9-2018

# Elementary Set Theory

Richard P. Millspaugh
*University of North Dakota*, richard.millspaugh@und.edu

# Elementary Set Theory

Richard P. Millspaugh
University of North Dakota

# Preface

This text is appropriate for a transition to abstract mathematics course that covers basic set theory, an introduction to the real numbers, and some cardinality. It grew from my notes for such a course at the University of North Dakota, which is usually taken by math majors during their sophomore year. Except for a few motivational examples in the early chapters, the text is as self-contained as possible and does not assume much prerequisite material, though it is helpful to have some mathematical maturity before attempting to read the text. In Chapters 6 and 7, I assume the reader is familiar with the material in Chapters 1 – 5, but Chapters 6 and 7 are independent of each other. The style throughout is informal.

In using this text for my course, I always cover the material in Chapters 1 – 5 in depth. At various times I have finished the semester with either Chapter 6, Chapter 7, or both if time permits. I have included a proof of the Cantor-Bernstein Theorem in the appendix for completeness, but the proof is beyond the reach of many students who are just beginning to read and write proofs on their own.

# Contents

Chapter 1

# Elementary Logic

> I am convinced that the act of thinking logically cannot possibly be natural to the human mind. If it were, then mathematics would be everybody's easiest course at school and our species would not have taken several millennia to figure out the scientific method
>
> *Neil deGrasse Tyson*

> Anyone who cannot cope with mathematics is not fully human. At best he is a tolerable subhuman who has learned to wear shoes, bathe, and not make messes in the house.
>
> *Robert Heinlein*

## Introduction

In some sense, this text is about mathematical proofs. Why do mathematicians require proofs? How are you supposed to read and understand a proof? If you have to prove something yourself, how do you know where to start? How do you know when you're finished? Perhaps most importantly, what is a proof?

Mathematicians use proofs for many reasons, but a very simple answer to the last question above is that a proof is a logical argument to show that a statement is true. Unlike the experimental sciences, mathematicians do not accept a statement as true based on data or on statistical reasoning. We might collect data, but only to determine whether or not we believe that something is true. Consider the following:

**Theorem.** *If $p$ is an even integer, then $p^2$ is even.*

This statement is true, but how do we know that? We may start by squaring some even integers: $2^2 = 4$ is even, $8^2 = 64$ is even, $(-12)^2 = 144$ is even. Try a few more on your own. While this kind of experimentation certainly leads us to believe the statement is true, how can we be sure the pattern we think we see is always true? A statement like this one claims that something is true for *all* even integers. There are infinitely many even integers, so we can't possibly try all of them! However unlikely it may seem, it is possible that the first 3,000,012 examples we try will work, but the next one won't, or even that the statement is true for all but a single even integer.[1] In order to be certain that such a statement is true, we must carefully define what it means for an integer to be even, then use that property to prove that the square of *every* even integer is even. We will return to this example in the next chapter.

## 1.1 Propositions

**Definition.** A *proposition* is a statement that is either true or false, but not both. The *truth value* of a proposition is true (T) if the sentence is true and false (F) if the sentence is false.

Let's consider several sentences.

- *Two plus two equals four.* This sentence is true, hence a proposition.
- *Seven minus three equals twelve.* This sentence is false, hence a proposition.
- *It will snow in Grand Forks on March 17, 2525.* This sentence is either true or false, even if nobody currently alive will ever know which. It is a proposition, we just don't happen to know the truth value.
- *Go clean your room.* This sentence is a command, not a proposition.
- *Is it raining outside?* Again, this is not a proposition. It is a question.
- *This sentence is false.* This sentence is not a proposition because it cannot be either true or false. If it is true, then it's claim is false. If it's false, then it's claim must be true. We will not allow sentences that refer to themselves except as examples of what might go wrong if we are not careful.
- $x + 3 = 12$. This sentence cannot be said to be true or false without more information about the variable $x$. If $x = 0$, then it is false. If $x = 9$, then it is

[1] If this seems impossible, consider the following statement: *Every prime number is odd.*

true. Statements like this are not propositions, but are extremely important. We will discuss them in detail in Section [1.3].

We will use uppercase letters, frequently $P$ or $Q$, to stand for variable propositions in much the same way that you might use $x$ or $y$ to represent variable numbers in algebra.

## 1.2 Connectives and Truth Tables

Many of the propositions we are interested in are made up of more elementary propositions. For example, the proposition $S$: *today is Tuesday and it's raining* is made up of the two propositions $P$: *today is Tuesday* and $Q$: *it's raining*. The word *and* in $S$ is called a connective since it gives us a way to connect two propositions and form another. In this section we will look at several kinds of connectives, beginning with conjunction.

### 1.2.1 Conjunction

**Definition.** The *conjunction* of the propositions $P$ and $Q$ is the proposition $P$ *and* $Q$, denoted $P \wedge Q$. The conjunction $P \wedge Q$ is true when both $P$ and $Q$ are true and false if either $P$ or $Q$ (or both) are false.

We will sometimes keep track of the truth values of propositions in a *truth table* , where we list the truth values of a propositions in terms of the truth values of elementary propositions.

| $P$ | $Q$ | $P \wedge Q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | F |

The table above indicates that when $P$ and $Q$ are both true, $P \wedge Q$ is true; when $P$ is true and $Q$ is false, $P \wedge Q$ is false; etc. Note that in this case there are four rows in the table. For a proposition made up of $n$ elementary propositions, there will be $2^n$ rows in the truth table because there are two possible truth values for each of the elementary propositions. This makes it cumbersome to construct truth tables for very complicated propositions. Nevertheless, we will find them to be a convenient tool.

### 1.2.2 Disjunction

We next consider propositions of the form $P$ *or* $Q$. We have to be a bit more careful defining what we mean in this case, because the word *or* can be ambiguous in english. Let's consider a couple of english sentences to see why:

- *Either it's Tuesday or it's raining.*
- *Do you prefer coffee or tea?*

In the first of these sentences we mean that at least one of the two conditions must be met, it's Tuesday or it's raining. If it's raining on a Tuesday, this proposition is still true. In this case *or* is inclusive in the sense that it includes the possiblity that both conditions are met. In the second sentence, we presume that only one of the two options is possible. This use of the word *or* is exclusive since it excludes the possibility of both conditions being true at the same time. In normal discourse this kind of ambiguity doesn't usually cause any difficulty because we can determine the meaning from the context. We do not want to allow this kind of ambiguity in logical propositions, so we always use the word *or* in the inclusive sense. In other words, $P \vee Q$ is true if at least one of $P$ or $Q$ is true.

**Definition.** The *disjunction* of $P$ and $Q$ is the proposition $P$ *or* $Q$, denoted $P \vee Q$, which is true whenever at least one of $P$ or $Q$ is true.

Here is a truth table for the proposition $P \vee Q$.

| $P$ | $Q$ | $P \vee Q$ |
|---|---|---|
| T | T | T |
| T | F | T |
| F | T | T |
| F | F | F |

### 1.2.3 Implication

Most mathematical propositions have the form *If* $P$*, then* $Q$. Of course, either of $P$ or $Q$ might be propositions made of several other propositions.

Let's consider an example:

*If the student is on the basketball team, then she won't be in class on Friday.*

Consider two students in my Friday class, Jill and Pat. We will assume that Jill is on the basketball team and that Pat is not. Most of us would agree that Jill will not be in class Friday if the statement is true, so if Jill is in class then the statement must be false. What does the statement tell us about Pat? If she shows up for class Friday there's certainly nothing false about the statement, but what if she doesn't show up for class? Does that make the statement false? No! The statement makes no claim about Pat, so her attendence or absence doesn't impact the truth of the statement.

**Definition.** The proposition *If P, then Q* is called an *implication* and is denoted $P \Rightarrow Q$. The proposition $P$ is the *hypothesis* of the implication and $Q$ is the *conclusion*. The implication is false only when $P$ is true and $Q$ is false.

Here is a truth table for $P \Rightarrow Q$.

| $P$ | $Q$ | $P \Rightarrow Q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | T |
| F | F | T |

As a student of mathematics, it is absolutely essential that you understand what an implication means and what it doesn't mean. To say that $P \Rightarrow Q$ is true does not mean that $P$ is true or that $Q$ is true, it does mean that there is a relationship between the truth values of these two propositions. The implication $P \Rightarrow Q$ is false when $P$ is true and $Q$ is false; it is true when either $P$ is false or $Q$ is true.

There are several related implications related to the implication $P \Rightarrow Q$ that we will occassionally find these useful. Be aware that these are not all equivalent. You will determine which are equivalent to the original implication in Exercise 1.3.

**Definition.** For the implication $P \Rightarrow Q$:

- The *converse* is $Q \Rightarrow P$.
- The *contrapositive* is $\neg Q \Rightarrow \neg P$.
- The *inverse* of is $\neg P \Rightarrow \neg Q$.

### 1.2.4 Logical Equivalence

**Definition.** Two propositions $P$ and $Q$ are said to be *logically equivalent* if they always have the same truth value. We use the connective *iff*, read "if and only if," and use the symbol $\Leftrightarrow$. The proposition $P \Leftrightarrow Q$ is true when $P$ and $Q$ have the same truth value.

| $P$ | $Q$ | $P \Leftrightarrow Q$ |
|---|---|---|
| T | T | T |
| T | F | F |
| F | T | F |
| F | F | T |

### 1.2.5 Negation

**Definition.** The *negation* of $P$, denoted $\neg P$ and sometimes read "not $P$," is the proposition whose truth value is always opposite that of $P$.

Note that negation is not actually a connective since it applies to a single proposition rather than connecting two propositions.

| $P$ | $\neg P$ |
|---|---|
| T | F |
| F | T |

### 1.2.6 Tautology and Contradiction

**Definition.** A *tautology* is a proposition that is always true, regardless of the truth values of the elementary propositions that make it up.

**Definition.** A *contradiction* is a proposition that is always false.

**Example 1.1.** *The proposition $P \vee \neg P$ is an example of a tautology. One way to see this is to look at a truth table. Notice that all truth values in the column for $P \vee \neg P$ are true. We can also use this truth table to see that $P \wedge \neg P$ is a contradiction because every truth value in that column is false.*

| $P$ | $\neg P$ | $P \vee \neg P$ | $P \wedge \neg P$ |
|---|---|---|---|
| $T$ | $F$ | $T$ | $F$ |
| $F$ | $T$ | $T$ | $F$ |

**Example 1.2.** *Use truth tables to show that the following are tautologies.*

*(i)* $P \Rightarrow (P \vee Q)$

*(ii)* $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

**Solutions**

*(i) We must construct a truth table with a column for* $P \Rightarrow (P \vee Q)$ *and show that the truth values in that column are all T.*

| $P$ | $Q$ | $P \vee Q$ | $P \Rightarrow (P \vee Q)$ |
|---|---|---|---|
| $T$ | $T$ | $T$ | $T$ |
| $T$ | $F$ | $T$ | $T$ |
| $F$ | $T$ | $T$ | $T$ |
| $F$ | $F$ | $F$ | $T$ |

*(ii) Note that we can either construct a truth table with a column for the desired equivalence and show that the truth values are all T, or we can construct a truth table with the columns for* $P \Rightarrow Q$ *and* $\neg Q \Rightarrow \neg P$ *and show that the truth values are always equal to each other. We will do the latter since it is less work.*

| $P$ | $Q$ | $\neg P$ | $\neg Q$ | $P \Rightarrow Q$ | $\neg Q \Rightarrow \neg P$ |
|---|---|---|---|---|---|
| $T$ | $T$ | $F$ | $F$ | $T$ | $T$ |
| $T$ | $F$ | $F$ | $T$ | $F$ | $F$ |
| $F$ | $T$ | $T$ | $F$ | $T$ | $T$ |
| $F$ | $F$ | $T$ | $T$ | $T$ | $T$ |

## 1.3 Predicates, Instantiation, and Quantification

We return our attention now to statements that involve variables, like $x + 3 = 12$. Such a statement is called a *predicate* and we will usually indicate it with $P(x)$

rather than $P$. Before a predicate takes on a truth value, we need to know something about the variable. We noted before that if $x = 0$, then the statement is false; but if $x = 9$, then the statement is true. What if $x$ represents my desk? In that case the statement is complete nonsense, but you probably feel like there's something a little bit unfair about that choice for $x$. We see an equation and usually think that the variable must represent a number, right? The first thing you should know about any variable in a predicate is what it can represent. This is called the *universe* or the *domain of discourse*. In mathematics, we will be very explicit about what universe we are talking about.

### 1.3.1 Instantiation

Let's understand that in our predicate $P(x)$ from the previous paragraph, we declare that the universe is the set of real numbers. That still doesn't turn $P(x)$ into a proposition because, as noted above, $P(x)$ doesn't take on a truth value until we know which real number $x$ indicates. One way to do this is called *instantiation*, which means choosing a particular value for the variable(s). Consider for example the sentence: *Let* $x = 2$*, then* $x + 3 = 12$. In this case the sentence is a proposition with truth value F.

The other option is *quantification* of the variable(s). We will discuss two kinds of quantifiers, *universal* and *existential*. You might occasionally encounter other quantifiers, but they are not necessary.

### 1.3.2 Universal Quantification

**Definition.** A *universal quantifier* indicates that the predicate is true for all instances of the variable in the given universe. It is typically indicated by using the phrase "for every" or "for all," and can be denoted symbolically by $\forall$ in symbolic statements.

The following sentences are universally quantified propositions. Only the second is true.

- *For every real number* $x$*,* $x + 3 = 12$.
- *The square of* $x$ *is nonnegative for all real* $x$.
- *The square of* $x$ *is nonnegative for all complex* $x$.

### 1.3.3 Existential Quantification

**Definition.** An *existential quantifier* indicates that the predicate is true for at least one instance of the variable in the given universe. It is typically indicate by the phrase "for some" or "there exists," and can be denoted by $\exists$ in symbolic statements.

The following sentences are existentially quantified. All three of these are true.

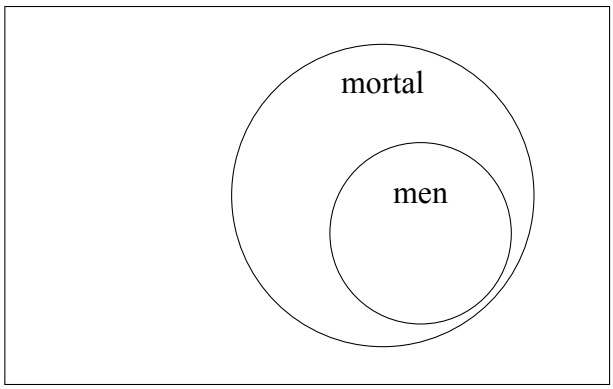
- *There is a real number $x$ so that $x + 3 = 12$.*
- *The square of $x$ is nonnegative for some real $x$.*
- *The square of $x$ is nonnegative for some complex $x$.*

### 1.3.4 Syllogisms and Venn Diagrams

A *syllogism* is a form of logical argument that deduces a conclusion based on two premises. For example:

*All men are mortal. Socrates is a man. Hence Socrates is mortal.*

This is a valid syllogism. If we assume that the premises are true, then the conclusion must follow. One tool we can use to help think about syllogisms is a *Venn diagram*, which in it's simplest form is a collection of circles that represent the various categories in the premises. In this case we will have one circle representing mortals and another representing men. Since one of our premises is that all men are mortal, the circle representing men is completely contained inside the circle representing mortals:



Since Socrates is a man, hence inside the circle representing men, he must of necessity also be inside the circle representing mortals, hence the syllogism is valid.

**Example 1.3.** *Determine whether each of the following syllogisms is valid.*

*(i) Some students are freshmen. Pat is a student. Hence Pat is a freshman.*

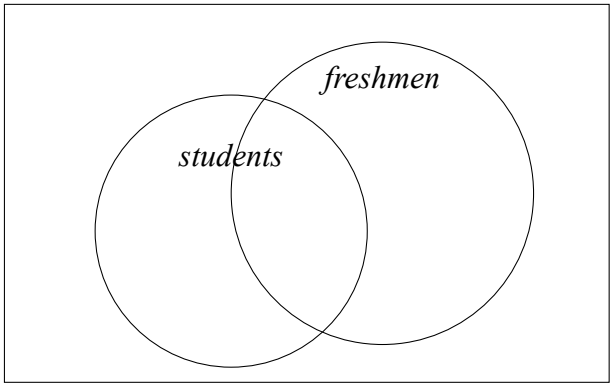
*(ii) No cats are dogs. Jade is a cat. Hence Jade is not a dog.*

*(iii) Some cats are psychopaths. Jawa is a cat. Hence Jawa is a psychopath.*

*(iv) Some Billywiggles are Bleepzigs. Some Bleepzigs are Jabberwoks. Hence some Billywiggles are Joabberwoks.*

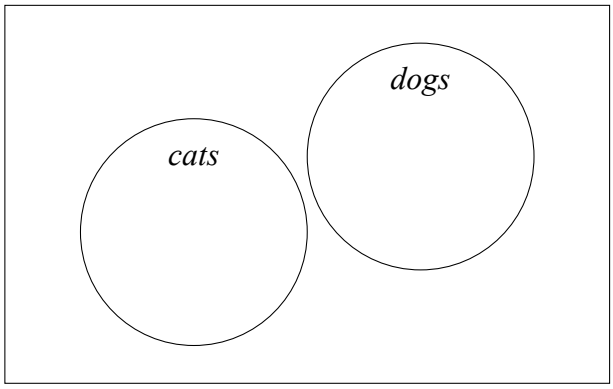
**Solutions**

*(i) The circle for students should overlap the circle for freshmen, but need not be contained within it since our assumption is that only some students are freshmen.. Here is a Venn diagram:*



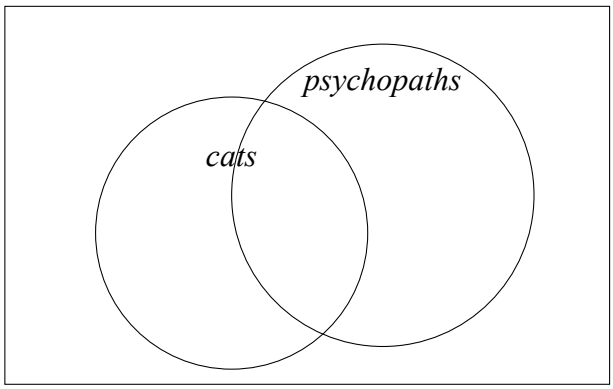

*Note that Pat may be in the student circle without being inside the freshmen circle, so the syllogism is not valid.*

*(ii) In this case, the circle for cats should be completely outside the circle for dogs since no cats are dogs. Here is a Venn diagram:*



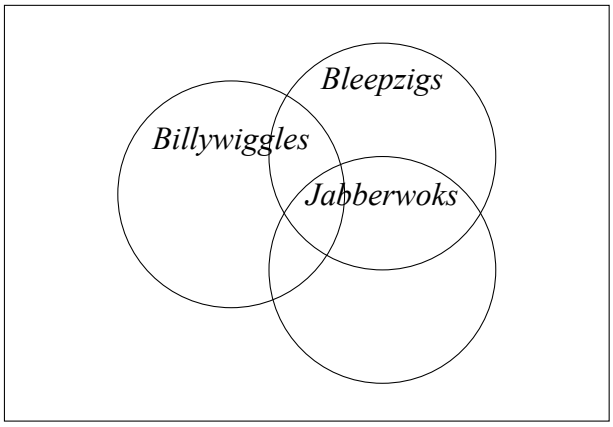

*Since Jade must be within the cats circle, Jade cannot be within the dogs circle, so the syllogism is valid.*

*(iii) Here is a Venn diagram:*

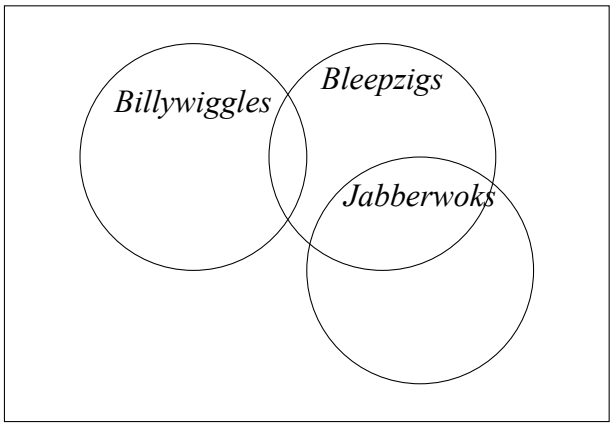



*Since Jawa must be in the cats circle, but may or may not be within the psychopaths circle, this syllogism is not valid.*

*(iv) This requires a slightly more complicated Venn diagram, and we must be very careful about what is absolutely necessary. It is possible for the Venn diagram to look like this:*




*On the other hand, it is also possible for the Venn diagram to look like the following:*




*This syllogism is not valid.*

### 1.3.5 Quantification of Several Variables

A predicate can have two or more variables. In order to use the predicate in a proposition, a universe must be declared for each variable and each variable must be instantiated or quantified. We will discuss the various ways a two variable predicate might be quantified by considering an example.

