Logic and Proof for Teachers

Logic and Proof for Teachers

Lesa L. Beverly
Stephen F. Austin State University

Kimberly M. Childs
Stephen F. Austin State University

Thomas W. Judson
Stephen F. Austin State University

Deborah A. Pace
Stephen F. Austin State University

October 24, 2019

Edition: Annual Edition 2019

Website: http://faculty.sfasu.edu/judsontw/lpt/index.html

Preface

Logic and proof are two of the most important areas of study for students intending to teach middle or secondary mathematics. *The Mathematical Education of Teachers II* published for the Conference Board of the Mathematical Sciences (2012) by the American Mathematical Society and Mathematical Association of America emphasizes the need for teachers to understand mathematical reasoning and thinking. *Logic and Proof for Teachers* is intended for a one-semester course on logic and proof for students intending to teach middle or high school mathematics. The book grew out of a set of notes written by Kimberly M. Childs and Deborah A. Pace for the *Foundation of Mathematics* course (MTH 300) at Stephen F. Austin State University. During Summer 2019, I converted the notes to PreTeXt and added a chapter on the integers. The open source version of this book has received support from the National Science Foundation (Awards #DUE–1625223 and #DUE–1821329).

Thomas W. Judson
Nacogdoches, Texas 2019

Contributors to the 2019 Edition

Brian Beavers
Department of Mathematics and Statistics
Stephen F. Austin State University
beaversbd@sfasu.edu

Jane H. Long
Department of Mathematics and Statistics
Stephen F. Austin State University
longjh@sfasu.edu

Clint Richardson
Department of Mathematics and Statistics
Stephen F. Austin State University
crichardson@sfasu.edu

Contents

Chapter 1

Logic

TEXAS STATE BOARD FOR EDUCATOR CERTIFICATION (SBEC): MATHEMATICS STANDARDS COVERED.

- STANDARD III: GEOMETRY AND MEASUREMENT: The mathematics teacher understands and uses geometry, spatial reasoning, measurement concepts and principles, and technology appropriate to teach the statewide curriculum (Texas Essential Knowledge and Skills [TEKS]) in order to prepare students to use mathematics.
- STANDARD V: MATHEMATICAL PROCESSES: The mathematics teacher understands and uses mathematical processes to reason mathematically, to solve mathematical problems, to make mathematical connections within and outside of mathematics, and to communicate mathematically.
- STANDARD VI: MATHEMATICAL PERSPECTIVES: The mathematics teacher understands the historical development of mathematical ideas, the interrelationship between society and mathematics, the structure of mathematics, and the evolving nature of mathematics and mathematical knowledge.

As noted in the preface, one useful definition of mathematics is the body of knowledge obtained by applying logic (deductive and inductive) to a system of axioms. Our first thought is to deal with things which conform to a bivalent system of logic; that is, things which are either true or false.

1.1 Definitions

Definition 1.1.1 A ***statement*** is a sentence which is either true or false. We will notationally speak of a statement p or a statement q. $\Diamond$

Example 1.1.2 Each of the following sentences are statements.

1. George Washington was the first President of the United States.
2. $2 + 3 = 5$.

3. There are 12 inches in a foot.

4. Harry S. Truman was the second President of the United States.

5. $4 \cdot 8 = 12$.

6. There are 30 inches in a yard.

□

Certainly we recognize some underlying knowledge is required in interpreting the sentences in Example 1.1.2. For instance, in the sentence "$2 + 3 = 5$," we assume recognition of the concepts of 2, 3, 5, and addition base 10. Nevertheless, we must make some general knowledge assumptions, and certainly the six sentences of Example 1.1.2 are statements. (The first three sentences are true while the last three are false.)

Example 1.1.3 Each of the following sentences are not statements.

1. $2 + 3$

2. Study mathematics.

3. Three is a nice number.

4. Chris Hemsworth, who plays Thor in the *Avengers* series, is a handsome man.

Clearly, the problem in each of these sentences is that their truth or falsity cannot be uniquely determined. Actually, Item 3 and Item 4 could be statements provided that we have good definitions of "nice numbers" and "handsome". □

Example 1.1.4 Consider the following sentence. "This sentence is false." This is not a statement. Why? The sentence in question is an example of what is known in mathematics as a paradox. If it is true, then it is false, while on the other hand, if it is false, then it is true. Such paradoxes are not statements.

□

What, then, is an axiom? Surely it must be a statement, but also something more. As we study a body of mathematical knowledge, we encounter new statements, some of which can be proven from the existing system. These statements are called lemmas, theorems, facts, etc. Other statements cannot be proven. If we can in fact prove that the truth value of the statement is independent of the existing system, we have a potential axiom. We can either assume the statement is true, adding it to our system as an axiom, or we could assume the statement is false, adding its negative (or some form of its negative) to our system as an axiom. Surely, quite different bodies of knowledge would evolve depending on what axiom we added. The best examples of this concept are Euclidean geometry and the various non-Euclidean geometries.

Logicians as well as some other mathematicians are deeply concerned with such questions of creating minimal systems of axioms and developing mathematics very systematically from them. Such important but esoteric questions are beyond the scope and intent of this course. However, the remainder of this chapter will attempt to create a firm, logical base which will be used throughout this text and many subsequent courses the student will encounter.

For our purposes the student needs a basic feel for the flow of mathematics and a concrete understanding of the concept of bivalent logic applied to statements.

1.1.1 Exercises

Determine whether or not the following sentences represent statements. If so, state the truth value.

1. $7 \cdot 9 = 63$.

2. There are more males than females registered in this class.

3. *Gone with the Wind* is a good book.

4. Eggs are a good source of calcium.

5. $64 \div 2 = 37$.

6. $ax^2 + bx + c$.

7. $ax^2 + bx + c = 0$.

8. The metric system of measurement is difficult to learn.

9. Summer is the best season of the year.

10. There are 30 people registered for this class.

11. $\sqrt{64} = 9$.

12. Today is a beautiful day.

1.2 Compound Statements

In Section 1.1 we defined a statement to be a sentence which is either true or false. Many statements we are interested in studying are actually combinations of several simpler ones. Then the problem of determining the truth value (truth or falsity) of such statements becomes one of discovering the truth value of the statements being combined as well as understanding the methods of combination. We will at this time consider the negation, conjunction, and disjunction of statements.

Definition 1.2.1 Let p be a statement. The ***negation*** of p, denoted $\sim p$, is a statement forming the denial of p. The statement $\sim p$, read "not p," has the opposite truth value of p. ◊

Example 1.2.2

1. Consider the statement, "Austin is the capital of Texas." The negation of that statement would be the statement, "Austin is not the capital of Texas."

2. The statement "$2 + 3 = 5$" has as its negation the statement "$2 + 3 \neq 5$."

□

Since one of our stated concerns in this section is the determination of the truth value of a given statement based upon the truth values of its component statements, we consider the concept of a truth table. Very simply, a truth table is exactly a table which indicates the relationships between the truth values of the statements forming the table. Thus, the truth table below (Table 1.2.3) indicates the relationship between the statements p and $\sim p$, giving us the basic table for a negation.

Table 1.2.3 Truth table for negation

p	$\sim p$
T	F
F	T

Notice that the table shows that if p is true, then $\sim p$ is false and if p is false, then $\sim p$ is true. Truth tables become very useful when we deal with more complicated statements.

The first type of compound statement we consider is the conjunction. When combining statements in logic, the most important aspect of the definition is the truth value of the resulting statement in terms of the component statements.

Definition 1.2.4 Let p and q be statements. The ***conjunction*** of p and q, denoted $p \wedge q$, is the compound statement obtained by connecting and with the English connective "and." The conjunction is true only when both p and q are true. ◊

Example 1.2.5 The compound statement "Austin is the capital of Texas, and five is greater than two" is obtained by using "and" to connect the two statements "Austin is the capital of Texas" and "five is greater than two." □

The key to understanding the conjunction is the truth table below (Table 1.2.6), which systematically exhibits the four possible combinations of the truth values for p and q. Thus, we see that the conjunction of two statements is true only in the case when both statements are true.

Table 1.2.6 Truth table for conjunction

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Definition 1.2.7 Let p and q be statements. The ***disjunction*** of p and q, denoted $p \vee q$, is the compound statement obtained by connecting and with the English connective "or." The conjunction is true when at least one of the statements is true. ◊

A brief comment about "or" must be noted. As used in a mathematical/logical sense, "or" is interpreted in the inclusive sense. That is, or is interpreted as and/or, meaning one and/or the other is true. Consider carefully the truth table for the disjunction (Table 1.2.8). So we see the disjunction is false only when both p and q are false. (The exclusive use of "or" would yield truth only if exactly one of the two statements were true.)

Table 1.2.8 Truth table for disjunction

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Example 1.2.9 Consider the four disjunctions.

1. Austin is the capital of Texas or five is greater than two.
2. Austin is the capital of Texas or five is less than two.
3. Austin is not the capital of Texas or two is less than five.
4. Austin is not the capital of Texas or five is less than two.

Here we see the first three compound sentences are disjunctions which are true, while the disjunction in (4) is false. □

Another way of logically combining statements is the conditional statement, which is the heart of mathematical logic.

Definition 1.2.10 Let p and q be statements. The ***conditional statement*** is the compound statement obtained by considering this statement: "if p, then q" or "p implies q," and is denoted $p \to q$. The conditional is true unless p is true and q is false. ♢

In mathematics/logic the truth table for a conditional statement is given in Table 1.2.11.

Table 1.2.11 Truth table for a conditional statement

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 1.2.12 Consider the four conditional statements.

1. If Austin is the capital of Texas, then five is greater than two.
2. If Austin is the capital of Texas, then five is less than two.
3. If Austin is not the capital of Texas, then two is less than five.
4. If Austin is not the capital of Texas, then five is less than two.

Here we see the first three compound sentences are disjunctions which are true, while the disjunction in (4) is false. Here we see by the truth table defining the truth value of a conditional statement that (1), (3),and (4) are true conditional statements while (2) is a false conditional statement. Notice that we can determine the truth value of these statements even though the component statements appear to be totally unrelated in terms of cause and effect! □

We emphasize that the student must understand that conditional statements have truth values precisely as assigned by the definition. That is, to determine truth value, we do not need to be able to "prove" or "disprove" the consequence from the hypothesis. Certainly "proving" things will be the ultimate focus of this course, but at this time we are simply discovering the ways of combining statements logically and the resulting truth values of such combinations.

The last compound statement we will introduce is the biconditional statement.

Definition 1.2.13 Consider two statements p and q. The ***biconditional statement*** is the compound statement "p if and only if q" or "p is equivalent to q," denoted $p \leftrightarrow q$. Frequently we write "p iff q" as a shorthand notation for "p if and only if q." ♢

Two statements, no matter how complicated, are equivalent when they have precisely the same truth value. You can find the truth table for the biconditional statement in Table 1.2.14.

Table 1.2.14 Truth table for a biconditional statement

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Example 1.2.15 Consider the four biconditional statements.

1. If Austin is the capital of Texas if and only if five is greater than two.
2. If Austin is the capital of Texas if and only if five is less than two.
3. If Austin is not the capital of Texas if and only if two is less than five.
4. If Austin is not the capital of Texas if and only if five is less than two.

Here we see that (1) and (4) are true biconditional statements while (2) and (3) are false. □

Mathematicians often use other expressions to describe conditional type statements. A few of the most common such expressions are given below.

- $p \leftrightarrow q$: "p is a necessary and sufficient condition for q."
- $p \to q$: "p is a sufficient condition for q."
- $q \to p$: "p is a necessary condition for q."

Since it is easy to confuse these expressions, you must always carefully identify the hypothesis and conclusion before working with any conditional type statement.

Again we stress that we are not attempting to "prove" anything yet, but rather only define a compound statement and its truth value in terms of the truth values of the statements used to obtain it.

In order to determine the truth values of more complicated statements, it is critical that you thoroughly understand and remember these five basic truth tables. That is, sufficient time must be spent digesting these tables and examples in order that you need not constantly refer back to the basic tables when working on more difficult ones.

Before going on to the last definition and fact of this section, we give an example of a more involved statement along with a step-by-step approach to constructing the associated table. We note that there are several methods available for constructing truth tables. We will exhibit one in the example below and employ an alternate approach in the proof of Fact 1.2.20 at the end of this section. You should adopt the one most comfortable and appropriate for dealing with the statement at hand.

Example 1.2.16 Let us construct the truth table (Table 1.2.17) for the statement

$$(q \wedge p) \vee [q \wedge (\sim p)].$$

After listing the component statements and all possible combinations of truth values associated with them in the table, the remaining compound statements should be given in the order in which they will be considered. This is done much like ordering of operations in an arithmetic problem or an algebraic expression.

Table 1.2.17 Truth table for $(q \wedge p) \vee [q \wedge (\sim p)]$

p	q	$\sim p$	$q \wedge p$	$q \wedge (\sim p)$	$(q \wedge p) \vee [q \wedge (\sim p)]$
T	T	F	T	F	T
T	F	F	F	F	F
F	T	T	F	T	T
F	F	T	F	F	F

□

We now give a final definition that relates conditional statements and negation.

Definition 1.2.18 Consider two statements p and q. The statement $q \to p$ is the ***converse*** of $p \to q$. The statement $\sim q \to \sim p$ is the ***contrapositive*** of $p \to q$. The statement $\sim p \to \sim q$ is the ***inverse*** of $p \to q$. ◊

It is worth noting that the converse of the inverse is the contrapositive. You should also note that the terms "inverse" and "negation" are not interchangeable.

Remark 1.2.19 About Notation. You should be aware that there are conventions governing the use or lack of use of parentheses in logical statements that are similar to those used to interpret algebraic expressions. Although we sometimes use grouping symbols for emphasis, such grouping symbols are often unnecessary for clarity of meaning. For example, the expression $[(\sim p) \wedge q] \to [(\sim r) \vee (\sim s)]$ could have been written $\sim p \wedge q \to \sim r \vee \sim s$. It is important for you to realize that the negation symbol preceding the p statement applies only to p unless indicated otherwise. However, the grouping symbols in the expressions $[\sim (p \wedge q)] \to [(\sim r) \to (\sim s)]$ and $\sim \{(p \wedge q) \to [(\sim r) \to (\sim s)]\}$ produce statements with entirely different meanings.

Fact 1.2.20 *Consider two statements p and q.*

1. $(p \to q) \leftrightarrow [(\sim q) \to (\sim p)]$*; that is, the conditional is equivalent to its contrapositive.*

2. $[(\sim p) \to (\sim q)] \leftrightarrow (q \to p)$*; that is, the inverse is equivalent to the converse.*

Proof. To demonstrate the proof of (1) in Fact 1.2.20, we need only examine the corresponding truth table Table 1.2.21. Since the last two columns are the same, the conditional statement and its contrapostive are equivalent.

Table 1.2.21 Truth table for $(p \to q) \leftrightarrow (\sim q \to \sim p)$

p	q	$\sim p$	$\sim q$	$p \to q$	$\sim q \to \sim p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

We will leave the proof of (2) as an exercise. ■

1.2.1 Exercises

1. Translate the following English statements using propositional notation.

(a) An integer is odd if and only if its square is odd.

(b) If I do not study, then I will fail this class.

(c) Either I will go shopping or I will go to a movie.

(d) I was well qualified, but I did not get the job.

(e) If n is an integer, then n is even or n is odd.

(f) The square of an even integer is an even integer.

2. Negate each of the following statements. (Refer to the definition of negation.)

(a) A positive number is larger than zero.

(b) If today is Saturday, then I do not have to go to work.

(c) Dogs can bark and cats can climb trees.

(d) If $x^2 - 9 = 0$,then either $x = 3$ or $x = -3$.

Note: The difficulties of negating compound statements will be vastly simplified by the tautologies studied in the next section.

3. For the conditional statements given below, give the converse, the inverse, and the contrapositive.

(a) If I teach third grade, then I am an elementary school teacher.

