naturally, the "shortest" of these expressions will be preferred. Since electronic circuits can be described as Boolean functions with $B = B_2$, this economization is quite useful.

In what follows, we make use of Exercise 7.1.5 in Section 7.1 for counting number of functions.

Example 12.6.1: Two Variables Over B_2

Consider any Boolean algebra of order 2, $[B; \vee, \wedge, -]$. How many functions $f : B^2 \to B$ are there? First, all Boolean algebras of order 2 are isomorphic to $[B_2; \vee, \wedge, -]$ so we want to determine the number of functions $f : B_2^2 \to B_2$. If we consider a Boolean function of two variables, x_1 and x_2, we note that each variable has two possible values 0 and 1, so there are 2^2 ways of assigning these two values to the $k = 2$ variables. Hence, the table below has $2^2 = 4$ rows. So far we have a table such as this one:

x_1	x_2	$f(x_1, x_2)$
0	0	?
0	1	?
1	0	?
1	1	?

How many possible different functions can there be? To list a few: $f_1(x_1, x_2) = x_1$, $f_2(x_1, x_2) = x_2$, $f_3(x_1, x_2) = x_1 \vee x_2$, $f_4(x_1, x_2) = (x_1 \wedge \overline{x_2}) \vee x_2$, $f_5(x_1, x_2) = x_1 \wedge x_2 \vee \overline{x_2}$, etc. Each of these will fill in the question marks in the table above. The tables for f_1 and f_3 are

x_1	x_2	$f_1(x_1, x_2)$
0	0	0
0	1	0
1	0	1
1	1	1

x_1	x_2	$f_3(x_1, x_2)$
0	0	0
0	1	1
1	0	1
1	1	1

Two functions are different if and only if their tables are different for at least one row. Of course by using the basic laws of Boolean algebra we can see that $f_3 = f_4$. Why? So if we simply list by brute force all "combinations" of x_1 and x_2 we will obtain unnecessary duplication. However, we note that for any combination of the variables x_1, and x_2 there are only two possible values for $f(x_1, x_2)$, namely 0 or 1. Thus, we could write $2^4 = 16$ different functions on 2 variables.

Now, let's count the number of different Boolean functions in a more general setting. We will consider two cases: first, when $B = B_2$, and second, when B is any finite Boolean algebra with 2^n elements.

Let $B = B_2$. Each function $f : B^k \to B$ is defined in terms of a table having 2^k rows. Therefore, since there are two possible images for each element of B^k, there are 2 raised to the 2^k, or 2^{2^k} different functions. We will show that every one of these

functions is a Boolean function.

Now suppose that $|B| = 2^n > 2$. A function from B^k into B can still be defined in terms of a table. There are $|B|^k$ rows to each table and $|B|$ possible images for each row. Therefore, there are 2^n raised to the power 2^{nk} different functions. We will show that if $n > 1$, not every one of these functions is a Boolean function.

Since all Boolean algebras are isomorphic to a Boolean algebra of sets, the analogues of statements in sets are useful in Boolean algebras.

Definition 12.6.2: Minterm

A Boolean expression generated by $x_1, x_2, \ldots, x_k$ that has the form

$$\bigwedge_{i=1}^{k} y_i,$$

where each y_i may be either x_i or $\overline{x_i}$ is called a minterm generated by $x_1, x_2, \ldots, x_k$. We use the notation $M_{\delta_1 \delta_2 \cdots \delta_k}$ for the minterm generated by $x_1, x_2, \ldots, x_k$, where $y_i = x_i$ if $\delta_i = 1$ and $y_i = \bar{x}_i$ if $\delta_i = 0$

An example of the notation is that $M_{110} = x_1 \wedge x_2 \wedge \bar{x_3}$.

By a direct application of the Rule of Products we see that there are 2^k different minterms generated by $x_1, \ldots, x_k$.

Definition 12.6.3: Minterm Normal Form

A Boolean expression generated by $x_1, \ldots, x_k$ is in minterm normal form if it is the join of expressions of the form $a \wedge m$, where $a \in B$ and m is a minterm generated by $x_1, \ldots, x_k$. That is, it is of the form

$$\bigvee_{j=1}^{p} (a_j \wedge m_j) \tag{12.6.1}$$

where $p = 2^k$, and $m_1, m_2, \ldots, m_p$ are the minterms generated by $x_1, \ldots, x_k$.

Note 12.6.1

- We seem to require every minterm generated by $x_1, \ldots, x_k$, in (12.6.1), and we really do. However, some of the values of a_j can be $\mathbf{0}$, which effectively makes the corresponding minterm disappear.
- If $B = B_2$, then each a_j in a minterm normal form is either 0 or 1. Therefore, $a_j \wedge m_j$ is either 0 or m_j.

Theorem 12.6.1: Uniqueness of Minterm Normal Form

Let $e(x_1, \ldots, x_k)$ be a Boolean expression over B. There exists a unique minterm normal form $M(x_1, \ldots, x_k)$ that is equivalent to $e(x_1, \ldots, x_k)$ in the sense that e and M define the same function from B^k into B.

The uniqueness in this theorem does not include the possible ordering of the minterms in M (commonly referred to as "uniqueness up to the order of minterms"). The proof of this theorem would be quite lengthy, and not very instructive, so we will leave it to the interested reader to attempt. The implications of the theorem are very interesting, however.

If $|B| = 2^n$, then there are 2^n raised to the 2^k different minterm normal forms. Since each different minterm normal form defines a different function, there are a like number of Boolean functions from B^k into B. If $B = B_2$, there are as many Boolean functions (2 raised to the 2^k) as there are functions from B^k into B, since there are 2 raised to the 2^n functions from B^k into B. The significance of this result is that any desired function can be realized using electronic circuits having 0 or 1 (off or on, positive or negative) values.

More complex, multivalued circuits corresponding to boolean algebras with more than two values would not have this flexibility because of the number of minterm normal forms, and hence the number of boolean functions, is strictly less than the number of functions.

We will close this section by examining minterm normal forms for expressions over B_2 , since they are a starting point for circuit economization.

Example 12.6.2

Consider the Boolean expression $f(x_1, x_2) = x_1 \vee \overline{x_2}$. One method of determining the minterm normal form of f is to think in terms of sets. Consider the diagram with the usual translation of notation in Figure 12.6.1. Then

$$\begin{aligned} f(x_1, x_2) &= (\overline{x_1} \wedge \overline{x_2}) \vee (x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2) \\ &= M_{00} \vee M_{10} \vee M_{11} \end{aligned}$$

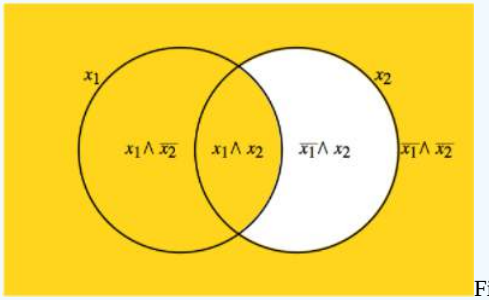


Figure 12.6.1: Visualization of minterms for $x_1 \vee \bar{x_2}$

Table 12.6.1: Definition of the boolean function g

x_1	x_2	x_3	$g(x_1, x_2, x_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

Example 12.6.3

Consider the function $g : B_2^3 \to B_2$ defined by Table 12.6.1.

The minterm normal form for g can be obtained by taking the join of minterms that correspond to rows that have an image value of 1. If $g(a_1, a_2, a_3) = 1$, then include the minterm $y_1 \wedge y_2 \wedge y_3$ where

$$y_j = \begin{cases} x_j & \text{if } a_j = 1 \\ \bar{x_j} & \text{if } a_j = 0 \end{cases}$$

Or, to use alternate notation, include $M_{a_1 a_2 a_3}$ in the expression if and only if $g(a_1, a_2, a_3) = 1$

Therefore,

$$g(x_1, x_2, x_3) = (\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}) \vee (\overline{x_1} \wedge x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \overline{x_3}).$$

The minterm normal form is a first step in obtaining an economical way of expressing a given Boolean function. For functions of more than three variables, the above set theory approach tends to be awkward. Other procedures are used to write the normal form. The most convenient is the Karnaugh map, a discussion of which can be found in any logical design/switching theory text (see, for example, [18]), on Wikipedia.

12.6.1: Exercises

Exercise 12.6.1

a. Write the 16 possible functions of Example 12.6.1.
b. Write out the tables of several of the above Boolean functions to show that they are indeed different.
c. Determine the minterm normal forms of

i. $g_1(x_1, x_2) = x_1 \vee x_2$,
ii. $g_2(x_1, x_2) = \overline{x_1} \vee \overline{x_2}$
iii. $g_3(x_1, x_2) = \overline{x_1 \wedge x_2}$
iv. $g_4(x_1, x_2) = 1$

Answer

a.

$f_1(x_1, x_2) = 0$
$f_2(x_1, x_2) = (\overline{x_1} \wedge \overline{x_2})$
$f_3(x_1, x_2) = (\overline{x_1} \wedge x_2)$
$f_4(x_1, x_2) = (x_1 \wedge \overline{x_2})$
$f_5(x_1, x_2) = (x_1 \wedge x_2)$
$f_6(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2)) = \overline{x_1}$
$f_7(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (x_1 \wedge \overline{x_2})) = \overline{x_2}$
$f_8(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = ((x_1 \wedge x_2) \vee (\overline{x_1} \wedge \overline{x_2}))$
$f_9(x_1, x_2) = ((\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})) = ((x_1 \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2))$
$f_{10}(x_1, x_2) = ((\overline{x_1} \wedge x_2) \vee (x_1 \wedge x_2)) = x_2$
$f_{11}(x_1, x_2) = ((x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = x_1$
$f_{12}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})) = (\overline{x_1} \vee \overline{x_2})$
$f_{13}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2) \vee (x_1 \wedge x_2)) = (\overline{x_1} \vee x_2)$
$f_{14}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = (x_1 \vee \overline{x_2})$
$f_{15}(x_1, x_2) = ((\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = (x_1 \vee x_2)$
$f_{16}(x_1, x_2) = ((\overline{x_1} \wedge \overline{x_2}) \vee (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2)) = 1$

b. The truth table for the functions in part (a) are

x_1	x_2	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
0	0	0	1	0	0	0	1	1	1
0	1	0	0	1	0	0	1	0	0
1	0	0	0	0	1	0	0	1	0
1	1	0	0	0	0	1	0	0	1

x_1	x_2	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	1	1	1	0	1
0	1	1	1	0	1	1	0	1	1
1	0	1	0	1	1	0	1	1	1
1	1	0	1	1	0	1	1	1	1

c.

i. $g_1(x_1, x_2) = f_{15}(x_1, x_2)$
ii. $g_2(x_1, x_2) = f_{12}(x_1, x_2)$
iii. $g_3(x_1, x_2) = f_{12}(x_1, x_2)$
iv. $g_4(x_1, x_2) = f_{16}(x_1, x_2)$

Exercise 12.6.2

Consider the Boolean expression $f(x_1, x_2, x_3) = (\overline{x_3} \wedge x_2) \vee (\overline{x_1} \wedge x_3) \vee (x_2 \wedge x_3)$ on $\left[B_2^3; \vee, \wedge, -\right]$.

a. Simplify this expression using basic Boolean algebra laws.
b. Write this expression in minterm normal form.
c. Write out the table for the given function defined by f and compare it to the tables of the functions in parts a and b.
d. How many possible different functions in three variables on $[B_2; \vee, \wedge, -]$ are there?

Exercise 12.6.3

Let $[B; \vee, \wedge, -]$ be a Boolean algebra of order 4, and let f be a Boolean function of two variables on B.

a. How many elements are there in the domain of f?
b. How many different Boolean functions are there of two, variables? Three variables?
c. Determine the minterm normal form of $f(x_1, x_2) = x_1 \vee x_2$.
d. If $B = \{0, a, b, 1\}$, define a function from B^2 into B that is not a Boolean function.

Answer

a. The number of elements in the domain of f is $16 = 4^2 = |B|^2$
b. With two variables, there are $4^3 = 256$ different Boolean functions. With three variables, there are $4^8 = 65536$ different Boolean functions.
c. $f(x_1,\ x_2) = (1 \wedge \overline{x_1} \wedge \overline{x_2}) \vee (1 \wedge \overline{x_1} \wedge \overline{x_2}) \vee (1 \wedge x1 \wedge \overline{x_2}) \vee (0 \wedge x1 \wedge x2)$
d. Consider $f : B^2 \to B$, defined by $f(0,0) = 0$, $f(0,1) = 1$, $f(1,0) = a$, $f(1,1) = a$, and $f(0,a) = b$, with the images of all other pairs in B^2 defined arbitrarily. This function is not a Boolean function. If we assume that it is Boolean function then f can be computed with a Boolean expression $M(x_1, x_2)$. This expression can be put into minterm normal form:

$$M(x_1, x_2) = (c_1 \wedge \overline{x_1} \wedge \overline{x_2}) \vee (c_2 \wedge \overline{x_1} \wedge x_2) \vee (c_3 \wedge x_1 \wedge \overline{x_2}) \vee (c_4 \wedge x_1 \wedge x_2)$$

$$\begin{aligned} f(0,0) &= 0 \Rightarrow M(0,0) = 0 \Rightarrow c_1 = 0 \\ f(0,1) &= 1 \Rightarrow M(0,0) = 1 \Rightarrow c_2 = 1 \\ f(1,0) &= a \Rightarrow M(0,0) = a \Rightarrow c_3 = a \\ f(1,1) &= a \Rightarrow M(0,0) = a \Rightarrow c_4 = a \end{aligned}$$

Therefore, $M(x_1, x_2) = (\overline{x_1} \wedge x_2) \vee (a \wedge x_1 \wedge \overline{x_2}) \vee (a \wedge x_1 \wedge x_2)$ and so, using this formula,
$M(0, a) = (\overline{0} \wedge a) \vee (a \wedge 0 \wedge \overline{a}) \vee (a \wedge 0 \wedge a) = a$ This contradicts $f(0, a) = b$, and so f is not a Boolean function.

12.7: A Brief Introduction to Switching Theory and Logic Design

Disclaimer

I'm still looking for a good application for drawing logic gates. The figures here are quite rough.

Early computers relied on many switches to perform the logical operations needed for computation. This was true as late as the 1970's when early personal computers such as the Altair (Figure 12.7.1) started to appear. Pioneering computer scientists such as Claude Shannon realized that the operation of these computers could be simplified by making use of an isomorphism between computer circuits and boolean algebra. The term ***Switching Theory*** was used at the time. Logical gates realized through increasingly smaller and smaller integrated circuits still perform the same functions as in early computers, but using purely electronic means. In this section, we give examples of some switching circuits. Soon afterward, we will transition to the more modern form of circuits that are studied in ***Logic Design***, where gates replace switches. Our main goal is to give you an overview of how boolean functions corresponds to any such circuit. We will introduce the common system notation used in logic design and show how it corresponds with the mathematical notation of Boolean algebras. Any computer scientist should be familiar with both systems.

Figure 12.7.1: The Altair Computer, an early PC, by Todd Dailey, Creative Commons

The simplest switching device is the on-off switch. If the switch is closed/ON, current will pass through it; if it is open/OFF, current will not pass through it. If we designate ON by 1, and OFF by 0, we can describe electrical circuits containing switches by Boolean expressions with the variables representing the variable states of switches or the variable bits passing through gates.

The electronics involved in these switches take into account whether we are negating a switch or not. For electromagnetic switches, a magnet is used to control whether the switch is open or closed. The magnets themselves may be controlled by simple ON/OFF switches. There are two types of electromagnetic switches. One is normally open (OFF) when the magnet is not activated, but activating the magnet will close the circuit and the switch is then ON. A separate type of switch corresponds with a negated switch. For that type, the switch is closed when the magnet is not activated, and when the magnet is activated, the switch opens. We won't be overly concerned with the details of these switches or the electronics corresponding to logical gates. We will simply assume they are available to plug into a circuit. For simplicity, we use the inversion symbol on a variable that labels a switch to indicate that it is a switch of the second type, as in Figure 12.7.3

Note 12.7.1

Standby power generators that many people have in their homes use a transfer switch to connect the generator to the home power system. This switch is open (OFF) if there is power coming from the normal municipal power supply. It stays OFF because a magnet is keeping it open. When power is lost, the magnet is no longer activated, and the switch closes and is ON. So the transfer switch is a normally ON switch.

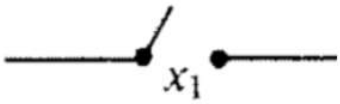


Figure 12.7.2: Representation of a normally OFF switch controlled by variable x_1

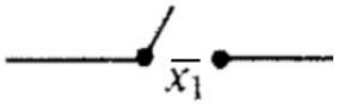


Figure 12.7.3: Representation of a normally ON switch controlled by variable x_1

The standard notation used for Boolean algebra operations in switching theory and logic design is $+$ for join, instead of $\vee$; and $\cdot$ for meet, instead of $\wedge$. Complementation is the same in both notational systems, denoted with an overline.

The expression $x_1 \cdot x_2$ represents the situation in which a series of two switches appears in sequence as in Figure 12.7.4 In order for current to flow through the circuit, both switches must be ON; that is, they must both have the value 1. Similarly, a pair of parallel switches, as in Figure 12.7.5, is described algebraically by $x_1 + x_2$. Here, current flows through this part of the circuit as long as at least on of the switches is ON.

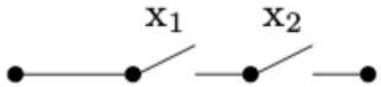


Figure 12.7.4: Two switches in AND configuration realizing $x_1 \cdot x_2$

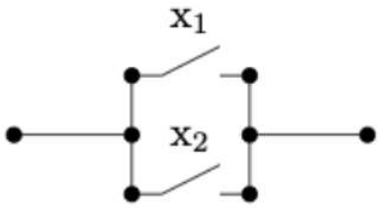


Figure 12.7.5: Two switches in OR configuration realizing $x_1 + x_2$

All laws and concepts developed previously for Boolean algebras hold. The only change is purely notational. We make the change in this section solely to introduce the reader to another frequently used system of notation.

Many of the laws of Boolean algebra can be visualized thought switching theory. For example, the distributive law of meet over join is expressed as

$$x_1 \cdot (x_2 + x_3) = x_1 \cdot x_2 + x_1 \cdot x_3.$$

The switching circuit analogue of the above statement is that the circuits in the two images below are equivalent. In circuit (b), the presence of two x_1's might represent two electromagnetic switches controlled by the same magnet.

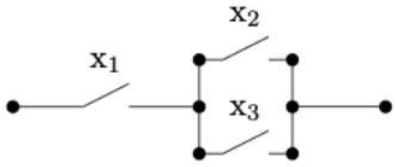


Figure 12.7.6: (a)

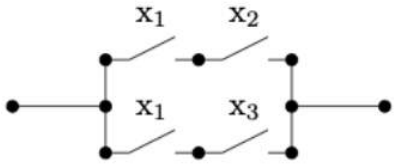


Figure 12.7.7: (b)

The circuits in a computer are now composed of large quantities of gates, which serve the same purpose as switches, but can be miniaturized to a great degree. For example, the OR gate, usually drawn as in Figure 12.7.8 implements the logical OR function. This happens electronically, but is equivalent to Figure 12.7.5. The AND gate, which is equivalent to two sequential switches is shown in Figure 12.7.8

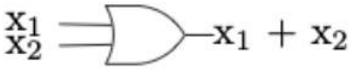


Figure 12.7.8: An OR gate

Figure 12.7.9: An AND gate

The complementation process is represented in a gate diagram by an inverter, as pictured in Figure 12.7.10

Figure 12.7.10: Inverter, or NOT gate

When drawing more complex circuits, multiple AND's or OR's are sometimes depicted using a more general gate drawing. For example if we want to depict an OR gate with three inputs that is ON as long as at least one input is ON, we would draw it as in Figure 12.7.11, although this would really be two binary gates, as in Figure 12.7.12 Both diagrams are realizing the boolean expression $x_1 + x_2 + x_3$. Strictly speaking, the gates in Figure 12.7.12represent $(x_1 + x_2) + x_3$, but the associative law for join tells us that the grouping doesn't matter.

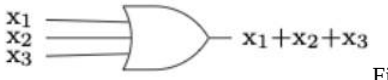


Figure 12.7.11: Simple version of a ternary OR gate

Figure 12.7.12: A ternary OR gate created with binary OR gates

In Figure 12.7.13, we show a few other commonly used gates, XOR, NAND, and NOR, which correspond to the boolean exressions $x_1 \oplus x_2$, $\overline{x_1 \cdot x_2}$, and $\overline{x_1 + x_2}$, respectively.

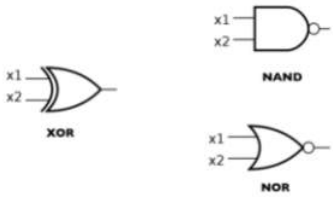


Figure 12.7.13: Other common gates

Let's start with a logic circuit and see how the laws of boolean algebra can help us simplify it.

Example 12.7.1: Simplification of a Circuit

Consider the circuit in Figure 12.7.14 As usual, we assume that three inputs enter on the left and the output exits on the right.

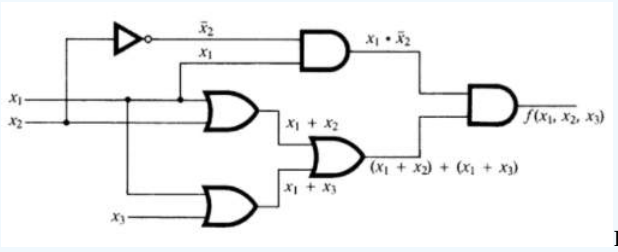


Figure 12.7.14: Initial gate diagram

If we trace the inputs through the gates we see that this circuit realizes the boolean function

$$f(x_1, x_2, x_3) = x_1 \cdot \overline{x_2} \cdot ((x_1 + x_2) + (x_1 + x_3)).$$

We simplify the boolean expression that defines f, simplifying the circuit in so doing. You should be able to identify the laws of Boolean algebra that are used in each of the steps. See Exercise 12.7.1.

$$\begin{aligned} x_1 \cdot \overline{x_2} \cdot ((x_1 + x_2) + (x_1 + x_3)) &= x_1 \cdot \overline{x_2} \cdot (x_1 + x_2 + x_3) \\ &= x_1 \cdot \overline{x_2} \cdot x_1 + x_1 \cdot \overline{x_2} \cdot x_2 + x_1 \cdot \overline{x_2} \cdot x_3 \\ &= x_1 \cdot \overline{x_2} + 0 \cdot x_1 + x_3 \cdot x_1 \cdot \overline{x_2} \\ &= x_1 \cdot \overline{x_2} + x_3 \cdot x_1 \cdot \overline{x_2} \\ &= x_1 \cdot \overline{x_2} \cdot (1 + x_3) \\ &= x_1 \cdot \overline{x_2} \end{aligned}$$

Therefore, $f(x_1, x_2, x_3) = x_1 \cdot \overline{x_2}$, which can be realized with the much simpler circuit in Figure 12.7.15 without using the input x_3.

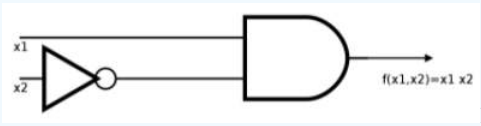


Figure 12.7.15: Simplified gate diagram

Next, we start with a table of desired outputs based on three bits of input and design an efficient circuit to realize this output.

Example 12.7.2

Consider the following table of desired outputs for the three input bits x_1, x_2, x_3.

Table 12.7.1: Desired output table

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

The first step is to write the Minterm Normal Form, Definition 13.6.3, of f. Since we are working with the two value Boolean algebra, B_2, the constants in each minterm are either 0 or 1, and we simply list the minterms that have a 1. These correspond with the rows of the table above that have an output of 1. We will then attempt to simplify the expression as much as possible.

$$\begin{aligned} f(x_1, x_2, x_3) &= (\overline{x_1} \cdot \overline{x_2} \cdot x_3) + (x_1 \cdot \overline{x_2} \cdot \overline{x_3}) + (x_1 \cdot \overline{x_2} \cdot x_3) \\ &= \overline{x_2} \cdot ((\overline{x_1} \cdot x_3) + (x_1 \cdot \overline{x_3}) + (x_1 \cdot x_3)) \\ &= \overline{x_2} \cdot ((\overline{x_1} \cdot x_3) + x_1 \cdot (\overline{x_3} + x_3)) \\ &= \overline{x_2} \cdot ((\overline{x_1} \cdot x_3) + x_1) \end{aligned}$$

Therefore we can realize our table with the boolean function $f(x_1, x_2, x_3) = \overline{x_2} \cdot ((\overline{x_1} \cdot x_3) + x_1)$. A circuit diagram for this function is Figure 12.7.16 But is this the simplest circuit that realizes the table? See Exercise 12.7.3

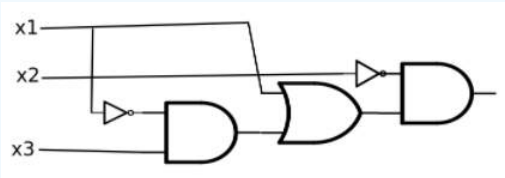


Figure 12.7.16: A realization of the table of desired outputs.

12.7.1: 13.7.1: Exercises

Exercise 12.7.1

List the laws of boolean algebra that justify the steps in the simplification of the boolean function $f(x_1, x_2, x_3)$ in Example 12.7.1. Some steps use more than one law.

Answer

1. Associative, commutative, and idempotent laws.
2. Distributive law.
3. Idempotent and complement laws.
4. Null and identity laws
5. Distributive law.
6. Null and identity laws.

Exercise 12.7.2

Write the following Boolean expression in the notation of logic design.

$$(x_1 \wedge \overline{x_2}) \vee (x_1 \wedge x_2) \vee (\overline{x_1} \wedge x_2)\,.$$

Answer

$$(x_1 \cdot \overline{x_2}) + (x_1 \cdot x_2) + (\overline{x_1} \cdot x_2).$$

Exercise 12.7.3

Find a further simplification of the boolean function in Example 12.7.2, and draw the corresponding gate diagram for the circuit that it realizes.

Answer

A simpler boolean expression for the function is $\overline{x_2} \cdot (x_1 + x_3)$.

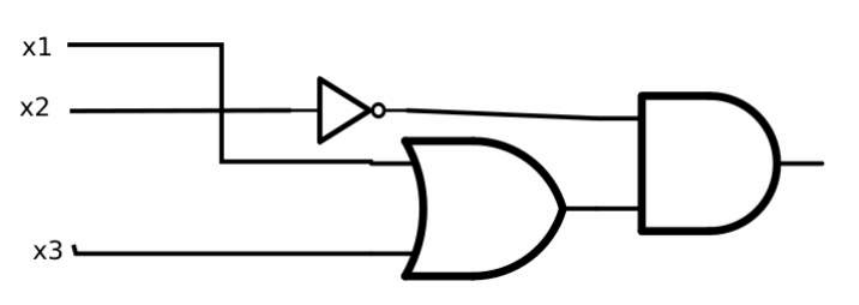


Figure 12.7.17: An even simpler circuit

Exercise 12.7.4

Consider the switching circuit in Figure 12.7.18

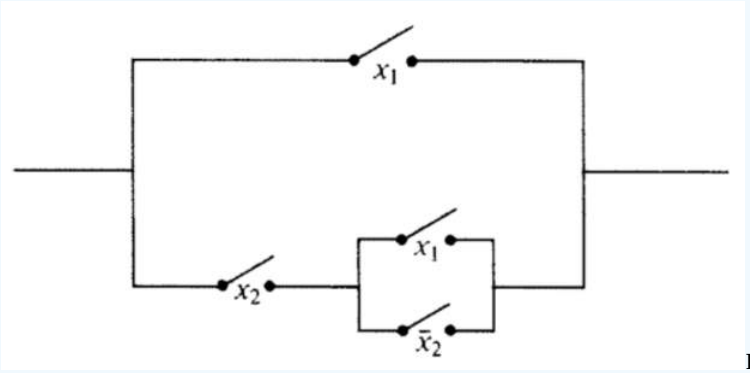


Figure 12.7.18: Can this circuit be simplified?

a. Draw the corresponding gate diagram for this circuit.
b. Construct a table of outputs for each of the eight inputs to this circuit.
c. Determine the minterm normal of the Boolean function based on the table.
d. Simplify the circuit as much as possible.

Exercise 12.7.5

Consider the circuit in Figure 12.7.19

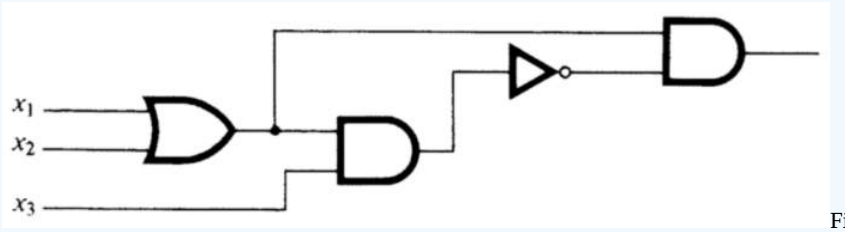


Figure 12.7.19: Can this circuit be simplified?

a. Trace the inputs though this circuit and determine the Boolean function that it realizes.
b. Construct a table of outputs for each of the eight inputs to this circuit.
c. Find the minterm normal form of f.
d. Draw the circuit based on the minterm normal form.
e. Simplify the circuit algebraically and draw the resulting circuit.

Exercise 12.7.6

Consider the Boolean function $f(x_1, x_2, x_3, x_4) = x_1 + (x_2 \cdot (\overline{x_1} + x_4) + x_3 \cdot (\overline{x_2} + \overline{x_4}))$.

a. Simplify f algebraically.
b. Draw the gate diagram based on the simplified version of f.

Exercise 12.7.7

Draw a logic circuit using only AND, OR and NOT gates that realizes an XOR gate.

Exercise 12.7.8

Draw a logic circuit using only AND, OR and NOT gates that realizes the Boolean function on three variables that returns 1 if the majority of inputs are 1 and 0 otherwise.

CHAPTER OVERVIEW

13: Monoids and Automata

The first topic is monoid theory. The second is automata theory, in which computers and other machines are described in abstract terms.

13.1: Monoids

Recall that in Section 11.2 we introduced systems called monoids. Here is the formal definition.

Definition 13.1.1: Monoid

A monoid is a set M together with a binary operation $*$ with the properties

- $*$ is associative: $\forall a, b, c \in M,\ (a * b) * c = a * (b * c)$ and
- $*$ has an identity in M: $\exists e \in M$ such that $\forall a \in M,\ a * e = e * a = a$

Note 13.1.1

Since the requirements for a group contain the requirements for a monoid, every group is a monoid.

Example 13.1.1: Some Monoids

a. The power set of any set together with any one of the operations intersection, union, or symmetric difference is a monoid.
b. The set of integers, $\mathbb{Z}$, with multiplication, is a monoid. With addition, $\mathbb{Z}$ is also a monoid.
c. The set of $n \times n$ matrices over the integers, $M_n(\mathbb{Z})$, $n \geq 2$, with matrix multiplication, is a monoid. This follows from the fact that matrix multiplication is associative and has an identity, I_n. This is an example of a noncommutative monoid since there are matrices, A and B, for which $AB \neq BA$.
d. $[\mathbb{Z}_n; \times_n]$, $n \geqslant 2$, is a monoid with identity 1.
e. Let X be a nonempty set. The set of all functions from X into X, often denoted X^X, is a monoid over function composition. In Chapter 7, we saw that function composition is associative. The function $i : X \to X$ defined by $i(a) = a$ is the identity element for this system. If $|X|$ is greater than 1 then it is a noncommutative monoid. If X is finite, $|X^X| = |X|^{|X|}$. For example, if $B = \{0, 1\}$, $|B^B| = 4$. The functions $z, u, i,$ and t, defined by the graphs in Figure 13.1.1, are the elements of B^B. This monoid is not a group. Do you know why?
One reason why B^B is noncommutative is that $t \circ z \neq z \circ t$ because $(t \circ z)(0) = t(z(0)) = t(0) = 1$ while $(z \circ t)(0) = z(t(0)) = z(1) = 0$.

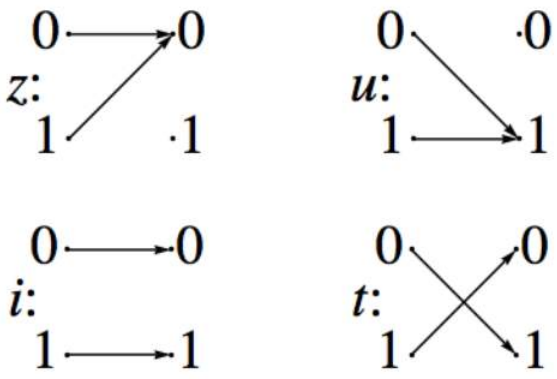


Figure 13.1.1: The functions on B_2

Virtually all of the group concepts that were discussed in Chapter 11 are applicable to monoids. When we introduced subsystems, we saw that a submonoid of monoid M is a subset of M; that is, it is a monoid with the operation of M. To prove that a subset is a submonoid, you can apply the following theorem.

Theorem 13.1.1: Submonoid Test

Assume $[M; *]$ is a monoid and K is a nonempty subset of M. Then K is a submonoid of M if and only if the following two conditions are met.

- If $a, b \in K$, then. $a * b \in K$; i. e., K is closed with under $*$.
- The identity of M belongs to K.

Often we will want to discuss the smallest submonoid that includes a certain subset S of a monoid M. This submonoid can be defined recursively by the following definition.

Definition 13.1.2: Submonoid Generated by a Set

If S is a subset of monoid $[M;*]$, the submonoid generated by S, $\langle S\rangle$, is defined by:.

a. (Basis) The identity of M belongs to $\langle S\rangle$; and $a\in S\Rightarrow a\in\langle S\rangle$.
b. (Recursion) $a,b\in\langle S\rangle\Rightarrow a*b\in\langle S\rangle$.

Note 13.1.2

If $S=\{a_1,a_2,\ldots,a_n\}$, we write $\langle a_1,a_2,\ldots,a_n\rangle$ in place of $\langle\{a_1,a_2,\ldots,a_n\}\rangle$.

Example 13.1.2: Some Submonoids

a. One example of a submonoid of $[\mathbb{Z};+]$ is $\langle 2\rangle=\{0,2,4,6,8,\ldots\}$.
b. The power set of $\mathbb{Z}$, $\mathcal{P}(\mathbb{Z})$, over union is a monoid with identity $\emptyset$. If $S=\{\{1\},\{2\},\{3\}\}$,then $\langle S\rangle$ is the power set of $\{1,2,3\}$.If $S=\{\{n\}:n\in\mathbb{Z}\}$, then $\langle S\rangle$ is the set of finite subsets of the integers.

As you might expect, two monoids are isomorphic if and only if there exists a translation rule between them so that any true proposition in one monoid is translated to a true proposition in the other.

Example 13.1.3

$M=[\mathcal{P}\{1,2,3\};\cap]$ is isomorphic to $M_2=\left[\mathbb{Z}_2^3;\cdot\right]$, where the operation in M_2 is componentwise mod 2 multiplication. A translation rule is that if $A\subseteq\{1,2,3\}$, then it is translated to (d_1,d_2,d_3) where

$$d_i=\begin{cases}1 & \text{if } i\in A\\ 0 & \text{if } i\notin A\end{cases}$$

Two cases of how this translation rule works are:

$$\begin{array}{ccc}\{1,2,3\} & \text{is the identity for } M_1 & \{1,2\}\cap\{2,3\}=\{2\}\\ \updownarrow & & \updownarrow\\ (1,1,1) & \text{is the identity for } M_2 & (1,1,0)\cdot(0,1,1)=(0,1,0)\end{array}.$$

A more precise definition of a monoid isomorphism is identical to the definition of a group isomorphism, Definition 11.7.2.

13.1.1: Exercises

Exercise 13.1.1

For each of the subsets of the indicated monoid, determine whether the subset is a submonoid.

a. $S_1=\{0,2,4,6\}$ and $S_2=\{1,3,5,7\}$ in $[\mathbb{Z}_8;\times_8]$.
b. $\{f\in\mathbb{N}^{\mathbb{N}}:f(n)\leqslant n,\forall n\in\mathbb{N}\}$ and $\left\{f\in\mathbb{N}^{\mathbb{N}}:f(1)=2\right\}$ in the monoid $[\mathbb{N}^{\mathbb{N}};\circ]$.
c. $\{A\subseteq\mathbb{Z}\mid A\text{ is finite}\}$ and $\{A\subseteq\mathbb{Z}\mid A^c\text{ is finite}\}$ in $[\mathcal{P}(\mathbb{Z});\cup]$.

Answer

1. S_1 is not a submonoid since the identity of $[\mathbb{Z}_8;\times_8]$,which is 1, is not in S_1. S_2 is a submonoid since $1\in S_2$ and S_2 is closed under multiplication; that is, for all $a,b\in S_2$, $a\times_8 b$ is in S_2.
2. The identity of $\mathbb{N}^{\mathbb{N}}$ is the identity function $i:\mathbb{N}\to\mathbb{N}$ defined by $i(a)=a,\ \forall a\in\mathbb{N}$. If $a\in\mathbb{N}$, $i(a)=a\leq a$, thus the identity of $\mathbb{N}^{\mathbb{N}}$ is in S_1. However, the image of 1 under any function in S_2 is 2, and thus the identity of $\mathbb{N}^{\mathbb{N}}$ is not in S_2, so S_2 is not a submonoid. The composition of any two functions in S_1, f and g, will be a function in S_1:

$$\begin{aligned}(f \circ g)(n) &= f(g(n)) \leq g(n) \text{ since } f \text{ is in } S_1 \\ &\leq n \text{ since } g \text{ is in } S_1 \Rightarrow f \circ g \in S_1\end{aligned}$$

and the two conditions of a submonoid are satisfied and S_1 is a submonoid of $\mathbb{N}^{\mathbb{N}}$.

3. The first set is a submonoid, but the second is not since the null set has a non-finite complement.

Exercise 13.1.2

For each subset, describe the submonoid that it generates.

a. $\{3\}$ in $[\mathbb{Z}_{12}; \times_{12}]$
b. $\{5\}$ in $[\mathbb{Z}_{25}; \times_{25}]$
c. the set of prime numbers in $[\mathbb{P}; \cdot]$
d. $\{3, 5\}$ in $[\mathbb{N}; +]$

Exercise 13.1.3

$n \times n$ matrix of real numbers is called ***stochastic*** if and only if each entry is nonnegative and the sum of entries in each column is 1. Prove that the set of stochastic matrices is a monoid over matrix multiplication.

Answer

The set of $n \times n$ real matrices is a monoid under matrix multiplication. This follows from the laws of matrix algebra in Chapter 5. To prove that the set of stochastic matrices is a monoid over matrix multiplication, we need only show that the identity matrix is stochastic (this is obvious) and that the set of stochastic matrices is closed under matrix multiplication. Let A and B be $n \times n$ stochastic matrices.

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

The sum of the j^{th} column is

$$\begin{aligned}\sum_{j=1}^{n} (AB)_{ij} &= \sum_{k=1}^{n} a_{1k} b_{kj} + \sum_{k=1}^{n} a_{1k} b_{kj} + \cdots + \sum_{k=1}^{n} a_{nk} b_{kj} \\ &= \sum_{k=1}^{n} (a_{1k} b_{kj} + a_{1k} b_{kj} + \cdots + a_{nk} b_{kj}) \\ &= \sum_{k=1}^{n} b_{kj} (a_{1k} + a_{1k} + \cdots + a_{nk}) \\ &= \sum_{k=1}^{n} b_{kj} \quad \text{since } A \text{ is stochastic} \\ &= 1 \quad \text{since } B \text{ is stochastic}\end{aligned}$$

Exercise 13.1.4

A ***semigroup*** is an algebraic system $[S; *]$ with the only axiom that $*$ be associative on S. Prove that if S is a finite set, then there must exist an idempotent element, that is, an $a \in S$ such that $a * a = a$.

Exercise 13.1.5

Let B be a Boolean algebra and M the set of all Boolean functions on B. Let $*$ be defined on M by $(f * g)(a) = f(a) \wedge g(a)$. Prove that $[M; *]$ is a monoid. Construct the operation table of $[M; *]$ for the case of $B = B_2$.

Answer

Let $f,\ g,\ h \in M$, and $a \in B$.

$$\begin{aligned}((f*g)*h)(a) &= (f*g)(a) \wedge h(a) \\ &= (f(a) \wedge g(a)) \wedge h(a) \\ &= f(a) \wedge (g(a) \wedge h(a)) \\ &= f(a) \wedge (g*h)(a) \\ &= (f*(g*h))(a)\end{aligned}$$

Therefore $(f*g)*h = f*(g*h)$ and $*$ is associative.

The identity for $*$ is the function $u \in M$ where $u(a) = 1 =$ the "one" of B. If $a \in B$, $(f*u)(a) = f(a) \wedge u(a) = f(a) \wedge 1 = f(a)$. Therefore $f*u = f$. Similarly, $u*f = f$.

There are $2^2 = 4$ functions in M for $B = B_2$. These four functions are named in the text. See Figure 13.1.1 The table for $*$ is

$*$	z	i	t	u
z	z	z	z	z
i	z	i	z	i
t	z	z	t	t
u	z	i	t	u

13.2: Free Monoids and Languages

In this section, we will introduce the concept of a language. Languages are subsets of a certain type of monoid, the free monoid over an alphabet. After defining a free monoid, we will discuss languages and some of the basic problems relating to them. We will also discuss the common ways in which languages are defined.

Let A be a nonempty set, which we will call an alphabet. Our primary interest will be in the case where A is finite; however, A could be infinite for most of the situations that we will describe. The elements of A are called letters or symbols. Among the alphabets that we will use are $B = \{0, 1\}$, and the set of ASCII (American Standard Code for Information Interchange) characters, which we symbolize as $ASCII$.

Definition 13.2.1: Strings over an Alphabet

A string of length n, $n \geqslant 1$ over alphabet A is a sequence of n letters from A: $a_1 a_2 \ldots a_n$. The null string, λ, is defined as the string of length zero containing no letters. The set of strings of length n over A is denoted by A^n. The set of all strings over A is denoted A^*.

Note 13.2.1

a. If the length of string s is n, we write $|s| = n$.
b. The null string is not the same as the empty set, although they are similar in many ways. $A^0 = \{\lambda\}$.
c. $A^* = A^0 \cup A^1 \cup A^2 \cup A^3 \cup \cdots$ and if $i \neq j$, $A^i \cap A^j = \emptyset$; that is, $\{A^0, A^1, A^2, A^3, \ldots\}$ is a partition of A^*.
d. An element of A can appear any number of times in a string.

Theorem 13.2.1

If A is countable, then A^* is countable.