We consider the predicate $P(x, y)$ given by $x + y = 0$. Throughout, we will will assume that the universe for both $x$ and $y$ is the set of real numbers.[2] Without

[2] In general, distinct variables might sometimes come from different universes.

redefining the universe every time, both variables could be universally quantified, both could be existentially quantified, or one could be universally quantified and the other existentially quantified. We are particularly interested in determining when each proposition will be true and whether the order of the quantifiers matters.

- $\forall x\ \forall y\ P(x,y)$: This proposition can be read as *for all (real) $x$ and for all (real) $y$, $x + y = 0$*, which says the sum of any two real numbers is 0. Clearly this is false.
- $\forall y\ \forall x\ P(x,y)$: Restating this as we did above, it is not difficult to see that this proposition is equivalent to the first one.
- $\exists x\ \exists y\ P(x,y)$: We can read this as *there is an $x$ so that there is a $y$ so that $x + y = 0$*, which says that there are real numbers $x$ and $y$ such that $x + y = 0$. This is true. Once again, reversing the order of the quantifiers doesn't matter.
- $\forall x\ \exists y\ P(x,y)$: This proposition says that *for every $x$ there is a $y$ such that $x + y = 0$*, in other words every real number has an additive inverse, which is certainly true.
- $\exists y\ \forall x\ P(x,y)$: The variables here are quantified the same, but the order is changed. Does that matter? The proposition this time says *there is a $y$ so that for all $x$, $x + y = 0$*. In other words, there is some real number $y$ so that adding any real number to $y$ yields a sum of 0, which is certainly false!

The moral of the last example is that you must be careful to quantify variables in the correct order when some variables are universally quantified and some are existentially quantified.

## 1.4 Negations

As mentioned previously in [1.2.5], the negation of a proposition is the proposition with the opposite set of truth values. In this section we are going to discuss the negations of compound propositions, which can be an important step in some kinds of proofs. We begin with two theorems that tell how to find the negations of propositions involving connectives.

**Theorem 1.1.** *Given any propositions $P$ and $Q$, $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$.*

To see that this theorem is true, we first make sure that we understand what it is saying. The variables in this case are actually propositions $P$ and $Q$, both of which are universally quantified. The theorem asserts that the compound proposition $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$ is always true, so we must demonstrate that no matter what the truth values of $P$ and $Q$ are, the statement in the theorem is a tautology. We proceed by constructing a truth table.

| $P$ | $Q$ | $\neg Q$ | $P \Rightarrow Q$ | $\neg(P \Rightarrow Q)$ | $P \wedge \neg Q$ |
|---|---|---|---|---|---|
| T | T | F | T | F | F |
| T | F | T | F | T | T |
| F | T | F | T | F | F |
| F | F | T | T | F | F |

The truth of the next theorem can be established in a similar fashion, which we leave tothe exercises (see 1.9).

**Theorem 1.2. (DeMorgan's Laws)** *Given any propostions $P$ and $Q$:*

*(i)* $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$

*(ii)* $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$

We can use these results to understand the negations of more complicated propositions. Suppose we want to know how to negate the proposition $P \Rightarrow (Q \wedge R)$. We apply what we know one step at a time, beginning with the implication:

$$\begin{aligned} \neg\big(P \Rightarrow (Q \wedge R)\big) &\Leftrightarrow P \wedge \big(\neg(Q \wedge R)\big) && \text{(Theorem 1.1)} \\ &\Leftrightarrow P \wedge (\neg Q \vee \neg R) && \text{(Theorem 1.2(i))} \end{aligned}$$

**Example 1.4.** *Find the negation of each of the following propositions.*

*(i)* $P \wedge (Q \Rightarrow R)$

*(ii)* $(P \vee Q) \wedge (P \vee R)$

**Solutions**

*(i) We apply Theorems 1.1 and 1.2 where indicated.*

$$\begin{aligned} \neg\big(P \wedge (Q \Rightarrow R)\big) &\Leftrightarrow \big(\neg P \vee \neg(Q \Rightarrow R)\big) && \textit{(Theorem 1.2(i))} \\ &\Leftrightarrow \big(\neg P \vee (Q \wedge \neg R)\big) && \textit{(Theorem 1.1} \end{aligned}$$

*(ii) We apply Theorem 1.2 where indicated.*

$$\begin{aligned}\neg\big((P \vee Q) \wedge (P \vee R)\big) &\Leftrightarrow \big(\neg(P \vee Q) \vee \neg(P \vee R)\big) \qquad \textit{(Theorem 1.2(i))} \\ &\Leftrightarrow \big((\neg P \wedge \neg Q) \vee (\neg P \wedge \neg R)\big) \qquad \textit{(Theorem 1.2(i,ii))}\end{aligned}$$

# Chapter 1 Exercises

**1.1.** Show that $\neg(\neg P) \Leftrightarrow P$ is a tautology.

**1.2.** Determine whether each of the following is a tautology, a contradiction, or neither one.

(i) $(P \Rightarrow Q) \Rightarrow Q$

(ii) $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$

(iii) $(P \Rightarrow Q) \Leftrightarrow (Q \Rightarrow P)$

(iv) $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$

(v) $(P \Rightarrow Q) \wedge (P \Rightarrow \neg Q)$

(vi) $P \wedge (P \Rightarrow Q) \wedge (P \Rightarrow \neg Q)$

(vii) $(\neg Q \wedge (P \Rightarrow Q)) \Rightarrow \neg P$

(viii) $((P \vee Q) \wedge \neg Q) \Rightarrow P$

(ix) $((P \vee Q) \Rightarrow R) \Rightarrow (P \Rightarrow R)$

**1.3.** Determine whether or not each of the following is equivalent to the implication $P \Rightarrow Q$.

(i) The converse: $Q \Rightarrow P$

(ii) The contrapositive: $\neg Q \Rightarrow \neg P$

(iii) The inverse: $\neg P \Rightarrow \neg Q$

**1.4.** Use truth tables to prove the following:

(i) Disjunction is commutative, i.e. $P \vee Q$ is equivalent to $Q \vee P$.

(ii) Conjunction is commutative.

(iii) Disjunction is associative, i.e. $P \vee (Q \vee R)$ is equivalent to $(P \vee Q) \vee R$.

(iv) Conjunction is associative.

**1.5.** Show that $P \wedge (Q \vee R)$ is not equivalent to $(P \wedge Q) \vee R$.

**1.6.** Use truth tables for each of the following:

(i) Show that conjunction distributes over disjunction, i.e. that $P \wedge (Q \vee R)$ is equivalent to $(P \wedge Q) \vee (P \wedge R)$.

(ii) Show that disjunction distributes over conjunction.

**1.7.** Determine whether or not each of the following syllogisms is valid.

(i) Some dogs are beagles. Snoopy is a dog. Hence Snoopy is a beagle.

(ii) All cats are independent. Some pets are cats. Hence some pets are independent.

(iii) No pigs fly. Porky is a pig. Hence Porky does not fly.

(iv) No orcs are ogres. All ogres are green. Hence no orcs are green.

**1.8.** Negate each of the following:

(i) Every cloud has a silver lining.

(ii) If it's Tuesday, this must be Belgium.

(iii) There is a light at the end of every tunnel.

**1.9.** Use truth tables to show that:

(i) $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$

(ii) $\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q))$

**1.10.** Use a truth table to show that $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$

**1.11.** One way of defining what it means for a function $f$ to be continuous at a point $x_0$ is as follows:
*Let $f$ be a function and let $x_0 \in \mathbb{R}$ be a point in the domain of $f$. We say that $f$ is continuous at $x_0$ if the following is true:*

> *For every $\epsilon > 0$ there is a $\delta > 0$ so that for every $t \in \mathbb{R}$, if $|x_0 - t| < \delta$ then $|f(x_0) - f(t)| < \epsilon$.*

What does it mean to say that $f$ is not continuous at $x_0$?

Chapter 2

# Logical Arguments

> The fact that mathematics is symbolic logic is one of the greatest discoveries of our age.
>
> *Bertrand Russell*

> Reductio ad absurdum, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.
>
> *Godfrey Hardy*

## Introduction

Loosely speaking, a mathematical proof is a logical argument. It is probably more correct to say that a mathematical proof is a way of indicating how a logical argument could be carried out, but for now let's not worry about that distinction. In this chapter we will learn what we mean by a logical argument and look at some common types of mathematical proofs.

The first proofs most students encounter are two-column proofs, frequently in high school geometry. In this kind of proof the first column consists of a series of statements and the second a series of justifications for those statements. Allowable justifications might be assumptions, definitions, theorems, or consequences of previous steps. We concern ourselves first with the rules that allow us to deduce propositions from previous propositions.

## 2.1 Rules of Inference

We accept the following two basic rules of thought:

> The *Law of Excluded Middle* says that given any proposition $P$, we may deduce $P \vee \neg P$. In words, either $P$ is true or $\neg P$ is true.
>
> The *Law of non-Contradiction* says that given any proposition $P$, we may deduce $\neg(P \wedge \neg P)$. In words, $P$ and $\neg P$ cannot both be true.

A *rule of inference* is a logical rule consisting of a hypothesis and a conclusion. Whenever the hypothesis is true, the conclusion must also be true. For our purposes this means that once we have deduced all of the hypotheses, we may also deduce the conclusion. Rules of inference are closely related to tautologies. In fact, they are essentially the same thing. While every tautology gives rise to a rule of inference, in practice the seven listed in the table below will usually suffice.

*Table 2.1: Rules of Inference*

Table 2.1: Rules of Inference

| **Name** | **Hypotheses** | **Conclusion** |
|---|---|---|
| Modus ponens | $P$ and $P \Rightarrow Q$ | $Q$ |
| Modus tolens | $\neg Q$ and $P \Rightarrow Q$ | $\neg P$ |
| Hypothetical syllogism | $P \Rightarrow Q$ and $Q \Rightarrow R$ | $P \Rightarrow R$ |
| Addition | $P$ | $P \vee Q$ |
| Simplification | $P \wedge Q$ | $P$ |
| Conjunction | $P$ and $Q$ | $P \wedge Q$ |
| Disjunctive syllogism | $P \vee Q$ and $\neg P$ | $Q$ |

The Rule of Addition, for example, comes from the tautology $P \Rightarrow (P \vee Q)$. Since the implication is always true, knowing that the hypothesis is true will tell us that the conclusion must also be true. We can verify each of the Rules of Infernece in Table 2.1 by constructing a truth table for the associated tautology.

### 2.1.1 Propositional Arguments

In this section we consider theorems from logic rather than from mathematics. We will look at arguments in which the form of each proposition is important rather

than the content of the propositions. Each of our Rules of Inference is actually a *propositional argument*, where accepting the hypotheses forces us to accept the conclusion. We use the following notation for propositional arguments, where the propositions above the line are hypotheses and the proposition(s) below the line are the conclusion(s). We precede the conclusions(s) with the symbol $\therefore$ which is read "therefore." Please note that not all authors use this symbol.

**Example 2.1.** *Here is the rule modus tolens in our notation:*

$$\begin{array}{l} \neg Q \\ \underline{P \Rightarrow Q} \\ \therefore \neg P \end{array}$$

**Example 2.2.** *Express the following rules of inference as propositional arguments.*

*(i) Modus ponens*

*(ii) Hypothetical syllogism*

**Solutions.**

$$\text{(i)} \quad \begin{array}{l} P \\ \underline{P \Rightarrow Q} \\ \therefore Q \end{array}$$

$$\text{(ii)} \quad \begin{array}{l} P \Rightarrow Q \\ \underline{Q \Rightarrow R} \\ \therefore P \Rightarrow R \end{array}$$

**Definition.** A propositional argument is said to be *valid* if accepting the hypotheses forces us to accept the conclusion(s).

How do we determine whether or not a propositional argument is valid? One option is to constuct a truth table, but that can be very tedious. Our preferred option is to construct a logical argument which begins by assuming each of the hypotheses is true and deduces consequences using our rules of inference. Each deduced proposition is a step in our proof that can be justified as either a hypothesis, a consequence of previous steps and a rule of inference, or a proposition that is logically equivalent to a previous step. The proof is complete when we have deduced the desired conclusion.

**Example 2.3.** *Prove that the following argument is valid:*

$$\begin{array}{l} P \\ P \Rightarrow Q \\ \underline{(Q \vee R) \Rightarrow S} \\ \therefore\ S \end{array}$$

| *Proof.* | | | |
|---|---|---|---|
| | *(1)* | $P$ | hypothesis |
| | *(2)* | $P \Rightarrow Q$ | hypothesis |
| | *(3)* | $Q$ | modus ponens, (1) and (2) |
| | *(4)* | $Q \vee R$ | addition, (3) |
| | *(5)* | $(Q \vee R) \Rightarrow S$ | hypothesis |
| | *(6)* | $S$ | modus ponens, (4) and (5) |

**Example 2.4.** *Prove that the following argument is valid:*

$$\begin{array}{l} \underline{P \Rightarrow (Q \wedge \neg Q)} \\ \therefore\ \neg P \end{array}$$

| *Proof.* | | | |
|---|---|---|---|
| | *(1)* | $P \Rightarrow (Q \wedge \neg Q)$ | hypothesis |
| | *(2)* | $\neg(Q \wedge \neg Q)$ | Excluded Middle |
| | *(3)* | $\neg P$ | modus tolens, (1) and (2) |

The argument in Example 2.4 says that if a proposition $P$ implies a contradiction, then $\neg P$ must be true. We will use this result in the sequel as the basis for proofs by contradiction.

### 2.1.2 Arguments with Quantifiers

Arguments involving quantified propositions require us to have rules of inference for instantiation and quantification. The *rules for instantiation* when we can deduce statements about particular elements of the domain given quantified statements. The *rules for generalization* tell us when we can deduce quantified statements given deductions about particular elements of the domain. We give these rules in Table 2.2.

*Table 2.2: Rules of Quantification*

**Example 2.5.** *Prove that the following argument is valid:*

Table 2.2: Rules of Quantification

| **Name** | **Rule** |
|---|---|
| Universal Instantiation | $\forall x\ P(x) \therefore P(c)$ whenever $c$ is in the domain of $x$ |
| Existential Instantiation | $\exists x\ P(x) \therefore P(c)$ for some $c$ in the domain of $x$ |
| Universal Generalization | $P(c)$ for *arbitrary* $c$ in the doamin of $x \therefore \forall x\ P(x)$ |
| Existential Generalization | $P(c)$ for *some* $c$ in the domain of $x \therefore \exists x\ P(x)$ |

$$\begin{array}{l} \forall x\ (P(x) \wedge Q(x)) \\ \underline{\exists x\ (P(x) \Rightarrow R(x))} \\ \therefore\ \exists x\ (Q(x) \wedge R(x)) \end{array}$$

*Proof.*

| | | |
|---|---|---|
| *(1)* | $\exists x\ (P(x) \Rightarrow R(x))$ | hypothesis |
| *(2)* | $P(c) \Rightarrow R(c)$ *for some* $c$ | existential quantification, (1) |
| *(3)* | $\forall x\ (P(x) \wedge Q(x))$ | hypothesis |
| *(4)* | $P(c) \wedge Q(c)$ | universal quantification, (3) |
| *(5)* | $Q(c)$ | simplification, (4) |
| *(6)* | $P(c)$ | simplification, (4) |
| *(7)* | $R(c)$ | modus ponens, (2) and (6) |
| *(8)* | $Q(c) \wedge R(c)$ | conjunction, (5) and (7) |
| *(9)* | $\exists x\ (Q(x) \wedge R(x))$ | existential generalization, (8) |

## 2.2 Proving Mathematical Theorems

Most mathematical statements are implications of the form $P \Rightarrow Q$, where $P$ or $Q$ might be compound propositions. In this section we will look at some methods for proving implications. Note that we are using some definitions and results from other areas of mathematics that we have not explicitly stated. We will not allow ourselves to make those kinds of assumptions once we begin our study of set theory.

### 2.2.1 Direct Proofs

A direct proof of the implication $P \Rightarrow Q$ assumes that the hypothesis $P$ is true, then uses definitions, previously proved theorems, and the rules of inference to deduce that the conclusion $Q$ must also be true.

**Theorem 2.1.** *If $n$ is an even integer, then $n^2$ is even.*

The first step in trying to prove any theorem is to make sure you know what it means. In this case, we need to know the definition of an even integer and of the square of an integer. An integer $n$ is even if it can be written as $n = 2k$ for some integer $k$. The square of $n$ is the product $n^2 = n \times n$.

| | | | |
|---|---|---|---|
| *Proof.* | (1) | $n$ is an even integer | hypothesis |
| | (2) | $n = 2k$ for some integer $k$ | definition, (1) |
| | (3) | $n^2 = (2k)^2$ | definition, (2) |
| | (4) | $n^2 = 4k^2$ | algebra, (3) |
| | (5) | $n^2 = 2(2k^2)$ | algebra, (4) |
| | (4) | $n^2$ is even | definition, (5) |

Although the two-column proof above is valid, it is not written in a format that mathematicians usually find acceptable. We prefer proofs that are written using complete sentences, paragraphs, and correct grammar and punctuation. Here is a better presentation for the previous proof.

*Proof of Theorem 2.1.* Let $n$ be an even integer, then by definition $n = 2k$ for some integer $k$. Squaring both sides yields $n^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, $2(2k^2)$ is even as desired. □

We will present some proofs in each format for the remainder of this chapter. You should become used to translating two-column proofs into paragraph format.

The proof of the following theorem is left as an exercise for the reader.

**Theorem 2.2.** *The square of an odd integer is odd.*

### 2.2.2 Proving the Contrapositive

In Exercise 1.3 you showed that the contrapositive of an implication is logically equivalent to the implication. Sometimes it is easier to prove the contrapositive of the implication we are interested in. Consider the following example.

**Theorem 2.3.** *If $n$ is an integer and $n^2$ is even, then $n$ is even.*

We might try to begin this proof as we did the proof of Theorem 2.1. First assume that $n^2$ is even. By definition we know that $n^2 = 2k$ for some integer $k$. Now what? In the previous example we were able to square $2k$ and see that the result was even, but taking the square root doesn't tell us anything useful. Instead we prove the contrapositive of the theorem: *If $n$ is an integer that is not even, then $n^2$ is not even.* We use the fact that every integer is either even or odd, but never both.

| | | |
|---|---|---|
| *Proof.* (1) | $n$ is an odd integer | hypothesis |
| (2) | if $n$ is odd, $n^2$ odd | Theorem 2.2 |
| (3) | $n^2$ is odd | modus ponens, (1) and (2) |
| (4) | if $n$ is even, $n^2$ is even | Theorem 2.1 |
| (5) | $n$ is odd | modus tolens, (3) and (4) |

The next theorem can be proved in a similar fashion and is left as an exercise.

**Theorem 2.4.** *If $n$ is an integer and $n^2$ is odd, then $n$ is odd.*

### 2.2.3 Proof by Contradiction

A proof by contradiction, or *reductio ad absurdum* begins by assuming that the result we are trying to prove is false, then deriving a contradiction from that assumption. It is easy to confuse this with a direct proof of the contrapositive, which makes different beginning assumptions. To prove the implication $P \Rightarrow Q$ by proving the contrapositive, you assume $\neg Q$ and use that to prove $\neg P$. A proof by contradiction assumes $P \wedge \neg Q$ and derives a contradiction $R \wedge \neg R$. Here is a classic example of a proof by contradiction.

**Theorem 2.5.** *There is no rational number $x$ such that $x^2 = 2$.*

*Proof.* Suppose to the contrary that there is a rational number $x$ with $x^2 = 2$. Since $x$ is rational, we may express $x$ as a fraction $p/q$ in lowest terms, in other words $p$ and $q$ are integers and no integer evenly divides both of them. Since $x = p/q$ and $x^2 = 2$, we have $p^2/q^2 = 2$, or:

$$p^2 = 2q^2 \tag{2.1}$$

Since $q^2$ is an integer, $p^2 = 2q^2$ is even. So $p$ is an integer and $p^2$ is even, so Theorem 2.3 implies that $p$ is even. This allows us to write $p = 2k$ for some integer $k$. We plug this into equation 2.1 to see that $4k^2 = 2q^2$, so $q^2 = 2k^2$. Now $q$ is an integer and $q^2$ is even, so another application of Theorem 2.3 implies that $q$ is even. We now know that both $p$ and $q$ are even, so 2 divides both of them. This contradicts our choice of $p$ and $q$, so our assumption that $x$ is rational must be incorrect. □

### 2.2.4 Proof by Cases

To prove the implication $P \Rightarrow Q$ by cases, we make use of the following argument.:

$$\begin{array}{l} P \Rightarrow (R \vee S) \\ R \Rightarrow Q \\ \underline{S \Rightarrow Q} \\ \therefore\ P \Rightarrow Q \end{array}$$

You will be asked to show that this argument is valid in Exercise 2.2.

