2021

An Axiomatic Construction of the Real Number System

Leonard Van Wyk
vanwykla@jmu.edu

AN AXIOMATIC CONSTRUCTION OF THE REAL NUMBER SYSTEM

LEONARD VAN WYK

Contents

1. Introduction 3
2. The Natural Numbers 4
3. The Integers 12
4. A Brief Introduction to Rings 18
5. The Rationals 24
6. Order 30
7. Sequences 37
8. The Reals 43
9. The Reals II 50
A. The Basics of Logic 57
B. The Basics of Sets 60
C. Relations and Functions 65

1. Introduction

This material was developed over a number of years of teaching a course entitled *The Real Number System* at James Madison University. The material is accessible to any student who had a Calculus course in sequences and some sort of "introduction to proofs" course. Starting with the Peano Axioms (minus those that essentially state that equality is an equivalence relation and if b is a natural number and $a = b$, then a is also a natural number), we construct the algebraic properties of the natural numbers ($\mathbb{N}$, which includes 0 in this text), the integers ($\mathbb{Z}$), the rationals ($\mathbb{Q}$), and the reals ($\mathbb{R}$), as well as the notion of order on these sets.

It is an unusual course, one that is not typically offered to undergraduates. The material is axiomatic and very linear in nature. But the tools used in the development of the material provide a concrete introduction to those used in abstract algebra and real analysis courses and experience has shown that most students who have taken this course fare better in those subsequent courses than those who haven't.

Appendices A-C contain a quick review of the usual introductory topics that are found in many bridge courses. These chapters can be skimmed or omitted for more advanced students.

Chapters 2-5 are algebraic in nature. The primary tool of Chapter 2 is induction, while Chapter 3 and Chapter 5 heavily use equivalence relations and the notion of a well-defined binary operation on a set of equivalence classes. (The material of Chapter 5 is often covered in the more general case of the construction of a field of quotients of an integral domain in some abstract algebra courses.) Chapter 4 is, as its title states, a brief introduction to some terms in the study of rings.

Chapter 6 develops the notion of order of the naturals, integers, and rationals. This is necessary in order to define the notion of distance between two numbers, which is required for convergence of sequences. If you are pressed for time, you might want to omit this section.

Chapters 7-9 are analytic in nature. Quantifiers are used extensively, and since that seems to be one of the difficulties students have in analysis courses, these chapters provide a nice foundation for those. The reals are constructed as equivalence classes of rational Cauchy sequences, and their various properties follow from those of the rationals.

The amount of material is generally suitable for a semester class.

2. The Natural Numbers

In this section, we construct the set of natural numbers, $\mathbb{N}$, from a set of five axioms known as the Peano Axioms. The primary tool used is mathematical induction. Almost all of the material from this point on will probably be new to the student.

We will start with the fact that equality is an equivalence relation, and use the symbol "0" and a function, the "successor function" $\mathbb{N} \to \mathbb{N}$, $n \mapsto n'$. We will call n' the **successor** of n.

The following are the Peano axioms of the natural numbers.

Peano Axioms. (1) 0 is a natural number.

(2) For every natural number n, n' is a natural number.
(3) For every natural number n, $n' \neq 0$.
(4) If $n' = m'$, then $n = m$.
(5) If T is a set such that
  - $0 \in T$, and
  - for every natural number n, if $n \in T$ then $n' \in T$,

  then T contains every natural number.

You should be thinking that $n' = n + 1$, but we can't say that now because we don't know how to add. Notice the last axiom is a version of the induction principle, which you have certainly seen before:

Principle of Mathematical Induction. For each natural number n, let $P(n)$ be a proposition about n. Assume:

(1) $P(0)$ is true.
(2) Whenever $P(n)$ is true, it follows that $P(n')$ is true.

Then $P(n)$ is true for all natural numbers n.

The first part is the **base**, while the second is the **inductive step**. We will also use this (Peano Axiom 5 or the Principle of Mathematical Induction) to define various things "inductively." We'll refer to this principle as *PMI*.

Our goal is to show that the set of natural numbers, $\{0, 1, 2, 3, \dots\}$, *including its algebraic structure* (addition, multiplication, etc.) can be deduced solely from these axioms.

Notice that Peano Axiom 3 states 0 is not a successor of anything. The next result shows that 0 is the *only* non-successor.

Theorem 2.1. *If $a \neq 0$, then there exists b such that $a = b'$.*

Proof. Let $M = \{0\} \cup \{x \mid \exists b \text{ such that } x = b'\}$. (In other words, M consists of 0 together with the elements that are successors of something.)

Let $P(n)$ be the statement "$n \in M$." By definition, $0 \in M$, so $P(0)$ is true. Suppose $P(n)$ is true, i.e., $n \in M$. We need to show $P(n')$ is true, i.e., $n' \in M$. Since $n \in M$, either $n = 0$ or $\exists b$ such that $n = b'$. So either $n' = 0'$ or $n' = (b')'$. In either case, n' is a successor, so $n' \in M$. (Or, put another way, n' is the successor of ... n.) Thus $P(n')$ is true. Thus by Peano Axiom 5, $M = \mathbb{N}$.

Since every $a \neq 0$ must be an element of the second set in the definition of M, namely $\{x \mid \exists b \text{ such that } x = b'\}$, it follows that every nonzero natural number is a successor. □

We now define the binary operation of addition on $\mathbb{N}$ inductively.

Definition 2.1. Let a and b be natural numbers. The **sum** $a + b$ of a and b is defined inductively as:

(1) $a + 0 = a$, and
(2) $a + b' = (a + b)'$.

From this definition alone, we can use induction to prove the following familiar properties of addition.

Notice the form of Definition 2.1. Part (1) defines addition by 0, while part (2) defines addition of a by the successor of b in terms of the successor of the natural number $a + b$, which is already defined. The right hand side of each of these equations is known, and we use those to define the left hand side of the equations.

Theorem 2.2. *Let a, b, and c be natural numbers. Then*

(1) $0 + b = b$.
(2) $a + (b + c) = (a + b) + c$.
(3) $a + b = b + a$.
(4) If $a + c = b + c$, *then* $a = b$.
(5) If $a + b = 0$, *then* $a = b = 0$.

Definition 2.1 (1) and Theorem 2.2 (1) show that 0 is a **2-sided identity** under addition. Theorem 2.2 (2) is the **associative law** of addition. Theorem 2.2 (3) is the **commutative law** of addition. Theorem 2.2 (4) is the **right cancelation law**.

Proof. Parts (1) and (4) are left as exercises.

(2) Induct on c.

Let $P(n)$ be the statement, "$a + (b + n) = (a + b) + n$."

Base.

$$\begin{aligned} a+(b+0) &= a+b && \text{Definition 2.1 (1)} \\ &= (a+b)+0 && \text{Definition 2.1 (1)} \end{aligned}$$

So $P(0)$ is true.

Inductive Step. Assume $P(n)$ is true, i.e., $a+(b+n)=(a+b)+n$. We must prove $P(n')$ is true, i.e., $a+(b+n')=(a+b)+n'$. But

$$\begin{aligned} a+(b+n') &= a+(b+n)' && \text{Definition 2.1 (2)} \\ &= (a+(b+n))' && \text{Definition 2.1 (2)} \\ &= ((a+b)+n)' && \text{Inductive Hypothesis} \\ &= (a+b)+n' && \text{Definition 2.1 (2).} \end{aligned}$$

Thus $P(n')$ is true.

It follows by PMI that $P(n)$ is true for all natural numbers n.

(3) This is a bit tricky since there is nothing in the definition of addition that allows us to reverse the order of the elements. It really requires "double induction." The first of these induction proofs we will form as a lemma.

Lemma. $a'+b=a+b'$.

Proof. Induct on b. Let $P(n)$ be the statement "$a'+n=a+n'$."

Base.

$$\begin{aligned} a'+0 &= a' && \text{Definition 2.1 (1)} \\ &= (a+0)' && \text{Definition 2.1 (1)} \\ &= a+0' && \text{Definition 2.1 (2)} \end{aligned}$$

Thus $P(0)$ is true.

Inductive Step. Assume $P(n)$ is true, i.e., $a'+n=a+n'$. We must prove $P(n')$ is true, i.e., $a'+n'=a+n''$. But

$$\begin{aligned} a'+n' &= (a'+n)' && \text{Definition 2.1 (2)} \\ &= (a+n')' && \text{Inductive Hypothesis} \\ &= a+n'' && \text{Definition 2.1 (2).} \end{aligned}$$

Thus $P(n')$ is true.

It follows by PMI that $P(n)$ is true for all natural numbers n.

□

Now we are in a position to prove $a+b=b+a$ by inducting on a. Let $Q(n)$ be the statement "$n+b=b+n$."

Base.

$$\begin{aligned} 0+b &= b && \text{Theorem 2.2 (1)} \\ &= b+0 && \text{Definition 2.1 (1).} \end{aligned}$$

Thus $Q(0)$ is true.

Inductive Step. Assume $Q(n)$ is true, i.e., $n+b=b+n$. We must prove $Q(n')$ is true, i.e., $n'+b=b+n'$. But

$$\begin{aligned} n'+b &= n+b' && \text{Lemma} \\ &= (n+b)' && \text{Definition 2.1 (2)} \\ &= (b+n)' && \text{Inductive Hypothesis} \\ &= b+n' && \text{Definition 2.1 (2).} \end{aligned}$$

Thus $Q(n')$ is true.

It follows by PMI that $Q(n)$ is true for all natural numbers n.

(5) Assume $a+b=0$.

Suppose $a \neq 0$. Then by Theorem 2.1, there exists c such that $a=c'$. Hence

$$\begin{aligned} 0 &= a+b && \text{Hypothesis} \\ &= c'+b && \text{Above} \\ &= b+c' && \text{Theorem 2.2 (3)} \\ &= (b+c)' && \text{Definition 2.1 (2),} \end{aligned}$$

which contradicts Peano Axiom 3 (0 is not a successor). So $a=0$.

Thus if $a+b=0$, we have $0+b=0$. But, by Theorem 2.2 (1), we know $0+b=b$. So $b=0$.

Hence $a=b=0$.

□

Now we need an inductive definition for the binary operation of multiplication on $\mathbb{N}$.

Definition 2.2. Let a and b be natural numbers. The **product** ab (or $a \cdot b$) of a and b is defined inductively as:

(1) $a \cdot 0 = 0$, and
(2) $a \cdot b' = ab + a$.

As before, we will use this inductive definition of the product of two natural numbers to prove some familiar properties.

Theorem 2.3. *Let a, b, and c be natural numbers. Then*

(1) $0 \cdot b = 0$.
(2) $a(b+c) = ab+ac$.
(3) $a(bc) = (ab)c$.
(4) $ab = ba$.
(5) If $ab=0$, *then* $a=0$ *or* $b=0$.

(6) If $ac = bc$ and $c \neq 0$, then $a = b$.

Definition 2.2 (1) and Theorem 2.3 (1) show that 0 is a **2-sided zero** for multiplication. Theorem 2.3 (2) is the **left distributive law** of multiplication over addition. Theorem 2.3 (3) is the **associative law** of multiplication. Theorem 2.3 (4) is the **commutative law** of multiplication. Theorem 2.3 (6) is the **right cancelation law** for multiplication.

Proof. Parts (1), (2), and (5) are left as exercises.

(3) Induct on c.

Let $P(n)$ be the statement, "$a(bn) = (ab)n$."

Base.

$$\begin{aligned} a(b \cdot 0) &= a \cdot 0 && \text{Definition 2.2 (1)} \\ &= 0 && \text{Definition 2.2 (1)} \\ &= (ab) \cdot 0 && \text{Definition 2.2 (1).} \end{aligned}$$

So $P(0)$ is true.

Inductive Step. Assume $P(n)$ is true, i.e., $a(bn) = (ab)n$. We must prove $P(n')$ is true, i.e., $a(bn') = (ab)n'$. But

$$\begin{aligned} a(bn') &= a(bn + b) && \text{Definition 2.2 (2)} \\ &= a(bn) + ab && \text{Theorem 2.3 (2)} \\ &= (ab)n + ab && \text{Inductive Hypothesis} \\ &= (ab)n' && \text{Definition 2.2 (2)} \end{aligned}$$

Thus $P(n')$ is true.

It follows by PMI that $P(n)$ is true for all natural numbers n.

(4) As with addition, the commutative property is a tough one to prove. We need a lemma.

Lemma. $a'b = ab + b$.

Proof. Induct on b. Let $P(n)$ be the statement "$a'n = an + n$."

Base.

$$\begin{aligned} a' \cdot 0 &= 0 && \text{Definition 2.2 (1)} \\ &= 0 + 0 && \text{Definition 2.1 (1)} \\ &= a \cdot 0 + 0 && \text{Definition 2.2 (1)} \end{aligned}$$

Thus $P(0)$ is true.

Inductive Step. Assume $P(n)$ is true, i.e., $a'n = an+n$. We must prove $P(n')$ is true, i.e., $a'n' = an' + n'$. But

$$\begin{aligned} a'n' &= a'n + a' && \text{Definition 2.2 (2)} \\ &= (an+n)+a' && \text{Inductive Hypothesis} \\ &= an+(n+a') && \text{Associative Law of Addition} \\ &= an+(n'+a) && \text{Lemma from Theorem 2.2 (3)} \\ &= (an+a)+n' && \text{Associative and Commutative Laws of Addition} \\ &= an'+n' && \text{Definition 2.2 (2).} \end{aligned}$$

Thus $P(n')$ is true.

It follows by PMI that $P(n)$ is true for all natural numbers n.

□

Now we are in a position to prove $ab = ba$ by inducting on a. Let $Q(n)$ be the statement "$nb = bn$."

Base.

$$\begin{aligned} 0 \cdot b &= 0 && \text{Theorem 2.3 (1)} \\ &= b \cdot 0 && \text{Definition 2.2 (1).} \end{aligned}$$

Thus $Q(0)$ is true.

Inductive Step. Assume $Q(n)$ is true, i.e., $nb = bn$. We must prove $Q(n')$ is true, i.e., $n'b = bn'$. But

$$\begin{aligned} n'b &= nb+b && \text{Lemma} \\ &= bn+b && \text{Inductive Hypothesis} \\ &= bn' && \text{Definition 2.2 (2).} \end{aligned}$$

Thus $Q(n')$ is true.

It follows by PMI that $Q(n)$ is true for all natural numbers n.

(6) We will induct on b, which is certainly not an obvious choice.