Proof

Case 1. Given the alphabet $B = \{0, 1\}$, we can define a bijection from the positive integers into B^*. Each positive integer has a binary expansion $d_k d_{k-1} \cdots d_1 d_0$, where each d_j is 0 or 1 and $d_k = 1$. If n has such a binary expansion, then $2^k \leq n \leq 2^{k+1}$. We define $f : \mathbb{P} \to B^*$ by $f(n) = f(d_k d_{k-1} \cdots d_1 d_0) = d_{k-1} \cdots d_1 d_0$, where $f(1) = \lambda$. Every one of the 2^k strings of length k are the images of exactly one of the integers between 2^k and $2^{k+1} - 1$. From its definition, f is clearly a bijection; therefore, B^* is countable.

Case 2: A is Finite. We will describe how this case is handled with an example first and then give the general proof. If $A = \{a, b, c, d, e\}$, then we can code the letters in A into strings from B^3. One of the coding schemes (there are many) is $a \leftrightarrow 000, b \leftrightarrow 001, c \leftrightarrow 010, d \leftrightarrow 011,$ and $e \leftrightarrow 100$.Now every string in A^* corresponds to a different string in B^*; for example, ace. would correspond with 000010100The cardinality of A^* is equal to the cardinality of the set of strings that can be obtained from this encoding system. The possible coded strings must be countable, since they are a subset of a countable set, B^*. Therefore, A^* is countable.

If $|A| = m$, then the letters in A can be coded using a set of fixed-length strings from B^*. If $2^{k-1} < m \leq 2^k$, then there are at least as many strings of length k in B^k as there are letters in A. Now we can associate each letter in A with with a different element of B^k. Then any string in A^*. corresponds to a string in B^*. By the same reasoning as in the example above, A^* is countable.

Case 3: A is Countably Infinite. We will leave this case as an exercise.

Definition 13.2.2: Concatenation

Let $a = a_1 a_2 \cdots a_m$ and $b = b_1 b_2 \cdots b_n$ be strings of length m and n, respectively. The concatenation of a with b, $a + b$, is the string $a_1 a_2 \cdots a_m b_1 b_2 \cdots b_n$ of length $m + n$.

There are several symbols that are used for concatenation. We chose to use the one that is also used in Python and SageMath.

```
1 'good'+'bye'
```

The set of strings over any alphabet is a monoid under concatenation.

Note 13.2.2

a. The null string is the identity element of $[A^*; +]$. Henceforth, we will denote the monoid of strings over A by A^*.
b. Concatenation is noncommutative, provided $|A| > 1$.
c. If $|A_1| = |A_2|$, then the monoids A_1^* and A_2^* are isomorphic. An isomorphism can be defined using any bijection $f : A_1 \to A_2$. If $a = a_1 a_2 \cdots a_n \in A_1^*$, $f^*(a) = (f(a_1)f(a_2) \cdots f(a_n))$ defines a bijection from A_1^* into A_2^*. We will leave it to the reader to prove that for all $a, b, \in A_1^*, f^*(a+b) = f^*(a) + f^*(b)$.

The languages of the world, English, German, Russian, Chinese, and so forth, are called natural languages. In order to communicate in writing in any one of them, you must first know the letters of the alphabet and then know how to combine the letters in meaningful ways. A formal language is an abstraction of this situation.

Definition 13.2.3: Formal Language

If A is an alphabet, a formal language over A is a subset of A^*.

Example 13.2.1: Some Formal Languages

a. English can be thought of as a language over of letters $A, B, \cdots Z$, both upper and lower case, and other special symbols, such as punctuation marks and the blank. Exactly what subset of the strings over this alphabet defines the English language is difficult to pin down exactly. This is a characteristic of natural languages that we try to avoid with formal languages.
b. The set of all ASCII stream files can be defined in terms of a language over ASCII. An ASCII stream file is a sequence of zero or more lines followed by an end-of-file symbol. A line is defined as a sequence of ASCII characters that ends with the a "new line" character. The end-of-file symbol is system-dependent.
c. The set of all syntactically correct expressions in any computer language is a language over the set of ASCII strings.
d. A few languages over B are
   - $L_1 = \{s \in B^* \mid s \text{ has exactly as many 1's as it has 0's}\}$
   - $L_2 = \{1 + s + 0 \mid s \in B^*\}$
   - $L_3 = \langle 0, 01 \rangle$ = the submonoid of B^* generated by $\{0, 01\}$.

Investigation 13.2.1: Two Fundamental Problems: Recognition and Generation

The generation and recognition problems are basic to computer programming. Given a language, L, the programmer must know how to write (or generate) a syntactically correct program that solves a problem. On the other hand, the compiler must be written to recognize whether a program contains any syntax errors.

Problem 13.2.1: The Recognition Problem

Given a formal language over alphabet A, the Recognition Problem is to design an algorithm that determines the truth of $s \in L$ in a finite number of steps for all $s \in A^*$. Any such algorithm is called a recognition algorithm.

Definition 13.2.4: Recursive Language

A language is recursive if there exists a recognition algorithm for it.

Example 13.2.2: Some Recursive Languages

a. The language of syntactically correct propositions over set of propositional variables expressions is recursive.

b. The three languages in 7(d) are all recursive. Recognition algorithms for L_1 and L_2 should be easy for you to imagine. The reason a recognition algorithm for L_3 might not be obvious is that the definition of L_3 is more cryptic. It doesn't tell us what belongs to L_3, just what can be used to create strings in L_3. This is how many languages are defined. With a second description of L_3, we can easily design a recognition algorithm. You can prove that

$$L_3 = \{s \in B^* \mid s = \lambda \text{ or } s \text{ starts with a 0 and has no consecutive 1's}\}.$$

Problem 13.2.2: The Generation Problem

Design an algorithm that generates or produces any string in L. Here we presume that A is either finite or countably infinite; hence, A^* is countable by Theorem 13.2.1, and $L \subseteq A^*$ must be countable. Therefore, the generation of L amounts to creating a list of strings in L. The list may be either finite or infinite, and you must be able to show that every string in L appears somewhere in the list.

Theorem 13.2.2: Recursive Implies Generating

a. If A is countable, then there exists a generating algorithm for A^*.
b. If L is a recursive language over a countable alphabet, then there exists a generating algorithm for L.

Proof

Part (a) follows from the fact that A^* is countable; therefore, there exists a complete list of strings in A^*.

To generate all strings of L, start with a list of all strings in A^* and an empty list, W, of strings in L. For each string s, use a recognition algorithm (one exists since L is recursive) to determine whether $s \in L$. If $s \in L$, add it to W; otherwise "throw it out." Then go to the next string in the list of A^*.

Example 13.2.3

Since all of the languages in 7(d) are recursive, they must have generating algorithms. The one given in the proof of Theorem 13.2.2 is not usually the most efficient. You could probably design more efficient generating algorithms for L_2 and L_3; however, a better generating algorithm for L_1 is not quite so obvious.

The recognition and generation problems can vary in difficulty depending on how a language is defined and what sort of algorithms we allow ourselves to use. This is not to say that the means by which a language is defined determines whether it is recursive. It just means that the truth of the statement "L is recursive" may be more difficult to determine with one definition than with another. We will close this section with a discussion of grammars, which are standard forms of definition for a language. When we restrict ourselves to only certain types of algorithms, we can affect our ability to determine whether $s \in L$ is true. In defining a recursive language, we do not restrict ourselves in any way in regard to the type of algorithm that will be used. In the next section, we will consider machines called finite automata, which can only perform simple algorithms.

One common way of defining a language is by means of a ***phrase structure grammar*** (or grammar, for short). The set of strings that can be produced using set of grammar rules is called a phrase structure language.

Example 13.2.4: Zeros Before Ones

We can define the set of all strings over B for which all 0's precede all 1's as follows. Define the starting symbol S and establish rules that S can be replaced with any of the following: λ, $0S$, or $S1$. These replacement rules are usually called production rules. They are usually written in the format $S \to \lambda$, $S \to 0S$, and $S \to S1$. Now define L to be the set of all strings that can be produced by starting with S and applying the production rules until S no longer appears. The strings in L are exactly the ones that are described above.

Definition 13.2.5: Phase Structure Grammar

A phrase structure grammar consists of four components:

1. A nonempty finite set of terminal characters, T. If the grammar is defining a language over A, T is a subset of A^*.
2. A finite set of nonterminal characters, N.
3. A starting symbol, $S \in N$.
4. A finite set of production rules, each of the form $X \to Y$, where X and Y are strings over $A \cup N$ such that $X \neq Y$ and X contains at least one nonterminal symbol.

If G is a phrase structure grammar, $L(G)$ is the set of strings that can be produced by starting with S and applying the production rules a finite number of times until no nonterminal characters remain. If a language can be defined by a phrase structure grammar, then it is called a phrase structure language.

Example 13.2.5: Alternating Bits Language

The language over B consisting of strings of alternating 0's and 1's is a phrase structure language. It can be defined by the following grammar:

1. Terminal characters: λ, 0, and 1
2. Nonterminal characters: S, T, and U
3. Starting symbol: S
4. Production rules:

$$\begin{array}{lll} S \to T & S \to U & S \to \lambda \\ S \to 0 & & S \to 1 \\ S \to 0T & & S \to 1U \\ T \to 10T & & T \to 10 \\ U \to 01U & & U \to 01 \end{array}$$

These rules can be visualized with a graph:

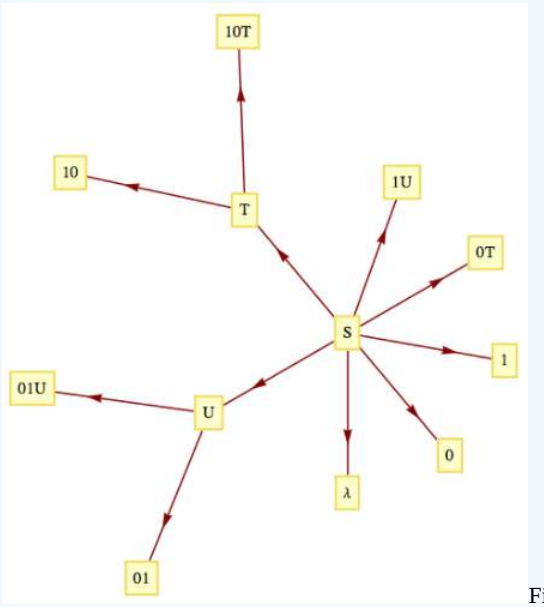


Figure 13.2.1: Production rules for the language of alternating 0's and 1's

We can verify that a string such as 10101 belongs to the language by starting with S and producing 10101 using the production rules a finite number of times: $S \to 1U \to 101U \to 10101$.

Example 13.2.6: Valid SageMath Variables

Let G be the grammar with components:

1. Terminal symbols = all letters of the alphabet (both upper and lower case), digits 0 through 9, and underscore
2. Nonterminal symbols: $\{I, X\}$,
3. Starting symbol: I
4. Production rules: $I \to \alpha$, where α is any letter, $I \to \alpha + X$ for any letter α, $X \to X + \beta$ for any letter, digit or underscore, β, and $X \to \beta$ for any letter, digit or underscore, β. There are a total of $52 + 52 + 63 + 63 = 230$ production rules for this grammar. The language $L(G)$ consists of all valid SageMath variable names.

Example 13.2.7: Backus-Naur Form

Backus-Naur form (BNF) is a popular alternate form of defining the production rules in a grammar. If the production rules $A \to B_1, A \to B_2, \ldots A \to B_n$ are part of a grammar, they would be written in BNF as $A ::= B_1 \mid B_2 \mid \cdots \mid B_n$. The symbol $\mid$ in BNF is read as "or" while the $::=$ is read as "is defined as." Additional notations of BNF are that $\{x\}$, represents zero or more repetitions of x and $[y]$ means that y is optional.

A BNF version of the production rules for a SageMath variable, I, is

$$\begin{aligned} letter &::= a \mid b \mid c \mid \cdots \mid z \mid A \mid B \mid \cdots \mid Z \\ digit &::= 0 \mid 1 \mid \cdots \mid 9 \\ I &::= letter\{letter \mid digit \mid \_\} \end{aligned}$$

Example 13.2.8: The Language of Simple Arithmetic Expressions

An arithmetic expression can be defined in BNF. For simplicity, we will consider only expressions obtained using addition and multiplication of integers. The terminal symbols are (,) , + , * , - , and the digits 0 through 9. The nonterminal symbols are E (for expression), T (term), F (factor), and N (number). The starting symbol is E. Production rules are

$$\begin{aligned} E &::= E + T \mid T \\ T &::= T * F \mid F \\ F &::= (E) \mid N \\ N &::= [-]\text{digit}\{\text{digit}\} \end{aligned} \quad .$$

One particularly simple type of phrase structure grammar is the regular grammar.

Definition 13.2.6: Regular Grammar

A regular (right-hand form) grammar is a grammar whose production rules are all of the form $A \to t$ and $A \to tB$, where A and B are nonterminal and t is terminal. A left-hand form grammar allows only $A \to t$ and $A \to Bt$. A language that has a regular phrase structure language is called a regular language.

Example 13.2.9

a. The set of Sage variable names is a regular language since the grammar by which we defined the set is a regular grammar.
b. The language of all strings for which all 0's precede all 1's (Example 13.2.4) is regular; however, the grammar by which we defined this set is not regular. Can you define these strings with a regular grammar?
c. The language of arithmetic expressions is not regular.

13.2.1: Exercises

Exercise 13.2.1

a. If a computer is being designed to operate with a character set of 350 symbols, how many bits must be reserved for each character? Assume each character will use the same number of bits.
b. Do the same for 3,500 symbols.

Answer

a. For a character set of 350 symbols, the number of bits needed for each character is the smallest n such that 2^n is greater than or equal to 350. Since $2^9 = 512 > 350 > 2^8$, 9 bits are needed,
b. $2^{12} = 4096 > 3500 > 2^{11}$; therefore, 12 bits are needed.

Exercise 13.2.2

It was pointed out in the text that the null string and the null set are different. The former is a string and the latter is a set, two different kinds of objects. Discuss how the two are similar.

Exercise 13.2.3

What sets of strings are defined by the following grammar?

a. Terminal symbols: λ , 0 and 1
b. Nonterminal symbols: S and E
c. Starting symbol: S
d. Production rules: $S \to 0S0, S \to 1S1, S \to E, E \to \lambda, E \to 0, E \to 1$

Answer

This grammar defines the set of all strings over B for which each string is a palindrome (same string if read forward or backward).

Exercise 13.2.4

What sets of strings are defined by the following grammar?

a. Terminal symbols: λ, a, b, and c
b. Nonterminal symbols: S, T, U and E
c. Starting symbol: S
d. Production rules:

$$\begin{array}{ccc} S \to aS & S \to T & T \to bT \\ T \to U & U \to cU & U \to E \\ & E \to \lambda & \end{array}$$

Exercise 13.2.5

Define the following languages over B with phrase structure grammars. Which of these languages are regular?

a. The strings with an odd number of characters.
b. The strings of length 4 or less.
c. The palindromes, strings that are the same backwards as forwards.

Answer

a. Terminal symbols: The null string, 0, and 1. Nonterminal symbols: S, E. Starting symbol: S. Production rules: $S \to 00S$, $S \to 01S$, $S \to 10S$, $S \to 11S$, $S \to E$, $E \to 0$, $E \to 1$ This is a regular grammar.

b. Terminal symbols: The null string, 0, and 1. Nonterminal symbols: S, A, B, C Starting symbol: S Production rules: $S \to 0A$, $S \to 1A$, $S \to \lambda$, $A \to 0B$, $A \to 1B$, $A \to \lambda$, $B \to 0C$, $B \to 1C$, $B \to A$, $C \to 0$, $C \to 1$, $C \to \lambda$ This is a regular grammar.
c. See Exercise 13.2.3 This language is not regular.

Exercise 13.2.6

Define the following languages over B with phrase structure grammars. Which of these languages are regular?

a. The strings with more 0's than 1's.
b. The strings with an even number of 1's.
c. The strings for which all 0's precede all 1's.

Exercise 13.2.7

Prove that if a language over A is recursive, then its complement is also recursive.

Answer

If s is in A^* and L is recursive, we can answer the question "Is s in L^c?" by negating the answer to "Is s in L?"

Exercise 13.2.8

Use BNF to define the grammars in Exercises 13.2.3and 13.2.4.

Exercise 13.2.9

a. Prove that if $X_1, X_2, \ldots$is a countable sequence of countable sets, the union of these sets, $\bigcup_{i=1}^{\infty} X_i$ is countable.
b. Using the fact that the countable union of countable sets is countable, prove that if A is countable, then A^* is countable.

Answer

a. List the elements of each set X_i in a sequence x_{i1}, x_{i2}, $x_{i3} \cdots$. Then draw arrows as shown below and list the elements of the union in order established by this pattern: x_{11}, x_{21}, x_{12}, x_{13}, x_{22}, x_{31}, x_{41}, x_{32}, x_{23}, x_{14}, $x_{15} \cdots$,
b. Each of the sets A^1, A^2, $A^3, \cdots$, are countable and A^* is the union of these sets; hence A^* is countable.

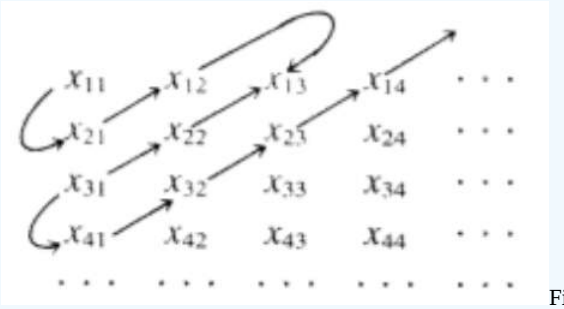


Figure 13.2.2: Exercise 13.2.9

13.3: Automata, Finite-State Machines

In this section, we will introduce the concept of an abstract machine. The machines we will examine will (in theory) be capable of performing many of the tasks associated with digital computers. One such task is solving the recognition problem for a language. We will concentrate on one class of machines, finite-state machines (finite automata). And we will see that they are precisely the machines that are capable of recognizing strings in a regular grammar.

Given an alphabet X, we will imagine a string in X^* to be encoded on a tape that we will call an input tape. When we refer to a tape, we might imagine a strip of material that is divided into segments, each of which can contain either a letter or a blank.

The typical abstract machine includes an input device, the read head, which is capable of reading the symbol from the segment of the input tape that is currently in the read head. Some more advanced machines have a read/write head that can also write symbols onto the tape. The movement of the input tape after reading a symbol depends on the machine. With a finite-state machine, the next segment of the input tape is always moved into the read head after a symbol has been read. Most machines (including finite-state machines) also have a separate output tape that is written on with a write head. The output symbols come from an output alphabet, Z, that may or may not be equal to the input alphabet. The most significant component of an abstract machine is its memory structure. This structure can range from a finite number of bits of memory (as in a finite-state machine) to an infinite amount of memory that can be stored in the form of a tape that can be read from and written on (as in a Turing machine).

Definition 13.3.1: Finite-State Machine

A finite-state machine is defined by a quintet (S, X, Z, w, t) where

1. $S = \{s_1, s_2, \ldots, s_r\}$ is the state set, a finite set that corresponds to the set of memory configurations that the machine can have at any time.
2. $X = \{x_1, x_2, \ldots, x_m\}$ is the input alphabet.
3. $Z = \{z_1, z_2, \ldots, z_n\}$ is the output alphabet.
4. $w : X \times S \to Z$ is the output function, which specifies which output symbol $w(x, s) \in Z$ is written onto the output tape when the machine is in state s and the input symbol x is read.
5. $t : X \times S \to S$ is the next-state (or transition) function, which specifies which state $t(x, s) \in S$ the machine should enter when it is in state s and it reads the symbol x.

Example 13.3.1: Vending Machine as a Finite-State Machine

Many mechanical devices, such as simple vending machines, can be thought of as finite-state machines. For simplicity, assume that a vending machine dispenses packets of gum, spearmint (S), peppermint (P), and bubble (B), for 25 cents each. We can define the input alphabet to be

$$\{\text{deposit 25 cents, press S, press P, press B}\}$$

and the state set to be $\{\text{Locked, Select}\}$, where the deposit of a quarter unlocks the release mechanism of the machine and allows you to select a flavor of gum. We will leave it to the reader to imagine what the output alphabet, output function, and next-state function would be. You are also invited to let your imagination run wild and include such features as a coin-return lever and change maker.

Example 13.3.2: A Parity Checking Machine

The following machine is called a parity checker. It recognizes whether or not a string in B^* contains an even number of 1s. The memory structure of this machine reflects the fact that in order to check the parity of a string, we need only keep track of whether an odd or even number of 1's has been detected.

The input alphabet is $B = \{0, 1\}$ and the output alphabet is also B. The state set is $\{even, odd\}$. The following table defines the output and next-state functions.

x	s	$w(x,s)$	$t(x,s)$
0	even	0	even
0	odd	1	odd
1	even	1	odd
1	odd	0	even

Note how the value of the most recent output at any time is an indication of the current state of the machine. Therefore, if we start in the even state and read any finite input tape, the last output corresponds to the final state of the parity checker and tells us the parity of the string on the input tape. For example, if the string 11001010 is read from left to right, the output tape, also from left to right, will be 10001100. Since the last character is a 0, we know that the input string has even parity.

An alternate method for defining a finite-state machine is with a transition diagram. A transition diagram is a directed graph that contains a node for each state and edges that indicate the transition and output functions. An edge (s_i, s_j) that is labeled x/z indicates that in state s_i the input x results in an output of z and the next state is s_j. That is, $w(x, s_i) = z$ and $t(x, s_i) = s_j$. The transition diagram for the parity checker appears in Figure 13.3.1. In later examples, we will see that if there are different inputs, x_i and x_j, while in the same state resulting in the same transitions and outputs, we label a single edge $x_i, x_j / z$ instead of drawing two edges with labels x_i / z and x_j / z.

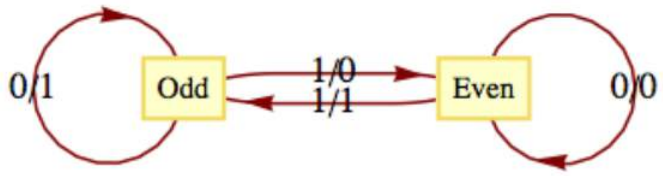


Figure 13.3.1: Transition Diagram for a Parity Checker

One of the most significant features of a finite-state machine is that it retains no information about its past states that can be accessed by the machine itself. For example, after we input a tape encoded with the symbols 01101010 into the parity checker, the current state will be even, but we have no indication within the machine whether or not it has always been in even state. Note how the output tape is not considered part of the machine's memory. In this case, the output tape does contain a "history" of the parity checker's past states. We assume that the finite-state machine has no way of recovering the output sequence for later use.

Example 13.3.3: A Baseball Machine

Consider the following simplified version of the game of baseball. To be precise, this machine describes one half-inning of a simplified baseball game. Suppose that in addition to home plate, there is only one base instead of the usual three bases. Also, assume that there are only two outs per inning instead of the usual three. Our input alphabet will consist of the types of hits that the batter could have: out (O), double play (DP), single (S), and home run (HR). The input DP is meant to represent a batted ball that would result in a double play (two outs), if possible. The input DP can then occur at any time. The output alphabet is the numbers 0, 1, and 2 for the number of runs that can be scored as a result of any input. The state set contains the current situation in the inning, the number of outs, and whether a base runner is currently on the base. The list of possible states is then 00 (for 0 outs and 0 runners), 01, 10, 11, and end (when the half-inning is over). The transition diagram for this machine appears in Figure 13.3.2

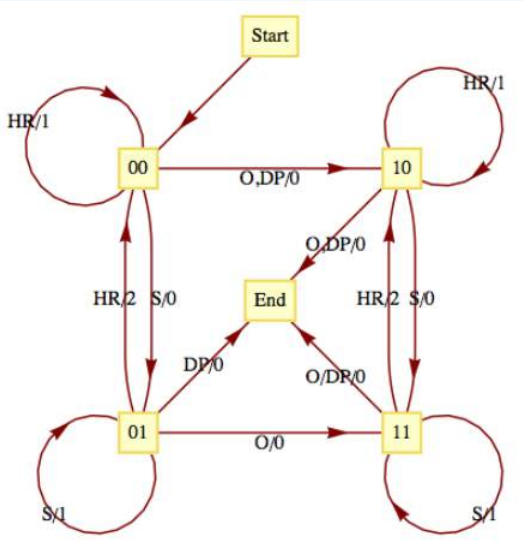


Figure 13.3.2: Transition Diagram for a Simplified Game of Baseball

Let's concentrate on one state. If the current state is 01, 0 outs and 1 runner on base, each input results in a different combination of output and next-state. If the batter hits the ball poorly (a double play) the output is zero runs and the inning is over (the limit of two outs has been made). A simple out also results in an output of 0 runs and the next state is 11, one out and one runner on base. If the batter hits a single, one run scores (output = 1) while the state remains 01. If a home run is hit, two runs are scored (output = 2) and the next state is 00. If we had allowed three outs per inning, this graph would only be marginally more complicated. The usual game with three bases would be quite a bit more complicated, however.

Example 13.3.4: Recognition in Regular Languages

As we mentioned at the outset of this section, finite-state machines can recognize strings in a regular language. Consider the language L over $\{a, b, c\}$ that contains the strings of positive length in which each a is followed by b and each b is followed by c. One such string is $bccabcbc$. This language is regular. A grammar for the language would be nonterminal symbols $\{A, B, C\}$ with starting symbol C and production rules $A \to bB$, $B \to cC$, $C \to aA$, $C \to bB$, $C \to cC$, $C \to c$. A finite-state machine (Figure 13.3.3) that recognizes this language can be constructed with one state for each nonterminal symbol and an additional state (Reject) that is entered if any invalid production takes place. At the end of an input tape that encodes a string in $\{a, b, c\}^*$, we will know when the string belongs to L based on the final output. If the final output is 1, the string belongs to L and if it is 0, the string does not belong to L. In addition, recognition can be accomplished by examining the final state of the machine. The input string belongs to the language if and only if the final state is C.

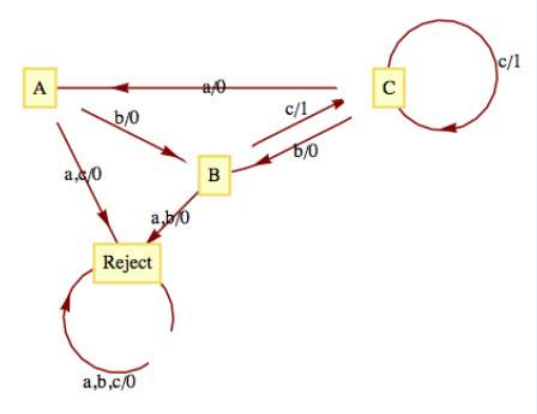


Figure 13.3.3

The construction of this machine is quite easy: note how each production rule translates into an edge between states other than Reject. For example, $C \to bB$ indicates that in State C, an input of b places the machine into State B. Not all sets of production rules can be as easily translated to a finite-state machine. Another set of production rules for L is $A \to aB$, $B \to bC$, $C \to cA$, $C \to cB$, $C \to cC$ and $C \to c$. Techniques for constructing finite-state machines from production rules is not our objective here. Hence we will only expect you to experiment with production rules until appropriate ones are found.

Example 13.3.5: A Binary Adder

A finite-state machine can be designed to add positive integers of any size. Given two integers in binary form, $a = a_n a_{n-1} \cdots a_1 a_0$ and $b = b_n b_{n-1} \cdots b_1 b_0$, the machine take as its input sequence the corresponding bits of a and b reading from right to left with a "parity bit" added

$$a_0 b_0 \left(a_0 +_2 b_0\right), a_1 b_1 \left(a_1 +_2 b_1\right) \ldots, a_n b_n \left(a_n +_2 b_n\right), 111$$

Notice the special input 111 at the end. All possible inputs except the last one must even parity (contain an even number of ones). The output sequence is the sum of a and b, starting with the units digit, and comes from the set $\{0, 1, \lambda\}$. The transition diagram for this machine appears in Figure 13.3.4

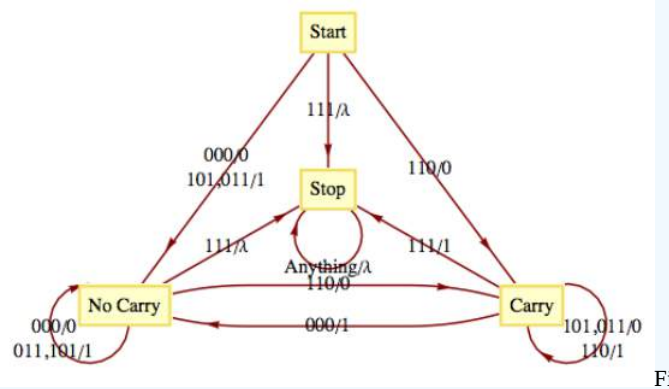


Figure 13.3.4: Transition Diagram for a binary adder

13.3.1: 14.3.1: Exercises

Exercise 13.3.1

Draw a transition diagram for the vending machine described in Example 13.3.1.

Answer

x	s	$Z(x,s)$	$t(x,s)$
Deposit25 ¢	Locked	Nothing	Select
Deposit25 ¢	Select	Return25 ¢	Select
Press$S$	Locked	Nothing	Locked
Press$S$	Select	Dispense$S$	Locked
Press$P$	Locked	Nothing	Locked
Press$P$	Select	Dispense$P$	Locked
Press$B$	Locked	Nothing	Locked
Press$B$	Select	Dispense$B$	Locked

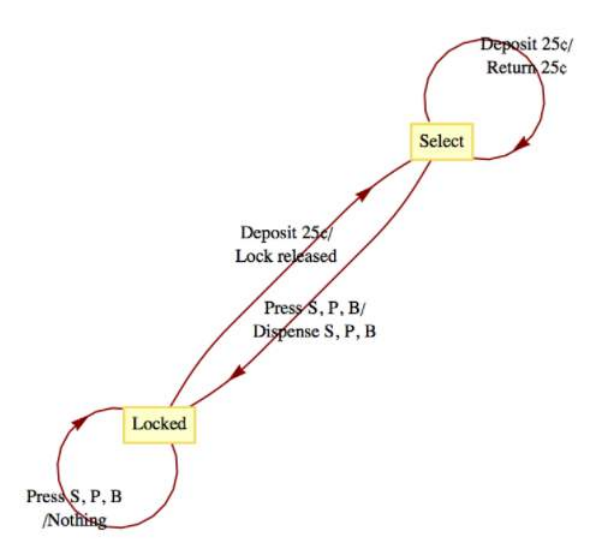


Figure 13.3.5: Vending Machine Transitions

Exercise 13.3.2

Construct finite-state machines that recognize the regular languages that you identified in Section 14.2.

Exercise 13.3.3

What is the input set for the binary adding machine in Example 13.3.5?

Answer

$\{000, 011, 101, 110, 111\}$

Exercise 13.3.4

What input sequence would be used to compute the sum of 1101 and 0111 (binary integers)? What would the output sequence be?

Exercise 13.3.5

The Gray Code Decoder. The finite-state machine defined by the following figure has an interesting connection with the Gray Code.

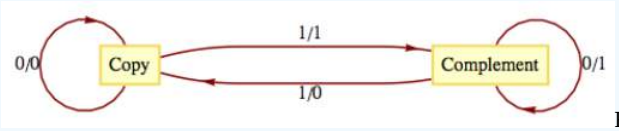


Figure 13.3.6: Gray Code Decoder

Given a string $x = x_1x_2 \cdots x_n \in B^n$, we may ask where x appears in G_n. Starting in Copy state, the input string x will result in an output string $z \in B^n$, which is the binary form of the position of x in G_n. Recall that positions are numbered from 0 to $2^n - 1$.

a. In what positions $(0 - 31)$ do 10110, 00100, and 11111 appear in G_5?
b. Prove that the Gray Code Decoder always works.

Answer

a.

- Input: 10110, Output: 11011 $\Rightarrow$ 10110 is in position 27
- Input: 00100, Output: 00111 $\Rightarrow$ 00100 is in position 7
- Input:11111, Output: 10101 $\Rightarrow$ 11111 is in position 21

b. Let $x = x_1x_2 \ldots x_n$ and recall that for $n \geq 1$, $G_{n+1} = \begin{pmatrix} 0G_n \\ 1G_n^r \end{pmatrix}$, where G_n^r is the reverse of G_n. To prove that the Gray Code Decoder always works, let $p(n)$ be the proposition "Starting in Copy state, x's output is the position of x in G_n; and starting in Complement state, x's output is the position of x in G_n^r." That p(1) is true is easy to verify for both possible values of x, 0 and 1. Now assume that for some $n \geq 1$, $p(n)$ is true and consider $x = x_1x_2 \ldots x_nx_{n+1}$.
If $x_1 = 0$, x's output is a zero followed by the output for $(x_2 \ldots x_nx_{n+1})$ starting in Copy state. By the induction hypothesis, this is zero followed by the position of $(x_2 \ldots x_nx_{n+1})$ in G_n, which is the position of x in G_{n+1}, by the definition of G.
If $x_1 = 1$, x's output is a one followed by the output for $(x_2 \ldots x_nx_{n+1})$ starting in Complement state. By the induction hypothesis, this is one followed by the position of $(x_2 \ldots x_nx_{n+1})$ in G_n^r, which is the position of x in G_{n+1}, by the definition of G. □

13.4: The Monoid of a Finite-State Machine

In this section, we will see how every finite-state machine has a monoid associated with it. For any finite-state machine, the elements of its associated monoid correspond to certain input sequences. Because only a finite number of combinations of states and inputs is possible for a finite-state machine there is only a finite number of input sequences that summarize the machine. This idea is illustrated best with a few examples.

Consider the parity checker. The following table summarizes the effect on the parity checker of strings in B^1 and B^2. The row labeled "Even" contains the final state and final output as a result of each input string in B^1 and B^2 when the machine starts in the even state. Similarly, the row labeled "Odd" contains the same information for input sequences when the machine starts in the odd state.

Input String	0	1	00	01	10	11
Even	$(\text{Even}, 0)$	$(\text{Odd}, 1)$	$(\text{Even}, 0)$	$(\text{Odd}, 1)$	$(\text{Odd}, 1)$	$(\text{Even}, 0)$
Odd	$(\text{Odd}, 1)$	$(\text{Even}, 1)$	$(\text{Odd}, 1)$	$(\text{Even}, 1)$	$(\text{Even}, 0)$	$(\text{Odd}, 1)$
Same Effect as			0	1	1	0

Note how, as indicated in the last row, the strings in B^2 have the same effect as certain strings in B^1. For this reason, we can summarize the machine in terms of how it is affected by strings of length 1. The actual monoid that we will now describe consists of a set of functions, and the operation on the functions will be based on the concatenation operation.

Let T_0 be the final effect (state and output) on the parity checker of the input 0. Similarly, T_1 is defined as the final effect on the parity checker of the input 1. More precisely,

$$T_0(\text{even}) = (\text{even}, 0) \quad \text{and} \quad T_0(\text{odd}) = (\text{odd}, 1),$$

while

$$T_1(\text{even}) = (\text{odd}, 1) \quad \text{and} \quad T_1(\text{odd}) = (\text{even}, 0).$$

In general, we define the operation on a set of such functions as follows: if s, t are input sequences and T_s and T_t, are functions as above, then $T_s * T_t = T_{st}$, that is, the result of the function that summarizes the effect on the machine by the concatenation of s with t. Since, for example, 01 has the same effect on the parity checker as 1, $T_0 * T_1 = T_{01} = T_1$. We don't stop our calculation at T_{01} because we want to use the shortest string of inputs to describe the final result. A complete table for the monoid of the parity checker is

$*$	T_0	T_1
T_0	T_0	T_1
T_1	T_1	T_0

What is the identity of this monoid? The monoid of the parity checker is isomorphic to the monoid $[\mathbb{Z}_2; +_2]$.

This operation may remind you of the composition operation on functions, but there are two principal differences. The domain of T_s is not the codomain of T_t and the functions are read from left to right unlike in composition, where they are normally read from right to left.

You may have noticed that the output of the parity checker echoes the state of the machine and that we could have looked only at the effect on the machine as the final state. The following example has the same property, hence we will only consider the final state.

Example 13.4.1

The transition diagram for the machine that recognizes strings in $B*$ that have no consecutive 1's appears in Figure 13.4.1. Note how it is similar to the graph in Figure 9.1.1. Only a "reject state" has been added, for the case when an input of 1 occurs while in State a. We construct a similar table to the one in the previous example to study the effect of certain strings on this machine. This time, we must include strings of length 3 before we recognize that no "new effects" can be found.

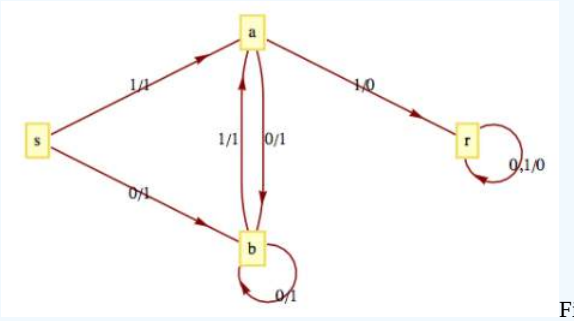


Figure 13.4.1: No Consecutive Ones Monoid

Inputs	0	1	00	01	10	11	000	001	010	011	100	101	110	111
s	b	a	b	a	b	r	b	a	b	r	b	a	r	r
a	b	r	b	a	r	r	b	a	b	r	r	r	r	r
b	b	a	b	a	b	r	b	a	b	r	b	a	r	r
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Same as			0				0	01	0	11	10	1	11	11

The following table summarizes how combinations of the strings $0, 1, 01, 10,$ and 11 affect this machine.

$*$	T_0	T_1	T_{01}	T_{10}	T_{11}
T_0	T_0	T_1	T_{01}	T_{10}	T_{11}
T_1	T_{10}	T_{11}	T_1	T_{11}	T_{11}
T_{01}	T_0	T_{11}	T_{01}	T_{11}	T_{11}
T_{10}	T_{10}	T_1	T_1	T_{10}	T_{11}
T_{11}	T_{11}	T_{11}	T_{11}	T_{11}	T_{11}

All the results in this table can be obtained using the previous table. For example,

$$T_{10} * T_{01} = T_{1001} = T_{100} * T_1 = T_{10} * T_1 = T_{101} = T_1$$

and

$$T_{01} * T_{01} = T_{0101} = T_{010} T_1 = T_0 T_1 = T_{01}$$

Note that none of the elements that we have listed in this table serves as the identity for our operation. This problem can always be remedied by including the function that corresponds to the input of the null string, T_λ. Since the null string is the identity for concatenation of strings, $T_s T_\lambda = T_\lambda T_s = T_s$ for all input strings s.

Example 13.4.2: The Unit-Time Delay Machine

A finite-state machine called the unit-time delay machine does not echo its current state, but prints its previous state. For this reason, when we find the monoid of the unit-time delay machine, we must consider both state and output. The transition diagram of this machine appears in Figure 13.4.2

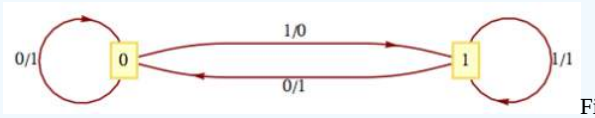


Figure 13.4.2

Input	0	1	00	01	10	11	100 or000	101 or001	110 or101	111 or011
0	$(0,0)$	$(1,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
1	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
Same as							00	01	10	11

Again, since no new outcomes were obtained from strings of length 3, only strings of length 2 or less contribute to the monoid of the machine. The table for the strings of positive length shows that we must add T_λ to obtain a monoid.

$*$	T_0	T_1	T_{00}	T_{01}	T_{10}	T_{11}
T_0	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_1	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}
T_{00}	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_{01}	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}
T_{10}	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_{11}	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}

.

13.4.1: 14.4.1: Exercises

Exercise 13.4.1

For each of the transition diagrams in Figure 13.4.3, write out tables for their associated monoids. Identify the identity in terms of a string of positive length, if possible.

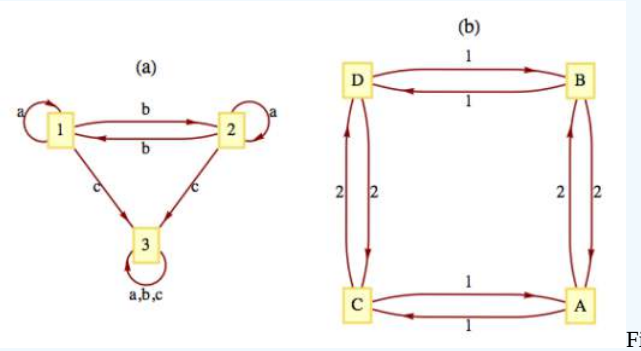


Figure 13.4.3: Exercise 13.4.3

Hint

Where the output echoes the current state, the output can be ignored.

Answer

a.

Input String	a	b	c	aa	ab	ac
1	$(a,1)$	$(a,2)$	$(c,3)$	$(a,1)$	$(a,2)$	$(c,3)$
2	$(a,2)$	$(a,1)$	$(c,3)$	$(a,2)$	$(a,1)$	$(c,3)$
3	$(c,3)$	$(c,3)$	$(c,3)$	$(c,3)$	$(c,3)$	$(c,3)$
Input String	ba	bb	bc	ca	cb	cc
1	$(a,2)$	$(a,1)$	$(c,3)$	$(c,3)$	$(c,3)$	$(c,3)$
2	$(a,1)$	$(a,2)$	$(c,3)$	$(c,3)$	$(c,3)$	$(c,3)$
3	$(c,3)$	$(c,3)$	$(c,3)$	$(c,3)$	$(c,3)$	$(c,3)$

We can see that $T_aT_a = T_{\text{aa}} = T_a$, $T_aT_b = T_{\text{ab}} = T_b$, etc. Therefore, we have the following monoid:

	T_a	T_b	T_b
T_a	T_a	T_b	T_c
T_b	T_b	T_a	T_c
T_c	T_c	T_c	T_c

Notice that T_a is the identity of this monoid.

b.

Input String	1	2	11	12	21	22
A	C	B	A	D	D	A
B	D	A	B	C	C	B
C	A	D	C	B	B	C
D	B	C	D	A	A	D

Input String	111	112	121	122	211	212	221	222
A	C	B	B	C	B	C	C	B
B	D	A	A	D	A	D	D	A
C	B	C	C	B	C	B	B	C
D	B	C	C	B	C	B	B	C

We have the following monoid:

	T_1	T_2	T_{11}	T_{12}
T_1	T_{11}	T_{12}	T_1	T_2
T_2	T_b	T_{11}	T_2	T_1
T_{11}	T_1	T_2	T_{11}	T_{12}
T_{12}	T_2	T_1	T_{12}	T_{11}

Notice that T_{11} is the identity of this monoid.

Exercise 13.4.2

What common monoids are isomorphic to the monoids obtained in the previous exercise?

Exercise 13.4.3

Can two finite-state machines with nonisomorphic transition diagrams have isomorphic monoids?