Here is a very simple example of a proof by cases. We make use of some of the order properties of the real numbers. In particular, we know that multiplying both sides of an inequality by a positive number preserves the inequality, and multiplying both sides of an inequality by a negative number reverses the inequality.

**Theorem 2.6.** *If $x$ is a real number, then $x^2 \geq 0$.*

*Proof.* If $x$ is a real number, then either $x \geq 0$ or $x < 0$.

Case 1. If $x \geq 0$, then we may multiply both sides of this inequality by 0 to see that $x^2 \geq x \cdot 0 = 0$.

Case 2. If $x < 0$, then muliplying both sides of the inequality by $x$ reverses the inequality, yielding $x^2 > x \cdot 0 = 0$. Since $x^2 > 0$ we have $x^2 \geq 0$. (Why?)

In either case we have $x^2 \geq 0$, so the result is true. □

## 2.3 Proving Quantified Statements

### 2.3.1 Universally Quantified Statements

On the simplest level, a universally quantified statement has the form $\forall x\ P(x)$. To prove such a proposition, we assume that $x$ is in the required domain and show that $P(x)$ must be true. It is frequently helpful to think of such a statement as an implication where the hypothesis is that $x$ is in the required domain, and the conclusion is $P(x)$. In fact, we have alreadu seen such an example when we proved Theorem 2.6. We could restate this theorem as follows:

**Alternate Theorem 2.6.** *For every real number $x$, $x^2 \geq 0$.*

Since universally quantified statements can be thought of as implications, we can use the same proof techniques.

### 2.3.2 Existentially Quantified Statements

Existentially quantified statements are significantly different than implications and universally quantified statements. To prove the statement $\exists x, P(x)$ we must show that there is at least one $x$ in the domain that satisfies $P(x)$. One way to do this is simply to find a single particular example. The following theorem can be proved in this way.

**Theorem 2.7.** *There is a positive integer $N$ such that $N$, $N+1$, $N+2$, $N+3$, and $N+4$ are all composite (not prime).*

*Proof.* Let $N = 6! + 2$, then $N$ is divisible by 2, $N + 1 = 6! + 3$ is divisible by 3, $N + 2 = 6! + 4$ is divisible by 4, $N + 3 = 6! + 5$ is divisible by 5, and $N + 4 = 6! + 6$ is divisible by 6. □

We note one thing about the last proof. We could just as easily have used the much smaller number $N = 24$ since 24, 25, 26, 27, and 28 are all composite. Can you see any advantage to using the number we used?

There are some instances where it is easier to show that some $x$ satifies $P(x)$ without actually finding a particular $x$ that works. Here is an elementary example that works by demonstrating that one of two possible choices must work, without determining which it is. We assume familiarity with the rules for exponents, as well as the existence of an irrational number $x$ such that $x^2 = 2$.

**Theorem 2.8.** *There exist irrational numbers $a$ and $b$ so that $a^b$ is rational.*

*Proof.* First note that $\sqrt{2}$ is irrational, but

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^{\,2} = 2$$

is rational. Now it is certainly true that $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational. If $\sqrt{2}^{\sqrt{2}}$ is rational, then we set $a = \sqrt{2}$ and $b = \sqrt{2}$ to find the example we need. If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we set $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ to find the example we need. Either way, there are irrational numbers $a$ and $b$ such that $a^b$ is rational. □

### 2.3.3 Counterexamples.

Consider the following proposition:

**Conjecture.** *Every integer is even.*

It probably seems clear to you that this statement is false, but how could you prove that? To prove that a proposition is false we must show that it's negation is true, so we first find the negation of the original statement:

*Some integer is not even.*

We have transformed our original problem (proving that a statement is false) into something more familar (proving that a statement is true): How do we prove the second statement is true? As noted above, one way to prove an existentially quantified statement is simply to find the object it says exists. In this case, we must find an integer that is not even. Of course, we know many such integers. Any odd integer will do. So our proof that the original statement is false consists of finding an example that makes it false: the integer $x = 1$ is not even. Note that you shouldn't just say that there are such examples, you should give a particular one that your reader can check. An example showing that a universally quantified statement is false is called a *counterexample* to that statement.

## 2.4 Mathematical Induction

There is another type of proof that is frequently used to prove statements about the natural numbers, i.e. the numbers $1, 2, 3, \ldots$.

**The Principle of Mathematical Induction.** Let $P(n)$ be a statement about the natural number $n$.

(i) If $P(1)$ is true, and

(ii) if $P(k) \implies P(k+1)$ for every natural number $k$,

then $P(n)$ is true for every natural number $n$.

All proofs by induction use the following basic outline. To prove $P(n)$ for all natural numbers $n$,

(i) Base Case: Show that $P(1)$ is true.

(ii) Inductive Step: Prove the implication $P(k) \implies P(k+1)$ for all $k \in \mathbb{N}$. Note: in proving that $P(k) \implies P(k+1)$, the assumption that $P(k)$ is true is often referred to as the inductive hypothesis.

(iii) It is considered good form to clearly state that the statement $P(n)$ is now true for all natural numbers $n$ by induction.

You might think of a proof by induction as similar to knocking over a row of dominoes. If you know that knocking over any domino will cause the next one to fall, then knocking over the first domino will cause all of the dominoes to fall. Keep in mind that *you must complete all of the steps above in an inductive proof*. Here are a couple of examples.

**Theorem 2.9.** *For each natural number n,* $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

*Proof.* If $n = 1$, then

$$\sum_{i=1}^{n} i = \sum_{i=1}^{1} i = 1 = \frac{1(2)}{2} = \frac{n(n+1)}{2},$$

so the formula holds for $n = 1$.

Now suppose that the formula holds for some $k \in \mathbb{N}$. In other words, we are assuming that $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. We want to show that the formula must hold for

$n = k+1$. Using our assumption, we compute:

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}\end{aligned}$$

Hence the formula holds for $n = k+1$. By induction, the formula must hold for all $n \in \mathbb{N}$. □

# Chapter 2 Exercises

**2.1.** Show that the following argument is valid:

$$\begin{array}{l} P \\ \neg Q \\ P \Rightarrow (Q \vee R) \\ \hline \therefore\ R \end{array}$$

**2.2.** Show that the following argument is valid:

$$\begin{array}{l} P \Rightarrow (R \vee S) \\ R \Rightarrow Q \\ S \Rightarrow Q \\ \hline \therefore\ P \Rightarrow Q \end{array}$$

**2.3.** Show that the following argument is valid:

$$\begin{array}{l} \forall x\ (P(x) \Rightarrow Q(x)) \\ \exists x\ (Q(x) \Rightarrow R(x)) \\ \hline \therefore\ \exists x\ (P(x) \Rightarrow R(x)) \end{array}$$

**2.4.** Which of the following is the best interpretation of the statement: *Every blue meanie is fuzzy*?

(i) There are blue meanies and at least one of them is fuzzy.

(ii) There are blue meanies and at least two of them are fuzzy.

(iii) There are blue meanies and all of them are fuzzy.

(iv) There may not be any blue meanies, but if there are at least one of them is fuzzy.

(v) There may not be any blue meanies, but if there are at least two of them are fuzzy.

(vi) There may not be any blue meanies, but if there are all of them are fuzzy.

**2.5.** Which of the following is the best interpretation of the statement: *Some blue meanies are fuzzy*?

(i) There are blue meanies and at least one of them is fuzzy.

(ii) There are blue meanies and at least two of them are fuzzy.

(iii) There are blue meanies and all of them are fuzzy.

(iv) There may not be any blue meanies, but if there are at least one of them is fuzzy.

(v) There may not be any blue meanies, but if there are at least two of them are fuzzy.

(vi) There may not be any blue meanies, but if there are all of them are fuzzy.

**2.6.** Using the proof of Theorem 2.1 as an example, prove Theorem 2.2.

**2.7.** Rewrite the proof of Theorem 2.3 in paragraph format.

**2.8.** Using the proof of Theorem 2.3 as an example, prove Theorem 2.4.

**2.9.** Prove the following:

(i) Some prime number is even.

(ii) There is an integer whose square is not positive.

(iii) There is a city $A$ in North Dakota that is further south than Paris, France.

(iv) There are positive integers $a$ and $b$ such that $ab < a + b$.

(v) There are irrational numbers $a$ and $b$ such that the sum $a + b$ is rational.

**2.10.** Show that the following are false:

(i) Every student in this class has green hair.

(ii) For every real number $x$, $x^2 - 1 \geq 0$.

(iii) Every prime number is less than 1000.

(iv) For all irrational numbers $a$ and $b$, the product $ab$ is irrational.

(v) For all prime numbers $n$ and $m$, the sum $n + m$ is composite.

**2.11.** To show that the statement $\forall x\ P(x)$ is false, it suffices to show that there is an $c$ in the domain of $x$ such that $\neg P(c)$; the value $c$ is called a counterexample. Assume that we believe the statement $\exists x\ P(x)$ is false. Can we prove this by finding a $c$ in the domain of $x$ such that $\neg P(c)$? Justify your answer.

**2.12.** Use induction to prove that $\sum_{i=0}^{n} 2^i = (2^{n+1} - 1)$ for every natural number $n$.

**2.13.** Prove that $\sum_{i=1}^{n} i^2 = \dfrac{n(n+1)(2n+1)}{6}$ for every natural number $n$.

**2.14.** Use induction to prove that $2n \leq 2^n$ for every natural number $n$.

**2.15.** It is sometimes true that statements about the natural numbers are not true for small numbers, but are true for all natural numbers that are large enough. We can modify the Principle of Mathematical Induction so that it is applicable in these situations as follows:

Let $P(n)$ be a statement about the natural number $n$.

(i) If $P(a)$ is true, and

(ii) if $P(k) \implies P(k+1)$ for all $k \geq a$,

then $P(n)$ is true for all natural numbers $n \geq a$.

Use this version of induction to prove that $3^n < n!$ for every integer $n \geq 7$.

Chapter 3

# Set Theory

> Later mathematicians will regard set theory as a disease from which we have recovered.
>
> *Henri Poincaré*

> …No one shall be able to drive us from the paradise that Cantor created for us.
>
> *David Hilbert*

## Introduction

After the work of Newton and Leibniz in the early 18th century, there was rapid progress in analysis and the theory of functions. In the 19th century, mathematicians began to find examples that challenged their intuitive understanding of functions, continuity, and infinite series. The work of Cantor, Dedekind, Weierstrass, and others in the last half of the 19th century eventually allowed all of mathematics to be based on a common foundation. Based on the ideas and insights of Georg Cantor, the new theory of sets was not immediately accepted by all mathematicians of the day. The most serious problem was that Cantor treated infinite sets as objects and defined operations on those objects. Gauss, Poincaré, and Kronecker were among the mathematical greats who attacked set theory, sometimes in a particularly vicious and personal way. Other mathematicians, notably Weierstrass and Dedekind, were early supporters of Cantor's work. Cantor was unable to obtain a position at any of Germany's prestigious research universities and spent his entire 44 year academic career in a relatively minor position. Distraught over continuing

resistance to his work, Cantor had a breakdown and spent the last years of his life in a mental institution.

# 3.1 What is a Set?

## 3.1.1 Naive set theory

Early work with sets assumed only that any collection that could be clearly specified (there is a rule for determining whether or not something is in the collection) could be considered a set, and that two sets were the same if they contained the same elements. These properties are sufficient to allow most mathematicians to study the groups or fields or topological spaces they are interested in. The finer points of what actually is, or is not, a set just don't come up most of the time. A mathematician should be aware, however, that there are in fact some restrictions. Perhaps the most important is that sets are not allowed to be elements of themselves.

## 3.1.2 Russell's Paradox

In 1902, philosopher and mathematician Bertrand Russell published his famous paradox. Closely related to the Liar's Paradox, Russell's Paradox exploits a form of self-reference. More specifically, the paradox works only if we allow the possibility that a set might be an element of itself. To avoid this kind of problem, we will not allow any set to be an element of itself. We will talk more about Russell's version of this paradox later, but for now let's deal with a popularization that doesn't depend so much on the language of sets.

**Example 3.1. The Barber's Paradox.** *A certain small town has only one barber. He shaves only those men in town who do not shave themselves. Who shaves the barber?*

# 3.2 Elements and Subsets

## 3.2.1 Elements

We will think of a set as a collection of objects, called it's *elements*. These objects might be points, numbers, people, kitchen appliances, other sets, or any other objects we are interested in talking about. For a set to be well-defined, we must have

a way to determine whether or not a given object is in the set. We consider two sets to be equal if they contain exactly the same elements. Note that an object is either an element of a set or not, the elements of a set do not occur in a particular order and the same object cannot be an element of the set more than once.

One way to indicate a set is to simply list all of the elements between set braces $\{$ and $\}$. The set of positive integers less than 3 is $\{1,2\}$. We will find it useful to have a special notation for the set which has no elements. To this end, let $\emptyset = \{\}$.

**Example 3.2.** *Let* $A = \{1,2,4,8\}$, $B = \{8,2,1,4\}$, $C = \{1,2,1,4,8\}$, *and* $D = \{1,2,3,4,8\}$. *Of these sets,* $A = B = C$ *because they each contain the same elements. It doesn't matter that we listed the elements in a different order when we defined* $A$ *than when we defined* $B$*, or that we listed* $1$ *as an element of* $C$ *more than once. The set* $D$ *is different from the others since it contains the element* $3$ *and the other sets do not.*

**Example 3.3.** *Let* $X = \{1,2,\{2\}\}$. *Note that this set contains some elements that are numbers and some elements that are sets of numbers. We consider those different objects. For example* $1$ *is an element of* $X$*, but* $\{1\}$ *is not an element of* $X$*. On the other hand, both* $2$ *and* $\{2\}$ *are elements of* $X$.

We indicate that the object $x$ is an element of the set $A$ by writing $x \in A$. We write $x \notin A$ if $x$ is not an element of $A$. Listing all of the elements of a set works well when the set contains only a few elements, but what about sets with many elements? In this case, we use *set builder* notation to denote the set. An important part of this notation is the use of the vertical bar $|$ (some texts use a colon in place of the vertical bar), read "such that." So the set $A = \{x \mid x^2 - 2 = 0\}$ is read "the set of all elements $x$ such that $x^2 - 2 = 0$." An object will be an element of this set if and only if it satisfies the equation $x^2 - 2 = 0$.

There are also a few sets that are useful enough to deserve their ownspecial notation. In particular, $\mathbb{N}$ denotes the set of natural numbers, $\mathbb{Z}$ the set of integers, $\mathbb{Q}$ the set of rational numbers, $\mathbb{R}$ the set of real numbers, and $\mathbb{C}$ the set of complex numbers.

### 3.2.2 Subsets

**Definition.** Given two sets $A$ and $B$ we say that $A$ is a *subset* of $B$, or that $A$ is contained in $B$, if every element of $A$ is also an element of $B$. In this case we write $A \subset B$ (sometimes $A \subseteq B$).

Since every natural number is also an integer and every integer is a real number, $\mathbb{N} \subset Z$ and $\mathbb{Z} \subset R$.

**Example 3.4.** *Define the sets* $A = \{1,2,3\}$, $B = \{1,2,\{3\},4\}$, *and* $C = \{1,2,3,\{4\}\}$. *Then* $A$ *is a subet of* $C$ *because each element of* $A$ *is also an element of* $C$. *Note that* $A$ *is not a subset of* $B$ *because* $3$ *is an element of* $A$, *but not an element of* $B$ *- remember that* $3$ *and* $\{3\}$ *are different objects.*

Given any set $A$, it is certainly true that every element of $A$ is an element of $A$. In other words, every set is a subset of itself. Note also that the empty set is a subset of every set $A$ since there are no elements of the empty set which are not in $A$.

**Definition.** A subset $B$ of $A$ is said to be a *proper subset* of $A$ if $B \neq \emptyset$ and $B \neq A$.

**Theorem 3.1.** *If* $A \subset B$ *and* $B \subset C$, *then* $A \subset C$.

*Proof.* Suppose that $a \in A$. Since $A \subset B$ it follows that $a \in B$. Now $B \subset C$, so we may say that $a \in C$ as desired. □

The preceding proof is a simple example of a direct proof. Let's pause for a moment and analyze this proof. The statement we want to prove is a universally quantified statement about elements of $A$: every element of $A$ is also an element of $C$. We begin by considering an arbitrary element of $A$, which we have named $a$. The goal is to use our hypotheses ($A \subset B$ and $B \subset C$) to arrive at the conclusion that $a \in C$. First we note that every element of $A$ is also an element of $B$ since $A \subset B$. This allows us to state that $a \in B$. Once we have $a \in B$ we may use the second hypothesis to see that $a \in C$ since $B \subset C$. So starting with any element at all of the set $A$ we have shown that it must also be an element of $C$, which is the definition of $A \subset C$. We conclude that $A \subset C$ as desired.

Note that the preceding proof is a syllogism: *All elements of* $A$ *are elements of* $B$. *All elements of* $B$ *are elements of* $C$. *Hence all elements of* $A$ *are elements of* $C$. This is certainly not true of all direct proofs, but is true on occasion.

### 3.2.3 Universal sets

In many instances, all of the sets we may be interested in are subsets of some particular set $U$. In this case we say that $U$ is a *universal set*, or that $U$ is the *universe*. For example, all of the functions we study in single variable calculus have domains and ranges that are subsets of the universal set $\mathbb{R}$.

### 3.2.4 Equality of sets

We say that two sets are equal if they contain exactly the same elements. In other words, $A = B$ means that every element of $A$ is an element of $B$ and every element of $B$ is an element of $A$. In other words, we have the following:

**Theorem 3.2.** *Given any two sets $A$ and $B$, $A = B$ if and only if $A \subset B$ and $B \subset A$.*

This theorem will become one of our most valuable tools for showing that two sets are equal.

## 3.3 Operations on Sets

### 3.3.1 Union and intersection

**Definition.** The *union* of two sets $A$ and $B$ is the set:

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$$

**Definition.** The *intersection* of $A$ and $B$ is the set:

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$$

Before proceding we note that $P \vee Q$ is equivalent to $Q \vee P$, so it follows immediately from our definition that $A \cup B = B \cup A$. Similarly we have $A \cap B = B \cap A$ since $P \wedge Q$ is equivalent to $Q \wedge P$.

**Example 3.5.** *Define $A = \{1,2,3,4,5\}$ and $B = \{2,4,6,8,10\}$. Then*

$$A \cup B = \{1,2,3,4,5,6,8,10\} \text{ and } A \cap B = \{2,4\}.$$

The following theorem summarizes several useful algebraic properties of unions and intersections.

**Theorem 3.3.** *Let $A$, $B$, and $C$ be any sets in the universal set $U$. Then:*

*(i) (Commutative Laws)*

*(a)* $A \cup B = B \cup A$

*(b)* $A \cap B = B \cap A$

*(ii) (Associative Laws)*

*(a)* $A \cup (B \cup C) = (A \cup B) \cup C$

*(b)* $A \cap (B \cap C) = (A \cap B) \cap C$

*(iii) (Distributive Laws)*

*(a)* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

*(b)* $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

*(iv) (Idempotence)*

*(a)* $A \cup A = A$

*(b)* $A \cap A = A$

*(v) (Identities)*

*(a)* $A \cup \emptyset = A$

*(b)* $A \cap U = A$

*Proofs.* We prove some of these properties here and leave the remainder for the exercises.

**Commutative Laws.** The Commutative Laws follow immediately from our defintions as noted in the text.

**Associative Laws.** We prove the Associative Law for unions here. Rather than applying Theorem 3.2, we show that $(x \in A \cup (B \cup C)$ is equivalent to $x \in (A \cup B) \cup C$ using the associativity of disjunction at $(*)$

$$\begin{aligned} x \in A \cup (B \cup C) &\Leftrightarrow (x \in A) \vee (x \in B \cup C) \\ &\Leftrightarrow (x \in A) \vee \big((x \in B) \vee (x \in C)\big) \\ &\Leftrightarrow \big((x \in A) \vee (x \in B)\big) \vee (x \in C) \qquad (*) \\ &\Leftrightarrow (x \in A \cup B) \vee (x \in C) \\ &\Leftrightarrow x \in (A \cup B) \cup C \end{aligned}$$

**Distributive Laws.** We show that union distributes over intersection using the fact that disjunction distributes over conjunction at $(**)$.

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow (x \in A) \vee (x \in B \cap C) \\ &\Leftrightarrow (x \in A) \vee \big((x \in B) \wedge (x \in C)\big) \\ &\Leftrightarrow \big((x \in A) \vee (x \in B)\big) \wedge \big((x \in A) \vee (x \in C)\big) \qquad (**) \\ &\Leftrightarrow (x \in A \cup B) \wedge (x \in A \cup C) \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C) \end{aligned}$$

**Idempotence.** We prove that $A \cap A = A$. This time we make use of Theorem 3.2. Assume first that $x \in A \cap A$, then by definition $x \in A$ and $x \in A$. From this we may deduce that $x \in A$. Since this is true for every $x \in A \cap A$, we have shown that $A \cap A \subset A$. Now assume that $y \in A$, then we have $y \in A$ and $y \in A$. It follows that $y \in A \cap A$ for every $y \in A$, so $A \subset A \cap A$. We now apply Theorem 3.2 to see that $A \cap A = A$.