(b) If I do not get to class on time, then I will not be allowed to take the exam.

(c) I will return the calls and dictate the letter when I arrive at the office.

(d) If $(x + 1)(x - 4) = 0$, then $x = -1$ or $x = 4$.

(e) If a number has a factor of 4, then it has a factor of 2.

4. Restate the following in a logically equivalent form.

(a) It is not true that both today is Wednesday and the month is June.

(b) It is not true that yesterday I both ate breakfast and watched television.

(c) It is not raining, or it is not July.

5. In the following statements, remove those grouping symbols which are unnecessary for clarity of meaning.

(a) $p \vee [(\sim p) \wedge q]$

(b) $[\sim(p \to q)] \wedge q$

(c) $[p \wedge (\sim q)] \vee (p \wedge q)$

(d) $\{\sim[p \vee (\sim r)] \vee (q \wedge p)\} \to p$

6. Construct truth tables for the following compound statements.

(a) $p \vee (\sim p \wedge q)$

(b) $\sim(p \to q) \wedge q$

(c) $(p \wedge \sim q) \vee (p \wedge q)$

(d) $[\sim(p \vee \sim r) \wedge (p \vee q)] \to p$

7. For integers x and y, find the inverse, the converse, the contrapositive, and the negation of each of the following statements.

(a) If $x = 3$, then $x^4 = 81$.

(b) If $x > 0$, then $x \neq -4$.

(c) If x is odd and y is even, then xy is even.

(d) If $x^2 = x$, then either $x = 0$ or $x = 1$.

(e) If $xy \neq 0$, then $x \neq 0$ and $y \neq 0$.

8. Give two examples from mathematics which satisfy the given conditions.

(a) A statement and its converse that are both true.

(b) A statement that is true, but its converse is false.

(c) A biconditional statement that is true.

(d) A biconditional statement that is false.

9. Decide if the conditional statements are true or false.

(a) If n is a natural number, then the last digit of n^4 is 0, 1, 5, or 6.

(b) If the last digit of a natural number is 0, 1, 5, or 6, then it is a fourth power of some natural number.

(c) n is a natural number only if $n + 1$ is a whole number.

(d) $n + 1$ is a whole number if n is a natural number.

10. Let m and n be integers and consider the statement $p \to q$ given by, "If $m + n$ is even, then m and n are even."

(a) Express the contrapositive, converse, and inverse of the given conditional.

(b) For the given conditional or any statements in part (a) that are false, give a counterexample.

1.3 Tautologies, Contradictions, & Quantifiers

By definition, a simple statement is either true or false. In mathematics/logic, statements which are always true or always false are of great value, but the greatest benefit occurs when dealing with compound statements fitting this description. We give the formal definitions below.

Definition 1.3.1 A compound statement which is always true is called a ***tautology***, while a compound statement which is always false is called a ***contradiction***. ◊

Example 1.3.2 The statement $p \leftrightarrow \sim p$ is a contradiction since its truth table indicates this statement is always false (Table 1.3.3). That is, a statement and its negation can never have the same truth value.

Table 1.3.3 Truth table for $p \leftrightarrow \sim p$

p	$\sim p$	$p \leftrightarrow \sim p$
T	F	F
F	T	F

□

Example 1.3.4 The statement $p \leftrightarrow \sim(\sim p)$ is a tautology since its truth table indicates this statement is always true (Table 1.3.5). Thus, the double negation of a statement is equivalent to the original statement.

Table 1.3.5 Truth table for $p \leftrightarrow \sim(\sim p)$

p	$\sim p$	$\sim(\sim p)$	$p \leftrightarrow \sim(\sim p)$
T	F	T	T
F	T	F	T

□

The following theorem enumerates a list of tautologies which will be useful to us. The proofs will be left as exercises.

Theorem 1.3.6 *The following are tautologies. Statements (1)–(13) are basic properties, while (14)–(22) can be considered additional laws.*

1. $p \leftrightarrow p$
2. $p \leftrightarrow \sim(\sim p)$
3. $[\sim(p \vee q)] \leftrightarrow [(\sim p) \wedge (\sim q)]$
4. $[\sim(p \wedge q)] \leftrightarrow [(\sim p) \vee (\sim q)]$
5. $[\sim(p \rightarrow q)] \leftrightarrow [p \wedge (\sim q)]$
6. $[\sim(p \leftrightarrow q)] \leftrightarrow \{[p \wedge \sim q)] \vee [q \wedge \sim p)]\}$
7. $(p \vee q) \leftrightarrow (\sim p \rightarrow q)$
8. $(p \rightarrow q) \leftrightarrow (\sim q \rightarrow \sim p)$
9. $(\sim p \rightarrow \sim q) \leftrightarrow (q \rightarrow p)$
10. $[(p \rightarrow q) \wedge (q \rightarrow p)] \leftrightarrow (p \leftrightarrow q)$
11. $\{(\sim p) \rightarrow [q \wedge (\sim q)]\} \rightarrow p$
12. $(p \leftrightarrow q) \rightarrow [(r \wedge p) \rightarrow (r \wedge q)]$
13. $(p \leftrightarrow q) \rightarrow [(r \vee p) \leftrightarrow (r \vee q)]$
14. $(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$
15. $(p \wedge q) \leftrightarrow (q \wedge p)$
16. $(p \vee q) \leftrightarrow (q \vee p)$
17. $[(p \rightarrow p) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
18. $[(p \leftrightarrow p) \wedge (q \leftrightarrow r)] \rightarrow (p \rightarrow r)$
19. $[p \vee (q \wedge r)] \leftrightarrow [(p \vee q) \wedge (p \vee r)]$
20. $[p \wedge (q \vee r)] \leftrightarrow [(p \wedge q) \vee (p \wedge r)]$
21. $[p \vee (q \vee r)] \leftrightarrow [(p \vee q) \vee r]$
22. $[p \wedge (q \wedge r)] \leftrightarrow [(p \wedge q) \wedge r]$

1.3.1 Historical Note

Augustus De Morgan (27 June 1806–18 March 1871) was a British mathematician and logician. Use internet and/or library resources to research his major contributions to the fields of mathematics and logic, specifically De Morgan's Laws. The following theorem lists some useful contradictions, and again, the proof requires construction of the appropriate truth tables and is left to the exercises.

Theorem 1.3.7 *The following statements are contradictions.*

1. $(p \to q) \wedge (p \wedge \sim q)$
2. $[(p \vee q) \wedge \sim p] \wedge \sim q$
3. $(p \wedge q) \wedge \sim p$

You should be aware that the list of possible tautologies and contradictions we could have chosen is virtually endless. We have simply chosen those which will be of most benefit to us later.

As a final example we will provide the following example of a truth table involving three statements.

Example 1.3.8 The following truth table (Table 1.3.9) can be used to verify the statement

$$[(p \to q) \vee r] \leftrightarrow [(p \wedge \sim q) \to r].$$

Since the columns for $(p \to q) \vee r$ and $(p \wedge \sim q) \to r$ match, we have a tautology.

Table 1.3.9 Truth table for $[(p \to q) \vee r] \leftrightarrow [(p \wedge \sim q) \to r]$

p	q	r	$p \to q$	$(p \to q) \vee r$	$\sim q$	$p \wedge \sim q$	$(p \wedge \sim q) \to r$
T	T	T	T	T	F	F	T
T	T	F	T	T	F	F	T
T	F	T	F	T	T	T	T
T	F	F	F	F	T	T	F
F	T	T	T	T	F	F	T
F	T	F	T	T	F	F	T
F	F	T	T	T	T	F	T
F	F	F	T	T	T	F	T

□

1.3.2 Exercises

1. Verify each of the following using truth tables.

(a) Statements (1)—(13) of Theorem 1.3.6.

(b) Statements (14)—(22) of Theorem 1.3.6.

2. Verify each of the following using truth tables.

(a) Part (1) of Theorem 1.3.7.

(b) Part (2) of Theorem 1.3.7.

(c) Part (3) of Theorem 1.3.7.

3. Using the appropriate tautologies from Theorem 1.3.6, negate the following statements.

(a) A foot has 12 inches and a yard has three feet.

(b) Either I will get a job or I will not be able to pay my bills.

(c) If you study logic one hour per day, then you will make an A in the course.

(d) If $x^2 - 5x + 6 = 0$, then $x - 3 = 0$ or $x - 2 = 0$.

(e) An integer m is odd if and only if m^2 is odd.

(f) If m is an even integer, then $m + 1$ is odd and m^2 is even.

(g) I will call home if I win the game.

4. State the converse, inverse, and contrapositive of the statements indicated below.

(a) The statement in (c) of Exercise 1.3.2.3.

(b) The statement in (d) of Exercise 1.3.2.3.

(c) The statement in (f) of Exercise 1.3.2.3.

(d) The statement in (g) of Exercise 1.3.2.3.

5. Justify why each of the following are true by way of a truth table and a brief paragraph explaining what the statement means.

(a) $[\sim p \wedge (p \vee q)] \to q$

(b) $[(p \to q) \wedge \sim q] \to \sim p$

(c) $[\sim p \to (q \wedge \sim q)] \to p$

1.4 Propositional Functions and Quantifiers

In mathematics we frequently wish to consider sentences (propositions) which involve variables. Since for different values of the variables (called propositional variables) we get different propositions with possibly different truth values, we call such sentences ***propositional functions*** or ***open sentences***.

Example 1.4.1 For each real number x consider the sentence $x^2 + x = 1$. Thus, $x^2 + x = 1$ is a propositional function which has different truth values. The proposition is true for $x = 1$ and $x = -2$ and false for all other values of the propositional variable. □

We can limit propositional functions by prefixing various expressions we call quantifiers, the most important of which are existential quantifiers and universal quantifiers. Phrases such as

- "there exists a value x"
- "there are x, y, and z"
- "for some values of x"
- "at least one value of x"

make use of ***existential quantifiers***. On the other hand, phrases such as

- "for each value of x"
- "for every value of x"
- "for all values of x"
- "no value of x"

are called ***universal quantifiers***.

Example 1.4.2 For each real number x consider the propositional function $p(x)$ that states $x^2 + x = 1$. We can alter that propositional function using the two types of quantifiers.

1. There exists x such that $p(x)$ is true.
2. For all x, $p(x)$ is true.

Clearly, (1) is true and (2) is false. □

Notationally, we will let $p(x)$ be a propositional function which states p is true for each x. Using the existential quantifier, we change $p(x)$ into a proposition, namely "There exists x such that $p(x)$." In mathematics, "there exists" is replaced by the symbol $\exists$, and we replace the statement above by $(\exists x)(p(x))$, which is read "There exists x such that $p(x)$ is true."Similarly, we use the notation for the universal quantifier, $\forall$, and we have the proposition $(\forall x)(p(x))$, which is read "For all x, $p(x)$ is true."

Example 1.4.3 Consider all states in the USA and the propositional function $p(x)$, which states that x is a state which borders on the Pacific Ocean. The proposition $(\forall x)(p(x))$ is false, while the proposition $(\exists x)(p(x))$, is true. □

Remark 1.4.4 Caution! Be careful when using the symbols $\exists$ and $\forall$. While their use is quite common in logic, it is very easy to write confusing sentences. You will rarely see these symbols used in an algebra or calculus textbook. You may wish to avoid using these symbols for the time being.

General forms of qualified statements with their negations can be found in Table 1.4.5.

Table 1.4.5 Truth table for negation

Statement	Negation
Some a are b.	No a is b.
Some a are not b.	All a are b.
All a are b.	Some a are not b.
No a is b.	Some a are b.

1.4.1 Exercises

1. Write each of the following statements in "if-then" form.

(a) Every figure that is a square is a rectangle.

(b) All integers are rational numbers.

(c) Figures with exactly 3 sides may be triangles.

(d) It rains only if it is cloudy.

2. The open sentence "$x^2 + 8 = 6x$," can be made either true or false by using different quantifiers. For example, "For some whole number x, $x^2 + 8 = 6x$" is true, since $x = 4$ or $x = 2$ make the equation true; however, "For all whole numbers x. $x^2 + 8 = 6x$," is false since the equation is false for the whole number $x = 0$ (and for countless other values of x).

Use an appropriate quantifier to make each of the following open sentences true, where x is a whole number. Then use quantifiers to make each statement false.

(a) $x + 5 = 8$

(b) $x + x^2 = x(x + 1)$

(c) $x \cdot 1 = x \cdot 3$

(d) $x^2 + 1 = 0$

3. Negate the following statements.

(a) There exists at least one real number x such that $x^2 = 9$.

(b) There is no real number x that makes the sentence $x^2 = -1$ true.

(c) Some students attend night school.

(d) No children are allowed in this building.

(e) There is some number that is both odd and even.

(f) All college students are math or engineering majors.

(g) For all real numbers x, if x is positive, then $-x$ is negative.

(h) Some cars are red, and all students take math.

(i) There are some people who go to school in the morning and work in the afternoons.

(j) Not all numbers are rational and positive.

(k) All dogs have 4 legs.

(l) Not all rectangles are squares.

4. Find the negation of each of the following.

(a) $p \wedge (q \vee r)$

(b) $\sim p \wedge (q \rightarrow p)$

(c) $[p \wedge (q \rightarrow r)] \vee (\sim q \wedge p)$

(d) x^2 is even only if x is even.

(e) There is an integer x such that $x/2$ is an integer, and for every integer y, $x/(2y)$ is not an integer.

(f) For every postive integer x, either x is prime or $x^2 + 1$ is prime.

Chapter 2

Arguments and Proofs

An argument may be described as a group of statements, one of which is claimed to follow from the others. Arguments have structure. In mathematics, the statement which is supposedly validated by the others is called the conclusion; those statements which are claimed to provide justification for the conclusion are called the hypotheses.

The type of reasoning used in arguments is traditionally divided into two basic types, deductive and inductive. It is often said that deductive reasoning involves moving from the general to the specific, whereas inductive reasoning involves moving from specific observations to claims of general principles. However, this description is a generalization that is not always the case. The major distinction might better be described in terms of whether or not the conclusion must always follow from the hypotheses. In a ***deductive argument*** it is claimed that the conclusion must be true if the hypotheses are true; that is, it is impossible for the conclusion to fail if the hypotheses hold true.

In contrast, an ***inductive argument*** involves the claim that the conclusion probably follows from the hypotheses. Deductive arguments do not become "more valid" by adding hypotheses, whereas inductive arguments may become stronger or weaker by adding hypotheses.

2.1 Deductive Reasoning

Deductive or direct reasoning is a process of reaching a conclusion from one (or more) statements, called the hypothesis (or hypotheses). This somewhat informal definition can be rephrased using the language and symbolism of the preceding sections. An ***argument*** is a set of statements in which one of the statements is called the conclusion and the rest make up the hypothesis. A ***valid argument*** is an argument in which the conclusion must be true whenever the hypotheses are true. In the case of a valid argument we say the conclusion follows from the hypothesis. For example, consider the following argument: "If it is snowing, then it is cold. It is snowing. Therefore, it is cold." In this argument, when the two statements in the hypothesis, namely, "if it is snowing, then it is cold" and "It is snowing" are both true, then one can conclude that "It is cold." That is, this argument is valid since the conclusion follows necessarily from the hypotheses.

It is important to distinguish between the notions of truth and validity. While individual statements may be either true or false, arguments cannot. Similarly, arguments may be described as valid or invalid, but statements cannot. An argument is said to be an invalid argument if its conclusion can be false when its hypothesis is true. An example of an invalid argument is the following: "If it is raining, then the streets are wet. The streets are wet. Therefore, it is raining." For convenience, we will represent this argument symbolically as $[(p \to q) \wedge p] \to p$. This is an invalid argument since the streets could be wet from a variety of causes (e.g., fire hydrant open, sprinkler system malfunction, etc.) without having had any rain. It is possible for valid arguments to contain either true or false hypotheses, as indicated in the two valid arguments in Example 2.1.1.