Answer

Yes, just consider the unit time delay machine of Figure 13.4.2 Its monoid is described by the table at the end of Section 14.4 where the T_λ row and T_λ column are omitted. Next consider the machine in Figure 14.5.3. The monoid of this machine is:

	T_λ	T_0	T_1	T_{00}	T_{01}	T_{10}	T_{11}
T_λ	T_λ	T_0	T_1	T_{00}	T_{01}	T_{10}	T_{11}
T_0	T_0	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_1	T_1	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}
T_{00}	T_{00}	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_{01}	T_{01}	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}
T_{10}	T_{10}	T_{00}	T_{01}	T_{00}	T_{01}	T_{10}	T_{11}
T_{11}	T_{11}	T_{10}	T_{11}	T_{00}	T_{01}	T_{10}	T_{11}

Hence both of these machines have the same monoid, however, their transition diagrams are nonisomorphic since the first has two vertices and the second has seven.

13.5: The Machine of a Monoid

Any finite monoid $[M; *]$ can be represented in the form of a finite-state machine with input and state sets equal to M. The output of the machine will be ignored here, since it would echo the current state of the machine. Machines of this type are called ***state machines***. It can be shown that whatever can be done with a finite-state machine can be done with a state machine; however, there is a trade-off. Usually, state machines that perform a specific function are more complex than general finite-state machines.

Definition 13.5.1: Machine of a Monoid

If $[M; *]$ is a finite monoid, then the machine of M, denoted $m(M)$, is the state machine with state set M, input set M, and next-state function $t : M \times M \to M$ defined by $t(s, x) = s * x$.

Example 13.5.1

We will construct the machine of the monoid $[\mathbb{Z}_2; +_2]$. As mentioned above, the state set and the input set are both $\mathbb{Z}_2$. The next state function is defined by $t(s, x) = s +_2 x$. The transition diagram for $m(\mathbb{Z}_2)$ appears in Figure 13.5.1. Note how it is identical to the transition diagram of the parity checker, which has an associated monoid that was isomorphic to $[\mathbb{Z}_2; +_2]$.

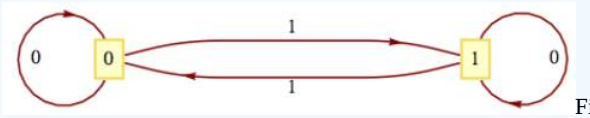


Figure 13.5.1: The machine of $[\mathbb{Z}_2; +_2]$

Example 13.5.2

The transition diagram of the monoids $[\mathbb{Z}_2; \times_2]$ and $[\mathbb{Z}_3; \times_3]$ appear in Figure 13.5.2

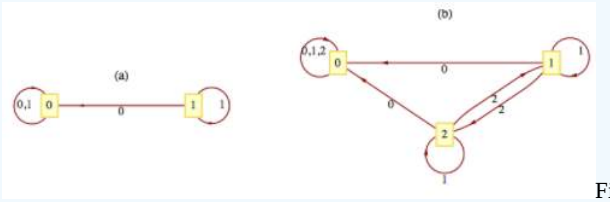


Figure 13.5.2: The machines of $[\mathbb{Z}_2; \times_2]$ and $\mathbb{Z}_3; \times_3]$

Example 13.5.3

Let U be the monoid that we obtained from the unit-time delay machine (Example 14.4.2). We have seen that the machine of the monoid of the parity checker is essentially the parity checker. Will we obtain a unit-time delay machine when we construct the machine of U? We can't expect to get exactly the same machine because the unit-time delay machine is not a state machine and the machine of a monoid is a state machine. However, we will see that our new machine is capable of telling us what input was received in the previous time period. The operation table for the monoid serves as a table to define the transition function for the machine. The row headings are the state values, while the column headings are the inputs. If we were to draw a transition diagram with all possible inputs, the diagram would be too difficult to read. Since U is generated by the two elements, T_0 and T_1, we will include only those inputs. Suppose that we wanted to read the transition function for the input T_{01}. Since $T_{01} = T_0 T_1$, in any state $s, t(s, T_{01}) = t(t(s, T_0), T_1)$. The transition diagram appears in Figure 13.5.3

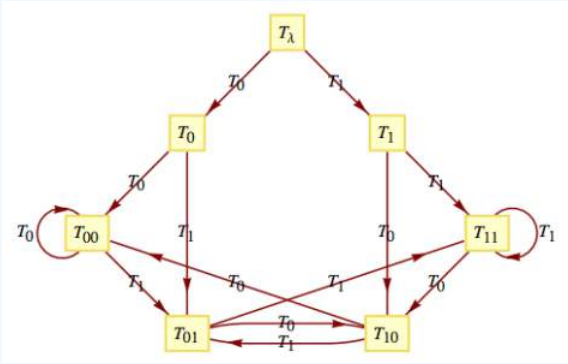


Figure 13.5.3: Copy and Paste Caption here. (Copyright; author via source)

If we start reading a string of 0's and 1's while in state T_λ and are in state T_{ab} at any one time, the input from the previous time period (not the input that sent us into T_{ab}, the one before that) is a. In states T_λ, T_0 and T_1, no previous input exists.

13.5.1: 14.5.1: Exercises

Exercise 13.5.1

Draw the transition diagrams for the machines of the following monoids:

a. $[\mathbb{Z}_4; +_4]$
b. The direct product of $[\mathbb{Z}_2; \times_2]$ with itself.

Answer

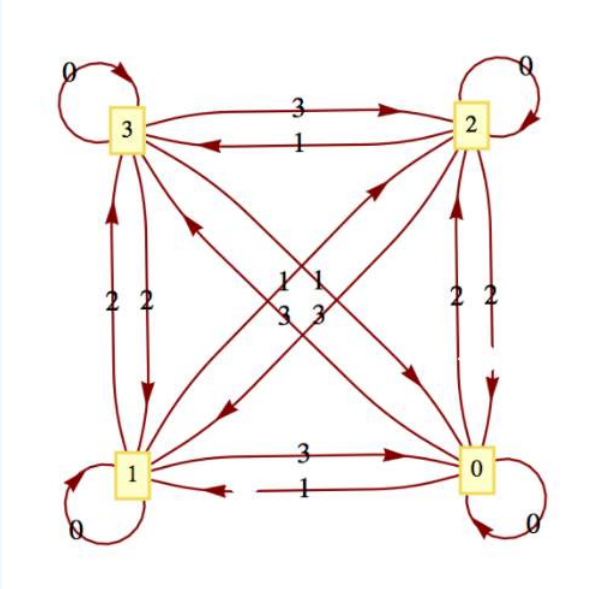


Figure 13.5.4: (a)

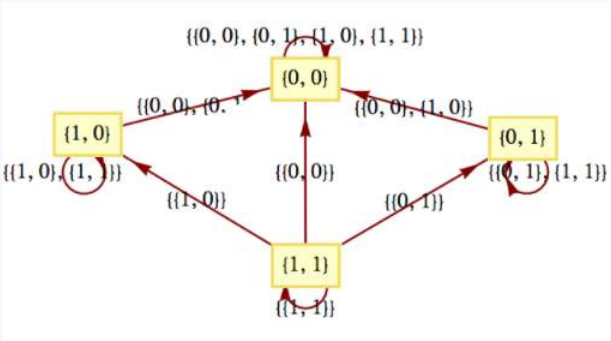


Figure 13.5.5: (b)

Exercise 13.5.2

Even though a monoid may be infinite, we can visualize it as an infinite-state machine provided that it is generated by a finite number of elements. For example, the monoid B^* is generated by 0 and 1. A section of its transition diagram can be obtained by allowing input only from the generating set. The monoid of integers under addition is generated by the set $\{-1, 1\}$. The transition diagram for this monoid can be visualized by drawing a small portion of it, as in Figure 13.5.6. The same is true for the additive monoid of integers, as seen in Figure 13.5.7.

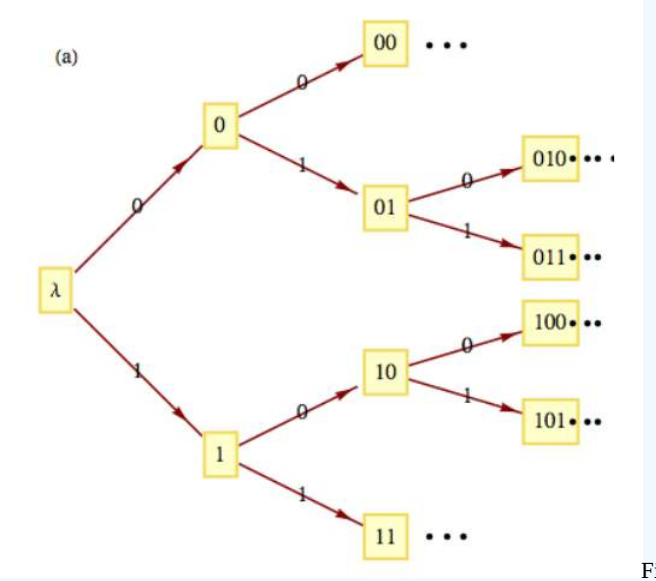


Figure 13.5.6: An infinite machine B^*

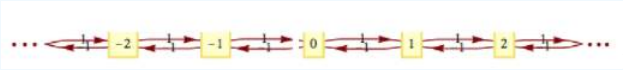


Figure 13.5.7: An infinite machine $[\mathbb{Z}; +]$

a. Draw a transition diagram for $\{a, b, c\}$
b. Draw a transition diagram for $[\mathbb{Z} \times \mathbb{Z}; \text{componentwise addition}]$.
c. Draw a transition diagram for $[\mathbb{Z}; +]$ with generating set $\{5, -2\}$.

CHAPTER OVERVIEW

14: Group Theory and Applications

> ***alternating group***
>
> *N objects are ordered, and you*
> *Switch consecutive pairs two by two.*
> *All reorders you get*
> *Will comprise a new set*
> *Called an* ***alternating group*** *when you're through.*
>
> *Chris Doyle, The Omnificent English Dictionary in Limerick Form*

In Chapter 11, we introduced groups as a typical algebraic system. The associated concepts of subgroup, group isomorphism, and direct products of groups were also introduced. Groups were chosen for that chapter because they are among the simplest types of algebraic systems. Despite this simplicity, group theory abounds with interesting applications. In this chapter we will introduce some more important concepts in elementary group theory, and some of their applications.

14.1: Cyclic Groups

Groups are classified according to their size and structure. A group's structure is revealed by a study of its subgroups and other properties (e.g., whether it is abelian) that might give an overview of it. Cyclic groups have the simplest structure of all groups.

Definition 14.1.1: Cyclic Group

Group G is cyclic if there exists $a \in G$ such that the cyclic subgroup generated by a, $\langle a \rangle$, equals all of G. That is, $G = \{na | n \in \mathbb{Z}\}$, in which case a is called a generator of G. The reader should note that additive notation is used for G.

Example 14.1.1: A Finite Cyclic Group

$\mathbb{Z}_{12} = [\mathbb{Z}_{12}; +_{12}]$, where $+_{12}$ is addition modulo 12, is a cyclic group. To verify this statement, all we need to do is demonstrate that some element of $\mathbb{Z}_{12}$ is a generator. One such element is 5; that is, $\langle 5 \rangle = \mathbb{Z}_{12}$. One more obvious generator is 1. In fact, 1 is a generator of every $[\mathbb{Z}_n; +_n]$. The reader is asked to prove that if an element is a generator, then its inverse is also a generator. Thus, $-5 = 7$ and $-1 = 11$ are the other generators of $\mathbb{Z}_{12}$. The remaining eight elements of the group are not generators.

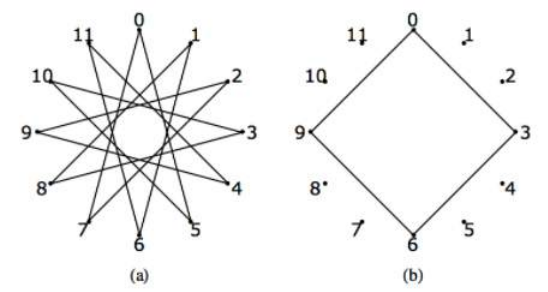


Figure 14.1.1: Copy and Paste Caption here. (Copyright; author via source)

Figure 14.1.1(a) is an example of “string art” that illustrates how 5 generates $\mathbb{Z}_{12}$. Twelve tacks are placed evenly around a circle and numbered 0 through 11. A string is tied to tack 0, and is then looped around every fifth tack. As a result, the numbers of the tacks that are reached are exactly the ordered multiples of 5 modulo 12: 5, 10, 3, ... , 7, 0. Note that if every seventh tack were used, the same artwork would be produced. If every third tack were connected, as in Figure 14.1.1(b), the resulting loop would only use four tacks; thus 3 does not generate $\mathbb{Z}_{12}$.

Example 14.1.2: The Group of Integers is Cyclic

The additive group of integers, $[\mathbb{Z}; +]$, is cyclic:

$$\mathbb{Z} = \langle 1 \rangle = \{n \cdot 1 | n \in \mathbb{Z}\}$$

This observation does not mean that every integer is the product of an integer times 1. It means that

$$\mathbb{Z} = \{0\} \cup \{\overbrace{1+1+\cdots+1}^{n \text{ terms}} \mid n \in \mathbb{P}\} \cup \{\overbrace{(-1)+(-1)+\cdots+(-1)}^{n \text{ terms}} \mid n \in \mathbb{P}\}$$

Theorem 14.1.1: Cyclic Implies Abelian

If $[G; *]$ is cyclic, then it is abelian.

Proof

Let a be any generator of G and let $b, c \in G$. By the definition of the generator of a group, there exist integers m and n such that $b = ma$ and $c = na$. Thus, using Theorem 11.3.9,

$$\begin{aligned} b * c &= (ma) * (na) \\ &= (m+n)a \\ &= (n+m)a \\ &= (na) * (ma) \\ &= c * b \end{aligned}$$

One of the first steps in proving a property of cyclic groups is to use the fact that there exists a generator. Then every element of the group can be expressed as some multiple of the generator. Take special note of how this is used in theorems of this section.

Up to now we have used only additive notation to discuss cyclic groups. Theorem 14.1.1 actually justifies this practice since it is customary to use additive notation when discussing abelian groups. Of course, some concrete groups for which we employ multiplicative notation are cyclic. If one of its elements, a, is a generator,

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

Example 14.1.3: A Cyclic Multiplicative Group

The group of positive integers modulo 11 with modulo 11 multiplication, $[\mathbb{Z}_{11}^*; \times_{11}]$, is cyclic. One of its generators is 6: $6^1 = 6$, $6^2 = 3$, $6^3 = 7, \ldots, 6^9 = 2$, and $6^{10} = 1$, the identity of the group.

Example 14.1.4: A Non-Cyclic Group

The real numbers with addition, $[\mathbb{R}; +]$ is a noncyclic group. The proof of this statement requires a bit more generality since we are saying that for all $r \in \mathbb{R}$, $\langle r \rangle$ is a proper subset of $\mathbb{R}$. If r is nonzero, the multiples of r are distributed over the real line, as in Figure 14.1.2 It is clear then that there are many real numbers, like $r/2$, that are not in $\langle r \rangle$.

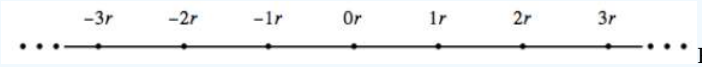


Figure 14.1.2: Elements of $\langle r \rangle, r > 0$

The next two proofs make use of the Theorem 11.4.1.

The following theorem shows that a cyclic group can never be very complicated.

Theorem 14.1.2: Possible Cyclic Group Structures

If G is a cyclic group, then G is either finite or countably infinite. If G is finite and $|G| = n$, it is isomorphic to $[\mathbb{Z}_n; +_n]$. If G is infinite, it is isomorphic to $[\mathbb{Z}; +]$.

Proof

Case 1: $|G| < \infty$. If a is a generator of G and $|G| = n$, define $\phi : \mathbb{Z}_n \to G$ by $\phi(k) = ka$ for all $k \in \mathbb{Z}_n$.

Since $\langle a \rangle$ is finite, we can use the fact that the elements of $\langle a \rangle$ are the first n nonnegative multiples of a. From this observation, we see that ϕ is a surjection. A surjection between finite sets of the same cardinality must be a bijection. Finally, if $p, q \in \mathbb{Z}_n$,

$$\begin{aligned} \phi(p) + \phi(q) &= pa + qa \\ &= (p+q)a \\ &= (p +_n q)a \quad \text{see exercise 15.1.10} \\ &= \phi(p +_n q) \end{aligned}$$

Therefore ϕ is an isomorphism.

Case 2: $|G| = \infty$. We will leave this case as an exercise.

Theorem 14.1.3: Subgroups of Cyclic Groups

Every subgroup of a cyclic group is cyclic.

Proof

Let G be cyclic with generator a and let $H \leq G$. If $H = \{e\}$, H has e as a generator. We may now assume that $|H| \geq 2$ and $a \neq e$. Let m be the least positive integer such that ma belongs to H. This is the key step. It lets us get our hands on a generator of H. We will now show that $c = ma$ generates H. Certainly, $\langle c \rangle \subseteq H$, but suppose that $\langle c \rangle \neq H$. Then there exists $b \in H$ such that $b \notin \langle c \rangle$. Now, since b is in G, there exists $n \in \mathbb{Z}$ such that $b = na$. We now apply the division property and divide n by m. $b = na = (qm + r)a = (qm)a + ra, \quad$ where $0 \leq r < m$. We note that r cannot be zero for otherwise we would have $b = na = q(ma) = qc \in \langle c \rangle$. Therefore, $ra = na - (qm)a \in H$. This contradicts our choice of m because $0 < r < m$.

Example 14.1.5: All Subgroups of $\mathbb{Z}_{10}$

The only proper subgroups of $\mathbb{Z}_{10}$ are $H_1 = \{0, 5\}$ and $H_2 = \{0, 2, 4, 6, 8\}$. They are both cyclic: $H_1 = \langle 5 \rangle$, while $H_2 = \langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle$. The generators of $\mathbb{Z}_{10}$ are 1, 3, 7, and 9.

Example 14.1.6: All Subgroups of $\mathbb{Z}$

With the exception of $\{0\}$, all subgroups of $\mathbb{Z}$ are isomorphic to $\mathbb{Z}$. If $H \leq \mathbb{Z}$, then H is the cyclic subgroup generated by the least positive element of H. It is infinite and so by Theorem 14.1.3it is isomorphic to $\mathbb{Z}$.

We now cite a useful theorem for computing the order of cyclic subgroups of a cyclic group:

Theorem 14.1.4: The Order of Elements of a Finite Cyclic Group

If G is a cyclic group of order n and a is a generator of G, the order of ka is n/d, where d is the greatest common divisor of n and k.

Proof

The proof of this theorem is left to the reader.

Example 14.1.7: Computation of an Order in a Cyclic Group

To compute the order of $\langle 18 \rangle$ in $\mathbb{Z}_{30}$, we first observe that 1 is a generator of $\mathbb{Z}_{30}$ and $18 = 18(1)$. The greatest common divisor of 18 and 30 is 6. Hence, the order of $\langle 18 \rangle$ is 30/6, or 5.

At this point, we will introduce the idea of a fast adder, a relatively modern application (Winograd, 1965) of an ancient theorem, the Chinese Remainder Theorem. We will present only an overview of the theory and rely primarily on examples.

Out of necessity, integer addition with a computer is addition modulo n, for n some larger number. Consider the case where n is small, like 64. Then addition involves the addition of six-digit binary numbers. Consider the process of adding 31 and 1. Assume the computer's adder takes as input two bit strings $a = \{a_0, a_1, a_2, a_3, a_4, a_5\}$ and $b = \{b_0, b_1, b_2, b_3, b_4, b_5\}$ and outputs $s = \{s_0, s_1, s_2, s_3, s_4, s_5\}$, the sum of a and b. Then, if $a = 31 = (1, 1, 1, 1, 1, 0)$ and $b = 1 = (1, 0, 0, 0, 0, 0)$, s will be (0, 0, 0, 0, 0, 1), or 32. The output $s = 1$ cannot be determined until all other outputs have been determined. If addition is done with a finite-state machine, as in Example 14.3.5, the time required to get s will be six time units, where one time unit is the time it takes to get one output from the machine. In general, the time required to obtain s will be proportional to the number of bits. Theoretically, this time can be decreased, but the explanation would require a long digression and our relative results would not change that much. We will use the rule that the number of time units needed to perform addition modulo n is proportional to $\lceil \log_2 n \rceil$.

Now we will introduce a hypothetical problem that we will use to illustrate the idea of a fast adder. Suppose that we had to add 1,000 numbers modulo $27720 = 8 \cdot 9 \cdot 5 \cdot 7 \cdot 11$. By the rule above, since $2^{14} < 27720 < 2^{15}$, each addition would take 15 time

units. If the sum is initialized to zero, 1,000 additions would be needed; thus, 15,000 time units would be needed to do the additions. We can improve this time dramatically by applying the Chinese Remainder Theorem.

Theorem 14.1.5: Chinese Remainder Theorem (CRT)

Let $n_1, n_2, \ldots, n_p$ be integers that have no common factor greater than one between any pair of them; i. e., they are relatively prime. Let $n = n_1 n_2 \cdots n_p$. Define

$$\theta : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_p}$$

by

$$\theta(k) = (k_1, k_2, \ldots, k_p)$$

where for $1 \leq i \leq p$, $0 \leq k_i < n_i$ and $k \equiv k_i \pmod{n_i}$. Then θ is an isomorphism from $\mathbb{Z}_n$ into $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_p}$.

The Chinese Remainder Theorem can be stated in several different forms, and its proof can be found in many abstract algebra texts.

As we saw in Chapter 11, $\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$. This is the smallest case to which the CRT can be applied. An isomorphism between $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ is

$$\begin{aligned} \theta(0) &= (0,0) \quad \theta(3) = (1,0) \\ \theta(1) &= (1,1) \quad \theta(4) = (0,1) \\ \theta(2) &= (0,2) \quad \theta(5) = (1,2) \end{aligned}$$

Let's consider a somewhat larger case. We start by selecting a modulus that can be factored into a product of relatively prime integers: $n = 21,600 = 2^5 3^3 5^2$. In this case the factors are $2^5 = 32$, $3^3 = 27$, and $5^2 = 25$. They need not be powers of primes, but it is easy to break the factors into this form to assure relatively prime numbers. To add in $\mathbb{Z}_n$, we need $\lceil \log_2 n \rceil = 15$ time units. Let $G = \mathbb{Z}_{32} \times \mathbb{Z}_{27} \times \mathbb{Z}_{25}$. The CRT gives us an isomorphism between $\mathbb{Z}_{21600}$ and G. The basic idea behind the fast adder, illustrated in Figure 14.1.3, is to make use of this isomorphism. The notation `x += a` is interpreted as the instruction to add the value of `a` to the variable `x`.

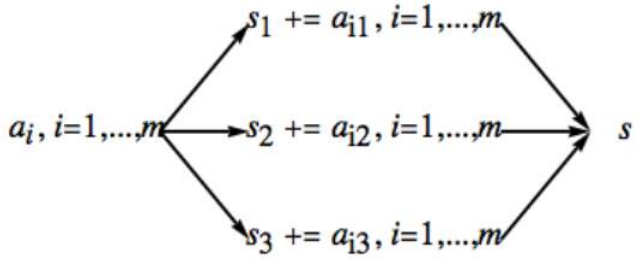


Figure 14.1.3: Fast Adder Scheme

Assume we have several integers $a_1, \ldots, a_m$ to be added. Here, we assume $m = 20$. We compute the sum `s` to compare our result with this true sum.

```
a=[1878,1384,84,2021,784,1509,1740,1201,2363,1774,
   1865,33,1477,894,690,520,198,1349,1278,650]
s =0
for t in a:
    s+=t
s
```

Although our sum is an integer calculation, we will put our calculation in the context of the integers modulo 21600. The isomophism from $\mathbb{Z}_{21600}$ into $G = \mathbb{Z}_{32} \times \mathbb{Z}_{27} \times \mathbb{Z}_{25}$ is defined in Sage as `theta`. In addition we demonstrate that the operations in these groups are preserved by `theta`.

```
G=cartesian_product([Integers(32),Integers(27),Integers(25)])
def theta(x):
    return G((x%32,x%27,x%25))
```

```
[theta(1878)+theta(1384),theta(1878+1384)]
```

We initialize the sums in each factor of the range of `theta` to zero and decompose each summand t into a triple $\theta(t) = (t_1, t_2, t_3) \in G$.

```
sum=G((0,0,0))
for t in a:
    sum+=theta(t)
sum
```

Addition in G can be done in parallel so that each new subtotal in the form of the triple (s_1, s_2, s_3) takes only as long to compute as it takes to add in the largest modulus, $\log_2 32 = 5$ time units, if calculations are done in parallel. By the time rule that we have established, the addition of 20 numbers can be done in $20 \cdot 5 = 100$ time units, as opposed to $20 \cdot 15 = 300$ time units if we do the calculations in $\mathbb{Z}_{21600}$. However the result is a triple in G. The function that performs the inverse of `theta` is built into most mathematics programs, including Sage. In Sage the function is `crt` . We use this function to compute the inverse of our triple, which is an element of $\mathbb{Z}_{21600}$. The result isn't the true sum because the modulus 21600 is not large enough. However, we verify that our result is congruent to the true sum modulo 21600.

```
isum=crt([12,13,17],[32,27,25])
[isum,(s-isum)%(21600)]
```

In order to get the true sum from our scheme, the modulus would need to be increased by moving from 21600 to, for example, $21600 * 23 = 496800$. Mapping into the new group, $G = \mathbb{Z}_{32} \times \mathbb{Z}_{27} \times \mathbb{Z}_{25} \times \mathbb{Z}_{23}$ will take slightly longer, as will the inversion process with `crt` , but adding the summands that are in the form of quadruples can be done with no additional time.

The computation of $\theta^{-1}(s_1, s_2, s_3)$ that is done by the Sage function `crt` can be accomplished in a variety of ways. All of them ultimately are simplified by the fact that θ^{-1} is also an isomorphism. One approach is to use the isomorphism property to realize that the value of $\theta^{-1}(s_1, s_2, s_3)$ is $s_1\theta^{-1}(1,0,0) + s_2\theta^{-1}(0,1,0) + s_3\theta^{-1}(0,0,1)$. The arithmetic in this expression is in the domain of θ and is more time consuming, but it need only be done once. This is why the fast adder is only practical in situations where many additions must be performed to get a single sum.

The inverse images of the "unit vectors" can be computed ahead of time.

```
u=[crt([1,0,0],[32,27,25]),
   crt([0,1,0],[32,27,25]),crt([0,0,1],[32,27,25])]
u
```

The result we computed earlier can be computed directly by in the larger modulus.

```
(7425*12 + 6400*13+ 7776* 17)%21600
```

To further illustrate the potential of fast adders, consider increasing the modulus to $n = 2^5 3^3 5^2 7^2 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \approx 3.1 \times 10^{21}$. Each addition using the usual modulo n addition with full adders would take 72 time units. By decomposing each summand into 15-tuples according to the CRT, the time is reduced to $\lceil \log_2 49 \rceil = 6$ time units per addition.

14.1.1: Exercises

Exercise 14.1.1

What generators besides 1 does $[\mathbb{Z}; +]$ have?

Answer

The only other generator is -1.

Exercise 14.1.2

Suppose $[G;*]$ is a cyclic group with generator g. If you build a graph of with vertices from the elements of G and edge set $E=\{(a,g*a)\mid a\in G\}$, what would the graph look like? If G is a group of even order, what would a graph with edge set $E'=\{(a,g^2*a)\mid a\in G\}$ look like?

Exercise 14.1.3

Prove that if $|G|>2$ and G is cyclic, G has at least two generators.

Answer

If $|G|=m$, $m>2$, and $G=\langle a\rangle$, then a, $a^2,\ldots,a^{m-1}$, $a^m=e$ are distinct elements of G. Furthermore, $a^{-1}=a^{m-1}\neq a$, If $1\leq k\leq m$, a^{-1} generates a^k:

$$\begin{aligned}\left(a^{-1}\right)^{m-k}&=\left(a^{m-1}\right)^{m-k}\\&=a^{m^2-m-mk+k}\\&=\left(a^m\right)^{m-k-1}*a^k\\&=e*a^k=a^k\end{aligned}$$

Similarly, if G is infinite and $G=\langle a\rangle$, then a^{-1} generates G.

Exercise 14.1.4

If you wanted to list the generators of $\mathbb{Z}_n$ you would only have to test the first $n/2$ positive integers. Why?

Exercise 14.1.5

Which of the following groups are cyclic? Explain.

a. $[\mathbb{Q};+]$
b. $[\mathbb{R}^+;\cdot]$
c. $[6\mathbb{Z};+]$ where $6\mathbb{Z}=\{6n|n\in\mathbb{Z}\}$
d. $\mathbb{Z}\times\mathbb{Z}$
e. $\mathbb{Z}_2\times\mathbb{Z}_3\times\mathbb{Z}_{25}$

Answer

a. No. Assume that $q\in\mathbb{Q}$ generates $\mathbb{Q}$. Then $\langle q\rangle=\{nq:n\in\mathbb{Z}\}$. But this gives us at most integer multiples of q, not every element in $\mathbb{Q}$.
b. No. Similar reasoning to part a.
c. Yes. 6 is a generator of $6\mathbb{Z}$.
d. No.
e. Yes, $(1,1,1)$is a generator of the group.

Exercise 14.1.6

For each group and element, determine the order of the cyclic subgroup generated by the element:

a. $\mathbb{Z}_{25}$, 15
b. $\mathbb{Z}_4\times\mathbb{Z}_9$, $(2,6)$ (apply Exercise 14.1.8)
c. $\mathbb{Z}_{64}$, 2

Exercise 14.1.7

How can Theorem 14.1.4be applied to list the generators of $\mathbb{Z}_n$? What are the generators of $\mathbb{Z}_{25}$? Of $\mathbb{Z}_{256}$?

Answer

Theorem 14.1.4implies that a generates $\mathbb{Z}_n$ if and only if the greatest common divisor of n and a is 1. Therefore the list of generators of $\mathbb{Z}_n$ are the integers in $\mathbb{Z}_n$ that are relatively prime to n. The generators of $\mathbb{Z}_{25}$ are all of the nonzero elements except 5, 10, 15, and 20. The generators of $\mathbb{Z}_{256}$ are the odd integers in $\mathbb{Z}_{256}$ since 256 is 2^8.

Exercise 14.1.8

Prove that if the greatest common divisor of n and m is 1, then (1, 1) is a generator of $\mathbb{Z}_n \times \mathbb{Z}_m$, and hence, $\mathbb{Z}_n \times \mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{nm}$.

Exercise 14.1.9

a. Illustrate how the fast adder can be used to add the numbers 21, 5, 7, and 15 using the isomorphism between $\mathbb{Z}_{77}$ and $\mathbb{Z}_7 \times \mathbb{Z}_{11}$.
b. If the same isomorphism is used to add the numbers 25, 26, and 40, what would the result be, why would it be incorrect, and how would the answer differ from the answer in part a?

Answer

a. $\theta : \mathbb{Z}_{77} \to \mathbb{Z}_7 \times \mathbb{Z}_{11}$ maps the given integers as follows:

$$\begin{array}{rcl} 21 & \to & (0,10) \\ 5 & \to & (5,5) \\ 7 & \to & (0,7) \\ 15 & \to & \underline{(1,4)} \\ \text{sum} = 48 & \leftarrow & (6,4) = \text{ sum} \end{array}$$

The final sum, 48, is obtained by using the facts that $\theta^{-1}(1,0) = 22$ and $\theta^{-1}(0,1) = 56$

$$\begin{aligned} \theta^{-1}(6,4) = 6 \times_{77} \theta^{-1}(1,0) + 4 \times_{77} \theta^{-1}(0,1) & \\ = 6 \times_{77} 22 +_{77} 4 \times_{77} 56 & \\ = 55 +_{77} 70 & \\ = 48 & \end{aligned}.$$

b. Using the same isomorphism:

$$\begin{array}{rcl} 25 & \to & (4,3) \\ 26 & \to & (5,4) \\ 40 & \to & (5,7) \\ & & \text{sum} = (0,3) \end{array}$$

$$\begin{aligned} \theta^{-1}(0,3) &= 3 \times_{77} \theta^{-1}(0,1) \\ &= 3 \times_{77} 56 \\ &= 14 \end{aligned}.$$

The actual sum is 91. Our result is incorrect, since 91 is not in $\mathbb{Z}_{77}$. Notice that 91 and 14 differ by 77. Any error that we get using this technique will be a multiple of 77.

Exercise 14.1.10

Prove that if G is a cyclic group of order n with generator a, and $p, q \in \{0, 1, \ldots, n-1\}$, then $(p+q)a = (p +_n q)\, a$.

14.2: Cosets and Factor Groups

Consider the group $[\mathbb{Z}_{12}; +_{12}]$. As we saw in the previous section, we can picture its cyclic properties with the string art of Figure 15.1.1. Here we will be interested in the non-generators, like 3. The solid lines in Figure 14.2.1 show that only one-third of the tacks have been reached by starting at zero and jumping to every third tack. The numbers of these tacks correspond to $\langle 3 \rangle = \{0, 3, 6, 9\}$.

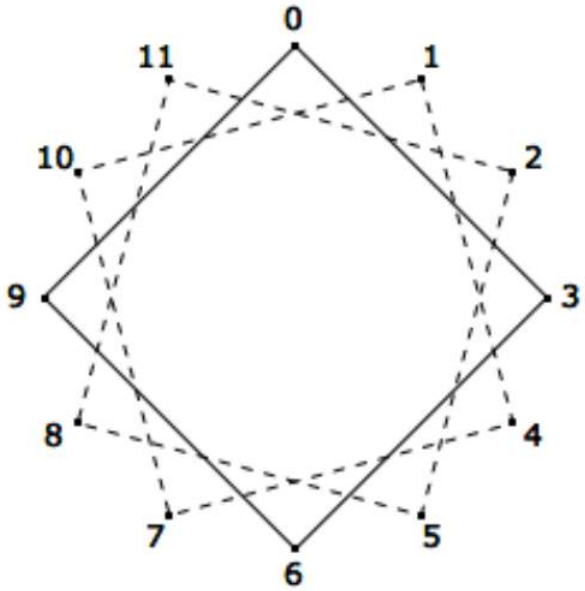


Figure 14.2.1: "String art" cosets

What happens if you start at one of the unused tacks and again jump to every third tack? The two broken paths on Figure 14.2.1 show that identical squares are produced. The tacks are thus partitioned into very similar subsets. The subsets of $\mathbb{Z}_{12}$ that they correspond to are $\{0, 3, 6, 9\}, \{1, 4, 7, 10\}$,and $\{2, 5, 8, 11\}$.These subsets are called cosets. In particular, they are called cosets of the subgroup $\{0, 3, 6, 9\}$.We will see that under certain conditions, cosets of a subgroup can form a group of their own. Before pursuing this example any further we will examine the general situation.

Definition 14.2.1: Coset

If $[G; *]$ is a group, $H \leq G$ and $a \in G$, the left coset of H generated by a is

$$a * H = \{a * h | h \in H\}$$

and the right coset of H generated by a is

$$H * a = \{h * a | h \in H\}.$$

Note 14.2.1

a. H itself is both a left and right coset since $e * H = H * e = H$.
b. If G is abelian, $a * H = H * a$ and the left-right distinction for cosets can be dropped. We will normally use left coset notation in that situation.

Definition 14.2.2: Cost Representative

Any element of a coset is called a representative of that coset.

One might wonder whether a is in any way a special representative of $a * H$ since it seems to define the coset. It is not, as we shall see.

Remark 14.2.1: A Duality Principle

A duality principle can be formulated concerning cosets because left and right cosets are defined in such similar ways. Any theorem about left and right cosets will yield a second theorem when "left" and "right" are exchanged for "right" and "left."

Theorem 14.2.1

If $b \in a * H$, then $a * H = b * H$, and if $b \in H * a$, then $H * a = H * b$.

Proof

In light of the remark above, we need only prove the first part of this theorem. Suppose that $x \in a * H$. We need only find a way of expressing x as "b times an element of H." Then we will have proven that $a * H \subseteq b * H$. By the definition of $a * H$, since b and x are in $a * H$, there exist h_1 and h_2 in H such that $b = a * h_1$ and $x = a * h_2$. Given these two equations, $a = bh_1^{-1}$ and

$$x = a * h_2 = (b * h_1^{-1}) * h_2 = b * (h_1^{-1} * h_2)$$

Since $h_1, h_2 \in H$, $h_1^{-1} * h_2 \in H$, and we are done with this part of the proof. In order to show that $b * H \subseteq a * H$, one can follow essentially the same steps, which we will let the reader fill in.

Example 14.2.1

In Figure 14.2.1, you can start at either 1 or 7 and obtain the same path by taking jumps of three tacks in each step. Thus,

$$1 +_{12} \{0, 3, 6, 9\} = 7 +_{12} \{0, 3, 6, 9\} = \{1, 4, 7, 10\}.$$

The set of left (or right) cosets of a subgroup partition a group in a special way:

Theorem 14.2.2: Cosets Partition a Group

If $[G; *]$ is a group and $H \leq G$, the set of left cosets of H is a partition of G. In addition, all of the left cosets of H have the same cardinality. The same is true for right cosets.

Proof

That every element of G belongs to a left coset is clear because $a \in a * H$ for all $a \in G$. If $a * H$ and $b * H$ are left cosets, we will prove that they are either equal or disjoint. If $a * H$ and $b * H$ are not disjoint, $a * H \cap b * H$ is nonempty and some element $c \in G$ belongs to the intersection. Then by Theorem 14.2.1, $c \in a * H \Rightarrow a * H = c * H$ and $c \in b * H \Rightarrow b * H = c * H$. Hence $a * H = b * H$.

We complete the proof by showing that each left coset has the same cardinality as H. To do this, we simply observe that if $a \in G$, $\rho : H \to a * H$ defined by $\rho(h) = a * h$ is a bijection and hence $|H| = |a * H|$. We will leave the proof of this statement to the reader.

The function ρ has a nice interpretation in terms of our opening example. If $a \in \mathbb{Z}_{12}$, the graph of $\{0, 3, 6, 9\}$is rotated $(30a)^\circ$ to coincide with one of the three cosets of $\{0, 3, 6, 9\}$.

Corollary 14.2.1: A Coset Counting Formula

If $|G| < \infty$ and $H \leq G$, the number of distinct left cosets of H equals $\frac{|G|}{|H|}$. For this reason we use G/H to denote the set of left cosets of H in G

Proof

This follows from the partitioning of G into equal sized sets, one of which is H.

Example 14.2.2

The set of integer multiples of four, $4\mathbb{Z}$, is a subgroup of $[\mathbb{Z};+]$. Four distinct cosets of $4\mathbb{Z}$ partition the integers. They are $4\mathbb{Z}$, $1+4\mathbb{Z}$, $2+4\mathbb{Z}$, and $3+4\mathbb{Z}$, where, for example, $1+4\mathbb{Z}=\{1+4k|k\in\mathbb{Z}\}$. $4\mathbb{Z}$ can also be written $0+4\mathbb{Z}$.

Convention 14.2.1: Distinguished Representatives

Although we have seen that any representative can describe a coset, it is often convenient to select a distinguished representative from each coset. The advantage to doing this is that there is a unique name for each coset in terms of its distinguished representative. In numeric examples such as the one above, the distinguished representative is usually the smallest nonnegative representative. Remember, this is purely a convenience and there is absolutely nothing wrong in writing $-203+4\mathbb{Z}$, $5+4\mathbb{Z}$, or $621+4\mathbb{Z}$ in place of $1+4\mathbb{Z}$ because $-203,5,621\in 1+4\mathbb{Z}$.

Before completing the main thrust of this section, we will make note of a significant implication of Theorem 14.2.2 Since a finite group is divided into cosets of a common size by any subgroup, we can conclude:

Theorem 14.2.3: Lagrange's Theorem

The order of a subgroup of a finite group must divide the order of the group.

One immediate implication of Lagrange's Theorem is that if p is prime, $\mathbb{Z}_p$ has no proper subgroups.

We will now describe the operation on cosets which will, under certain circumstances, result in a group. For most of this section, we will assume that G is an abelian group. This is one sufficient (but not necessary) condition that guarantees that the set of left cosets will form a group.

Definition 14.2.3: Operation on Cosets

Let C and D be left cosets of H, a subgroup of G with representatives c and d, respectively. Then

$$C\otimes D=(c*H)\otimes(d*H)=(c*d)*H$$

The operation $\otimes$ is called the operation induced on left cosets by $*$.

In Theorem 14.2.4, later in this section, we will prove that if G is an abelian group, $\otimes$ is indeed an operation. In practice, if the group G is an additive group, the symbol $\otimes$ is replaced by $+$, as in the following example.

Example 14.2.3: Computing with Cosets of $4\mathbb{Z}$

Consider the cosets described in Example 14.2.2 For brevity, we rename $0+4\mathbb{Z}$, $1+4\mathbb{Z}$, $2+4\mathbb{Z}$, and $3+4\mathbb{Z}$ with the symbols $\bar{0}$, $\bar{1}$, $\bar{2}$, and $\bar{3}$. Let's do a typical calculation, $\bar{1}+\bar{3}$. We will see that the result is always going to be $\bar{0}$, no matter what representatives we select. For example, $9\in\bar{1}$, $7\in\bar{3}$, and $9+7=16\in\bar{0}$. Our choice of the representatives $\bar{1}$ and $\bar{3}$ were completely arbitrary.

In general, $C\otimes D$ can be computed in many ways, and so it is necessary to show that the choice of representatives does not affect the result. When the result we get for $C\otimes D$ is always independent of our choice of representatives, we say that "$\otimes$ is well defined." Addition of cosets is a well-defined operation on the left cosets of $4\mathbb{Z}$ and is summarized in the following table. Do you notice anything familiar?

$\otimes$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Example 14.2.4: Cosets of the Integers in the Group of Real Numbers

Consider the group of real numbers, $[\mathbb{R};+]$, and its subgroup of integers, $\mathbb{Z}$. Every element of $\mathbb{R}/\mathbb{Z}$ has the same cardinality as $\mathbb{Z}$. Let $s,t\in\mathbb{R}$. $s\in t+\mathbb{Z}$ if s can be written $t+n$ for some $n\in\mathbb{Z}$. Hence s and t belong to the same coset if they differ by an integer. (See Exercise $14.2.6$ for a generalization of this fact.)