Let $P(n)$ be the statement, "If $ac = nc$ and $c \neq 0$, then $a = n$."

Base.

$$\begin{aligned} ac = 0 \cdot c \text{ and } c \neq 0 &\Rightarrow ac = 0 \text{ and } c \neq 0 && \text{Theorem 2.3 (1)} \\ &\Rightarrow (a = 0 \text{ or } c = 0) \text{ and } c \neq 0 && \text{Theorem 2.3 (5)} \\ &\Rightarrow a = 0 && [(p \vee q) \wedge \sim q] \Rightarrow p. \end{aligned}$$

So $P(0)$ is true.

Inductive Step. Assume $P(n)$ is true. We must prove $P(n')$ is true, i.e., If $ac = n'c$ and $c \neq 0$, then $a = n'$. So assume $ac = n'c$ and $c \neq 0$. By Peano Axiom 3, we know $n' \neq 0$. Since $c \neq 0$, it follows from the contrapositive of Theorem 2.3 (5) that $n'c \neq 0$. But since $ac = n'c$, it then follows that $ac \neq 0$. Thus, since $c \neq 0$, we must have $a \neq 0$ too. So, by Theorem 2.1, there exists x such that $a = x'$.

Okay, now we're ready to finish this off.

$$\begin{array}{rlll}
ac = n'c \text{ and } c \neq 0 & \Rightarrow & x'c = n'c \text{ and } c \neq 0 & (a = x') \\
& \Rightarrow & xc + c = nc + c \text{ and } c \neq 0 & \text{Lemma from Theorem 2.3 (4)} \\
& \Rightarrow & xc = nc \text{ and } c \neq 0 & \text{Theorem 2.2 (4)} \\
& \Rightarrow & x = n & \text{Inductive Hypothesis} \\
& \Rightarrow & x' = n' & \text{It's the successor } \textit{function} \\
& \Rightarrow & a = n' & (a = x').
\end{array}$$

Thus $P(n')$ is true.

It follows by PMI that $P(n)$ is true for all natural numbers n.

□

We need a multiplicative identity. Let's call it ... 1.

Definition 2.3. $1 = 0'$.

Note that by Peano Axiom (3), $0' \neq 0$, so $1 \neq 0$.

Theorem 2.4. *Let a and b be natural numbers. Then*

(1) $1 \cdot b = b \cdot 1 = b$*.*

(2) $a' = a + 1$*.*

(3) If $ab = 1$*, then* $a = b = 1$*.*

Proof. Parts (1) and (2) are left as exercises.

(3) Assume $ab = 1$. Then $a \neq 0$ by Theorem 2.3 (1) and similarly, $b \neq 0$ by Theorem 2.3 (4), for otherwise $ab = 0$. Thus there are natural numbers c and d so that $a = c'$ and $b = d'$. By (2), $1 = ab = c'd' = (c+1)(d+1)$.

The distributive laws and commutativity of multiplication proven in Theorem 2.3 allow us to "foil" the product $(c+1)(d+1)$, yielding $dc+d+c+1 = 1$. Theorem 2.2 (4) then yields $dc + d + c = 0$, so $d(c+1) + c = 0$. So from Theorem 2.2 (5) we have $d(c+1) = c = 0$.

Since $c = 0$ and $a = c'$, $a = 1$. Thus $1 = ab = 1 \cdot b = b$ also, by Theorem 2.4 (1).

□

Theorem 2.4 (1) states that 1 is a two-sided identity under multiplication.

Problems. 1. Prove Theorem 2.2 (1) by inducting on b.

2. Prove Theorem 2.2 (4) by inducting on c.

3. Prove Theorem 2.3 (1) by inducting on b.
4. Prove Theorem 2.3 (2) by inducting on c.
5. Prove Theorem 2.3 (5). This does not require induction. Use Problem 4 of Section A, Theorem 2.1, and Theorem 2.2 (5).
6. Prove Theorem 2.4 (1). (Use Definition 2.2 (2) to show $b \cdot 0' = b$.)
7. Use Theorem 2.4 (1) to prove Theorem 2.4 (2). (Use Definition 2.1 (2) to compute $a + 0'$.)

3. The Integers

In this chapter, we axiomatically construct the set of integers, $\mathbb{Z}$, starting with the elements of $\mathbb{N}$. To do this rigorously, we will introduce an equivalence relation on $\mathbb{N} \times \mathbb{N}$, ordered pairs of natural numbers. Addition and multiplication will be defined on these equivalence classes in a way that uses the same operation on $\mathbb{N}$; the most difficult part of the chapter involves showing our proposed definitions of addition and multiplication on these equivalence classes are "well-defined." Once this is done, the algebraic properties of $\mathbb{Z}$ will follow from the algebraic properties of $\mathbb{N}$.

Definition 3.1. Let $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Define $(a, b) \overset{\mathbb{Z}}{\sim} (c, d)$ provided $a + d = b + c$.

Theorem 3.1. *The relation* $\overset{\mathbb{Z}}{\sim}$ *in Definition 3.1 is an equivalence relation on* $\mathbb{N} \times \mathbb{N}$.

Proof. Exercise. □

For example, $(5, 3) \overset{\mathbb{Z}}{\sim} (3, 1)$ and $(5, 11) \overset{\mathbb{Z}}{\sim} (1, 7)$. (You should be thinking $a - b$ when you see (a, b).) Notice that in the first example, the difference between each first component and second component is $+2$, while in the second example, the difference between each first component and second component is -6. This is how we construct the integers.

Definition 3.2. The set of equivalence classes in Definition 3.1 is the set of **integers**, denoted $\mathbb{Z}$.

Consider the equivalence class

$$[(5, 3)] = \{(2, 0), (3, 1), (4, 2), (5, 3), (6, 4), \dots\}.$$

We identify this with the integer 2. Similarly, we identify the equivalence class $[(5, 11)]$ with the integer -6.

Now that we have a formal definition of $\mathbb{Z}$, we want to be able to verify that the usual operations of addition and multiplication hold. The problem is that we are now trying to add/multiply entire sets (the equivalence classes), and we want to somehow use the numbers in the ordered pairs in those sets to do this. Since each set contains infinitely many ordered pairs, we must make a choice of some sort, and if our binary operations are to be "well-defined," we have to get the same result no matter which ordered pair we choose.

Recall that the following are equivalent (TFAE):

- $x = [(a, b)]$
- $(a, b) \in x$

- (a, b) is a representative of x

We would now like to define addition on this set of equivalence classes, $\mathbb{Z}$, that coincides with our experience with addition of integers. To that end, assume (a, b) is a representative of the integer x and (c, d) is a representative of the integer y. We want to compute $x + y$ by adding these representatives, thinking of (a, b) as $a - b$, etc., to see what definition we should establish for addition. To compute the sum $x + y$, we use $(a, b) + (c, d)$, which we think of as $(a - b) + (c - d)$, or equivalently, $(a + c) - (b + d)$, which is the representative $(a + c, b + d)$.

So we hope to define $[(a, b)] + [(c, d)]$ to be $[(a + c, b + d)]$. But first we have to make sure that choosing different representatives from the equivalence classes $[(a, b)]$ and $[(c, d)]$ doesn't change the equivalence class of the sum. The following theorem does just that: it shows that NO MATTER WHICH REPRESENTATIVE ORDERED PAIRS WE CHOOSE FROM EACH EQUIVALENCE CLASS, THE RESULTING SUMS ARE ALL IN THE SAME EQUIVALENCE CLASS.

Theorem 3.2. *Assume* $(a_1, b_1) \overset{\mathbb{Z}}{\sim} (a_2, b_2)$ *and* $(c_1, d_1) \overset{\mathbb{Z}}{\sim} (c_2, d_2)$, *where each component is a natural number. Then* $(a_1 + c_1, b_1 + d_1) \overset{\mathbb{Z}}{\sim} (a_2 + c_2, b_2 + d_2)$.

Proof. Exercise. □

You will see something similar to Theorem 3.2 every time you try to extend a binary operation to a set of equivalence classes of elements that already have a binary operation $\cdot$ defined on them. Basically, you are trying to show the operation

$$[x] \odot [y] = [x \cdot y]$$

makes sense, i.e., is independent of the choice of representative from $[x]$ and $[y]$. Notice that on left side of this equation, we are performing the operation $\odot$ on two *sets*, while on the right side of the equation, we are performing the operation $\cdot$ on two *elements* of those sets.

Anyway, we can now **define addition of integers**:

Definition 3.3. Let $[(a, b)], [(c, d)] \in \mathbb{Z}$. Then their **sum** is

$$[(a, b)] + [(c, d)] = [(a + c, b + d)].$$

Note that each integer $x \in \mathbb{Z}$ is an equivalence class $x = [(a, b)]$, for some $a, b \in \mathbb{N}$. We will need to use this fact and Definition 3.3 to prove various properties of addition of integers.

Definition 3.4. Let $0_{\mathbb{Z}} = [(0, 0)]$.

By the definition of $\overset{\mathbb{Z}}{\sim}$, $\forall n \in \mathbb{N}$, $[(n,n)] = [(0,0)] = 0_{\mathbb{Z}}$.

Theorem 3.3. *(1) For each $a, b \in \mathbb{Z}$, $a + b = b + a$.*

(2) For each $a, b, c \in \mathbb{Z}$, $a + (b + c) = (a + b) + c$.

(3) For each $a \in \mathbb{Z}$, $a + 0_{\mathbb{Z}} = a$.

(4) For each $a \in \mathbb{Z}$, there exists $b \in \mathbb{Z}$ such that $a + b = 0_{\mathbb{Z}}$.

Theorem 3.3 (1) and Theorem 3.3 (2) show is the commutative and associative laws of addition extend to $\mathbb{Z}$. Theorem 3.3 (3) shows $\mathbb{Z}$ contains an additive identity, and Theorem 3.3 (4) shows that every element of $\mathbb{Z}$ has an additive inverse.

Proof. Parts (2) and (4) are left as exercises.

(1) Let $a = [(m,n)]$ and $b = [(k,l)]$. Then

$$\begin{aligned} a + b &= [(m,n)] + [(k,l)] \\ &= [(m+k, n+l)] && \text{Definition of addition} \\ &= [(k+m, l+n)] && \text{Commutativity of addition of naturals} \\ &= [(k,l)] + [(m,n)] && \text{Definition of addition} \\ &= b + a. \end{aligned}$$

(3) Let $a = [(m,n)]$. Then

$$\begin{aligned} a + 0_{\mathbb{Z}} &= [(m,n)] + [(0,0)] \\ &= [(m+0, n+0)] && \text{Definition of addition} \\ &= [(m,n)] \\ &= a. \end{aligned}$$

□

The element b in Theorem 3.3 (4) is unique, for if $a + b = a + \bar{b} = 0_{\mathbb{Z}}$, then $b = 0_{\mathbb{Z}} + b = (\bar{b} + a) + b = \bar{b} + (a + b) = \bar{b} + 0_{\mathbb{Z}} = \bar{b}$. Following convention, we'll denote the additive inverse of the integer a by $-a$.

As we did with addition, we would now like to define multiplication on the set of equivalence classes, $\mathbb{Z}$, that coincides with our experience. To that end, assume (a,b) is a representative of the integer x and (c,d) is a representative of the integer y. We want to compute xy by multiplying these representatives, thinking of (a,b) as $a - b$, etc., to see what definition we should establish. To compute the product xy, we use $(a,b) \cdot (c,d)$, which we think of as $(a-b) \cdot (c-d)$, or equivalently, $ac - ad - bc + bd = (ac + bd) - (ad + bc)$, which is the representative $(ac + bd, ad + bc)$.

So we hope to define $[(a,b)] \cdot [(c,d)]$ to be $[(ac+bd, ad+bc)]$. But, as before, we first have to make sure that choosing different representatives from the equivalence classes doesn't change the product. The following theorem does just that: it shows that WE GET THE SAME PRODUCT NO MATTER WHICH REPRESENTATIVE ORDERED PAIR WE CHOOSE FROM EACH EQUIVALENCE CLASS.

Theorem 3.4. *Assume* $(a_1,b_1) \overset{\mathbb{Z}}{\sim} (a_2,b_2)$ *and* $(c_1,d_1) \overset{\mathbb{Z}}{\sim} (c_2,d_2)$*, where each component is a natural number. Then* $(a_1c_1+b_1d_1, a_1d_1+b_1c_1) \overset{\mathbb{Z}}{\sim} (a_2c_2+b_2d_2, a_2d_2+b_2c_2)$.

Proof. By hypothesis, we know

$$\begin{aligned} a_1+b_2 &= b_1+a_2 \text{ and} \\ c_1+d_2 &= d_1+c_2. \end{aligned}$$

We want to show

$$(a_1c_1+b_1d_1)+(a_2d_2+b_2c_2) = (a_1d_1+b_1c_1)+(a_2c_2+b_2d_2).$$

Since neither side of this equation has any common terms that could be factored, in order to use the equations we know, we must add additional terms. Fortunately, we have the various laws of addition and multiplication of natural numbers at our disposal (associativity, commutativity, the distributive laws), and we will use those freely.

To that end, we take the first term of the left-hand side of the equation we want and add a couple of terms to it:

$$\begin{aligned} (a_1c_1+b_1d_1)+[(b_2c_1+a_2d_1)] &= c_1(a_1+b_2)+d_1(b_1+a_2) \\ &= c_1(b_1+a_2)+d_1(a_1+b_2) \\ &= (b_1c_1+a_1d_1)+\{(a_2c_1+b_2d_1)\}. \end{aligned}$$

Then, we take the second term on the left-hand side of the equation, and add the last term above to it:

$$\begin{aligned} (a_2d_2+b_2c_2)+\{(a_2c_1+b_2d_1)\} &= a_2(c_1+d_2)+b_2(c_2+d_1) \\ &= a_2(c_2+d_1)+b_2(c_1+d_2) \\ &= (a_2c_2+b_2d_2)+[(b_2c_1+a_2d_1)]. \end{aligned}$$

Adding these two equations together yields[1]

$$(a_1c_1+b_1d_1)+(a_2d_2+b_2c_2)+[\ \ ]+\{\ \ \} = (a_1d_1+b_1c_1)+(a_2c_2+b_2d_2)+[\ \ ]+\{\ \ \}.$$

Canceling $[\ \ ]+\{\ \ \}$ from both sides, using Theorem 4.2(4), yields the desired equation. □

[1] Here $[\ \ ] = [(b_2c_1+a_2d_1)]$ and $\{\ \ \} = \{(a_2c_1+b_2d_1)\}$.