Example 2.1.1

- Arguement 1:
  - All counting numbers are positive.
  - All positive numbers are larger than negative 2.
  - Therefore, all counting numbers are larger than negative 2.
- Arguement 2:
  - All numbers are positive.
  - All positive numbers are larger than 5.
  - Therefore, all numbers are larger than 5.

Note that in both Arguments 1 and 2, the conclusions follow necessarily from the hypotheses. Thus, Argument 2 is considered valid even though both hypotheses are false. It should also be noted that an argument may be invalid even though the hypotheses and the conclusion are true. In Argument 3 below, even though both hypotheses may be true, it is possible for the conclusion to be either true or false; thus, the argument is invalid.

- Arguement 3:
  - If it is raining outside, then the lawn gets wet.
  - It is not raining outside.
  - Therefore, the lawn is not wet.

The truth table below (Table 2.1.2) shows that Arguement 3 is invalid, since it is possible to have the hypotheses, $(p \to q) \wedge \sim p$, true with the conclusion, $\sim q$, false. This situation, of course, makes the statement $[(p \to q) \wedge \sim p] \to \sim q$ false, and the argument is invalid. □

Table 2.1.2 Truth table for $[(p \to q) \wedge \sim p] \to \sim q$

p	q	$\sim p$	$\sim q$	$p \to q$	$(p \to q) \wedge \sim p$	$[(p \to q) \wedge \sim p] \to \sim q$
T	T	F	F	T	F	T
T	F	F	T	F	F	T
F	T	T	F	T	T	F
F	F	T	T	T	T	T

TAKS CONNECTION.

How might a student apply deductive reasoning to answer the following question taken from the 2006 Texas Assessment of Knowledge and Skills (TAKS) Grade 5 Mathematics test?

Sue is taller than Bianca and shorter than Colette. If Colette is shorter than Dora, who is the shortest person?

- F. Sue
- G. Bianca
- H. Colette
- J. Dora

Example 2.1.3 Charles Dodgson (1832–1898) was an English mathematician who taught logic at Oxford University. As a teacher of logic and a lover of nonsense, he designed entertaining puzzles to train people in systematic reasoning. In these puzzles he would string together a list of implications, purposefully nonsensical so that his students would not influenced by any preconceived opinions. The task presented to the student was to use all the listed implications to arrive at an inescapable conclusion. You may know Charles Dodgson better by his pen name Lewis Carroll, author of *Alice's Adventures in Wonderland* and *Through the Looking-Glass*.

For example, consider the following statements.

1. All babies are illogical.
2. Nobody is despised who can manage a crocodile.
3. Illogical persons are despised.

Let

p it is a baby
q it is logical
r it can manage a crocodile
s it is despised.

The statements now translate to

1. $p \rightarrow \sim q$ (All babies are illogical.)
2. $r \rightarrow \sim s$ or $s \rightarrow \sim r$ (Nobody is despised who can manage a crocodile.)
3. $\sim q \rightarrow s$ (Illogical persons are despised.)

Linking these statements together, we see that $p \rightarrow \sim q \rightarrow s \rightarrow \sim r$. In other words, $p \rightarrow \sim r$ or "babies cannot manage crocodiles." □

Translating a conditional statement into "if-then" form can be quite confusing. The statement "All babies are illogical" is not in a very useful form; however, we can write an equivalent "if-then" statement: "If it is a baby, then it is not logical." Consider the following examples.

- "It rains only if I carry an umbrella" can be rewritten as "If it rains, then I carry an umbrella."
- "All citizens of Egypt speak Arabic." can be rewritten as "If someone is a citizen of Egypt, then they speak Arabic."
- "Unless it is sunny, I carry an umbrella." can be rewritten as "If it is not sunny, I carry an umbrella."

- "No one in MTH 300 speaks Chinese." can be rewritten as "If you are in MTH 300, then you do not speak Chinese."
- "For cows to fly it is sufficient that 3 + 4 = 8." can be rewritten as "If 3 + 4 = 8, then cows fly."
- "For cows to fly it is necessary that 3 + 4 = 8." can be rewritten as "If cows fly, then 3 + 4 = 8."
- "When it rains, I carry an umbrella." can be rewritten as "If it rains, I carry an umbrella."

2.1.1 Exercises

1. Rewrite the following conditional statements as "if-then" statements.

(a) All citizens of Egypt speak Arabic.

(b) Dallas is the capital of Texas only if $2 + 3 \neq 7$.

(c) Nacogdoches is the oldest city in Texas unless mermaids exist.

(d) No resident of Boston likes hot peppers.

(e) For $3 + 7 = 10$ it is necessary that cows fly.

(f) For $3 + 7 = 10$ it is sufficient that cows fly.

(g) I carry and umbrella when it rains.

(h) I carry an umbrella only if it rains.

See how many of the following Lewis Carroll puzzles you can solve.

2.

- All babies are illogical.
- Nobody is despised who can manage a crocodile.
- Illogical persons are dispised.

3.

- None of the unnoticed things, met with at sea, are mermaids.
- Things entered in the log, as met with at sea, are sure to be worth remembering.
- I have never met with anything worth remembering, when on a voyage.
- Things met with at sea, that are noticed, are sure to be recorded in the log.

4.

- No ducks waltz.
- No officers ever decline to waltz.
- All my poultry are ducks.

5.

- No birds, except ostriches, are 9 feet high.
- There are no birds in this aviary that belong to anyone but me.

- No ostrich lives on mince pies.
- I have no birds less than 9 feet high.

6.

- All writers, who understand human nature, are clever.
- No one is a true poet unless he can stir the hearts of men.
- Shakespeare wrote "Hamlet."
- No writer, who does not understand human nature, can stir the hearts of men.
- None but a true poet could have written "Hamlet."

7.

- No kitten, that loves fish, is unteachable.
- No kitten without a tail will play with a gorilla.
- Kittens with whiskers always love fish.
- No teachable kitten has green eyes.
- No kittens have tails unless they have whiskers

8.

- No shark ever doubts that he is well fitted out.
- A fish, that cannot dance a minuet, is contemptible.
- No fish is quite certain that it is well fitted out, unless it has three rows of teeth.
- All fishes, except sharks, are kind to children.
- No heavy fish can dance a minuet.
- A fish with three rows of teeth is not to be despised.

2.2 Three Forms of Valid Arguments

Three especially important forms of valid arguments, used repeatedly in logic, are discussed next.

2.2.1 Law of Detachment (Direct Reasoning): $[((p \to q) \wedge p)] \to q$

The Law of Detachment is the most commonly used principle of deductive reasoning. In words, this law says that whenever a conditional statement and its hypothesis are true, the conclusion is also true. That is, the conclusion can be "detached" from the conditional (see Example 2.2.1).

Example 2.2.1

- If the units digit of a number is zero, then the number is a multiple of 10.
- The units digit in the number 40 is zero.

- Therefore, 40 is a multiple of 10.

□

Special types of diagrams, called Euler (pronounced "oiler") diagrams, can also be used to help determine the validity of arguments. The argument in Example 2.2.1 can be visualized using an Euler diagram as indicated in Figure 2.2.2.

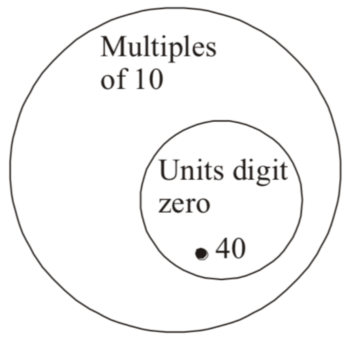


Figure 2.2.2 Euler diagram for direct reasoning

2.2.2 Law of Syllogism (Transitive Reasoning): $[(p \to q) \wedge (q \to r)] \to (p \to r)$

The Law of Syllogism is also called transitive reasoning or the chain rule. Examples of the Law of Syllogism occur repeatedly in mathematics. The following argument is an application of this law.

Example 2.2.3

- If a number is a multiple of eight, then it is a multiple of four.
- If a number is a multiple of four, then it is a multiple of two.
- Therefore, if a number is a multiple of eight, then it is a multiple of two.

An Euler diagram for this argument is given in Figure 2.2.4. Notice that if x is any number that is a multiple of eight, then x is also a multiple of four. Then, since x is a multiple of four, x must also be a multiple of two. □

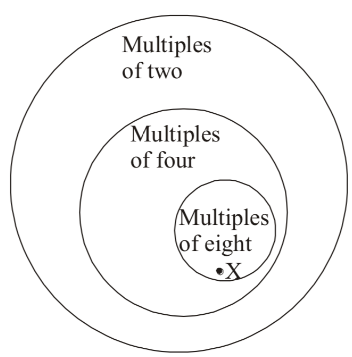


Figure 2.2.4 Euler diagram for transitive reasoning

2.2.3 Law of Contraposition (Indirect Reasoning): $[(p \to q) \wedge \sim q] \to \sim p$

Since the contrapositive of a conditional is logically equivalent to the original conditional, $\sim q \to \sim p$ is logically equivalent to $p \to q$. Then, by applying the Law of Detachment to the contrapositive of $p \to q$, we may deduce $\sim p$.

Example 2.2.5

- If a number is a power of 3, then its units digit is 1, 3, 7, or 9.
- The units digit ins 3,124 is not 1, 3, 7, or 9.
- Therefore, 3,124 is not a power of 3.

In words, the Law of Contraposition says that whenever a conditional is true and its conclusion is false, then the hypothesis is also false. (In other words, if a conditional is true and the negation of its conclusion is also true, then the negation of its hypothesis is true.) Again, an Euler diagram may be used to help determine the validity of the argument (Figure 2.2.6). □

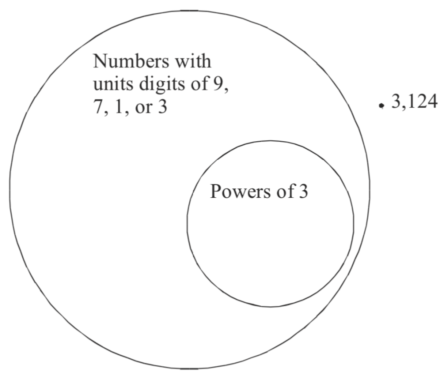


Figure 2.2.6 Euler diagram indirect reasoning

2.2.4 Exercises

1. Determine the validity of the following arguments. Justify your thinking.

(a)
- All equilateral triangles are equiangular.
- All equiangular triangles are isosceles.
- Therefore, all equilateral triangles are isosceles.

(b)
- All equilateral triangles are equiangular.
- All equiangular triangles are isosceles.
- Therefore all isosceles triangles are equilateral.

(c)
- If you study every day, then you will be successful.
- You do not study every day.
- Therefore, you will not be successful.

(d)
- If you study every day, then you will be successful.
- You are not successful.
- Therefore, you did not study every day.

(e)
- Some females are doctors.

- All doctors are college graduates.
- Therefore, all females are college graduates.

(f)
- If the alarm goes off, then I will call the police.
- I called the police.
- So the alarm went off.

(g)
- If the alarm goes off, then I will call the police.
- If I call the police, then I will file a report.
- The alarm went off, so I will file a report.

(h)
- If today is Friday, then tomorrow is Saturday.
- Tomorrow is Monday, so today is not Friday.

(i)
- All teachers are smart.
- Some teachers are funny.
- Therefore, some smart people are funny.

(j)
- If a student is a freshman, then the student takes English.
- Mark is a junior.
- Therefore, Mark does not take English.

2. Determine a valid conclusion that follows from each of the following statements and explain your reasoning.

(a) If you come to class every day, then you will be successful. You come to class every day.

(b) If Jana does not fall, then she will win the race. Jana does not win the race.

(c) Every square is a rectangle. Some parallelograms are rhombuses. Every rectangle is a parallelogram.

3. Suppose that $r \to s$ is false. Determine the truth values (true, false, or cannot be determined) of each of the following statements.

(a) $s \to r$

(b) $s \vee r$

(c) $s \wedge r$

(d) $\sim r$

(e) $\sim s \to r$

(f) $\sim s \wedge r$

4. What conclusions can be deduced from these sets of hypotheses? (Let f stand for a statement that is false.)

(a)

Hypotheses:	p or q
	$\sim p$
Conclusion	?

(b)

Hypotheses:	$\sim p \to f$
Conclusion	?

(c)

Hypotheses:	$(p \wedge q) \to r$
	p
Conclusion	? (Give a conditional statement.)

5. There are three forms of invalid reasoning which commonly occur.

- *Fallacy of the converse.*

$$\begin{array}{ll} \text{If } p, \text{ then } q. & \\ q & \\ \hline p & \text{(invalid)} \end{array}$$

- *Fallacy of the inverse.*

$$\begin{array}{ll} \text{If } p, \text{ then } q. & \\ \sim p & \\ \hline \sim q & \text{(invalid)} \end{array}$$

- *False transitivity.*

$$\begin{array}{ll} \text{If } p, \text{ then } q. & \\ \text{If } p, \text{ then } r. & \\ \hline \text{If } q, \text{ then } r. & \text{(invalid)} \end{array}$$

Which fallacies occur in the following arguments?

(a) If I am a good person, nothing bad will happen to me. Nothing happened to me. Therefore, I am a good person.

(b) If you work hard, you will be wealthy and wise. Therefore, if you are wealthy, then you will be wise.

2.3 Proofs

As we stated both in the preface as well as earlier in this chapter, our working definition of mathematics is that it is the application of inductive and deductive logic to a system of axioms. It is not our purpose in this text to formalize the logical procedure required to provide formalistic proofs. Rather, we wish to arm the student with the basic logic and methods of attack used to form convincing arguments of the validity of the statements encountered in a reasonably careful study of the foundations of mathematics.

Since we will need a working definition of the word “proof,” we agree that a proof is a logical sequence of steps which validate the truth of the proposition in question. In this vein the reader should review those statements which we have proven and note that usually we merely showed that certain definitions were satisfied. For example, when we proposed certain statements were equivalent, we established that they had the same truth value. Surely, as we proceed further, we will be forced to provide proofs which require longer and at times more subtle sequences of logical statements. Our endeavor, as well as yours, will be to convince the reader of the truth of the propositions in question.

There are, however, some general approaches to proofs which are based on the various tautologies and contradictions presented in Section 1.3. Most theorems are merely conditional statements of the form, “If p, then q.” Certainly, p and q might themselves be complicated compound statements, but that should not be allowed to cloud the issue at this time, so let us consider a typical theorem and a few general types of proof.

Theorem 2.3.1 *If p, then q.*

2.3.1 Method 1: Direct Proof

Recall from the truth table of a conditional sentence that when p is false, q can have any truth value and the conditional will still be true. Thus, we need only consider the case when p is true and argue that q must also be true. Hence, we assume p is true and by applying various known tautologies and apparent implications, we argue q is also true.

Example 2.3.2 We will prove the statement: "Let m and n be integers. If m is even and n is even, then $m+n$ is even."

Proof. Assume the hypothesis, "m is even and n is even" is true. By definition of conjunction, it follows that the component statements "m is even" and "n is even" are true. But since even numbers are by definition multiples of 2, there must exist integers r and s such that $m = 2r$ and $n = 2s$. Then substitution yields

$$m + n = 2r + 2s = 2(r + s).$$

Since the set of integers is closed under addition, the number $r + s$ is also an integer. Thus, we have written $m + n$ as 2 times an integer, so we have shown $m + n$ is even. That is, the conclusion "$m + n$ is even" is true whenever the hypothesis "m is even and n is even" is true. □

2.3.2 Method 2: Proof by Contradiction

We know that $[\sim(p \to q)] \leftrightarrow [p \wedge (\sim q)]$ by part (5) of Theorem 1.3.6. If we begin by assuming $p \wedge (\sim q)$ is true and reach a contradiction, it must be the case that $p \wedge (\sim q)$ is false. But $p \wedge (\sim q)$ being false and yet equivalent to $\sim(p \to q)$ implies that $\sim(p \to q)$ is also false or $p \to q$ is true. Therefore, in proving by contradiction, we assume p and $\sim q$ are both true and reach a contradiction. This logically shows that the statement $p \to q$ as argued above.