**Identities.** We prove here that $A \cup \emptyset = A$. Assume first that $x \in A \cup \emptyset$, then $x \in A$ or $x \in \emptyset$. By definition we know that $x \notin \emptyset$, so it follows that $x \in A$.[1] We have shown that $A \cup \emptyset \subset A$. Now suppose that $y \in A$, then we may deduce that $y \in A$ or $y \in \emptyset$. By definition it follows that $y \in A \cup \emptyset$ and we have shown that $A \subset A \cup \emptyset$. We may now apply Theorem 3.2 to see that $A \cup \emptyset = A$ as desired. □

### 3.3.2 Complements

**Definition.** The *relative complement* of $B$ in $A$ (also called the set difference) is the set:

$$A \setminus B = \{a \mid a \in A \text{ and } a \notin B\}$$

In a given universe $U$, we may also define the *complement* of a set $A$ to be the set:

$$A' = U \setminus A$$

**Theorem 3.4** (DeMorgan)**.** *Let A, B, and C be sets. Then:*

*(i)* $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$, *and*

[1] Which rule of inference allows us to deduce that $x \in A$?

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

*Proof of Theorem 3.4(i).* Rather than using Theorem 3.2 we use Theorem 1.2 to show that an element is in $A \setminus (B \cup C)$ if and only if it is in $(A \setminus B) \cup (A \setminus C)$.

$$\begin{aligned} x \in A \setminus (B \cup C) &\Leftrightarrow (x \in A) \wedge (x \notin B \cup C) \\ &\Leftrightarrow (x \in A) \wedge \neg(x \in B \vee x \in C) \\ &\Leftrightarrow (x \in A) \wedge \big(\neg(x \in B) \wedge \neg(x \in C)\big) \\ &\Leftrightarrow (x \in A) \wedge (x \notin B) \wedge (x \notin C) \\ &\Leftrightarrow \big((x \in A) \wedge (x \notin B)\big) \wedge \big((x \in A) \wedge (x \notin C)\big) \\ &\Leftrightarrow (x \in A \setminus B) \wedge (x \in A \setminus C) \\ &\Leftrightarrow x \in (A \setminus B) \cap (A \setminus C) \end{aligned}$$

□

### 3.3.3 Cartesian products

**Definition.** The *(Cartesian) product* of two sets $A$ and $B$ is the set:

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\},$$

where $(a, b)$ denotes an ordered pair, not an interval.

Note that $A \times B$ is simply the set of all ordered pairs with first coordinates in $A$ and second coordinates in $B$. For example, the Cartesian plane used in Calculus is the set $\mathbb{R} \times \mathbb{R}$.

**Theorem 3.5.** *For any sets A, B, and C:*

*(i)* $(A \cup B) \times C = (A \times C) \cup (B \times C)$

*(ii)* $(A \cap B) \times C = (A \times C) \cap (B \times C)$

*(iii)* $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$

*Proof of Theorem 3.5(i).* First suppose that $(x, y) \in (A \cup B) \times C$. By definition we have $x \in A \cup B$ and $y \in C$. Since $x \in A \cup B$, either $x \in A$ or $x \in B$. If $x \in A$, then we have $x \in A$ and $y \in C$, so $(x, y) \in A \times C$. If $x \in B$, then we have $x \in B$ and $y \in C$, so $(x, y) \in B \times C$. We can now say that

$(x,y) \in A \times C$ or $(x,y) \in B \times C$, so $(x,y) \in (A \times C) \cup (B \times C)$. Hence $(A \cup B) \times C \subset (A \times C) \cup (B \times C)$.

To see that the converse is true, suppose that $(x,y) \in (A \times C) \cup (B \times C)$. Either $(x,y) \in A \times C$ or $(x,y) \in B \times C$. If $(x,y) \in A \times C$, then $x \in A \subset (A \cup B)$ and $y \in C$, so $(x,y) \in (A \cup B) \times C$. If $(x,y) \in B \times C$, then $x \in B \subset (A \cup B)$ and $y \in C$, so $(x,y) \in (A \cup B) \times C$. Hence $(A \times C) \cup (B \times C) \subset (A \cup B) \times C$. Therefore, $(A \cup B) \times C = (A \times C) \cup (B \times C)$ as desired. □

Since $A \times B$ is a set of ordered pairs, $A \times B \neq B \times A$. You should make sure that you look at an example to understand why this is true. This requires us to state another theorem that seems very similar to the last one. The proof of the following theorem involves making obvious changes to the previous proof and checking that all of the details still work.

**Theorem 3.6.** *For any sets A, B, and C:*

*(i)* $A \times (B \cup C) = (A \times B) \cup (A \times C)$

*(ii)* $A \times (B \cap C) = (A \times B) \cap (A \times C)$

*(iii)* $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

It may be tempting to assume that we could combine these two theorems somehow and obtain statements like $(A \times B) \setminus (C \times D) = (A \setminus C) \times (B \setminus D)$. This statement is generally false, however, as shown by the following.

**Example 3.6.** *Let* $A = \{1,2,3\}$, $B = \{5,6\}$, $C = \{1,2\}$, *and* $D = \{6\}$. *Then:*

$$(A \times B) \setminus (C \times D) = \{(1,5),(2,5),(3,5),(3,6)\}$$

*but*

$$(A \setminus C) \times (B \setminus D) = \{(3,5)\}$$

## 3.4 Collections of Sets

Some of the structures used in pure mathematics require the use of sets whose elements are other sets. It is customary, though not necessary, to refer to these kinds of sets as collections of sets. When working with sets and collections of sets, it can be particularly confusing to keep track of which set is an element of which other set, as opposed to being a subset.

### 3.4.1 The power set of a set

**Definition.** Let $A$ be any set. The *power set* of $A$ is the set $\mathcal{P}(A) = \{B \mid B \subset A\}$.

In words, the power set of $A$ is the set whose elements are the subsets of $A$. Note that for any set $A$ we have $\emptyset \in \mathcal{P}(A)$ and $A \in \mathcal{P}(A)$, so $\mathcal{P}(A)$ is nonempty for every set $A$. The power set of $A$ is frequently denoted $2^A$.

**Theorem 3.7.** *For any sets $A$ and $B$, $A \subset B$ if and only if $\mathcal{P}(A) \subset \mathcal{P}(B)$.*

*Proof.* First assume that $A \subset B$ and let $X \in \mathcal{P}(A)$. By definition $X \subset A$, so Theorem 3.1 implies that $X \subset B$. Hence $X \in \mathcal{P}(B)$ and $\mathcal{P}(A) \subset \mathcal{P}(B)$. Conversely, if we assume that $\mathcal{P}(A) \subset \mathcal{P}(B)$, then $A \in \mathcal{P}(A) \subset \mathcal{P}(B)$ and $A \subset B$ by definition. □

**Theorem 3.8.** *For any sets $A$ and $B$, $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.*

*Proof.* First note that $A \cap B \subset A$ by Exercise 3.9, so Theorem 3.7 implies that $\mathcal{P}(A \cap B) \subset \mathcal{P}(A)$. The same reasoning shows that $\mathcal{P}(A \cap B) \subset \mathcal{P}(B)$, so we have $\mathcal{P}(A \cap B) \subset \mathcal{P}(A) \cap \mathcal{P}(B)$ by Exercise 3.10.

Now suppose that $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$, then $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$. By definition $X \subset A$ and $X \subset B$, so $X \subset A \cap B$ by Exercise 3.10. It follows that $\mathcal{P}(A \cap B) \supset \mathcal{P}(A) \cap \mathcal{P}(B)$, so $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$ as desired. □

# Chapter 3 Exercises

**3.1.** Explain why there is no consistent answer to the question in Example 3.1.

**3.2.** Here are some common infinite sets:
$P = \{n \mid n \text{ is prime}\}$ is the set of all prime numbers.
$E = \{n \mid n = 2k \text{ for some } k \in \mathbb{Z}\}$ is the set of all even integers.

How would you write the set of all odd integers in set builder notation? What about the set of all integer powers of 2?

**3.3.** Let $A = \{1, 2, \{1,2\}, \{1,3\}, 4\}$. Determine whether each of the following is en element of $A$, a subset of $A$, both an element of $A$ and a subset of $A$, or neither an element of $A$ nor a subset of $A$.

(i) $1$

(ii) $3$

(iii) $\{1\}$

(iv) $\{1,2\}$

(v) $\{1,3\}$

(vi) $\{1,4\}$

**3.4.** Let $A$ and $B$ be sets and suppose you know that $A$ is not a subset of $B$. Which of the following is necessarily true? Choose all correct responses.

(i) If $x \in A$, then $x \notin B$.

(ii) If $x \in B$, then $x \in A$.

(iii) There is an element $x \in A$ so that $x \notin B$.

(iv) There is an element $x \in B$ so that $x \notin A$.

**3.5.** Let $A$ and $B$ be sets and suppose that $x \notin A \cup B$. Which of the following is necessarily true? Choose all correct responses.

(i) $x \notin A$ or $x \notin B$

(ii) $x \notin A$ and $x \notin B$

(iii) $x \in A$ or $x \in B$

(iv) $x \in A$ and $x \in B$

**3.6.** Let $A$ and $B$ be sets and suppose that $x \notin A \cap B$. Which of the following is necessarily true? Choose all correct responses.

(i) $x \notin A$ or $x \notin B$

(ii) $x \notin A$ and $x \notin B$

(iii) $x \in A$ or $x \in B$

(iv) $x \in A$ and $x \in B$

**3.7.** Define the following sets: $A = \{1,3,9,27\}$, $B = \{1,2,4,8\}$, $P = \{n \mid n \text{ is a prime integer}\}$, and $E = \{n \mid n = 2k \text{ for some } k \in \mathbb{N}\}$. Find each of the following:

(i) $A \cup B$

(ii) $A \cap B$

(iii) $P \cap E$

**3.8.** Prove the following parts of Theorem 3.3.

(i) Theorem 3.3 ii (b)

(ii) Theorem 3.3 iii (b)

(iii) Theorem 3.3 iv (a)

(iv) Theorem 3.3 v (b)

**3.9.** For any sets $A$ and $B$, prove that:

(i) $A \subset A \cup B$

(ii) $A \cap B \subset A$

(iii) $A \cap \emptyset = \emptyset$

**3.10.** Let $A$, $B$, and $C$ be sets. Prove that $A \subset B \cap C$ if and only if $A \subset B$ and $A \subset C$.

**3.11.** Let $A$, $B$, and $C$ be sets. Prove that if $A \subset B \cup C$ and $A \cap B = \emptyset$, then $A \subset C$.

**3.12.** Prove part (ii) of Theorem 3.4.

**3.13.** Let $A$ and $B$ be sets in a universal set $U$. Prove the following:

(i) $A \setminus B = A \cap B'$

(ii) $A \setminus B = A$ if and only if $A \cap B = \emptyset$.

(iii) $A \setminus B = \emptyset$ if and only if $A \subset B$.

**3.14.** Prove the following:

(i) Theorem 3.5(ii)

(ii) Theorem 3.5(iii)

**3.15.** Determine whether or not each of the following is true. If so, provide a proof. If not, provide a counterexample.

(i) $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)$

(ii) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

**3.16.** Let $A$ and $B$ be sets.

(i) Show that $\mathcal{P}(A) \cup \mathcal{P}(B) \subset \mathcal{P}(A \cup B)$.

(ii) Show that $\mathcal{P}(A \cup B)$ is not generally a subset of $\mathcal{P}(A) \cup \mathcal{P}(B)$.

Chapter 4

# Relations

> The power of mathematics is often to change one thing into another, to change geometry into language.
>
> *Marcus du Sautoy*

> Mathematics is the art of giving the same name to different things.
>
> *Henri Poincar e*

## Introduction

The first mathematical relation most students become aware of is the standard order on the natural numbers, which is later extended to the integers and finally the reals. A relation is a much more general concept, and by now you have probably worked with several others, perhaps without thinking about them as relations. In this chapter we define what we mean by a relation between sets, then define an equivalence relation on a set and use that idea to develop the set of rational numbers.

## 4.1 Relations

**Definition.** Given two sets $A$ and $B$, a *relation* from $A$ to $B$ is a subset of $A \times B$. The relations we will be most interested in are usually from a set $A$ to itself, in which case we say that the relation is a relation on $A$. If $S$ is a relation, we frequently use the notation $xSy$ to indicate that the ordered pair $(x, y)$ is in $S$.

Let's look at some examples of relations.

**Example 4.1.** *The usual ordering $<$ on $\mathbb{R}$ is a relation on $\mathbb{R}$. We don't usually think of this relation as a set of ordered pairs, but we could. Define a subset $L$ of $\mathbb{R} \times \mathbb{R}$ by $L = \{(a,b) \mid b - a \text{ is positive}\}$. In other words, an ordered pair $(a,b)$ is in the relation if $a < b$.*

**Example 4.2.** *The set of points on a circle is another example of a relation on $\mathbb{R}$. For example, we could let $C = \{(x,y) \mid x^2 + y^2 = 1\}$.*

**Example 4.3.** *A relation need not be something you've encountered before or that you necessarily have a use for. Let $A$ denote the set of people in this room, and $B$ the set of possible hair colors. One might define a relation $H$ from $A$ to $B$ by: $H = \{(x,y) \mid y \text{ is } x\text{'s hair color}\}$.*

**Definition.** Let $A$ be a nonempty set and let $\sim$ be a relation on $A$. We say that $\sim$ is:

(i) *reflexive* if $a \sim a$ for every $a \in A$;

(ii) *symmetric* if $a \sim b$ implies $b \sim a$ for every $a, b \in A$;

(iii) *antisymmetric* if $a \sim b$ and $b \sim a$ imply $a = b$ for every $a, b \in A$.

(iv) *transitive* if $a \sim b$ and $b \sim c$ imply $a \sim c$ for every $a, b, c \in A$.

Note that symmetry and antisymmetry are not logical opposites, though the names may lead you to believe otherwise. It is possible for a relation to satisfy both of these properties, or to satisfy neither of them.

**Example 4.4.** *Let $<$ denote the relation "less than" on $\mathbb{R}$. Determine which of the properties listed above are satisfied by $<$.*

- *$<$ is not reflexive since $1 \not< 1$*
- *$<$ is not symmetric since $1 < 7$ and $7 \not< 1$*
- *$<$ is antisymmetric because the hypotheses $a < b$ and $b < a$ are never both satisfied*
- *$<$ is transitive since $a < b$ and $b < c$ implies that $a < c$*

## 4.2 Equivalence Relations

Consider the following question: Are $\pi/4$ and $25\pi/4$ measurements of the same angle? It's certainly true that when we place these angles in standard position they have the same terminal side, which means that we can treat them as the same much of the time. On the other hand, if we think of the angle as a rotation, these two angles are certainly different. If you're playing pin the tail on the donkey, being spun through an angle of $25\pi/4$ is going to make you dizzier than being spun through an angle of $\pi/4$. Intuitively, the terminal side of the angle in this setting tells us what direction we end up pointing in. The angle tells us how far we rotated to end up pointing in that direction. When we are only concerned with the terminal side of an angle, how do we tell when two numbers are measures for *equivalent* angles? You probably learned in a trigonometry or precalculus class that two measurements represent equivalent angles when they differ by an integer multiple of $2\pi$. In other words, two angles $\alpha$ and $\beta$ are said to be *equivalent* when there is an integer $n$ such that $\alpha - \beta = 2\pi n$. In the following example we consider this relation between real numbers.

**Example 4.5.** *For $x, y \in \mathbb{R}$ we define $x \sim y$ if there is an integer $n$ such that $x - y = 2\pi n$. Show that $\sim$ is reflexive, symmetric, and transitive.*

- *For any $x \in \mathbb{R}$ we have $x - x = 0 = 2\pi(0)$. Since $0 \in \mathbb{Z}$, $x \sim x$ and $\sim$ is relexive.*

- *Suppose that $x \sim y$, then there is an $n \in \mathbb{Z}$ so that $x - y = 2\pi n$. It follows that $y - x = 2\pi(-n)$. Since $-n \in \mathbb{Z}$ we have $y \sim x$ and $\sim$ is symmetric.*

- *Let $x, y, z \in \mathbb{R}$; assume that $x \sim y$ and $y \sim z$. By definition there are integers $n, m \in \mathbb{Z}$ such that $x - y = 2\pi n$ and $y - z = 2\pi m$. It follows that:*

$$x - z = (x - y) - (y - z) = 2\pi n + 2\pi m = 2\pi(n + m)$$

  *Now we have $x \sim z$, which shows that $\sim$ is transitive.*

**Definition.** A relation on a set $A$ that is reflexive, symmetric, and transitive is said to be an *equivalence relation* on $A$.

### 4.2.1 Equivalence classes

**Definition.** Let $A$ be a set and let $\sim$ be an equivalence relation on $A$. For any $a \in A$ the set $[a] = \{b \in A \mid b \sim a\}$ is called the *equivalence class* of $a$.

Given a set $A$ and an equivalence relation on $A$, the set of equivalence classes form a *partition* of the set $X$. In other words, the collection of equivalence classes is a collection of nonempty subsets of $A$ with the proprties that every element of $A$ is in some equivalence class and no two distinct equivalence classes intersect each other. We formalize this in the following theorem:

**Theorem 4.1.** *Let $A$ be a nonempty set and $\sim$ an equivalence relation on $A$. For each $a \in A$, let $[a] = \{b \in A \mid a \sim b\}$.*

*(i) For each $a \in A$, $a \in [a]$.*

*(ii) If $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$.*

*Proof of (i).* Since $\sim$ is reflexive, $a \sim a$ for each $a \in A$. By definition this implies that $a \in [a]$ and (i) is satisfied. □

*Proof of (ii).* Suppose that $[a] \cap [b] \neq \emptyset$ and let $c \in [a] \cap [b]$. Then $c \sim a$ and $c \sim b$.

Since $c \sim a$ and $\sim$ is symmetric, it follows that $a \sim c$. Now we have $a \sim c$ and $c \sim b$, so $a \sim b$ by transitivity. Let $x \in [a]$, then $x \sim a$ by definition. From transitivity it follows that $x \sim b$, so $x \in [b]$. Hence $[a] \subset [b]$.

Since $a \sim b$, it must also be true that $b \sim a$ by symmetry. Let $y \in [b]$, then $y \sim b$ by definition. From transitivity it follows that $y \sim a$, so $y \in [a]$. Hence $[b] \subset [a]$.

Since $[a] \subset [b]$ and $[b] \subset [a]$, $[a] = [b]$ by Theorem 3.2. □

**Example 4.6.** *Consider the equivalence relation $\equiv_5$ of Exercise 4.2 there are five equivalence classes associated with this equivalence relation:*

$$[0] = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$
$$[1] = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$$
$$[2] = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$$
$$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$$
$$[4] = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$$

*The equivalence classes are sets of integers that have the same remainder when divided by 5.*

In the previous example, note that we had several ways to refer to each equivalence class. For example $[1] = [16]$, so we may as well have used $[16]$ as a name for this equivalence class. In this context the numbers 1 and 16 (or any other member of the class) are called *representatives* of this equivalence class, and any representative can be used to name the equivalence class.

## 4.3 The rational numbers

In this section we are going to show how to use the ideas in this chapter to construct the set of rational numbers. We assume that the sets $\mathbb{N}$ of natural numbers and $\mathbb{Z}$ of integers are given and have their usual properties.[1] Note that in this text the number 0 is not an element of the set of natural numbers. We will use the characterization of the rationals as the set of numbers that can be expressed as a fraction of integers, so we begin by defining the set $\mathbb{F} = \mathbb{Z} \times \mathbb{N}$. Note that $\mathbb{F}$ is the set of all ordered pairs $(a, b)$ where $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. We want to think of $\mathbb{F}$ as a set of fractions of integers, so we denote an ordered pair $(a, b) \in \mathbb{F}$ by $a/b$ or $\frac{a}{b}$.

Note that a fraction is not quite the same thing as a rational number, for example $1/2$ and $3/6$ are different fractions that represent the same rational number. We define an equivalence relation $\cong$ on $\mathbb{F}$ that clarifies when two fractions represent the same rational as follows:

**Definition.** Given two fractions $a/b$ and $c/d$ in $\mathbb{F}$, we say that $a/b \cong c/d$ if $ad = bc$.

**Theorem 4.2.** *The relation $\cong$ is an equivalence relation on $\mathbb{F}$.*

*Proof.* To see that $\cong$ is reflexive, note that for every $a/b \in \mathbb{F}$ we have $ab = ba$, so $a/b \cong a/b$.

Now suppose that $a/b \cong c/d$, then by definition $ad = bc$. Using the fact that multiplication is commutative we see that $cb = da$, so $c/d \cong a/b$ and $\cong$ is symmetric.