So we can now **define multiplication of integers**:

Definition 3.5. Let $[(a, b)], [(c, d)] \in \mathbb{Z}$. Then their **product** is

$$[(a, b)] \cdot [(c, d)] = [(ac + bd, ad + bc)].$$

As with addition, since multiplication is defined by choosing any representative ordered pair from our equivalence class, proving the following theorem is very straightforward.

Theorem 3.5. *(1) For each $a, b \in \mathbb{Z}$, $ab = ba$.*

(2) For each $a, b, c \in \mathbb{Z}$, $a(bc) = (ab)c$.

(3) For each $a, b, c \in \mathbb{Z}$, $a(b + c) = ab + ac$.

This theorem shows the various multiplicative properties (commutativity, associativity, left distributive law) on $\mathbb{N}$ from Theorem 2.3 extend to $\mathbb{Z}$. The proof of each part is similar to those in Theorem 3.3: pick ordered pairs for each equivalence class (i.e., element of $\mathbb{Z}$) and use the appropriate definitions/properties to derive the desired result.

Proof. Parts (2) and (3) are left as exercises.

(1) Let $a = [(m, n)]$ and $b = [(k, l)]$. Then

$$\begin{aligned} ab &= [(mk + nl, ml + nk)] && \text{Definition of multiplication} \\ &= [(km + ln, kn + lm)] && \text{Commutativity laws of naturals} \\ &= ba && \text{Definition of multiplication.} \end{aligned}$$

□

In light of the various theorems in this section, and using the function ϕ in Problem 9, we may identify every natural number n with the integer $[(n, 0)]$ and consider the set of integers as a superset of the set of natural numbers. Every integer is either a natural number or the additive inverse of a natural number, with the familiar algebraic structure given by the rules of addition and multiplication we learned as children.

The only property of the integers which we still haven't developed is that of order; that will come in a later section.

Problems. 1. Prove Theorem 3.1.

2. Draw a section of the lattice points of $\mathbb{N} \times \mathbb{N}$ in the Cartesian plane. Connect points that are equivalent under the relation $\overset{\mathbb{Z}}{\sim}$ of Definition 3.1. Show that each equivalence class is identified with the integer that is the x-intercept of the line you get.
3. Prove Theorem 3.2.
4. Prove Theorem 3.3 (2).
5. Prove Theorem 3.3 (4).
6. Prove Theorem 3.5 (2).
7. Prove Theorem 3.5 (3).
8. Prove $1_{\mathbb{Z}} = [(1, 0)]$ is a multiplicative identity for $\mathbb{Z}$, i.e., $\forall a \in \mathbb{Z}$, $a \cdot 1_{\mathbb{Z}} = 1_{\mathbb{Z}} \cdot a = a$.
9. Define the function $\phi : \mathbb{N} \to \mathbb{Z}$ by $\phi(n) = [(n, 0)]$.
   (a) Prove ϕ is an injection.
   (b) Figure out what ϕ has to do with Problem 2.
   (c) Prove $\phi(m + n) = \phi(m) + \phi(n)$ and $\phi(mn) = \phi(m)\phi(n)$. (So ϕ sends the sum/product of m and n to the sum/product of $\phi(m)$ and $\phi(n)$.)
10. Let $m, n, k, l, r \in \mathbb{N}$. Prove

$$[(m, n)] \cdot [(k, l)] = [(k, l)] \cdot [(m + r, n + r)].$$

4. A Brief Introduction to Rings

In this chapter, we generalize some of the algebraic properties of the integers to sets with two binary operations, similar to addition and multiplication of integers. The benefit of doing this is that any result we can prove from our basic assumptions will apply to all such algebraic structures. This chapter provides a taste of the type of material covered in an "abstract algebra" course.

Let's look at what we developed in the last chapter. We built a set, $\mathbb{Z}$, with two binary operations defined on it, $+$ and $\cdot$, that satisfied some properties (among others):

(1) $+$ was associative.
(2) $+$ had an identity, namely 0.
(3) Every element $n \in \mathbb{Z}$ had an inverse under $+$, namely $-n$.
(4) $+$ was commutative.
(5) $\cdot$ was associative.
(6) $\cdot$ distributed over $+$ from both the left and the right[2].

This brings up an obvious question: what can be said about *every* set with two binary operations that possesses these same properties? And, what other such sets are there? The answer to both questions is, "lots," and such objects are called *rings*.

Definition 4.1. A **ring** is a nonempty set R with two binary operations (usually denoted $+$ and $\cdot$) such that

(1) $+$ is associative.
(2) $+$ has an identity element (usually denoted 0).
(3) Every element of $a \in R$ has an inverse under $+$ (usually denoted $-a$).
(4) $+$ is commutative.
(5) $\cdot$ is associative.
(6) For all $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

If, in addition,

(7) $\cdot$ is commutative,

then R is a **commutative ring**. If (1) – (6) hold and

(8) $\cdot$ has an identity (usually denoted 1),

[2] That is, $a \cdot (b + c) = ab + ac$ and $(a + b) \cdot c = ac + bc$ are the two distributive laws of multiplication over addition. An interesting exercise is to write the (false) distributive laws of addition over multiplication.

then R is a **ring with 1** or **ring with unity**. If all of the above hold, then R is a **commutative ring with unity**.

We saw in the last chapter that $\mathbb{Z}$ under the usual operations forms a commutative ring with unity. If you take a course in abstract algebra, you will see many examples of various types of rings, but you all have some experience with one example: matrices.

Let's restrict our attention to the set of 2×2 matrices under the usual matrix addition (component-wise) and multiplication ("row times column"). The *type* of ring we get depends on the set of entries; in general, the set of 2×2 matrices with entries in the ring R is denoted by $M_2(R)$.

Example 4.1. If $\mathbb{R}$ is the set of real numbers (whatever *they* are), then $M_2(\mathbb{R})$ is a noncommutative ring with unity, as you probably learned if you had any linear algebra. All of the required properties using only addition are easy to show. Proving matrix multiplication is associative is somewhat tedious, but it is true nonetheless. The zero matrix, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, serves as the additive identity, and the identity matrix, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, serves as the multiplicative identity (hence its name). Showing matrix multiplication is not commutative is an easy exercise; just pick two matrices at random and they probably won't commute.

But there is something else about matrix multiplication that we haven't seen with our sets of numbers. For example,

$$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

In other words, the product of those two *nonzero* matrices equals the *zero* matrix (the additive identity). It's easy to construct other such examples. This phenomenon has a name.

Definition 4.2. A nonzero element $a \in R$ is called a **zero divisor** if there exists a nonzero element $b \in R$ such that $ab = 0$.

Hopefully your experience tells you that the set of integers does *not* have any zero divisors. The next theorem proves it.

Theorem 4.1. *The set of integers under $+$ and $\cdot$ has no zero divisors.*

Proof. Let $a, b \in \mathbb{Z}$. Assume $ab = 0_{\mathbb{Z}}$ and $a \neq 0_{\mathbb{Z}}$. We must show $b = 0_{\mathbb{Z}}$. (See Problem 4 of Section A[3].)

Let $a = [(m,n)]$ and let $b = [(k,l)]$. By definition of multiplication, $ab = [(m,n)][(k,l)] = [(mk+nl, ml+nk)]$. Since $ab = 0_{\mathbb{Z}}$ and the zero element of $\mathbb{Z}$ is the equivalence class of ordered pairs whose first and second components are equal, we must have $mk + nl = ml + nk$. Also, since $a \neq 0_{\mathbb{Z}}$, we must have $m \neq n$. So, using a notion fully developed in Chapter 6, either $m > n$ or $m < n$.

By the symmetry of the equation $mk+nl = ml+nk$, there is no loss of generality to assume $m > n$. Thus there exists a nonzero natural number i such that $m = n + i$. But then we have $(n+i)k + nl = (n+i)l + nk$, from which it follows that $ik = il$, so $k = l$. Since $b = [(k,l)]$, we must have $b = 0_{\mathbb{Z}}$. □

So the set of integers under the usual operations is a commutative ring with unity that has no zero divisors. There is a name for such a thing.

Definition 4.3. An **integral domain** is a commutative ring with unity which has no zero divisors.[4]

So the the ring of integers is an example of an integral domain.

At the beginning of this section, we asked what could be said about an arbitrary ring. Below are some properties that must hold for every ring, no matter how bizarre it is. Recall that $-a$ denotes the additive inverse of a, and 0 denotes the additive identity in R.

Theorem 4.2. *Let R be a ring. Then*

(1) $\forall a \in R$, $0 \cdot a = a \cdot 0 = 0$.
(2) $\forall a, b \in R$, $a(-b) = -ab = (-a)b$.
(3) $\forall a, b \in R$, $(-a)(-b) = ab$.

Proof. Part (1) is left as an exercise.

(2) There are two things to prove here: that both $a(-b)$ and $(-a)b$ equal $-ab$, i.e., both are the additive inverse of ab. In order to show that x is the additive inverse of ab, you must simply show $x + ab = 0$.

To that end, $a(-b) + ab = a(-b+b) = a(0) = 0$. Similarly, $(-a)b + ab = 0$. So, *by definition*, $a(-b) = -ab$ and $(-a)b = -ab$.

[3] We are really proving "If $ab = 0_{\mathbb{Z}}$, then $a = 0_{\mathbb{Z}}$ or $b = 0_{\mathbb{Z}}$." This is logically equivalent to "If $ab = 0_{\mathbb{Z}}$ and $a \neq 0_{\mathbb{Z}}$, then $b = 0_{\mathbb{Z}}$".

[4] There is an additional technical assumption that $1 \neq 0$.

(3) By part 2, $(-a)(-b) = -(-a)b$. By part 2 again, $-(-a)b = -(-ab)$. But since ab is the additive inverse of $-ab$, $-(-ab) = ab$. Thus $(-a)(-b) = ab$.

□

Every ring R has an additive identity, denoted 0, and every element $a \in R$ has an additive inverse, denoted $-a$, that satisfies $a + (-a) = 0$. If a ring has unity, then it has a **multiplicative identity**, denoted 1. In this case, an element $a \in R$ might have a **multiplicative inverse**, that is, an element $b \in R$ that satisfies $ab = ba = 1$.

In the ring of integers, $\mathbb{Z}$, the element 5 does not have a multiplicative inverse in $\mathbb{Z}$, since there is no integer n so that $5n = 1_{\mathbb{Z}}$. In the next section, we will enlarge the set of integers to include multiplicative inverses of nonzero integers, resulting in the set of rationals.

Problems. 1. (This problem requires some linear algebra.) Recall $M_2(\mathbb{R})$ is the set of 2×2 matrices with real entries.

(a) Prove multiplication in $M_2(\mathbb{R})$ is not commutative.

(b) Which elements in $M_2(\mathbb{R})$ have multiplicative inverses?

2. Let $2\mathbb{Z}$ denote the set of even integers. Show $2\mathbb{Z}$, under the usual operations of addition and multiplication, is a commutative ring without unity.
3. (This problem requires some linear algebra.) Let $2\mathbb{Z}$ denote the set of even integers. You can assume $M_2(2\mathbb{Z})$ is a ring. Prove it is noncommutative without unity.
4. Prove Theorem 4.2 (1) by using the distributive laws. Here is how to start: $0 \cdot a + 0 \cdot a = (0 + 0) \cdot a$.
5. The set of polynomials in x with real coefficients forms a ring under the usual operations of addition and multiplication of functions:

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (fg)(x) &= f(x)g(x). \end{aligned}$$

What is the additive identity of this ring? Does this ring have unity?

6. Let $\mathbb{Z}_6$ be the set $\{0, 1, 2, 3, 4, 5\}$ with addition and multiplication given by the tables below:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(a) Is there an additive identity?
(b) Which elements have additive inverses?
(c) Is there a multiplicative identity?
(d) Are there any zero-divisors?

7. Let $X = \{a, b\}$. Then $\mathcal{P}(X)$ is *almost* a ring, where the product of two subsets $A, B \subseteq X$ is computed as $A \cap B$ and the sum of A and B is computed as $A \cup B$.
   (a) If $U, V, W \subseteq X$, write out the left distributive law.
   (b) Create tables for addition and multiplication, as in Problem 6.
   (c) Is there an additive identity?
   (d) Is there a multiplicative identity?
   (e) Which elements have additive inverses?
   (f) Which elements have multiplicative inverses?
8. What must be true about the ring R if $(a+b)^2 = a^2 + 2ab + b^2$ always holds[5]?
9. Prove you can cancel in an integral domain, i.e., if $ax = ay$ and $a \neq 0$, then $x = y$. Why do you need to be in an integral domain to do this? Give an example from Problem 6 of three nonzero elements a, x, and y so that $ax = ay$ but $x \neq y$.

A **monoid** is a set M with a binary operation $*$ that satisfies:

- $*$ is associative, that is, $\forall a, b, c \in M$, $a * (b * c) = (a * b) * c$, and
- M has an identity element, e, such that $\forall a \in M$, $e * a = a * e = a$.

So $\mathbb{N}$ under $+$ is a monoid with identity 0. (For those of you who have had some group theory, a monoid is like a group without the requirement that all elements have inverses.) To answer Problems 1-5, if the binary operation is not associative, then it is not a monoid. If it is associative, show it has or doesn't have an identity element. For associativity, you can appeal to things

[5] Here $2ab = ab + ab$.

you already know, like addition and multiplication of any numbers is associative.

---

10. Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices with real entries. Either show this is a monoid under matrix multiplication[6] or show it isn't.
11. Let X be a nonempty set. Either show the set of all functions $X \to X$ under function composition ($(f \circ g)(x) = f(g(x))$) is a monoid or show it isn't.
12. Let $\mathbb{Z}_+$ be the set of positive integers. Either show $\mathbb{Z}_+$ under multiplication is a monoid or show it isn't.
13. Let X be a nonempty set. Either show the power set of X, $\mathcal{P}(X)$, under $\bigcap$ is a monoid or show it isn't.
14. On the set $\mathbb{Z}$ of integers. Define $a * b$ as a^b. Either show $\mathbb{Z}$ with this binary operation is a monoid or show it isn't.
15. Let M be a monoid under $*$ and let $a \in M$. If M is finite, prove $\exists m, n \in \mathbb{Z}_+$, $m \neq n$, such that $a^m = a^n$. (Here $a^m = a * a * a * \cdots * a$ (m times).)

[6] This is how matrix multiplication works: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$.