Example 2.3.3 We will prove the statement: "Let x and y be positive real numbers. If $x \neq y$, then $x^2 \neq y^2$."

Proof. For positive real numbers x and y, assume $x \neq y$ and $x^2 = y^2$. Then

$$x^2 - y^2 = (x - y)(x + y) = 0.$$

Hence, either $x - y = 0$ or $x + y = 0$. We assumed that $x \neq y$, so $x - y \neq 0$. Consequently, $x + y = 0$ or $x = -y$, which contradicts the assumption that both x and y are positive. Therefore, $x^2 \neq y^2$ if $x \neq y$. □

2.3.3 Method 3: Proof by Contrapositive (Indirect Proof)

Since we know that $(p \to q) \leftrightarrow (\sim q \to \sim p)$ by part (8) of Theorem 1.3.6, we can prove $\sim q \to \sim p$ instead of $p \to q$. That is, we assume that $\sim q$ is true and argue that $\sim p$ is true. So essentially, a proof by contraposition is a direct proof applied to a statement that is equivalent to the one we wish to prove.

Example 2.3.4 As in Example 2.3.3, we will prove the statement: "Let x and y be positive real numbers. If $x \neq y$, then $x^2 \neq y^2$." However, we will directly prove the equivalent statement, "If $x^2 = y^2$, the $x = y$."

Proof. Assume that $x^2 = y^2$. Then

$$x^2 - y^2 = (x - y)(x + y) = 0.$$

Consequently, $x - y = 0$ or $x + y = 0$. Since both x and y are positive, $x + y$ must also be positive. Hence, $x + y \neq 0$. Therefore, $x - y = 0$ or $x = y$. □

2.3.4 Counterexamples

We can use a counterexample to prove that a statement is false. In considering the truth value of a conditional statement $p \to q$, we would know the statement is false if we could find a single example for which p is true but q is false.

Example 2.3.5 Consider the statement: "Let m and n be integers. If m is even, then $m + n$ is even." By considering a single example such as $m = 2$ and $n = 3$, and observing that

$$m + n = 2 + 3 = 5$$

is not even, we have established the conditional statement is false. □

2.3.5 Exercises

1. Let m and n represent integers. Prove by the direct method.

(a) If n is even, then $-n$ is even.

(b) If n is odd, then $-n$ is odd.

(c) If m is even and n is odd, then $m + n$ is odd.

(d) If m is odd, then $m^2 + 1$ is even.

2. Using facts from Exercise 2.3.5.1, prove the given statement by the method indicated.

If $m + n$ is even and m is odd, then n is odd.

(a) Direct method.

(b) Contraposition.

(c) Contradiction.

Chapter 3

Sets

TEXAS STATE BOARD FOR EDUCATOR CERTIFICATION (SBEC): MATHEMATICS STANDARDS COVERED.

- STANDARD V: MATHEMATICAL PROCESSES: The mathematics teacher understands and uses mathematical processes to reason mathematically, to solve mathematical problems, to make mathematical connections within and outside of mathematics, and to communicate mathematically.
- STANDARD VI: MATHEMATICAL PERSPECTIVES: The mathematics teacher understands the historical development of mathematical ideas, the interrelationship between society and mathematics, the structure of mathematics, and the evolving nature of mathematics and mathematical knowledge.

3.1 Sets

An underlying idea of mathematics is the concept of a collection of objects or a set.

Definition 3.1.1 A **set** is a collection of distinct objects, which are called the **elements** of the set. We will use capital letters to denote sets, for example a, B, S, T, etc. If x is an element of a set S, we use the notation $x \in S$. As is frequently done in mathematics, if x is not an element of a set S, we denote this by $x \notin S$. Two sets, A and B, are **equal** (denoted $A = B$) if and only if they have precisely the same elements. $\Diamond$

Definition 3.1.2 A set which is comprised of some (or all) of the elements of $\mathbb{U}$, some **universal set**, is called a subset of $\mathbb{U}$ and is denoted $S \subseteq \mathbb{U}$. If $A \subseteq \mathbb{U}$ and $B \subseteq \mathbb{U}$, we further state that A is a **subset** of B, denoted $A \subseteq B$ or $A \subseteq B$, if each element of A is also an element of B. Moreover, if $A \subseteq B$ but $A \neq B$, we say that A is a **proper subset** of B and write $A \subsetneq B$. $\Diamond$

Example 3.1.3 Let $\mathbb{U} = \{a, b, c, \ldots, z\}$, $S = \{a, b, s, u\}$, $T = \{a, u\}$, and $W = \{b, d\}$. The $S \subseteq \mathbb{U}$, $T \subseteq \mathbb{U}$, $W \subseteq \mathbb{U}$, and $T \subseteq S$. However, $W \not\subseteq S$, $W \not\subseteq T$, $T \not\subseteq W$, and $S \not\subseteq W$. We read $W \not\subseteq S$ as "W is not a subset of S." In addition, $S \subset \mathbb{U}$, $T \subset \mathbb{U}$, $W \subset \mathbb{U}$, and $T \subset S$. $\square$

When referring to the definition of subset, you should note that to prove $A \subseteq B$, one would naturally consider an arbitrary element x of A and prove that $x \in B$. In other words, we must prove the conditional statement "If $x \in A$, then $x \in B$."

Fact 3.1.4 *Let A and B be sets. Then $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. We sometimes refer to this method of proof as "proofs by double inclusion."*

Without entering into a philosophical argument, we define $\emptyset$ to be the set with no elements, called the **empty set**, the **void set**, or the **null set**. This set is extremely useful and should be understood carefully.

Fact 3.1.5 *Let $\mathbb{U}$ be any universal set and $A \subseteq \mathbb{U}$. Then $\emptyset \subseteq A$ and $\emptyset \subseteq \mathbb{U}$.*

Proof. By definition of subset, we must show each element in $\emptyset$ is also an element of A (or $\mathbb{U}$, if we are proving $\emptyset \subseteq \mathbb{U}$); however, since there are no elements in to check, the definition is satisfied.

Let us consider the proof above logically. Recall that $A \subseteq B$ is a conditional statement (if $x \in A$, then $x \in B$). So we need to examine "If $x \in \emptyset$, then $x \in A$." But $\emptyset$ has no elements, so $x \in \emptyset$ is false, meaning the conditional is true. ■

The next definition introduces several basic ways of combining sets which are used throughout mathematics.

Definition 3.1.6 Let $\mathbb{U}$ be the universal set with A and B subsets of $\mathbb{U}$. Then

- $A \cup B = \{x \in \mathbb{U} \mid x \in A \text{ or } x \in B\}$, which is called A **union** B.
- $A \cap B = \{x \in \mathbb{U} \mid x \in A \text{ and } x \in B\}$, which is called A **intersect** B.
- $\overline{A} = \{x \in \mathbb{U} \mid x \notin A\}$, which is called the **complement** of A.
- $A \setminus B = \{x \in \mathbb{U} \mid x \in A \text{ or } x \notin B\}$, which is read A **minus** B.
- A and B are set to be **disjoint** if $A \cap B = \emptyset$.

◊

While not sufficient for proof, Venn diagrams can be useful in visualizing these concepts (Figure 3.1.7–3.1.10).

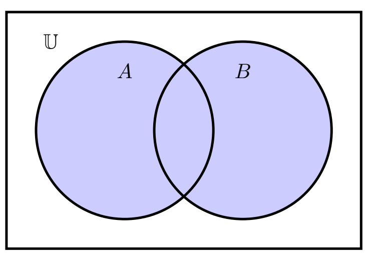


Figure 3.1.7 The shaded area represents $A \cup B$

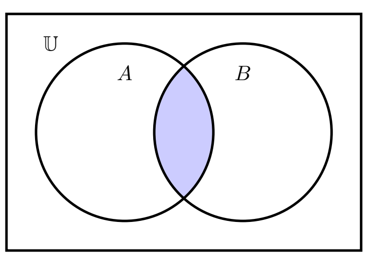


Figure 3.1.8 The shaded area represents $A \cap B$

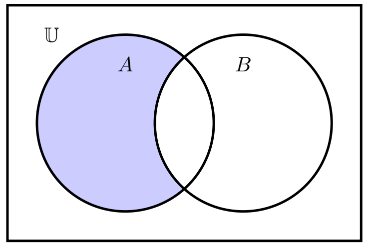


Figure 3.1.9 The shaded area represents $A \setminus B$

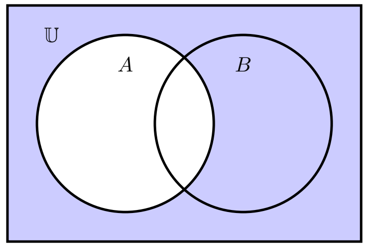
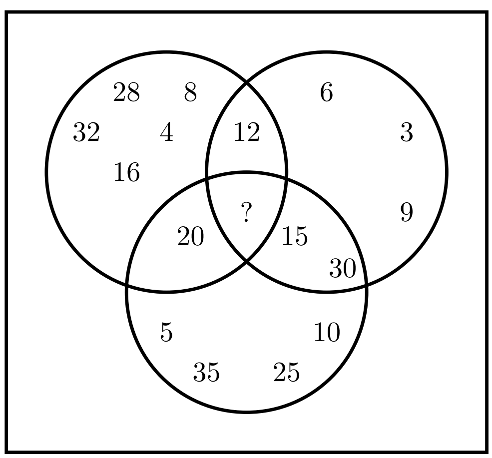


Figure 3.1.10 The shaded area represents $\overline{A}$

TAKS CONNECTION.

How might a student apply the concept of set intersections to answer the following question taken from the 2006 Texas Assessment of Knowledge and Skills (TAKS) Grade 5 Mathematics test?

The Venn diagram below is used to classify counting numbers according to a set of rules.



Which one of the following numbers belongs in the region of the diagram marked by the question mark?

- A. 45
- B. 50
- C. 60
- D. 65

Definition 3.1.11 If A is a set, then the **power set** of A is the set $\mathcal{P}(A) = \{B \mid B \subseteq A\}$. ◊

Example 3.1.12 If $A = \{1, 2\}$, then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, A\}$. If $B = \{a, b, c\}$, then $\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, B\}$. □

Definition 3.1.13 If A and B are sets, then $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$ is called the **Cartesian product** or the **cross product** of A and B. ◊

Example 3.1.14 If $A = \{1, 2\}$ and $B = \{a, b, c\}$, then $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$. □

Fact 3.1.15 *Let A, B, and C be subsets of a universal set $\mathbb{U}$. Then*

1. $A \subseteq A \cup B$.
2. $A \cap B \subseteq A$.
3. $A \setminus B \subseteq A$.
4. $A \setminus B$ *and* $B \setminus A$ *are disjoint.*
5. A *and* $\overline{A}$ *are disjoint.*
6. *If* $A \subseteq B$ *and* $B \subseteq C$, *then* $A \subseteq C$.
7. $A \cup B = B \cup A$.
8. $A \cap B = B \cap A$.
9. $A \cap (B \cap C) = (A \cap B) \cap C$.
10. $A \cup (B \cup C) = (A \cup B) \cup C$.
11. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
12. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
13. $A \subseteq B$ *if and only if* $\overline{B} \subseteq \overline{A}$.
14. $A \setminus B = A \cap \overline{B}$.
15. $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
16. $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
17. $\overline{\overline{A}} = A$.
18. $A \cup \emptyset = \emptyset \cup A = A$.
19. $A \cap \emptyset = \emptyset \cap A = \emptyset$.
20. $A \cup \mathbb{U} = \mathbb{U} \cup A = \mathbb{U}$.
21. $A \cap \mathbb{U} = \mathbb{U} \cap A = A$.

Example 3.1.16 We will prove (3) in Fact 3.1.15. That is, we will show $A \setminus B \subseteq A$.

Proof: Let $x \in A \setminus B$. Then $x \in A$ but $x \notin B$. By the definition of a subset $A \setminus B \subseteq A$. That is, "if $x \in A \setminus B$, then $x \in A$." □

Example 3.1.17 We will prove (7) in Fact 3.1.15. That is, we will show $A \cup B = B \cup A$.

Proof: Let $x \in A \cup B$. Then $x \in A$ or $x \in B$ by the definition of $A \cup B$. Hence, $x \in B$ or $x \in A$. By the definition of union $x \in B \cup A$. We have argued by direct proof that "$x \in A \cup B$, then $x \in B \cup A$." Thus, $A \cup B \subseteq B \cup A$. By reversing the proof, we can show that $B \cup A \subseteq A \cup B$. Therefore, $A \cup B = B \cup A$

□

Example 3.1.18 We will prove (16) in Fact 3.1.15. That is, we will show $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Proof: To show $\overline{A \cap B} = \overline{A} \cup \overline{B}$, we again use the method of double inclusion. Let $x \in \overline{A \cap B}$. Then $x \notin A \cap B$. Recalling the definition of intersection, we notice that the statement $x \notin A \cap B$ parallels the logic statement $\sim(p \wedge q)$. DeMorgan's Laws for logic tell us that $[\sim(p \wedge q)] \leftrightarrow [\sim p \vee \sim q]$. So we now have $x \notin A$ or $x \notin B$; hence, $x \in \overline{A}$ or $x \in \overline{B}$. Thus, by definition of union, $x \in A \cup B$. Consequently, $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$.

To see that $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$ let $y \in \overline{A} \cup \overline{B}$. Then $y \in \overline{A}$ or $y \in \overline{B}$, which means that $y \notin A$ or $y \notin B$. Arguing as above, we have $y \notin A \cap B$. Thus, $y \in \overline{A \cap B}$, and $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. □

As indicated, the proofs of the other parts of this fact are left as exercises.

3.1.1 Historical Note

Unlike most areas of mathematics, which arise as a result of the cumulative efforts of many mathematicians, sometimes over several generations, set theory is the creation of a single individual. Georg Ferdinand Ludwig Phillip Cantor (27 June 1806–18 March 1871) was a German mathematician, born in Russia. Use internet and/or library resources to research his major contributions to the area of set theory, specifically the concept of cardinality and Cantor's Theorem.

3.1.2 Exercises

1. Let $\mathbb{U} = \{1, 2, \ldots 10\}$, $A = \{1, 2, 3, 4, 5\}$, $B = \{2, 3, 5\}$, $D = \{1, 3, 5, 7, 9\}$, and $E = \{2, 4, 6, 8, 10\}$. Label each of the statements below as True or False and explain.

(a) D and E are disjoint.

(b) $A \subseteq E$.

(c) $B \subset A$.

(d) $A \subset \mathbb{U}$.

(e) $(A \cap D) \subset A$.

(f) $(A \cup E) \subset \mathbb{U}$.

(g) $(D \cup E) \subset \mathbb{U}$.

(h) $(D \cup E) = \mathbb{U}$.

(i) $6 \in D$.

(j) $\{8\} \in E$.

(k) $\emptyset \subseteq B$.

(l) $\{2, 3\} \subseteq B$.

(m) $5 \subseteq B$.

(n) $\emptyset \subseteq \emptyset$.

(o) $\overline{D} = E$.

(p) $\overline{B \cup D} \subseteq E$.

2. Using the sets in Exercise 3.1.2.1, find:

(a) $\overline{B}$

(b) $D \setminus A$

(c) $\overline{D} \cap \overline{A}$

(d) $\overline{D \cup A}$

(e) $E \cap (B \cup D)$

(f) $\overline{A} \cap (B \setminus D)$

(g) $\overline{D \cap E}$

(h) $\overline{D \setminus E}$

3. Prove (1) in Fact 3.1.15

4. Prove (2) in Fact 3.1.15

5. Prove (4) in Fact 3.1.15

6. Prove (5) in Fact 3.1.15

7. Prove (6) in Fact 3.1.15

8. Prove (8) in Fact 3.1.15

9. Prove (9) in Fact 3.1.15

10. Prove (10) in Fact 3.1.15

11. Prove (11) in Fact 3.1.15

12. Prove (12) in Fact 3.1.15

13. Prove the second half of Part (13) in Fact 3.1.15

14. Prove (14) in Fact 3.1.15

15. Prove (15) in Fact 3.1.15

16. Prove (17) in Fact 3.1.15

17. Prove (18) in Fact 3.1.15

18. Prove (19) in Fact 3.1.15

19. Prove (20) in Fact 3.1.15

20. Prove (21) in Fact 3.1.15

For each of the following problems, assume A, B, C, and D are subsets of some universal set $\mathbb{U}$. In problems Exercise 3.1.2.21–3.1.2.33, prove that the statements are true.