It remains to show that $\cong$ is transitive, which is a little bit more work. Assume that $a/b \cong c/d$ and $c/d \cong e/f$, then by definition we have $ad = bc$ and $cf = de$. We multiply equal expressions, then perform some algebra, making sure that we

[1] For an axiomatic development of the natural numbers and integers, see [D] or [H].

do not try to divide by 0:

$$\begin{aligned}(ad)(cf) &= (bc)(de)\\ (af)(cd) &= (be)(cd)\\ af &= be\end{aligned}$$

Now we have $a/b \cong e/f$ and $\cong$ is transitive as desired. □

We now define the set of rationals to be the set of equivalence classes of fractions. In this construction the two fractions $1/2$ and $3/6$ do indeed represent the same rational number since they are representatives of the same equivalence class. This construction might be a bit unsatisfying in the sense that it tells us nothing about how we might add or multiply rational numbers. Even if we know how to add fractions, how would we add two equivalence classes of fractions? One possibility is that we might add two equivalence classes by adding their representatives, so for example we might try:

$$\left[\frac{1}{2}\right] \oplus \left[\frac{2}{3}\right] = \left[\frac{1(3)+2(2)}{2(3)}\right] = \left[\frac{5}{6}\right]$$

There is a potential problem with this, though. There are infinitely many choices of fractions representing each rational number. Are we sure that we arrive at the same result for all of those possible choices? The next theorem says that we do.

**Theorem 4.3.** *Suppose that $a/b \cong x/y$ and $c/d \cong w/z$, where $a/b$, $c/d$, $x/y$, and $w/z$ are all in $\mathbb{F}$, then:*

$$\frac{ad+bc}{bd} \cong \frac{xz+yw}{yz}.$$

*Proof.* By hypothesis we have $ay = bx$ and $cz = dw$. We want to show that $(ad+bc)(yz) = (bd)(xz+yw)$. Using our hypotheses we have:

$$\begin{aligned}(ad+bc)(yz) &= (ad)(yz)+(bc)(yz)\\ &= (ay)(dz)+(cz)(by)\\ &= (bx)(dz)+(dw)(by)\\ &= (bd)(xz)+(bd)(yw)\\ &= (bd)(xz+yw),\end{aligned}$$

which completes the proof. □

The proof of the following theorem is left for exercise 4.6.

**Theorem 4.4.** *Suppose that $a/b \cong x/y$ and $c/d \cong w/z$, where $a/b$, $c/d$, $x/y$, and $w/z$ are all in $\mathbb{F}$, then:*

$$\frac{ac}{bd} \cong \frac{xw}{yz}.$$

Theorems 4.3 and 4.4 allow us to make the following definitions, where we may choose any representative from each equivalence class.

**Definition.** Let $[a/b]$ and $[c/d]$ be rational numbers, then we define addition and multiplication by:

$$\left[\frac{a}{b}\right] \oplus \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right] \quad \text{and} \quad \left[\frac{a}{b}\right] \otimes \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right].$$

# Chapter 4 Exercises

**4.1.** Determine whether or not each of the following relations is reflexive, symmetric, antisymmetric, and/or transitive. Are any of these equivalence relations?

(i) The relation $\leq$ on $\mathbb{R}$.

(ii) Equality on $\mathbb{R}$, i.e. the set of ordered pairs of real numbers whose first and second coordinates are equal.

(iii) The relation $\mid$ on $\mathbb{N}$, where $a \mid b$ means that $b = an$ for some $n \in \mathbb{N}$.

(iv) The relation $\sim$ on $\mathbb{N}$ defined by $a \sim b$ if there is an integer $n > 1$ that evenly divides both $a$ and $b$.

**4.2.** Define the relation $\equiv_5$ on $\mathbb{Z}$ by: $a \equiv_5 b$ if there is an integer $n$ so that $b - a = 5n$. Show that $\equiv_5$ is an equivalence relation on $\mathbb{Z}$. Note: this is a fairly common equivalence relation. The phrase $a \equiv_5 b$ is usually read "$a$ is equivalent to $b$ modulo 5."

**4.3.** A relation on a set $X$ is said to be a *partial order* on $X$ if it is reflexive, antisymmetric, and transitive. Let $X = \mathcal{P}(\mathbb{R})$ and consider the inclusion relation defined by $A \subset B$.

(i) Show that $\subset$ is a partial order on $X$.

(ii) Is strict inclusion $\subsetneq$ a partial order on $X$?

**4.4.** Define a relation $\sim$ on $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ by $(x, y) \sim (w, z)$ if $x^2 + y^2 = w^2 + z^2$. Show that $\sim$ is an equivalence relation on $\mathbb{R}^2$.

**4.5.** Consider the equivalence relation defined in Exercise 4.4. For each point $(x, y) \in \mathbb{R}^2$, the equivalence class $[(x, y)]$ is a familiar geometric figure in $\mathbb{R}^2$. What is it?

**4.6.** Prove Theorem 4.4.

Chapter 5

# Functions

> It is indeed a surprising and fortunate fact that nature can be expressed by relatively low-order mathematical functions.
>
> *Rudolf Carnap*

> As far as the laws of mathematics refer to reality, they are not certain; and as far as they are certain, they do not refer to reality.
>
> *Albert Einstein*

## 5.1 Introduction

As anybody who has taken a calculus class knows, functions are important in mathematics. In this chapter we will define a function between two sets as a special type of relation between those sets. This definition grew from attempts to resolve various paradoxes that were discovered in the 19th century that challenged the intuitive characterizations of functions that were accepted at the time.

## 5.2 Definition

You probably think of functions in several ways based on what you have seen in previous courses. Functions can be rules for computing things, some people think of them as machines (plug in one number and get out another), and of course we all know that a graph is only the graph of a function if it passes the vertical line test. Most of these ideas match the way that mathematicians thought of functions

(and the way they worked with them) at some time or another. It wasn't until the late 19th century that the concept of a function was defined in terms of sets. We present such a definition here:

**Definition.** Let $A$ and $B$ be sets. A *function* $f$ from $A$ to $B$ is a relation from $A$ to $B$ with the additional property that for each $a \in A$ there is exactly one ordered pair $(a,b)$ in $f$ having $a$ as a first coordinate. In this case, the set $A$ is called the *domain* of $f$ and the set $B$ is called the *codomain* of $f$. If $f$ is a function from $A$ to $B$, we denote this by writing $f : A \to B$.

Do not confuse the codomain of a function with its range. The codomain of a function is the set that second coordinates must come from. The range is the subset of the codomain containing all of those second coordinates. Sometimes those sets are the same, but sometimes they are not.

Note that our definition requires that every element of the domain be the first coordinate of one, and only one, ordered pair in a function. It does not, however, require that each element of the codomain be a second coordinate, or that it be the second coordinate of only one ordered pair. Satisfying these requirements would make our function surjective or injective, respectively. We discuss these kinds of functions in Section 5.3.

Before going any further, let's consider a couple of examples.

**Example 5.1.** *Consider the sets* $A = \{1,2,3,4\}$ *and* $B = \{1,3,5,7\}$. *Define the following relations from* $A$ *to* $B$*:*

*(i)* $f = \{(1,3),(2,1),(3,5),(4,7)\}$

*(ii)* $g = \{(1,1),(3,3)\}$

*(iii)* $h = \{(1,1),(2,3),(3,5),(4,1)\}$

*(iv)* $j = \{(1,1),(2,3),(3,5),(4,7),(2,7)\}$

*(v)* $Pat = \{(1,1),(2,3),(3,5),(4,7),(1,1)\}$

*The relation* $f$ *is certainly a function. Each element of* $A$ *is a first coordinate of one and only one ordered pair.*

*The relation* $g$ *is not a function because 2 and 4 are elements of* $A$*, but are not first coordinates of ordered pairs.*

*The relation* $h$ *is a function. The fact that 1 is a second coordinate of two ordered pairs, or that 7 is not the second coordinate of any, do not violate our definition.*

*The relation $j$ is not a function because 2 is the first coordinate of two distinct ordered pairs.*

*Finally, Pat is also a function. We make two comments here. First, the fact that the ordered pair $(1,1)$ is listed twice does not violate our definition of a function. Each ordered pair is either in the relation or not, it cannot be two distinct elements of the relation. Second, while we will usually use letters like $f$ or $g$ to denote functions, and adhering to this convention makes life easier for us, there is no real requirement that we do so. We can name a relation, and thus also a function, in some other manner if there is a reason to do so.*

The functions in the previous example are obviously constructed to fit the definition, but may not strike you as the kinds of things you think of as functions. What about the kinds of functions we are used to?

**Example 5.2.** *Define the following relations from $\mathbb{R}$ to $\mathbb{R}$.*

*(i)* $f = \{(x,y) \mid x \in \mathbb{R} \text{ and } y = x^2\}$

*(ii)* $g = \{(x,y) \mid x \in \mathbb{R} \text{ and } x = y^2\}$

*The relation $f$ is a function (make sure you understand why). In fact, it is a function that should be familiar to you. The second coordinates are squares of the first coordinates, so this is the usual squaring function on $\mathbb{R}$.*

*The relation $g$ is not a function from $\mathbb{R}$ to $\mathbb{R}$. Despite appearances, there are elements of $\mathbb{R}$ which are not first coordinates: $-1$ is one such element, but any negative number will do. This relation also violates our definition in another way. Both $(4,2)$ and $(4,-2)$ satisfy the definition of $g$, so 4 is the first coordinate of more than one ordered pair in $g$. In fact, every positive real number is the first coordinate of two ordered pairs in $g$.*

It probably seems unnatural to you to write the squaring function $f : \mathbb{R} \to \mathbb{R}$ as we did in Example 5.2. Wouldn't it be easier to write this function as $f(x) = x^2$, the same way we did in algebra or calculus classes? Once we know that $f$ is a function, we can use this notation.

Suppose that $f : A \to B$ is a function. If $a \in A$ and $(a,b) \in f$, we say that $b$ is the *value* of the function $f$ at $a$ and denote this by writing $b = f(a)$.

Now the notation $f(x) = x^2$ indicates that for each $x \in \mathbb{R}$, $x^2$ is the value of the function at $x$. Please be careful to distinguish between the name of the function $f$ and an arbitrary value of the function $f(x)$.

**Example 5.3.** *Here are some examples of important types of functions. Assume each of the sets is nonempty.*

*(i) Let $A$ be any set. The* identity function *$i : A \to A$ is defined by $i(a) = a$ for each $a \in A$.*

*(ii) Let $A$ and $B$ be sets and let $b_0 \in B$. The function $k : A \to B$ defined by $k(a) = b_0$ for all $a \in A$ is called a* constant function.

*(iii) Let $A$ and $B$ be any sets. The* coordinate projections *$\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$ are defined by $\pi_A(a,b) = a$ and $\pi_B(a,b) = b$ for each $(a,b) \in A \times B$.*

*(iv) Let $A$ be any subset of $\mathbb{R}$. The* characteristic function *$\chi_A : \mathbb{R} \to \{0,1\}$ of $A$ is defined by*

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

*Note: try and sketch a graph of the characteristic function of $\mathbb{Q}$.*

### 5.2.1 Binary Operations

Standard addition and multiplication on $\mathbb{R}$ are both examples of functions used to compute a single real number from two given real numbers. This kind of function is important enough to deserve it's own name.

**Definition.** A *binary operation* on a set $X$ is a function $* : X \times X \to X$. If $*$ is a binary operation on $X$, we usually use the notation $x * y$ to denote the value $*(x,y)$.

**Example 5.4.** *The standard addition and multiplication operations on $\mathbb{N}$, $\mathbb{Z}$, or $\mathbb{R}$ are all examples on binary operations. Note that they are all different binary operations.*

**Example 5.5.** *Subtraction is a binary operation on the sets $\mathbb{Z}$ or $\mathbb{R}$. Subtraction on $\mathbb{N}$ is not a binary operation on $\mathbb{N}$ since, for example, $7 - 12$ is not defined on $\mathbb{N}$.*

**Definition.** We say that a binary operation $*$ on a set $X$ is:

- *commutative* if $x * y = y * x$ for all $x, y \in X$.

- *associative* if $(x * y) * z = x * (y * z)$ for all $x, y, z \in X$.

Addition and multiplication on $\mathbb{Z}$ (or on $\mathbb{N}$ or $\mathbb{R}$ for that matter) are commutative and associative, which you have probably known since your first algebra class. Subtraction on $\mathbb{Z}$ is not commutative since, for example, $4 - 2 \neq 2 - 4$. Subtraction on $\mathbb{Z}$ also fails to be associative since, for example, $(5 - 1) - 3 = 1 \neq 7 = 5 - (1 - 3)$.

**Example 5.6.** *Define the operation $*$ on $\mathbb{Z}$ by $a * b = (ab)^2$. We claim that $*$ is commutative. To see this, let $a$ and $b$ be arbitrary integers. Then:*

$$\begin{aligned} a * b &= (ab)^2 \\ &= a^2 b^2 \\ &= b^2 a^2 \\ &= (ba)^2 \\ &= b * a \end{aligned}$$

*We leave it as an exercise to determine whether or not $*$ is associative.*

## 5.3 Injective, Surjective, and Bijective Functions

**Definition.** A function $f : X \to Y$ is said to be:

- *injective* or *one-to-one* if for all $x, y \in X$, if $f(x) = f(y)$, then $x = y$.
- *surjective* or *onto* if for each $y \in Y$, there is an $x \in X$ such that $f(x) = y$.
- *bijective* or *a one-to-one correspondence* if $f$ is both injective and surjective.

**Example 5.7.** *Let's consider the functions we defined in Example 5.3.*

*(i) For any nonempty set $A$, the identity function $i : A \to A$ is bijective. Assume first that $a, b \in A$ with $i(a) = i(b)$. Since $i(a) = a$ and $i(b) = b$, this implies that $a = b$ and $i$ is injective. To see that $i$ is surjective, let $c$ be any element of $A$. Then $i(c) = c$, so $i$ is surjective.*

*(ii) In general, constant functions are neither injective nor surjective. Assume for the moment that $A$ and $B$ each have more than one element and let $k : A \to B$ be the constant function $k(a) = b_0$. Choose two elements $a_1 \neq a_2$ in $A$, then $k(a_1) = b_0 = k(a_2)$ and $k$ is not injective. If $b \neq b_0$ and $b \in B$, then $b \neq k(a)$ for any $a \in A$ and $k$ is not surjective.*

*(iii) Next we consider the coordinate projection $\pi_A : A \times B \to A$. Once again, we assume that $A$ and $B$ have more than one element each. The function $\pi_A$ is surjective. To see this suppose that $a \in A$ and choose some $b_0 \in B$, then $\pi_A(a, b_0) = a$. Choose $a \in A$ and $b_1 \neq b_2$ both in $B$. Then $(a, b_1) \neq (a, b_2)$ but $\pi_A(a, b_1) = a = \pi_A(a, b_2)$, so $\pi_A$ is not injective. The coordinate projection $\pi_B : A \times B \to B$ is also surjective but not injective. The proofs are similar.*

*(iv) Finally, consider the characteristic function $\chi_A : \mathbb{R} \to \{0, 1\}$ of some subset $A$ of $\mathbb{R}$. Once again we assume that $A$ has more than one element. For any two elements $a \neq b$ of $A$ we have $\chi_A(a) = 1 = \chi_A(b)$, so $\chi_A$ is not injective. If $a \in A$ and $c \in \mathbb{R} \setminus A$, then $\chi_A(a) = 1$ and $\chi_A(c) = 0$. Since $0$ and $1$ are the only elements of the codomain, $\chi_A$ is surjective. Note however that the proof that $\chi_A$ is surjective requires that we be able to find points in $A$ and points in $\mathbb{R} \setminus A$. If $A = \mathbb{R}$, then $\chi_A$ is not surjective because $\mathbb{R} \setminus A = \emptyset$.*

## 5.4 Compositions of Functions

**Definition.** Let $f : X \to Y$ and $g : Y \to Z$ be functions. The *composition* $g \circ f : X \to Z$ is the function from $X$ to $Z$ defined by $g \circ f(x) = g(f(x))$. In other words to find $g \circ f(x)$, first find $f(x)$, then plug the result into the function $g$. In terms of ordered pairs, the composition is

$$g \circ f = \{(x, z) \mid (x, y) \in f \text{ and } (y, z) \in g \text{ for some } y \in Y\}.$$

**Theorem 5.1.** *Let $f : X \to Y$ and $g : Y \to Z$ be functions.*

*(i) If $f$ and $g$ are injective, then $g \circ f : X \to Z$ is injective.*

*(ii) If $f$ and $g$ are surjective, then $g \circ f : X \to Z$ is surjective.*

*Proof of (i).* Assume that $f : X \to Y$ and $g : Y \to Z$ are injective. Let $x_1$ and $x_2$ be distinct elements of $X$. Since $f$ is injective, $f(x_1)$ and $f(x_2)$ are distinct elements of the set $Y$. Now since $g$ is injective, $g(f(x_1))$ and $g(f(x_2))$ are distinct elements of $Z$. Therefore $g \circ f$ is injective as desired. □

*Proof of (ii).* Assume that $f : X \to Y$ and $g : Y \to Z$ are surjective. Let $z$ be an arbitrary element of $Z$. Since $g$ is surjective, there must be some element $y \in Y$ such that $g(y) = z$. Now since $f$ is surjective there must be an element $x \in X$ with $f(x) = y$, so $g(f(x)) = g(y) = z$ and $g \circ f : X \to Z$ is surjective as desired. □

Combining the two parts of Theorem 5.1, we have the following:

**Corollary 5.1.1.** *If $f : X \to Y$ and $g : Y \to Z$ are bijective functions, then $g \circ f : X \to Z$ is bijective.*

It is natural to ask whether or not the converses of the statements in Theorem 5.1 are true. We consider the converse of 5.1 *(i)* in the following example and theorem.

**Example 5.8.** *Define $f : \mathbb{N} \to \mathbb{R}$ by $f(n) = n^2$. Since no two natural numbers (which are all positive) have the same square, $f$ is injective. Define $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = x^2$. Since $g(-2) = 4 = g(2)$, $g$ is not injective. Now we consider the composition $g \circ f : \mathbb{N} \to \mathbb{R}$ of these functions. For each $n \in \mathbb{N}$ we have $g(f(n)) = g(n^2) = (n^2)^2 = n^4$. Let $m, n \in \mathbb{N}$ with $m^4 = n^4$, then*

$$0 = m^4 - n^4 = (m^2 + n^2)(m - n)(m + n),$$

*so $m = n$ or $m = -n$. But $m$ and $n$ are both positive, so $m \neq -n$ and it must be true that $m = n$. Hence $g \circ f : \mathbb{N} \to \mathbb{R}$ is injective.*

This example shows that it is possible for $g \circ f$ to be injective when $g$ is not. The next result says that if $g \circ f$ is injective, then it does follow that $f$ is injective.

**Theorem 5.2.** *Let $f : X \to Y$ and $g : Y \to Z$ be functions such that $g \circ f : X \to Z$ is injective. Then $f : X \to Y$ must be injective.*

*Proof.* We prove that if $f : X \to Y$ is not injective, then $g \circ f : X \to Z$ is not injective, which is the contrapositive of the desired proposition. Suppose that $f$ is not injective, then there must be elements $x_1 \neq x_2$ in $X$ with $f(x_1) = f(x_2)$. Since $g$ is a function, it must be true that $g(f(x_1)) = g(f(x_2))$. Since $x_1 \neq x_2$ but $g \circ f(x_1) = g \circ f(x_2)$, $g \circ f$ is not injective. □

We leave the proof of the corresponding result for surjective functions as an exercise.

**Theorem 5.3.** *Let $f : X \to Y$ and $g : Y \to Z$ be functions such that $g \circ f : X \to Z$ is surjective. Then $g : Y \to Z$ must be surjective.*

### 5.4.1 Inverses of functions

**Definition.** If $f : X \to Y$ is a function, the *inverse* of $f$ is the relation $g$ from $Y$ to $X$ given by:

$$g = \{(y, x) \mid (x, y) \in f\}$$

By this definition every function will have an inverse relation. Note however that the inverse of a function is not generally a function, as we see in the following example.

**Example 5.9.** *Let $f : \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x) = x^2$, then the inverse of $f$ is the relation $g = \{(x^2, x) \mid x \in \mathbb{R}\}$. Note that $g$ is not a function since both $(4, 2)$ and $(4, -2)$ are in $g$.*

**Definition.** If $f : X \to Y$ is a function and the inverse of $f$ is also a function, we say that $f$ is *invertible* and use $f^{-1} : Y \to X$ to denote the inverse.

**Question 5.1.** When is a function $f : X \to Y$ invertible?

Thinking back to what you've seen in previous courses for a moment, you are likely to have been taught that a function from $\mathbb{R}$ to $\mathbb{R}$ will have an inverse if it passes the "horizontal line test." Do you remember why? One way to think of this is that the graph of the inverse is the reflection through the line $y = x$ of the graph of the function. Since we want the reflection (the graph of the inverse) to pass the vertical line test, the graph of the original function should pass the horizontal line test. There should be some relationship between this condition and the answer to our question.