5. The Rationals

In Chapter 3, we built the integers as equivalence classes of an equivalence relation on ordered pairs of natural numbers; the equivalence relation identified ordered pairs with a common difference between their first and second components. In this chapter, we build the rationals as equivalence classes of an equivalence relation on ordered pairs of integers with nonzero second component; the equivalence relation will identify ordered pairs with a common quotient of their first and second components. As with Chapter 3, once we show our definitions of addition and multiplication on these equivalence classes are well-defined, the algebraic properties of the rationals will follow from the corresponding algebraic properties of the integers.

Since we have already built the integers, we no longer need to consider individual integers as subsets of $\mathbb{N} \times \mathbb{N}$. Rather, we can consider our starting elements as elements of $\mathbb{Z}$, and we have all the usual properties of $\mathbb{Z}$ (except for order) at our disposal.

Definition 5.1. Let $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$. Define $(a, b) \overset{\mathbb{Q}}{\sim} (c, d)$ provided $ad = bc$.

Notice the similarity between this definition and Definition 3.1 on $\mathbb{N} \times \mathbb{N}$; both are of the form $(a, b) \sim (c, d)$ provided $a * d = b * c$ for a binary operation $*$.

Theorem 5.1. *The relation* $\overset{\mathbb{Q}}{\sim}$ *in Definition 5.1 is an equivalence relation on* $\mathbb{Z} \times (\mathbb{Z} - \{0\})$.

Proof. Exercise. □

For example, $(5, 3) \overset{\mathbb{Q}}{\sim} (10, 6)$ and $(2, 5) \overset{\mathbb{Q}}{\sim} (6, 15)$. (You should be thinking $\frac{a}{b}$ when you see (a, b); notice the second component is never 0.) In the first example, the quotient between each first component and second component is $\frac{5}{3}$ in reduced form, while in the second example, the quotient between each first component and second component is $\frac{2}{5}$ in reduced form. When you first learned about rational numbers, you were asked to represent your fractions in reduced form; these reduced forms were really representatives of equivalence classes of fractions. So, to make this precise, we construct the rationals as equivalence classes of the set of ordered pairs of integers with nonzero second component.

Definition 5.2. The set of equivalence classes in Definition 5.1 is the set of **rationals**, denoted $\mathbb{Q}$.

Consider the equivalence class

$$[(5,3)] = \{\ldots, (-15,-9), (-10,-6), (-5,-3), (5,3), (10,6), (15,9)\ldots\}.$$

We identify this with the rational number $\frac{5}{3}$. Similarly, we identify the equivalence class $[(2,5)]$ with the rational number $\frac{2}{5}$. We will write $0_{\mathbb{Q}}$ for the rational number $[(0,1)]$ and $1_{\mathbb{Q}}$ for the rational number $[(1,1)]$; notice $1_{\mathbb{Q}} \neq 0_{\mathbb{Q}}$. See Problem 2.

As with the integers, we want to define the usual operations of addition and multiplication on the rationals, but since we will be trying to add and multiply entire *equivalence classes* using representative elements, we must show these operations are well-defined before we can do anything else.

We would like to define addition on this set of equivalence classes, $\mathbb{Q}$, that coincides with our experience with addition of rationals. To that end, assume (a,b) is a representative of the rational x and (c,d) is a representative of the rational y. We want to compute $x+y$ by adding these representatives, thinking of (a,b) as $\frac{a}{b}$, etc., to see what definition we should establish for addition. To compute the sum $x+y$, we use $(a,b)+(c,d)$, which we think of as $\frac{a}{b}+\frac{c}{d}$, or equivalently, $\frac{ad+bc}{bd}$, which is the representative $(ad+bc, bd)$. So we hope to define $[(a,b)]+[(c,d)]$ to be $[(ad+bc, bd)]$.

We would also like to define multiplication on this set of equivalence classes in a sensible fashion. If, as above, (a,b) is a representative of the rational x and (c,d) is a representative of the rational y, then to compute the product xy, we use $(a,b)\cdot(c,d)$, which we think of as $\frac{a}{b}\cdot\frac{c}{d}$, or equivalently, $\frac{ac}{bd}$, which is the representative (ac, bd). So we hope to define $[(a,b)]\cdot[(c,d)]$ to be $[(ac,bd)]$.

As we did when defining addition and multiplication of integers, we must show both of these binary operations are independent of choices of representatives from the equivalence classes that form the elements of $\mathbb{Q}$.

Theorem 5.2. *Assume $(a_1,b_1) \overset{\mathbb{Q}}{\sim} (a_2,b_2)$ and $(c_1,d_1) \overset{\mathbb{Q}}{\sim} (c_2,d_2)$, where each ordered pair lies in $\mathbb{Z}\times(\mathbb{Z}-\{0\})$. Then*

(1) $(a_1d_1+b_1c_1, b_1d_1) \overset{\mathbb{Q}}{\sim} (a_2d_2+b_2c_2, b_2d_2)$, and
(2) $(a_1c_1, b_1d_1) \overset{\mathbb{Q}}{\sim} (a_2c_2, b_2d_2)$.

Proof. Notice that for each part, $b_1d_1 \neq 0$ and $b_2d_2 \neq 0$, since the second component of each of the original ordered pairs is an element of $\mathbb{Z}-\{0\}$.

Part (1) is left as an exercise.

(2) Assume $(a_1,b_1) \overset{\mathbb{Q}}{\sim} (a_2,b_2)$ and $(c_1,d_1) \overset{\mathbb{Q}}{\sim} (c_2,d_2)$. Then $a_1b_2 = b_1a_2$ and $c_1d_2 = d_1c_2$. Using the commutative and associative properties of the integers as well as these

two equations, we have $(a_1c_1)(b_2d_2) = (a_1b_2)(c_1d_2) = (b_1a_2)(d_1c_2) = (b_1d_1)(a_2c_2)$. But this implies $(a_1c_1, b_1d_1) \overset{\mathbb{Q}}{\sim} (a_2c_2, b_2d_2)$, which is what we need. □

Theorem 5.2 allows us to define addition and multiplication of rationals:

Definition 5.3. Let $[(a,b)], [(c,d)] \in \mathbb{Q}$.

(1) Their **sum** is

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)].$$

(2) Their **product** is

$$[(a,b)] \cdot [(c,d)] = [(ac, bd)].$$

We will use these definitions to prove the familiar properties of addition and multiplication hold for $\mathbb{Q}$. And what are these familiar properties? They are contained in Definition 4.1, the definition of a ring.

Theorem 5.3. *The set of rationals, $\mathbb{Q}$, under the operations of addition and multiplication above, form a commutative ring with unity. The element $0_{\mathbb{Q}} = [(0,1)]$ serves as the additive identity and the element $1_{\mathbb{Q}} = [(1,1)]$ serves as the multiplicative identity.*

Proof. Let $q, r, s \in \mathbb{Q}$, where $(a,b) \in q$, $(c,d) \in r$, and $(e,f) \in s$. Since $a, b, c, d, e, f \in \mathbb{Z}$, we can use the properties of the integers developed in Chapter 3, such as the commutative and associative laws, freely.

(1) $+$ **is associative.**

$$\begin{aligned}
(q+r)+s &= ([(a,b)] + [(c,d)]) + [(e,f)] \\
&= [(ad+bc, bd)] + [(e,f)] \\
&= [((ad+bc)f + bde, bdf)] \\
&= [(adf + bcf + bde, bdf)] \\
&= [(adf + b(cf+de), bdf)] \\
&= [(a,b)] + [(cf+de, df)] \\
&= [(a,b)] + ([(c,d)] + [(e,f)]) \\
&= q + (r+s).
\end{aligned}$$

(2) $+$ **has an identity element.** Exercise: show $0_{\mathbb{Q}} = [(0,1)]$ serves as the additive identity.

(3) **Every element has an inverse under** $+$**.** Exercise: show $-q = [(-a,b)]$ serves as the additive inverse of q.

(4) $+$ **is commutative.**

$$\begin{aligned} q+r &= [(a,b)]+[(c,d)] \\ &= [(ad+bc,bd)] \\ &= [(cb+da,db)] \\ &= [(c,d)]+[(a,b)] \\ &= r+q. \end{aligned}$$

(5) $\cdot$ **is associative.** Exercise.

(6) **The left and right distributive laws hold.** We will show the left distributive law holds; once (7) is proven, the right distributive law will follow.

$$\begin{aligned} q(r+s) &= [(a,b)]([(c,d)]+[(e,f)]) \\ &= [(a,b)][(cf+de,df)] \\ &= [(acf+ade,bdf)] \\ &= [(b(acf+ade),b(bdf))] \quad \text{(Since } (acf+ade,bdf) \overset{\mathbb{Q}}{\sim} (b(acf+ade),b(bdf))\text{)} \\ &= [(acbf+bdae,bdbf)] \\ &= [(ac,bd)]+[(ae,bf)] \\ &= [(a,b)][(c,d)]+[(a,b)][(e,f)] \\ &= qr+qs. \end{aligned}$$

Notice it is not necessary to have $(a,b)((c,d)+(e,f)) = (a,b)(c,d)+(a,b)(e,f)$.

(7) $\cdot$ **is commutative.** Exercise.

(8) $\cdot$ **has an identity.** Exercise: show $1_{\mathbb{Q}} = [(1,1)]$ serves as the multiplicative identity.

□

The usual notation for rationals, $\frac{a}{b}$ for $[(a,b)]$, gives the usual formulas for addition and multiplication of rationals:

- $\dfrac{a}{b}\cdot\dfrac{c}{d} = \dfrac{ac}{bd}$
- $\dfrac{a}{b}+\dfrac{c}{d} = \dfrac{ad+bc}{bd}$

The integers under the usual operations of addition and multiplication, and the rationals under the same operations, both form a commutative ring with 1. But there is a property that the rationals possess that the integers do not: solutions to equations of the form $ax = 1$ for every nonzero element a. The integers only have such a solution for $a = \pm 1$, while the rationals have a solution for all nonzero a:

Theorem 5.4. *Every nonzero rational number*[7] *has a multiplicative inverse in* $\mathbb{Q}$.

Proof. Let $q \in \mathbb{Q}$ and let $(a, b) \in q$. Since q is a nonzero rational, a is a nonzero integer (see Problem 2). So $(b, a) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$. Since

$$\begin{aligned} [(a,b)][(b,a)] &= [(ab,ba)] \\ &= [(1,1)] \quad \text{(Since } (ab,ba) \overset{\mathbb{Q}}{\sim} (1,1)\text{)} \\ &= 1_{\mathbb{Q}} \end{aligned}$$

and multiplication is commutative, $[(b, a)]$ is the multiplicative inverse of $[(a, b)]$. □

In terms of the usual notation, $\frac{b}{a}$ is the multiplicative inverse of $\frac{a}{b}$; the former exists exactly when a is nonzero.

Commutative rings with this property have a special name.

Definition 5.4. A **field** is a commutative ring with unity in which every nonzero element has a multiplicative inverse.

Recall an integral domain is a commutative ring with unity that has no zero divisors. An obvious question to ask is: what is the relationship between integral domains and fields?

Theorem 5.5. *Every field is an integral domain.*

Proof. Since both fields and integral domains are commutative rings with unity, we only need to show that the property of every nonzero element having a multiplicative inverse guarantees there are no zero divisors.

Let F be a field (under the operations $+$ and $\cdot$), let $a, b \in F$, and assume $ab = 0$ where $a, b \neq 0$. Since $a \neq 0$, a has a multiplicative inverse, a^{-1} (this is standard notation for multiplicative inverses). But then $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(0) = 0$, which contradicts the assumption that $b \neq 0$. Thus F has no zero divisors, and is an integral domain. □

At this point, you should be curious about the converse of Theorem 5.5. See Problem 9.

Finally, Problem 9 in Section 3 identified each natural number n with the integer $[(n, 0)]$ in a way that preserved both addition and multiplication; this allowed us to consider $\mathbb{N}$ as a subset of $\mathbb{Z}$. In a similar way, the set of integers can be identified with a subset of $\mathbb{Q}$; see Problem 11. In particular, the additive

[7] That is, every rational except $0_{\mathbb{Q}}$.

identity $0_{\mathbb{Z}}$ of $\mathbb{Z}$ is identified with the additive identity $0_{\mathbb{Q}}$ of $\mathbb{Q}$, and $1_{\mathbb{Z}}$ in the former is identified with $1_{\mathbb{Q}}$ in the latter.

Problems. 1. Prove Theorem 5.1.

2. Prove $(a,b) \in 0_{\mathbb{Q}}$ iff $a = 0$, $(a,b) \in 1_{\mathbb{Q}}$ iff $a = b$, and $1_{\mathbb{Q}} \neq 0_{\mathbb{Q}}$.
3. Prove Theorem 5.2 (1).
4. Prove Theorem 5.3 (2).
5. Prove Theorem 5.3 (3).
6. Prove Theorem 5.3 (5).
7. Prove Theorem 5.3 (7).
8. Prove Theorem 5.3 (8).
9. Show the converse of Theorem 5.5 is false by considering $\mathbb{Z}$.
10. In Section 3 Problem 2, we saw that the integers could be identified with the set of x-intercepts of lines with slope 1 that pass through lattice points of the plane. Show that the line that passes through the origin and the point $(a,b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$, namely the line $y = \frac{b}{a}x$, contains all ordered pairs in the equivalence class $[(a,b)]$. Thus the rationals can be identified with the set of lines through the origin with rational slope.
11. Define $\psi : \mathbb{Z} \to \mathbb{Q}$ by $\psi(a) = [(a,1)]$ (i.e., $a \mapsto \frac{a}{1}$). Prove ψ is an injection.
12. Let $\psi : \mathbb{Z} \to \mathbb{Q}$ be as in Problem 11. Prove for all $a, b \in \mathbb{Z}$, $\psi(a+b) = \psi(a)+\psi(b)$ and $\psi(ab) = \psi(a)\psi(b)$. (So, just like the map $\phi : \mathbb{N} \to \mathbb{Z}$ in Section 3, Problem 9, ψ is an embedding of $\mathbb{Z}$ into $\mathbb{Q}$ that preserves both addition and multiplication, so we can think of $\mathbb{Z} \subseteq \mathbb{Q}$ both in a set-theoretical sense and an algebraic sense.)
13. Find 99 rational numbers greater than $\frac{3}{1234567}$ and less than $\frac{4}{1234567}$.
14. Let T be the subset of rationals that can be expressed as $\frac{a}{3^i}$ for some $a \in \mathbb{Z}$ and some $i \in \mathbb{N}$.
    (a) Prove T is *closed* under addition, that is, the sum of any two elements of T is an element of T.
    (b) Prove T is closed under multiplication too, that is, the product of any two elements of T is an element of T.