Now consider the coset $0.25+\mathbb{Z}$. Real numbers that differ by an integer from 0.25 are $1.25, 2.25, 3.25, \ldots$ and $-0.75, -1.75, -2.75, \ldots$ If any real number is selected, there exists a representative of its coset that is greater than or equal to 0 and less than 1. We will call that representative the distinguished representative of the coset. For example, 43.125 belongs to the coset represented by 0.125; $-6.382+\mathbb{Z}$ has 0.618 as its distinguished representative. The operation on $\mathbb{R}/\mathbb{Z}$ is commonly called addition modulo 1. A few typical calculations in $\mathbb{R}/\mathbb{Z}$ are

$$\begin{gathered}(0.1+\mathbb{Z})+(0.48+\mathbb{Z})=0.58+\mathbb{Z}\\(0.7+\mathbb{Z})+(0.31+\mathbb{Z})=0.01+\mathbb{Z}\\-(0.41+\mathbb{Z})=-0.41+\mathbb{Z}=0.59+\mathbb{Z}\\\text{and in general, } -(a+\mathbb{Z})=(1-a)+\mathbb{Z}\end{gathered}.$$

Example 14.2.5: Cosets in a Direct Product

Consider $F=(\mathbb{Z}_4\times\mathbb{Z}_2)/H$, where $H=\{(0,0),(0,1)\}$. Since $\mathbb{Z}_4\times\mathbb{Z}_2$ is of order 8, each element of F is a coset containing two ordered pairs. We will leave it to the reader to verify that the four distinct cosets are $(0,0)+H$, $(1,0)+H$, $(2,0)+H$ and $(3,0)+H$. The reader can also verify that F is isomorphic to $\mathbb{Z}_4$, since F is cyclic. An educated guess should give you a generator.

Example 14.2.6

Consider the group ${\mathbb{Z}_2}^4=\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$. Let H be $\langle(1,0,1,0)\rangle$, the cyclic subgroup of ${\mathbb{Z}_2}^4$ generate by (1,0,1,0). Since

$$(1,0,1,0)+(1,0,1,0)=(1+_2 1, 0+_2 0, 1+_2 1, 0+_2 0)=(0,0,0,0)$$

the order of H is 2 and , ${\mathbb{Z}_2}^4/H$ has $|\mathbb{Z}_2^4/H|=\frac{|\mathbb{Z}_2^4|}{|H|}=\frac{16}{2}=8$ elements. A typical coset is

$$C=(0,1,1,1)+H=\{(0,1,1,1),(1,1,0,1)\}$$

Note that since $2(0,1,1,1)=(0,0,0,0), 2C=C\otimes C=H,$ the identity for the operation on ${\mathbb{Z}_2}^4/H$. The orders of non-identity elements of this factor group are all 2, and it can be shown that the factor group is isomorphic to ${\mathbb{Z}_2}^3$.

Theorem 14.2.4: Coset Operation is Well-Defined (Abelian Case)

If G is an abelian group, and $H\leq G,$ the operation induced on cosets of H by the operation of G is well defined.

Proof

Suppose that a, b, and a', b'. are two choices for representatives of cosets C and D. That is to say that $a,a'\in C$, $b,b'\in D$. We will show that $a*b$ and $a'*b'$ are representatives of the same coset. Theorem 14.2.1 implies that $C=a*H$ and $D=b*H,$ thus we have $a'\in a*H$ and $b'\in b*H$. Then there exists $h_1,h_2\in H$ such that $a'=a*h_1$ and $b'=b*h_2$ and so

$$a'*b'=(a*h_1)*(b*h_2)=(a*b)*(h_1*h_2)$$

by various group properties and the assumption that G is abelian, which lets us reverse the order in which b and h_1 appear in the chain of equalities. This last expression for $a'*b'$ implies that $a'*b'\in(a*b)*H$ since $h_1*h_2\in H$ because H is a subgroup of G. Thus, we get the same coset for both pairs of representatives.

Theorem 14.2.5

Let G be a group and $H \leq G$. If the operation induced on left cosets of H by the operation of G is well defined, then the set of left cosets forms a group under that operation.

Proof

Let C_1, C_2, and C_3 be the left cosets with representatives r_1, r_2, and r_3, respectively. The values of $C_1 \otimes (C_2 \otimes C_3)$ and $(C_1 \otimes C_2) \otimes C_3$ are determined by $r_1 * (r_2 * r_3)$ and $(r_1 * r_2) * r_3$, respectively. By the associativity of $*$ in G, these two group elements are equal and so the two coset expressions must be equal. Therefore, the induced operation is associative. As for the identity and inverse properties, there is no surprise. The identity coset is H, or $e * H$, the coset that contains G's identity. If C is a coset with representative a; that is, if $C = a * H$, then C^{-1} is $a^{-1} * H$.

$$(a * H) \otimes \left(a^{-1} * H\right) = \left(a * a^{-1}\right) * H = e * H = \text{ identity coset.}$$

Definition 14.2.4: Factor Group

Let G be a group and $H \leq G$. If the set of left cosets of H forms a group, then that group is called the factor group of "G modulo H." It is denoted G/H.

Note 14.2.2

If G is abelian, then every subgroup of G yields a factor group. We will delay further consideration of the non-abelian case to Section 15.4.

Remark 14.2.2: On Notation

It is customary to use the same symbol for the operation of G/H as for the operation on G. The reason we used distinct symbols in this section was to make the distinction clear between the two operations.

14.2.1: Exercises

Exercise 14.2.1

Consider $\mathbb{Z}_{10}$ and the subsets of $\mathbb{Z}_{10}$, $\{0,1,2,3,4\}$ and $\{5,6,7,8,9\}$. Why is the operation induced on these subsets by modulo 10 addition not well defined?

Answer

An example of a valid correct answer: Call the subsets A and B respectively. If we choose $0 \in A$ and $5 \in B$ we get $0 +_{10} 5 = 5 \in B$. On the other hand, if we choose $3 \in A$ and $8 \in B$, we get $3 +_{10} 8 = 1 \in A$. Therefore, the induced operation is not well defined on $\{A, B\}$.

Exercise 14.2.2

Can you think of a group G, with a subgroup H such that $|H| = 6$ and $|G/H| = 6$? Is your answer unique?

Exercise 14.2.3

For each group and subgroup, what is G/H isomorphic to?

a. $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ and $H = \langle (2,0) \rangle$. Compare to Example 14.2.5
b. $G = [\mathbb{C}; +]$ and $H = \mathbb{R}$.
c. $G = \mathbb{Z}_{20}$ and $H = \langle 8 \rangle$.

Answer

a. The four distinct cosets in G/H are $H=\{(0,0),(2,0)\}, (1,0)+H=\{(1,0),(3,0)\}, (0,1)+H=\{(0,1),(2,1)\}$, and $(1,1)+H=\{(1,1),(3,1)\}$. None of these cosets generates G/H; therefore G/H is not cyclic. Hence G/H must be isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2$.
b. The factor group is isomorphic to $[\mathbb{R};+]$. Each coset of $\mathbb{R}$ is a line in the complex plane that is parallel to the x-axis: $\tau:\mathbb{C}/\mathbb{R}\to\mathbb{R},$ where $T(\{a+bi\mid a\in\mathbb{R}\})=b$ is an isomorphism.
c. $\langle 8\rangle=\{0,4,8,12,16\}\Rightarrow|\mathbb{Z}_{20}/\langle 8\rangle|=4$. The four cosets are: $\bar{0}$, $\bar{1}$, $\bar{2}$, and $\bar{3}$. 1 generates all four cosets. The factor group is isomorphic to $[\mathbb{Z}_4;+_4]$ because $\bar{1}$ is a generator.

Exercise 14.2.4

For each group and subgroup, what is G/H isomorphic to?

a. $G=\mathbb{Z}\times\mathbb{Z}$ and $H=\{(a,a)|a\in\mathbb{Z}\}$.
b. $G=[\mathbb{R}^*;\cdot]$ and $H=\{1,-1\}$.
c. $G={\mathbb{Z}_2}^5$ and $H=\langle(1,1,1,1,1)\rangle$.

Exercise 14.2.5

Assume that G is a group, $H\leq G,$ and $a,b\in G$. Prove that $a*H=b*H$ if and only if $b^{-1}*a\in H$.

Answer

$$\begin{aligned} a*H=b*H &\Leftrightarrow a\in bH \\ &\Leftrightarrow a=b*h \text{ for some } h\in H \\ &\Leftrightarrow b^{-1}*a=h \text{ for some } h\in H \\ &\Leftrightarrow b^{-1}*a\in H \end{aligned}$$

Exercise 14.2.6

a. Real addition modulo r, $r>0,$ can be described as the operation induced on cosets of $\langle r\rangle$ by ordinary addition. Describe a system of distinguished representatives for the elements of $\mathbb{R}/\langle r\rangle$.
b. Consider the trigonometric function sine. Given that $\sin(x+2\pi k)=\sin x$ for all $x\in\mathbb{R}$ and $k\in\mathbb{Z},$ show how the distinguished representatives of $\mathbb{R}/\langle 2\pi\rangle$ can be useful in developing an algorithm for calculating the sine of a number.

Exercise 14.2.7

Complete the proof of Theorem 14.2.2by proving that if $a\in G,$ $\rho:H\to a*H$ defined by $\rho(h)=a*h$ is a bijection.

14.3: Permutation Groups

14.3.1: Symmetric Groups

At the risk of boggling the reader's mind, we will now examine groups whose elements are functions. Recall that a permutation on a set A is a bijection from A into A. Suppose that $A = \{1, 2, 3\}$. There are $3! = 6$ different permutations on A. We will call the set of all 6 permutations S_3. They are listed in the following table. The matrix form for describing a function on a finite set is to list the domain across the top row and the image of each element directly below it. For example $r_1(1) = 2$.

Table 14.3.1: Elements of S_3

$i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

The operation that will give $\{i, r_1, r_2, f_1, f_2, f_3\}$ a group structure is function composition. Consider the "product" $r_1 \circ f_3$:

$$\begin{aligned} r_1 \circ f_3(1) &= r_1\left(f_3(1)\right) = r_1(2) = 3 \\ r_1 \circ f_3(2) &= r_1\left(f_3(2)\right) = r_1(1) = 2 \\ r_1 \circ f_3(3) &= r_1\left(f_3(3)\right) = r_1(3) = 1 \end{aligned} .$$

The images of 1, 2, and 3 under $r_1 \circ f_3$ and f_2 are identical. Thus, by the definition of equality for functions, we can say $r_1 \circ f_3 = f_2$. The complete table for the operation of function composition is given in Table 14.3.2

Table 14.3.2: Operation Table for S_3

$\circ$	i	r_1	r_2	f_1	f_2	f_3
i	i	r_1	r_2	f_1	f_2	f_3
r_1	r_1	r_2	i	f_3	f_1	f_2
r_2	r_2	i	r_1	f_2	f_3	f_1
f_1	f_1	f_2	f_3	i	r_1	r_2
f_2	f_2	f_3	f_1	r_2	i	r_1
f_3	f_3	f_1	f_2	r_1	r_2	i

List 14.3.1

We don't even need the table to verify that we have a group. Based on the following observations, the set of all permutations on any finite set will be a group.

1. Function composition is always associative.
2. The identity for the group is i. If g is any one of the permutations on A and $x \in A$,

$$(g \circ i)(x) = g(i(x)) = g(x) \qquad (i \circ g)(x) = i(g(x)) = g(x)$$

   Therefore $g \circ i = i \circ g = g$.
3. A permutation, by definition, is a bijection. In Chapter 7 we proved that this implies that it must have an inverse and the inverse itself is a bijection and hence a permutation. Hence all elements of S_3 have an inverse in S_3. If a permutation is displayed in matrix form, its inverse can be obtained by exchanging the two rows and rearranging the columns so that the top row is in order. The first step is actually sufficient to obtain the inverse, but the sorting of the top row makes it easier to recognize the inverse.

   For example, let's consider a typical permutation on $\{1, 2, 3, 4, 5\}$, $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$.

$$f^{-1} = \begin{pmatrix} 5 & 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}.$$

Note 14.3.1

From Table 14.3.2, we can see that S_3 is non-abelian. Remember, non-abelian is the negation of abelian. The existence of two elements that don't commute is sufficient to make a group non-abelian. In this group, r_1 and f_3 is one such pair: $r_1 \circ f_3 = f_2$ while $f_3 \circ r_1 = f_1$, so $r_1 \circ f_3 \neq f_3 \circ r_1$. Caution: Don't take this to mean that every pair of elements has to have this property. There are several pairs of elements in S_3 that do commute. In fact, the identity, i, must commute with everything. Also every element must commute with its inverse.

Definition 14.3.1: Symmetric Group

Let A be a nonempty set. The set of all permutations on A with the operation of function composition is called the symmetric group on A, denoted S_A.

The cardinality of a finite set A is more significant than the elements, and we will denote by S_n the symmetric group on any set of cardinality n, $n \geq 1$.

Example 14.3.1: The Significance of S_3

Our opening example, S_3, is the smallest non-abelian group. For that reason, all of its proper subgroups are abelian: in fact, they are all cyclic. Figure 14.3.1 shows the Hasse diagram for the subgroups of S_3.

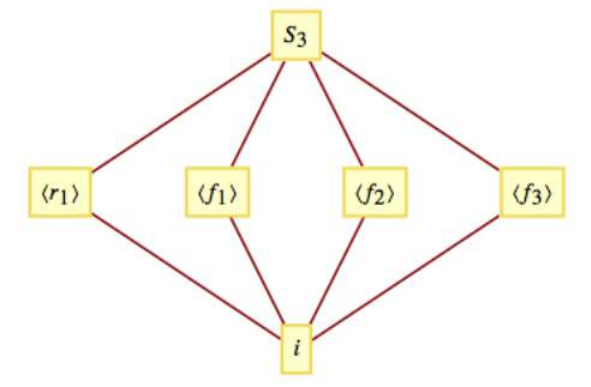


Figure 14.3.1: Lattice diagram of subgroups of S_3

Example 14.3.2: Smallest Symmetric Groups

The only abelian symmetric groups are S_1 and S_2 , with 1 and 2 elements, respectively. The elements of S_2 are $i = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ and $\alpha = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$. S_2 is isomorphic to $\mathbb{Z}_2$.

Theorem 14.3.1

For $n \geq 1$, $|S_n| = n!$ and for $n \geq 3$, S_n is non-abelian.

Proof

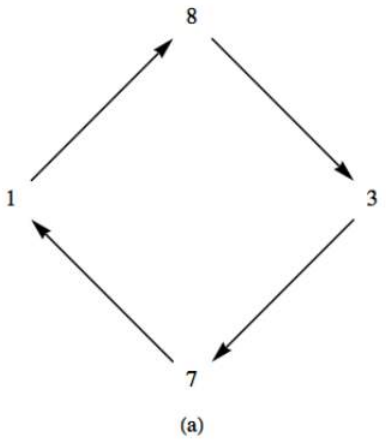
The first part of the theorem follows from the extended rule of products (see Chapter 2). We leave the details of proof of the second part to the reader after the following hint. Consider f in S_n where $f(1) = 2$, $f(2) = 3$, $f(3) = 1$, and $f(j) = j$ for $3 < j \leq n$. Therefore the cycle representation of f is $(1, 2, 3)$. Now define g in a similar manner so that when you compare $f(g(1))$ and $g(f(1))$ you get different results.

14.3.2: Cycle Notation

A second way of describing a permutation is by means of cycles, which we will introduce first with an example. Consider $f \in S_8$ defined using the now-familiar matrix notation:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 7 & 6 & 5 & 4 & 1 & 3 \end{pmatrix}$$

Consider the images of 1 when f is applied repeatedly. The images $f(1)$, $f(f(1))$, $f(f(f(1)))$, ... are $8, 3, 7, 1, 8, 3, 7, \ldots$.In Figure 14.3.2(a), this situation is represented by a graph with vertices 1, 8, 3, and 7 and shows that the values that you get by repeatedly applying f cycle through those values. This is why we refer to this part of f as a cycle of length 4. Of course starting at 8, 3, or 7 also produces the same cycle with only the starting value changing.



(8,3,7,1)
(3,7,1,8)
(7,1,8,3)
or
(1,8,3,7)

(b)

Figure 14.3.2: Representations of a cycle of length 4

Figure 14.3.2(a) illustrates how the cycle can be represented in a visual manner, but it is a bit awkward to write. Part (b) of the figure presents a more universally recognized way to write a cycle. In (b), a cycle is represented by a list where the image of any number in the list is its successor. In addition, the last number in the list has as its image the first number.

The other elements of the domain of f are never reached if you start in the cycle $(1, 8, 3, 7)$,and so looking at the images of these other numbers will produce numbers that are disjoint from the set $\{1, 8, 3, 7\}$.The other disjoint cycles of f are (2), (4, 6), and (5). We can express f as a product of disjoint cycles: $f = (1, 8, 3, 7)(2)(4, 6)(5)$or $f = (1, 8, 3, 7)(4, 6)$,where the absence of 2 and 5 implies that $f(2) = 2$ and $f(5) = 5$.

Note 14.3.2: Disjoint Cycles

We say that two cycles are disjoint if no number appears in both cycles, as is the case in our expressions for f above. Disjoint cycles can be written in any order. Thus, we could also say that $f = (4, 6)(1, 8, 3, 7)$.

Note 14.3.3: Composition of Permutations

We will now consider the composition of permutations written in cyclic form by an example. Suppose that $f = (1, 8, 3, 7)(4, 6)$and $g = (1, 5, 6)(8, 3, 7, 4)$are elements of S_8. To calculate $f \circ g$, we start with simple concatenation:

$$f \circ g = (1, 8, 3, 7)(4, 6)(1, 5, 6)(8, 3, 7, 4) \tag{14.3.1}$$

Although this is a valid expression for $f \circ g$, our goal is to express the composition as a product of disjoint cycles as f and g were individually written. We will start by determining the cycle that contains 1. When combining any number of cycles, they are always read from right to left, as with all functions. The first cycle in (14.3.1) does not contain 1; thus we move on to the second. The image of 1 under that cycle is 5. Now we move on to the next cycle, looking for 5, which doesn't appear. The fourth cycle does not contain a 5 either; so $f \circ g(1) = 5$.

At this point, we would have written "$f \circ g = (1, 5$" on paper. We repeat the steps to determine $f \circ g(5)$. This time the second cycle of (14.3.1) moves 5 to 6 and then the third cycle moves 6 to 4. Therefore, $f \circ g(5) = 4$. We continue until the cycle (1, 5, 4, 3) is completed by determining that $f \circ g(3) = 1$. The process is then repeated starting with any number that does not appear in the cycle(s) that have already been completed.

The final result for our example is $f \circ g = (1, 5, 4, 3)(6, 8, 7)$. Since $f(2) = 2$ and $g(2) = 2$, $f \circ g(2) = 2$ and we need not include the one-cycle (2) in the final result, although it can be included.

Example 14.3.3: Some Compositions

a. $(1,2,3,4)(1,2,3,4) = (1,3)(2,4)$
b. $(1,4)(1,3)(1,2) = (1,2,3,4)$.

Notice that cyclic notation does not indicate the set which is being permuted. The examples above could be in S_5, where the image of 5 is 5. This ambiguity is usually overcome by making the context clear at the start of a discussion.

Definition 14.3.2: Transposition

A transposition is a cycle of length 2.

Observation 14.3.1: About Transpositions

$f = (1,4)$ and $g = (4,5)$ are transpositions in S_5. However, $f \circ g = (1,4,5)$ and $g \circ f = (1,5,4)$ are not transpositions; thus, the set of transpositions is not closed under composition. Since $f^2 = f \circ f$ and $g^2 = g \circ g$ are both equal to the identity permutation, f and g are their own inverses. In fact, every transposition is its own inverse.

Theorem 14.3.2: Decomposition into Cycles

Every cycle of length greater than 2 can be expressed as a product of transpositions.

Proof

We need only indicate how the product of transpositions can be obtained. It is easy to verify that a cycle of length k, $(a_1, a_2, a_3, \ldots, a_k)$, is equal to the following product of $k-1$ transpositions:

$$(a_1, a_k) \cdots (a_1, a_3)\,(a_1, a_2)$$

Of course, a product of cycles can be written as a product of transpositions just as easily by applying the rule above to each cycle. For example,

$$(1,3,5,7)(2,4,6) = (1,7)(1,5)(1,3)(2,6)(2,4)$$

Unlike the situation with disjoint cycles, we are not free to change the order of these transpositions.

14.3.3: Parity of Permutations and the Alternating Group

A decomposition of permutations into transpositions makes it possible to classify then and identify an important family of groups.

The proofs of the following theorem appears in many abstract algebra texts.

Theorem 14.3.3

Every permutation on a finite set can be expressed as the product of an even number of transpositions or an odd number of transpositions, but not both.

Theorem 14.3.3 suggests that S_n can be partitioned into its "even" and "odd" elements. For example, the even permutations of S_3 are i, $r_1 = (1,2,3) = (1,3)(1,2)$ and $r_2 = (1,3,2) = (1,2)(1,3)$. They form a subgroup, $\{i, r_1, r_2\}$ of S_3.

In general:

Definition 14.3.3: The Alternating Group

Let $n \geq 2$. The set of even permutations in S_n is a proper subgroup of S_n called the alternating group on $\{1,2,\ldots,n\}$, denoted A_n.

We justify our statement that A_n is a group:

Theorem 14.3.4

Let $n \geq 2$. The alternating group is indeed a group and has order $\frac{n!}{2}$.

Proof

In this proof, the symbols s_i and t_i stand for transpositions and p, q are even nonnegative integers. If $f, g \in A_n$, we can write the two permutations as products of even numbers of transpositions, $f = s_1 s_2 \cdots s_p$ and $g = t_1 t_2 \cdots t_q$. Then

$$f \circ g = s_1 s_2 \cdots s_p t_1 t_2 \cdots t_q$$

Since $p + q$ is even, $f \circ g \in A_n$, and A_n is closed with respect to function composition. With this, we have proven that A_n is a subgroup of S_n by Theorem 11.5.2.

To prove the final assertion, let B_n be the set of odd permutations and let $\tau = (1, 2)$. Define $\theta : A_n \to B_n$ by $\theta(f) = f \circ \tau$. Suppose that $\theta(f) = \theta(g)$. Then $f \circ \tau = g \circ \tau$ and by the right cancellation law, $f = g$. Hence, θ is an injection. Next we show that θ is also a surjection. If $h \in B_n$, h is the image of an element of A_n. Specifically, h is the image of $h \circ \tau$.

$$\begin{aligned} \theta(h \circ \tau) &= (h \circ \tau) \circ \tau \\ &= h \circ (\tau \circ \tau) \quad \text{Why?} \\ &= h \circ i \quad \text{Why?} \\ &= h \end{aligned}$$

Since θ is a bijection, $|A_n| = |B_n| = \frac{n!}{2}$.

Example 14.3.4: The Sliding Tile Puzzle

Consider the sliding-tile puzzles pictured in Figure 14.3.3. Each numbered square is a tile and the dark square is a gap. Any tile that is adjacent to the gap can slide into the gap. In most versions of this puzzle, the tiles are locked into a frame so that they can be moved only in the manner described above. The object of the puzzle is to arrange the tiles as they appear in Configuration (a). Configurations (b) and (c) are typical starting points. We propose to show why the puzzle can be solved starting with (b), but not with (c).

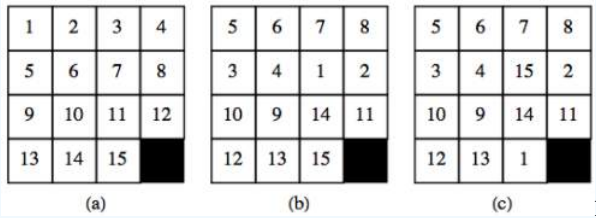


Figure 14.3.3: Configurations of the sliding tile puzzle

We will associate a change in the configuration of the puzzle with an element of S_{16}. Imagine that a tile numbered 16 fills in the gap. For any configuration of the puzzle, the identity i, is the function that leave the configurate "as is." In general, if $f \in S_{16}$, and $1 \leq k \leq 16$, $f(k)$ is the position to which the tile in position k is moved by f that appears in the position of k in configuration (a). If we call the functions that, starting with configuration (a), result in configurations (b) and (c) by the names f_1 and f_2, respectively,

$$f_1 = (1, 5, 3, 7)(2, 6, 4, 8)(9, 10)(11, 14, 13, 12)(15)(16)$$

and

$$f_2 = (1, 5, 3, 7, 15)(2, 6, 4, 8)(9, 10)(11, 14, 13, 12)(16).$$

How can we interpret the movement of one tile as a permutation? Consider what happens when the 12 tile of i slides into the gap. The result is a configuration that we would interpret as $(12, 16)$, a single transposition. Now if we slide the 8 tile into the 12 position, the result is or $(8, 16, 12)$. Hence, by "exchanging" the tiles 8 and 16, we have implemented the function $(8, 12)(12, 16) = (8, 12, 16)$.

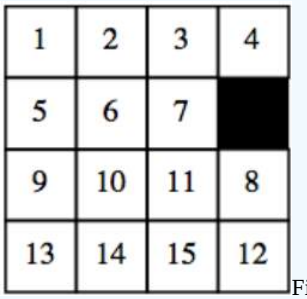


Figure 14.3.4: The configuration $(8, 12, 16)$

Every time you slide a tile into the gap, the new permutation is a transposition composed with the old permutation. Now observe that to start with initial configuration and terminate after a finite number of moves with the gap in its original position, you must make an even number of moves. Thus, configuration corresponding any permutation that leaves 16 fixed cannot be solved if the permutation is odd. Note that f_2 is an odd permutation; thus, Puzzle (c) can't be solved. The proof that all even permutations, such as f_1, can be solved is left to the interested reader to pursue.

14.3.4: Dihedral Groups

Observation 14.3.2: Realization of Groups

By now we've seen several instances where a group can appear through an isomorphic copy of itself in various settings. The simplest such example is the cyclic group of order 2. When this group is mentioned, we might naturally think of the group $[\mathbb{Z}_2; +_2]$, but the groups $[\{-1, 1\}; \cdot]$ and $[S_2; \circ]$ are isomorphic to it. None of these groups are necessarily more natural or important than the others. Which one you use depends on the situation you are in and all are referred to as ***realizations*** of the cyclic group of order 2. The next family of groups we will study, the dihedral groups, has two natural realizations, first as permutations and second as geometric symmetries.

The family of dihedral groups is indexed by the positive integers greater than or equal to 3. For $k \geq 3$, $\mathcal{D}_k$ will have $2k$ elements. We first describe the elements and the operation on them using geometry.

We can describe $\mathcal{D}_n$ in terms of symmetries of a regular n-gon ($n = 3$: equilateral triangle, $n = 4$: square, $n = 5$: regular pentagon,. . .). Here we will only concentrate on the case of $\mathcal{D}_4$. If a square is fixed in space, there are several motions of the square that will, at the end of the motion, not change the apparent position of the square. The actual changes in position can be seen if the corners of the square are labeled. In Figure 14.3.5, the initial labeling scheme is shown, along with the four axes of symmetry of the square.

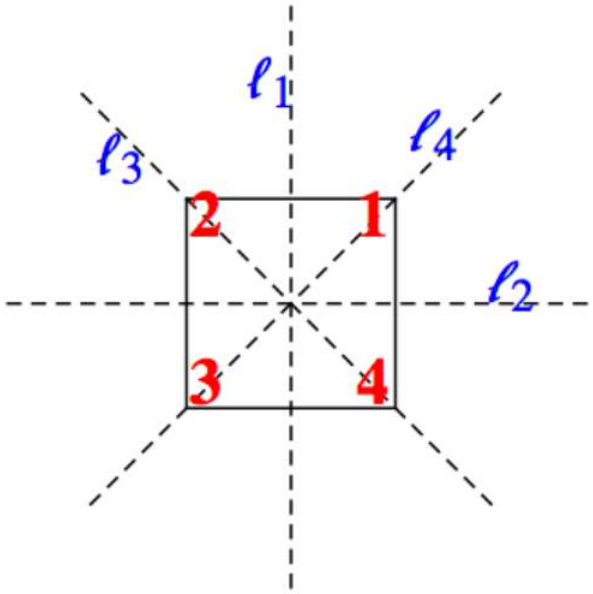


Figure 14.3.5: Axes of symmetry of the square

It might be worthwhile making a square like this with a sheet of paper. Be careful to label the back so that the numbers match the front. Two motions of the square will be considered equivalent if the square is in the same position after performing either motion. There are eight distinct motions. The first four are 0°, 90°, 180°, and 270° clockwise rotations of the square, and the other four are the 180° flips along the axes l_1, l_2, l_3, and l_4. We will call the rotations i, r_1, r_2, and r_3, respectively, and the flips f_1, f_2, f_3, and f_4, respectively. Figure 14.3.6 illustrates r_1 and f_1. For future reference, we also include the permutations to which they correspond.

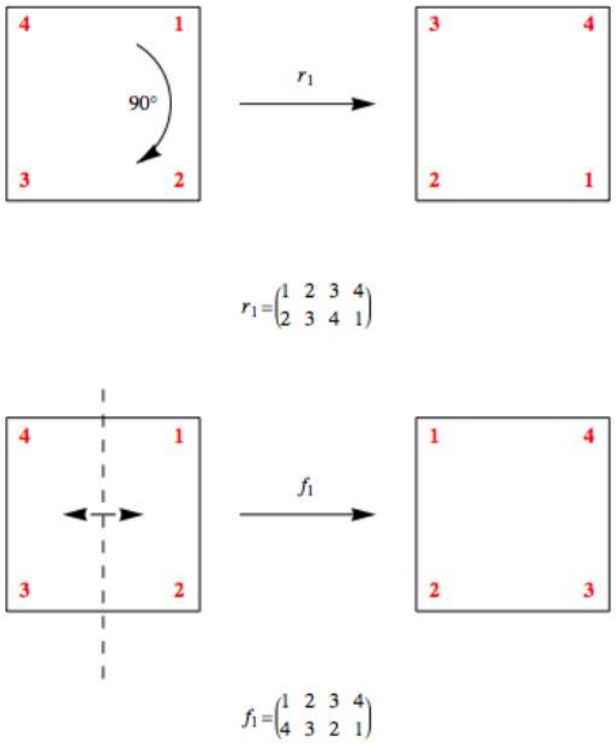


Figure 14.3.6: Two elements of $\mathcal{D}_4$

What is the operation on this set of symmetries? We will call the operation "followed by" and use the symbol $*$ to represent it. The operation will be to combine motions, applying motions from right to left, as with functions. We will illustrate how $*$ is computed by finding $r_1 * f_1$. Starting with the initial configuration, if you perform the f_1 motion, and then immediately perform r_1 on the result, we get the same configuration as if we just performed f_4, which is to flip the square along the line l_4. Therefore, $r_1 * f_1 = f_4$. An important observation is that $f_1 * r_1 \neq f_4$, meaning that this group is nonabelian. The reader is encouraged to verify this on their own.

We can also realize the dihedral groups as permutations. For any symmetric motion of the square we can associate with it a permutation. In the case of $\mathcal{D}_4$, the images of each of the numbers 1 through 4 are the positions on the square that each of the corners 1 through 4 are moved to. For example, since corner 4 moves to position 1 when you perform r_1, the corresponding function will map 4 to 1. In addition, 1 gets mapped to 2, 2 to 3 and 3 to 4. Therefore, r_1 is the cycle $(1, 2, 3, 4)$. The flip f_1 transposes two pairs of corners and corresponds to $(1, 4)(2, 3)$. If we want to combine these two permutations, using the same names as with motions, we get

$$r_1 \circ f_1 = (1, 2, 3, 4) \circ (1, 4)(2, 3) = (1)(2, 4)(3) = (2, 4)$$

Notice that this permutation corresponds with the flip f_4.

Although $\mathcal{D}_4$ isn't cyclic (since it isn't abelian), it can be generated from the two elements r_1 and f_1:

$$\mathcal{D}_4 = \langle r_1, f_1 \rangle = \left\{ i, r_1, {r_1}^2, {r_1}^3, f_1, r_1 \circ f_1, {r_1}^2 \circ f_1, {r_1}^3 \circ f_1 \right\}$$

It is quite easy to describe any of the dihedral groups in a similar fashion. Here is the formal definition

Definition 14.3.4: Dihedral Group

Let n be a positive integer greater than or equal to 3. If $r = (1, 2, \ldots, n)$, an n-cycle, and $f = (1, n)(2, n-1)\ldots$ Then

$$\mathcal{D}_n = \langle r, f \rangle = \left\{ i, r, r^2, \ldots, r^{n-1}, f, r \circ f, r^2 \circ f, \ldots, r^{n-1} \circ f \right\}$$

is the nth dihedral group.

Note 14.3.4: Caution

You might notice that we use a script D, $\mathcal{D}$, for the dihedral groups. Occasionally you might see an ordinary D in other sources for the dihedral groups. Don't confuse it with the set of divisors of n, which we denote by D_n. Normally the context of the discussion should make the meaning of D_n clear.

Example 14.3.5: A Letter-Facing Machine

An application of $\mathcal{D}_4$ is in the design of a letter-facing machine. Imagine letters entering a conveyor belt to be postmarked. They are placed on the conveyor belt at random so that two sides are parallel to the belt. Suppose that a postmarker can recognize a stamp in the top right corner of the envelope, on the side facing up. In Figure 14.3.7, a sequence of machines is shown that will recognize a stamp on any letter, no matter what position in which the letter starts. The letter P stands for a postmarker. The letters R and F stand for rotating and flipping machines that perform the motions of r_1 and f_1.

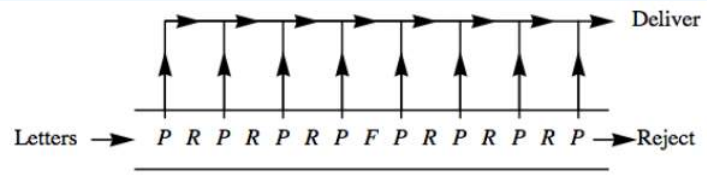


Figure 14.3.7: A letter facer

The arrows pointing up indicate that if a letter is postmarked, it is taken off the conveyor belt for delivery. If a letter reaches the end, it must not have a stamp. Letter-facing machines like this have been designed (see [16]). One economic consideration is that R-machines tend to cost more than F-machines. R-machines also tend to damage more letters. Taking these facts into consideration, the reader is invited to design a better letter-facing machine. Assume that R-machines cost \$800 and F-machines cost \$500. Be sure that all corners of incoming letters will be examined as they go down the conveyor belt.

14.3.5: Exercises

Exercise 14.3.1

Given $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, and $h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$, compute

a. $f \circ g$
b. $g \circ h$
c. $(f \circ g) \circ h$
d. $f \circ (g \circ h)$
e. h^{-1}
f. $h^{-1} \circ g \circ h$
g. f^{-1}

Answer

a. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$
b. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$

c. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$
d. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$
e. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$
f. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$
g. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

Exercise 14.3.2

Write f, g, and h from Exercise 14.3.1 as products of disjoint cycles and determine whether each is odd or even.

Exercise 14.3.3

Do the left cosets of $A_3 = \{i, r_1, r_2\}$ over S_3 form a group under the induced operation on left cosets of A_3? What about the left cosets of $\langle f_1 \rangle$?

Answer

S_3/A_3 is a group of order two. The operation on left cosets of $H = \langle f_1 \rangle$ is not well defined and so a group cannot be formed from left cosets of H.

Exercise 14.3.4

In its realization as permutations, the dihedral group $\mathcal{D}_3$ is equal to S_3. Can you give a geometric explanation why? Why isn't $\mathcal{D}_4$ equal to S_4?

Exercise 14.3.5

a. Complete the list of elements of $\mathcal{D}_4$ and write out a table for the group in its realization as symmetries.
b. List the subgroups of $\mathcal{D}_4$ in a lattice diagram. Are they all cyclic? To what simpler groups are the subgroups of $\mathcal{D}_4$ isomorphic?

Answer

$\mathcal{D}_4 = \{i, r, r^2, r^3, f_1, f_2, f_3, f_4\}$ Where i is the identity function, $r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, and

$$f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$
$$f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

The operation table for the group is

$\circ$	i	r	r^2	r^3	f_1	f_2	f_3	f_4
i	i	r	r^2	r^3	f_1	f_2	f_3	f_4
r	r	r^2	r^3	i	f_4	f_3	f_1	f_2
r^2	r^2	r^3	i	r	f_2	f_1	f_4	f_3
r^3	r^3	i	r	r^2	f_3	f_4	f_2	f_1
f_1	f_1	f_3	f_2	f_4	i	r^2	r	r^3
f_2	f_2	f_4	f_1	f_3	r^2	i	r^3	r
f_3	f_3	f_2	f_4	f_1	r^3	r	i	r^2
f_4	f_4	f_1	f_3	f_2	r	r^3	r^2	i

A lattice diagram of its subgroups is

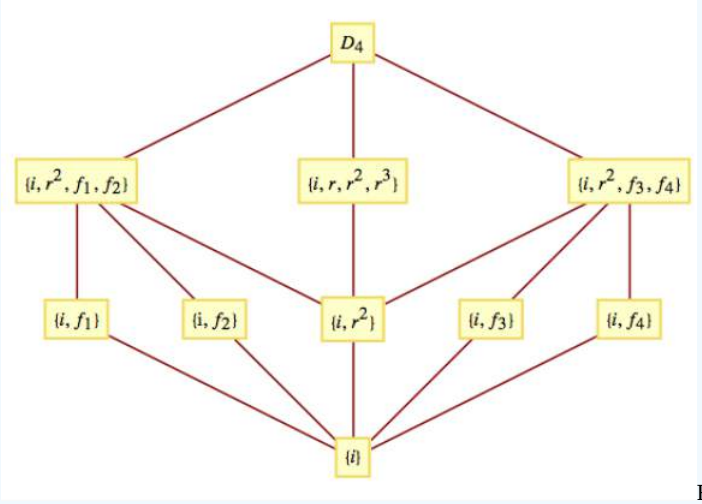


Figure 14.3.8: Subgroups of $\mathcal{D}_4$

All proper subgroups are cyclic except $\{i, r^2, f_1, f_2\}$ and $\{i, r^2, f_3, f_4\}$. Each 2-element subgroup is isomorphic to $\mathbb{Z}_2$; $\{i, r, r^2, r^3\}$ is isomorphic to $\mathbb{Z}_4$; and $\{i, r^2, f_1, f_2\}$ and $\{i, r^2, f_3, f_4\}$ are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exercise 14.3.6

Design a better letter-facing machine (see Example 14.3.5). How can you verify that a letter-facing machine does indeed check every corner of a letter? Can it be done on paper without actually sending letters through it?

Exercise 14.3.7

Prove by induction that if $r \geq 1$ and each t_i, is a transposition, then $(t_1 \circ t_2 \circ \cdots \circ t_r)^{-1} = t_r \circ \cdots \circ t_2 \circ t_1$

Answer

One solution is to cite Exercise 11.3.3 at the end of Section 11.3. It can be directly applied to this problem. An induction proof of the problem at hand would be almost identical to the proof of the more general statement.

$(t_1 t_2 \cdots t_r)^{-1} = t_r^{-1} \cdots t_2^{-1} t_1^{-1}$ by Exercise 11.3.3 of Section 11.3

$= t_r \cdots t_2 t_1$ since each transposition inverts itself. ■

Exercise 14.3.8

How many elements are there in $\mathcal{D}_5$? Describe them geometrically.

Exercise 14.3.9

Complete the proof of Theorem 14.3.1.

Answer

Part I: That $|S_k| = k!$ follows from the Rule of Products.

Part II: Let f be the function defined on $\{1, 2, \ldots, n\}$by $f(1) = 2$, $f(2) = 3$, $f(3) = 1$, and $f(j) = j$ for $4 \leq j \leq n$; and let g be defined by $g(1) = 1$, $g(2) = 3$, $g(3) = 2$, and $g(j) = j$ for $4 \leq j \leq n$. Note that f and g are elements of S_n. Next, $(f \circ g)(1) = f(g(1)) = f(1) = 2$, while $(g \circ f)(1) = g(f(1)) = g(2) = 3$, hence $f \circ g \neq g \circ f$ and S_n is non-abelian for any $n \geq 3$.

Exercise 14.3.10

How many left cosets does A_n, $n \geq 2$ have?

Exercise 14.3.11

Prove that $f \circ r = r^{n-1} \circ f$ in $\mathcal{D}_n$.

Exercise 14.3.12

a. Prove that the tile puzzles corresponding to $A_{16} \cap \{f \in S_{16} | f(16) = 16\}$ are solvable.
b. If $f(16) \neq 16$, how can you determine whether f's puzzle is solvable?

Exercise 14.3.13

a. Prove that S_3 is isomorphic to R_3, the group of 3×3 rook matrices (see Section 11.2 exercises).
b. Prove that for each $n \geq 2$, R_n is isomorphic to S_n.

Answer

a. Both groups are non-abelian and of order 6; so they must be isomorphic, since only one such group exists up to isomorphism. The function $\theta : S_3 \to R_3$ defined by

$$\begin{aligned} \theta(i) &= I & \theta(f_1) &= F_1 \\ \theta(r_1) &= R_1 & \theta(f_2) &= F_2 \\ \theta(r_2) &= R_2 & \theta(f_3) &= F_3 \end{aligned}$$

is an isomorphism,

b. Recall that since every function is a relation, it is natural to translate functions to Boolean matrices. Suppose that $f \in S_n$. We will define its image, $\theta(f)$, by

$$\theta(f)_{kj} = 1 \Leftrightarrow f(j) = k$$

That θ is a bijection follows from the existence of θ^{-1}. If A is a rook matrix,

$$\begin{aligned} \theta^{-1}(A)(j) = k &\Leftrightarrow \text{The 1 in column } j \text{ of } A \text{ appears in row } k \\ &\Leftrightarrow A_{kj} = 1 \end{aligned}$$

For $f, g \in S_n$,

$$\begin{aligned} \theta(f \circ g)_{kj} = 1 &\Leftrightarrow (f \circ g)(j) = k \\ &\Leftrightarrow \exists l \text{ such that } g(j) = l \text{ and } f(l) = k \\ &\Leftrightarrow \exists l \text{ such that } \theta(g)_{lj} = 1 \text{ and } \theta(f)_{kl} = 1 \\ &\Leftrightarrow (\theta(f)\theta(g))_{kj} = 1 \end{aligned}$$

Therefore, θ is an isomorphism.

14.4: Normal Subgroups and Group Homomorphisms

Our goal in this section is to answer an open question from earlier in this chapter and introduce a related concept. The question is: When are left cosets of a subgroup a group under the induced operation? This question is open for non-abelian groups. Now that we have some examples to work with, we can try a few experiments.

14.4.1: Normal Subgroups

Example 14.4.1: Cosets of A_3

We have seen that $A_3 = \{i, r_1, r_2\}$ is a subgroup of S_3, and its left cosets are A_3 itself and $B_3 = \{f_1, f_2, f_3\}$. Whether $\{A_3, B_3\}$ is a group boils down to determining whether the induced operation is well defined. Consider the operation table for S_3 in Figure 14.4.1.