21. If $C \subseteq A$ or $C \subseteq B$, then $C \subseteq A \cup B$.

22. If $A \subseteq C$ and $B \subseteq C$, then $A \cap B \subseteq C$.

23. $A \setminus A = \emptyset$.

24. $A \setminus (A \setminus B) \subseteq B$.

25. If A or B are disjoint, then $B \subseteq \overline{A}$.

26. If $A \subseteq C$ and $B \subseteq D$, then $A \setminus D \subseteq C \setminus B$.

27. $A \setminus (B \setminus C) = A \cap (\overline{B} \cup C)$.

28. $(A \setminus B) \setminus C = A \setminus (B \cup C)$.

29. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

30. $A \subseteq B$ if and only if $A \cap B = A$.

31. $A \subseteq B$ if and only if $A \cup B = B$.

32. $B \subseteq A$ if and only if $A \cup \overline{B} = \mathbb{U}$.

33. If $A \subseteq B$ and $C \subseteq D$, then

(a) $A \cup C \subseteq B \cup D$ and

(b) $A \cap C \subseteq B \cap D$.

34. Prove or disprove:

(a) If $A \cup B = A \cup C$, then $B = C$.

(b) If $A \cap B = A \cap C$, then $B = C$.

35. Define $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Prove or disprove:

(a) $A \triangle B = B \triangle A$.

(b) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$.

(c) $A \triangle \emptyset = A$.

(d) $A \triangle A = \emptyset$.

(e) $A \triangle B = (A \cup B) \setminus (A \cap B)$.

(f) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

(g) $A \cup (B \triangle C) = (A \cup B) \triangle (A \cup C)$.

(h) $A \cap B = \emptyset$ if and only if $A \triangle B = A \cup B$.

36. Draw Venn diagrams to illustrate various parts of Fact 3.1.15.

37. For sets $A = \{1, 2, 3, 4, 5\}$, $B = \{3, 5, 7, 9\}$, and $C = \{a, b\}$, find:

(a) $\mathcal{P}(C)$.

(b) $A \times C$.

(c) $C \times (A \cap B)$.

(d) $(C \times A) \cap (C \times B)$.

38. Prove or disprove: If $A, B \in \mathcal{P}(S)$, then $A \cup B \in \mathcal{P}(S)$.

39. Prove or disprove: If $A, B \in \mathcal{P}(S)$, then $A \cap B \in \mathcal{P}(S)$.

40. Is it true that $A \times \emptyset = \emptyset \times A = \emptyset$? Justify your thinking.

Chapter 4

Relations

TEXAS STATE BOARD FOR EDUCATOR CERTIFICATION (SBEC): MATHEMATICS STANDARDS COVERED.

- STANDARD II: PATTERNS AND ALGEBRA: The mathematics teacher understands and uses patterns, relations, functions, algebraic reasoning, analysis, and technology appropriate to teach the statewide curriculum (Texas Essential Knowledge and Skills [TEKS]) in order to prepare students to use mathematics.
- STANDARD V: MATHEMATICAL PROCESSES: The mathematics teacher understands and uses mathematical processes to reason mathematically, to solve mathematical problems, to make mathematical connections within and outside of mathematics, and to communicate mathematically.
- STANDARD VI: MATHEMATICAL PERSPECTIVES: The mathematics teacher understands the historical development of mathematical ideas, the interrelationship between society and mathematics, the structure of mathematics, and the evolving nature of mathematics and mathematical knowledge.

In our everyday lives we encounter many circumstances which necessitate relating objects, sets, or people. Hiring is determined by comparing abilities of applicants and purchases are made based on relative prices. Descriptions such as "is faster than," "is the brother of," and "is smaller than" are heard countless times each day.

This concept of relating elements from different collections of objects is used extensively in mathematics. In previous courses, you have considered relations primarily from a very informal perspective; we will now approach the study of relations in a more formal way and give a formal definition of a relation below. A variety of special types of relations, including functions, will be considered in greater depth in this chapter.

4.1 Relations

For convenience, we restate the definition of the Cartesian product of sets with which you might already be familiar.

Definition 4.1.1 The ***Cartesian product*** of two sets A and B, denoted $A \times B$, is the set consisting of all ordered pairs in which the first element comes from set A and the second element comes from set B; that is, $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$. ♢

Definition 4.1.2 A ***relation*** R from a set A to a set B is a subset of $A \times B$. If R is a relation from A to A, we say R is a relation on A. ♢

While a relation may be described in a variety of ways, it is really just a set of ordered pairs.

Example 4.1.3 Let $A = \{a, b, c, d\}$ and $B = \{1, 2, 3\}$. Consider the following sets.

1. $R_1 = \{(a, 2), (b, 3), (c, 2), (d, 3)\}$
2. $R_2 = \{(a, 1), (a, 2), (b, 3)\}$
3. $R_3 = \{(a, 1), (b, 3), (c, 2)\}$
4. $R_4 = \{(a, a), (b, b), (c, c), (d, d)\}$
5. $R_5 = \{(d, a), (c, a), (d, d)\}$

Each of the sets R_1, R_2, and R_3 is a relation from A to B because the first elements in the ordered pairs are from A and the second elements are from B, while R_4 and R_5 are relations on A because both first and second elements are from A. □

Although relations are actually sets of ordered pairs, such collections of ordered pairs may be indicated in many ways. Notice that a relation is essentially a pairing of elements according to some criteria. For example, we may "pair" a person's name with his or her social security number, age, height, or the names of cities lived in. Sometimes relations are specified simply by listing these pairs in set form as in the example above. When relations are described in this form, the rules or criteria for the pairing are often not known. For instance, in R_1 of Example 4.1.3, we know that b and d are both related to 3, but we do not know why. Similarly, relations may be indicated in table or graphical form as in the below.

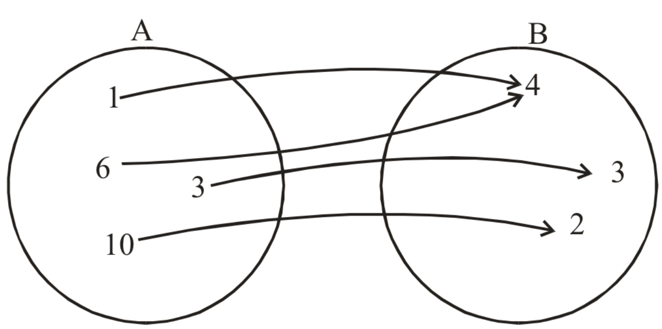
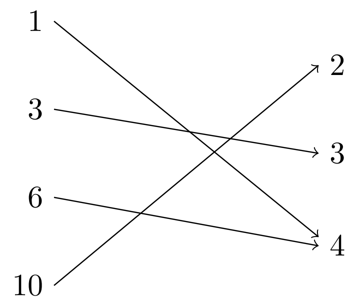


Figure 4.1.4 Pictorial representation R from A to B

Example 4.1.5 Figure 4.1.4 is a pictorial representation of of the relation $R = \{(1,4),(6,4),(3,3),(10,2)\}$ from $A = \{1,3,6,10\}$ to $B = \{2,3,4\}$. The arrow diagram below is a different way of representing the same relation.



A third representation of R is given in table form below.

Table 4.1.6 A table representation R from A to B

a	b
1	4
3	3
6	4
10	2

□

In many cases, listing all the ordered pairs in a relation is tedious or simply impossible. Under those circumstances the relation may be described in many different ways; associated ordered pairs are indicated by specifying a defining rule.

Example 4.1.7 The equation $x + y = 4$ describes a relation, R, consisting of an infinite set of ordered pairs whose components will satisfy the equation. Hence, the ordered pairs $(2,2)$, $(3/2, 5/2)$, $(-7, 11)$, and $(0,4)$ are a few of the elements in the relation. Precisely stated,

$$R(x,y) = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x + y = 4\}$$

That is, the relation described by the equation is actually the infinite set of ordered pairs of real numbers whose sum is equal to 4. In the following figure, we have indicated all the ordered pairs which satisfy the linear equation; this is sometimes called the graphical representation of the equation.

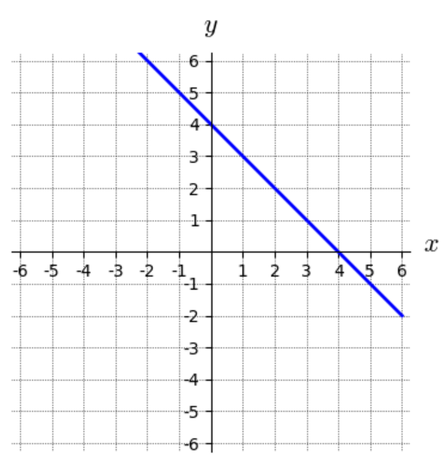


Figure 4.1.8 Graphical representation of $x + y = 4$

□

Example 4.1.9 Let $A = \{1, 2, 3, 4\}$ and define a relation R on A by

$$R(x, y) = \{(x, y) \in A \times A \mid x \leq y\}.$$

That is, R is the set of all ordered pairs whose components both come from the set A and in which the first component is less than or equal to the second. In this case we could enumerate R as follows:

$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$$

□

Notice in Example 4.1.9 that it is merely inconvenient to have to list all the ordered pairs implied by the rule given. However, if the set A were the set of all integers instead of the finite set $\{1, 2, 3, 4\}$, the same rule applied to A would yield an infinite set of ordered pairs that would be impossible to list. In such cases, it is convenient to use notation that refers to the relation by the criteria used for comparison. We say the relation R is "less than or equal to" or "$\leq$" rather than the actual set of ordered pairs, and instead of saying $(1, 3) \in R$, we say $1 \leq 3$.

Remark 4.1.10 In general, we often substitute the notation aRb for $(a, b) \in R$.

Then to determine whether two elements in the set are related, we simply substitute our familiar relation for R in the expression aRb. For example, instead of asking if the ordered pair $(3, 2)$ is an element of the relation "is greater than," we ask if 3 "is greater than" 2; that is, we usually write $3 > 2$ instead of writing $(3, 2) \in$ "$>$".

In considering each of the examples given in this section, it is clear that a relation between sets A and B need not "use up" all of both sets. This idea leads us to consider those subsets of A and B whose elements are paired by the relation, namely the domain and range.

Definition 4.1.11 If R is a relation from A to B, then the **domain** of R, $\text{Dom}(R)$ is defined by

$$\text{Dom}(R) = \{a \in A \mid (a, b) \in R \text{ for some } b \in B\}.$$

The **range**, denoted by $\text{Ran}(R)$, is defined by

$$\text{Ran}(R) = \{b \in B \mid (a, b) \in R \text{ for some } a \in A\}.$$

◊

By Definition 4.1.11, it is clear that $\text{Dom}(R)$ is a subset of A and $\text{Ran}(R)$ is a subset of B.

Informally, we designate the domain of a relation R as the set of all elements of the set A that are actually paired with (or mapped to) at least one element in B. The range of a relation R may be described as the set of all elements in the set B to which at least one element of A is mapped. These concepts are defined formally in the definition below.

Example 4.1.12 Consider the sets $R_1, R_2, \ldots, R_5$ as defined in Example 4.1.3. Then

1. $\text{Dom}(R_1) = A$ and $\text{Ran}(R_1) = \{2, 3\}$.
2. $\text{Dom}(R_2) = \{a, b\}$ and $\text{Ran}(R_2) = B$.
3. $\text{Dom}(R_3) = \{a, b, c\}$ and $\text{Ran}(R_3) = B$.

4. $\text{Dom}(R_4) = A$ and $\text{Ran}(R_4) = A$.
5. $\text{Dom}(R_5) = \{c, d\}$ and $\text{Ran}(R_5) = \{a, d\}$.

□

Example 4.1.13 Consider the equation $x^2 + y^2 = 1$ defined on $\mathbb{R}$. Let

$$R = \{(x, y) \in \mathbb{R} \times \mathbb{R}\} \mid x^2 + y^2 = 1\}.$$

Then $\text{Dom}(R) = \{x \mid -1 \leq x \leq 1\}$ and $\text{Ran}(R) = \{y \mid -1 \leq y \leq 1\}$ since substituting numbers whose squares are greater than 1 for either variable yields an equation with only complex solutions. □

We will investigate the concepts of domain and range in more detail in the study of functions. However, the reader may suspect that although these sets are sometimes easily found, often they will require some insight and work to determine!

Earlier we considered the relation "≤." If we were to consider the associated pairs in reverse order, we might describe this new list of ordered pairs by the relation "≥." Thus we see that relations are in some sense reversible, and we formalize this concept in the definition that follows.

Definition 4.1.14 If R is a relation from A to B, then the **inverse relation** of R, denoted by R^{-1}, is defined by

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}.$$

◊

Thus, R^{-1} is a new relation from B to A and consists of ordered pairs from R with the components reversed. Hence, the inverse relation of $R = \{(2, 3), (4, 7), (2, 9), (6, 9)\}$ is the relation $R^{-1} = \{(3, 2), (7, 4), (9, 2), (9, 6)\}$.

Consider the relation in Figure 4.1.15. The inverse relation R^{-1} from B to A can be found by simply reversing the arrows (Figure 4.1.16). In this case, $\text{Dom}(R) = \text{Ran}(R^{-1}$ and $\text{Ran}(R) = \text{Dom}(R^{-1})$.

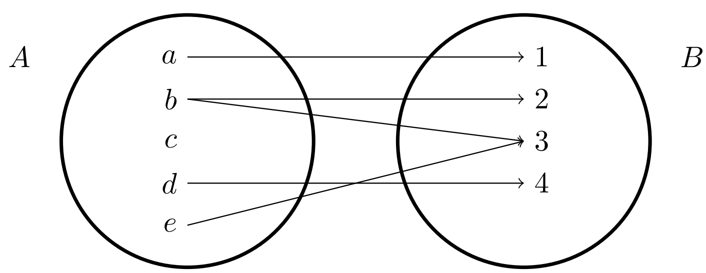


Figure 4.1.15 The relation R from A to B

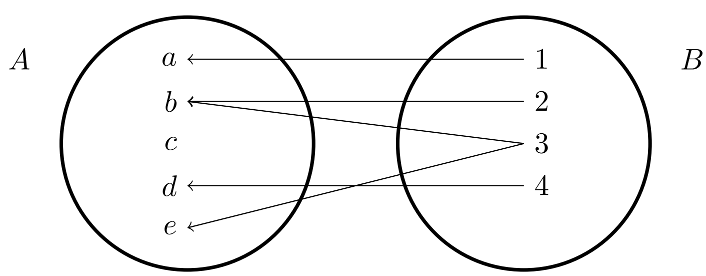


Figure 4.1.16 The relation R^{-1} from B to A

4.2 Equivalence Relations

One particular kind of relation that plays a vital role in mathematics is an equivalence relation. Before defining an equivalence relation, we will consider definitions and examples of each of the properties involved.

Definition 4.2.1 A relation R is **reflexive** if $(a, a) \in R$ for every $a \in A$. That is for each $a \in A$, We have aRa. $\Diamond$

It is important to realize that this definition involves a quantified expression, "for each $a \in A$." Recall from logic that when such an expression is negated, the quantifier changes. Hence, it follows that a relation is not reflexive if there exists even one element in A that is not related to itself.