For the graph of a function to pass the horizontal line test, i.e. no horizontal line intersects the graph more than once, means that no two points of the graph have the same height. In other words, no two distinct points on the graph have the same $y$-coordinate. Rephrasing, if $(x_1, y)$ and $(x_2, y)$ are both on the graph, then $x_1 = x_2$. But this is just our definition of what it means for a function to be injective. Perhaps injective functions and invertible functions are the same thing? We can show that every invertible function is injective.

**Theorem 5.4.** *If $f : X \to Y$ is an invertible function, then $f$ is injective.*

*Proof.* Suppose that $f$ is not injective, then there are two elements $x_1 \neq x_2$ of $X$ such that $f(x_1) = f(x_2)$. Let $y = f(x_1)$. By definition both $(y, x_1)$ and $(y, x_2)$ must be elements of the inverse of $f$. Since $x_1 \neq x_2$, this implies that the inverse of $f$ is not a function. Therefore, $f$ is not invertible. □

Unfortunately, this is not a complete answer to our question because the converse of Theorem 5.4 is not true. We have found a condition that all invertible functions must satisfy, but not all functions that satisfy this condition are invertible. The following example illustrates the difficulty.

**Example 5.10.** *Define $f : \mathbb{N} \to \mathbb{N}$ by $f(n) = n + 1$. This function is injective (if $m + 1 = n + 1$, then $m = n$), but not invertible according to our definition. The inverse relation $g$ contains all ordered pairs of the form $(n + 1, n)$ where $n \in \mathbb{N}$. For $g$ to be a function from $\mathbb{N}$ to $\mathbb{N}$, every element of $\mathbb{N}$ must be the first coordinate of exactly one ordered pair in $g$. The problem here is that $1$ is in $\mathbb{N}$, but $1 \neq n + 1$ for any $n \in \mathbb{N}$, so $1$ is not the first coordinate of any of the ordered pairs in $g$. Therefore $g$ is not a function from $\mathbb{N}$ to $\mathbb{N}$.*

For a function $f : X \to Y$ to be invertible, every element of the codomain $Y$ must be a first coordinate of some ordered pair in the inverse. That in turn means that every element of the codomain must be the second coordinate of some ordered pair in $f$. This is exactly what it means to say that $f$ is surjective. This leads us to believe the following:

**Theorem 5.5.** *If $f : X \to Y$ is invertible, then $f$ is surjective.*

*Proof.* Assume that $f : X \to Y$ is not surjective, then there is some element $y \in Y$ so that $y \neq f(x)$ for any $x \in X$. In other words, $y$ is not the second coordinate of an ordered pair in $f$. By definition then, $y$ will not be the first coordinate of any ordered pair in the inverse of $f$. Hence the inverse of $f$ is not a function from $Y$ to $X$ and $f$ is not invertible. □

We are now ready to give a complete answer to our question in the form of the following theorem.

**Theorem 5.6.** *A function $f : X \to Y$ is invertible if and only if it is bijective.*

*Proof.* If $f$ is invertible, then we may use Theorems 5.4 and 5.5 to establish the fact that $f$ is bijective.

To see that the converse is true, suppose that $f : X \to Y$ is a bijective function. Let $g = \{(y, x) \mid (x, y) \in f\}$ be the inverse of $f$. We must show that $g$ is a function from $Y$ to $X$, i.e. that every $y \in Y$ is the first coordinate of exactly one ordered pair in $g$. Let $y \in Y$. Since $f$ is surjective, $y = f(x)$ for some $x \in X$. By definition $(x, y) \in f$ implies that $(y, x) \in g$, so $y$ is the first coordinate of at least one ordered pair in $g$. Now suppose that $(y, x_1)$ and $(y, x_2)$ are both in $g$. By definition this means that $f(x_1) = y$ and $f(x_2) = y$. Since $f$ is injective this implies that $x_1 = x_2$. It follows that $y$ cannot be the first coordinate of more than one ordered pair in $g$, so $g$ is a function from $Y$ to $X$ and $f$ is invertible. □

# Chapter 5 Exercises

**5.1.** Let $A$ be a nonempty set. Explain why there are no functions from $A$ to $\emptyset$.

**5.2.** Is standard division a binary operation on $\mathbb{N}$? on $\mathbb{R}$? Justify your answer in each case.

**5.3.** Is the dot product a binary operation on $\mathbb{R}^3$? Recall that the dot product is defined by $(a,b,c)\cdot(d,e,f) = ad+be+cf$.

**5.4.** Determine whether or not the operation $*$ defined in Example 5.6 is an associative operation on $\mathbb{Z}$.

**5.5.** Determine whether or not each of the following binary operations on $\mathbb{R}$ is (a) commutative, (b) associative.

(i) $a * b = |a-b|$.

(ii) $a * b = \frac{a}{b^2+1}$.

(iii) $a * b = \max\{a,b\}$.

**5.6.** Let $f : X \to Y$ be a function; let $A$ and $B$ be subsets of $X$. For $Z \subset X$ define $f(Z) = \{f(z) \mid z \in Z\}$. Determine which of the following are true. If a statement is true, prove it. If a statement is false, find a counterexample.

(i) $f(A \cup B) \subset f(A) \cup f(B)$

(ii) $f(A \cup B) \supset f(A) \cup f(B)$

(iii) $f(A \cap B) \subset f(A) \cap f(B)$

(iv) $f(A \cap B) \supset f(A) \cap f(B)$

(v) $f(X \setminus A) \subset Y \setminus f(A)$

(vi) $f(X \setminus A) \supset Y \setminus f(A)$

**5.7.** For each of the false statements in the previous exercise, determine whether or not they are true under the following conditions. Prove or give a counterexample in each case.

(i) $f : X \to Y$ is an injective function.

(ii) $f : X \to Y$ is a surjective function.

**5.8.** Let $A = \{1, 2, 3\}$. For each of the following, either find a function satisfying the indicated properties or prove that no such function exists.

(i) A bijective function $f : A \to A$ other than the identity function.

(ii) An injective function $g : A \to A$ that is not surjective.

(iii) A surjective function $h : A \to A$ that is not injective.

(iv) A function $j : A \to A$ that is neither injective nor surjective.

**5.9.** Let $A = \{1, 2, 3\}$ and $B = \{4, 5\}$. For each of the following, either find a function satisfying the indicated properties or prove that no such function exists.

(i) A bijective function $f : A \to B$.

(ii) An injective function $g : A \to B$ that is not surjective.

(iii) A surjective function $h : A \to B$ that is not injective.

(iv) A function $j : A \to B$ that is neither injective nor surjective.

**5.10.** For each of the following, either find a function satisfying the indicated properties or prove that no such function exists.

(i) A bijective function $f : \mathbb{N} \to \mathbb{N}$ other than the identity.

(ii) An injective function $g : \mathbb{N} \to \mathbb{N}$ that is not surjective.

(iii) A surjective function $h : \mathbb{N} \to \mathbb{N}$ that is not injective.

(iv) A function $j : \mathbb{N} \to \mathbb{N}$ that is neither injective nor surjective.

**5.11.** Let $A$ be a nonempty set and $\sim$ an equivalence relation on $A$; let $\widehat{A}$ be the set of all equivalence classes. Prove that there is an injective function $f : \widehat{A} \to A$.

**5.12.** Find examples of sets $X$, $Y$, and $Z$ and functions $f : X \to Y$ and $g : Y \to Z$ so that $g \circ f : X \to Z$ is surjective but $f : X \to Y$ is not surjective.

**5.13.** Prove Theorem 5.3.

**5.14.** The standard integer addition operation $+$ is a function from $\mathbb{Z}^2 \to \mathbb{Z}$. Show that if $a \equiv_5 b$ (see Exercise 4.2) and $c \equiv_5 d$, then $a + c \equiv_5 b + d$. This shows that addition is *well-defined* with respect to this equivalence relation.

**5.15.** Let $f : X \to Y$ be an invertible function and let $f^{-1} : Y \to X$ denote the inverse of $f$. Show that $f^{-1}$ is bijective and that $f$ is the inverse of $f^{-1}$.

**5.16.** Let $f : X \to Y$ be a function and suppose that the function $g : Y \to X$ is the inverse of $f$. Show that the composition $g \circ f : X \to X$ is the identity function, i.e. that $g(f(x)) = x$ for every $x \in X$.

Chapter 6

# The Real Numbers

> The essence of mathematics is not to make simple things complicated, but to make complicated things simple.
>
> *Stan Gudder*

> Mathematics consists in proving the most obvious thing in the least obvious way.
>
> *George Polya*

## Introduction

We now turn our attention to developing a mathematical description of the real numbers. All of the results of calculus can be derived from these basic properties of the real number system, which is usually done in a first course in real analysis. Our basic assumptions about the real numbers are called axioms, and they are divided into several groups. Many of these axioms will be familiar to you from previous courses in algebra.

## 6.1 Field Axioms

Taken as a group, the field axioms tell us that the real numbers together with the operations of addition and multiplication form what is known as a *field*. Very informally, you might think of a field as something that satisfies the usual rules

you encountered in high school algebra. Fields and related objects are studied in more depth in a course in abstract algebra.

**Field Axioms.** The set of real numbers $\mathbb{R}$ is a collection of objects together with the two binary operations addition and multiplication that satisfy the following properties:

(i) Commutative Laws: For every $a, b \in \mathbb{R}$, $a + b = b + a$ and $ab = ba$.

(ii) Associative Laws: For every $a, b, c \in \mathbb{R}$, $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

(iii) Distributive Law: For every $a, b, c \in \mathbb{R}$, $a(b + c) = ab + ac$.

(iv) Identities: There are distinct elements 0 and 1 in $\mathbb{R}$ such that $a \cdot 1 = a$ and $a + 0 = a$ for every $a \in \mathbb{R}$.

(v) Additive Inverses: For every $a \in \mathbb{R}$, there is an element $-a \in \mathbb{R}$ such that $a + (-a) = 0$.

(vi) Multiplicative Inverses: For every $a \in \mathbb{R}$ with $a \neq 0$, there is an element $a^{-1} \in \mathbb{R}$ such that $aa^{-1} = 1$.

Any set of objects satisfying all of these properties is a *field*. Other examples of fields include the fields of rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$. As we develop further axioms for the real numbers, we will also narrow the list of fields that satisfy all of the axioms.

A number of the familiar algebraic properties of the real numbers are immediate consequences of the field axioms. A few of them are collected in the following theorem, though there are certainly many others.

**Theorem 6.1.** *For any real numbers $a, b, c$, the following are true:*

*(i) If $a + b = a + c$, then $b = c$.*

*(ii) $-(-a) = a$.*

*(iii) If $a \neq 0$ and $ab = ac$, then $b = c$.*

*(iv) If $a \neq 0$, then $(a^{-1})^{-1} = a$.*

*(v) $a \cdot 0 = 0$.*

*(vi)* $-a = (-1)a$.

*(vii)* *If* $ab = 0$, *then* $a = 0$ *or* $b = 0$.

*Proof.* We prove parts *(ii)*, *(iii)*, and *(vi)*. The remaining proofs are exercises.

We first show that *(ii)* is true. To see this, note that $-(-a)$ is the additive inverse of $-a$. The reader should justify each of the following steps:

$$\begin{aligned} a + (-a) &= 0 \\ &= -a + (-(-a)) \\ &= -(-a) + (-a) \end{aligned}$$

so $a + (-a) = -(-a) + (-a)$. We apply part *(i)* to see that $a = -(-a)$ as desired.

To prove *(iii)*, suppose that $a \neq 0$ and $ab = ac$. Since $a \neq 0$, $a$ has a multiplicative inverse $a^{-1}$. The reader should give a justification for each step of the following:

$$\begin{aligned} b &= 1 \cdot b \\ &= (a^{-1}a)b \\ &= a^{-1}(ab) \\ &= a^{-1}(ac) \\ &= (a^{-1}a)c \\ &= 1 \cdot c \\ &= c \end{aligned}$$

To prove *(vi)*, let $a$ be any real number. Then:

$$\begin{aligned} a + (-1)a &= 1 \cdot a + (-1)a \\ &= a(1 + (-1)) \\ &= a \cdot 0 \\ &= 0 \end{aligned}$$

Hence $a + (-1)a = 0 = a + (-a)$ and we may apply part *(i)* to see that $(-1)a = -a$. □

## 6.2 Order Axioms

As noted previously, there are a number of common fields. One of the differences between $\mathbb{R}$ and $\mathbb{C}$ is that we think of the real numbers as lying in order along a line. There is no natural way to organize the complex numbers in this fashion. The next group of axioms make precise what we mean when we say that the real numbers form an *ordered field*.

**Order Axioms.** There is an order $<$ defined on the real numbers $\mathbb{R}$ satisfying:

(i) Transitivity: If $a < b$ and $b < c$, then $a < c$.

(ii) Trichotomy: For every two real numbers $a$ and $b$, exactly one of the following holds:
$$a < b \quad \text{or} \quad a = b \quad \text{or} \quad b < a$$

(iii) If $a < b$, then $a + c < b + c$ for every $c \in \mathbb{R}$.

(iv) If $a < b$ and $c > 0$, then $ac < bc$.

We derive several consequences of the fact that $\mathbb{R}$ is an ordered field.

**Theorem 6.2.** *The following statements are true in* $\mathbb{R}$*:*

*(i)* $a > 0$ *iff* $-a < 0$.

*(ii) If* $a < b$*, then* $-a > -b$.

*(iii) If* $a \neq 0$*, then* $a^2 > 0$.

*(iv)* $1 > 0$.

*Proof.* To prove part *(i)*, assume first that $a > 0$. By Trichotomy we have either $-a < 0$, $-a = 0$, or $-a > 0$. We will show that two of these possibilities lead to contradictions, forcing the remaining option to be true. If $-a = 0$ then we have $a = a + 0 = a + (-a) = 0$, which contradicts the fact that $a > 0$. If $-a > 0$ then we have $0 = a + (-a) > a + 0 = a$, once again contradicting the fact that $a > 0$. We have shown that neither $-a = 0$ nor $-a > 0$ can be true, so it must be the case that $-a < 0$ as desired. The remaining direction of the proof of part *(i)* is left as a homework exercise.

We next prove part *(ii)*. The reader should determine which axiom or theorem justifies each step of the following:

$$\begin{aligned} a &< b \\ a + (-b) &< b + (-b) \\ a + (-b) &< 0 \\ ((-a) + a) + (-b) &< (-a) + 0 \\ -b &< -a \end{aligned}$$

The proofs of the remaining parts of the theorem are left to the reader. □

**Theorem 6.3.** *Let $a, b \in \mathbb{R}$.*

*(i) If $a > 0$ and $b > 0$, then $ab > 0$.*

*(ii) If $a < 0$ and $b < 0$, then $ab > 0$.*

*(iii) If $a > 0$ and $b < 0$, then $ab < 0$.*

**Theorem 6.4.** *Let $a \in \mathbb{R}$.*

*(i) If $a > 0$, then $a^{-1} > 0$.*

*(ii) If $a < 0$, then $a^{-1} < 0$.*

*Proof.* To prove part *(i)* we assume $a > 0$ and apply Trichotomy. If $a^{-1} < 0$, then $1 = aa^{-1} < 0$ by Theorem 6.3, but this contradicts Theorem 6.2*(iv)*. If $a^{-1} = 0$, then we have $1 = aa^{-1} = a \cdot 0 = 0$, which again contradicts Theorem 6.2*(iv)*. The only remaining possibility is that $a^{-1} > 0$ as desired.

The proof of *(ii)* is similar and is left for the reader. □

**Theorem 6.5.** *Let $a \geq 0$ and $b \geq 0$. Then $a < b$ iff $a^2 < b^2$.*

*Proof.* We assume throughout that $a \geq 0$ and $b \geq 0$. By Trichotomy we have exactly one of $a < b$, $a = b$, or $a > b$; we also have exactly one of $a^2 < b^2$, $a^2 = b^2$, or $a^2 > b^2$.

If $a < b$, then $a^2 < b^2$ by an application of exercise 6.8.

If $a = b$, then $a^2 = b^2$.

If $a > b$, then $a^2 > b^2$ by an application of exercise 6.8.

It now follows that $a < b$ if and only if $a^2 < b^2$. □

## 6.3 Completeness of $\mathbb{R}$

Our axioms so far insure that $\mathbb{R}$ is an ordered field. The field $\mathbb{Q}$ of rational numbers is also an ordered field, so we need something further to distinguish between $\mathbb{R}$ and $\mathbb{Q}$. Our last axiom is based on the observation that the field $\mathbb{Q}$ has *holes*, whereas $\mathbb{R}$ does not. Let's first consider an example to clarify what we mean by this.

**Example 6.1.** *Let $A$ and $B$ be the following sets:*

$$A = \{q \in \mathbb{Q} \mid q > 0 \text{ and } q^2 \leq 2\}$$
$$B = \{x \in \mathbb{R} \mid x > 0 \text{ and } x^2 \leq 2\}$$

*As we will show in Theorem 6.9, there is a real number $\sqrt{2}$ whose square is 2. The number $\sqrt{2}$ is in $B$ and $\sqrt{2}$ is larger than every other number in $B$.*

*As we showed in Theorem 2.5, there is no rational number whose square is 2. It can be shown that for every number in $A$, there are larger numbers that are also in $A$.*

### 6.3.1 Upper and lower bounds

**Definition.** Let $A$ be a nonempty set of real numbers. We say that a number $u$ is an *upper bound* for $A$ if $x \leq u$ for every $x \in A$. We say that a number $m$ is a *lower bound* for $A$ if $x \geq m$ for every $x \in A$. We say that $A$ is *bounded above* if $A$ has an upper bound, that $A$ is *bounded below* if $A$ has a lower bound, and that $A$ is *bounded* if $A$ is bounded above and below.

**Example 6.2.** *Let $A = \{a \mid a^2 < 5\}$, $B = [0,7)$, $C = \mathbb{N}$, and $D = \mathbb{Z}$.*

*The number $5$ is an upper bound for $A$ and $-3$ is a lower bound for $A$.*
*The set $B$ has an upper bound at $7$ and a lower bound at $0$.*
*The set $C$ has a lower bound at $1$, but no upper bound.*
*The set $D$ has no upper or lower bounds.*

The previous example illustrates several things. It is possible for a nonempty set to have both upper and lower bounds, just one bound, or no bounds at all. Upper and lower bounds may or may not be elements of the set. Finally, upper and lower bounds are not unique. Transitivity implies that if $M$ is an upper bound for a set $A$, then every number larger than $M$ is also an upper bound for $A$. Similarly, if $m$ is a lower bound for $A$ then every number smaller than $m$ is a lower bound for $A$.

Consider the set $A = \{a \mid a^2 \leq 5\}$ from the previous example again. We claimed that 5 is an upper bound, and that is certainly true, but note that 3 is also an upper bound. In some sense this smaller upper bound is a "better" bound for $A$ because it puts a tighter restriction on the size of the elements of $A$. This is approximately like saying that Grand Forks is a better way to describe the location of UND than North Dakota. In this sense the best possible upper bound would be the smallest one, if there is one. In this particular case, $A$ has a smallest upper bound in $\mathbb{R}$ ($\sqrt{5}$) but not in $\mathbb{Q}$. This is the basic difference between $\mathbb{Q}$ and $\mathbb{R}$ that we wish to capture in an axiom. First, we need another couple of definitions.

**Definition.** Let $A$ be a nonempty subset of $\mathbb{R}$. We say that a number $u$ is a *least upper bound* (LUB) for $A$ if both of the following are true:

(i) For every $a \in A$, $a \leq u$.

(ii) For every upper bound $b$ of $A$, $u \leq b$.

We say that a number $m$ is a *greatest lower bound* (GLB) for $A$ if both of the following are true:

(i) For every $a \in A$, $a \geq m$.

(ii) If $b$ is a lower bound for $A$, then $m \geq b$.

Note that a LUB is sometimes called a *supremum* and a GLB is sometimes called an *infimum*.

It is not hard to prove that, unlike upper bounds, a set can have only one least upper bound. This fact is made explicit in the following theorem, whose proof is left as exercise 6.15.

**Theorem 6.6.** *Let $A$ be a nonempty subset of $\mathbb{R}$. If $u$ and $v$ are least upper bounds for $A$, then $u = v$.*

The following theorem says that the least upper bound of a set must in some sense be "close to" the set.

**Theorem 6.7.** *Let $A$ be a nonempty subset of $\mathbb{R}$ and let $u$ be the least upper bound for $A$. If $x < u$, then there is an element $a \in A$ such that $x < a$.*

*Proof.* Suppose that $u$ is the least upper bound for $A$ and that $x < u$. Assume that there is no $a \in A$ such that $x < a$, then $a \leq x$ for every $a \in A$ by Trichotomy. It follows by definition that $x$ is an upper bound for $A$, but this contradicts the fact that $u$ is the least upper bound for $A$ since $x < u$. □

We are now ready to state our final axiom, which says that $\mathbb{R}$ is *complete*.