6. Order

To be able to build the real numbers from the rational numbers, we need the notion of order, that is, how one can tell when one number – whether a natural number, an integer, or a rational – is “bigger than” another. In this chapter, we develop order for the naturals, then for the integers, and finally for the rationals. As before, induction will be used when working with the naturals, while other algebraic methods will be used when working with the integers and rationals. In particular, for the last two of these sets of numbers, we will define what it means for such a number to be positive, and then use that notion to define order on the full set.

6.1. **Order on** $\mathbb{N}$.

Definition 6.1. Let $m, n \in \mathbb{N}$. Then $m \leq n$ provided there exists $k \in \mathbb{N}$ such that $m + k = n$.

Theorem 6.1. *$\leq$ is a partial order on $\mathbb{N}$.*

Proof. Let $a, b, c \in \mathbb{N}$.

(1) (Reflexive) Since $a + 0 = a$, $a \leq a$.
(2) (Antisymmetric) Assume $a \leq b$ and $b \leq a$. Then $\exists k, l \in \mathbb{N}$ such that $a + k = b$ and $b + l = a$. So $b = a + k = (b + l) + k = b + (l + k)$. Since $b + 0 = b + (l + k)$, $l + k = 0$ by Theorem 2.2 (4), and so $l = k = 0$ by Theorem 2.2 (5). Thus $a = b$.
(3) (Transitive). Exercise.

□

Notice by Theorem 2.4 (2), $\forall n \in \mathbb{N}$, $n + 1 = n'$. Thus $\forall n \in \mathbb{N}$, $n \leq n'$.

Not only do we have a partial order on $\mathbb{N}$, but also any two elements are comparable:

Theorem 6.2. *For all $m, n \in \mathbb{N}$, $m \leq n$ or $n \leq m$.*

Proof. Induct on n. Let $P(n)$ be the statement, “$m \leq n$ or $n \leq m$.”

Base. ($n = 0$.) Since $0 + m = m$, $0 \leq m$. Since $m \leq 0$ or $0 \leq m$, $P(0)$ is true.

Inductive Step. Assume $P(n)$ is true, i.e., $m \leq n$ or $n \leq m$.

Case 1: $m \leq n$**.** Then $m \leq n \leq n'$, so by transitivity, $m \leq n'$.

Case 2: $n \le m$. Then $\exists k$ such that $n + k = m$.
If $k = 0$, then $n = m$, so $m + 1 = n + 1 = n'$, so $m \le n'$.
If $k \neq 0$, then $\exists l$ such that $k = l' = l + 1$. Thus $n' + l = (n + 1) + l = n + (l + 1) = n + k = m$. So $n' \le m$.

Since $m \le n'$ or $n' \le m$, $P(n')$ is true.

It follows by PMI that $P(n)$ is true for all natural numbers n. □

The inductive step in Theorem 6.2 suggests a refined definition:

Definition 6.2. For $m, n \in \mathbb{N}$, $m < n$ provided there exists $k \neq 0$ such that $m + k = n$.

This definition immediately yields a familiar result: $m \le n$ iff $m < n$ or $m = n$. The former occurs when $k \neq 0$, while the latter occurs when $k = 0$.

Since any two elements of $\mathbb{N}$ are comparable, we have, $\forall m, n \in \mathbb{N}$, three distinct possibilities: (1) $m \le n$ but $n \not\le m$, (2) $n \le m$ but $m \not\le n$, and (3) $m \le n$ *and* $n \le m$. But (1) is equivalent to $m < n$, (2) is equivalent to $n < m$, and by the antisymmetric property of inequality, (3) is equivalent to $m = n$.

Thus we have the **trichotomy property** for $\mathbb{N}$: Exactly one of the following is true $\forall m, n \in \mathbb{N}$: $m < n$, $n < m$, or $m = n$.

Some familiar properties follow:

Theorem 6.3. *Let* $m, n, k \in \mathbb{N}$.

(1) $m \le n$ *iff* $m + k \le n + k$.
(2) If $k \neq 0$, *then* $m \le n$ *iff* $km \le kn$.
(3) If $m < n$, *then* $m + 1 \le n$.

Proof. Part (1) is left as an exercise.

(2) Assume $k \neq 0$.

($\Rightarrow$) If $m \le n$, then $\exists l \in \mathbb{N}$ such that $m + l = n$, so $mk + lk = nk$, so $mk \le nk$.

($\Leftarrow$) We'll prove the contrapositive. Assume $m > n$. Then $\exists l \in \mathbb{N}$, $l \neq 0$, such that $m = n + l$. But then $km = kn + kl$ with $kl \neq 0$, so $km > kn$.

(3) If $m < n$, then $\exists k \neq 0$ such that $m + k = n$. Since $k \neq 0$, $\exists l$ such that $k = l + 1$. So $(m + 1) + l = m + (l + 1) = m + k = n$. So $m + 1 \le n$.

□

The next theorem is equivalent to the Principle of Mathematical Induction, but we will only prove it follows from it. It is known as the **Well-Ordering Principle** and also as the **Least Natural Number Principle**. An element $x \in X$ is a **least element** of X if $\forall y \in X$, $x \le y$. Such elements are unique (see Problem 3).

Well-Ordering Principle. Every nonempty set of natural numbers has a least element.

Proof. Let T be a nonempty subset of $\mathbb{N}$. Define $S = \{n \in \mathbb{N} \mid \forall t \in T, n \leq t\}$. Then $0 \in S$, since $0 \leq n \ \forall n \in \mathbb{N}$. Also, $S \neq \mathbb{N}$, for otherwise $T = \emptyset$. Thus $\exists s \in S$ such that $s + 1 \notin S$, for otherwise the Principle of Mathematical Induction implies $S = \mathbb{N}$.

We claim s is the least element of T. Since $s \in S$, we already know $\forall t \in T$, $s \leq t$, so it only remains to show $s \in T$. But if $s \notin T$, then $\forall t \in T$, $s < t$, so $s + 1 \leq t$, so $s + 1 \in S$, a contradiction of the previous paragraph. Thus T has a least element, s. □

6.2. **Order on $\mathbb{Z}$.** Recall $\mathbb{Z}$ was defined as the set of equivalence classes of $\mathbb{N} \times \mathbb{N}$ under the relation $(a, b) \overset{\mathbb{Z}}{\sim} (c, d)$ provided $a + d = b + c$, and we really think of (a, b) as $a - b$. We want to use the order on $\mathbb{N}$ to define order on $\mathbb{Z}$. This next theorem essentially shows $\leq$ is well-defined on $\mathbb{Z}$.

Theorem 6.4. *Let $k, l, m, n \in \mathbb{N}$ and assume $(k, l) \overset{\mathbb{Z}}{\sim} (m, n)$. Then*

(1) $k < l$ iff $m < n$.
(2) $k > l$ iff $m > n$.
(3) $k = l$ iff $m = n$.

Proof. (1) Since $(k, l) \overset{\mathbb{Z}}{\sim} (m, n)$, we know $k + n = l + m$. Using this, together with the various properties of addition of the naturals, yields the following string of double implications:

$$\begin{aligned} k < l &\Leftrightarrow \exists x \neq 0 \text{ such that } k + x = l \\ &\Leftrightarrow \exists x \neq 0 \text{ such that } k + n + x = l + n \\ &\Leftrightarrow \exists x \neq 0 \text{ such that } l + m + x = l + n \quad \text{(since } k + n = l + m\text{)} \\ &\Leftrightarrow \exists x \neq 0 \text{ such that } m + x = n \\ &\Leftrightarrow m < n \end{aligned}$$

(2) The argument is similar to that of (1).
(3) Exercise. See Problem 4.

□

Definition 6.3. Let $a = [(m, n)] \in \mathbb{Z}$. Then a is **positive** if $m > n$, and a is **negative** provided $m < n$.

By Theorem 6.4, these concepts are well-defined. Notice the integer $0 = 0_{\mathbb{Z}}$, which was defined as $[(0,0)]$, is neither positive nor negative. Problem 6 revisits the identification of the natural number n with the integer $[(n,0)]$, i.e., the nonzero natural numbers and the positive integers can be considered identical. So, **sums and products of positive integers are positive**, since sums and products of nonzero natural numbers are nonzero natural numbers, by Theorem 2.2 (5) and Theorem 2.3 (5). Problem 7 shows for all nonzero integers a, either a or $-a$ is positive, but not both.

Now that we can tell which integers are positive, we can order $\mathbb{Z}$:

Definition 6.4. Let $a, b \in \mathbb{Z}$. Then $a < b$ if $b - a$ is positive and $a > b$ if $b - a$ is negative.

Problem 7 applied to $b - a$ gives the **trichotomy property for** $\mathbb{Z}$: Exactly one of the following is true $\forall a, b \in \mathbb{Z}$: $a < b$, $a > b$, or $a = b$. We can now write what we are used to writing: a is positive if $a > 0$, and a is negative if $a < 0$. As usual, we write $a \leq b$ if $a < b$ or $a = b$, and similarly for $a \geq b$.

Here are some familiar properties:

Theorem 6.5. *Let $a, b, c \in \mathbb{Z}$.*

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

Proof. Part (1) is left as an exercise.

(2) We have that $b - a > 0$. Since $c > 0$ and the product of positive integers is positive by Theorem 2.3 (5), we have $c(b - a) > 0$. It follows by the commutative and distributive laws for $\mathbb{Z}$ that $bc - ac > 0$. Thus $ac < bc$.

□

The following should not be surprising.

Corollary 6.1. *Let x be any nonzero integer. Then $x^2 > 0$.*

Proof. If $x > 0$, then Theorem 6.5 (2) implies $xx > 0x = 0$, so $x^2 > 0$. On the other hand, if $x < 0$, then by Definition 6.4, $0-x$ is positive. Thus $(0-x)(0-x) = (-x)(-x)$ is positive. But by Theorem 4.2 (3), $(-x)(-x) = x^2$. So $x^2 > 0$ in this case as well. □

6.3. **Order on $\mathbb{Q}$.** Now we want to extend the order we have developed on $\mathbb{Z}$ to all of $\mathbb{Q}$ by reducing questions about signs of quotients of integers to questions about signs of products of integers, since our experience tells us that the sign of a quotient of two integers is the same as the sign of their product. Recall the equivalence relation on $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ that yielded $\mathbb{Q}$: $(a, b) \overset{\mathbb{Q}}{\sim} (c, d)$ provided $ad = bc$. We will use this to define positive/negative rationals. But first, we must show this notion is well-defined:

Theorem 6.6. *Assume $(a, b) \overset{\mathbb{Q}}{\sim} (c, d)$ in $\mathbb{Z} \times (\mathbb{Z} - \{0\})$. Then $ab > 0$ iff $cd > 0$.*

Proof. Since $(a, b) \overset{\mathbb{Q}}{\sim} (c, d)$, we know $ad = bc$, so $(ad)(bd) = (bc)(bd)$. (Notice $b, d \in \mathbb{Z} - \{0\}$.). Thus $(ab)(d^2) = (cd)(b^2)$. Corollary 6.1 implies that both d^2 and b^2 are positive.

Assume $ab > 0$. By Theorem 6.5 (2), $(ab)(d^2) > (0)(d^2) = 0$. Substitution yields $(cd)(b^2) > 0$. We assert this implies $cd > 0$, for if $cd < 0$, then Theorem 6.5 (2) yields $(cd)(b^2) < 0$, a contradiction.

A similar argument shows if $cd > 0$, then $ab > 0$.

□

We can now divide the rationals into the same three categories that we divided the naturals and the integers.

Definition 6.5. Let $q = [(a, b)] \in \mathbb{Q}$. Then q is **positive** if $ab > 0$, q is **negative** if $ab < 0$, and $q = 0$ if $a = 0$.

As usual, we will write $q > 0$ if q is positive, etc. This provides the order on $\mathbb{Q}$ we need:

Definition 6.6. Let $q, r \in \mathbb{Q}$. Then $q < r$ if $r - q$ is positive and $q > r$ if $r - q$ is negative.

Theorem 6.7. *Both the sum and the product of two positive rationals are positive.*

Proof. Suppose q and r are positive rationals, and let $q = \frac{a}{b}$ and $r = \frac{c}{d}$. (Note: This really means (a, b) is a representative of q, etc.) Then by hypothesis, $ab > 0$ and $cd > 0$.

Since $q + r = \frac{ad+bc}{bd}$, in order to show $q + r > 0$, we must show the integer inequality $(ad + bc)bd > 0$. As in the proof of Theorem 6.6, $abd^2 > 0$ and $cdb^2 > 0$, so $abd^2 + cdb^2 > 0$, which implies $(ad + bc)bd > 0$, as desired.

The proof that the product of two positive rationals is positive is left as an exercise. □

Here is the extension of Theorem 6.5 to $\mathbb{Q}$:

Theorem 6.8. *Let $q, r, s \in \mathbb{Q}$.*

(1) If $q < r$, then $q + s < r + s$.
(2) If $q < r$ and $s > 0$, then $qs < rs$.

Proof. Part (1) is left as an exercise.

(2) Since $q < r$, we know $r-q$ is positive. Since s is positive, by Theorem 6.7, $(r - q)s = rs - qs$ is also positive. Thus $qs < rs$.

□

Here is another familiar result:

Theorem 6.9. *Let $q, r \in \mathbb{Q}$. Then $q < r$ iff $-r < -q$.*

Proof. $q < r$ iff $r - q$ is positive iff $(-q) - (-r)$ is positive iff$-r < -q$. □

While there is a "next largest natural number" and a "next largest integer," there is no such thing as a "next largest rational":

Theorem 6.10. *If q and r are rationals with $q < r$, then there exists a rational s such that $q < s < r$.*

Proof. Maybe the easiest such s is the average of q and r.

Since $q < r$, applying Theorem 6.8 (1) twice yields $q + q < q + r < r + r$, so $2q < q + r < 2r$. Multiplying all terms by $\frac{1}{2}$, using Theorem 6.8 (2) twice, gives $q < \frac{1}{2}(q + r) < r$. Thus $s = \frac{1}{2}(q + r)$ satisfies our required condition.