$\circ$	i	r_1	r_2	f_1	f_2	f_3
i	i	r_1	r_2	f_1	f_2	f_3
r_1	r_1	r_2	i	f_3	f_1	f_2
r_2	r_2	i	r_1	f_2	f_3	f_1
f_1	f_1	f_2	f_3	i	r_1	r_2
f_2	f_2	f_3	f_1	r_2	i	r_1
f_3	f_3	f_1	f_2	r_1	r_2	i

Figure 14.4.1: Operation table for S_3

We have shaded in all occurrences of the elements of B_3 in gray. We will call these elements the gray elements and the elements of A_3 the white ones.

Now consider the process of computing the coset product $A_3 \circ B_3$. The "product" is obtained by selecting one white element and one gray element. Note that white "times" gray is always gray. Thus, $A_3 \circ B_3$ is well defined. Similarly, the other three possible products are well defined. The table for the factor group S_3/A_3 is

$\circ$	A_3	B_3
A_3	A_3	B_3
B_3	B_3	A_3

Clearly, S_3/A_3 is isomorphic to $\mathbb{Z}_2$. Notice that A_3 and B_3 are also the right cosets of A_3. This is significant.

Example 14.4.2: Cosets of Another Subgroup of S_3

Now let's try the left cosets of $\langle f_1 \rangle$ in S_3. There are three of them. Will we get a complicated version of $\mathbb{Z}_3$? The left cosets are $C_0 = \langle f_1 \rangle$, $C_1 = r_1 \langle f_1 \rangle = \{r_1, f_3\}$, and $C_2 = r_2 \langle f_1 \rangle = \{r_2, f_2\}$.

The reader might be expecting something to go wrong eventually, and here it is. To determine $C_1 \circ C_2$ we can choose from four pairs of representatives:

$$r_1 \in C_1, r_2 \in C_2 \longrightarrow r_1 \circ r_2 = i \in C_0$$
$$r_1 \in C_1, f_2 \in C_2 \longrightarrow r_1 \circ f_2 = f \in C_0$$
$$f_3 \in C_1, r_2 \in C_2 \longrightarrow f_3 \circ r_2 = f_2 \in C_2$$
$$f_3 \in C_1, f_2 \in C_2 \longrightarrow f_3 \circ f_2 = r_2 \in C_2$$

This time, we don't get the same coset for each pair of representatives. Therefore, the induced operation is not well defined and no factor group is produced.

Observation 14.4.1

This last example changes our course of action. If we had gotten a factor group from $\{C_0, C_1, C_2\}$, we might have hoped to prove that every collection of left cosets forms a group. Now our question is: How can we determine whether we will get a factor group? Of course, this question is equivalent to: When is the induced operation well defined? There was only one step in the proof of Theorem 15.2.4, where we used the fact that G was abelian. We repeat the equations here:

$$a' * b' = (a * h_1) * (b * h_2) = (a * b) * (h_1 * h_2)$$

since G was abelian.

The last step was made possible by the fact that $h_1 * b = b * h_1$. As the proof continued, we used the fact that $h_1 * h_2$ was in H and so $a' * b'$ is $(a * b) * h$ for some h in H. All that we really needed in the "abelian step" was that $h_1 * b = b * (\text{something in } H) = b * h_3$. Then, since H is closed under G's operation, $h_3 * h_2$ is an element of H. The consequence of this observation is that we define a certain kind of subgroup that guarantees that the inducted operation is well-defined.

Definition 14.4.1: Normal Subgroup

If G is a group, $H \leq G$, then H is a normal subgroup of G, denoted $H \triangleleft G$, if and only if every left coset of H is a right coset of H; i. e. $a * H = H * a \quad \forall a \in G$

Theorem 14.4.1

If $H \leq G$, then the operation induced on left cosets of H by the operation of G is well defined if and only if any one of the following conditions is true:

a. H is a normal subgroup of G.
b. If $h \in H$, $a \in G$, then there exists $h' \in H$ such that $h * a = a * h'$.
c. If $h \in H$, $a \in G$, then $a^{-1} * h * a \in H$.

Proof

We leave the proof of this theorem to the reader.

Be careful, the following corollary is not an "...if and only if..." statement.

Corollary 14.4.1

If $H \leq G$, then the operation induced on left cosets of H by the operation of G is well defined if either of the following two conditions is true.

a. G is abelian.
b. $|H| = \frac{|G|}{2}$.

Example 14.4.3: A Non-Normal Subgroup

The right cosets of $\langle f_1 \rangle \leq S_3$ are $\{i, f_1\}$, $\{r_1 f_2\}$, and $\{r_2, f_3\}$. These are not the same as the left cosets of $\langle f_1 \rangle$. In addition, $f_2{}^{-1} f_1 f_2 = f_2 f_1 f_2 = f_3 \notin \langle f_1 \rangle$. Thus, $\langle f_1 \rangle$ is not normal.

The improper subgroups $\{e\}$ and G of any group G are normal subgroups. $G/\{e\}$ is isomorphic to G. All other normal subgroups of a group, if they exist, are called ***proper normal subgroups***.

Example 14.4.4

By Condition b of Corollary 14.4.1, A_n is a normal subgroup of S_n and S_n/A_n is isomorphic to $\mathbb{Z}_2$.

Example 14.4.5: Subgroups of A_5

A_5, a group in its own right with 60 elements, has many proper subgroups, but none are normal. Although this could be done by brute force, the number of elements in the group would make the process tedious. A far more elegant way to approach the verification of this statement is to use the following fact about the cycle structure of permutations. If $f \in S_n$ is a permutation with a certain cycle structure, $\sigma_1 \sigma_2 \cdots \sigma_k$, where the length of σ_i is ℓ_i, then for any $g \in S_n$, $g^{-1} \circ f \circ g$, which is the conjugate of f by g, will have a cycle structure with exactly the same cycle lengths. For example if we take $f = (1,2,3,4)(5,6)(7,8,9) \in S_9$ and conjugate by $g = (1,3,5,7,9)$,

$$\begin{aligned} g^{-1} \circ f \circ g &= (1,9,7,5,3) \circ (1,2,3,4)(5,6)(7,8,9) \circ (1,3,5,7,9) \\ &= (1,4,9,2)(3,6)(5,8,7) \end{aligned}$$

Notice that the condition for normality of a subgroup H of G is that the conjugate of any element of H by an element of G must be remain in H.

To verify that A_5 has no proper normal subgroups, you can start by cataloging the different cycle structures that occur in A_5 and how many elements have those structures. Then consider what happens when you conjugate these different cycle structures with elements of A_5. An outline of the process is in the exercises.

Example 14.4.6

Let G be the set of two by two invertible matrices of real numbers. That is,

$$G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc \neq 0 \right\}$$

We saw in Chapter 11 that G is a group with matrix multiplication.

This group has many subgroups, but consider just two: $H_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \neq 0 \right\}$ and $H_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| ad \neq 0 \right\}$. It is fairly simple to apply one of the conditions we have observed for normallity that H_1 a normal subgroup of G, while H_2 is not normal in G.

14.4.2: Homomorphisms

Think of the word isomorphism. Chances are, one of the first images that comes to mind is an equation something like

$$\theta(x * y) = \theta(x) \diamond \theta(y)$$

An isomorphism must be a bijection, but the equation above is the algebraic property of an isomorphism. Here we will examine functions that satisfy equations of this type.

Definition 14.4.2: Homomorphism

Let $[G; *]$ and $[G'; \diamond]$ be groups. $\theta : G \to G'$ is a homomorphism if $\theta(x * y) = \theta(x) \diamond \theta(y)$ for all $x, y \in G$.

Many homomorphisms are useful since they point out similarities between the two groups (or, on the universal level, two algebraic systems) involved.

Example 14.4.7: Decreasing Modularity

Define $\alpha : \mathbb{Z}_6 \to \mathbb{Z}_3$ by $\alpha(n) = n \bmod 3$. Therefore, $\alpha(0) = 0$, $\alpha(1) = 1$, $\alpha(2) = 2$, $\alpha(3) = 1+1+1 = 0$, $\alpha(4) = 1$, and $\alpha(5) = 2$. If $n, m \in \mathbb{Z}_6$. We could actually show that α is a homomorphism by checking all $6^2 = 36$ different cases for the formula

$$\alpha(n +_6 m) = \alpha(n) +_3 \alpha(m) \tag{14.4.1}$$

but we will use a line of reasoning that generalizes. We have already encountered the Chinese Remainder Theorem, which implies that the function $\beta : \mathbb{Z}_6 \to \mathbb{Z}_3 \times \mathbb{Z}_2$ defined by $\beta(n) = (n \bmod 3, n \bmod 2)$. We need only observe that equating the first coordinates of both sides of the equation

$$\beta(n +_6 m) = \beta(n) + \beta(m) \tag{14.4.2}$$

gives us precisely the homomorphism property.

Theorem 14.4.2: Group Homomorphism Properties

If $\theta : G \to G'$ is a homomorphism, then:

a. $\theta(e) = \theta(\text{the identity of } G) = \text{the identity of } G' = e'$.
b. $\theta\left(a^{-1}\right) = \theta(a)^{-1}$ for all $a \in G$.
c. If $H \leq G$, then $\theta(H) = \{\theta(h) | h \in H\} \leq G'$.

Proof

a. Let a be any element of G. Then $\theta(a) \in G'$.

$$\begin{aligned} \theta(a) \diamond e' &= \theta(a) && \text{by the definition of } e' \\ &= \theta(a * e) && \text{by the definition of } e \\ &= \theta(a) \diamond \theta(e) && \text{by the fact that } \theta \text{ is a homomorphism} \end{aligned}$$

By cancellation, $e' = \theta(e)$.

b. Again, let $a \in G$. $e' = \theta(e) = \theta\left(a * a^{-1}\right) = \theta(a) \diamond \theta\left(a^{-1}\right)$. Hence, by the uniqueness of inverses, $\theta(a)^{-1} = \theta\left(a^{-1}\right)$.

c. Let $b_1, b_2 \in \theta(H)$. Then there exists $a_1, a_2 \in H$ such that $\theta(a_1) = b_1$, $\theta(a_2) = b_2$. Recall that a compact necessary and sufficient condition for $H \leq G$ is that $x * y^{-1} \in H$ for all $x, y \in H$. Now we apply the same condition in G':

$$\begin{aligned} b_1 \diamond {b_2}^{-1} &= \theta(a_1) \diamond \theta(a_2)^{-1} \\ &= \theta(a_1) \diamond \theta\left({a_2}^{-1}\right) \\ &= \theta\left(a_1 * {a_2}^{-1}\right) \in \theta(H) \end{aligned}$$

since $a_1 * {a_2}^{-1} \in H$, and so we can conclude that $\theta(H) \leq G'$.

Corollary 14.4.2

Since a homomorphism need not be a surjection and part (c) of Theorem 14.4.2is true for the case of $H = G$, the range of θ, $\theta(G)$, is a subgroup of G'

Example 14.4.8

If we define $\pi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\pi(n) = n + 4\mathbb{Z}$, then π is a homomorphism. The image of the subgroup $4\mathbb{Z}$ is the single coset $0 + 4\mathbb{Z}$, the identity of the factor group. Homomorphisms of this type are called natural homomorphisms. The following theorems will verify that π is a homomorphism and also show the connection between homomorphisms and normal subgroups. The reader can find more detail and proofs in most abstract algebra texts.

Theorem 14.4.3

If $H \triangleleft G$, then the function $\pi : G \to G/H$ defined by $\pi(a) = aH$ is a homomorphism.

Proof

We leave the proof of this theorem to the reader.

Definition 14.4.3: Natural Homomorphism

If $H \triangleleft G$, then the function $\pi : G \to G/H$ defined by $\pi(a) = aH$ is called the natural homomorphism.

Based on Theorem 14.4.3, every normal subgroup gives us a homomorphism. Next, we see that the converse is true.

Definition 14.4.4: Kernel of a Homomorphism

Let $\theta : G \to G'$ be a homomorphism, and let e and e' be the identities of G and G', respectively. The kernel of θ is the set $\ker\theta = \{a \in G \mid \theta(a) = e'\}$

Theorem 14.4.4

Let $\theta : G \to G'$ be a homomorphism from G into G'. The kernel of θ is a normal subgroup of G.

Proof

Let $K = \ker\theta$. We can see that K is a subgroup of G by letting $a, b \in K$ and verify that $a * b^{-1} \in K$ by computing $\theta(a * b^{-1}) = \theta(a) * \theta(b)^{-1} = e' * e'^{-1} = e'$. To prove normality, we let g be any element of G and $k \in K$. We compute $\theta(g * k * g^{-1})$ to verify that $g * k * g^{-1} \in K$.

$$\begin{aligned}\theta(g * k * g^{-1}) &= \theta(g) * \theta(k) * \theta(g^{-1}) \\ &= \theta(g) * \theta(k) * \theta(g)^{-1} \\ &= \theta(g) * e' * \theta(g)^{-1} \\ &= \theta(g) * \theta(g)^{-1} \\ &= e'\end{aligned}$$

Based on this most recent theorem, every homomorphism gives us a normal subgroup.

Theorem 14.4.5: Fundamental Theorem of Group Homomorphisms

Let $\theta : G \to G'$ be a homomorphism. Then $\theta(G)$ is isomorphic to $G/\ker\theta$.

Example 14.4.9

Define $\theta : \mathbb{Z} \to \mathbb{Z}_{10}$ by $\theta(n) = n \bmod 10$. The three previous theorems imply the following:

- $\pi : \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$ defined by $\pi(n) = n + 10\mathbb{Z}$ is a homomorphism.
- $\{n \in \mathbb{Z} | \theta(n) = 0\} = \{10n \mid n \in \mathbb{Z}\} = 10\mathbb{Z} \triangleleft \mathbb{Z}$.
- $\mathbb{Z}/10\mathbb{Z}$ is isomorphic to $\mathbb{Z}_{10}$.

Example 14.4.10

Let G be the same group of two by two invertible real matrices as in Example 14.4.6. Define $\Phi : G \to G$ by $\Phi(A) = \frac{A}{\sqrt{|\det A|}}$. We will let the reader verify that Φ is a homomorphism. The theorems above imply the following.

- $\ker \Phi = \{A \in G | \Phi(A) = I\} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}, a \neq 0 \right\} \triangleleft G$. This verifies our statement in Example 14.4.6. As in that example, let $\ker \Phi = H_1$.
- G/H_1 is isomorphic to $\{A \in G \mid \det A = 1\}$.
- $\pi : G \to G/H_1$ defined, naturally, by $\pi(A) = AH_1$ is a homomorphism.

For the remainder of this section, we will be examining certain kinds of homomorphisms that will play a part in our major application to homomorphisms, coding theory.

Example 14.4.11

Consider $\Phi : {\mathbb{Z}_2}^2 \to {\mathbb{Z}_2}^3$ defined by $\Phi(a,b) = (a, b, a +_2 b)$. If $(a_1, b_1), (a_2, b_2) \in {\mathbb{Z}_2}^2$,

$$\begin{aligned} \Phi\left((a_1, b_1) + (a_2, b_2)\right) &= \Phi\left(a_1 +_2 a_2, b_1 +_2 b_2\right) \\ &= \left(a_1 +_2 a_2, b_1 +_2 b_2, a_1 +_2 a_2 +_2 b_1 +_2 b_2\right) \\ &= (a_1, b_1, a_1 +_2 b_1) + (a_2, b_2, a_2 +_2 b_2) \\ &= \Phi\left(a_1, b_1\right) + \Phi\left(a_2, b_2\right) \end{aligned}$$

Since $\Phi(a,b)=(0,0,0)$ implies that $a = 0$ and $b = 0$, the kernel of Φ is $\{(0,0)\}$. By previous theorems, $\Phi\left({\mathbb{Z}_2}^2\right) = \{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\}$ is isomorphic to ${\mathbb{Z}_2}^2$.

We can generalize the previous example as follows: If $n, m \geq 1$ and A is an $m \times n$ matrix of 0's and 1's (elements of $\mathbb{Z}_2$), then $\Phi : {\mathbb{Z}_2}^m \to {\mathbb{Z}_2}^n$ defined by

$$\Phi\left(a_1, a_2, \ldots, a_m\right) = \left(a_1, a_2, \ldots, a_m\right) A$$

is a homomorphism. This is true because matrix multiplication is distributive over addition. The only new idea here is that computation is done in $\mathbb{Z}_2$. If $a = (a_1, a_2, \ldots, a_m)$ and $b = (b_1, b_2, \ldots, b_m)$, $(a+b)A = aA + bA$ is true by basic matrix laws. Therefore, $\Phi(a+b) = \Phi(a) + \Phi(b)$.

14.4.3: Exercises

Exercise 14.4.1

Which of the following functions are homomorphisms? What are the kernels of those functions that are homomorphisms?

a. $\theta_1 : \mathbb{R}^* \to \mathbb{R}^+$ defined by $\theta_1(a) = |a|$.

b. $\theta_2 : \mathbb{Z}_5 \to \mathbb{Z}_2$ where $\theta_2(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$.

c. $\theta_3 : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, where $\theta_3(a,b) = a + b$.

d. $\theta_4 : S_4 \to S_4$ defined by $\theta_4(f) = f \circ f = f^2$.

Answer

a. Yes, the kernel is $\{1, -1\}$

b. No, since $\theta_2\left(2 +_5 4\right) = \theta_2(1) = 1$, but $\theta_2(2) +_2 \theta_2(4) = 0 +_2 0 = 0$
A follow-up might be to ask what happens if 5 is replaced with some other positive integer in this part.

c. Yes, the kernel is $\{(a, -a) | a \in \mathbb{R}\}$

d. No. A counterexample, among many, would be to consider the two transpositions $t_1 = (1,3)$ and $t_2 = (1,2)$. Compare $\theta_4(t_1 \circ t_2)$ and $\theta_4(t_1) \circ \theta_4(t_2)$.

Exercise 14.4.2

Which of the following functions are homomorphisms? What are the kernels of those functions that are homomorphisms?

a. $\alpha_1 : M_{2\times 2}(\mathbb{R}) \to \mathbb{R}$, defined by $\alpha_1(A) = A_{11}A_{22} + A_{12}A_{21}$.
b. $\alpha_2 : (\mathbb{R}^*)^2 \to \mathbb{R}^*$ defined by $\alpha_2(a, b) = ab$.
c. $\alpha_3 : \{A \in M_{2\times 2}(\mathbb{R}) | \det A \neq 0\} \to \mathbb{R}^*$, where $\alpha_3(A) = \det A$.
d. $\alpha_4 : S_4 \to S_4$ defined by $\alpha_4(f) = f^{-1}$.

Exercise 14.4.3

Show that D_4 has one proper normal subgroup, but that $\langle (1, 4)(2, 3)\rangle$ is not normal.

Answer

$\langle r\rangle = \{i, r, r^2, r^3\}$ is a normal subgroup of D_4. To see you could use the table given in the solution of Exercise 15.3.5 of Section 15.3 and verify that $a^{-1}ha \in \langle r\rangle$ for all $a \in D_4$ and $h \in \langle r\rangle$. A more efficient approach is to prove the general theorem that if H is a subgroup G with exactly two distinct left cosets, than H is normal. $\langle f_1\rangle$ is not a normal subgroup of D_4. $\langle f_1\rangle = \{i, f_1\}$ and if we choose $a = r$ and $h = f_1$ then $a^{-1}ha = r^3 f_1 r = f_2 \notin \langle f_1\rangle$

Exercise 14.4.4

Prove that the function Φ in Example 14.4.10is a homomorphism.

Exercise 14.4.5

Define the two functions $\alpha : {\mathbb{Z}_2}^3 \to {\mathbb{Z}_2}^4$ and $\beta : {\mathbb{Z}_2}^4 \to \mathbb{Z}_2$ by $\alpha(a_1, a_2, a_3) = (a_1, a_2, a_3, a_1 +_2 a_2 +_2 a_3)$, and $\beta(b_1, b_2, b_3, b_4) = b_1 + b_2 + b_3 + b_4$ Describe the function $\beta \circ \alpha$. Is it a homomorphism?

Answer

$(\beta \circ \alpha)(a_1, a_2, a_3) = 0$ and so $\beta \circ \alpha$ is the trivial homomorphism, but a homomorphism nevertheless.

Exercise 14.4.6

Express Φ in Example 14.4.10in matrix form.

Exercise 14.4.7

Prove that if G is an abelian group, then $q(x) = x^2$ defines a homomorphism from G into G. Is q ever an isomorphism?

Answer

Let $x, y \in G$.

$$\begin{aligned} q(x * y) &= (x * y)^2 \\ &= x * y * x * y \\ &= x * x * y * y \quad \text{since } G \text{ is abelian} \\ &= x^2 * y^2 \\ &= q(x) * q(y) \end{aligned}$$

Hence, q is a homomorphism. In order for q to be an isomorphism, it must be the case that no element other than the identity is its own inverse.

$$\begin{aligned} x \in \text{Ker}(q) &\Leftrightarrow q(x) = e \\ &\Leftrightarrow x * x = e \\ &\Leftrightarrow x^{-1} = x \end{aligned}$$

Exercise 14.4.8

Prove that if $\theta : G \to G'$ is a homomorphism, and $H \triangleleft G$, then $\theta(H) \triangleleft \theta(G)$. Is it also true that $\theta(H) \triangleleft G'$?

Exercise 14.4.9

Prove that if $\theta : G \to G'$ is a homomorphism, and $H' \leq \theta(G)$, then $\theta^{-1}(H') = \{a \in G | \theta(a) \in H'\} \leq G$.

Answer

Proof: Recall that the inverse image of H' under θ is $\theta^{-1}(H') = \{g \in G | \theta(g) \in H'\}$.

Closure: Let $g_1, g_2 \in \theta^{-1}(H')$, then $\theta(g_1), \theta(g_2) \in H'$. Since H' is a subgroup of G',

$$\theta(g_1) \diamond \theta(g_2) = \theta(g_1 * g_2) \in H' \Rightarrow g_1 * g_2 \in \theta^{-1}(H')$$

Identity: By Theorem 14.4.2(a), $e \in \theta^{-1}(H')$.

Inverse: Let $a \in \theta^{-1}(H')$. Then $\theta(a) \in H'$ and by Theorem 14.4.2(b), $\theta(a)^{-1} = \theta\left(a^{-1}\right) \in H'$ and so $a^{-1} \in \theta^{-1}(H')$.

Exercise 14.4.10

Following up on Example 14.4.5, prove that A_5 is a simple group; i. e., it has no proper normal subgroups.

a. Make a list of the different cycle structures that occur in A_5 and how many elements have those structures.
b. Within each set of permutations with different cycle structures, identify which subsets are closed with respect to the conjugation operation. With this you will have a partition of A_5 into conjugate classes where for each class, C, $f, g \in C$ if and only if $\exists \phi \in A_5$ such that $\phi^{-1} \circ f \circ \phi = g$.
c. Use the fact that a normal subgroup of A_5 needs to be a union of conjugate classes and verify that no such union exists.

14.5: Coding Theory, Group Codes

14.5.1: Transmission Problem

In this section, we will introduce the basic ideas involved in coding theory and consider solutions of a coding problem by means of group codes.

Imagine a situation in which information is being transmitted between two points. The information takes the form of high and low pulses (for example, radio waves or electric currents), which we will label 1 and 0, respectively. As these pulses are sent and received, they are grouped together in blocks of fixed length. The length determines how much information can be contained in one block. If the length is r, there are 2^r different values that a block can have. If the information being sent takes the form of text, each block might be a character. In that case, the length of a block may be seven, so that $2^7 = 128$ block values can represent letters (both upper and lower case), digits, punctuation, and so on. During the transmission of data, noise can alter the signal so that what is received differs from what is sent. Figure $14.5.1$ illustrates the problem that can be encountered if information is transmitted between two points.

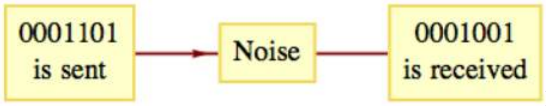


Figure 14.5.1: A noisy transmission

Noise is a fact of life for anyone who tries to transmit information. Fortunately, in most situations, we could expect a high percentage of the pulses that are sent to be received properly. However, when large numbers of pulses are transmitted, there are usually some errors due to noise. For the remainder of the discussion, we will make assumptions about the nature of the noise and the message that we want to send. Henceforth, we will refer to the pulses as bits.

We will assume that our information is being sent along a ***binary symmetric channel***. By this, we mean that any single bit that is transmitted will be received improperly with a certain fixed probability, p, independent of the bit value. The magnitude of p is usually quite small. To illustrate the process, we will assume that $p = 0.001$, which, in the real world, would be considered somewhat large. Since $1 - p = 0.999$, we can expect 99.9% of all bits to be properly received.

Suppose that our message consists of 3,000 bits of information, to be sent in blocks of three bits each. Two factors will be considered in evaluating a method of transmission. The first is the probability that the message is received with no errors. The second is the number of bits that will be transmitted in order to send the message. This quantity is called the rate of transmission:

$$\text{Rate} = \frac{\text{Message length}}{\text{Number of bits transmitted}}$$

As you might expect, as we devise methods to improve the probability of success, the rate will decrease.

Suppose that we ignore the noise and transmit the message without any coding. The probability of success is $0.999^{3000} = 0.0497124$. Therefore we only successfully receive the message in a totally correct form less than 5% of the time. The rate of $\frac{3000}{3000} = 1$ certainly doesn't offset this poor probability.

Our strategy for improving our chances of success will be to send an encoded message across the binary symmetric channel. The encoding will be done in such a way that small errors can be identified and corrected. This idea is illustrated in Figure $14.5.2$

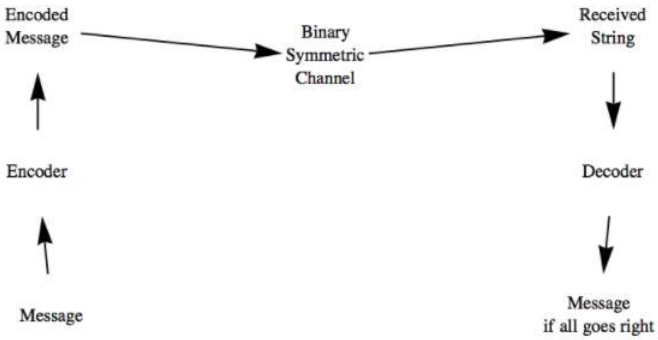


Figure 14.5.2: The Coding Process

In our examples, the functions that will correspond to our encoding and decoding devices will all be homomorphisms between Cartesian products of $\mathbb{Z}_2$.

14.5.2: Error Detection

Suppose that each block of three bits $a = (a_1, a_2, a_3)$ is encoded with the function $e : {\mathbb{Z}_2}^3 \to {\mathbb{Z}_2}^4$, where

$$e(a) = (a_1, a_2, a_3, a_1 +_2 a_2 +_2 a_3)$$

When the encoded block is received, the four bits will probably all be correct (they are correct approximately 99.6% of the time), but the added bit that is sent will make it possible to detect single errors in the block. Note that when $e(a)$ is transmitted, the sum of its components is $a_1 +_2 a_2 +_2 a_3 +_2 (a_1 +_2 a_2 +_2 a_3) = 0, \quad$ since $a_i + a_i = 0$ in $\mathbb{Z}_2$.

If any single bit is garbled by noise, the sum of the received bits will be 1. The last bit of $e(a)$ is called the parity bit. A parity error occurs if the sum of the received bits is 1. Since more than one error is unlikely when p is small, a high percentage of all errors can be detected.

At the receiving end, the decoding function acts on the four-bit block $b = (b_1, b_2, b_3, b_4)$ with the function $d : {\mathbb{Z}_2}^4 \to \mathbb{Z}_2^4$, where

$$d(b) = (b_1, b_2, b_3, b_1 +_2 b_2 +_2 b_3 +_2 b_4)$$

The fourth bit is called the parity-check bit. If no parity error occurs, the first three bits are recorded as part of the message. If a parity error occurs, we will assume that a retransmission of that block can be requested. This request can take the form of automatically having the parity-check bit of $d(b)$ sent back to the source. If 1 is received, the previous block is retransmitted; if 0 is received, the next block is sent. This assumption of two-way communication is significant, but it is desirable to make this coding system useful. It is reasonable to expect that the probability of a transmission error in the opposite direction is also 0.001. Without going into the details, we will report that the probability of success is approximately 0.990 and the rate is approximately 3/5. The rate includes the transmission of the parity-check bit to the source.

14.5.3: Error Correction

Next, we will consider a coding process that can correct errors at the receiving end so that only one-way communication is needed. Before we begin, recall that every element of ${\mathbb{Z}_2}^n$, $n \geq 1$, is its own inverse; that is, $-b = b$. Therefore, $a - b = a + b$.

Noisy three-bit message blocks are difficult to transmit because they are so similar to one another. If a and b are in ${\mathbb{Z}_2}^3$, their difference, $a +_2 b$, can be thought of as a measure of how close they are. If a and b differ in only one bit position, one error can change one into the other. The encoding that we will introduce takes a block $a = (a_1, a_2, a_3)$ and produces a block of length 6 called the ***code word*** of a. The code words are selected so that they are farther from one another than the messages are. In fact, each code word will differ from each other code word by at least three bits. As a result, any single error will not push a code word close enough to another code word to cause confusion. Now for the details.

Let $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$. We call G the generator matrix for the code, and let $a = (a_1, a_2, a_3)$ be our message.

Define $e : {\mathbb{Z}_2}^3 \to {\mathbb{Z}_2}^6$ by

$$e(a) = aG = (a_1, a_2, a_3, a_4, a_5, a_6)$$

where

$$\begin{aligned} a_4 &= a_1 +_2 a_2 \\ a_5 &= a_1 +_2 a_3 \\ a_6 &= a_2 +_2 a_3 \end{aligned}$$

Notice that e is a homomorphism. Also, if a and b are distinct elements of ${\mathbb{Z}_2}^3$, then $c = a + b$ has at least one coordinate equal to 1. Now consider the difference between $e(a)$ and $e(b)$:

$$\begin{aligned} e(a) + e(b) &= e(a + b) \\ &= e(c) \\ &= (d_1, d_2, d_3, d_4, d_5, d_6) \end{aligned}$$

Whether c has 1, 2, or 3 ones, $e(c)$ must have at least three ones. This can be seen by considering the three cases separately. For example, if c has a single one, two of the parity bits are also 1. Therefore, $e(a)$ and $e(b)$ differ in at least three bits.

Now consider the problem of decoding the code words. Imagine that a code word, $e(a)$, is transmitted, and $b=(b_1,b_2,b_3,b_4,b_5,b_6)$ is received. At the receiving end, we know the formula for $e(a)$, and if no error has occurred in transmission,

$$\begin{array}{l} b_1 = a_1 \\ b_2 = a_2 \\ b_3 = a_3 \\ b_4 = a_1 +_2 a_2 \\ b_5 = a_1 +_2 a_3 \\ b_6 = a_2 +_2 a_3 \end{array} \Rightarrow \begin{array}{lllllllllll} b_1 & +_2 & b_2 & & & +_2 & b_4 & & & & = 0 \\ b_1 & & & +_2 & b_3 & & & +_2 & b_5 & & = 0 \\ & & b_2 & +_2 & b_3 & & & & & +_2 \; b_6 & = 0 \end{array}$$

The three equations on the right are called parity-check equations. If any of them are not true, an error has occurred. This error checking can be described in matrix form.

Let

$$P = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

P is called the parity-check matrix for this code. Now define $p:{\mathbb{Z}_2}^6 \to {\mathbb{Z}_2}^3$ by $p(b)=bP$. We call $p(b)$ the syndrome of the received block. For example, $p(0,1,0,1,0,1)=(0,0,0)$and $p(1,1,1,1,0,0)=(1,0,0)$

Note that p is also a homomorphism. If the syndrome of a block is $(0,0,0)$, we can be almost certain that the message block is (b_1,b_2,b_3).

Next we turn to the method of correcting errors. Despite the fact that there are only eight code words, one for each three-bit block value, the set of possible received blocks is ${\mathbb{Z}_2}^6$, with 64 elements. Suppose that b is not a code word, but that it differs from a code word by exactly one bit. In other words, it is the result of a single error in transmission. Suppose that w is the code word that b is closest to and that they differ in the first bit. Then $b+w=(1,0,0,0,0,0)$ and

$$\begin{aligned} p(b) &= p(b)+p(w) \quad \text{since } p(w)=(0,0,0) \\ &= p(b+w) \quad \text{since } p \text{ is a homomorphism} \\ &= p(1,0,0,0,0,0) \\ &= (1,1,0) \end{aligned}$$

Note that we haven't specified b or w, only that they differ in the first bit. Therefore, if b is received, there was probably an error in the first bit and $p(b)=(1,1,0)$, the transmitted code word was probably $b+(1,0,0,0,0,0)$ and the message block was $(b_1+_2 1,b_2,b_3)$. The same analysis can be done if b and w differ in any of the other five bits.

This process can be described in terms of cosets. Let W be the set of code words; that is, $W=e\left({\mathbb{Z}_2}^3\right)$. Since e is a homomorphism, W is a subgroup of ${\mathbb{Z}_2}^6$. Consider the factor group ${\mathbb{Z}_2}^6/W$:

$$|{\mathbb{Z}_2}^6/W| = \frac{|{\mathbb{Z}_2}^6|}{|W|} = \frac{64}{8} = 8$$

Suppose that b_1 and b_2 are representatives of the same coset. Then $b_1=b_2+w$ for some w in W. Therefore,

$$\begin{aligned} p\left(b_1\right) &= p\left(b_1\right)+p(w) \quad \text{since } p(w)=(0,0,0) \\ &= p\left(b_1+w\right) \\ &= p\left(b_2\right) \end{aligned}$$

and so b_1 and b_2 have the same syndrome.

Finally, suppose that d_1 and d_2 are distinct and both have only a single coordinate equal to 1. Then d_1+d_2 has exactly two ones. Note that the identity of ${\mathbb{Z}_2}^6$, $(0,0,0,0,0,0)$,must be in W. Since d_1+d_2 differs from the identity by two bits, $d_1+d_2 \notin W$. Hence d_1 and d_2 belong to distinct cosets. The reasoning above serves as a proof of the following theorem.

Theorem 14.5.1

There is a system of distinguished representatives of ${\mathbb{Z}_2}^6 / W$ such that each of the six-bit blocks having a single 1 is a distinguished representative of its own coset.

Now we can describe the error-correcting process. First match each of the blocks with a single 1 with its syndrome. In addition, match the identity of W with the syndrome $(0,0,0)$ as in the table below. Since there are eight cosets of W, select any representative of the eighth coset to be distinguished. This is the coset with syndrome $(1,1,1)$.

Syndrome			Error Correction					
0	0	0	0	0	0	0	0	0
1	1	0	1	0	0	0	0	0
1	0	1	0	1	0	0	0	0
0	1	1	0	0	1	0	0	0
1	0	0	0	0	0	1	0	0
0	1	0	0	0	0	0	1	0
0	0	1	0	0	0	0	0	1
1	1	1	1	0	0	0	0	1

When block b is received, you need only compute the syndrome, $p(b)$, and add to b the error correction that matches $p(b)$.

We will conclude this example by computing the probability of success for our hypothetical situation. It is $\left(0.999^6+6\cdot 0.999^5\cdot 0.001\right)^{1000}=0.985151$. The rate for this code is $\frac{1}{2}$.

Example 14.5.1: Another Linear Code

Consider the linear code with generator matrix

$$G=\begin{pmatrix}1&1&0&1&0\\0&1&1&0&0\\0&0&0&1&1\end{pmatrix}.$$

Since G is 3×5, this code encodes three bits into five bits. The natural question to ask is what detection or correction does it afford? We can answer this question by constructing the parity check matrix. We observe that if $\vec{b}=(b_1,b_2,b_3)$ the encoding function is

$$e(\vec{b})=\vec{b}G=(b_1,b_1+b_2,b_2,b_1+b_3,b_3)$$

where addition is mod 2 addition. If we receive five bits (c_1,c_2,c_3,c_4,c_5) and no error has occurred, the following two equations would be true.

$$c_1+c_2+c_3=0 \tag{14.5.1}$$
$$c_1+c_4+c_5=0 \tag{14.5.2}$$

Notice that in general, the number of parity check equations is equal to the number of extra bits that are added by the encoding function. These equations are equivalent to the single matrix equation $(c_1,c_2,c_3,c_4,c_5)H=\vec{0}$, where

$$H=\begin{pmatrix}1&1\\1&0\\1&0\\0&1\\0&1\end{pmatrix}$$

At a glance, we can see that this code will not correct most single bit errors. Suppose an error $\vec{e} = (e_1, e_2, e_3, e_4, e_5)$ is added in the transmission of the five bits. Specifically, suppose that 1 is added (mod 2) in position j, where $1 \leq j \leq 5$ and the other coordinates of $\vec{e}$ are 0. Then when we compute the syndrome of our received transmission, we see that

$$\vec{c}H = (\vec{b}G + \vec{e})H = (\vec{b}G)H + \vec{e}H = \vec{e}H.$$

But $\vec{e}H$ is the j^{th} row of H. If the syndrome is $(1, 1)$ we know that the error occurred in position 1 and we can correct it. However, if the error is in any other position we can't pinpoint its location. If the syndrome is $(1, 0)$, then the error could have occurred in either position 2 or position 3. This code does detect all single bit errors but only corrects one fifth of them.

14.5.4: Exercises

Exercise 14.5.1

If the error-detecting code is being used, how would you act on the following received blocks?

a. $(1, 0, 1, 1)$
b. $(1, 1, 1, 1)$
c. $(0, 0, 0, 0)$

Answer

a. Error detected, since an odd number of 1's was received; ask for retransmission.
b. No error detected; accept this block.
c. No error detected; accept this block.

Exercise 14.5.2

Express the encoding and decoding functions for the error-detecting code using matrices.

Exercise 14.5.3

If the error-correcting code from this section is being used, how would you decode the following blocks? Expect an error that cannot be fixed with one of these.

a. $(1, 0, 0, 0, 1, 1)$
b. $(1, 0, 1, 0, 1, 1)$
c. $(0, 1, 1, 1, 1, 0)$
d. $(0, 0, 0, 1, 1, 0)$
e. $(1, 0, 0, 0, 0, 1)$
f. $(1, 0, 0, 1, 0, 0)$

Answer

a. Syndrome = $(1, 0, 1)$. Corrected coded message is $(1, 1, 0, 0, 1, 1)$ and original message was $(1, 1, 0)$.
b. Syndrome = $(1, 1, 0)$. Corrected coded message is $(0, 0, 1, 0, 1, 1)$ and original message was $(0, 0, 1)$.
c. Syndrome = $(0, 0, 0)$. No error, coded message is $(0, 1, 1, 1, 1, 0)$ and original message was $(0, 1, 1)$.
d. Syndrome = $(1, 1, 0)$. Corrected coded message is $(1, 0, 0, 1, 1, 0)$ and original message was $(1, 0, 0)$.
e. Syndrome = $(1, 1, 1)$. This syndrome occurs only if two bits have been switched. No reliable correction is possible.
f. Syndrome = $(0, 1, 0)$. Corrected coded message is $(1, 0, 0, 1, 1, 0)$ and original message was $(1, 0, 0)$.

Exercise 14.5.5

Consider the linear code defined by the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

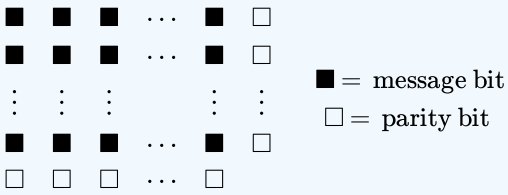
a. What size blocks does this code encode and what is the length of the code words?
b. What are the code words for this code?
c. With this code, can you detect single bit errors? Can you correct all, some, or no single bit errors?

Answer

Let G be the 9×10 matrix obtained by augmenting the 9×9 . The function $e : \mathbb{Z}_2{}^9 \to \mathbb{Z}_2{}^{10}$ defined by $e(a) = aG$ will allow us to detect single errors, since $e(a)$ will always have an even number of ones.

Exercise 14.5.6: Rectangular Codes

To build a rectangular code, you partition your message into blocks of length m and then factor m into $k_1 \cdot k_2$ and arrange the bits in a $k_1 \times k_2$ rectangular array as in the figure below. Then you add parity bits along the right side and bottom of the rows and columns. The code word is then read row by row.



For example, if m is 4, then our only choice is a 2 by 2 array. The message 1101 would be encoded as

1	1	0
0	1	1
1	0	

and the code word is the string 11001110.

a. Suppose that you were sent four bit messages using this code and you received the following strings. What were the messages, assuming no more than one error in the transmission of coded data?
   i. 11011000
   ii. 01110010
   iii. 10001111
b. If you encoded n^2 bits in this manner, what would be the rate of the code?
c. Rectangular codes are linear codes. For the 3 by 2 rectangular code, what are the generator and parity check matrices?

Exercise 14.5.7

Suppose that the code in Example 14.5.1is expanded to add the column

$$\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

to the generator matrix G, can all single bit errors be corrected? Explain your answer.

Answer

Yes, you can correct all single bit errors because the parity check matrix for the expanded code is

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since each possible syndrome of single bit errors is unique we can correct any error.

Index

Glossary

Antisymmetric | A relation R on a set A is an antisymmetric relation provided that for all x,y∈Ax, if x R y and y R x, then x=y.

Biconditional | P if and only if Q

Bijection | A function f:A -> B such that f is both an injection and a surjection

Bipartite graph | A graph for which it is possible to divide the vertices into two disjoint sets such that there are no edges between any two vertices in the same set

Boolean algebra | a lattice that contains a least element and a greatest element and that is both complemented and distributive. The notation $[B;\vee,\wedge,\bar{}]$ is used to denote the boolean algebra with operations join, meet and complementation.

Cardinality | The number of elements in a set

Chromatic number | The minimum number of colors required in a proper vertex coloring of the graph

Complement of a set | Let *U* be the universal set. A^c ={x in *U*, x is not in A}

Complete graph | A graph in which every pair of vertices is adjacent

Conditional Statement | If P then Q. P is the antecedent (hypothesis) and Q is the consequent (conclusion)

Congruent | Two integers are congruent mod n (n a positive integer) if the integers leave the same remainder upon division by n

Conjecture | a guess in mathematics

Conjunction | P and Q

Contrapositive | Of the conditional, if not Q then not P, logically equivalent to if P then Q

Converse | Of the conditional, if Q then P

Countably infinite | A set that can be put into one-to-one correspondence with the set of natural numbers

Cyclic group | Group G is cyclic if there exists a∈G such that the cyclic subgroup generated by a, ⟨a⟩ equals all of G. That is, G={na|n∈Z} in which case a is called a generator of G. The reader should note that additive notation is used for G

Digraph | A directed graph

Direct Proof | Argument that is based on "If P then Q" and "P" implies Q

Disjunction | P and Q

Division algorithm | Let m and d be integers with d>0. Then, there exists unique integers q and r with 0<=r < d such that m = dq+r

Equivalence class |
For each a∈A, the equivalence class of aa determined by ∼ is the subset of A, denoted by [a], consisting of all the elements of A that are equivalent to a

Equivalence relation | A relation that is reflexive, symmetric and transitive

Euclidean algorithm | Let a and b be integers with a≠0 and b>0. Then gcd(a, b) is the only natural number d such that (a) d divides a and d divides b, and (b) if k is an integer that divides both a and b, then k divides d

Euler circuit | An Euler path which starts and stops at the same vertex

Euler path | A walk which uses each edge exactly once

Existential operator | There exists

Formal Language | If A is an alphabet, a formal language over A is a subset of A^*.