**The Completeness Axiom.** Let $A$ be a nonempty subset of $\mathbb{R}$. If $A$ has an upper bound, then $A$ has a least upper bound.

There are a number of consequences of the Completeness Axiom, most of which are beyond the scope of this text. We will look at only a couple of them. We begin with the fairly intuitive seeming fact that for any real number $x$, there is a natural number larger than $x$.

**Theorem 6.8.** *(Archimedian Property) If $x \in \mathbb{R}$, then there is a number $n_x \in \mathbb{N}$ such that $x \leq n_x$.*

*Proof.* Assume to the contrary that there is a real number $x$ so that $n < x$ for every natural number $n$. In this case $x$ is an upper bound for the set $\mathbb{N}$. Applying the Completeness Axiom, $\mathbb{N}$ must have a least upper bound $m$ in $\mathbb{R}$. Since $m-1 < m$, Theorem 6.7 implies that there is a natural number $n$ such that $m-1 < n$. Now $n+1$ is also a natural number and $m < n+1$, which contradicts the fact that $m$ is an upper bound for $\mathbb{N}$. □

We previously commented, without proof, that the Completeness Axiom would allow us to distinguish $\mathbb{R}$ from $\mathbb{Q}$. We will now make this explicit by proving that there is at least one real number that is not rational.[1] We proved previously (Theorem 2.5) that there is no rational number whose square is 2. We now show that the Completeness Axiom implies that there must be a real number $x$ with $x^2 = 2$.

**Theorem 6.9.** *There is a number $x \in \mathbb{R}$ such that $x^2 = 2$.*

*Proof.* Let $A = \{a \in \mathbb{R} \mid a^2 \leq 2\}$. Note that $A$ is not empty since $1 \in A$. We claim that 2 is an upper bound for $A$. To see this note that if $t > 2$, then $t^2 > 2 \cdot 2 = 4 > 2$ (see exercise 6.8), so $t \notin A$. Since $A$ is a nonempty subset of $\mathbb{R}$ that is bounded above, $A$ must have a least upper bound $x$. We will use Trichotomy to show that $x^2 = 2$.

Assume first that $x^2 < 2$. Note that $\frac{2x+1}{2-x^2}$ is a positive real number. By the Archimedian Property there must be a natural number $n$ such that $n > \frac{2x+1}{2-x^2}$. Since $n > \frac{2x+1}{2-x^2} > 0$, it follows that $\frac{1}{n} < \frac{2-x^2}{2x+1}$. We will show that $x + \frac{1}{n} \in A$, which will contradict the fact that $x$ is an upper bound for $A$. To see that $x + \frac{1}{n} \in A$, we

[1] In fact there are more irrational numbers than there are rational numbers, as we shall see in the final chapter.

compute:

$$\begin{aligned}\left(x+\frac{1}{n}\right)^2 &= x^2+\frac{2x}{n}+\frac{1}{n^2}\\ &= x^2+\frac{1}{n}\left(2x+\frac{1}{n}\right)\\ &\leq x^2+\frac{1}{n}(2x+1)\\ &< x^2+(2-x^2)\\ &= 2\end{aligned}$$

Now $x+\frac{1}{n}\in A$, which leads to the desired contradiction. It follows that $c^2<2$ cannot hold.

Next suppose that $x^2>2$. In this case $\frac{2x}{x^2-2}$ is a positive number and we may find $m\in\mathbb{N}$ such that $m>\frac{2x}{x^2-2}$. This in turn implies that $\frac{1}{m}<\frac{x^2-2}{2x}$. We show that $(x-\frac{1}{m})^2>2$:

$$\begin{aligned}\left(x-\frac{1}{m}\right)^2 &= x^2-\frac{2x}{m}+\frac{1}{m^2}\\ &> x^2-\frac{2x}{m}\\ &> x^2-(2x)\frac{x^2-2}{2x}\\ &= 2\end{aligned}$$

Now Theorem 6.5 implies that if $s>x-\frac{1}{m}$, then $s^2>(x-\frac{1}{m})^2>2$, so $x-\frac{1}{m}$ is an upper bound for $A$. This would contradict the fact that $x$ is the least upper bound for $A$, so $x^2>2$ cannot hold.

The only possibility left is that $x^2=2$ as desired. □

# Chapter 6 Exercises

**6.1.** Prove part *(i)* of Theorem 6.1.

**6.2.** Prove part *(iv)* of Theorem 6.1.

**6.3.** Prove part *(v)* of Theorem 6.1.

**6.4.** Prove part *(vii)* of Theorem 6.1.

**6.5.** Use the field axioms to show that $-0 = 0$ and $1^{-1} = 1$.

**6.6.** Prove that $(-a)b = -(ab) = a(-b)$ for all real numbers $a$ and $b$.

**6.7.** Use the field axioms and Theorem 6.1 to show that for any $a \in \mathbb{R}$, $(-a)(-a) = a^2$.

**6.8.** If $a > b \geq 0$ and $c > d \geq 0$, prove that $ac > bd$.

**6.9.** If $a$ and $b$ are nonzero real numbers and $a < b$, prove that $b^{-1} < a^{-1}$.

**6.10.** Complete the proof of part *(i)* of Theorem 6.2 by showing that if $a < 0$, then $-a > 0$.

**6.11.** Prove part *(iii)* of Theorem 6.2.

**6.12.** Prove part *(iv)* of Theorem 6.2.

**6.13.** Prove Theorem 6.3.

**6.14.** Prove part *(ii)* of Theorem 6.4.

**6.15.** Prove Theorem 6.6.

**6.16.** Prove that if $u$ is an upper bound for $A$ and $u \in A$, then $u$ is the least upper bound for $A$.

**6.17.** Show that every nonempty subset of $\mathbb{R}$ with a lower bound has a greatest lower bound.

**6.18.** Let $A$ and $B$ be two nonempty subsets of $\mathbb{R}$ such that $A \cup B = \mathbb{R}$. If $A$ and $B$ satisfy the further property that $a < b$ for every $a \in A$ and $b \in B$, then $A$ and $B$ form a *Dedekind cut* of $\mathbb{R}$. The Completeness Axiom is sometimes replaced with Dedekind's Axiom, which says that given any Dedekind cut of $\mathbb{R}$, either $A$ has a largest element or $B$ has a smallest element. Assuming the field and order axioms for $\mathbb{R}$, as well as their consequences, prove the following:

(i) The Completeness Axiom implies Dedekind's Axiom.

(ii) Dedekind's Axiom implies the Completeness Axiom.

Chapter 7

# Introduction to Cardinality

> One of the most amazing things about mathematics is the people who do math aren't usually interested in application, because mathematics itself is truly a beautiful art form. It's structures and patterns, and that's what we love, and that's what we get off on.
>
> *Danica McKellar*

> Why, sometimes I've believed as many as six impossible things before breakfast.
>
> *The Red Queen*

## Introduction

What do we mean when we say that there are *four* suits in a standard deck of cards? More generally, what does it mean to count any collection of objects? Since you may no longer actually think about counting, it may help to watch a child who is just learning to count. Given four objects to count, the child is likely to point to each object in turn and count "one, two, three, four." In other words, the child is explicitly constructing a bijective function between the objects she is counting and the elements of the set $\{1, 2, 3, 4\}$. Our goal in this chapter is to extend this idea to infinite sets.

## 7.1 The Cardinality of a Set

Let $A$ and $B$ be two sets. We define the relation $\equiv$ by $A \equiv B$ if there is a bijective function $f : A \to B$. In this case we say that $A$ and $B$ are *equinumerous* or that they have the same *cardinality*. We define $A \preceq B$ to mean that there is an injective function $f : A \to B$. We may also write this as $B \succeq A$. We write $A \prec B$ to indicate that $A \preceq B$ and $A \not\equiv B$. Note: it is fairly common to use the notation $|A| = |B|$ rather than $A \equiv B$.

**Theorem 7.1.** *The relation $\equiv$ defined above is an equivalence relation.*

*Proof.* Let $A$, $B$, and $C$ be arbitrary sets.

Since the identity function on any set is a bijection, $A \equiv A$ and $\equiv$ is reflexive.

If $A \equiv B$, then there is a bijection $f : A \to B$. Applying Theorem 5.6, the function $f$ is invertible. By Exercise 5.15 the inverse function $f^{-1} : Y \to X$ is a bijection. Hence $B \equiv A$ and $\equiv$ is symmetric.

To see that $\equiv$ is transitive, suppose that $A \equiv B$ and $B \equiv C$. By definition there are bijective functions $f : A \to B$ and $g : B \to C$. Now apply Corollary 5.1.1 to see that $g \circ f : A \to C$ is a bijective function. Hence $A \equiv C$ and $\equiv$ is transitive. Therefore, $\equiv$ is an equivalence relation as desired. □

Note that Theorem 7.1 allows us to say that two sets $A$ and $B$ have the same cardinality if we are able to find a bijection from $A$ to $B$ or a bijection from $B$ to $A$.

**Theorem 7.2.** *The relation $\preceq$ is reflexive and transitive.*

*Proof.* Let $A$, $B$, and $C$ be any sets. Since the identity function on any set is injective, $A \preceq A$ and $\preceq$ is reflexive. To see that $\preceq$ is transitive, suppose that $A \preceq B$ and $B \preceq C$. By definition there are injections $f : A \to B$ and $g : B \to C$. We apply Theorem 5.1 to see that the composition $g \circ f : A \to C$ is also injective, hence $A \preceq C$ as desired. □

While we would probably not expect $\preceq$ to be symmetric, it wouldn't be too surprising if it was antisymmetric. If $A \preceq B$ and $B \preceq A$, does it follow that $A \equiv B$? Georg Cantor (1845-1918) was interested in just this question. One of his doctoral students, Felix Bernstein (1878-1956) was able to prove that the answer is yes. The resulting theorem is usually known as the Cantor-Bernstein Theorem.

**Theorem 7.3** (Cantor-Bernstein)**.** *If $A \preceq B$ and $B \preceq A$, then $A \equiv B$.*

We defer the proof of this theorem to the Appendix. The following example uses the same ideas as the proof in order to construct a bijection between the open interval $(-1,1)$ and the closed interval $[-1,1]$.

**Example 7.1.** *Define the functions $f : (-1,1) \to [-1,1]$ and $g : [-1,1] \to (-1,1)$ by $f(x) = x$ and $g(x) = x/2$, respectively. It is easy to show that both of these functions are injective, so $(-1,1) \preceq [-1,1]$ and $[-1,1] \preceq (-1,1)$. The Canter-Bernstein Theorem implies that there must be a bijection between the open interval $(-1,1)$ and the closed interval $[-1,1]$, but the theorem itself doesn't tell us how to find such a bijection. We construct such a bijection here.*

*We wish to find a bijective function $h : (-1,1) \to [-1,1]$. For most elements $x \in (-1,1)$ we want $h(x) = f(x) = x$. Unfortunately, if we let $h(x) = f(x)$ for all $x$, then the function is not bijective because $-1 \neq f(x)$ and $1 \neq f(x)$ for all $x \in (-1,1)$. We use the function $g$ to help us fix this problem. Consider first the element $1 \in [-1,1]$. While $1 \neq f(x)$ for any $x$, there is an element of the open interval associated with $1$ by $g$. In particular $g(1) = 1/2$. We could define $h$ so that $h(1/2) = 1$ and $h(x) = f(x)$ for other $x \in (-1,1)$, but that creates a new problem. Now $1$ is in the image of the function, but $1/2$ is not. To fix this we let $h(1/4) = 1/2$, because $g(1/2) = 1/4$. Of course, now $1/4$ is not in the image of $h$. We continue fixing one problem at a time using $g$, each time creating a new problem. Naturally, we will need to do the same with $-1$.*

*These particular functions are simple enough that we can write down a formula for the function $h$ that we end up with. We end up defining $h : (-1,1) \to [-1,1]$ by*

$$h(x) = \begin{cases} 2^{-(n-1)} & \text{if } x = 2^{-n} \text{ for some } n \in \mathbb{N} \\ -2^{-(n-1)} & \text{if } x = -2^{-n} \text{ for some } n \in \mathbb{N} \\ x & \text{otherwise} \end{cases}$$

*We claim that this function is the desired bijection.*

*We first show that $h$ is surjective. To see this, let $t \in [-1,1]$. If $t = 2^{-(n-1)}$ for some $n \in \mathbb{N}$, then $h(2^{-n}) = t$. If $t = -2^{-(n-1)}$ for some $n \in \mathbb{N}$, then $h(-2^{-n}) = t$. For any other $t \in [-1,1]$ we have $h(t) = t$. In any case $t = h(x)$ for some $x \in (-1,1)$, so $h$ is surjective.*

*To see that $h$ is injective, suppose that $x \neq y$ are both elements of $(-1,1)$. We consider several cases.*

Case 1. $x = 2^{-n}, y = 2^{-k}$ for some $n, k \in \mathbb{N}$. *Since $x \neq y$, it follows that $n \neq k$. Hence $n - 1 \neq k - 1$ and we have $h(x) = 2^{-(n-1)} \neq 2^{-(k-1)} = h(y)$.*

Case 2. $x = -2^{-n}$, $y = -2^{-k}$ for some $n, k \in \mathbb{N}$. *Since $x \neq y$, it follows that $n \neq k$. Hence $n - 1 \neq k - 1$ and we have $h(x) = -2^{-(n-1)} \neq -2^{-(k-1)} = h(y)$.*

Case 3. $x = 2^{-n}$, $y = -2^{-k}$ for some $n, k \in \mathbb{N}$. *In this case we have $h(x) = 2^{-(n-1)} \neq -2^{-(k-1)} = h(y)$.*

Case 4. $x = -2^{-n}$, $y = 2^{-k}$ for some $n, k \in \mathbb{N}$. *In this case we have $h(x) = -2^{-(n-1)} \neq 2^{-(k-1)} = h(y)$.*

Case 5. $x = \pm 2^{-n}$ for some $n \in \mathbb{N}$ and $y \neq \pm 2^{-k}$ for any $k \in \mathbb{N}$. *In this case we have $h(x) = \pm 2^{-(n-1)} \neq y = h(y)$.*

Case 6. $y = \pm 2^{-n}$ for some $n \in \mathbb{N}$ and $x \neq \pm 2^{-k}$ for any $k \in \mathbb{N}$. *In this case we have $h(x) = x \neq \pm 2^{-(n-1)} = h(y)$.*

Case 7. $x \neq \pm 2^{-n}$ and $y \neq \pm 2^{-n}$ for any $n \in \mathbb{N}$. *In this case we have $h(x) = x \neq y = h(y)$.*

*In all cases we have $h(x) \neq h(y)$, so $h$ is injective.*

## 7.2 Finite Sets

**Question.** What does it mean to say that a set $A$ is finite?

At first glance, this may seem like something you've known for a long time. Don't we just mean that we can count the elements of $A$? If so, is the number of cells in your body finite? Can you count them? Maybe the answer to our question isn't quite so obvious after all.

Let's try to make our answer a bit more precise. First, for any natural number $n$ we define the set $\mathbb{N}_n = \{k \in \mathbb{N} \mid k \leq n\}$. So $\mathbb{N}_4 = \{1, 2, 3, 4\}$, for example.

Next, we use the sets $\mathbb{N}_n$ to formalize the idea of counting introduced in the introduction to this chapter. We say that a set $A$ has $n$ elements if $\mathbb{N}_n \equiv A$.

Now it seems that we can say the set $A$ is finite if $A$ has $n$ elements for some $n \in \mathbb{N}$. Almost, but we're still forgetting something. Is the empty set finite? Clearly we would like to say that the empty set has zero elements, making it finite. This doesn't quite fit our scheme, so we must treat the empty set as a special case. In keeping our previous idea, here is one way to do so.

**Definition.** Let $A$ be a set. If $A = \emptyset$, we say that $A$ has 0 elements. If $A \equiv \mathbb{N}_n$ for some $n \in \mathbb{N}$, we say that $A$ has $n$ elements. Finally, we say that $A$ is *finite* if it has $n$ elements for some $n \in \mathbb{N} \cup \{0\}$. We say that $A$ is *infinite* if it is not finite.

Applying Theorem 5.1 and Exercise 7.1, we obtain the following:

**Theorem 7.4.** *If $A$ is finite, then $A \preceq \mathbb{N}$.*

Now that we have a definition of finite, let's reconsider the set $C$ of cells in your body. Is $C$ finite? If so, for which $n$ is $C \equiv \mathbb{N}_n$? We still can't really count them, so perhaps we've just obscured the question rather than answering it. Scientists estimate that there are about 10,000,000,000,000 cells in the average adult human body. That's not an actual count of the number of cells in any individual human body, though. These kinds of estimates are based on the sizes of various kinds of cells and the approximate proportion of each kind of cell in the body. In fact, we could determine the maximum number of cells that might be in a person's body by figuring out how many of the smallest kinds of cells would be required to build a body of a particular volume, or weight, etc. It seems reasonable to think that we could say a set was finite if we were sure it had at most $n$ elements for some natural number $n$. That is the intent of the next result.

**Theorem 7.5.** *If $A \preceq \mathbb{N}_n$ for some natural number $n$, then $A$ is finite.*

Before attempting to prove this result, let's make sure we understand what we are trying to prove. We are assuming that there is an injective function $f : A \to \mathbb{N}_n$. Unfortunately, our definition of finite requires us to produce a bijective function to some $\mathbb{N}_k$ and the function $f$ is probably not bijective. Since $f$ is injective, the potential difficulty is that there are extra elements of $\mathbb{N}_n$ (i.e. $f$ is not surjective). This seems like something we should be able to overcome without much difficulty since a set with fewer elements than some finite set should certainly be finite. How do we construct the required bijection though? Let's first consider a simpler result which will prove useful.

**Lemma 7.2.1.** *Let $f : A \to \mathbb{N}_n$ be an injective function that is not surjective. Then there is an injective function $g : A \to \mathbb{N}_{n-1}$.*

*Proof of Lemma.* Since $f : A \to \mathbb{N}_n$ is not surjective, the set $B = \mathbb{N}_n \setminus f(A)$ is nonempty. Choose $b \in B$. If $b = n$, then $f(a) \neq n$ for any element $a \in A$ and we may define $g : A \to \mathbb{N}_{n-1}$ by $g(a) = f(a)$ for each $a \in A$. If $b \neq n$, we define $g$ by:

$$g(a) = \begin{cases} f(a) & \text{if } f(a) \neq n \\ b & \text{if } f(a) = n \end{cases}$$

In either case $g : A \to \mathbb{N}_{n-1}$ is as desired since for all $a \in A$, $g(a) \neq n$.

It remains to be shown that $g$ is injective. Suppose that $a_1, a_2 \in A$ and that $g(a_1) = g(a_2) = m$. If $m = b$, then by definition of $g$ we have $f(a_1) = n = f(a_2)$. If $m \neq b$, then our definition of $g$ implies that $f(a_1) = m = f(a_2)$. In either case we have $f(a_1) = f(a_2)$, so $a_1 = a_2$ because the function $f$ is injective. Therefore $g$ is injective as desired. □

We will now prove the theorem.

*Proof of Theorem 7.5.* First note that if $A = \emptyset$, then $A$ is finite by definition. We assume for the remainder of the proof that $A \neq \emptyset$. By hypothesis, there is an injective function $f_0 : A \to \mathbb{N}_n$ for some natural number $n$. If $f_0$ is also surjective, then we have the desired bijection. If $f_0$ is not surjective, then we may apply Lemma 7.2.1 to find an injection $f_1 : A \to \mathbb{N}_{n-1}$. We now consider the function $f_1$.

If $f_1 : A \to \mathbb{N}_{n-1}$ is surjective, then $f_1$ is a bijection. If $f_1$ is not surjective, then we again apply Lemma 7.2.1 to find an injective function $f_2 : A \to \mathbb{N}_{n-2}$.

We continue this process recursively. If any of the injective functions $f_i : A \to \mathbb{N}_{n-i}$ are surjective, then we have the desired bijection and the proof is complete. We claim that this must occur for some $0 \leq i \leq n-1$. To see this, suppose that $f_{n-2} : A \to \mathbb{N}_2$ is not surjective. Applying Lemma 7.2.1 we find an injection $f_{n-1} : A \to \mathbb{N}_1$. Since $A \neq \emptyset$, we may choose $a \in A$. Now $f_{n-1}(a)$ must be an element of $\mathbb{N}_1 = \{1\}$, so $f_{n-1}(a) = 1$. It follows that $f_{n-1}$ is surjective as desired.

We have shown that there is a bijective function $f_i : A \to \mathbb{N}_{n-1}$ for some $0 \leq i \leq n-1$, so $A \equiv \mathbb{N}_{n-i}$ and $A$ is finite. □

We conclude this section with a question, the answer to which may seem obvious to you.