□

Lastly, here is a famous and useful theorem:

Theorem 6.11. *(**The Archimedean Property for** $\mathbb{Q}$) Let s and r be positive rationals. Then there exists a positive integer n such that $nr > s$.*

Proof. Let a, b, c, d be positive integers such that $r = \frac{a}{b}$ $s = \frac{c}{d}$, and let $n = c(b+1)$. Then

$$\begin{aligned} rn &= \frac{a}{b} \cdot c(b+1) \\ &= \frac{ac(b+1)}{b} \\ &> ac \\ &= \frac{acd}{d} \\ &\geq \frac{c}{d} \quad \text{(since } ad \geq 1\text{)} \\ &= s. \end{aligned}$$

□

This theorem essentially says that no matter how big $s > 0$ is and no matter how small $r > 0$ is, if you add r to itself enough times ($nr = r + r + r + \ldots r$), you will get a rational bigger than s. The saying is "you can fill a large tub with a small spoon."

Problems. 1. Finish the proof of Theorem 6.1 (i.e., $\leq$ is transitive).

2. Prove Theorem 6.3 (1). Theorem 2.2 (4) might be useful.
3. Let X be a partially ordered set under $\preceq$. An element $x \in X$ is a **least element** of X if $\forall y \in X$, $x \preceq y$. Use the antisymmetric property of $\preceq$ to show that if X has a least element, then it is unique.
4. Prove Theorem 6.4 (3). Again, Theorem 2.2 (4) might be useful.
5. Show that Theorem 6.5(2) with $a = 0$ implies *the product of two positive integers is positive.*
6. Problem 9 in Section 3.2 identifies each natural number n with the integer $[(n, 0)]$. Use this to identify the set of positive integers, as in Definition 6.3, with the nonzero elements of $\mathbb{N}$.
7. Show that for every nonzero integer a, either a or $-a$ is positive, but not both. Notice if $a = [(m, n)]$ is nonzero, then $m \neq n$.
8. Prove Theorem 6.5 (1). Notice if $b - a$ is positive, then so is $b - a + (c - c)$.
9. Prove Theorem 6.8 (1). Notice if $r - q$ is positive, then so is $r - q + (s - s)$, so the same argument as that in the proof of Theorem 6.5 (1) holds.
10. Finish the proof of Theorem 6.6. Specifically, show if $cd > 0$, then $ab > 0$.
11. Finish the proof of Theorem 6.7.

7. Sequences

In this chapter, we study sequences of rational numbers. Much of this material will be familiar from Calculus, with three notable exceptions. First, the terms of our sequences will be rationals, not arbitrary reals. Secondly, we will discuss subsequences of sequences, which you might not have seen before. Thirdly, we will define the notion of a Cauchy sequence, which might also be a new concept. The material from this point on will be more analytic than algebraic; the flavor is that of a course in "advanced Calculus" or "real analysis" than of "abstract algebra." Quantifiers are used heavily in the definitions, so consider them carefully.

We will assume all algebraic properties of $\mathbb{Q}$ from Chapter 5 as well as its order properties from Chapter 6.

Recall $\mathbb{Z}_+$ is the set of positive integers. Similarly, $\mathbb{Q}_+$ denotes the set of positive rationals.

Definition 7.1. A **sequence** of elements of a set X is a function $f : \mathbb{Z}_+ \to X$. We write a_n for $f(n)$ and denote the sequence by (a_n).

You have seen sequences of real numbers (or "real-valued sequences") in Calculus. In this section, we only study sequences of rational numbers, such as $a_n = \frac{n}{n+1}$ $(\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots)$.

Before we can talk about what it means for a sequence to "converge," we need the concept of absolute value of any rational q, $|q|$:

$$|q| = \begin{cases} q & \text{if } q \geq 0 \\ -q & \text{if } q < 0 \end{cases}$$

In Chapter 6, we saw that any two rationals are comparable under $\leq$, which allows us to place them in increasing order, forming the "rational line." Using this line, $\forall q \in \mathbb{Q}$, $|q|$ can be interpreted as the distance between q and 0. Using the definition of absolute value, we see $\forall q, r \in \mathbb{Q}$,

$$|q - r| = \begin{cases} q - r & \text{if } q \geq r \\ r - q & \text{if } q < r \end{cases}$$

From this, $|q - r|$ can be interpreted as **the distance between** q **and** r**.** This interpretation will be used often.

Definition 7.2. A sequence of rationals (a_n) **converges in** $\mathbb{Q}$ provided $\exists a \in \mathbb{Q}$ such that $\forall \epsilon \in \mathbb{Q}_+$, $\exists N \in \mathbb{Z}_+$ such that $|a_n - a| < \epsilon$ whenever $n > N$. We write $\lim\limits_{n\to\infty} a_n = a$ or $(a_n) \to a$ in this case. If no such $a \in \mathbb{Q}$ exists, we say (a_n) **diverges in** $\mathbb{Q}$.

The idea is that the terms a_n of a convergent sequence get arbitrarily close (and stay close) to the limit a as n gets large. Limits of convergent sequences are unique. The proof is the same as the one you should have seen in Calculus.

We need some technical results about absolute value.

Theorem 7.1. *Let* $a, b \in \mathbb{Q}$ *and assume* $b > 0$. *Then* $|a| < b$ *iff* $-b < a < b$.

Proof. We use Theorem 6.9 extensively: $\forall q, r \in \mathbb{Q}$, $q < r$ iff $-r < -q$.

Notice if $a = 0$, the theorem is true, since $0 < b$ iff $-b < 0 < b$. So we can assume $a \neq 0$.

($\Rightarrow$) Assume $|a| < b$. If $a > 0$, then $a = |a| < b$. Since $a < b$, $-b < -a$. Since $-a < a$, $-b < a$. Thus $-b < a < b$. On the other hand, if $a < 0$, then $a < 0 < b$. Also, $-a = |a| < b$, so $-b < a$. So, again, $-b < a < b$.

($\Leftarrow$) Assume $-b < a < b$. If $a > 0$, then $|a| = a < b$. On the other hand, if $a < 0$, then since $-b < a$, we have $|a| = -a < b$.

□

Triangle Inequality. Let $a, b \in \mathbb{Q}$. Then $|a + b| \leq |a| + |b|$.

Proof. Notice the statement is trivially true if either $a = 0$ or $b = 0$, so assume neither a nor b is 0.

Since $-|a| \leq a \leq |a|$ and $-|b| \leq b \leq |b|$, adding these gives $-(|a| + |b|) \leq a + b \leq (|a| + |b|)$, so applying Theorem 7.1 with $\leq$ instead of $<$ gives $|a + b| \leq (|a| + |b|)$. □

Now we can continue our study of sequences.

Definition 7.3. Let (a_n) be a sequence. The sequence (a_{k_n}) is a **subsequence** of (a_n) provided $k_n < k_{n+1}$ for all n.

The idea is that a subsequence of a sequence contains a subset of the terms of the original, but keeps them in order (since $n \leq k_n < k_{n+1}$). For example, if $a_n = 2n - 1$, then the terms of (a_n) are $1, 3, 5, 7, 9, 11, \ldots$. If $k_n = 2n$, then the subsequence (a_{k_n}) has terms $3, 7, 11, 15, \ldots$.

Theorem 7.2. *If* (a_n) *is convergent, then every subsequence of* (a_n) *converges to the same value as* (a_n).

Proof. Assume (a_n) converges to $a \in \mathbb{Q}$, let (a_{k_n}) be a subsequence of (a_n), and let $\epsilon \in \mathbb{Q}_+$. Then $\exists N \in \mathbb{Z}_+$ such that $|a_n - a| < \epsilon$ whenever $n > N$. But $n > N$ implies $k_n \geq n > N$, so $|a_{k_n} - a| < \epsilon$ whenever $n > N$. So $(a_{k_n}) \to a$. □

The contrapositive of Theorem 7.2 is handy: *if either a subsequence of a sequence diverges or two subsequences converge to different things, then the original sequence must diverge.*

Definition 7.4. The sequence (a_n) is

- **bounded above** if $\exists U \in \mathbb{Q}$ such that $\forall n \in \mathbb{Z}+$, $a_n \leq U$.
- **bounded below** if $\exists L \in \mathbb{Q}$ such that $\forall n \in \mathbb{Z}+$, $a_n \geq L$.
- **bounded** if it is bounded above and below.

Notice that (a_n) is bounded iff $\exists K \in \mathbb{Q}$ such that $\forall n \in \mathbb{Z}_+$, $|a_n| \leq K$, since we can take $K = \max\{|U|, |L|\}$.

Theorem 7.3. *If (a_n) is convergent, then (a_n) is bounded.*

Proof. By hypothesis, for $\epsilon = 1$, $\exists N \in \mathbb{Z}_+$ such that $|a_n - a| < 1$ whenever $n > N$. But then $|a_n| = |a_n - a + a| \leq |a_n - a| + |a| < 1 + |a|$ whenever $n > N$. Thus $|a_n| < 1 + |a|$ whenever $n > N$, so $\{a_n \mid n > N\}$ is bounded. It remains to consider the first N terms of a_n, which might be greater than $1 + |a|$ or less than $-1 - |a|$. But since there are only finitely many of these terms, if we take $K = \max\{1 + |a|, |a_1|, |a_2|, \ldots, |a_N|\}$, then $|a_n| \leq K$ for all n. □

Definition 7.5. The sequence (a_n) is **Cauchy** if $\forall \epsilon \in \mathbb{Q}_+$, $\exists N \in \mathbb{Z}_+$ such that $|a_n - a_m| < \epsilon$ whenever $n, m > N$.

The idea is that the terms of a Cauchy sequence get arbitrarily close (and stay close) to *each other* as n gets large.

Theorem 7.4. *If (a_n) is convergent, then (a_n) is Cauchy.*

Proof. Assume $(a_n) \to a$, and let $\epsilon \in \mathbb{Q}_+$. Then $\exists N \in \mathbb{Z}_+$ such that $|a_n - a| < \frac{\epsilon}{2}$ whenever $n > N$. So, if $n, m > N$, $|a_n - a_m| = |(a_n - a) + (a - a_m)| \leq |a_n - a| + |a - a_m| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$. Thus (a_n) is Cauchy. □

Theorem 7.5. *If (a_n) is Cauchy, then (a_n) is bounded.*

Proof. Following the proof of Theorem 7.3, for $\epsilon = 1$, $\exists N \in \mathbb{Z}_+$ such that $|a_n - a_m| < 1$ whenever $n, m > N$. So using $m = N + 1$, we have $|a_n - a_{N+1}| < 1$ whenever $n > N$, so $-1 < a_n - a_{N+1} < 1$, so $a_{N+1} - 1 < a_n < a_{N+1} + 1$. So for $n > N$, we have $a_{N+1} - 1$ for a lower bound for (a_n) and $a_{N+1} + 1$ as an upper bound. However, one of the earlier terms may be bigger/smaller, so we must take the max/min of $\{a_1, a_2, \ldots, a_N, a_{N+1} \pm 1\}$ for our bounds. □

So from Theorem 7.4 and Theorem 7.5, we have

Convergent ⇒ Cauchy ⇒ bounded.

Notice this gives Theorem 7.3, Convergent ⇒ bounded. In fact, none of these three implications is reversible. Problem 10 asks for a counterexample to two of them. Here is the third:

Example 7.1. Let (a_n) be the rational sequence defined by

$$\begin{aligned} a_1 &= 1.4 \\ a_2 &= 1.41 \\ a_3 &= 1.414 \\ &\vdots \\ a_n &= 1.b_1b_2\ldots b_n \\ &= \text{ the first } n+1 \text{ digits of the decimal expansion of } \sqrt{2}. \end{aligned}$$

Then (a_n) is a rational sequence, since each term has a terminating decimal expansion.

We assert that (a_n) is Cauchy. Given $\epsilon \in \mathbb{Q}_+$, the Archimedean Property shows there exists $N \in \mathbb{Z}_+$ such that $\epsilon \cdot 10^N > 1$, i.e., $1 \times 10^{-N} < \epsilon$. But then, if $n > m > N$, we have the following decimal representation for $a_n - a_m$:

$$\begin{aligned} a_n - a_m &= 1.b_1b_2\ldots b_m\ldots b_n - 1.b_1b_2\ldots b_m \\ &= 0.\underbrace{000\ldots 00}_{m \text{ digits}}b_{m+1}b_{m+2}\ldots b_n \\ &< 0.\underbrace{000\ldots 01}_{m \text{ digits}} \\ &< 0.\underbrace{000\ldots 01}_{N \text{ digits}} \\ &= 1 \times 10^{-N} \\ &< \epsilon, \end{aligned}$$

from which it follows that (a_n) is Cauchy.

But (a_n) does not converge to any rational number. It does have a limit, namely $\sqrt{2}$, but that limit is not rational; see Problem 12. So (a_n) is Cauchy but not convergent in $\mathbb{Q}$.

Example 7.2. You may recall from Calculus that the sequence $a_n = (1 + \frac{1}{n})^n$ converges to the irrational number e. (The proof involved using the natural logarithmic function and L'Hôpital's Rule.) As in Example 7.1, each term of this sequence is rational, the sequence is Cauchy, but it doesn't converge in $\mathbb{Q}$.

Tossing in "limit points" to eliminate non-convergent Cauchy sequences of rationals like the one in the above examples is next. This will give us the irrational numbers.

Problems. 1. Find a formula for the general term a_n of the sequence, assuming the pattern continues: $\{4, -1, \frac{1}{4}, -\frac{1}{16}, \frac{1}{64}, \ldots\}$.

2. If $a_n = \dfrac{3 + 5n^2}{n + n^2}$, find the limit of the sequence (a_n).
3. If $a_n = \dfrac{(2n-1)!}{(2n+1)!}$, find the limit of the sequence (a_n).
4. Here is the recursive step for a sequence (a_n):
$$a_{n+1} = \begin{cases} \frac{1}{2}a_n & \text{if } a_n \text{ is even} \\ 3a_n + 1 & \text{if } a_n \text{ is odd} \end{cases}$$
The sequence itself depends on the base term a_1; different values of a_1 give different sequences. For example, if $a_1 = 5$, then the sequence (a_n) is $5, 16, 4, 2, 1, 4, 2, 1, 4, 2, 1, \ldots$.
   (a) Write out enough terms of the sequence (a_n) if $a_1 = 10$ until you see a similar ending pattern.
   (b) Do the same if $a_1 = 11$.