Graph | an ordered pair G=(V,E) consisting of a nonempty set V (called the *vertices*) and a set E (called the *edges*) of two-element subsets of V

Greatest common divisor |
The largest natural number that divides both a and b is called the greatest common divisor of a and b

Hasse diagram | an illustration of a poset

Homomorphism | Let [G;∗] and [G′;⋄]be groups. θ:G→G′ is a homomorphism if θ(x∗y)=θ(x)⋄θ(y) for all x,y∈G

Indirect Proof | Argument based upon the contrapositive

Injection | A function f:A->B is an injection, if for every a and b in the domain of f, f(a)=f(b) implies a = b.

Intersection of two sets | Let *U* be the universal set. A intersect B = {x in *U*, x is in A and x is in B}

Inverse | Of the conditional, if not P then not Q

Isomorphism |
between two graphs G1 and G2 is a bijection f:V1→V2 between the vertices of the graphs such that if {a,b} is an edge in G1 then {f(a),f(b)} is an edge in G2

Lattice | a poset (L,⪯)for which every pair of elements has a greatest lower bound and least upper bound

Logical equivalence | Two expressions are logically equivalent provided that they have the same truth value for all possible combinations of truth values for all variables appearing in the two expressions

Monoid | a set M together with a binary operation ∗∗ with the properties

- ∗∗ is associative: ∀a,b,c∈M, (a∗b)∗c=a∗(b∗c) and
- ∗∗ has an identity in M:M: ∃e∈Msuch that ∀a∈M, a∗e=e∗a=a

Negation | not P

Partial order | Let ⪯⪯ be a relation on a set L.L. We say that ⪯⪯ is a partial ordering on LL if it is reflexive , antisymmetric , and transitive . That is:

1. ⪯ is reflexive : a⪯a∀a∈L
2. ⪯ is antisymmetric : a⪯b and a≠b⇒b⋠a∀a,b∈L
3. ⪯ is transitive : a⪯b and b⪯c⇒a⪯c∀a,b,c∈L

The set together with the relation (L,⪯) is called a poset.

Principle of Mathematical Induction | A technique of proof whereby If T is a subset of N such that

1. 1∈T, and
2. For every k∈N, if k∈T, then (k+1)∈T.

Then T=N.

Proof by Contradiction | Given "If P then Q" assume "P and not Q" to arrive at "P and not P"

Reflexive |
The relation R is reflexive on A provided that for each x∈A, x R x or, equivalently, (x,x)∈R

Relation | Let A and B be sets. A relation R from the set A to the set B is a subset of A×B

Set | A well-defined collection of objects

Statement | a declarative sentence that is either true or false but not both

String |
A string of length n, n⩾1 over alphabet A is a sequence of nn letters from A: $a_1a_2\ldots a_n$. The set of all strings over A is A^*.

Subgraph | We say that G1=(V1,E1) is a *subgraph* of G2=(V2,E2) provided V1⊆V2 and E1⊆E2

Surjection | A function f:A ->B is a surjection if for every b in B there exists an a in A such that f(a)=b.

Symmetric | The relation R is symmetric provided that for every x,y∈A, if x R y, then y R x or, equivalently, for every x,y∈Ax, if (x,y)∈R, then (y,x)∈R

Symmetric group |
Let A be a nonempty set . The set of all permutations on A with the operation of function composition is called the symmetric group on A, denoted S_A.

The Well-Ordering Principle | for the natural numbers states that any nonempty set of natural numbers must contain a least element equivalent to the Principle of Mathematical Induction

Transitive | The relation R is transitive provided that for every x,y,z∈A, if x R y and y R z, then x R z or, equivalently, for every x,y,z∈A, if (x,y)∈R and (y,z)∈R, then (x,z)∈R

Tree | A (connected) graph with no cycles. (A non-connected graph with no cycles is called a forest.) The vertices in a tree with degree 1 are called leaves

Truth table | a summary of all the truth values of a statement

Uncountably infinite | An infinite set for which there does not exist a one to one correspondence with the natural numbers

Union of two sets | Let *U* be the universal set. A U B ={x in *U*, such that x is in A or x is in B}

Universal operator | For all or for every

Vertex coloring | An assignment of colors to each of the vertices of a graph. A vertex coloring is proper if adjacent vertices are always colored differently

Appendix A: Guidelines for Writing Mathematical Proofs

One of the most important forms of mathematical writing is writing mathematical proofs. The writing of mathematical proofs is an acquired skill and takes a lot of practice. Throughout the textbook, we have introduced various guidelines for writing proofs. These guidelines are in Sections 1.1, 1.2, 3.1, 3.2, 3.3, and 4.1.

Following is a summary of all the writing guidelines introduced in the text. This summary contains some standard conventions that are usually followed when writing a mathematical proof.

1. **Know your audience**. Every writer should have a clear idea of the intended audience for a piece of writing. In that way, the writer can give the right amount of information at the proper level of sophistication to communicate effectively. This is especially true for mathematical writing. For example, if a mathematician is writing a solution to a textbook problem for a solutions manual for instructors, the writing would be brief with many details omitted. However, if the writing was for a students' solution manual, more details would be included.
2. As an example, an exercise in a text might read, "Prove that if x is an odd integer, then x^2 is an odd integer." This could be started as follows:

   Theorem. If x is an odd integer, then x^2 is an odd integer.
   Proof: We assume that x is an odd integer ....
3. **Begin the proof with a statement of your assumptions**. Follow the statement of your assumptions with a statement of what you will prove.

   Proof. We assume that x and y are odd integers and will prove that $x \cdot y$ is an odd integer.
4. **Use the pronoun "we."** If a pronoun is used in a proof, the usual convention is to use "we" instead of "I." The idea is to stress that you and the reader are doing the mathematics together. It will help encourage the reader to continue working through the mathematics. Notice that we started the proof of Theorem 1.8 with "We assume that... ."
5. **Use italics for variables when using a word processor.** When using a word processor to write mathematics, the word processor needs to be capable of producing the appropriate mathematical symbols and equations. The mathematics that is written with a word processor should look like typeset mathematics. This means that variables need to be italicized, boldface is used for vectors, and regular font is used for mathematical terms such as the names of the trigonometric functions and logarithmic functions.

   For example, we do not write sin x or $sin\ x$. The proper way to typeset this is sin x.
6. **Do not use $*$ for multiplication or ^ for exponents**. Leave this type of notation for writing computer code. The use of this notation makes it difficult for humans to read. In addition, avoid using / for division when using a complex fraction.
   For example, it is very difficult to read $(x^3-3x^2+1/2)/(2x/3-7)$; the fraction

   $$\frac{x^3-3x^2+\frac{1}{2}}{\frac{2x}{3}-7} \qquad \text{(Appendix A.1)}$$

   is much easier to read.
7. **Use complete sentences and proper paragraph structure**. Good grammar is an important part of any writing. Therefore, conform to the accepted rules of grammar. Pay careful attention to the structure of sentences. Write proofs using **complete sentences** but avoid run-on sentences. Also, do not forget punctuation, and always use a spell checker when using a word processor.
8. **Keep the reader informed**. Sometimes a theorem is proven by proving the contrapositive or by using a proof by contradiction. If either proof method is used, this should be indicated within the first few lines of the proof. This also applies if the result is going to be proven using mathematical induction.

Example

- We will prove this result by proving the contrapositive of the statement.
- We will prove this statement using a proof by contradiction.
- We willassume to the contrary that... .
- We will use mathematical induction to prove this result.

In addition, make sure the reader knows the status of every assertion that is made. That is, make sure it is clearly stated whether an assertion is an assumption of the theorem, a previously proven result, a well-known result, or something from the reader's mathematical background.

9. **Display important equations and mathematical expressions.** Equations and manipulations are often an integral part of the exposition. Do not write equations, algebraic manipulations, or formulas in one column with reasons given in another column (as is often done in geometry texts). Important equations and manipulations should be displayed. This means that they should be centered with blank lines before and after the equation or manipulations, and if one side of an equation does not change, it should not be repeated. For example,

   Using algebra, we obtain

$$\begin{aligned} x \cdot y &= (2m+1)(2n+1) \\ &= 4mn+2m+2n+1 \\ &= 2(2mn+m+n)+1. \end{aligned} \qquad \text{(Appendix A.2)}$$

   Since m and n are integers, we conclude that ... .

10. **Equation numbering guidelines.** If it is necessary to refer to an equation later in a proof, that equation should be centered and displayed, and it should be given a number. The number for the equation should be written in paren- theses on the same line as the equation at the right-hand margin.

Example

Since x is an odd integer, there exists an integer n such that

$$x = 2n+1 \qquad \text{(Appendix A.3)}$$

Later in the proof, there may be a line such as

Then, using the result in equation (A.3), we obtain ... .

Please note that we should only number those equations we will be referring to later in the proof. Also, note that the word "equation" is not capitalized when we are referring to an equation by number. Although it may be appropriate to use a capital "E," the usual convention in mathematics is not to capitalize.

11. **Do not use a mathematical symbol at the beginning of a sentence.**
    For example, we should not write, "Let n be an integer. n is an odd integer provided that ... ." Many people find this hard to read and often have to reread it to understand it. It would be better to write, "An integer n is an odd integer provided that ... ."
12. **Use English and minimize the use of cumbersome** notation. Do not use the special symbols for quantifiers $\forall$ (for all), $\exists$ (there exists), $\ni$ (such that), or $\therefore$ (therefore) in formal mathematical writing. It is often easier to write, and usually easier to read, if the English words are used instead of the symbols. For example, why make the reader interpret

$$(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x+y=0) \qquad \text{(Appendix A.4)}$$

    where it is possible to write

    For each real number x, there exists a real number y such that $x+y=0$, or more succinctly (if appropriate)

    Every real number has an additive inverse.

13. **Tell the reader when the proof has been completed.** Perhaps the best way to do this is to say outright that, “This completes the proof.” Although it may seem repetitive, a good alternative is to finish a proof with a sentence that states precisely what has been proven. In any case, it is usually good practice to use some “end of proof symbol” such as ■.
14. **Keep it simple**. It is often difficult to understand a mathematical argument no matter how well it is written. Do not let your writing help make it more difficult for the reader. Use simple, declarative sentences and short paragraphs, each with a simple point.
15. **Write a first draft of your proof and then revise it**. Remember that a proof is written so that readers are able to read and understand the reasoning in the proof. Be clear and concise. Include details but do not ramble. Do not be satisfied with the first draft of a proof. Read it over and refine it. Just like any worthwhile activity, learning to write mathematics well takes practice and hard work. This can be frustrating. Everyone can be sure that there will be some proofs that are difficult to construct, but remember that proofs are a very important part of mathematics. So work hard and have fun.

Appendix B: Answers for the Progress Checks

Section 1.1

Progress Check 1.2

1. This proposition is false. A counterexample is $a = 2$ and $b = 1$. For these values, $(a+b)^2 = 9$ and $a^2 + b^2 = 5$.
2. This proposition is true, as we can see by using $x = 3$ and $y = 7$. We could also use $x = -2$ and $y = 9$. There are many other possible choices for x and y.
3. This proposition appears to be true. Anytime we use an example where x is an even integer, the number x^2 is an even integer. However, we cannot claim that this is true based on examples since we cannot list all of the examples where x is an even integer.
4. This proposition appears to be true. Anytime we use an example where x and y are both integers, the number $x \cdot y$ is an odd integer. However, we cannot claim that this is true based on examples since we cannot list all of the examples where both x and y are odd integers.

Progress Check 1.4

1. (a) This does not mean the conditional statement is false since when $x = -3$, the hypothesis is false, and the only time a conditional statement is false is when the hypothesis is true and the conclusion is false.
   (b) This does not mean the conditional statement is true since we have not checked all positive real numbers, only the one where $x = 4$.
   (c) All examples should indicate that the conditional statement is true.
2. The number ($n2 - n + 41$) will be a prime number for all examples of \(n\) that are less than 41. However, when $n = 41$, we get

$$\begin{aligned} n^2 - n + 41 &= 41^2 - 41 + 41 \\ n^2 - n + 41 &= 41^2 \end{aligned} \qquad \text{(Appendix B.1)}$$

   So in the case where $n = 41$, the hypothesis is true (41 is a positive integer) and the conclusion is false (41^2 is not prime). Therefore, 41 is a counterexample that shows the conditional statement is false. There are other counterexamples (such as $n = 42$, $n = 45$, and $n = 50$), but only one counterexample is needed to prove that the statement is false.

Progress Check 1.5

1. We can conclude that this function is continuous at 0.
2. We can make no conclusion about this function from the theorem.
3. We can make no conclusion about this function from the theorem.
4. We can conclude that this function is not differentiable at 0.

Progress Check 1.7

1. The set of rational numbers is closed under addition since $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.
2. The set of integers is not closed under division. For example, $\frac{2}{3}$ is not an integer.
3. The set of rational numbers is closed under subtraction since $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$.

Section 1.2

Progress Check 1.10

All examples should indicate the proposition is true. Following is a proof.

Proof. We assume that m is an odd integer and will prove that ($3m^2 + 4m + 6$). Since m is an odd integer, there exists an integer k such that $mD = 2k + 1$. Substituting this into the expression ($3m^2 + 4m + 6$) and using algebra, we obtain

$$\begin{aligned} 3m^2 + 4m + 6 &= 3(2k+1)^2 + 4(2k+1) + 6 \\ &= (12k^2 + 12k + 3) + (8k + 4) + 6 \\ &= 12k^2 + 20k + 13 \\ &= 12k^2 + 20k + 12 + 1 \\ &= 2(6k^2 + 10k + 6) + 1 \end{aligned}$$

Progress Check 1.11

Proof. We let m be a real number and assume that m, $m+1$, and $m+2$ are the lengths of the three sides of a right triangle. We will use the Pythagorean Theorem to prove that $m = 3$. Since the hypotenuse is the longest of the three sides, the Pythagorean Theorem implies that $m^2 + (m+1)^2 = (m+2)^2$. We will now use algebra to rewrite both sides of this equation as follows:

$$\begin{aligned} m^2 + (m^2 + 2m + 1) &= m^2 + 4m + 4 \\ 2m^2 + 2m + 1 &= m^2 + 4m + 4 \end{aligned}$$

The last equation is a quadratic equation. To solve for m, we rewrite the equation in standard form and then factor the left side. This gives

$$\begin{aligned} m^2-2m-3 &= 0 \\ (m-3)(m+1) &= 0 \end{aligned}$$

The two solutions of this equation are $m=3$ and $m=-1$. However, since m is the length of a side of a right triangle, m must be positive and we conclude that $m=3$. This proves that if m, $m+1$, and $m+2$ are the lengths of the three sides of a right triangle, then $m=3$.

Section 2.1

Progress Check 2.1

1. Whenever a quadrilateral is a square, it is a rectangle, or a quadrilateral is a rectangle whenever it is a square.
2. A quadrilateral is a square only if it is a rectangle.
3. Being a rectangle is necessary for a quadrilateral to be a square.
4. Being a square is sufficient for a quadrilateral to be a rectangle.

Progress Check 2.2

P	Q	$P \wedge \neg Q$	$\neg(P \wedge Q)$	$\neg P \wedge \neg Q$	$\neg P \vee \neg Q$
T	T	F	F	F	F
T	F	T	T	F	T
F	T	F	T	F	T
F	F	F	T	T	T

Statements (2) and (4) have the same truth table.

Progress Check 2.4

P	$\neg P$	$P \vee \neg P$	$P \wedge \neg P$
T	F	T	F
F	T	T	F

P	Q	$P \vee Q$	$P \rightarrow (P \vee Q)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

Section 2.2

Progress Check 2.7

1. Starting with the suggested equivalency, we obtain

$$\begin{aligned} (P \wedge \neg Q) \rightarrow R &\equiv \neg(P \wedge \neg Q) \vee R \\ &\equiv (\neg P \vee \neg(\neg Q)) \vee R \\ &\equiv \neg P \vee (Q \vee R) \\ &\equiv P \rightarrow (Q \vee R) \end{aligned} \qquad \text{(Appendix B.2)}$$

2. For this, let P be,"3 is a factor of $a \cdot b$," let Q be, "is a factor of a," and let R be, "3 is a factor of b." Then the stated proposition is written in the form $P \rightarrow (Q \vee R)$. Since this is logically equivalent to $(P \wedge \neg Q) \rightarrow R$, if we prove that

   if 3 is a factor of $a \cdot b$ and 3 is not a factor of a, then 3 is a factor of b, then we have proven the original proposition.

Section 2.3

Progress Check 2.9

1. $10 \in A$, $22 \in A$, $13 \notin A$, $0 \in A$, $-12 \notin A$
2. $A = B, A \subseteq B, B \subseteq A, A \subseteq C, A \subseteq D, B \subseteq C, B \subseteq D$

Progress Check 2.11

1. (a) Two values of x for which $P(x)$ is false are $x=3$ and $x=-4$.
   (b) The set of all x for which $P(x)$ is true is the set {-2, -1, 0, 1, 2}.

2. (a) Two examples for which $R(x, y, z)$ is false are: $x = 1, y = 1, z = 1$ and $x = 3, y = -1, z = 5$.
   (b) Two examples for which $R(x, y, z)$ is true are: $x = 3, y = 4, z = 5$ and $x = 5, y = 12, z = 13$.

Progress Check 2.13

1. The truth set is the set of all real numbers whose square is less than or equal to 9. The truth set is $\{x \in \mathbb{R} \mid x^2 \leq 9\} = \{x \in \mathbb{R} \mid -3 \leq x \leq 3\}$.
2. The truth set is the set of all integers whose square is less than or equal to 9. The truth set is {-3, -2, -1, 0, 1, 2, 3}.
3. The truth sets in Parts (1) and (2) equal are not equal. One purpose of this progress check is to show that the truth set of a predicate depends on the predicate and on the universal set.

Progress Check 2.15

$A = \{4n - 3 \mid n \in \mathbb{N}\} = \{x \in \mathbb{N} \mid x = 4n - 3 \text{ for some natural number } n\}$.

\(B = \{-2n\ |\ \text{n is a nonnegative integer\}.\)

$C = \{(\sqrt{2})^{2m-1} \mid m \in \mathbb{N}\} = \{(\sqrt{2})^n \mid n \text{ is an odd natural number}\}$.

$D = \{3^n \mid n \text{ is a nonnegative integer}\}$.

Section 2.4

Progress Check 2.18

1. • For each real number a, $a + 0 = a$.
   • $(\exists a \in \mathbb{R})(a + 0 \neq a)$.
   • There exists a real number a such that $a + 0 \neq a$.
2. • For each real number x, sin $(2x)$ = 2(sin x)(cos x).
   • $(\exists x \in \mathbb{R})$ (sin $(2x) \neq 2$ (sin x) (cos x)).
   • There exists a real number x such that sin $(2x) \neq 2$ (sin x) (cos x).
3. • For each real number x, $\tan^2 x + 1 = \sec^2 x$.
   • $(\exists x \in \mathbb{R})(\tan^2 x + 1 \neq \sec^2 x)$.
   • There exists a real number x such that $\tan^2 x + 1 \neq \sec^2 x$.
4. • There exists a rational number x such that $x^2 - 3x - 7 = 0$.
   • $(\forall x \in \mathbb{Q})(x^2 - 3x - 7 \neq 0)$.
   • For each rational number x, $x^2 - 3x - 7 \neq 0$.
5. • There exists a real number x such that $x^2 + 1 = 0$.
   • $(\forall x \in \mathbb{R})(x^2 + 1 \neq 0)$.
   • For each real number x, $x^2 + 1 \neq 0$.

Progress Check 2.19

1. A counterexample is $n = 4$ since $4^2 + 4 + 1 = 21$, and 21 is not prime.
2. A counterexample is $x = \frac{1}{4}$ since $\frac{1}{4}$ is positive and $2(\frac{1}{4})^2 = \frac{1}{8}$ and $\frac{1}{8} \leq \frac{1}{4}$.

Progress Check 2.20

1. An integer n is a multiple of 3 provided that $\exists k \in \mathbb{Z})(n = 3k)$.
4. An integer n is not a multiple of 3 provided that $\forall k \in \mathbb{Z})(n \neq 3k)$.
5. An integer n is not a multiple of 3 provided that for every integer k, $n \neq 3k$.

Progress Check 2.21

- $(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x + y \neq 0)$.
- There exist integers x and y such that $x + y \neq 0$.

Section 3.1

Progress Check 3.2

2. For each example in Part (1), the integer a divides the sum $b + c$.
3. Conjecture: For all integers a, b, and c with $a \neq 0$, if a divides b and a divides c, then a divides $b + c$.
4. A Know-show table for a proof of the conjecture in Part (3).

Step	Know	Reason
P	$a \mid b$ and $a \mid c$	Hypothesis
$P1$	$(\exists s \in \mathbb{Z})(b = a \cdot s)$ $(\exists t \in \mathbb{Z})(c = a \cdot t)$	Definition of "divides"
$P2$	$b + c = as + at$	Substituting for b and c
$P3$	$b + c = a(s + t)$	Distributive property

$Q1$	$s+t$ is an integer	$\mathbb{Z}$ is closed under addition
Q	$a \mid (b+c)$	Definition of "divides"
Step	**Show**	**Reason**

Progress Check 3.3

A counterexample for this statement will be values of a and b for which 5 divides a or 5 divides b, and 5 does not divide $5a+b$. One counterexample for the statement is $a=5$ and $b=1$. For these values, the hypothesis is true since 5 divides a and the conclusion is false since $5a+b=26$ and 5 does not divide 26.

Progress Check 3.4

1. Some integers that are congruent to 5 modulo 8 are -11, -3, 5, 13, and 21.
2. \(\{x \in \mathbb{Z}\ |\ x \equiv 5\text{ (mod 8)}\} = \{..., -19, -11, -3, 5, 13, 21, 29, ...\}\).
3. For example, -3 + 5 = 2, -11 + 29 = 18, 13 + 21 = 34.
4. If we subtract 2 from any of the sums obtained in Part (3), the result will be a multiple of 8. This means that the sum is congruent to 2 modulo 8. For example, $2-2=0$, $18-2=16$, $34-2=32$.

Progress Check 3.6

1. To prove that 8 divides $(a+b-2)$, we can prove that there exists an integer q such that $(a+b-2=8q$).
2. Since 8 divides $(a-5)$ and $(b-5)$, there exist integers k and m such that $a-5-8k$ and $b-5=8m$.
3. $a=5+8k$ and $b=5+8m$.
4. $a+b-2=(5+8k)+5+8m)-2=8+8k+8m=8(1+k+m)$.
5. ***Proof.*** Let a and b be integers and assume that $a \equiv 5$ (mod 8) and $b \equiv 5$ (mod 8). We will prove that $(a+b) \equiv 2$ (mod 8\). Since 8 divides $(a-5)$ and $(b-5)$, there exist integers k and m such that $a-5=8k$ and $b-5=8m$. We then see that
\[\begin{array} {a + b - 2} &= & {(5 + 8k) + (5 + 8m) - 2] \\ {} &= & {8 + 8k + 8m} \\ {} &= & {8(1 + k + m)} \end{array}\]
By the closure properties of the integers, $(1+k+m)$ is an integer and so the last equation proves that 8 divides $(a+b-2$) and hence, $(a+b) \equiv 2$ (mod 8). This proves that if $a \equiv 5$ (mod 8) and $b \equiv 5$ (mod 8), then $(a+b) \equiv 2$ (mod 8).

Section 3.2

Progress Check 3.8

1. For all real numbers a and b, if $ab=0$, then $a=0$ or $b=0$.
2. For all real numbers a and b, if $ab=0$ and $a \neq 0$, $b=0$
3. This gives

$$\frac{1}{a}(ab)=\frac{1}{a}\cdot 0. \qquad \text{(Appendix B.3)}$$

We now use the associative property on the left side of this equation and simplify both sides of the equation to obtain

$$\begin{aligned} (\frac{1}{a}\cdot a)b &= 0 \\ 1\cdot b &= 0 \\ b &= 0 \end{aligned} \qquad \text{(Appendix B.4)}$$

Therefore, $b=0$ and this completes the proof of a statement that is logically equivalent to the contrapositive. Hence, we have proved the proposition.

Section 3.3

Progress Check 3.15

1. There exists a real number x such that x is irrational and $\sqrt[3]{x}$ is rational.
2. There exists a real number x such that $x+\sqrt{2}$ is rational and $(-x+\sqrt{2})$ is rational.
3. There exist integers a and b such that 5 divides ab and 5 does not divide a and 5 does not divide b.
4. There exist real numbers a and b such that $a>0$ and $b>0$ and $\frac{2}{a}+\frac{2}{b}=\frac{4}{a+b}$.

Progress Check 3.16

1. Some integers that are congruent to 2 modulo 4 are -6. -2, 2, 6, 10, and some integers that are congruent to 3 modulo 6 are: -9, -3, 3, 9, 15. There are no integers that are in both of the lists.
2. For this proposition, it is reasonable to try a proof by contradiction since the conclusion is stated as a negation.

3. Proof. We will use a proof by contradiction. Let $n \in \mathbb{Z}$ and assume that $n \equiv 2 \pmod 4$ and that $n \equiv 3 \pmod 6$. Since $n \equiv 2 \pmod 4$, we know that 4 divides $n-2$. Hence, there exists an integer k such that

$$n-2 = 4k. \qquad \text{(Appendix B.5)}$$

We can also use the assumption that $n \equiv 3 \pmod 6$ to conclude that 6 divides $n-3$ and that there exists an integer m such that

$$n-3 = 6m. \qquad \text{(Appendix B.6)}$$

If we now solve equations (B.5) and (B.6) for n and set the two expressions equal to each other, we obtain

$$4k+2 = 6m+3. \qquad \text{(Appendix B.7)}$$

However, this equation can be rewritten as

$$2(2k+1) = 2(3m+1)+1. \qquad \text{(Appendix B.8)}$$

Since $2k+1$ is an integer and $3m+1$ is an integer, this last equation is a contradiction since the left side is an even integer and the right side is an odd integer. Hence, we have proven that if $n \equiv 2 \pmod 4$, then $n \equiv 3 \pmod 6$.

Progress Check 3.18

1. $x^2+y^2 = (2m+1)^2+(2n+1)^2 = 2(2m^2+2m+2n^2+2n+1)$.
2. Using algebra to rewrite the last equation, we obtain

$$4m^2+4m+4n^2+4n+2 = 4k^2. \qquad \text{(Appendix B.9)}$$

If we divide both sides of this equation by 2, we see that $2m^2+2m+2n^2+2n+1 = 2k^2$ or

$$2(m^2+m+n^2+n)+1 = 2k^2. \qquad \text{(Appendix B.10)}$$

However, the left side of the last equation is an odd integer and the right side is an even integer. This is a contradiction, and so we have proved that for all integers x and y, if x and y are odd integers, then there does not exist an integer z such that $x^2+y^2 = z^2$.

Section 3.4

Progress Check 3.21

Proposition. For each integer n, n^2-5n+7 is an odd integer.

Proof. Let n be an integer. We will prove that n^2-5n+7 is an odd integer by examining the case where n is even and the case where n is odd.

In the case where n is even, there exists an integer m such that $n = 2m$. So in this case,

$$\begin{aligned} n^2-5n+7 &= (2m^2)-5(2m)+7 \\ &= 4m^2-10m+6+1 \\ &= 2(2m^2-5m+3)+1. \end{aligned}$$

Since $(2m^2-5m+3)$ is an integer, the last equation shows that if n is even, then n^2-5n+7 is odd.

In the case where n is odd, there exists an integer m such that $n = 2m+1$. So in this case,

$$\begin{aligned} n^2-5n+7 &= (2m+1)^2-5(2m+1)+7 \\ &= 4m^2-14m+3 \\ &= 2(2m^2-7m+1)+1. \end{aligned}$$

Since $(2m^2-7m+1)$ is an integer, the last equation shows that if n is odd, then n^2-5n+7 is odd. Hence, by using these two cases, we have shown that for each integer n, n^2-5n+7 is an odd integer.

Progress Check 3.24

1. |4.3| = 4.3 and |-π| = π
2. (a) $t = 12$ or $t = -12$
   (b) $t+3 = 5$ or $t+3 = -5$. So $t = 2$ or $t = -8$.
   (c) $t-4 = \frac{1}{5}$ or $t-4 = -\frac{1}{5}$. So $t = \frac{21}{5}$ or $t = \frac{19}{5}$.
   (d) $3t-4 = 8$ or $3t-4 = -8$. So $t = 4$ or $t = -\frac{4}{3}$.

Section 3.5

Progress Check 3.26

1. (a) The possible remainders are 0, 1, 2, and 3.
   (b) The possible remainders are 0, 1, 2, 3, 4, 5, 6, 7, and 8.

   (a) $17 = 5 \cdot 3 + 2$
   (b) $-17 = (-6) \cdot 3 + 1$
   (c) $73 = 10 \cdot 7 + 3$
   (d) $-73 = (-11) \cdot 7 + 4$
   (e) $436 = 16 \cdot 27 + 4$
   (f) $539 = 4 \cdot 110 + 99$

Progress Check 3.29

Proof. Let n be a natural number and let a, b, c and d be integers.We assume that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ and will prove that $(a+c) \equiv (b+d) \pmod{n}$. Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, n divides $a-b$ and $c-d$ and so there exist integers k and q such that $a-b=nk$ and $c-d=nq$. We can then write $a=b+nk$ and $c=d+nq$ and obtain

$$\begin{aligned} a+c &= (b+nk)+(d+nq) \\ &= (b+d)+n(k+q) \end{aligned} .$$

By subtracting $(b+d)$ from both sides of the last equation, we see that

$(a+c)-(b+d)=n(k+q)$.

Since $(k+q)$ is an integer, this proves that n divides $(a+c)-(b+d)$, and hence, we can conclude that $(a+c) \equiv (b+d) \pmod{n}$.

Progress Check 3.34

Case 2. ($a \equiv 2 \pmod 5$). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 2^2 \pmod 5 \text{ or } a^2 \equiv 4 \pmod 5.$$

This proves that if $a \equiv 2 \pmod 5$, then $a^2 \equiv 4 \pmod 5$.

Case 3. ($a \equiv 3 \pmod 5$). In this case, we use Theorem 3.28 to conclude that

$$a^2 \equiv 3^2 \pmod 5 \text{ or } a^2 \equiv 9 \pmod 5.$$

We also know that $9 \equiv 4 \pmod 5$. So we have $a^2 \equiv 9 \pmod 5$ and $9 \equiv 4 \pmod 5$, and we can now use the transitive property of congruence (Theorem 3.30) to conclude that $a^2 \equiv 4 \pmod 5$. This proves that if $a \equiv 3 \pmod 5$, then $a^2 \equiv 4 \pmod 5$.

Section 4.1

Progress Check 4.1

1. It is not possible to tell if $1 \in T$ and $5 \in T$.
2. True.
3. True. The contrapositive is, "If $2 \in T$, then $5 \in T$," which is true.
4. True.
5. False. If $k \in T$, then $k+1 \in T$.
6. True, since "k \notin t\) OR $k+1 \in T$ " is logically equivalent to "If $k \in T$, then $k+1 \in T$."
7. It is not possible to tell if this is true. It is the converse of the conditional statement, “For each integer k, if $k \in T$, then $k+1 \in T$."
8. True. This is the contrapositive of the conditional statement, “For each integer k, if $k \in T$, then $k+1 \in T$."

Progress Check 4.3

Proof. Let $P(n)$ be the predicate, "$1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$." For basis step, notice that the equation $1 = \dfrac{1(1+1)}{2}$ shows that $P(1)$ is true. Now let k be a natural number an assume that $P(k)$ is true. That is, assume that

$$1+2+3+\cdots+k = \frac{k(k+1)}{2}. \qquad \text{(Appendix B.11)}$$

We now need to prove that $P(k+1)$ is true or that

$$1+2+3+\cdots+k+(k+1) = \frac{(k+1)(k+2)}{2}. \qquad \text{(Appendix B.12)}$$

By adding $(k+1)$ to both sides of equation (B.11), we see that

$$\begin{aligned} 1+2+3+\cdots+k+(k+1) &= \frac{k(k+1)}{2}+(k+1) \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{k^2+3k+2}{2} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

By comparing the last equation to equation (2), we see that we have proved that if $P(k)$ is true, then $P(k+1)$ is true, and the inductive step has been established. Hence, by the Principle of Mathematical Induction, we have proved that for each integer n, $1+2+3+\cdots+n=\frac{n(n+1)}{2}$.

Progress Check 4.5

For the inductive step, let k be a natural number and assume that $P(k)$ is true. That is, assume that $5^k \equiv 1 \pmod 4$.

1. To prove that $P(k+1)$ is true, we must prove $5^{k+1} \equiv 1 \pmod 4$.
2. Since $5^{k+1} = 5 \cdot 5^k$, we multiply both sides of the congruence $5^k \equiv 1 \pmod 4$ by 5 and obtain

$$5 \cdot 5^k \equiv 5 \cdot 1 \pmod 4 \text{ or } \quad 5^{k+1} \equiv 5 \pmod 4. \qquad \text{(Appendix B.13)}$$

3. Since $5^{k+1} \equiv 5 \pmod 4$ and we know that $5 \equiv 1 \pmod 4$, we can use the transitive property of congruence to obtain $5^{k+1} \equiv 1 \pmod 4$. This proves that if $P(k)$ is true, then $P(k+1)$ is true, and hence, by the Principle of Mathematical Induction, we have proved that for each natural number n, $5^n \equiv 1 \pmod 4$.

Section 4.2

Progress Check 4.8

1. For each natural number n, if $n \geq 3$, then $3^n > 1+2^n$.
2. For each natural number n, if $n \geq 6$, then $2^n > (n+1)^2$.
3. For each natural number n, if $n \geq 6$, then $(1+\frac{1}{n})^n > 2.5$.

Progress Check 4.10

Construct the following table and use it to answer the first two questions. The table shows that $P(3)$, $P(5)$, and $P(6)$ are true. We can also see that $P(2)$, $P(4)$, and $P(7)$ are false. It also appears that if $n \in \mathbb{N}$ and $n \geq 8$, then $P(n)$ is true.

x	0	1	2	3	4	0	1	2	0	1	1
y	0	0	0	0	0	1	1	1	2	2	3
$\mathbf{3x+5y}$	0	3	6	9	12	5	8	11	10	13	18

The following proposition provides answers for Problems (3) and (4).

Proposition 4.11. For all natural numbers n with $n \geq 8$, there exist non-negative integers x and y such that $n = 3x+5y$.

Proof. (by mathematical induction) Let $\mathbb{Z}^* = \{x \in \mathbb{Z} \mid x \geq 0\}$, and for each natural number n, let $P(n)$ be, "there exist $x, y \in \mathbb{Z}^*$ such that $n = 3x+5y$."

Basis Step: Using the table above, we see that $P(8)$, $P(9)$, and $P(10)$ are true.

Inductive Step: Let $k \in \mathbb{N}$ with $k \geq 13$. assume that $P(8)$, $P(9)$, ..., $P(k)$ are true. Now, notice that

$$k+1 = 3+(k-2).$$

Since $k \geq 10$, we can conclude that $k-2 \geq 8$ and hence $P(k-2)$ is true. Therefore, there exist non-negative integers u and v such that $k-2 = (3u+5v)$. Using this equation, we see that

$$\begin{aligned} &= 3+(3u+5v) \\ &= 3(1+u)+5v. \end{aligned}$$

Hence, we can conclude that $P(k+1)$ is true. This proves that if $P(8)$, $P(9)$, ..., $P(k)$ are true, then $P(k+1)$ is true. Hence, by the Second Principle of Mathematical Induction, for all natural numbers n with $n \geq 8$, there exist nonnegative integers x and y such that $n = 3x+5y$.

Section 4.3

Progress Check 4.12

Proof. We will use a proof by induction. For each natural number n, we let $P(n)$ be,

f_{3n} is an even natural number.

Since $f_3 = 2$, we see that $P(1)$ is true and this proves the basis step.

For the inductive step, we let k be a natural number and assume that $P(k)$ is true. That is, assume that f_{3k} is an even natural number. This means that there exists an integer m such that

$$f_{3k} = 2m. \qquad \text{(Appendix B.14)}$$

We need to prove that $P(k+1)$ is true or that $f_{3(k+1)}$ is even. Notice that $3(k+1) = 3k+3$ and, hence, \(f_{3(k + 1) = f_{3k + 3}\). We can now use the recursion formula for the Fibonacci numbers to conclude that

$$f_{3k+3} = f_{3k+2} + f_{3k+1}\ .$$

Using the recursion formula again, we get $f_{3k+2} = f_{3k+1} + f_{3k}$. Putting this all together, we see that

$$\begin{aligned} f_{3(k+1)} &= f_{3k+3} \\ &= f_{3k+2} + f_{3k+1} \\ &= (f_{3k+1} + f_{3k}) + f_{3k+1} \\ &= 2f_{3k+1} + f_{3k}. \end{aligned} \qquad \text{(Appendix B.15)}$$

We now substitute the expression for f_{3k} in equation (B.14) into equation (B.15). This gives

$$\begin{aligned} f_{3(k+1)} &= 2f_{3k+1} + 2m \\ f_{3(k+1)} &= 2(f_{3k+1} + m) \end{aligned} \qquad \text{(Appendix B.16)}$$

This preceding equation shows that $f_{3(k+1)}$ is even. Hence it has been proved that if $P(k)$ is true, then $P(k+1)$ is true and the inductive step has been established. By the Principle of Mathematical Induction, this proves that for each natural number n, the Fibonacci number f_{3n} is an even natural number.

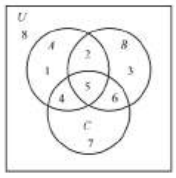
Section 5.1

Progress Check 5.3

A	$\not\subset, \not\subseteq, \neq$	B
5	$\in$	B
A	$\neq$	C
$\{1,2\}$	$\subset, \subseteq, \neq$	A
6	$\notin$	A

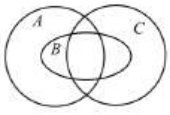
$\emptyset$	$\subset, \subseteq, \neq$	A
$\{5\}$	$\subset, \subseteq, \neq$	B
$\{1,2\}$	$\neq$	C
$\{4,2,1\}$	$\subseteq, =$	A
B	$\neq$	$\emptyset$

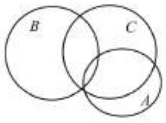
Progress Check 5.4

1. 

Using the standard Venn diagram for three sets shown above:

(a) For the set $(A \cap B) \cap C$, region 5 is shaded.
(b) For the set $(A \cap B) \cup C$, the regions 2, 4, 5, 6, 7 are shaded.
(c) For the set $(A^c \cup B)$, the regions 2, 3, 5, 6, 7, 8 are shaded.
(d) For the set $(A^c \cap (B \cup C))$, the regions 3, 6, 7 are shaded.

2. 

3. 

Section 5.2

Progress Check 5.8

$A = \{x \in \mathbb{Z} \mid x \text{ is multiple of } 9\}$ and $B = \{x \in \mathbb{Z} \mid x \text{ is a multiple of } 3\}$.

1. The set A is a subset of B. To prove this, we let $x \in A$. Then there exists an integer m such that $x = 9m$, which can be written as

$$x = 3(3m). \qquad \text{(Appendix B.17)}$$

Since $3m \in \mathbb{Z}$, the last equation proves that x is a multiple of 3 and so $x \in B$. Therefore, $A \subseteq B$.

2. The set A is not equal to the set B. We note that $3 \in B$ but $3 \notin A$. Therefore, $B \nsubseteq A$ and, hence, $A \neq B$.

Progress Check 5.9

Step	Know	Reason
P	$A \subseteq B$	Hypothesis
$P1$	Let $x \in B^c$.	Choose an arbitrary element of B^c.
$P2$	If $x \in A$, then $x \in B$.	Definition of "subset"
$P3$	If $x \notin B$, then $x \notin A$.	Contrapositive
$P4$	If $x \in B^c$, then $x \in A^c$.	Step $P3$ and definition of "complement"
$Q2$	The element x is in A^c.	Step $P1$ and $P4$
$Q1$	Every element of B^c is an element of A^c.	The choose-an-element method with Steps $P1$ and $Q2$.
Q	$B^c \subseteq A^c$	Definition of "subset"

Progress Check 5.12

Proof. Let A and B be subsets of some universal set. We will prove that $A - B = A \cap B^c$ by proving that each set is a subset of the other set. We will first prove that $A - B \subseteq A \cap B^c$. Let $x \in A - B$. We then know that $x \in A$ and $x \notin B$. However, $x \notin B$ implies that $x \in B^c$. Hence, $x \in A$ and $x \in B^c$, which means that $x \in A \cap B^c$. This proves that $A - B \subseteq A \cap B^c$.

To prove that $A \cap B^c \subseteq A - B$, we let $y \in A \cap B^c$. This means that $y \in A$ and $y \in B^c$, and hence, $y \in A$ and $y \notin B$. Therefore, $y \in A - B$ and this proves that $A \cap B^c \subseteq A - B$. Since we have proved that each set is a subset of the other set, we have proved that $A - B = A \cap B^c$.

Progress Check 5.15

Proof. Let $A = \{x \in \mathbb{Z} \mid x \equiv 3 \pmod{12}\}$ and $B = \{y \in \mathbb{Z} \mid y \equiv 2 \pmod{8}\}$. We will use a proof by contradiction to prove that $A \cap B = \emptyset$. So we assume that $A \cap B \neq \emptyset$ and let $x \in A \cap B$. We can then conclude that $x \equiv 3 \pmod{12}$ and that $x \equiv 2 \pmod{8}$. This means that there exist integers m and n such that

$$x = 3 + 12m \text{ and } x = 2 + 8n.$$

By equating these two expressions for x, we obtain $3 + 12m = 2 + 8n$, and this equation can be rewritten as $1 = 8n - 12m$. This is a contradiction since 1 is an odd integer and $8n - 12m$ is an even integer. We have therefore proved that $A \cap B = \emptyset$.

Section 5.3

Progress Check 5.19

1. In our standard configuration for a Venn diagram with three sets, regions 1, 2, 4, 5, and 6 are the shaded regions for both $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$.
2. Based on the Venn diagrams in Part (1), it appears that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Progress Check 5.21

1. Using our standard configuration for a Venn diagram with three sets, regions 1, 2, and 3 are the regions that are shaded for both $(A \cup B) - C$ and $(A - C) \cup (B - C)$.