**Question 7.1.** If $m, n \in \mathbb{N}$ and $m \neq n$, can you prove that $\mathbb{N}_m \not\equiv \mathbb{N}_n$?

## 7.3 Denumerable Sets

Georg Cantor was able to define a complete system of infinite numbers and of arithmetic on those numbers. We will not discuss his system here, but we will look at one particular kind of infinite number that is important in many areas of mathematics.

**Theorem 7.6.** *If $A$ is an infinite set and $B$ is a finite subset of $A$, then the set $A \setminus B$ is infinite.*

*Proof.* Suppose to the contrary that $A \setminus B$ is finite. It is easy to show that for any subset $B \subset A$, $A = B \cup (A \setminus B)$. Since both $B$ and $A \setminus B$ are finite, it follows from Exercise 7.4 that $A$ is finite. This contradicts our hypothesis that $A$ is infinite, so it must true that $A \setminus B$ is infinite. □

**Definition.** Let $A$ be a set. We say that $A$ is:

- *denumerable* if $A \equiv \mathbb{N}$.
- *countable* if $A$ is either finite or denumerable.
- *uncountable* if $A$ is infinite and not denumerable.

**Example 7.2.** *The set $A = \{2k \mid k \in \mathbb{N}\}$ of even natural numbers is denumerable. To see this, define the function $f : \mathbb{N} \to A$ by $f(n) = 2n$. It is routine to check that $f$ is a bijection, so $\mathbb{N} \equiv A$ as desired.*

The preceding example points out a very important difference between finite and infinite sets. The set $A$ is a proper subset of $\mathbb{N}$, but has the same cardinality as $\mathbb{N}$. Compare this to Exercise 7.5. All infinite sets have proper subsets of the same cardinality. In fact, this property is sometimes used to define what it means for a set to be infinite.

We would like to determine which of our results about finite sets are also true for denumerable sets. If $A$ and $B$ are denumerable, must $A \cup B$ also be denumerable? Are subsets of denumerable sets denumerable? Is there an analog of Theorem 7.5? Are there other ways to tell that a set is denumerable?

**Theorem 7.7.** *If $A$ is a denumerable set and $B \equiv A$, then $B$ is denumerable.*

*Proof.* By definition we have $A \equiv \mathbb{N}$. Since $\equiv$ is an equivalence relation, it follows that $B \equiv \mathbb{N}$ as desired. □

**Theorem 7.8.** *If $A \subset \mathbb{N}$, then $A$ is countable.*

*Proof.* If $A$ is finite, then $A$ is countable by definition.

Assume that $A$ is infinite. We define a function $f : \mathbb{N} \to A$ as follows. Recall that every nonempty subset of $\mathbb{N}$ has a smallest element. Let $f(1)$ be the smallest element of $A_0 = A$. Since $A$ is an infinite the set $A_1 = A \setminus \{f(1)\}$ is nonempty, so we may define $f(2)$ to be the smallest element of $A_1$. Continuing

recursively, suppose that we have defined $f(1), \ldots, f(n)$ for some $n \in \mathbb{N}$. Let $A_n = A \setminus \{f(1), \ldots, f(n)\}$. Since $\{f(1), \ldots, f(n)\}$ is finite, $A_n$ is infinite by Theorem 7.6. In particular, $A_n$ is nonempty and we may define $f(n+1)$ to be the smallest element of this set. Before showing that $f$ is bijective we note the following facts that follow immediately from our construction:

(i) For every natural number $n$, $A \setminus A_n = \{f(1), \ldots, f(n)\}$.

(ii) For every natural number $n$, $f(n) \geq n$.

(iii) For all natural numbers $m, n$, if $f(n) \in A_m$ then $m < n$.

(iv) For all natural numbers $m < n$, $f(n) \in A_m$.

(v) For all natural numbers $m \leq n$, $f(m) \notin A_n$.

For any two natural numbers $m < n$ we shown that $f(n) \in A_m$ and $f(m) \notin A_m$, so $f(n) \neq f(m)$ and $f$ is injective.

To see that $f$ is surjective, let $k \in A$. We must show that $k = f(m)$ for some $m \in \mathbb{N}$. If $k = f(k)$, we are done. Otherwise we have $f(k) > k$. Now $f(k)$ is the smallest element of $A_{k-1}$ and $k < f(k)$, so $k \notin A_{k-1}$. We also know that $k \in A$, so it follows that $k \in A \setminus A_{k-1} = \{f(1), \ldots, f(k-1)\}$. Therefore $k = f(n)$ for some $1 \leq n < k$ and $f$ is surjective as desired. □

Applying Theorem 7.8, Theorem 5.1, and Corollary 5.1.1 we have:

**Corollary 7.8.1.** *A subset of a countable set is countable.*

**Corollary 7.8.2.** *A set $A$ is countable if and only if $A \preceq \mathbb{N}$.*

Note that this Corollary allows us to say that a set $A$ is countable if we can find an injection from $A$ to $\mathbb{N}$. This is equivalent to finding a surjection from $\mathbb{N}$ to $A$, as you will show in exercise 7.8. This allows us to conclude the following:

**Corollary 7.8.3.** *A set $A$ is countable if either of the following is true:*

*(i) There is an injection $f : A \to \mathbb{N}$.*

*(ii) There is a surjection $f : \mathbb{N} \to A$.*

**Theorem 7.9.** *The union of two denumerable sets is denumerable.*

*Proof.* Suppose that we are given any two denumerable sets $A$ and $B$. By definition there are bijective functions $f : A \to \mathbb{N}$ and $g : B \to \mathbb{N}$. We define a function $h : A \cup B \to \mathbb{N}$ by the following rule:

$$h(x) = \begin{cases} 2f(x) & \text{if } x \in A \\ 2g(x)+1 & \text{if } x \notin A \end{cases}$$

We claim that $h$ is an injection. To see this, let $x \neq y$ be two elements of $A \cup B$. If $x \in A$ and $y \notin A$, then $h(x) \neq h(y)$ since $h(x)$ is even and $h(y)$ is odd. Similarly if $x \notin A$ and $y \in A$, then $h(x) \neq h(y)$. If $x$ and $y$ are both in $A$, then $h(x) = 2f(x)$ and $h(y) = 2f(y)$, so $h(x) \neq h(y)$ because $f$ is injective. Finally, if neither $x$ nor $y$ are in $A$, then $h(x) = 2g(x)+1$ and $h(y) = 2g(y)+1$, so $h(x) \neq h(y)$ because $g$ is injective. In any case, we have shown that $h(x) \neq h(y)$ so $h : A \cup B \to \mathbb{N}$ is injective.

We have shown that $A \cup B \preceq \mathbb{N}$, so $A \cup B$ must be countable. Note however that the function $h$ constructed above is not necessarily a bijection. (Do you see why?) To see that $A \cup B$ is actually denumerable, note that $A \subset A \cup B$. Applying Exercise 7.1 it follows that $A \preceq A \cup B$. Since $\mathbb{N} \preceq A$ we may apply Theorem 7.2 to obtain $\mathbb{N} \preceq A \cup B$. It now follows from the Cantor-Bernstein Theorem that $A \cup B \equiv \mathbb{N}$ as desired. □

Using Mathematical Induction on the number of sets, we obtain:

**Corollary 7.9.1.** *The union of finitely many denumerable sets is denumerable.*

**Theorem 7.10.** *The set* $\mathbb{N} \times \mathbb{N}$ *is denumerable.*

*Proof.* Since $\mathbb{N} \times \mathbb{N}$ is infinite, we need only show that it is countable. Define the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(a,b) = 2^{a-1}(2b-1)$. We will show that $f$ is injective, then apply Corollary 7.8.3 to obtain the desired result.

To see that $f$ is injective, suppose that

$$2^{a-1}(2b-1) = 2^{c-1}(2d-1) \tag{7.1}$$

for $(a,b),(c,d) \in \mathbb{N} \times \mathbb{N}$. We show first that $a = c$. If not, then we may assume without loss of generality that $a < c$. Dividing both sides of equation 7.1 by $2^{a-1}$ yields $(2b-1) = 2^{c-a}(2d-1)$. But this is a contradiction since the quantity on the left side of the equation is odd and the quantity on the right is even. Since $a = c$, we may reduce equation 7.1 to $(2b-1) = (2d-1)$, from which it follows that $b = d$. Now $(a,b) = (c,d)$ and $f$ is injective as desired.[1] □

[1] While it is not necessary for the purposes of this example, it is not to difficult to show that the function $f$ defined here is actually bijective.

### 7.3.1 The set $\mathbb{Q}$

At first glance it may seem that there are more rational numbers than there are natural numbers. After all, there are infinitely many rational numbers between any two natural numbers. One of Cantor's accomplishments was to show that the set of rational numbers is actually denumerable. Our intuition developed from years of working with finite sets just doesn't serve us very well when working with infinite sets.

**Lemma 7.3.1.** *The set $\mathbb{Q}^+$ of positive rational numbers is countable.*

*Proof.* Let $\mathbb{F} = \{\frac{a}{b} \mid a, b \in \mathbb{N}\}$ be the set of fractions whose numerators and denominators are natural numbers. We claim that $\mathbb{F} \equiv \mathbb{N} \times \mathbb{N}$. To see this, define $f : \mathbb{F} \to \mathbb{N} \times \mathbb{N}$ by $f\left(\frac{a}{b}\right) = (a, b)$. We leave it to you to show that $f$ is a bijection (see exercise 7.7), so $\mathbb{F} \equiv \mathbb{N} \times \mathbb{N}$. We may now apply Theorems 7.10 and 7.7 to see that $\mathbb{F}$ is denumerable. Since the positive rationals are exactly those numbers that can be expressed as fractions of natural numbers, the function taking each fraction in $\mathbb{F}$ to the corresponding rational number is a surjection from $\mathbb{F}$ onto $\mathbb{Q}^+$. We now apply Corollary 7.8.3 to see that $\mathbb{Q}^+$ is countable. □

Since the function taking every positive rational to it's additive inverse is bijective, the following Corollary follows immediately from our Lemma.

**Corollary 7.10.1.** *The set $\mathbb{Q}^-$ of negative rational numbers is countable.*

We know that $\mathbb{Q}^+$, $\mathbb{Q}^-$, and $\{0\}$ are all countable sets. Applying Exercise 7.10 we may conclude that:

**Theorem 7.11.** *The set of $\mathbb{Q}$ of rational numbers is countable.*

### 7.3.2 The set $\mathbb{R}$

By this point it may seem possible that all sets are countable, making denumerability a useless distinction. We will show that this is not true by demonstrating that the set of real numbers is uncountable. First recall that every real number can be written as an infinite decimal. There is one danger in using such representations, it is possible to have different decimal representations that represent the same real number: e.g. $1.0\overline{0} = 0.9\overline{9}$. There is only one way that this can happen, though. A real number with a decimal expansion ending in an infinite string of 0's also has an expansion ending in an infinite string of 9's. If we disallow expansions ending

in a string of 0's (the decimal expansions we normally think of as terminating), the infinite decimal representation of each real number is unique. This is important in the following proof since we will want to know that real numbers with different infinite decimal expansions are distinct.

**Theorem 7.12.** *The set* $\mathbb{R}$ *of real numbers is uncountable.*

*Proof.* Suppose to the contrary that the set $\mathbb{R}$ is countable, then there is a surjection $f : \mathbb{N} \to \mathbb{R}$. For convenience we use the notation $x_n$ to denote the $n$ th digit to the right of the decimal place in the unique infinite decimal expansion of $x$. In particular, the $n$ th digit to the right of the decimal place in the expansion of $f(m)$ will be denoted $f(m)_n$. For example if $f(2) = \pi = 3.141592\ldots$, then $f(2)_4 = 5$. We will construct a real number $y$ such that $y \neq f(n)$ for any $n \in \mathbb{N}$, which contradicts the fact that $f$ is surjective.

For each $n \in \mathbb{N}$, define:

$$y_n = \begin{cases} 1 & \text{if } f(n)_n = 9 \\ 9 & \text{if } f(n)_n \neq 9 \end{cases}$$

Next we define

$$y = \sum_{i=1}^{\infty} \frac{y_i}{10^i}$$

so $y = 0.y_1y_2y_3\ldots$. In other words, $y$ is the unique real number in $(0, 1]$ such that the $n$ th term to the right of the decimal place in the infinite decimal expansion of $y$ is $y_n$. By definition, $y_n \neq f(n)_n$ for every $n \in \mathbb{N}$, so $y \neq f(n)$ for any $n \in \mathbb{N}$ as desired. □

# Chapter 7 Exercises

**7.1.** Show that if $A \subset B$, then $A \preceq B$.

**7.2.** Prove that the relation $\prec$ is transitive.

**7.3.** Prove that a subset of a finite set is finite.

**7.4.** Let $A$ and $B$ be finite sets. Prove the following:

(i) $A \cap B$ is finite.

(ii) $A \cup B$ is finite.

**7.5.** Let $A$ be a finite set and let $B$ be a proper subset of $A$.

(i) Prove that $B \preceq A$.

(ii) Prove that $A$ and $B$ are not equinumerous. *Note: this will also answer Question 7.1.*

**7.6.** Prove that a countable set with an infinite subset must be denumerable.

**7.7.** Show that the function $f : \mathbb{F} \to \mathbb{N} \times \mathbb{N}$ defined in the proof of Lemma 7.3.1 is a bijection.

**7.8.** Let $A$ and $B$ be nonempty sets. Prove that there is an injection $f : A \to B$ if and only if there is a surjection $g : B \to A$.

**7.9.** Prove that each of the following sets is denumerable.

(i) The set of nonnegative integers $\mathbb{N} \cup \{0\}$.

(ii) The set of integers $\mathbb{Z}$.

**7.10.** Prove the following.

(i) The union of two countable sets is countable.

(ii) The union of finitely many countable sets is countable.

**7.11.** Let $A$ and $B$ be denumerable sets. Prove that the set $A \times B$ is denumerable.

**7.12.** Let $A$, $B$, and $C$ be sets. Define $A \times B \times C = \{(a, b, c) \mid a \in A \text{ and } b \in B \text{ and } c \in C\}$. Prove that $A \times B \times C \equiv (A \times B) \times C$.

**7.13.** For each natural number $n$, let $\mathbb{N}^n$ denote the set of ordered $n$-tuples of natural numbers, so $\mathbb{N}^3 = \mathbb{N} \times \mathbb{N} \times \mathbb{N}$, etc. Prove that $\mathbb{N}^n$ is countable.

**7.14.** Let $\mathbb{S}$ denote the set of sequences of 0's and 1's, so a typical element of $\mathbb{S}$ looks like $(x_1, x_2, x_3, \ldots)$ where each $x_i$ is either 0 or 1. Prove that $\mathbb{S}$ is uncountable.

# The Cantor-Bernstein Theorem

In this appendix we present a proof of the Cantor-Bernstein Theorem. The proof uses the same idea we used to construct the bijection between an open interval and a closed interval in Example 7.1. First we introduce some convenient notation.

Let $f : X \to Y$ be any function. For $A \subset X$, the *image* of $A$ is the set $f(A) = \{f(x) \mid x \in A\}$. For $B \subset Y$ we use $f^{-1}(B)$ to denote the set $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$. The set $f^{-1}(B)$ is called the *preimage* of $B$. We also use the notation $f^{-1}(x)$ to denote $f^{-1}(\{x\})$. You should not assume from our use of this notation that the function $f$ is invertible! If $f : X \to X$ we use the notation $f^2$ to denote the function $f \circ f : X \to X$. Recursively, for a natural number $n \geq 2$, $f^{n+1}$ is used to denote the function $f \circ f^n : X \to X$. Finally, we define $f^0$ to be the identity function on $X$.

**Conjecture** (Cantor-Bernstein)**.** *If $X \preceq Y$ and $Y \preceq X$, then $X \equiv Y$.*

*Proof.* By hypothesis there exist injections $f : X \to Y$ and $g : Y \to X$. We will find a bijective function $h : X \to Y$ with the property that $h(x) = f(x)$ for most $x \in X$ and $h(x) = g^{-1}(x)$ (since $g$ is injective, $g^{-1}(x)$ is always a single point) for the remaining $x \in X$. As in Example 7.1, we use $g^{-1}(x)$ only as necessary to insure that the final function is bijective.

For every point $y \in Y \setminus f(X)$, we define a sequence of points in $X$ as follows: $x_1 = g(y)$, $x_2 = g(f(x_1)) = g \circ f(g(y))$, $x_3 = g(f(x_2)) = (g \circ f)^2(g(y))$, and in general $x_{n+1} = g(f(x_n)) = (g \circ f)^{n-1}(g(y))$ for each $n \in \mathbb{N}$. Note that since $g$ is injective $g^{-1}(x_1)$ contains only the point $y$ and that for $k \geq 2$, $g^{-1}(x_k)$ contains only the point $x_{k-1}$. Define the set

$$S = \{x \mid x = (g \circ f)^n(g(y)) \text{ for some } y \in Y \setminus f(X) \text{ and for some } n \in \mathbb{N} \cup \{0\}\}.$$

In other words, the set $S$ contains every point of each of the sequences we created above. This set will be the set of points on which $h$ is not the same as $f$.

STEP 1: We prove the following facts about the set $S$.

(i) If $y \in Y \setminus f(X)$, then $g(y) \in S$.

(ii) If $x \in S$, then $g \circ f(x) \in S$.

(iii) If $g(f(x)) \in S$, then $x \in S$.

For $y \in Y \setminus f(X)$ we have $g(y) = (g \circ f)^0(g(y))$, so (i) is true.

If $x \in S$, then $x = (g \circ f)^n(g(y))$ for some $n \in \mathbb{N} \cup \{0\}$ and some $y \in Y \setminus f(X)$. Now $g \circ f(x) = (g \circ f)^{n+1}(g(y))$, so $g \circ f(x) \in S$ and (ii) holds.

To see that (iii) is true, suppose that $g(f(x)) = (g \circ f)^n(g(y))$ for some $y \in Y \setminus f(X)$ and some $n \in \mathbb{N} \cup \{0\}$. If $n = 0$ then we have $g(f(x)) = g(y)$. Since $g$ is injective this would imply $y = f(x)$, which contradicts our choice of $y$. Hence $n \geq 1$ and the point $w = (g \circ f)^{n-1}(g(y))$ is an element of $S$ by definition. Now $g \circ f(w) = (g \circ f)^n(g(y)) = g \circ f(x)$. But $g \circ f$ is injective by Theorem 5.1, so we have $w = x$ and $x \in S$ as desired.

STEP 2: We now define the function $h : X \to Y$.

For $x \in X$ we define:

$$h(x) = \begin{cases} g^{-1}(x) & \text{if } x \in S \\ f(x) & \text{otherwise.} \end{cases}$$

Clearly $h(x)$ is defined for every $x \in X \setminus S$. If $x \in S$ then by definition $x = (g \circ f)^n(g(y))$ for some $n$ and $y$, but this implies that $x \in g(Y)$ and $g^{-1}(x)$ is nonempty. We must also be sure that we have actually defined a function, i.e. that there is only one point in $g^{-1}(x)$ for each $x \in S$. To this end, suppose that $y_1$ and $y_2$ are each in $g^{-1}(x)$ for some $x \in S$. By definition we have $g(y_1) = g(y_2)$. Since $g$ is injective this implies that $y_1 = y_2$ as desired. It remains to be shown that $h$ is bijective.

STEP 3: We show that $h$ is surjective.

Let $z \in Y$. Either $g(z) \in S$ or not.

CASE 1: If $g(z) \in S$, then $h(z) = g^{-1}(g(z)) = z$.

CASE 2: Suppose $g(z) \notin S$. By (i) $z \notin Y \setminus f(X)$, so there is an $x \in X$ such that $f(x) = z$. Since $g(f(x)) = g(z) \notin S$, $x \notin S$ by (ii). Therefore $h(x) = f(x) = z$.

In either case we have shown that $z \in h(X)$, so $h$ is surjective as desired.

STEP 4: We show that $h$ is injective, which will complete the proof of the theorem.

Suppose that $h(x_1) = h(x_2)$ for some $x_1, x_2 \in X$. We consider several cases.

CASE 1: Suppose that neither of $x_1$ or $x_2$ are in $S$. Then $f(x_1) = h(x_1) = h(x_2) = f(x_2)$ and $x_1 = x_2$ because $f$ is injective.

CASE 2: Suppose both $x_1$ and $x_2$ are in $S$. Then $g^{-1}(x_1) = h(x_1) = h(x_2) = g^{-1}(x_2)$, so there is an element $y \in S$ so that $g(y) = x_1$ and $g(y) = x_2$. This implies that $x_1 = x_2$ because $g$ is a function.
CASE 3: Finally, suppose that $x_1 \in S$ and $x_2 \notin S$. In this case we have $g^{-1}(x_1) = h(x_1) = h(x_2) = f(x_2)$, so $x_1 = g(g^{-1}(x_1) = g(f(x_2))$ and $g(f(x_2)) \in S$. Applying (iii) it follows that $x_2 \in S$, which is a contradiction. Therefore this case is impossible. Clearly it is also impossible to have $x_1 \notin S$ and $x_2 \in S$. □