Example 4.2.2 The relation "$\leq$" on $\mathbb{Z}$ has the reflexive property since every integer is less than or equal to itself. $\Box$

Example 4.2.3 The relation "$=$" on $\mathbb{R}$ is reflexive since every real number is equal to itself. $\Box$

Example 4.2.4 The relation $R = \{(2,3),(2,2),(3,2),(3,3)\}$ is not a reflexive relation on the set $A = \{1,2,3\}$ since $1 \in A$, but $(1,1) \notin R$. But R is reflexive when considered as a relation on the set $B = \{2,3\}$. $\Box$

Example 4.2.5 Let S be nonempty and $\mathcal{P}(S)$ be the power set of S. Then the subset relation is reflexive on $\mathcal{P}(S)$ since every set is a subset of itself. $\Box$

Definition 4.2.6 A relation R on A is **symmetric** if whenever $(a, b) \in R$, then $(b, a) \in R$. Alternatively, if aRb, then bRa. $\Diamond$

You should notice a major distinction in the nature of the definitions of these terms. The definition of reflexive is universal in that it must be true for all members of the set upon which it is defined. In contrast, the definition for the symmetric property is stated in the form of a conditional. (Remember from formal logic that a conditional, $p \to q$, is false only when p is true and q is false.) So to show a relation is not symmetric we must be able to find an ordered pair (a, b) in R such that (b, a) is not in R.

Example 4.2.7 Let $A = \{1,2,3,4\}$ and consider the given relations on A. The relations $R = \{(1,2),(2,1),(3,4),(4,3)\}$ and $S = \{(1,1)\}$ have the symmetric property. However, $T = \{(3,3).(2,4),(4,2),(1,2)\}$ is not symmetric since $(1,2) \in T$ but $(2,1) \notin T$. $\Box$

It is important to remember that to show a relation does *not* have a certain property, we need only provide a single counterexample.

Example 4.2.8 The relation "$\geq$" is not symmetric on $\mathbb{R}$ since $5 \geq 2$ but $2 \not\geq 5$. $\Box$

Example 4.2.9 Let A be the set of rectangles in the Cartesian plane, and let elements of A be related if they have the same area. Then this relation is symmetric. $\Box$

Definition 4.2.10 A relation R on A is **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$. $\Diamond$

A relation R is not transitive if there exist a, b, and c in A such that $(a, b) \in R$ and $(b, c) \in R$ but $(a, c) \notin R$.

Example 4.2.11 The relation "$<$" is transitive on $\mathbb{R}$. $\Box$

Example 4.2.12 Let $R = \{(1,1),(2,2),(3,3)\}$ on $\mathbb{Z}$. Then R is transitive since there do not exist integers a, b, and c such that $(a, b) \in R$ and $(b, c) \in R$ but $(a, c) \notin R$. $\Box$

Example 4.2.13 Let $R = \{(1,2),(2,3)\}$ on $\mathbb{Z}$. Then R is not transitive since $(1,2) \in R$ and $(2,3) \in R$ but $(1,3) \notin R$. $\square$

Definition 4.2.14 A relation R on A which is reflexive, symmetric, and transitive is called an **equivalence relation** on A. If two elements a and b are equivelent, we write $a \sim b$, unless of course there is already a notation in place such as "=." $\Diamond$

Example 4.2.15 Let $A = \{1,2,3\}$ and $R = \{(1,1),(2,2)\}$. Then R is not an equivalence relation on A. The relation is both transitive and symmetric but is not reflexive since $(3,3) \notin R$. $\square$

Example 4.2.16 Let $A = \{1,2,3\}$ and

$$S = \{(1,1),(2,2),(3,3),(1,2),(2,1),(2,3),(3,2)\}.$$

The relation S is both reflexive and symmetric but is not transitive, since $(1,2) \in S$ and $(2,3) \in S$ but $(1,3) \notin S$. $\square$

Example 4.2.17 Let $A = \{a,b\}$ and $\mathcal{P}(A)$ be the power set of A. Then the subset relation is reflexive and transitive but is not symmetric since $\{a\} \subseteq \{a,b\}$ but $\{a,b\} \nsubseteq \{a\}$. $\square$

Example 4.2.18 Consider the set $\mathbb{Z}$ and define $a \sim b$ if 5 divides $a-b$, denoted by $5 \mid (a-b)$; i.e., there is no remainder when $a-b$ is divided by 5. Then $2 \sim 12$, since $5 \mid (2-12)$ and $3 \not\sim 7$, since $5 \not| (3-7)$. We have defined an eqiuivalence relation on $\mathbb{Z}$. The proof is left as an exercise ((((Unresolved xref, reference "relations-exercise-integers-mod5"; check spelling or use "provisional" attribute)))). $\square$

Example 4.2.19 Consider the set $\mathbb{Z}$, and let n be a fixed integer that is not equal to zero. define $a \sim b$ if $n \mid (a-b)$. The relation is a generalization of Example 4.2.18 and is also an equivalence relation. $\square$

Example 4.2.20 Some other equivalence relations are "is the same age as" on the set of all people, "has the same area as" on the set of all rectangles in the Cartesian plane, and "lives on the same street as" on the set of all people living in a given city. $\square$

Consider the relation "is the same age as" on the set of all students in a given class. This relation groups the people in the class according to age. Each person in the class is in some group, even if it is a single member group. In addition, no person is in more than one group and all people in a specific group are the same age. These qualities are common to all equivalence relations, leading us to the following formal definition.

Definition 4.2.21 Let $\sim$ be an equivalence relation on A. If $x \in A$, then the **equivalence class** of x, denoted by $\overline{x}$, is defined by $\overline{x} = \{y \in A \mid x \sim y\}$. $\Diamond$

Example 4.2.22 Suppose $A = \{6,7,8,9,10\}$ and let the relation R on A be defined by aRb if a and b have the same remainder when divided by 2. This relation is an equivalence relation since it is reflexive, symmetric, and transitive. (Verification is left as an exercise.) Then by Definition 4.2.21,

$$\overline{6} = \overline{8} = \overline{10} = \{6,8,10\}$$

and

$$\overline{7} = \overline{9} = \{7,9\}.$$

Furthermore, $\overline{6}$ and $\overline{7}$ are disjoint sets whose union is A. So A has just partitioned into disjoint pieces where each piece can have different names. $\square$

The observations for the specific relation considered in Example 4.2.22 lead us to generalize these concepts to any equivalence relation defined on an arbitrary set.

Theorem 4.2.23 *Let $\sim$ be an equivalence relation on A. Then:*

1. *Each equivalence class is non-empty.*
2. *Any two equivalence classes are either equal or disjoint*
3. *The set A is equal to the union of all the equivalence classes.*

When given an equivalence relation on a set, we may find the classes generated by that relation by first choosing elements at random from the set. For example, suppose

$$A = \left\{ \frac{2}{3}, -\frac{1}{2}, -1, 0, \frac{4}{6}, \frac{0}{3}, -\frac{4}{8}, \frac{10}{15} \right\}.$$

and let the equivalence relation on be "=." To find the equivalence classes determined by the relation, we may choose any element in A, say $4/6$. Then $4/6 \in \overline{4/6}$, since $4/6 = 4/6$. The other elements of $\overline{4/6}$ are $2/3$ and $10/15$, since they are the only elements of A equal to $4/6$. Thus, $\overline{4/6} = \{4/6, 2/3, 10/15\}$. Part (2) of Theorem 4.2.23 implies we might just as easily have chosen $2/3 >$ or $10/15$, and we would have arrived at the same equivalence class. That is, since $2/3 \in \overline{4/6}$ and $10/15 \in \overline{4/6}$, then $\overline{2/3} = \overline{4/6} = \overline{10/15}$. So we conclude that we may designate an equivalence class completely using any of its elements.

TAKS CONNECTION.

How might a student apply the concept of equivalence classes to answer the following question taken from the 2006 Texas Assessment of Knowledge and Skills (TAKS) Grade 5 Mathematics test?

Stan was putting fruit into baskets. He wanted each basket to be more than 7/10 full. Which fraction is more than 7/10?

Which one of the following numbers belongs in the region of the diagram marked by the question mark?

- A. 4/5
- B. 1/2
- C. 2/3
- D. 3/5

Example 4.2.24 Let A be the set of all ordered pairs of real numbers, and define $(a, b) \sim (c, d)$ if $a^2 + b^2 = c^2 + d^2$). Before proceeding further, you should find some ordered pairs that are related and then verify that this indeed defines an equivalence relation. Then for any $(x, y) \in \mathbb{R} \times \mathbb{R}$, we have

$$\overline{(x, y)} = \{(s, t) \mid x^2 + y^2 = s^2 + t^2\}.$$

These equivalence classes are represented geometrically by circles centered at the origin. □

Before leaving this section, we introduce a visual method for representing finite relations. For rather small finite relations, these visual representations, called **digraphs**, can be very helpful in conceptualizing a relation and its properties.

In general, consider a finite set A and a relation R defined on it. Digraphs are constructed by drawing a small dot representing each element of A and labeling that circle appropriately. These dots are called the **vertices** of the graph. At each dot, say x, draw a directed line segment from it to any other dot, labeled y, if and only if xRy. These directed line segments are called **edges**. Then notice that the dots represent A and the edges represent the ordered pairs in R.

Example 4.2.25 Consider the set $A = \{a, b, c, d\}$and the relation

$$R = \{(a, a), (c, c), (a, b), (b, a), (b, d), (c, d), (b, c)\}.$$

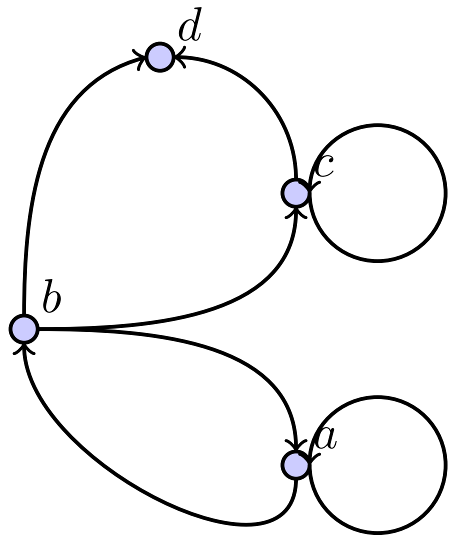


Figure 4.2.26 The digraph for the relation R on A

Notice that there is an edge representing every ordered pair in R (Figure 4.2.26). For those elements in A that are related to themselves, there is an edge that looks like a loop. In this relation there are only two loops since only a and c are related to themselves. From this example it is reasonable to conclude that for an arbitrary finite relation R defined on A, the relation will have the reflexive property if and only if each vertex has a loop. Thus, we can quickly see from the digraph that R is not reflexive. We may also conclude from the digraph that R is not symmetric and not transitive. Why? □

4.2.1 Exercises

1. Determine whether or not the following relations are reflexive, symmetric, or transitive. Which are equivalence relations on the given sets? Justify your thinking.

(a) $R = \{(1, 1), (3, 3), (5, 5)\}$ on $A = \{1, 3, 5\}$

(b) $R = \{(1, 1), (2, 2), (1, 2)\}$ on $A = \{1, 2\}$

(c) $R = \{(1, 1), (1, 2), (2, 1)\}$ on $A = \{1, 2\}$

(d) $R = \{(1, 3), (2, 3), (3, 2), (3, 1)\}$ on $A = \{1, 2, 3\}$

(e) $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 3), (2, 4)\}$ on $A = \{1, 2, 3, 4\}$

(f) $R = \{(3,4)\}$ on $A = \{3,4\}$

(g) $R = \{(3,3)\}$ on $A = \{3,4\}$

(h) $R = \{(1,1),(2,2),(3,3)\}$ on $A = \{1,2,3\}$

(i) $R = \{(1,1),(2,2),(3,3)\}$ on $A = \{1,2,3,4\}$

(j) $R = \{(1,3),(3,1),(1,1),(3,3)\}$ on $A = \{1,3\}$

(k) $R = \{(1,3),(3,1),(1,1),(3,3)\}$ on $A = \{1,2,3\}$

2. Prove the relation described in Example 4.2.18 is an equivalence relation.

3. Prove the relation described in Example 4.2.19 is an equivalence relation.

4. Prove the relation described in Example 4.2.22 is an equivalence relation.

5. Let $A = \{1,2,3,4\}$. For each of the parts below, find an example of a relation on the set that meets the conditions described.

(a) R is reflexive and symmetric but not transitive.

(b) R is reflexive and transitive but not symmetric.

(c) R is symmetric and transitive but not reflexive.

(d) R is reflexive but neither symmetric nor transitive.

6. Define $\sim$ on $\mathbb{R}$ by $A \sim b$ if and only if $|a| = |b|$. Prove $\sim$ is an equivalence relation on $\mathbb{R}$. For an arbitrary $t \in \mathbb{R}$, find $\bar{t}$. In

Exercise 4.2.1.7–4.2.1.13, a relation R is defined on a given set. In each case, prove or disprove: (a) R is reflexive. (b) R is symmetric, (c) R is transitive. In each problem where R is an equivalence relation, find $\overline{a}$, where a is any element in the set on which the relation is defined.

7. Define R on $\mathbb{N}$ by aRb if and only if $a = 10^k b$ for some $k \in \mathbb{Z}$.

8. Define R on $\mathbb{R}$ by xRy if and only if $x - y \in \mathbb{Z}$.

9. Define R on $\mathbb{N}$ by xRy if and only if $2 \mid (x+y)$.

10. Define R on $\mathbb{N}$ by xRy if and only if $3 \mid (x+y)$.

11. Define R on $\mathbb{R} \times \mathbb{R}$ by $(a,b)R(c,d)$ if and only if $a - c \in \mathbb{Z}$.

12. Define R on $\mathbb{R} \times \mathbb{R}$ by $(a,b)R(c,d)$ if and only if $a - c \in \mathbb{Z}$ and $b - d \in \mathbb{Z}$.

13. Define R on $\mathbb{Z} \times \mathbb{Z}$ by $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid |a-b| < 5\}$.

14. Let R_1 and R_2 be relations on A.

(a) If R_1 and R_2 are both reflexive, if $R_1 \cap R_2$reflexive? What about $R_1 \cup R_2$? Justify you answers.

(b) If R_1 and R_2 are both symmetric, if $R_1 \cap R_2$reflexive? What about $R_1 \cup R_2$? Justify you answers.

(c) If R_1 and R_2 are both transitive, if $R_1 \cap R_2$reflexive? What about $R_1 \cup R_2$? Justify you answers.

15. Let R for a relation on a finite nonempty set A. What can be said about the digraph of R if the relation is

(a) reflexive?

(b) not reflexive?

(c) symmetric?

(d) not symmetric?

(e) transitive?

(f) not transitive?

Jusitify your claim for each part.

16. Let $A = \{1, 2, 3, 4, 5\}$ and $R = \{(2, 3), (2, 4), (3, 5), (2, 5), (5, 5)\}$.

(a) Draw a digraph of this relation.

(b) Determine the properties of R, explaining in each case how you can tell from your digraph.

17. Draw a digraph of the relation $<$ on the set $A = \{1, 2, 3, 4\}$

18. Draw a digraph of the relation $\leq$ on the set $A = \{1, 2, 3, 4\}$

19. Draw a digraph of $\mathcal{P}(S)$ under the relation $\subseteq$, where $S = \{a, b\}$

4.3 Functions and Cardinality

Another special type of relation is a function.

Definition 4.3.1 A **function** from a set A to a set B is a relation from A to B, where each element of A is paired with exactly one element of B. In other words, each input value results in exactly one output value. ♢

Most of the mathematics that you have learned or will teach is based around the idea of functions. When students are asked to find a rule that defines a pattern, students are being asked to define a function. When you examine a sequence of values, you are examining a function. When you go to the Coke machine to get a soda, you are employing a function. (The input is your money. The output is the soda.) The dosage of medicine given to you when you are sick is a result of a function. The decision making process is an illustration of a function. Your daily life is a function whose domain is time and whose range is the activity you are doing at that time. They are everywhere!