2.
$$\begin{aligned}
(A \cup B) - C &= (A \cup B) \cap C^c && \text{(Theorem 5.20)} \\
&= C^c \cap (A \cup B) && \text{(Commutative Property)} \\
&= (C^c \cap A) \cup (C^c \cap B) && \text{(Distributive Property)} \\
&= (A \cap C^c) \cup (B \cap C^c) && \text{(Commutative Property)} \\
&= (A - C) \cup (B - C) && \text{(Theorem 5.20)}
\end{aligned}$$

Section 5.4

Progress Check 5.23

1. Let $A = \{1, 2, 3\}$, $T = \{1, 2\}$, $B = \{a, b\}$, and $C = \{a, c\}$.

(a) $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$
(b) $T \times B = \{(1, a), (1, b), (2, a), (2, b)\}$
(c) $A \times C = \{(1, a), (1, c), (2, a), (2, c), (3, a), (3, c)\}$
(d) $A \times (B \cap C) = \{(1, a), (2, a), (3, a)\}$
(e) $(A \times B) \cap (A \times C) = \{(1, a), (2, a), (3, a)\}$
(f) $A \times (B \cup C) = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c)\}$

(g) $(A \times B) \cup (A \times C) = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c),(3,a),(3,b),(3,c)\}$
(h) $A \times (B - C) = \{(1,b),(2,b),(3,b)\}$
(i) $(A \times B) - (A \times C) = \{(1,b),(2,b),(3,b)\}$
(j) $B \times A = \{(a,1),(b,1),(a,2),(b,2),(a,3),(b,3)\}$

2. $T \times B \subseteq A \times B$ $\quad A \times (B \cup C) = (A \times B) \cup (A \times C)$
$A \times (B \cap C) = (A \times B) \cap (A \times C)$ $\quad A \times (B - C) = (A \times B) - (A \times C)$

Progress Check 5.24

1. (a) $A \times B = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \le x \le 2 \text{ and } 2 \le y < 4\}$
(b) $T \times B = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 1 < x < 2 \text{ and } 2 \le y < 4\}$
(c) $A \times C = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \le x \le 2 \text{ and } 3 < y \le 6\}$
(d) $A \times (B \cap C) = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \le x \le 2 \text{ and } 3 < y < 4\}$
(e) $(A \times B) \cap (A \times C) = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \le x \le 2 \text{ and } 3 < y < 4\}$
(f) $A \times (B \cup C) = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \le x \le 2 \text{ and } 2 \le y \le 5\}$
(g) $(A \times B) \cup (A \times C) = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \le x \le 2 \text{ and } 2 \le y \le 5\}$
(h) $A \times (B - C) = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \le x \le 2 \text{ and } 2 \le y \le 3\}$
(i) $(A \times B) - (A \times C) = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \le x \le 2 \text{ and } 2 \le y \le 3\}$
(j) $B \times A = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 2 \le x < 4 \text{ and } 0 \le y \le 2\}$
2. $T \times B \subseteq A \times B$
$A \times (B \cap C) = (A \times C) \cap (A \times C)$
$A \times (B \cup C) = (A \times C) \cup (A \times C)$
$A \times (B - C) = (A \times C) - (A \times C)$

Section 5.5

Progress Check 5.26

1. $\bigcup_{j=1}^{6} A_j = \{1,2,3,4,5,6,9,16,25,36\}$
2. $\bigcap_{j=1}^{6} A_j = \{1\}$
3. $\bigcup_{j=3}^{6} A_j = \{3,4,5,6,9,16,25,36\}$
4. $\bigcap_{j=3}^{6} A_j = \{1\}$
5. $\bigcup_{j=1}^{\infty} A_j = \mathbb{N}$
6. $\bigcap_{j=1}^{\infty} A_j = \{1\}$

Progress Check 5.27

1. $A_1 = \{7,14\}$, $A_2 = \{10,12\}$, $A_3 = \{10,12\}$, $A_4 = \{8,14\}$.
2. The statement is false. For example, $2 \neq 3$ and $A_2 = A_3$.
3. The statement is false. For example, $1 \neq -1$ and $B_1 = B_{-1}$.

Progress Check 5.29

1. Since $\bigcup_{\alpha \in \mathbb{R}^+} A_\alpha = (-1, \infty)$, $(\bigcup_{\alpha \in \mathbb{R}^+} A_\alpha)^c = (-\infty, 1]$.
2. $\bigcap_{\alpha \in \mathbb{R}^+} A_\alpha^c = (-\infty, -1]$.
3. Since $\bigcap_{\alpha \in \mathbb{R}^+} A_\alpha = (-1, 0]$, $(\bigcap_{\alpha \in \mathbb{R}^+} A_\alpha)^c = (-\infty, 1] \cup (0, \infty)$.
4. $\bigcup_{\alpha \in \mathbb{R}^+} A_\alpha^c = (-\infty, -1] \cup (0, \infty)$.

Progress Check 5.32

All three families of sets ($\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ are disjoint families of sets. One the family $\mathcal{A}$ is a pairwise disjoint family of sets.

Section 6.1

Progress Check 6.1

1. $f(-3) = 24$
$f(\sqrt{8}) = 8 - 5\sqrt{8}$
2. $g(2) = -6, g(-2) = 14$
3. {-1, 6}
4. {-1, 6}
5. $\{\frac{5+\sqrt{33}}{2}, \frac{5-\sqrt{33}}{2}\}$
6. $\emptyset$

Progress Check 6.2

1. (a) The domain of the function f is the set of all people.
(b) A codomain for the function f is the set of all days in a leap year.

(c) This means that the range of the function f is equal to its codomain.
2. (a) The domain of the function s is the set of natural numbers.
(b) A codomain for the function s is the set of natural numbers.
(c) This means that the range of s is not equal to the set o natural numbers.

Progress Check 6.3

1. $f(-1) \approx -3$ and $f(2) \approx -2.5$.
2. Values of x for which $f(x) = 2$ are approximately -2.8, -1.9, 0.3, 1.2, and 3.5.
3. The range of f appears to be the closed interval [-3.2, 3.2] or $\{y \in \mathbb{R} \mid -3.2 \leq y \leq 3.2\}$.

Progress Check 6.4

Only the arrow diagram in Figure (a) can be used to represent a function from A to B. The range of this function is the set $\{a, b\}$.

Section 6.2

Progress Check 6.5

1. $f(0) = 0$, $f(1) = 1$, $f(2) = 1$, $f(3) = 1$, $f(4) = 1$.
2. $g(0) = 0$, $g(1) = 1$, $g(2) = 2$, $g(3) = 3$, $g(4) = 4$.

Progress Check 6.6

$I_{\mathbb{Z}_5} \neq f$ and $I_{\mathbb{Z}_5} = g$

Progress Check 6.7

1. 3.5
2. 4.02
3. \(\dfrac{\pi + \sqrt{2}{4}\)
4. The process of finding the average of a finite set of real numbers can be thought of as a function from $\mathcal{F}(\mathbb{R})$ to $\mathbb{R}$. So the domain is $\mathcal{F}(\mathbb{R})$, the codomain is $\mathbb{R}$, and we can define a function avg: $\mathcal{F}(\mathbb{R}) \to \mathbb{R}$ as follows: If $A \in \mathcal{F}(\mathbb{R})$ and $A = \{a_1, a_2, \ldots, a_n\}$, then ave $(A) = \dfrac{a_1 + a_2 + \cdots a_n}{n}$.

Progress Check 6.8

1. The sixth terms is $\dfrac{1}{18}$ and the tenth term is $\dfrac{1}{30}$.
2. The sixth terms is $\dfrac{1}{36}$ and the tenth term is $\dfrac{1}{100}$.
3. The sixth terms is 1 and the tenth term is 1.

Progress Check 6.9

1. $g(0, 3) = -3$; $g(3, -2) = 11$; $g(-3, -2) = 11$; $g(7, -1) = 50$.
2. $\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid n = m^2\}$
3. $\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid n = m^2 - 5\}$

Section 6.3

Progress Check 6.10

The functions k, F, and s are injections. The functions f and h are not injections.

Progress Check 6.11

The functions f and s are surjections. The functions k and F are not surjections.

Progress Check 6.15

The function f is an injection but not a surjection. To see that it is an injection, let $a, b \in \mathbb{R}$ and assume that $f(a) = f(b)$. This implies that $e^{-a} = e^{-b}$. Now use the natural logarithm function to prove that $a = b$. Since $e^{-x} > 0$ for each real number x, there is no $x \in \mathbb{R}$ such that $f(x) = -1$. So f is not a surjection.

The function g is an injection and is a surjection. The proof that g is an injection is basically the same as the proof that f is an injection. To prove that g is a surjection, let $b \in R_+$. To construct the real number a such that g.a/ D b, solve the equation $e^{-a} = b$ for a. The solution is $a = -\ln b$. It can then be verified that $g(a) = b$.

Progress Check 6.16

1. There are several ordered pairs $(a, b) \in \mathbb{R} \times \mathbb{R}$ such that $g(a, b) = 2$. For example, $g(0, 2) = 2$, $g(-1, 4) = 2$, and $g(2, -2) = 2$.
2. For each $z \in \mathbb{R}$, $g(0, z) = z$.
3. Part (1) implies that the function g is not an injection. Part (2) implies that the function g is a surjection since for each $z \in \mathbb{R}$, $(0, z)$ is in the domain of g and $g(0, z) = z$.

Section 6.4

Progress Check 6.17

The arrow diagram for $g \circ f : A \to B$ should show the following:

$$\begin{aligned} (g\circ f)(a) &= g(f(a)) & (g\circ f)(b) &= g(f(b)) \\ &= g(2) = 1 & &= g(3) = 2 \\ (g\circ f)(c) &= g(f(c)) & (g\circ f)(d) &= g(f(d)) \\ &= g(1) = 3 & &= g(2) = 1 \end{aligned}$$

The arrow diagram for $g \circ g : B \to B$ should show the following:

$$\begin{aligned} (g\circ f)(1) &= g(g(1)) & (g\circ g)(2) &= g(g(2)) \\ &= g(3) = 2 & &= g(1) = 3 \\ (g\circ g)(3) &= g(g(3)) & & g(f(d)) \\ &= g(2) = 1 \end{aligned}$$

Progress Check 6.18

1. $F = g \circ f$, where $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = x^2 + 3$, and $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^3$.
2. $G = h \circ f$, where $f : \mathbb{R} \to \mathbb{R}^+$ by $f(x) = x^2 + 3$, and $h : \mathbb{R}^+ \to \mathbb{R}$ by $h(x) = \text{In}x$.
3. $f = g \circ k$, where $k : \mathbb{R} \to \mathbb{R}$ by $k(x) = x^2 - 3$, and $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = |x|$.
4. $g = h \circ f$, where $f : \mathbb{R} \to \mathbb{R}$ by $f(x) = \dfrac{2x-3}{x^2+1}$, and $h : \mathbb{R} \to \mathbb{R}$ by $h(x) = \cos x$.

Progress Check 6.19

For the examples that are constructed:

1. $g \circ f$ should be an injection.
2. $g \circ f$ should be a surjection.
3. $g \circ f$ should be a bijection.

Section 6.5

Progress Check 6.23

Neither set can be used to define a function.

1. The set F does not satisfy the first condition of Theorem 6.22.
2. The set G does not satisfy the second condition of Theorem 6.22.

Progress Check 6.24

2. $f^{-1} = \{(r, a), (p, b), (q, c)\}$
$h^{-1} = \{(p, a), (q, b), (r, c), (q, d)\}$
$g^{-1} = \{(p, a), (q, b), (p, c)\}$

3. (a) f^{-1} is a function from C to A.
(b) g^{-1} is not a function from C to A since $(p, a) \in g^{-1}$ and $(p, c) \in g^{-1}$.
(c) h^{-1} is not a function from C to B since $(q, b) \in h^{-1}$ and $(q, d) \in h^{-1}$.

5. In order for the inverse of a function $F : S \to T$ to be a function from T to S, the function F must be a bijection.

Section 6.6

Progress Check 6.30

1. $f(A) = \{s, t\}$
2. $f(B) = \{f(x) \mid x \in b\} = \{x\}$
3. $f^{-1}(C) = \{x \in S \mid f(x) \in C\} = \{a, b, c, d\}$
4. $f^{-1}(D) = \{x \in S \mid f(x) \in D\} = \{a, d\}$

Progress Check 6.32

1. $f(0) = 2$ $f(2) = 6$ $f(4) = 2$ $f(6) = 6$
   $f(1) = 3$ $f(3) = 3$ $f(5) = 3$ $f(7) = 3$
2. (a) $f(A) = \{2, 3, 6\}$ $f^{-1}(C) = \{0, 1, 3, 4, 5, 7\}$
   $f(B) = \{2, 3, 6\}$ $f^{-1}(D) = \{1, 3, 5, 7\}$
3. (a) $f(A) \cap f(B) = \{2\}$ $f(A) \cap f(B) = \{2, 3, 6\}$
   So in this case, $f(A \cap B) \subseteq f(A) \cap f(B)$.
   (b) $f(A) \cup f(B) = \{2, 3, 6\}$ $f(A \cup B) = \{2, 3, 6\}$

So in this case, $f(A \cap B) \subseteq f(A \cup B)$.
(c) $f^{-1}(C) \cap f^{-1}(D) = f^{-1}(C \cap D) = \{1, 3, 5, 7\}$. So in this case, $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.
(d) $f^{-1}(C) \cup f^{-1}(D) = f^{-1}(C \cup D) = \{0, 1, 3, 4, 5, 7\}$. So in this case, $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
4. $f(A) = \{2, 3, 6\}$. Hence, $f^{-1}(f(A)) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ So in this case, $A \subseteq f^{-1}(f(A))$.

Section 7.1

Progress Check 7.2

1. (a) T is a relation on $\mathbb{R}$ since S is a subset of $\mathbb{R} \times \mathbb{R}$.
(b) Solve the equation $x^2 + 4^2 = 64$. This gives $x = \pm\sqrt{48}$.
Solve the equation $x^2 + 9^2 = 64$. There are no real number solutions. So there does not exist an $x \in \mathbb{R}$ such that $(x, 9) \in S$.
(c) dom$(T) = \{x \in \mathbb{R} \mid -8 \leq x \leq 8\}$ range$(T) = \{y \in \mathbb{R} \mid -8 \leq y \leq 8\}$
(d) The graph is a circle of radius 8 whose center is at the origin.
2. (a) R is a relation on A since R is a subset of $A \times A$.
(b) If we assume that each state except Hawaii has a land border in common with itself, then the domain and range of R are the set of all states except Hawaii. If we do not make this assumption, then the domain and range are the set of all states except Hawaii and Alaska.
(c) The first statement is true. If x has a land border with y, then y has a land border with x. The second statement is false. Following is a counterexample: (Michigan, Indiana) $\in R$, (Indiana, Illinois) $\in R$, but (Michigan, Illinois) $\notin R$.

Progress Check 7.3

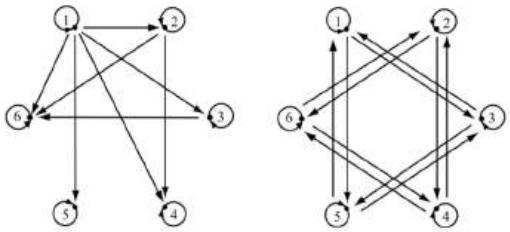
1. The domain of the divides relation is the set of all nonzero integers. The range of the divides relation is the set of all integers.
2. (a) This statement is true since for each $a \in \mathbb{Z}$, $a = a \cdot 1$.
(b) This statement is false: For example, 2 divides 4 but 4 does not divide 2.
(c) This statement is true by Theorem 3.1 on page 88.

Progress Check 7.4

1. Each element in the set F is an ordered pair of the form (x, y) where $y = x^2$.
2. (a) $A = \{-2, 2\}$
(b) $B = \{-\sqrt{10}, \sqrt{10}\}$
(c) $C = \{25\}$
(d) $D = \{9\}$
3. The graph of $y = x^2$ is a parabola with vertex at the origin that is concave up.

Progress Check 7.5

The directed graph for Part (a) is on the left and the directed graph for Part (b) is on the right.



Section 7.2

Progress Check 7.7

The relation R:

- Is not reflexive since $(c, c) \notin R$ and $(d, d) \notin R$.
- Is symmetric.
- Is not transitive. For example, $(c, a) \in R$, $(a, c) \in R$, but $(c, c) \notin R$.

Progress Check 7.9

- Proof that the relation $\sim$ is symmetric: Let $a, b \in \mathbb{Q}$ and assume that $a \sim b$. This means that $a - b \in \mathbb{Z}$. Therefore, $-(a - b) \in \mathbb{Z}$ and this means that $b - a \in \mathbb{Z}$, and hence, $b \sim a$.
- Proof that the relation $\sim$ is transitive: Let $a, b, c \in \mathbb{Q}$and assume that $a \sim b$ and $b \sim c$. This means that $a - b \in \mathbb{Z}$ and that $b - c \in \mathbb{Z}$. Therefore, $((a - b) + (b - c)) \in \mathbb{Z}$ and this means that $a - c \in \mathbb{Z}$, and hence, $a \sim c$.

Progress Check 7.11

The relation $\approx$ is reflexive on $\mathcal{P}(U)$ since for all $A \in \mathcal{P}(U)$, card(A)= card(A).

The relation $\approx$ is symmetric since for all $A, B \in \mathcal{P}(U)$, if card(A) = card(B), then using the fact that equality on $\mathbb{Z}$ is symmetric, we conclude that card(B) = card(A). That is, if A has the same number of elements as B, then B has the same number of elements as A.

The relation $\approx$ is transitive since for all $A, B, C \in \mathcal{P}(U)$, if card($A$) = card($B$) and card($B$) = card($C$), then using the fact that equality on $\mathbb{Z}$ is transitive, we conclude that card(A) = card(C). That is, if A and B have the same number of elements and B and C have the same number of elements, then A and C have the same number of elements.

Therefore, the relation $\approx$ is an equivalence relation on $\mathcal{P}(U)$.

Section 7.3

Progress Check 7.12

The distinct equivalence classes for the relation R are: $\{a, b, e\}$ and $\{c, d\}$.

Progress Check 7.13

The distinct congruence classes for congruence modulo 4 are

[0] = {..., -12, -8, -4, 0, 4, 8, 12, ...} [1] = {..., -11, -7, -3, 1, 5, 9, 13, ...}
[2] = {..., -10, -6, -2, 2, 6, 10, 14, ...} [1] = {..., -9, -5, -1, 3, 7, 11, 15, ...}

Progress Check 7.15

1. [5] = [-5] = {-5, 5} [π] = [-π] = {-π, π}
   [10] = [-10] = {-10, 10}
2. [0] = {0}
3. [a] = {-a, a}

Section 7.4

Progress Check 7.2

1. $\oplus$ | [0] | [1] — [0] | [0] | [1] — [1] | [1] | [0]

   $\odot$ | [0] | [1] — [0] | [0] | [0] — [1] | [0] | [1]

2. $\oplus$ | [0] | [1] | [2] | [3] | [4] | [5] —
   [0] | [0] | [1] | [2] | [3] | [4] | [5] —
   [1] | [1] | [2] | [3] | [4] | [5] | [0] —
   [2] | [2] | [3] | [4] | [5] | [0] | [1] —
   [3] | [3] | [4] | [5] | [0] | [1] | [2] —
   [4] | [4] | [5] | [0] | [1] | [2] | [3] —
   [5] | [5] | [0] | [1] | [2] | [3] | [4]

   $\odot$ | [0] | [1] | [2] | [3] | [4] | [5] —
   [0] | [0] | [0] | [0] | [0] | [0] | [0] —
   [1] | [0] | [1] | [2] | [3] | [4] | [5] —
   [2] | [0] | [2] | [4] | [0] | [2] | [4] —
   [3] | [0] | [3] | [0] | [3] | [0] | [3] —
   [4] | [0] | [4] | [2] | [0] | [4] | [2] —
   [5] | [0] | [5] | [4] | [3] | [2] | [1]

3. For all $a, b \in \mathbb{Z}$, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.
4. The statement in (a) is true and the statement in (b) is false. For example, in $\mathbb{Z}_6$, $[2] \odot [3] = [0]$.

Section 8.1

Progress Check 8.2

1. The remainder is 8.
2. gcd(12, 8) = 4
3. $12 = 8 \cdot 1 + 4$ and gcd(r, r_2) = gcd(8, 4) = 4.

Progress Check 8.4

1.

Original Pair	Equation from Division Algorithm	New Pair
(180, 126)	$180 = 126 \cdot 1 + 54$	(126, 54)
(126, 54)	$126 = 54 \cdot 2 + 18$	(54, 18)
(54, 18)	$54 = 18 \cdot 3 + 0$	

Consequently, gcd(180, 126) = 18.

2.

Original Pair	Equation from Division Algorithm	New Pair
(4208, 288)	$4208 = 288 \cdot 14 + 176$	(288, 176)
(288, 176)	$288 = 126 \cdot 1 + 112$	(176, 112)
(176, 112)	$176 = 112 \cdot 1 + 64$	(112, 64)
(112, 64)	$112 = 64 \cdot 1 + 48$	(64, 48)
(64, 48)	$64 = 48 \cdot 1 + 16$	(48, 16)

(48, 16)	$48 = 16 \cdot 3 + 0$

Consequently, gcd(4208. 288) = 16.

Progress Check 8.7

1. From Progress Check 8.4, gcd(180, 126) = 18.

$$\begin{aligned} 18 &= 126 - 54 \cdot 2 \\ &= 126 - (180 - 126) \cdot 2 \\ &= 126 \cdot 3 + 180 \cdot (-2) \end{aligned} \qquad \text{(Appendix B.18)}$$

So gcd(180, 126) = 18, and $18 = 126 \cdot 3 + 180 \cdot (-2)$.

2. From Progress Check 8.4, gcd(4208. 288) = 16.

$$\begin{aligned} 16 &= 64 - 48 \\ &= 64 - (112 - 64) = 64 \cdot 2 - 112 \\ &= (176 - 112) \cdot 2 - 112 = 176 \cdot 2 - 112 \cdot 3 \quad = \quad 176 \cdot 2 - (288 - 176) \cdot 3 = 176 \cdot 5 - 288 \cdot 3 \\ &= (4208 - 288 \cdot 14) \cdot 5 - 288 \cdot 3 \\ &= 4208 \cdot 5 + 288 \cdot (-73) \end{aligned} \qquad \text{(Appendix B.19)}$$

So gcd(4208. 288) = 16, and $16 = 4208 \cdot 5 + 288 \cdot (-73)$.

Section 8.2

Progress Check 8.10

1. If $a, p \in \mathbb{Z}$, p is prime, and p divides a, then gcd(a, p) = p.
2. If $a, p \in \mathbb{Z}$, p is prime, and p does not divide a, then gcd(a, p) = 1.
3. Three examples are gcd(4, 9) = 1, gcd(15, 16) = 1, gcd(8, 25) = 1.

Progress Check 8.13

Theorem 8.12. Let a, b, and c be integers. If a and b are relatively prime and $a \mid (bc)$. We will prove that a divides c.

Proof. Let a, b, and c be integers. Assume that a and b are relatively prime and $a \mid (bc)$. We will prove that a divides c.

Since a divides bc, there exists an integer k such that

$$bc = ak. \qquad \text{(Appendix B.20)}$$

In addition, we are assuming that a and b are relatively prime and hence gcd(a, b) = 1. So by Theorem 8.9, there exist integers m and n such that

$$am + bn = 1. \qquad \text{(Appendix B.21)}$$

We now multiply both sides of equation (B.21) by c. This gives

$$\begin{aligned} (am + bn)c &= 1 \cdot c \\ acm + bcn &= c \end{aligned} \qquad \text{(Appendix B.22)}$$

We can now use equation (B.20) to substitute $bc = ak$ in equation (B.22) and obtain

$$acm + akn = c.$$

If we now factor the left side of this last equation, we see that $a(cm + kn) = c$. Since $(cm + kn)$ is an integer, this proves that a divides c. Hence, we have proven that if a and b are relatively prime and $a \mid (bc)$, then $a \mid c$.

Section 8.3

Progress Check 8.20

2. $x = 2 + 3k$ and $y = 0 - 2k$, where k can be any integer. Again, this does not prove that these are the only solutions.

Progress Check 8.21

One of the Diophantine equations in Preview Activity 2 was $3x + 5y = 11$. We were able to write the solutions of this Diophantine equation in the form

$$x = 2 + 5k \text{ and } y = 1 - 3k,$$

where k is an integer. Notice that $x = 2$ and $y = 1$ is a solution of this equation. If we consider this equation to be in the form $ax + by = c$, then we see that $a = 3$, $b = 5$, and $c = 11$. Solutions for this equation can be written in the form

$$x = 2 + bk \text{ and } y = 1 - ak,$$

where k is an integer.

The other equation was $4x+6y=16$. So in this case, $a=4$, $b=6$, and $c=16$. Also notice that $d=\gcd(4,6)=2$. We note that $x=4$ and $y=0$ is one solution of this Diophantine equation and solutions can be written in the form

$$x=4+3k \text{ and } y=0-2k,$$

where k is an integer. Using the values of a, b, and d given above, we see that the solutions can be written in the form

$$x=2+\frac{b}{d}k \text{ and } y=0-\frac{a}{d},$$

where k is an integer.

Progress Check 8.24

1. Since 21 does not divide 40, Theorem 8.22 tells us that the Diophantine equation $63x+336y=40$ has no solutions. Remember that this means there is no ordered pair of integers (x, y) such that $63x+336y=40$. However, if we allow x and y to be real numbers, then there are real number solutions. In fact, we can graph the straight line whose equation is $63x+336y=40$ in the Cartesian plane. From the fact that there is no pair of integers x, y such that $63x+336y=40$, we can conclude that there is no point on the graph of this line in which both coordinates are integers.
2. To write formulas that will generate all the solutions, we first need to find one solution for $144x+225y=27$. This can sometimes be done by trial and error, but there is a systematic way to find a solution. The first step is to use the Euclidean Algorithm in reverse to write gcd(144, 225) as a linear combination of 144 and 225. See Section 8.1 to review how to do this. The result from using the Euclidean Algorithm in reverse for this situation is

$$144\cdot 11+225\cdot(-7)=9. \tag{Appendix B.23}$$

If we multiply both sides of this equation by 3, we obtain

$$144\cdot 33+225\cdot(-21)=27. \tag{Appendix B.24}$$

This means that $x_0=33$, $y_0=-21$ is a solution of the linear Diophantine equation $144x+225y=27$. We can now use Theorem 8.22 to conclude that all solutions of this Diophantine equation can be written in the form

$$x=33+\frac{225}{9}k \qquad y=-21-\frac{144}{9}k, \tag{Appendix B.25}$$

where $k\in\mathbb{Z}$.
We check this general solution as follows: Let $k\in\mathbb{Z}$. Then

$$\begin{aligned} 144x+225y &= 144(33+25k)+225(-21-16k) \\ &= (4752+3600k)+(-4725-3600k) \\ &= 27. \end{aligned} \tag{Appendix B.26}$$

Section 9.1

Progress Check 9.2

1. We first prove that $f:A\to B$ is an injection. So let $x, y\in A$ and assume that $f(x)=f(y)$. Then $x+350=y+350$ and we can conclude that $x=y$. Hence, f is an injection. To prove that f is a surjection, let $b\in B$. Then $351\le b\le 450$ and hence, $1\le b-350\le 100$ and so $b-350\in A$. In addtion, $f(b-350)=(b-350)+350=b$. This proves that f is a surjection, Hence, the function f is a bijection, and so, $A\approx B$.
2. If x and t are even integers and $F(x)=F(t)$, then $x+1=t+1$ and, hence, $x=t$. Therefore, F is an injection.
To prove that F is a surjection, let $y\in D$. This means that y is an odd integer and, hence, $y-1$ is an even integer. In addition,

$$F(y-1)=(y-1+1=y. \tag{Appendix B.27}$$

Therefore, F is a surjection and hence, F is a bijection. We conclude that $E\approx D$.
3. Let $x, t\in(0,1)$ and assume that $f(x)=f(t)$. Then $bx=bt$ and, thence, $x=t$. Therefore, f is an injection.
To prove that f is a surjection, let $y\in(0,b)$. Since $0<y<b$, we conclude that $0<\frac{y}{b}<1$ and that

$$f(\frac{y}{b})-b(\frac{y}{b}\backslash)=y. \tag{Appendix B.28}$$

Therefore, f is a surjection and hence f is a bijection. Thus, $(0,1)\approx(0,b)$.

Section 9.2

Progress Check 9.11

1. The set of natural numbers $\mathbb{N}$ is a subset of $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$. Since $\mathbb{N}$ is an infinite set, we can use Part (2) of Theorem 9.10 to conclude that $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ are infinite sets.
2. Use Part (1) of Theorem 9.10.
3. Prove that $\mathbb{E}^+ \approx \mathbb{N}$ and use Part (1) of Theorem 9.10.

Progress Check 9.12

1. Use the definition of a countably infinite set.
2. Since $\mathbb{E}^+ \approx \mathbb{N}$, we can conclude that card$(E^+) = \aleph_0$.
3. One function that can be used is $f : S \to \mathbb{N}$ defined by $f(m) = \sqrt{m}$ for all $m \in S$.

Progress Check 9.23

Player Two has a winning strategy. On the kth turn, whatever symbol Player One puts in the kth position of the kth row, Player Two must put the other symbol in the kth position of his or her row. This guarantees that the row of symbols produced by Player Two will be different that any of the rows produced by Player One.

This is the same idea used in Cantor's Diagonal Argument. Once we have a "list" of real numbers in normalized form, we create a real number that is not in the list by making sure that its kth decimal place is different than the kth decimal place for the kth number in the list. The one complication is that we must make sure that our new real number does not have a decimal expression that ends in all 9's. This was done by using only 3's and 5's.

Progress Check 9.25

1. ***Proof***. In order to find a bijection $f : (0, 1) \to (a, b)$, we will use the linear function through the points $(0, a)$ and $(1, b)$. The slope is $(b - a)$ and the y-intercept is $(0, a)$. So define $f : (0, 1) \to (a, b)$ by

$$f(x) = (b - a)x + a, \text{for each } x \in (0, 1). \qquad \text{(Appendix B.29)}$$

   Now, if $x, t \in (0, 1)$ and $f(x) = f(t)$, then

$$(b - a)x + a = (b - a)t + a. \qquad \text{(Appendix B.30)}$$

   This implies that $(b - a)x = (b - a)t$, and since $b - a \neq 0$, e can conclude that $x = t$. Therefore, f is an injection.

   To prove that f is a surjection, we let $y \in (a, b)$. If $x = \dfrac{y - a}{b - a}$, then

\begin{array} {rcl} {f(x)} &= & {f(\dfrac{y - a}{b - a})} \\ {} &= & {(b - a) (\dfrac{y - a}{b - a}) + a} \\ {} &= & {(y - a) + a} \\ {} &= & {y} \begin{array}

   This proves that f is a surjection. Hence, f is a bijection and $(0, 1) \approx (a, b)$. Therefore, (a, b) is uncountable and has cardinality c.
2. Now, if a, b, c, d are real number with $a < b$ and $c < d$, then we know that

$$(a, b) \approx (0, 1) \text{ and } (c, d) \approx (0, 1). \qquad \text{(Appendix B.31)}$$

   Since $\approx$ is an equivalence relation, we can conclude that $(a, b) \approx (c, d)$.

Appendix C: Answers and Hints for Selected Exercises

Section 1.1

1. Sentences (a), (c),(e), (f), (j) and (k) are statements. Sentence (h) is a statement if we are assuming that n is a prime number means that n is an integer.

2.

	Hypothesis	Conclusion
a.	n is a prime number.	n^2 has three positive divisors.
b.	a is an irrational number and b is an irrational number.	$a \cdot b$ is an irrational number.
c.	p is a prime number.	$p = 2$ or p is an odd number.
d.	p is a prime number and $p \neq 2$.	p is an odd number.

3. Statements (a), (c), and (d) are true.
4. (a) True when $a \neq 3$. (b) True when $a = 3$.

6. (a) This function has a maximum value when $x = \dfrac{5}{16}$.
(c) No conclusion can be made about this function.

9. (a) The set of rational numbers is not closed under division.
(b) The set of rational number sis not closed undre division since division by zero is not defined.
(c) The set of nonzero rational numbers is closed under division.
(d) The set of positive rational numbers is closed under division.
(e) The set of positive real numbers is not closed under subtraction.
(f)The set of negative rational numbers is not closed under division.
(g)The set of negative integers is closed under addition.

Section 1.2

1. (a)

Step	Know	Reason
P	m is an even integer.	Hypothesis
$P1$	There exists an integers k such that $m = 2k$.	Definition of an even integer
$P2$	$m+1 = 2k+1$	Algebra
$Q1$	There exists an integer q such that $m+1 = 2q+1$.	Substitution of $k = q$
Q	$m+1$ is an odd integer.	Definition of an odd integer

2. (c) We assume that x and y are odd integers and will prove that $x+y$ is an even integer. Since x and y are odd, there exist integers m and n such that $x = 2m+1$ and $y = 2n+1$. Then

$$\begin{aligned} x+y &= (2m+1)+(2n+1) \\ &= 2m+2n+2 \\ &= 2(m+n+1). \end{aligned} \qquad \text{(Appendix C.1)}$$

Since the integers are closed under addition, $(m+n+1)$ is an integer, and hence the last equation shows that $x+y$ is even. Therefore, we have proven that if x and y are odd integers, then $x+y$ is an even integer.
3. (b) Use Part (a) to prove this.

6. (a) Prove that their difference is equal to zero or prove that they are not zero and their quotient is equal to 1.
(d) Provethattwoofthesideshavethesamelength.Provethatthetriangle has two congruent angles. Prove that an altitude of the triangle

is a perpendicular bisector of a side of the triangle.

9. (a) Some examples of type 1 integers are -5, -2, 1, 4, 7, 10.
(c) All example should indicate the proposition is true.

10. (a) Let a and b be integers and assume that a and b are both type 1 integers. Then, there exist integers m and n such that $a = 3m + 1$ and $b = 3n + 1$. Now show that

$$a + b = 3(m + n) + 2.$$

The closure properties of the integers imply that $m + n$ is an integer. Therefore, the last equation tells us that $a + b$ is a type 2 integer. Hence, we have proved that if a and b are both type 1 integers, then $a + b$ is a type 2 integer.

Section 2.1

1. The statement was true. When the hypothesis is false, the conditional statement is true.

2. (a) P is false .
(b) $P \wedge Q$ is false.
(c) $P \vee Q$ is false.

4. (c) Cannot tell if $P \wedge R$ is true or false.

5. Statements (a) and (d) have the same truth table. Statements (b) and (c) have the same truth tables.

7. The two statements have the same truth table.

9. (c) The integer x is even only if x^2 is even.
(d) The integer x^2 is even is necessary for x to be even.

Section 2.2

1. (a) Converse: If $a^2 = 25$, then $a = 5$. Contrapositive: If $a^2 \neq 25$, then $a \neq 5$.
(b) Converse: If Laura is playing golf, then it is not raining. Contrapositive: If Laura is not playing golf, then it is raining.

2. (a) Disjunction: $a \neq 5$ or $a^2 = 25$. Negation: $a = 5$ and $a^2 = 25$.
(b) Disjunction: It is raining or Laura is playing golf. Negation: It is not raining and Laura is not playing golf.

3. (a) We will not win the first game or we will not win the second game.
(c) You mow the lawn and I will not pay you $20.
(f) You graduate from college, and you will not get a job and you will not go to graduate school.

7. (a) In this case, it may be better to work with the right side first.

$$\begin{aligned} (P \to R) \vee (Q \to R) &\equiv (\neg R \vee R) \vee (\neg Q \vee R) \\ &\equiv (\neg R \vee \neg Q) \vee (R \vee R) \\ &\equiv (\neg R \vee \neg Q) \vee R \qquad \equiv \neg(P \vee Q) \vee R \\ &\equiv (P \wedge Q) \to R. \end{aligned}$$

10. Statements (c) and (d) are logically equivalent to the given conditional statement. Statement (f) is the negation of the given conditional statement.
11. (d) This is the contrapositive of the given statement and hence, it is logically equivalent to the given statement.

Section 2.3

1. (a) $\frac{1}{2}, -2\}$
(d) $\{1, 2, 3, 4\}$
(e) $\{0.5, 4.5\}$

2. $A = \{n^2 \mid n \in \mathbb{N}$
$D = \{4n \mid n$is a nonnegative integer and $0 \leq n \leq 25\}$

3. The sets in (b) and (c) are equal to the given set.

5. (a) $\{x \in \mathbb{Z} \mid x \leq 5\}$
(e) \(\{x \in \mathbb{R}\ |\ x^2 > 10\}\)

Section 2.4

1. (a) There exists a rational number x such that $x^2 - 3x - 7 = 0$. This statement is false since the solutions of the equation are $x = \dfrac{3 \pm \sqrt{37}}{2}$, which are irrational numbers.

2. (b) $x = 0$ is a counterexample. The negation is: There exists a real number x such that $x^2 \leq 0$.
(g) $x = \dfrac{\pi}{2}$ is a counterexample. The negation is: There exists a real number x such that $\tan^2 x + 1 \neq \sec^2 x$.

3. (a) There exists a rational number x such that $x > \sqrt{2}$.
The negation is $(\forall x \in \mathbb{Q})(x \leq \sqrt{2})$, which is, For each rational number x, $x \leq \sqrt{2}$.

(c) For each integer x, x is even or x is odd.
The negation is $(\exists x \in \mathbb{Z}$ (x is odd and x is even), which is, There exists an integer x such that x is odd and x is even.

(e) For each integer x, if x^2 is odd, then x is odd.
The negation is $(\exists x \in \mathbb{Z}$ (x^2 is odd and x is even), which is, There exists an integer x such that x^2 is odd and x is even.
(h) There exists a real number x such that cos(2x) = 2 (cos$x$).
The negation is $(\forall x \in \mathbb{R}$ (cos(2x) $\neq$ 2(cos$x$)), which is, For each real number x, cos(2x) $\neq$ 2(cos$x$).

4. (a) There exist integers m and n such that $m > n$.
(c) There exists an integer n such that for each ineger m, $m^2 > n$.

5. (a) $(\forall m)(\forall n)(m \leq n)$.
For all inetgers m and n, $m \leq n$.
(e) $(\forall n)(\exists m)(m^2 \leq n)$.
For each integer n, there exists an integer m such that $m^2 \leq n$.

10. (a) A function f with domain $\mathbb{R}$ is strictly increasing provided that $(\forall x, y \in \mathbb{R})[(x < y) \rightarrow (f(x) < f(y))]$.

Section 3.1

1. (a) Remember that to prove that $a \mid (b - c)$, you need to prove that there exists an integer q such that $b - c = a \cdot q$.
(b) What do you need to do in order to prove that n^3 is odd? Notice that ifn is an odd integer, then there exists an integer k such that $n = 2k + 1$. Remember that to prove that n^3 is an odd integer, you need to prove that there exists an integer q such that $n^3 = 2q + 1$.
Or you can approach this as follows: If n is odd, then by Theorem 1.8, n^2 is odd. Now use the fact that $n^3 = n \cdot n^2$.
(c) If 4 divides $(a - 1)$, then there exists an integer k such that $a - 1 = 4k$. Write $a = 4k + 1$ and then use algebra to rewrite $(a^2 - 1)$.

3. (e) Make sure you first try some examples. How do you prove that an integer is an odd integer?
(f) The following algebra may be useful.

$$4(2m + 1)^2 + 7(2m + 1) + 6 = 6m^2 + 30m + 17.$$

4. (a) If $xy = 1$, then x and y are both divisors of 1, and the only divisors of 1 are -1 and 1.|
(b) Part (a) is useful in proving this.

3. Let $n \in \mathbb{N}$. For $a, b \in \mathbb{Z}$, you need to prove that if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$. Remember that for $x, y \in \mathbb{Z}$, $x \equiv y \pmod{n}$ if and only if $n \mid (x - y)$.

5. **Another hint**: $(4n + 3) - 2(2n + 1) = 1$.

8. (a) Assuming a and b are both congruent to 2 modulo 3, there exist integers m and n such that $a = 3m + 2$ and $b = 3n + 2$. Then show that

$$a + b = 3(m + n + 1) + 1$$

12. The assumptions mean that $n \mid (a - b)$ and that $n \mid (c - d)$. Use these divisibility relations to obtain an expression that is equal to a and to obtain an expression that is equal to c. Then use algebra to rewrite the resulting expressions for $a + c$ and $a \cdot c$.

Section 3.2

1. (a) Let n be an even integer. Since n is even, there exists an integer k such that $n = 2k$. Now use this to prove that n^3 must be even.
(b) Prove the contrapositive.
(c) Explain why Parts (a) and (b) prove this.
(d) Explain why Parts (a) and (b) prove this.

2. (a) The contrapositive is, For all integers a and b, if $ab \equiv 0 \pmod 6$, then $a \equiv 0 \pmod 6$ or $b \equiv 0 \pmod 6$.

4. (a) If $a \equiv 2 \pmod 5$, then there exists an integer k such that $a - 2 = 5k$. Then $a^2 = (2+5k)^2 = 4+20k+25k^2$. This means that $a^2 - 4 = 5(4k+5k^2)$.

6. One of the two conditional statements is true and one is false.

8. Prove both of the conditional statements: (1) If the area of the right triangle is $c^2/4$, then the right triangle is an isosceles triangle. (2) If the right triangle is an isosceles triange, then the area of the right triangle is $c^2/4$.

9. Prove the contrapositive.

10. Remember that there are two conditional statements associated with this biconditional statement. Be willing to consider the contrapositive of one of these conditional statements.

15. Define an appropriate function and use the Intermediate Value Theorem.

17. (b) Since 4 divides a, there exist an integer n such that $a = 4n$. Using this, we see that $b^3 = 16n^2$. This means that b3 is even and hence by Exercise (1), b is even. So there exists an integer m such that $b = 2m$. Use this to prove that m^3 must be even and hence by Exercise (1), m is even.

18. It may be necessary to factor a sum cubes. Recall that

$$u^3 + v^3 = (u+v)(u^2 - uv + v^2).$$

Section 3.3

1. (a) $P \vee C$

3. (a) Let r be a real number such that $r^2 = 18$. We will prove that r is irrational using a proof by contradiction. So we assume that r is a rational number.
(b) Do not attempt to mimic the proof that the square root of 2 is irrational (Theorem 3.20). You should still use the definition of a rational number but then use the fact that $\sqrt{18} = \sqrt{9 \cdot 2} = \sqrt{9}\sqrt{2} = 3\sqrt{2}$.

5. In each part, what is the contrapositive of the proposition? Why does it seem like the contrapositive will not be a good approach? For each statement, try a proof by contradiction.

6. Two of the propositions are true and the other two are false.

11. Recall that $\log_2 32$ is the real number a such that $2^a = 32$. That is, $a = \log_2 32$ means that $2^a = 32$. If we assume that a is rational, then there exist integers m and n, with $n \neq 0$, such that $a = \dfrac{m}{n}$.