   There is a very famous unproven conjecture, the Collatz conjecture, that if a_1 is any positive integer, then eventually you arrive at some $a_n = 1$. It has been shown to hold for positive integers up to 2.95×10^{20}, but of course there are still infinitely many more to check.
5. Negate Definition 7.2 to show what it means for $\lim\limits_{n\to\infty} a_n \neq a$.
6. Prove $(\frac{1}{n})$ converges to 0.
7. Using the negation of Definition 7.2, prove $((-1)^n)$ does not converge to 1.
8. Give three subsequences of $a_n = \frac{1}{n}$.
9. Use the contrapositive of Theorem 7.2 to show that $((-1)^n)$ diverges.
10. Give an example of a bounded sequence that is not Cauchy (hence not convergent).
11. There are different forms of the Triangle Inequality. Prove the following:

    If $\forall a, b \in \mathbb{Q}$, $|a + b| \leq |a| + |b|$, then $\forall a, b \in \mathbb{Q}$, $|a - b| \leq |a| + |b|$.

12. Prove $\sqrt{2}$ is irrational, or look up a proof and read it until you understand it.
13. Assume $(a_n) \to a$, let $k \in \mathbb{Q}$, and let $b_n = ka_n \ \forall n \in \mathbb{Z}_+$. Prove $(b_n) \to ka$.
14. Let s be a number with a non-terminating decimal expansion. Following the idea of Example 9.1, show the sequence (a_n) given by

$$\begin{aligned} a_n &= \text{(integer part of } s) \ + 0.b_1 b_2 \dots b_n \\ &= \text{(integer part of } s) + \text{the first } n \text{ digits after the decimal point of the decimal expansion} \end{aligned}$$

is a Cauchy sequence[8].

15. Here is a basic quantifier fact: Assume a is constant and $\epsilon > 0$. Prove if $\forall \epsilon$, $|x - a| < \epsilon$, then $x = a$. (Hint: Contrapositive.)
16. Let $a_n = \dfrac{1}{n^2}$ and let $k_n = n^3 + 1$. Find the first four terms of the subsequence (a_{k_n}) of (a_n). (Write them as fractions, not as decimals.)
17. In Calculus II, you studied infinite series by relating each to its sequence of partial sums. Specifically, the sequence of partial sums of the series $\displaystyle\sum_{n=1}^{\infty} a_n$ is (s_n), where $s_n = a_1 + a_2 + \cdots + a_n$. Then, $\displaystyle\sum_{n=1}^{\infty} a_n = \lim_{n\to\infty} s_n$. The problem is that you rarely can find a closed form for s_n.

    Here is a series where you **can** find a closed form for s_n: $\displaystyle\sum_{n=1}^{\infty} \left(\frac{1}{\sqrt{n}} - \frac{1}{\sqrt{n+1}} \right)$. Find a formula for s_n and use it to find the sum of the series. (Hint: Write out a few terms and observe.)
18. The only thing that matters for the convergence/divergence of a series is the **tail** of the series, that is, what happens to the terms eventually. For example, if two sequences differ in the first bazillion terms but are equal eventually, then either both converge or both diverge. Explain why only the tail of the sequence matters for convergence.

[8] For example, if $s = \frac{7}{3}$, then $a_1 = 2.3$, $a_2 = 2.33$, $a_3 = 2.333$, $\dots$.

8. The Reals

In this chapter, we will define the set of real numbers as a set of equivalence classes of Cauchy sequences of rational numbers. Then we will define the operations of addition and multiplication of those Cauchy sequences, and show that those operations are well-defined on the set of equivalence classes. Once those operations are shown to be well-defined, the various algebraic properties of the reals will follow from those of the rationals.

At this point, one might wonder why we don't try to build the reals from the rationals in the same way we built the rationals from the integers or the integers from the naturals: as equivalence classes of ordered pairs of rationals. One fundamental reason has to do with cardinality, or the "size" of the sets in question. There are just "too many" reals to construct in this fashion. We need, essentially, to use equivalence classes on $\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}\times\ldots$, which is what sequences of rationals really are, in order to get a set large enough to cover the reals.

We start by defining our equivalence relation on rational Cauchy sequences.

Definition 8.1. If (a_n) and (b_n) are rational Cauchy sequences, then $(a_n) \overset{\mathbb{R}}{\sim} (b_n)$ provided $\forall\epsilon \in \mathbb{Q}_+$, $\exists N \in \mathbb{Z}_+$ such that $|a_n - b_n| < \epsilon$ whenever $n > N$.

So $(a_n) \overset{\mathbb{R}}{\sim} (b_n)$ provided those two sequences become arbitrarily close to each other (and stay close) as n gets large.

Theorem 8.1. *The relation $\overset{\mathbb{R}}{\sim}$ in Definition 8.1 is an equivalence relation on the set of all rational Cauchy sequences.*

Proof. The reflexive and symmetric properties are exercises; see Problem 1. For the transitive property, assume $(a_n) \overset{\mathbb{R}}{\sim} (b_n)$ and $(b_n) \overset{\mathbb{R}}{\sim} (c_n)$, and let $\epsilon \in \mathbb{Q}_+$ be given. Then $\exists N_1, N_2 \in \mathbb{Z}_+$ such that $|a_n - b_n| < \frac{\epsilon}{2}$ whenever $n > N_1$ and $|b_n - c_n| < \frac{\epsilon}{2}$ whenever $n > N_2$, so by the triangle inequality,

$$|a_n - c_n| \leq |a_n - b_n| + |b_n - c_n| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon,$$

whenever $n > \max\{N_1, N_2\}$, so $(a_n) \overset{\mathbb{R}}{\sim} (c_n)$. □

An immediate consequence is that if $(a_n) \to a$, then $(a_n) \overset{\mathbb{R}}{\sim} (a)$, where (a) is a constant sequence (i.e., all the terms equal a). See Problem 2. So, by transitivity, *all rational Cauchy sequences with the same limit are equivalent to each other.*

We want to add and multiply rational sequences. Let's try the obvious thing: adding and multiplying term-by-term.

Definition 8.2. Let (a_n) and (b_n) be rational sequences. Define

(1) $(a_n) + (b_n) = (a_n + b_n)$ and
(2) $(a_n)(b_n) = (a_n b_n)$.

Notice the left hand sides of the equations are the sum/product of rational *sequences*, which we are trying to define, while the right hand sides are sequences determined by the sums/products of rational *numbers*, which we already know how to do.

These definitions hold for any sequences, but we only care about Cauchy sequences. So we need to show that sums/products of Cauchy sequences are also Cauchy.

Theorem 8.2. *If (a_n) and (b_n) are rational Cauchy sequences, then so are $(a_n + b_n)$ and $(a_n b_n)$.*

Proof. Assume (a_n) and (b_n) are rational Cauchy sequences. We know each $a_n + b_n$ and each $a_n b_n$ is rational, so we only need to show the resulting sequences are Cauchy. The proof that $(a_n + b_n)$ is Cauchy is similar to the proof of Theorem 8.1 and left as an exercise; see Problem 4.

Let $\epsilon \in \mathbb{Q}_+$. To show $(a_n b_n)$ is Cauchy, we must find $N \in \mathbb{Z}_+$ such that $|a_n b_n - a_m b_m| < \epsilon$ whenever $n, m > N$.

Since both (a_n) and (b_n) are Cauchy, they are both bounded (Theorem 7.5), so $\exists B_1, B_2 \in \mathbb{Q}_+$ such that $\forall n \in \mathbb{Z}_+$, $|a_n| < B_1$ and $|b_n| < B_2$. Notice

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n b_n - a_m b_m + (a_m b_n - a_m b_n)| \\ &= |a_n b_n - a_m b_n + a_m b_n - a_m b_m| \\ &\leq |a_n b_n - a_m b_n| + |a_m b_n - a_m b_m| \\ &= |b_n||a_n - a_m| + |a_m||b_n - b_m|. \end{aligned}$$

Since we have bounds on the size of $|b_n|$ and $|a_m|$, and we can make both $|a_n - a_m|$ and $|b_n - b_m|$ as small as we like (since they are Cauchy), we can make $|a_n b_n - a_m b_m|$ as small as we like as follows.

Let $B = \max\{B_1, B_2\}$. From the previous paragraph, $\forall n \in \mathbb{Z}_+$, $|a_n|, |b_n| < B$. Since both (a_n) and (b_n) are Cauchy, there exist $N_1, N_2 \in \mathbb{Z}_+$ such that $|a_n - a_m| < \frac{\epsilon}{2B}$ whenever $n, m > N_1$ and $|b_n - b_m| < \frac{\epsilon}{2B}$ whenever $n, m > N_2$. Then, whenever $n, m > \max\{N_1, N_2\} = N$, $|b_n||a_n - a_m| + |a_m||b_n - b_m| < B\frac{\epsilon}{2B} + B\frac{\epsilon}{2B} = \epsilon$. Thus $|a_n b_n - a_m b_m| < \epsilon$ whenever $n, m > N$. So $(a_n b_n)$ is Cauchy. □

So, we have an equivalence relation $\overset{\mathbb{R}}{\sim}$ on rational Cauchy sequences, and we can both add and multiply rational Cauchy sequences. The question is: can we extend the addition and multiplication of these sequences to the equivalence classes, i.e., are the following operations well-defined:

(1) $[(a_n)] + [(b_n)] = [(a_n + b_n)]$ and
(2) $[(a_n)][(b_n)] = [(a_n b_n)]$?

The answer is yes, by the following theorem.

Theorem 8.3. *Let (a_n), (b_n), (c_n), and (d_n) be rational Cauchy sequences, with $(a_n) \overset{\mathbb{R}}{\sim} (c_n)$ and $(b_n) \overset{\mathbb{R}}{\sim} (d_n)$. Then*

(1) $(a_n + b_n) \overset{\mathbb{R}}{\sim} (c_n + d_n)$ and
(2) $(a_n b_n) \overset{\mathbb{R}}{\sim} (c_n d_n)$.

Proof. As usual, the proof of the first, additive part is relatively easy, and is left as an exercise (see Problem 5). For the second part,

$$\begin{aligned} |a_n b_n - c_n d_n| &= |a_n b_n - c_n d_n + (a_n d_n - a_n d_n)| \\ &= |a_n b_n - a_n d_n + a_n d_n - c_n d_n| \\ &\leq |a_n b_n - a_n d_n| + |a_n d_n - c_n d_n| \\ &= |a_n||b_n - d_n| + |d_n||a_n - c_n|. \end{aligned}$$

Now we can follow the ideas of the proof of Theorem 8.2. Specifically, since (a_n) and (d_n) are Cauchy, there is some B so that $|a_n|, |d_n| < B$. Since $(a_n) \overset{\mathbb{R}}{\sim} (c_n)$ and $(b_n) \overset{\mathbb{R}}{\sim} (d_n)$, we can make $|b_n - d_n|$ and $|a_n - c_n|$ as small as we like by taking n large enough. So, following the proof of Theorem 8.2, given $\epsilon \in \mathbb{Q}_+$, there exists $N \in \mathbb{Z}_+$ such that $|a_n b_n - c_n d_n| < \epsilon$ whenever $n > N$. (See Problem 6.) □

So now we have a set of equivalence classes of rational Cauchy sequences that has well-defined operations of addition multiplication defined on it, given by

$$[(a_n)] + [(b_n)] = [(a_n + b_n)] \text{ and } [(a_n)][(b_n)] = [(a_n b_n)].$$

This set of classes with these operations is the set of real numbers, $\mathbb{R}$.

Definition 8.3. The set of **real numbers**, $\mathbb{R}$, is the set of equivalence classes of rational Cauchy sequences under the equivalence relation $\overset{\mathbb{R}}{\sim}$ in Definition 8.1.

Since we already know the set $\mathbb{Q}$ is a commutative ring with unity, and we add/multiply elements of these equivalence classes by choosing representative sequences of rationals and add/multiply those term-by-term, it follows that $\mathbb{R}$ is also a commutative ring with unity. (See Problem 8.) The additive identity is $[(0)]$, the multiplicative identity is $[(1)]$, and the additive inverse of $[(a_n)]$ is $[(-a_n)]$.

All of the properties of a commutative ring with unity for $\mathbb{R}$ follow directly from those of $\mathbb{Q}$, as the next example illustrates.

Example 8.1. To see that the left distributive rule holds for $\mathbb{R}$, let $[(a_n)], [(b_n)], [(c_n)] \in \mathbb{R}$. Then

$$\begin{array}{rcll} [(a_n)]([(b_n)] + [(c_n)]) & = & [(a_n)][(b_n + c_n)] & \text{Definition of } + \\ & = & [(a_n(b_n + c_n))] & \text{Definition of } \cdot \\ & = & [(a_nb_n + a_nc_n)] & \text{Left distributive law for } \mathbb{Q} \\ & = & [(a_nb_n)] + [(a_nc_n)] & \text{Definition of } + \\ & = & [(a_n)][(b_n)] + [(a_n)][(c_n)] & \text{Definition of } \cdot. \end{array}$$

Notice the left distributive law for $\mathbb{Q}$ is the essential step. The other ring properties are proved similarly.

We also expect $\mathbb{R}$ to be a field, but multiplicative inverses are a bit trickier, since we can't just take $[(\frac{1}{a_n})]$ to be the multiplicative inverse of an equivalence class $[(a_n)] \neq [(0)]$, since some of the individual terms a_i might be 0. Fortunately, in that case, the individual terms eventually are "bounded away from 0," as the next theorem shows, so we will be able to create an inverse for $[(a_n)]$.

Theorem 8.4. *If (a_n) is a rational Cauchy sequence and $[(a_n)] \neq [(0)]$, then $\exists q \in \mathbb{Q}_+$ and $\exists N \in \mathbb{Z}_+$ such that $|a_n| > q$ whenever $n > N$.*

Proof. Since $(a_n) \overset{\mathbb{R}}{\not\sim} (0)$, it follows that $(a_n) \not\to 0$, so $\exists \epsilon_0 \in \mathbb{Q}_+$ such that $\forall N' \in \mathbb{Z}_+$, $|a_l| \geq \epsilon_0$ for some $l > N'$. Since (a_n) is Cauchy, $\exists N \in \mathbb{Z}_+$ such that $|a_n - a_m| < \frac{\epsilon_0}{2}$ whenever $n, m > N$. So, from the previous line, there exists some $k > N$ such that $|a_k| \geq \epsilon_0$.