You have studied functions in lots of places. Perhaps you looked at several definitions, graphical representations, the function notation, characteristics, etc. We will be looking specifically at two characteristics of functions and their applications.

Definition 4.3.2 A function f from a set A to a set B is called **one-to-one** provided that each output results from exactly one input. That is, if $b \in \text{Ran}(f)$ with $f(a_1) = f(a_2) = b$, then $a_1 = a_2$.

A function f from a set A to a set B is called **onto** provided that every element of B is an element of $\text{Ran}(f)$. That is, for every $b \in B$, there exists $A \in A$ such that $f(a) = b$.

A function from a set A to a set B that is both one-to-one and onto is called a **one-to-one correspondence** or **bijection**. ♢

You are probably wondering what you can possibly learn about functions that you have not already seen (maybe more than once!). We are going to use the definitions of one-to-one and onto to study sets. Primarily, we are going to study the cardinality of sets.

Definition 4.3.3 The **cardinality** of a set A is the number of elments in the set, denoted $|A|$. ♢

At first this may not seem to difficult. You simply need to count the elements in the set. However, what if your sets are infinite? Again you might be asking why this is a big deal. The answer of how many elements is in an infinite set is infinitely many, right? Would you believe that there are different sizes of infinity? This is the foundation of cardinality and the study of mathematician Georg Cantor (see Subsection 3.1.1).

Definition 4.3.4 Two sets, A and B have the **same cardinality** if there is a one-to-one correspondence f from A to B.

A set A is finite with cardinality n provided that there is a one-to-one correspondence f from A to the set $\{1, 2, 3, 4, ..., n\}$.

The set of natural numbers is an infinite set with cardinality $\aleph_0$ (aleph naught), the smallest of all infinities. We say that the set of natural numbers are **countably infinite**. ♢

We are not going to spend a great deal of time discussing the sizes of infinity by name, but we are going to discuss the most common number sets to see whether they have the same cardinality as the natural numbers. Let's start with the set of whole numbers.

Theorem 4.3.5 *The set of whole numbers has the same cardinality as the natural numbers.*

At first glance, you might be inclined to say that the set of whole numbers has one more element than the set of natural numbers and thus, it is impossible for them to be of the same "size." Remember though that we are examining a different idea of "size". To show that the set of whole numbers has the same cardinality as the natural numbers, we simply have to demonstrate that there is a one-to-one correspondence between the two sets.

Proof. Consider the function f, mapping the set of whole numbers to the set of natural numbers, defined by $f(w) = w + 1$. Notice that this function maps 0 to 1, 1 to 2, 2 to 3 and so on. Because the function is linear, it is obviously one-to-one. Moreover, it is onto because if n is a natural number, then

$$f(n - 1) = (n - 1) + 1 = n.$$

(Note that since the natural numbers has a smallest element of 1, the smallest value of$n - 1$ is 0 which is the smallest whole number.)

Therefore, since f is a one-to-one correspondence, the set of whole numbers has the same cardinality as the set of natural numbers. Thus the set of whole numbers is also countably infinite. ■

Theorem 4.3.6 *The set of integers is countably infinite. That is, the set of integers has the same cardinality as the set of natural numbers.*

You may have a bit more difficulty buying into this idea. After all, the set of natural numbers is a proper subset of the integers! How can this set possibly be the same "size" as the natural numbers? Remember, cardinality is a different way to determine "size." The infinite sets that we are examining can not be counted in the ordinary way. Cardinality provides a tool that we can use to categorize the "size" of infinite sets.

After you get past the initial thoughts of denial, we can begin to think about how to develop the ont-to-one correspondence necessary to show that our claim is true. We know that an argument similar to the one we created for the set of whole numbers will not work because we wwould not account for any of the negative numbers. So what if we did a back and forth trick between the positive and negative integers. We know that we have even and odd natural numbers. What if we used the even to cover the positive numbers and the odds to cover the negative numbers? For example, we can send 1 to 0, 2 to 1, 3 to -1, 4 to 2, 5 to -2, and so on.

Proof. Consider the function f, mapping the natural numbers to the integers, defined by the following criteria.

- If $n = 1$, then $f(n) = 0$.
- If n is an even integer, then $f(n) = n/2$.
- If n is an odd integer and $n \neq 1$, then $f(n) = -(n-1)/2$.

Note that this function is one-to-one. We can examine the graph to verify, if necessary. Also the function is onto. To see this, let x be any integer. If x is 0, then we know $f(1) = 0$. If x is positive, then $f(2x) = 2x/2 = x$. Notice that $2x$ is an even natural number. If x is negative, then

$$f(-2x+1) = -((-2x+1)-1)/2 = -(-2x)/2 = x.$$

Notice $-2x+1$ is an odd natural number. Thus in all three cases, x is mapped to by some natural number and f is onto. Therefore, f is a one-to-one correspondence and the set of integers have the same cardinality as the set of natural numbers, and is thus a countably infinite set. ■

Theorem 4.3.7 *The set of rational numbers is countably infinite. That is, the set of rational numbers has the same cardinality as the set of natural numbers.*

This set is a bit harder to work with than the previous ones because the process of listing the rational numbers is difficult. We will eliminate some of the difficulty by working only with positive rational numbers. You should be able to explain how to adapt the solution to the complete set once you see the pattern.

Consider Figure 4.3.8. Notice that eventually, if the process was allowed to continue indefinitely, all rational numbers would be listed. Some numbers however are represented more than once. In order to preserve the one-to-one requirement, we need to eliminate any numbers that are equivalent to a rational number previously listed. The image below has made that adjustment.

$$\begin{array}{ccccccc}
\frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \cdots \\
\frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \frac{2}{6} & \cdots \\
\frac{3}{1} & \frac{3}{2} & \frac{3}{3} & \frac{3}{4} & \frac{3}{5} & \frac{3}{6} & \cdots \\
\frac{4}{1} & \frac{4}{2} & \frac{4}{3} & \frac{4}{4} & \frac{4}{5} & \frac{4}{6} & \cdots \\
\frac{5}{1} & \frac{5}{2} & \frac{5}{3} & \frac{5}{4} & \frac{5}{5} & \frac{5}{6} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

Figure 4.3.8 Listing the rational numbers

Now we are going to develop our map. Unlike previous examples, we are not going to state our rule but we are going to let a picture do the talking. Remember that all we have to do is to demonstrate a one-to-one onto function.

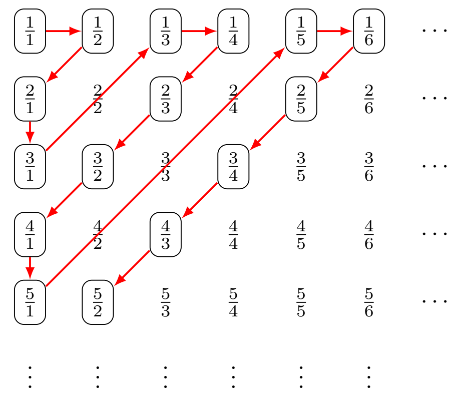


Figure 4.3.9 Listing the rational numbers without repetition.

So 1 will map to 1, 2 to 1/2, 3 to 2/1, 4 to 3/1, 5 to 1/3, etc. Notice that each rational number will eventually be the output for our function and will be the output for exactly one natural number. Thus, we have created a one-to-one correspondence between the natural numbers and the positive rational numbers. We can easily extend this idea by sending the even natural numbers to the positive rational numbers and the odd natural numbers to the negative rational numbers to show that there is a one-to-one correspondence from the natural numbers to the set of all rational numbers. Therefore, the set of rational numbers is countably infinite.

Theorem 4.3.10 *The set of real numbers is not countably infinite. That is, the set of real numbers does not have the same cardinality as the set of natural numbers.*

The real numbers will provide an example of a set that is "larger" than the set of natural numbers, whole numbers, integers, and rational numbers. To demonstrate, we will actually show that even the interval (0, 1) is not countable infinite. In other words, the set of numbers greater than zero and less than one cannot be put into a one-to-one correspondence with the set of natural numbers. To show that this is true, we will use a proof by contradiction.

We have to clear up a couple points before we begin. Frist, you whould realize that every number in the interval $(0, 1)$ can be written as an infinite decimal. For example,

$$0.25 = 0.250000000000000000\ldots$$

Also recall from our discussions with geometric sequences and series, we discussed that $0.99999\ldots = 1$. You can prove this using the fact that $0.9999\ldots$ is a geometric series with $r = 1/10$ and $a = 9/10$. Since $r < 1$, the infinite sum of the series is $S = 1/(1 - r)$. With this in mind, anytime that we have this situation occur (a infinite number of repeating 9's), we are going to assume that we will equate this number with its equivalency in terms of repeated zeros. For example,

$$0.555999999999\ldots = 0.556000000000\ldots.$$

This will ensure that our function is one-to-one.

Proof. Consider the interval $(0, 1)$ and assume to the contrary that this set of numbers in countable infinite. Since the set is countable infinite, every number in the set can be listed in a one-to-one correspondence with the natural numbers. So we can say that there is a first element which maps to 1, a second element which maps to 2, so on and so forth. In order to list these values in an ordered way, let's call the first number a_1 and denote it as

$$a_1 = 0.d_{11}d_{12}d_{13}d_{14}d_{15}d_{16}d_{17}d_{18}d_{19}\ldots,$$

where d_{11} is the digit in the first number in our list and in the first position beyond the decimal, d_{12} is the digit in the first number in the list and in the second position beyond the decimal, etc.

Then the second number in the list would look like

$$a_2 = 0.d_{21}d_{22}d_{23}d_{24}d_{25}d_{26}d_{27}d_{28}d_{29}\dots,$$

where d_{21} is the digit in the second number in our list and in the first position beyond the decimal, d_{22} is the digit in the second number in the list and in the second position beyond the decimal, etc.

In general then, the ith number in the list would look like

$$a_i = 0.d_{i1}d_{i2}d_{i3}d_{i4}d_{i5}d_{i6}d_{i7}d_{i8}d_{i9}\dots,$$

where d_{i1} is the digit in the ith number in our list and in the first position beyond the decimal, d_{i2} is the digit in the ith number in the list and in the second position beyond the decimal, etc.

We now have the following list of all numbers that are in the interval $(0, 1)$,

$$\begin{aligned}
a_1 &= 0.d_{11}d_{12}d_{13}d_{14}d_{15}d_{16}d_{17}d_{18}d_{19}\dots,\\
a_2 &= 0.d_{21}d_{22}d_{23}d_{24}d_{25}d_{26}d_{27}d_{28}d_{29}\dots,\\
a_3 &= 0.d_{31}d_{32}d_{33}d_{34}d_{35}d_{36}d_{37}d_{38}d_{39}\dots,\\
a_4 &= 0.d_{41}d_{42}d_{43}d_{44}d_{45}d_{46}d_{47}d_{48}d_{49}\dots,\\
a_5 &= 0.d_{51}d_{52}d_{53}d_{54}d_{55}d_{56}d_{57}d_{58}d_{59}\dots,\\
&\dots\\
a_i &= 0.d_{i1}d_{i2}d_{i3}d_{i4}d_{i5}d_{i6}d_{i7}d_{i8}d_{i9}\dots
\end{aligned}$$

The key here is the realization that based on our assumption, every single number in the interval $(0, 1)$ is represented somewhere in this list. This is where we will obtain our contradiction.

Consider the number

$$d = 0.d_1d_2d_3d_4d_5d_6d_7d_8d_9\dots,$$

where d_j is the jth digit beyond the decimal and is determined based on the following criteria:

If $d_{jj} \neq 5$, then $d_j = 5$; otherwise, $d_j = 2$.

Notice that this means that by definition of the number d, $d_1 \neq d_{11}$ and so the number d is not the number a_1. Similarly $d \neq a_2$ because $d_2 \neq d_{22}$. Continuing this line of thought, d is not the same as any number in this list because $d_j \neq d_{jj}$ for any natural number j. Thus is a number between 0 and 1 that is not in our list. This contradicts our assumption that there exists a one-to-one correspondence between the set of numbers greater than 0 and less than 1 and the set of natural numbers. Therefore the set of numbers in the interval $(0, 1)$ is not countably infinite ■

We say then that the set of numbers in the interval $(0, 1)$ is **uncountable** and thus, so is the set of real numbers.

4.3.1 Exercises

1. Show that the set of even numbers is countably infinite.

Chapter 5

Integers and the Division Algorithm

The integers are the building blocks of mathematics. In this chapter we will investigate the fundamental properties of the integers, including mathematical induction, the division algorithm, and the Fundamental Theorem of Arithmetic.

5.1 Mathematical Induction

Suppose we wish to show that

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

for any natural number n. This formula is easily verified for small numbers such as $n = 1$, 2, 3, or 4, but it is impossible to verify for all natural numbers on a case-by-case basis. To prove the formula true in general, a more generic method is required.

Suppose we have verified the equation for the first n cases. We will attempt to show that we can generate the formula for the $(n+1)$th case from this knowledge. The formula is true for $n = 1$ since

$$1 = \frac{1(1+1)}{2}.$$

If we have verified the first n cases, then

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n^2 + 3n + 2}{2} \\ &= \frac{(n+1)[(n+1)+1]}{2}. \end{aligned}$$

This is exactly the formula for the $(n+1)$th case.

This method of proof is known as **mathematical induction**. Instead of attempting to verify a statement about some subset S of the positive integers $\mathbb{N}$ on a case-by-case basis, an impossible task if S is an infinite set, we give a specific proof for the smallest integer being considered, followed by a generic argument showing that if the statement holds for a given case, then it must also hold for the next case in the sequence. We summarize mathematical induction in the following axiom.

Principle 5.1.1 First Principle of Mathematical Induction. *Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer n_0. If for all integers k with $k \geq n_0$, $S(k)$ implies that $S(k+1)$is true, then $S(n)$ is true for all integers n greater than or equal to n_0.*

Example 5.1.2 For all integers $n \geq 3$, $2^n > n + 4$. Since

$$8 = 2^3 > 3 + 4 = 7,$$

the statement is true for $n_0 = 3$. Assume that $2^k > k + 4$ for $k \geq 3$. Then $2^{k+1} = 2 \cdot 2^k > 2(k + 4)$. But

$$2(k + 4) = 2k + 8 > k + 5 = (k + 1) + 4$$

since k is positive. Hence, by induction, the statement holds for all integers $n \geq 3$. □

Example 5.1.3 Every integer $10^{n+1} + 3 \cdot 10^n + 5$ is divisible by 9 for $n \in \mathbb{N}$. For $n = 1$,

$$10^{1+1} + 3 \cdot 10 + 5 = 135 = 9 \cdot 15$$

is divisible by 9. Suppose that $10^{k+1} + 3 \cdot 10^k + 5$ is divisible by 9 for $k \geq 1$. Then

$$\begin{aligned} 10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5 &= 10^{k+2} + 3 \cdot 10^{k+1} + 50 - 45 \\ &= 10(10^{k+1} + 3 \cdot 10^k + 5) - 45 \end{aligned}$$

is divisible by 9. □

A nonempty subset S of $\mathbb{Z}$ is **well-ordered** if S contains a least element. Notice that the set $\mathbb{Z}$ is not well-ordered since it does not contain a smallest element. However, the natural numbers are well-ordered.

Principle 5.1.4 Principle of Well-Ordering. *Every nonempty subset of the natural numbers is well-ordered.*

The Principle of Well-Ordering is equivalent to the Principle of Mathematical Induction.

Theorem 5.1.5 *The Principle of Mathematical Induction implies the Principle of Well-Ordering. That is, every nonempty subset of $\mathbb{N}$ contains a least element.*

You can find the proof of Theorem 5.1.5 in Subsection A.0.2Induction can also be very useful in formulating definitions. For instance, there are two ways to define $n!$, the factorial of a positive integer n.

- The *explicit* definition: $n! = 1 \cdot 2 \cdot 3 \cdots (n - 1) \cdot n$.
- The *inductive* or *recursive* definition: $1! = 1$ and $n! = n(n-1)!$ for $n > 1$.