12. **Hint:** The only factors of 7 are -1, 1, -7, and 7.

13. (a) What happens if you expand $(\sin\theta + \cos\theta)^2$? Don'tforgetyourtrigono- metric identities.

14. **Hint**: Three consecutive natural numbers can be represented by n, $n+1$, and $n+2$, where $n \in \mathbb{N}$, or three consecutive natural numbers can be represented by $m-1$, m and $m+1$, where $m \in \mathbb{N}$.

Section 3.4

1. Use the fact that $n^2 + n = n(n+1)$.

2. Do not use the quadratic formula. Try a proof by contradiction. **Hint**: If there exists a solution of the equation that is an integer, then we can conclude that there exists an integer n such that $n^2 + n - u = 0$.

3. First write $n = 2m+1$ for some integer m. The integer m can be even or odd.

5. (c) For all integers a, b, and d with $d \neq 0$, if d divides the product ab, then d divides a or d divdes b.

8. Try a proof by contradiction with two cases: a is even or a is odd.

10. (a) One way is to use three cases: (i) $x > 0$; (ii) $x = 0$; and $x < 0$. For the first case, $-x < 0$ and $|-x| = -(-x) = x = |x|$.

11. (a) For each real number x, $|x| \geq a$ if and only if $x \geq a$ or $x \leq -a$.

Section 3.5

2. (b) Factor $n^3 - n$.
(c) Consider using cases based on congruence modulo 6.

3. Let $n \in \mathbb{N}$. For $a, b \in \mathbb{Z}$, you need to prove that if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$. Remember that for $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{n}$, then $n \mid (a-b)$. So there exists an integer k such that $a - b = nk$.

4. (a) Use the definition of congruence.
(b) Let $a \in \mathbb{Z}$. Corollary 3.32 tell us that if $a \not\equiv 0 \pmod{3}$, then $a \equiv 1 \pmod{3}$ or $a \equiv 2 \pmod{3}$.
(c) For one of the conditional statements, Part (b) tells us we can use a proof by cases using the following two cases: (1) $a \equiv 1 \pmod{3}$; (2) $a \equiv 2 \pmod{3}$.

6. The result in Part (c) of Exercise (4) may be helpful in a proof by contradiction.

8. (a) Remember that $3 \mid k$ if and only if $k \equiv 0 \pmod{3}$.

9. (a) Use a proof similar to the proof of Theorem 3.20. The result of Exercise (8) may be helpful.

12. (a) Use the results in Theorem 3.28 to prove that the remainder must be 1.

Section 4.1

1. The sets in Parts (a) and (b) are inductive.

2. A finite nonempty set is not inductive (why?) but the empty set is inductive (why?).

3. (a) For each $n \in \mathbb{N}$, let $P(n)$ be, $2 + 5 + 8 + \cdots + (3n-1) = \dfrac{n(3n+1)}{2}$. Verify that $P(1)$ is true. The key to the inductive step is that if $P(k)$ is true, then

$$\begin{aligned} 2 + 5 + 8 + \cdots + (3k-1) + [3(k+1)-1] &= (2 + 5 + 8 + \cdots + (3k-1)) + (3k+2) \\ &= \frac{3k(k+1)}{2} + (3k+2). \end{aligned}$$

Now use algebra to show that the last expression can be rewritten as $\dfrac{(k+1)(3k+4)}{2}$ and then explain why this completes the proof that if $P(k)$ is true, then $P(k+1)$ is true.

6. The conjecture is that for each $n \in \mathbb{N}$, $\sum_{j=1}^{n}(2j-1) = n^2$. The key to the inductive step is that

$$\begin{aligned} \sum_{j=1}^{k+1}(2j-1) &= \sum_{j=1}^{k}(2j-1) + [2(k+1)-1] \\ &= \sum_{j=1}^{k}(2j-1) + [2k+1]. \end{aligned}$$

8. (a) The key to the inductive step is that if $4^k = 1 + 3m$, then $4^k \cdot 4 = 4(1+3m)$, which implies that

$$4^{k+1} - 1 = 3(1+4m).$$

13. Let k be a natural number. If $a^k \equiv b^k \pmod{n}$, then since we are also assuming that $a \equiv b \pmod{n}$, we can use Part (2) of Theorem 3 to conclude that $a \cdot a^k \equiv b \cdot b^k \pmod{n}$.

14. Three consecutive natural numbers maybe represent by n, $n+1$, and $n+2$, where n is a natural number. For the inductive step, think before you try to do a lot of algebra. You should be able to complete a proof of the inductive step by expanding the cube of only one expression.

Section 4.2

1. (a) If $P(k)$ is true, then $3^k > 1 + 2^k$. Multiplying both sides of this inequality by 3 gives

$$3^{k+1} > 3 + 3 \cdot 2^k$$

Now, since $3>1$ and $3\cdot 2^k > 2^{k+1}$, we see that $3+3\cdot 2^k > 1+2^{k+1}$ and hence, $3^{k+1} > 1+2^{k+1}$. Thus, if $P(k)$ is ture, then $P(k+1)$ is true.

2. If $n \geq 5$, then $n^2 < 2^n$. For the inductive step, we assume that $k^2 < 2^k$ and that $k \geq 5$. With these assumptions, prove that

$$(k+1)^2 = k^2+2k+1 < 2^k+2k+1.$$

Now use the assumption that $k>4$ to prove that $2k+1<k^2$ and combine this with the assumption that $k^2<2^k$.

5. Let $P(n)$ be the predicate, "$8^n \mid (4n)!$." Verify that $P(0)$, $P(1)$, $P(2)$, and $P(3)$ are true. For the inductive step, the following fact about factorials may be useful:

$$\begin{aligned}[4(k+1)]! &= (4k+4)! \\ &= (4k+4)(4k+3)(4k+2)(4k+1)(4k)!.\end{aligned}$$

8. Let $P(n)$ be, "The natural number n can be written as a sum of natural numbers, each of which is a 2 or a 3." Verify that $P(4)$, $P(5)$, $P(6)$, and $P(7)$ are true.

To use the Second Principle of Mathematical Induction, assume that $k \in \mathbb{N}$, $k \geq 5$ and that $P(4)$, $P(5)$, ... $P(k)$ are true. Then notice that

$k+1 = (k-1)+2$.

Since $k-1 \leq 4$, we have assume that $P(k-1)$ is true. Use this to complete the inductive step.

12. Let $P(n)$ be, "Any set with n elements has $\dfrac{n(n-1)}{2}$ 2-element subsets." $P(1)$ is true since any set with only one element has no 2-element subsets. Let $k \in \mathbb{N}$ and assume that $P(k)$ is true. This means that any set with k elements has $\dfrac{k(k-1)}{2}$ 2-element subsets. Let A be a set with $k+1$ elements, and let $x \in A$. Now use the inductive hypothesis on the set $A-\{x\}$, and determine how the 2-element subsets of A are related to the set $A-\{x\}$.

16. (a) Use Theorem 4.9
(b) Assume $k \neq q$ and consider two cases: (i) $k<q$; (ii) $k>q$.

Section 4.3

1. For the inductive step, if $a_k = k!$, then

$$\begin{aligned}a_{k+1} &= (k+1)a_k \\ &= (k+1)k! \\ &= (k+1)!.\end{aligned}$$

2. (a) Let $P(n)$ be, "f_{4n} is a multiple of 3." Since $f_4 = 3$, $P(1)$ is true. If $P(k)$ is true, then there exists an integer m such that $f_{4k} = 3m$. Use the following:

$$\begin{aligned}f_{4(k+1)} &= f_{4k+4} \\ &= f_{4k+3}+f_{4k+2} \\ &= (f_{4k+2}+f_{4k+1})+(f_{4k+1}+f_{4k}) \\ &= f_{4k+2}+2f_{4k+1}+f_{4k} \\ &= (f_{4k+1}+f_{4k})+2f_{4k+1}+f_{4k}.\end{aligned}$$

(c) Let $P(n)$ be, "$f_1+f_2+\cdots+f_{n-1} = f_{n+1}-1$." Since $f_1 = f_3-1$, $P(2)$ is true. For $k \geq 2$, if $k \geq 2$, if $P(k)$ is true, then $f_1+f_2+\cdots+f_{k-1} = f_{k+1}-1$. Then

$$\begin{aligned}f_1+f_2+\cdots+f_{k-1})+f_k &= (f_{k+1}-1)+f_k \\ &= (f_{k+1}+f_k)-1 \\ &= f_{k+2}-1.\end{aligned}$$

This proves that if $P(k)$ is true, then $P(k+1)$ is true.

(f) Let $P(n)$ be, "$f_1^2+f_2^2+\cdots+f_n^2 = f_nf_{n+1}$." For the inductive step, use

$$\begin{aligned}(f_1^2+f_2^2+\cdots+f_k^2)+f_{k+1}^2 &= f_kf_{k+1}+f_{k+1}^2\\ f_1^2+f_2^2+\cdots+f_k^2+f_{k+1}^2 &= f_{k+1}(f_k+f_{k+1})\\ &= f_{k+1}f_{k+2}.\end{aligned}$$

6. For the inductive step, if $a_k = a\cdot r^{k-1}$, then

$$\begin{aligned}a_{k+1} &= r\cdot a_k\\ &= r(a\cdot r^{k-1})\\ &= a\cdot r^k.\end{aligned}$$

8. For the inductive step, use the assumption that \(S_{k} = a(\dfrac{1 - r^{k}}{1 - r})\) and the recursive definition to write $S_{k+1} = a + r\cdot S_k$.

9. (a) $a_2 = 7$, $a_3 = 12$, $a_4 = 17$, $a_5 = 22$, $a_6 = 27$.
(b) One possibility is: For each $n\in\mathbb{N}$, $a_n = 2+5(n-1)$.

12. (a) $a_2 = \sqrt{6}$, $a_3 = \sqrt{\sqrt{6}+5}\approx 2.729$, $a_4\approx 2.780$, $a_5\approx 2.789$, $a_6\approx 2.791$
(b) Let $P(n)$ be, "$a_n < 3$." Since $a_1 = 1$, $P(1)$ is true. For $k\in\mathbb{N}$, if $P(k)$ is true, then $a_k < 3$. Now

$$a_{k+1} = \sqrt{5+a_k}.$$

Since $a_k < 3$, this implies that $a_{k+1} < \sqrt{8}$ and hence, $a_{k+1} < 3$. This proves that if $P(k)$ is true, then $P(k+1)$ is true.

13. (a) $a_3 = 7$, $a_4 = 15$, $a_5 = 31$, $a_6 = 63$
(b) Think in terms of powers of 2.

14. (a) $a_3 = \dfrac{3}{2}$, $a_4 = \dfrac{7}{4}$, $a_5 = \dfrac{37}{24}$, $a_6 = \dfrac{451}{336}$

16. (b) $a_2 = 5$ $a_2 = 719$ $a_8 = 362879$
$a_3 = 23$ $a_2 = 5039$ $a_9 = 3628799$
$a_4 = 119$ $a_2 = 40319$ $a_{10} = 39916799$

18. (a) Let $P(n)$ be, "$L_n = 2f_{n+1} - f_n$." First, verify that $P(1)$ and $P(2)$ are true. Now let k be a natural number with $k\geq 2$ and assume that $P(1)$, $P(2)$, ..., $P(k)$ are all true. Since $P(k)$ and $P(k-1)$ are both assumed to be true, we can use them to help prove that $P(k+1)$ must then be true as follows:

$$\begin{aligned}L_{k+1} &= L_k + L_{k-1}\\ &= (2f_{k+1} - f_k) + (2f_k - f_{k-1})\\ &= 2(f_{k+1}+f_k) - (f_k + f_{k-1}\\ &= 2f_{k+2} - f_{k+1}.\end{aligned}$$

(b) Let $P(n)$ be, "$5f_n = L_{n-1} + L_{n+1}$." First, verify that $P(2)$ and $P(3)$ are true. Now let k be a natural number with $k\geq 3$ and assume that $P(2)$, $P(3)$, ..., $P(k)$ are all true. Since $P(k)$ and $P(k-1)$ are both assumed to be true, we can use them to help prove that $P(k+1)$ must then be true as follows:

$$\begin{aligned}5f_{k+1} &= 5f_k + 5_{k-1}\\ &= (L_{k-1} + L_{k+1}) + (L_{k-2} + Lk)\\ &= (L_{k-1} + L_{k-2}) - (L_k + L_{k+1})\\ &= L_k + L_{k+2}.\end{aligned}$$

.

Section 5.1

1. (a) $A = B$ (c) $C\neq D$ (e) $A\nsubseteq D$
(b) $A\subseteq B$ (d) $C\subseteq D$

2. In both cases, the two sets have preceisely the same elements.

3.

A	$\subset,\subseteq,\neq$	$B\emptyset$	$\subset,\subseteq,\neq$	A
5	$\in$	$C\{5\}$	$\subset,\subseteq,\neq$	C
$\lvert A\rvert$	$=$	$\lvert D\rvert A$	$\in$	$\mathcal{P}(b)$

5. (a) The set $\{a, b\}$ is a not a subset of $\{a, c, d, e\}$ since $b \in \{a, b\}$ and $b \in \{a, c, d, e\}$.

7. (c) $(A \cup B)^c = \{2, 8, 10\}$ (h) $(A \cap C) \cup (B \cap C) = \{3, 6, 9\}$
(d) $A^c \cap B^c = \{2, 8, 10\}$ (n) $(A \cup B) - D = \{1, 3, 5, 7, 9\}$
(e) $(A \cup B) \cap C = \{3, 6, 9\}$

9. (b) There exists an $x \in U$ such that $x \in (P - Q)$ and $x \notin (R \cap S)$. This can be written as, There exists an $x \in U$ such that $x \in P$, $x \notin Q$, and $x \notin R$ or $x \notin S$.

10. (a) The given statement is a conditional statement. We can rewrite the subset relations in terms of conditional sentences: $A \subseteq B$ means, "For all $x \in U$, if $x \in A$, then $x \in B$," and $B^c \subseteq A^c$ means, "For all $x \in U$, if $x \in B^c$, then $x \in A^c$."

Section 5.2

1. (a) The set A is a subset of B. A proof is required. The idea is that if $x \in A$, then $-2 < x < 2$. Since $x < 2$, we conclude that $x \in B$.
(b) The set B is not a subset of A. Give an example of a real number that is in B but not in A.

3. (b) $A \subseteq B$ $B \nsubseteq A$

7. (a) Start by letting x be an element of $A \cap B$.
(b) Start by letting x be an element of A.
(e) By Theorem 5.1, $\emptyset \subseteq A \cap \emptyset$. By Part (a), $A \cap \emptyset \subseteq \emptyset$. Therefore, $A \cap \emptyset = \emptyset$.

12. (a) Let $x \in A \cap C$. Then $x \in A$ and $x \in C$. Since we are assuming that $A \subseteq B$, we see that $x \in B$ and $x \in C$. This proves that $A \cap C \subseteq B \cap C$.

15. (a) "If $A \subseteq B$, then $A \cap B^c = \emptyset$ " is Proposition 5.14. To prove the other conditional statement, start with, "Let $x \in A$." Then use the assumption that $A \cap B^c = \emptyset$ to prove that x must be in B.
(b) To prove "If $AsubseteqB$, then $A \cup B = B$," first note that if $x \in B$, then $x \in A \cup B$ and, hence, $B \subseteq A \cup B$. Now let $x \in A \cup B$ and note that since $A \subseteq B$, if $x \in A$, then $x \in B$. Use this to argue that under the assumption that $A \subseteq B$, $A \cup B \subseteq B$.

Tp prove "If $A \cup B = B$, then $A \subseteq B$," start with, Let $x \in A$ and use this asusmption to prove that x must be an element of B.

Section 5.3

1. (a) Let $x \in (A^c)^c$. Then $x \notin A^c$, which means $x \in A$. Hence, $(A^c)^c \subseteq A$. Now prove that $A \subseteq (A^c)^c$.
(c) Let $x \in U$. Then $x \notin \emptyset$ and so $x \in \emptyset^c$. Therefore, $U \subseteq \emptyset^c$. Also, since every set we deal with is a subset of the universal set, $\emptyset^c \subseteq U$.

2. We will first prove that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. So we will use two cases: (1) $x \in B$; (2) $x \in C$. In Case (1), $x \in A \cap B$ and, hence $x \in (A \cap B) \cup (A \cap C)$. In Case (2), $x \in A \cap C$ and, hence, $x \in (A \cap B) \cup (A \cap C)$. This proves that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Now prove that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

4. (a) $A - (B \cup C) = (A - B) \cap (A - C)$.
(c) Using the algebra of sets, we obtain

$$\begin{aligned}(A - B) \cap (A - C) &= (A \cap B^c) \cap (A \cap C^c) \\ &= (A \cap A) \cap (B^c \cap C^c) \\ &= A \cap (B \cup C)^c \\ &= A - (B \cup C).\end{aligned}$$

9. (a) Use a proof by contradiction. Assume the sets are not disjoint and let $x \in A \cap (B - A)$. Then $x \in A$ and $x \in B - A$, which implies that $x \notin A$.

Section 5.4

1, (a) $A \times B = \{(1, a), (1, b), (1, c), (1, d), (2, a), (2, b), (2, c), (2, d)\}$
(b) $B \times A = \{(a, 1), (b, 1), (c, 1), (d, 1), (a, 2), (b, 2), (c, 2), (d, 2)\}$
(c) $A \times (B \cap C) = \{(1, a), (1, b), (2, a), (2, b)\}$

3. Start of proof that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$:
Let $u \in A \times (B \cap C)$. Then there exists $x \in A$ and there exists $y \in B \cap C$ such that $u = (x, y)$. Since $y \in B \cap C$, we know that $y \in B$ and $y \in C$. So we have

$u = (x, y)$, where $x \in A$ and $y \in B$. This means that $u \in A \times B$.
$u = (x, y)$, where $x \in A$ and $y \in C$. This means that $u \in A \times C$.

4. Start of proof that $(A \cup B) \times C \subseteq (A \times C) \cup (B \times C)$:

let $u \in (A \cup B) \times C$. Then there exists $x \in A \cup B$ and there exists $y \in C$ such that $u = (x, y)$. Since $x \in A \cup B$, we know that $x \in A$ or $x \in B$.

Section 5.5

1. (a) {3, 4}
(d) {3, 4, 5, 6, 7, 8, 9, 10}

2. (a) {5, 6, 7, ...}
(c) $\emptyset$
(d) {1, 2, 3, 4}
(f) $\emptyset$

3. (a) $\{x \in \mathbb{R} \mid -100 \leq x \leq 100\}$
(b) $\{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$

4. (a) We let $\beta \in \Lambda$ and let $x \in A_\beta$. Then $x \in A_\alpha$, for at lest one $\alpha \in \Lambda$ and, hence, $x \in \bigcup_{\alpha \in \Lambda} A_\alpha$. This proves that $A_\beta \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha$.

5. (a) We first let $x \in B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha)$. Then $x \in B$ and $x \in \bigcup_{\alpha \in \Lambda} A_\alpha$. This means that there exists an $\alpha \in \Lambda$ such that $x \in A_\alpha$. Hence, $x \in B \cap A_\alpha$, which implies that $x \in \bigcup_{\alpha \in \Lambda} (B \cap A_\alpha)$. This prove that $B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha) \subseteq \bigcup_{\alpha \in \Lambda} (B \cap A_\alpha)$, and we still need to prove that $\bigcup_{\alpha \in \Lambda} (B \cap A_\alpha) \subseteq B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha)$.

8. (a) Let $x \in B$. For each $\alpha \in \Lambda$, $B \subseteq A_\alpha$ and, hence, $x \in A_\alpha$. This means that for each $\alpha \in \Lambda$, $x \in A_\alpha$ and, hence, $x \in \bigcap_{\alpha \in \Lambda} A_\alpha$. Therefore, $B \subseteq \bigcap_{\alpha \in \Lambda} A_\alpha$

12. (a) We first rewrite the set difference and then use a distributive law.

$$\begin{aligned} (\bigcup_{\alpha \in \Lambda} A_\alpha) - B &= (\bigcup_{\alpha \in \Lambda} A_\alpha) \cap B^c \\ &= \bigcup_{\alpha \in \Lambda} (A_\alpha \cap B^c) \\ &= \bigcup_{\alpha \in \Lambda} (A_\alpha - B) \end{aligned}$$

Section 6.1

1. (a) $f(-3) = 15$, $f(-1) = 3$, $f(1) = -1$, $f(3) = 3$.

(b) The set of preimages of 0 is $\{0, 2\}$. The set of preimages of 4 is $\{\frac{2-\sqrt{20}}{2}, \frac{2+\sqrt{20}}{2}\}$. (Use the quadratic formula.)

(d) range$(f) = \{y \in \mathbb{R} \mid y \geq -1\}$.

4. (b) The set of preimages of 5 is $\{2\}$. There set of preimages of 4 is $\emptyset$.
(c) The range of the function f is the set of all odd integers.
(d) The graph of the function f consists of an infinite set of discrete points.

5. (b) dom$(F) = \{x \in \mathbb{R} \mid x > \frac{1}{2}\}$, range$(F) = \mathbb{R}$
(d) dom$(g) = \{x \in \mathbb{R} \mid x \neq 2 \text{ and } x \neq -2\}$,
range$(g) = \{y \in \mathbb{R} \mid y > 0\} \cup \{y \in \mathbb{R} \mid y \leq -1\}$

6. (a) $d(1) = 1$, $d(2) = 2$, $d(3) = 2$, $d(4) = 3$, $d(8) = 4$, $d(9) = 3$
(c) The only natural numbers n such that $d(n) = 2$ are the prime numbers. The set of preimages of the natural number 2 is the set of prime numbers.
(e) $d(2^0) = 1$, $d(2^1) = 2$, $d(2^2) = 3$, $d(2^3) = 4$
(f) The divisors of 2^n are 2^0, 2^1, 2^2, ..., 2^{n-1}, 2^n.

7. (a) The domain of S is $\mathbb{N}$. The power set of $\mathbb{N}$, $[\mathcal{P}(\mathbb{N})]$ can be the codomain. The rule for determining outputs is that for each $n \in \mathbb{N}$, $S(n)$ is the set of all distinct natural number factors of n.
(b) For example, $S(8) = \{1, 2, 4, 8\}$, $S(15) = \{1, 3, 5, 15\}$.
(c) For example, $S(2) = \{1, 2\}$, $S(3) = \{1, 3\}$, $S(31) = \{1, 31\}$.

Section 6.2

1. (a) $f(0) = 4$, $f(1) = 0$, $f(2) = 3$, $f(3) = 3$, $f(4) = 0$
(b) $g(0) = 4$, $g(1) = 0$, $g(2) = 3$, $g(3) = 3$, $g(4) = 0$
(c) The two functions are equal.

2. (c) The two functions are not equal. For example, $f(1) = 5$ and $g(1) = 4$.

4. (a) $\langle a_n \rangle$, where $a_n = \cos(n\pi)$ for each $n \in \mathbb{N}$. The domain is $\mathbb{N}$, and {-1, 1} can be the codomain. This sequence is equal to the sequence in Part (c).

5. (a) $p_1(1, x) = 1$, $p_1(1, y) = 1$, $p_1(1, z) = 1$, $p_1(2, x) = 2$, $p_1(2, y) = 2$, $p_1(2, z) = 2$
(c) range$(p_1) = A$, range$(p_2) = B$

6. Start of the inductive step: Let $P(n)$ be "A convex polygon with n sides has $\dfrac{n(n-3)}{2}$ diagonals." Let $k \in D$ and assume that $P(k)$ is true, that is, a convex polygon with k sides has $\dfrac{k(k-3)}{2}$ diagonals. Now let Q be convex polygon with $(k+1)$ sides. Let v be one of the $(k+1)$ vertices of Q and let u and w be the two vertices adjacent to v. By drawing the line segment from u to w and omitting the vertex v, we form a convex polygon with k sides. Now complete the inductive step.

7. (a) $f(-3, 4) = 9$, $f(-2, -7) = -23$
(b) $\{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid m = 4 - 3n\}$

9. (a) det $\begin{bmatrix} 3 & 5 \\ 4 & 1 \end{bmatrix}$ = -17, det $\begin{bmatrix} 1 & 0 \\ 0 & 7 \end{bmatrix}$ = 7, and det $\begin{bmatrix} 3 & -2 \\ 5 & 0 \end{bmatrix}$ = 10.

Section 6.3

2. (a) The function f is not an injection and is not a surjection.
(c) The function F is an injection and is a surjection.

3. (a) The function f is an injection and is not a surjection.
(b) The function F is an injection and is a surjection.

4. (a) Let $F : \mathbb{R} \to \mathbb{R}$ be defined by $F(x) = 5x + 3$ for all $x \in \mathbb{R}$. Let $x_1, x_2 \in \mathbb{R}$ and assume that $F(x_1) = F(x_2)$. Then $5x_1 + 3 = 5x_2 + 3$. Show that this implies that $x_1 = x_2$ and, hence, F is an injection.
Now let $y \in \mathbb{R}$. Then $\dfrac{y-3}{5} \in \mathbb{R}$. Prove that $F(\dfrac{y-3}{5}) = y$. Thus, F is a sujection and hence F is a bijection.
(b) Notice that for each $x \in \mathbb{Z}$, $G(x) \equiv 3 \pmod 5$. Now explain why G is not a surjection.

7. The birthday function is not an injection since there are two different people with the same birthday. The birthday function is a surjection since for each day of the year, there is a person that was born on that day.

9. (a) The function f is an injection and a surjection.
(b) The function g is an injection and is not a surjection.

Section 6.4

3. (a) $F(x) = (g \circ f)(x)$, $f(x) = e^x$, $g(x) = \cos x$
(b) $G(x) = (g \circ f)(x)$, $f(x) = \cos x$, $g(x) = e^x$

4. (a) For each $x \in A$. $(f \circ I_A)(x) = f(I_A(x)) = f(x)$. Therefore, $f \circ I_A = f$.

5. (a) $[(h \circ g) \circ f](x) = \sqrt[3]{\sin(x^2)}$; $[h \circ (g \circ f)](x) \sqrt[3]{\sin(x^2)}$

6. Start of a proof: Let A, B, and C be nonempty sets and let $f : A \to B$ and $g : B \to C$. Assume that f and g are both injections. Let $x, y \in A$ and assume that $(g \circ f)(x) = (g \circ f)(y)$.

7. (a) $f:\mathbb{R}\to\mathbb{R}$ by $f(x)=x$, $g:\mathbb{R}\to\mathbb{R}$ by $g(x)=x^2$. The function f is a surjection, but $g\circ f$ is not a surjection.
(f) By Part (1) of Theorem 6.21, this is not possible since if $g\circ f$ is an injection, then f is an injection.

Section 6.5

2. (b) $f^{-1}=\{(c,a),(b,b),(d,c),(a,d)\}$
(d) $(f^{-1}\circ f)(x)=x=(f\circ f^{-1})(x)$. This illustrates Corollary 6.28.

4. Using the notation from Corollary 6.28, if $y=f(x)$ and $x=f^{-1}(y)$, then

$$\begin{aligned}(f\circ f^{-1}(y) &= f(f^{-1}(y))\\ &= f(x)\\ &= y\end{aligned}$$

6. (a) Let $x,y\in A$ and assume that $f(x)=f(y)$. Apply g to both sides of this equation to prove that $(g\circ f)(x)=(g\circ f)(y)$. Since $g\circ f=I_A$, this impliies that $x=y$ and hence that f is an injection.
(b) Start by assuming that $f\circ g=I_B$, and then let $y\in B$. You need to prove there exists an $x\in A$ such that $f(x)=y$.
(d) $g:\mathbb{R}^+\to\mathbb{R}$ by $g(y)=\dfrac{1}{2}(\text{In}y+1)$

7. The inverse of f is not a function and the inverse of g is a function.

Section 6.6

1. (a) There exists an $x\in A\cap B$ such that $f(x)=y$.
(d) There exists an $a\in A$ such that $f(a)=y$ or there exists a $b\in B$ such that $f(b)=y$.
(f) $f(x)\in C\cup D$
(h) $f(x)\in C$ or $f(x)\in D$.

2. (b) $f^{-1}(f(A))=[2,5]$.
(e) $f(A\cap B)=[-5,-3]$
(d) $f(f^{-1}(C))=[-2,3]$
(f) $f(A)\cap f(B)=[-5,-3]$

3. (a) $g(A\times A)=\{6,12,18,24,36,54,72,108,216\}$
(b) $g^{-1}(C)=\{(1,1),(2,1),(1,2)\}$

4. (a) range$(F)=F(S)=\{1,4,9,16\}$

5. To prove $f(A\cup B)\subseteq f(A)\cup f(B)$, start by letting $y\in f(A\cup B)$. This means that there exists an x in $A\cup B$ such that $f(x)=y$. How do you prove that $y\in f(A)\cup f(B)$?

6. To prove that $f^{-1}(C\cap D)\subseteq f^{-1}(C)\cap f^{-1}(D)$, let $x\in f^{-1}(C\cap D)$. Then $f(x)\in C\cap D$. How do you prove that $x\in f^{-1}(C)\cap f^{-1}(D)$?

9. Statement (a) is true and Statement (b) is false.

Section 7.1

1. (a) The set $A\times B$ contains nine ordered pairs. The set $A\times B$ is a relation from A to B since $A\times B$ is a subset of $A\times B$.
(b) The set R is a relation from A to B since $R\subseteq A\times B$.
(c) dom$(R)=A$, range$(R)=\{p,q\}$
(d) $R^{-1}=\{(p,a),(q,b),(p,c),(q,a)\}$

2. Only the statement in Part (b) is true.

3. (a) The domain of D consists of the female citizens of the United States whose mother is a female citizen of the United States.
(b) The range of D consists of those female citizens of the United States who have a daughter that is a female citizen of the United States.

4. (a) $(S,T)\in R$ means that $S\subseteq T$.
(b) The domain of the subset relation is $\mathcal{P}(U)$.
(c) The range of the subsetr elation is $\mathcal{P}(U)$.

(d) $R^{-1} = \{(T, S) \in \mathcal{P}(U) \times \mathcal{P}(U) \mid S \subseteq T\}$.
(e) The relation R is not a function from $\mathcal{P}(U)$ to $\mathcal{P}(U)$ since any proper subset of U is a subset of more than one subset of U.

6. (a) $\{x \in \mathbb{R} \mid (x, 6) \in S\} = \{-8, 8\}$
$\{x \in \mathbb{R} \mid (x, 9) \in S\} = \{-\sqrt{19}, \sqrt{19}\}$
(b) The domain and range of S is the closed interval [-10, 10].
(d) The relation S is not a function from $\mathbb{R}$ to $\mathbb{R}$.

9. (a) $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid |a - b| \leq 2\}$
(b) dom$(R) = \mathbb{Z}$ and range$(R) = \mathbb{Z}$

Section 7.2

1. The relation R is not reflexive on A and is not symmetric. However, it is transitive since the conditional statement "For all $x, y, z \in A$, if $x \; R \; y$ and $y \; R \; z$, then $x \; R \; z$" is a true conditional statement.

4. The relation R is not reflexive on A, is symmetric, and is not transitive.

6. (a) The relation $\sim$ is an equivalence relation.
(b) $C = \{-5, 5\}$

10. The relation $\sim$ is an equivalence relation and the relation $\approx$ is not an equivalence relation.

15. (c) The set C is a circle of radius 5 with center at the origin.

Section 7.3

1. $[a] = [b] = \{a, b\}$; $[c] = \{c\}$; $[d] = [e] = \{d, e\}$

2. $[a] = [b] = [d] = \{a, b, d\}$; $[c] = \{c\}$; $[e] = [f] = \{e, f\}$

3. The equivalence classes are {0, 1, 2, ..., 9}, {10, 11, 12, ..., 99}, {100, 101, 102, ..., 999}, {1000}.

4. The congruence classes for the relation of congruence modulo 5 on the set of integers are

$[0] = \{5n \mid n \in \mathbb{Z}$ $[3] = \{5n + 3 \mid n \in \mathbb{Z}$
$[1] = \{5n + 1 \mid n \in \mathbb{Z}$
$[2] = \{5n + 2 \mid n \in \mathbb{Z}$ $[4] = \{5n + 4 \mid n \in \mathbb{Z}$

5. (a) The distinct equivalence classes are {0, 3, 6}, {1, 8}, {2, 7}, and {4, 5}.

6. (a) Let $x \in [\frac{5}{7}]$. Then $x - \frac{5}{7} \in \mathbb{Z}$, which means that there is an integer m such that $x - \frac{5}{7} = m$, or $x = \frac{5}{7} + m$. This proves that $x \in \{m + \frac{5}{7} \mid m \in \mathbb{Z}\}$ and, hence, that $[\frac{5}{7}] \subseteq \{m + \frac{5}{7} \mid m \in \mathbb{Z}\}$. We still need to prove that $\{m + \frac{5}{7} \mid m \in \mathbb{Z}\} \subseteq [\frac{5}{7}]$

9. (a) To prove the relation is symmetric, note that if $(a, b) \approx (c, d)$, then $ad = bc$. This implies that $cb = da$ and, hence, $(c, d) \approx (a, b)$
(c) $3a = 2b$

Section 7.4

1. (a)

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\odot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

(b)

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

2. (a) $[x] = [1]$ or $[x] = [3]$
(e) $[x] = [2]$ or $[x] = [3]$
(g) The equation has no solution.

3. The statement in (a) is false. The statement in (b) is true.

5. (a) The proof consists of the following computations:

$$[1]^1 = [1] \qquad [3]^1 = [9] = [4]$$
$$[2]^1 = [4] \qquad [4]^1 = [16] = [1].$$

17. (a) Prove the contrapostive by calculating $[a]^2 + [b]^2$ for all nonzero $[a]$ and $[b]$ in $\mathbb{Z}_3$.

Section 8.1

1. (a) gcd(21, 28) = 7
(b) gcd(-21, 28) = 7
(c) gcd(58, 63) = 1
(d) gcd(0, 12) = 12

2. (a) **Hint**: Prove that $k \mid [(a+1) - a]$.

4. (a) $|b|$ is the largest natural number that divides 0 and b.
(b) The integers b and $-b$ have the same divisors. Therefore, $\gcd(a, -b) = \gcd(a, b)$.

5. (a) gcd(36, 60) = 12 $12 = 36 \cdot 2 + 60 \cdot (-1)$
(a) gcd(901, 935) = 17 $17 = 901 \cdot 27 + 935 \cdot (-26)$
(a) gcd(901, -935) = 17 $17 = 901 \cdot 27 + (-935) \cdot (26)$

7. (a) $11 \cdot (-3) + 17 \cdot 2 = 1$
(b) $\dfrac{m}{11} + \dfrac{n}{17} = \dfrac{17m + 11n}{187}$

Section 8.2

1. The only natural number divisors of a prime number p are 1 and p.

2. Use cases: (1) p divides a; (2) p does not divide a. In this case, use the fact that gcd(a, p) = 1 to write the number 1 as a linear combination of a and p.

3. A hint for the inductive step: Write $p \mid (a_1 a_2 \cdots a_m) a_{m+1}$. Then look at two cases: (1) $p \mid a_{m+1}$; (2) p does not divide a_{m+1}.

4. (a) gcd(a, b) = 1. Why?
(b) gcd(a, b) = 1 or gcd(a, b) = 1=2. Why?

7. (a) gcd(16, 28) = 4. Also, $\frac{16}{4} = 4$, $\frac{28}{4} = 7$, and gcd(4, 7) = 1.

9. Part (b) of Exercise (8) can be helpful.

11. The statement is true. Start of a proof: If gcd(a, b) = 1 and $c \mid (a+b)$, then there exist integers x and y such that $ax+by=1$ and there exists an integer m such that $a+b=cm$.

Section 8.3

3. (a) $x=-3+14k, y=2-9k$
(b) $x=-1+11k, y=1+9k$
(c) No solution
(d) $x=2+3k, y=-2-4k$

4. There are several possible solutions to this problem, each of which can be generated from the solutions of the Diophantine equation $27x+50y=25$.

5. This problem can be solved by finding all solutions of a linear Diophantine equation in x and y, where both x and y are positive. The minimum number of people attending the banquet is 66.

6. (a) $y=12+16k$, $x_3=-1-3k$
(c) $x_1=y+3n$, $x_2=-y+4n$

Section 9.1

2. Use $f: A\times\{x\}\to A$ by $f(a,x)=a$, for all $(a,x)\in A\times\{x\}$.

4. Notice that $A=(A-\{x\})\cup\{x\}$. Use Theorem 9.6 to conclude that $A-\{x\}$ is finte. Then use Lemma 9.4.

5. (a) Since $A\cap B\subseteq A$, if A is finite, then Theorem 9.6 implies that $A\cap B$ is finte.

7. (a) Remember that two ordered pairs are equal if and only if their corresponding coordinates are equal. So if $h(a_1,c_1)=h(a_2,c_2)$, then $(f(a_1),g(c_1))=(f(a_2),g(c_2))$. We can then conclude that $f(a_1)=f(a_2)$ and $g(c_1)=g(c_2)$.

8. (a) If we define the function f by $f(1)=a$, $f(2)=b$, $f(3)=c$, $f(4)=a$, and $f(5)=b$, then we can use $g(a)=1$, $g(b)=1$, and $g(3)=c$. The function g is an injection.

Section 9.2

1. All except Part (d) are true.

2. (e) Either define an appropriate bijection or use Corollary 9.20 to conclude that $\mathbb{N}-\{4,5,6\}$ is countable. Prove that $\mathbb{N}-\{4,5,6\}$ cannot be finite.
(f) $\{m\in\mathbb{Z}\mid m\equiv 2 \pmod 3\}=\{3k+2\mid k\in\mathbb{Z}\}$

5. For each $n\in\mathbb{N}$, let $P(n)$ be "If card(B) = n, then $A\cup B$ is a countably infinte set."

Note that if card$(B)=k+1$ and $x\in B$, then card$(B-\{x\})=k$. Apply the inductive assumption to $B-\{x\}$.

6. Notice that if $h(n)=h(m)$, then since A and B are disjoint, either $h(n)$ and $h(m)$ are both in A or are both in B.

Also, if $y\in A\cup B$, then there are only two cases to consider: $y\in A$ or $y\in B$.

8. Since $A-B\subseteq A$, the set $A-B$ is countable. Now assume $A-B$ is finte and show that this leads to a contradiction.

Section 9.3

1. (a) $f:(0,\infty)\to\mathbb{R}$ by $f(x)=\text{In}x$ for all $x\in(0,\infty)$
(b) $g:(0,\infty)\to(a,\infty)$ by $g(x)=x+a$ for all $x\in(0,\infty)$. The function g is a bijection and so $(0,\infty)\approx(a,\infty)$. Then use Part (a).

2. Show that the assumption that the set of irrational numbers is countable leads to a contradiction.

3. Use Corollary 9.20.

Appendix D: List of Symbols

Symbol	Meaning
$\rightarrow$	Conditional statement
$\mathbb{R}$	set of real numbers
$\mathbb{Q}$	set of rational numbers
$\mathbb{Z}$	set of integers
$\mathbb{N}$	set of natural numbers
$y \in A$	y is an element of A
$z \notin A$	z is not an element of A
$\{ \mid \}$	set builder notation
$\forall$	universal quantifier
$\exists$	existential quantifier
$\emptyset$	the empty set
$\wedge$	conjunction
vee	disjunction
$\neg$	negation
$\leftrightarrow$	biconditional statement
$\equiv$	logically equivalent
$m \mid n$	m divides n
$a \equiv b \pmod{n}$	a is congruent to b modulo n
$\lvert x \rvert$	the absolute value of x
$A = B$	A equals B (set equality)
$A \subseteq B$	A is a subset of B
$A \nsubseteq B$	A is not a subset of B
$A \subset B$	A is a proper subset of B
$\mathcal{P}(A)$	power set of A
$\lvert A \rvert$	cardinality of a finite set A
$A \cap B$	intersection of A and B
A^c	complement of A
$A - B$	set difference of A and B
$A \times B$	Cartesian product of A and B
(a,b)	ordered pair
$\mathbb{R} \times \mathbb{R}$	Cartesian plane
$\mathbb{R}^2$	Cartesian plane
\(\bigcup_{X \in \mathcal{C}} X\)	union of a family of sets
\(\bigcap_{X \in \mathcal{C}} X\)	intersection of a finite family of sets
$\bigcup_{j=1}^{n} A_j$	union of a finite family of sets
$\bigcap_{j=1}^{n} A_j$	intersection of a finite family of sets

$\bigcup_{j=1}^{\infty} B_j$	union of an infinite family of sets
$\bigcap_{j=1}^{\infty} B_j$	intersection of a infinite family of sets
$\{A_\alpha \mid \alpha \in \Lambda\}$	indexed family of sets
$\bigcup_{\alpha\in\Lambda} A_\alpha$	union of an indexed family of sets
$\bigcap_{\alpha\in\Lambda} A_\alpha$	intersection of an indexed family of sets
$n!$	n factorial
$f_1, f_2, f_3, \ldots$	Fibonacci numbers
$s(n)$	sum of the divisors of n
$f : A \to B$	function from A to B
dom(f)	domain of the function f
codom(f)	codmain of the function f
$f(x)$	inage of x under f
range(f)	range of the function f
$d(n)$	number of divisors of n
I_A	identity function on the set A
p_1, p_2	projection functions
det(A)	determinant of A
A^T	transpose of A
det: $M_{2,2} \to \mathbb{R}$	determinant function
$g \circ f : A \to C$	composition of function f and g
f^{-1}	the inverse of the function f
Sin	the restricted sine function
Sin^{-1}	the inverse sine function
dom(R)	domain of the relation R
range(R)	range of the relation R
$x \ R \ y$	x is related to y
$x \not R \ y$	x is not related to y
$x \sim y$	x is related to y
$x \nsim y$	x is not related to y
R^{-1}	the inverse of the relation R
$[a]$	equivalence class of a
$[a]$	congruence class of a
$\mathbb{Z}_n$	the integers modulo n
$[a] \oplus [c]$	addition in $\mathbb{Z}_n$
$[a] \odot [c]$	multiplication in $\mathbb{Z}_n$
gcd(a, b)	greatest common divisor of a and b
$f(A)$	image of A under the function f
$f^{-1}(C)$	pre-image of C under the funtion f

$A \approx B$	A is equivalent to B A and B have the same cardinality
$\mathbb{N}_k$	$\mathbb{N}_k = \{1, 2, \ldots, k\}$
card$(A) = k$	cardinality of A is k
$aleph_0$	cardinality of $\mathbb{N}$
c	cardinal number of the continuum

Index

Detailed Licensing

Overview

Title: Discrete Structures

Webpages: 128

Applicable Restrictions: Noncommercial

All licenses found:

- CC BY-NC-SA 3.0: 61.7% (79 pages)
- CC BY-NC-SA 4.0: 19.5% (25 pages)
- Undeclared: 12.5% (16 pages)
- CC BY-SA 4.0: 6.3% (8 pages)

By Page