Every good mathematician or computer scientist knows that looking at problems recursively, as opposed to explicitly, often results in better understanding of complex issues.

5.1.1 Exercises

1. Prove that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

for $n \in \mathbb{N}$.

2. Prove that

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

for $n \in \mathbb{N}$.

3. Prove that $n! > 2^n$ for $n \geq 4$.

4. Prove that

$$x + 4x + 7x + \cdots + (3n-2)x = \frac{n(3n-1)x}{2}$$

for $n \in \mathbb{N}$.

5. Prove that $10^{n+1} + 10^n + 1$ is divisible by 3 for $n \in \mathbb{N}$.

6. Prove that $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5$ is divisible by 99 for $n \in \mathbb{N}$.

7. Use induction to prove that $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$ for $n \in \mathbb{N}$.

8. Prove that

$$\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

for $n \in \mathbb{N}$.

9. If x is a nonnegative real number, then show that $(1+x)^n - 1 \geq nx$ for $n = 0, 1, 2, \ldots$.

10. **Power Sets.** Let X be a set. Define the **power set** of X, denoted $\mathcal{P}(X)$, to be the set of all subsets of X. For example,

$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

For every positive integer n, show that a set with exactly n elements has a power set with exactly 2^n elements.

5.2 The Division Algorithm

An application of the Principle of Well-Ordering that we will use often is the division algorithm.

Theorem 5.2.1 Division Algorithm. *Let a and b be integers, with $b > 0$. Then there exist unique integers q and r such that*

$$a = bq + r$$

where $0 \leq r < b$.

Proof. This is a perfect example of the existence-and-uniqueness type of proof. We must first prove that the numbers q and r actually exist. Then we must show that if q' and r' are two other such numbers, then $q = q'$ and $r = r'$.

Existence of q and r. Let

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

If $0 \in S$, then b divides a, and we can let $q = a/b$ and $r = 0$. If $0 \notin S$, we can use the Well-Ordering Principle. We must first show that S is nonempty. If $a > 0$, then $a - b \cdot 0 \in S$. If $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$. In either case $S \neq \emptyset$. By the Well-Ordering Principle, S must have a smallest member, say $r = a - bq$. Therefore, $a = bq + r$, $r \geq 0$. We now show that $r < b$. Suppose that $r > b$. Then

$$a - b(q + 1) = a - bq - b = r - b > 0.$$

In this case we would have $a - b(q+1)$ in the set S. But then $a - b(q+1) < a - bq$, which would contradict the fact that $r = a - bq$ is the smallest member of S. So $r \leq b$. Since $0 \notin S$, $r \neq b$ and so $r < b$.

Uniqueness of q and r. Suppose there exist integers r, r', q, and q' such that

$$a = bq + r, 0 \leq r < b \quad \text{and} \quad a = bq' + r', 0 \leq r' < b.$$

Then $bq + r = bq' + r'$. Assume that $r' \geq r$. From the last equation we have $b(q - q') = r' - r$; therefore, b must divide $r' - r$ and $0 \leq r' - r \leq r' < b$. This is possible only if $r' - r = 0$. Hence, $r = r'$ and $q = q'$. ∎

Let a and b be integers. If $b = ak$ for some integer k, we write $a \mid b$. An integer d is called a **common divisor** of a and b if $d \mid a$ and $d \mid b$. The **greatest common divisor** of integers a and b is a positive integer d such that d is a common divisor of a and b and if d' is any other common divisor of a and b, then $d' \mid d$. We write $d = \gcd(a, b)$; for example, $\gcd(24, 36) = 12$ and $\gcd(120, 102) = 6$. We say that two integers a and b are **relatively prime** if $\gcd(a, b) = 1$.

Theorem 5.2.2 *Let a and b be nonzero integers. Then there exist integers r and s such that*

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Proof. Let

$$S = \{am + bn : m, n \in \mathbb{Z} \text{ and } am + bn > 0\}.$$

Clearly, the set S is nonempty; hence, by the Well-Ordering Principle S must have a smallest member, say $d = ar + bs$. We claim that $d = \gcd(a, b)$. Write $a = dq + r'$ where $0 \leq r' < d$. If $r' > 0$, then

$$\begin{aligned} r' &= a - dq \\ &= a - (ar + bs)q \\ &= a - arq - bsq \\ &= a(1 - rq) + b(-sq), \end{aligned}$$

which is in S. But this would contradict the fact that d is the smallest member of S. Hence, $r' = 0$ and d divides a. A similar argument shows that d divides b. Therefore, d is a common divisor of a and b.

Suppose that d' is another common divisor of a and b, and we want to show that $d' \mid d$. If we let $a = d'h$ and $b = d'k$, then

$$d = ar + bs = d'hr + d'ks = d'(hr + ks).$$

So d' must divide d. Hence, d must be the unique greatest common divisor of a and b. ∎

Corollary 5.2.3 *Let a and b be two integers that are relatively prime. Then there exist integers r and s such that $ar + bs = 1$.*

Among other things, Theorem 5.2.2 allows us to compute the greatest common divisor of two integers.

Example 5.2.4 Let us compute the greatest common divisor of 945 and 2415. First observe that

$$\begin{aligned} 2415 &= 945 \cdot 2 + 525 \\ 945 &= 525 \cdot 1 + 420 \\ 525 &= 420 \cdot 1 + 105 \\ 420 &= 105 \cdot 4 + 0. \end{aligned}$$

Reversing our steps, 105 divides 420, 105 divides 525, 105 divides 945, and 105 divides 2415. Hence, 105 divides both 945 and 2415. If d were another common divisor of 945 and 2415, then d would also have to divide 105. Therefore, $\gcd(945, 2415) = 105$.

If we work backward through the above sequence of equations, we can also obtain numbers r and s such that $945r + 2415s = 105$. Observe that

$$\begin{aligned} 105 &= 525 + (-1) \cdot 420 \\ &= 525 + (-1) \cdot [945 + (-1) \cdot 525] \\ &= 2 \cdot 525 + (-1) \cdot 945 \\ &= 2 \cdot [2415 + (-2) \cdot 945] + (-1) \cdot 945 \\ &= 2 \cdot 2415 + (-5) \cdot 945. \end{aligned}$$

So $r = -5$ and $s = 2$. Notice that r and s are not unique, since $r = 41$ and $s = -16$ would also work. □

To compute $\gcd(a, b) = d$, we are using repeated divisions to obtain a decreasing sequence of positive integers $r_1 > r_2 > \cdots > r_n = d$; that is,

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

To find r and s such that $ar + bs = d$, we begin with this last equation and substitute results obtained from the previous equations:

$$\begin{aligned} d &= r_n \\ &= r_{n-2} - r_{n-1} q_n \\ &= r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) \\ &= -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} \\ &\vdots \\ &= ra + sb. \end{aligned}$$

The algorithm that we have just used to find the greatest common divisor d of two integers a and b and to write d as the linear combination of a and b is known as the **Euclidean algorithm**.

5.2.1 Exercises

1. For each of the following pairs of numbers a and b, calculate $\gcd(a, b)$ and find integers r and s such that $\gcd(a, b) = ra + sb$.

(a) 14 and 39

(b) 234 and 165

(c) 1739 and 9923

(d) 471 and 562

(e) 23771 and 19945

(f) −4357 and 3754

2. Let a and b be nonzero integers. If there exist integers r and s such that $ar + bs = 1$, show that a and b are relatively prime.

3. Let a and b be integers such that $\gcd(a, b) = 1$. Let r and s be integers such that $ar + bs = 1$. Prove that

$$\gcd(a, s) = \gcd(r, b) = \gcd(r, s) = 1.$$

4. Let $x, y \in \mathbb{N}$ be relatively prime. If xy is a perfect square, prove that x and y must both be perfect squares.

5. Using the division algorithm, show that every perfect square is of the form $4k$ or $4k + 1$ for some nonnegative integer k.

6. Suppose that a, b, r, s are pairwise relatively prime and that

$$a^2 + b^2 = r^2$$
$$a^2 - b^2 = s^2.$$

Prove that a, r, and s are odd and b is even.

7. Let $n \in \mathbb{N}$. Use the division algorithm to prove that every integer is congruent mod n to precisely one of the integers $0, 1, \ldots, n-1$. Conclude that if r is an integer, then there is exactly one s in $\mathbb{Z}$ such that $0 \leq s < n$ and $[r] = [s]$. Hence, the integers are indeed partitioned by congruence mod n.

8. Define the **least common multiple** of two nonzero integers a and b, denoted by $\operatorname{lcm}(a, b)$, to be the nonnegative integer m such that both a and b divide m, and if a and b divide any other integer n, then m also divides n. Prove there exists a unique least common multiple for any two integers a and b.

9. If $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$, prove that $dm = |ab|$.

10. Show that $\operatorname{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.

11. Prove that $\gcd(a, c) = \gcd(b, c) = 1$ if and only if $\gcd(ab, c) = 1$ for integers a, b, and c.

12. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

13. **Fibonacci Numbers.** The Fibonacci numbers are

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

We can define them inductively by $f_1 = 1$, $f_2 = 1$, and $f_{n+2} = f_{n+1} + f_n$ for $n \in \mathbb{N}$.

(a) Prove that $f_n < 2^n$.

(b) Prove that $f_{n+1}f_{n-1} = f_n^2 + (-1)^n$, $n \geq 2$.

(c) Prove that $f_n = [(1 + \sqrt{5}\,)^n - (1 - \sqrt{5}\,)^n]/2^n\sqrt{5}$.

(d) Show that $\lim_{n\to\infty} f_n/f_{n+1} = (\sqrt{5} - 1)/2$.

(e) Prove that f_n and f_{n+1} are relatively prime.

5.3 Prime Numbers

Let p be an integer such that $p > 1$. We say that p is a **prime number**, or simply p is **prime**, if the only positive numbers that divide p are 1 and p itself. An integer $n > 1$ that is not prime is said to be **composite**.

Lemma 5.3.1 Euclid. *Let a and b be integers and p be a prime number. If $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Proof. Suppose that p does not divide a. We must show that $p \mid b$. Since $\gcd(a, p) = 1$, there exist integers r and s such that $ar + ps = 1$. So

$$b = b(ar + ps) = (ab)r + p(bs).$$

Since p divides both ab and itself, p must divide $b = (ab)r + p(bs)$. ■

Theorem 5.3.2 Euclid. *There exist an infinite number of primes.*

Proof. We will prove this theorem by contradiction. Suppose that there are only a finite number of primes, say $p_1, p_2, \ldots, p_n$. Let $P = p_1 p_2 \cdots p_n + 1$. Then P must be divisible by some p_i for $1 \leq i \leq n$. In this case, p_i must divide $P - p_1 p_2 \cdots p_n = 1$, which is a contradiction. Hence, either P is prime or there exists an additional prime number $p \neq p_i$ that divides P. ■

Theorem 5.3.3 Fundamental Theorem of Arithmetic. *Let n be an integer such that $n > 1$. Then*

$$n = p_1 p_2 \cdots p_k,$$

where $p_1, \ldots, p_k$ are primes (not necessarily distinct). Furthermore, this factorization is unique; that is, if

$$n = q_1 q_2 \cdots q_l,$$

then $k = l$ and the q_i's are just the p_i's rearranged.

The proof of Theorem 5.3.3 can be found in Subsection A.0.3

5.3.1 Exercises

1. Let $p \geq 2$. Prove that if $2^p - 1$ is prime, then p must also be prime.

2. Prove that there are an infinite number of primes of the form $6n + 5$.

3. Prove that there are an infinite number of primes of the form $4n - 1$.

4. Using the fact that 2 is prime, show that there do not exist integers p and q such that $p^2 = 2q^2$. Demonstrate that therefore $\sqrt{2}$ cannot be a rational number.

Appendix A

More on the Integers

A.0.1 Strong Induction

We have an equivalent statement of the Principle of Mathematical Induction that is often very useful.

Principle A.0.1 Second Principle of Mathematical Induction. *Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer n_0. If $S(n_0), S(n_0+1), \ldots, S(k)$ imply that $S(k+1)$ for $k \geq n_0$, then the statement $S(n)$ is true for all integers $n \geq n_0$.*

A.0.2 The Connection between Mathematical Induction and the Principle of Well Ordering

Lemma A.0.2 *The Principle of Mathematical Induction implies that 1 is the least positive natural number.*

Proof. Let $S = \{n \in \mathbb{N} : n \geq 1\}$. Then $1 \in S$. Assume that $n \in S$. Since $0 < 1$, it must be the case that $n = n + 0 < n + 1$. Therefore, $1 \leq n < n + 1$. Consequently, if $n \in S$, then $n + 1$ must also be in S, and by the Principle of Mathematical Induction, and $S = \mathbb{N}$. ■

Theorem A.0.3 *The Principle of Mathematical Induction implies the Principle of Well-Ordering. That is, every nonempty subset of $\mathbb{N}$ contains a least element.*

Proof. We must show that if S is a nonempty subset of the natural numbers, then S contains a least element. If S contains 1, then the theorem is true by Lemma A.0.2. Assume that if S contains an integer k such that $1 \leq k \leq n$, then S contains a least element. We will show that if a set S contains an integer less than or equal to $n + 1$, then S has a least element. If S does not contain an integer less than $n + 1$, then $n + 1$ is the smallest integer in S. Otherwise, since S is nonempty, S must contain an integer less than or equal to n. In this case, by induction, S contains a least element. ■

A.0.3 The Proof of the Fundamental Theorem of Arithmetic

Theorem A.0.4 Fundamental Theorem of Arithmetic. *Let n be an integer such that $n > 1$. Then*

$$n = p_1 p_2 \cdots p_k,$$

where $p_1, \ldots, p_k$ are primes (not necessarily distinct). Furthermore, this factorization is unique; that is, if

$$n = q_1 q_2 \cdots q_l,$$

then $k = l$ and the q_i's are just the p_i's rearranged.

Proof. Uniqueness. To show uniqueness we will use induction on n. The theorem is certainly true for $n = 2$ since in this case n is prime. Now assume that the result holds for all integers m such that $1 \leq m < n$, and

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

where $p_1 \leq p_2 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \leq \cdots \leq q_l$. By Lemma 5.3.1, $p_1 \mid q_i$ for some $i = 1, \ldots, l$ and $q_1 \mid p_j$ for some $j = 1, \ldots, k$. Since all of the p_i's and q_i's are prime, $p_1 = q_i$ and $q_1 = p_j$. Hence, $p_1 = q_1$ since $p_1 \leq p_j = q_1 \leq q_i = p_1$. By the induction hypothesis,

$$n' = p_2 \cdots p_k = q_2 \cdots q_l$$

has a unique factorization. Hence, $k = l$ and $q_i = p_i$ for $i = 1, \ldots, k$.

Existence. To show existence, suppose that there is some integer that cannot be written as the product of primes. Let S be the set of all such numbers. By the Principle of Well-Ordering, S has a smallest number, say a. If the only positive factors of a are a and 1, then a is prime, which is a contradiction. Hence, $a = a_1 a_2$ where $1 < a_1 < a$ and $1 < a_2 < a$. Neither $a_1 \in S$ nor $a_2 \in S$, since a is the smallest element in S. So

$$a_1 = p_1 \cdots p_r$$
$$a_2 = q_1 \cdots q_s.$$

Therefore,

$$a = a_1 a_2 = p_1 \cdots p_r q_1 \cdots q_s.$$

So $a \notin S$, which is a contradiction. ■

Appendix B

Notation

The following table defines the notation used in this book. Page numbers or references refer to the first appearance of each symbol.

Appendix C

GNU Free Documentation License

0. PREAMBLE. The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS. This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

The “publisher” means any person or entity that distributes copies of the Document to the public.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING. You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY. If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS. You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties — for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS. You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS. You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS. A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION. Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION. You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE. The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING. "Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents. To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C)  YEAR  YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with… Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Index

Colophon

This book was authored in PreTeXt.