Notice $|a_k| = |a_m + (a_k - a_m)| \leq |a_m| + |a_k - a_m|$. So for all $m > N$ (since we know $k > N$),

$$\begin{array}{rcl} |a_m| & \geq & |a_k| - |a_k - a_m| \\ & \geq & \epsilon_0 - |a_k - a_m| \\ & > & \epsilon_0 - \dfrac{\epsilon_0}{2} \\ & = & \dfrac{\epsilon_0}{2}. \end{array}$$

So taking $q = \frac{\epsilon_0}{2}$ satisfies the theorem. □

Theorem 8.4 allows us to construct multiplicative inverses of nonzero reals. For suppose (a_n) is a rational Cauchy sequence such that $[(a_n)] \neq [(0)]$. Then by Theorem 8.4, $\exists q \in \mathbb{Q}_+$, $\exists N \in \mathbb{Z}_+$ such that $|a_n| > q$ for all $n > N$. Thus, we can define the sequence b_n by

$$b_n = \begin{cases} \text{whatever you want} & \text{if } n \leq N \\ \frac{1}{a_n} & \text{if } n > N \end{cases}$$

Then clearly $(a_n b_n) \to 1$, so it appears $[(b_n)]$ is the multiplicative inverse of $[(a_n)]$. All that remains to be shown is that (b_n) Cauchy. (If not, then (b_n) has no equivalence class at all.) To see why this is so, notice that for $n > N$,

$$\begin{aligned} |b_n - b_m| &= \left| \frac{1}{a_n} - \frac{1}{a_m} \right| \\ &= \frac{|a_m - a_n|}{|a_n a_m|}. \end{aligned}$$

Let $\epsilon \in \mathbb{Q}_+$, and let $q \in \mathbb{Q}_+$ and $N_1 \in \mathbb{Z}_+$ be the values guaranteed in Theorem 8.4. Since (a_n) is Cauchy, $\exists N_2 \in \mathbb{Z}_+$ such that $|a_m - a_n| < q^2\epsilon$ whenever $n, m > N_2$. Then, for all $n, m > \max\{N_1, N_2\}$, $|b_n - b_m| = \frac{|a_m - a_n|}{|a_n a_m|} < \frac{q^2\epsilon}{|a_n a_m|} < \frac{q^2\epsilon}{q^2} = \epsilon$. Thus (b_n) is Cauchy, and $[(b_n)]$ is the multiplicative inverse of $[(a_n)]$.

So $\mathbb{R}$ is a commutative ring with unity in which every nonzero element has a multiplicative inverse, so $\mathbb{R}$ is a field.

Problem 9 in Chapter 3 used an injection $\phi : \mathbb{N} \to \mathbb{Z}$ that preserved both addition and multiplication to show we could consider $\mathbb{N} \subseteq \mathbb{Z}$. Problem 11 in Chapter 5 used an injection $\psi : \mathbb{Z} \to \mathbb{Q}$ that preserved both addition and multiplication to show we could consider $\mathbb{Z} \subseteq \mathbb{Q}$. In a similar way, we can consider $\mathbb{Q} \subseteq \mathbb{R}$ by defining $\lambda : \mathbb{Q} \to \mathbb{R}$ by $\lambda(a) = [(a)]$, where the latter is the equivalence class of the constant sequence (a). Then λ is an injection (see Problem 7), and for all $a, b \in \mathbb{Q}$, $\lambda(a + b) = \lambda(a) + \lambda(b)$ and $\lambda(ab) = \lambda(a)\lambda(b)$, so λ preserves both addition and multiplication. Also, $\lambda(0) = [(0)]$ and $\lambda(1) = [(1)]$. Thus the set of equivalence classes of convergent rational sequences – those that are equivalent to constant rational sequences – can be identified with the rational numbers by identifying each convergent rational sequence with its rational limit.

But there are other rational Cauchy sequences that do not converge at all in $\mathbb{Q}$, such as the sequences in Examples 7.1 and 7.2. Such sequences are not equivalent to constant rational sequences. Thus the set of equivalence classes of rational Cauchy sequences can be partitioned into two sets: those that are equivalent to constant rational sequences and those that are not. The latter are known as **irrational numbers**. (Note: The method of Example 7.1 shows how to construct a rational Cauchy sequence that converges to a given irrational number, in the sense you learned about in Calculus.)

Problems. 1. Prove $\overset{\mathbb{R}}{\sim}$ in Theorem 8.1 is reflexive and symmetric.

2. Assume $(a_n) \to a$, and let (a) be the constant sequence in which every element is the number a. Prove $(a_n) \overset{\mathbb{R}}{\sim} (a)$, where $\overset{\mathbb{R}}{\sim}$ is as in Definition 8.1.
3. Let $(a_n) = ((-1)^n)$, $(b_n) = ((-1)^{n+1})$, and $(c_n) = (\frac{1}{n})$. Find all possible sums and products of pairs of these three sequences, as in Definition 8.2.
4. Prove the sum part of Theorem 8.2.
5. Prove the first part of Theorem 8.3. This uses the usual techniques (the triangle inequality and a couple of $\frac{\epsilon}{2}$'s).
6. Finish the proof of the second part of Theorem 8.3.
7. Prove if $a, b \in \mathbb{Q}$ and $\forall \epsilon \in \mathbb{Q}_+$, $|a - b| < \epsilon$, then $a = b$. Then use that fact to prove the function $\lambda : \mathbb{Q} \to \mathbb{R}$ defined by $\lambda(a) = [(a)]$, where (a) is the constant sequence $a, a, a, \dots$, is an injection.
8. Prove both addition and multiplication of equivalence classes of rational Cauchy sequences are commutative.
9. We defined the relation $\overset{\mathbb{R}}{\sim}$ on the set $\mathcal{C}$ of rational Cauchy sequences, but it actually can be applied to the set of **all** rational sequences, Cauchy or not, using the same definition. Provide an example of two (unequal) rational sequences (a_n) and (b_n) that are **not** Cauchy but satisfy $(a_n) \overset{\mathbb{R}}{\sim} (b_n)$.
10. The rational Cauchy sequence $(\frac{1}{n})$ consists entirely of positive terms, but $[(\frac{1}{n})]$ has no multiplicative inverse. Explain why $[(n)]$ doesn't serve as its multiplicative inverse.
11. Let (a_n) be the sequence
$$2, 0, \frac{3}{2}, 0, \frac{4}{3}, 0, \frac{5}{4}, 0, \dots, \frac{n+1}{n}, 0, \dots$$
Then $(a_n) \overset{\mathbb{R}}{\not\sim} (0)$ but (a_n) is **not** "bounded away from 0" in the sense of Theorem 8.4. Why doesn't this example show Theorem 8.4 is false?

Now let's talk about decimals! You probably believe that a real number is rational iff its decimal representation is either terminating or repeating. It's easy to see how every terminating decimal can be written as a fraction of two integers. For example, $4.136 = \frac{4136}{1000}$.

You can also write every repeating decimal as a fraction of two integers. For example, given $4.327\overline{27}$, Let $x = 4.327\overline{27}$. Then $10x = 43.27\overline{27}$ and $1000x = 4327.27\overline{27}$. Subtracting these two equations yields $990x = 4284$, so $x = \frac{4284}{990}$.

12. But **why** is the decimal representation of every rational guaranteed to be repeating[9]? The answer comes from the Division Algorithm.
    (a) Write out $5 \div 7$ using long division until things start repeating.
    (b) What is the length of the repeating period?
    (c) What is the maximum possible length of the repeating period of a fraction of the form $\frac{a}{7}$? Hint: think of the possible remainders when you divide an integer by 7 in each step of the long division. (If you get a 0 remainder, then you get 0s forever.)
13. Another question is **when** is the decimal representation of a rational number terminating instead of repeating? The key is that every repeating decimal can be written as $\frac{a}{10^n}$ for some n, and that $10 = 2 \cdot 5$.
    (a) Write $\frac{71}{2^2 \cdot 5^3}$ as a terminating decimal.
    (b) Explain how you could write $\frac{a}{2^k 5^l}$ as a terminating decimal.
    (c) Finish the sentence: Assume $\frac{a}{b}$ is a fraction of two integers in lowest terms. Then the decimal representation of $\frac{a}{b}$ is terminating iff the prime factorization of b only contains the primes ....

[9] Notice every terminating decimal can be considered a repeating decimal where 0's are repeated, for example, $2.245 = 2.245000\overline{0}$.

9. The Reals II

In this chapter, we extend the notion of order to $\mathbb{R}$, which gives us the notion of convergent, real-valued sequences. We also summarize the various algebraic properties of $\mathbb{R}$, and identify an essential difference between the real and the rationals. We also introduce the topological notion of a neighborhood.

9.1. **Order on $\mathbb{R}$.** Following the procedure used in developing order on the other number systems, we first need to define what it means for $[(a_n)]$ to be positive, then use that to introduce an order on $\mathbb{R}$. Notice it is **not** sufficient to simply say that (a_n) is positive if $a_n > 0$ for all n, since $\frac{1}{n} > 0$ for all n, but $[(\frac{1}{n})] = [(0)]$.

Definition 9.1. The rational Cauchy sequence (a_n) is **positive** if $\exists q \in \mathbb{Q}_+$ and $\exists N \in \mathbb{Z}_+$ such that $a_n > q$ whenever $n > N$.

The idea is that the terms of (a_n) are eventually all greater than some fixed positive rational number q.

We want to apply this notion to equivalence classes of rational Cauchy sequences. The next theorem says we can, i.e., the notion of being positive is well-defined.

Theorem 9.1. *Let (a_n) and (b_n) be rational Cauchy sequences. If (a_n) is positive and $(a_n) \overset{\mathbb{R}}{\sim} (b_n)$, then (b_n) is positive.*

Proof. (Sketch) By hypothesis, if n is large enough, then $a_n > q$ for some $q \in \mathbb{Q}_+$ and b_n can be made arbitrarily close to a_n. So if we make b_n within $\frac{q}{2}$ of a_n, then $b_n > \frac{q}{2}$, and hence (b_n) will be positive. □

So a real number $[(a_n)]$ is positive if any representative of $[(a_n)]$ is a positive sequence in the sense of Definition 9.1.

Sums and products of positive sequences are positive as well:

Theorem 9.2. *Let (a_n) and (b_n) be rational Cauchy sequences. If (a_n) is positive and (b_n) is positive, then so are $(a_n + b_n)$ and $(a_n b_n)$.*

Proof. (Sketch) $a_n + b_n > q_1 + q_2 > 0$ and $a_n b_n > q_1 q_2 > 0$ when n is large enough. □

Definition 9.2. A rational Cauchy sequence (a_n) is a **null sequence** if $(a_n) \overset{\mathbb{R}}{\sim} (0)$.

By Theorem 8.4, if $(a_n) \overset{\mathbb{R}}{\not\sim} (0)$, then $\exists q \in \mathbb{Q}_+$ and $\exists N' \in \mathbb{Z}_+$, such that $|a_n| > q$ whenever $n > N'$. Since (a_n) is Cauchy, its terms eventually become as close as we like, so it follows that $\exists N \in \mathbb{Z}_+$ such that $\forall n > N$, either $a_n > q$ or $-a_n > q$. In other words, either (a_n) is positive or $(-a_n)$ is positive. So, given a rational Cauchy sequence (a_n), we have three possibilities:

(1) (a_n) is positive.
(2) $(-a_n)$ is positive.
(3) (a_n) is a null sequence.

In other words, we have the **trichotomy property for** $\mathbb{R}$.

As usual, we can define $(a_n) < (b_n)$ whenever $(b_n - a_n)$ is positive. By Theorem 9.1, these notions are well-defined under $\overset{\mathbb{R}}{\sim}$, so they apply to equivalence classes of rational Cauchy sequences under $\overset{\mathbb{R}}{\sim}$, so we have an order on $\mathbb{R}$.

With this order on $\mathbb{R}$, we can extend the usual piece-wise definition of the absolute value of a rational number to that of a real number, providing us with the notion of distance between the two reals r and s as $|r-s|$. This in turn enables us to extend the notion of convergent rational sequence to that of a convergent real sequence; the definition is the usual one you saw in Calculus: $(r_n) \to r$ provided $\forall \epsilon \in \mathbb{R}_+$, $\exists N \in \mathbb{Z}_+$ such that $|r_n - r| < \epsilon$ whenever $n > N$. An analog of Theorem 7.1 for $\mathbb{R}$ also holds – the proof is essentially identical – which gives us the triangle inequality for $\mathbb{R}$: $\forall x, y \in \mathbb{R}$, $|x + y| \leq |x| + |y|$.

At this point, we can consider $[(a_n)]$ as the limit of the sequence (a_n), where that limit can be rational or irrational. We have already seen that, for $a \in \mathbb{Q}$, $(a_n) \mapsto a$ iff $[(a_n)] = [(a)]$, and we have our embedding $\lambda : \mathbb{Q} \to \mathbb{R}$ given by $\lambda(a) = [(a)]$ from Chapter 8. Using limits of rational Cauchy sequences that did not converge in $\mathbb{Q}$, we can "plug the holes" in our rational line with these irrational limits to complete the real line.

9.2. **Some axioms of** $\mathbb{R}$**.** Up to this point, starting with the Peano Axioms, we did the following:

(1) Constructed $\mathbb{N}$.
(2) Used $\mathbb{N}$ to construct $\mathbb{Z}$.
(3) Used $\mathbb{Z}$ to construct $\mathbb{Q}$.
(4) Used $\mathbb{Q}$ to construct $\mathbb{R}$.

Each of these number systems has an order $\leq$ on it, and that order is total, i.e., any two elements of any system are comparable to each other.

Now let's shift perspective. Instead of building $\mathbb{R}$ through stages from $\mathbb{N}$, let's look at the axioms $\mathbb{R}$ satisfies. We'll list them from the most general (a group under addition) to the most specific (an ordered field):

- We have a nonempty set $\mathbb{R}$ with the binary operation $+$ that forms a **group**:
  (1) $+$ is associative.
  (2) $+$ has an identity element, 0.
  (3) Every element of $a \in \mathbb{R}$ has an inverse under $+$, $-a$.
- This group $\mathbb{R}$ is **abelian**:
  (4) $+$ is commutative.
- In addition, $\mathbb{R}$ has another binary operation $\cdot$ that makes $\mathbb{R}$ into a **ring**:
  (5) $\cdot$ is associative.
  (6) For all $a, b, c \in \mathbb{R}$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.
- The ring $\mathbb{R}$ is **commutative**:
  (7) $\cdot$ is commutative.
- The ring $\mathbb{R}$ **has unity** (or **has 1**):
  (8) $\cdot$ has an identity element, 1.
- $\mathbb{R}$ is a **field**:
  (9) Every nonzero element $a \in \mathbb{R}$ has an inverse under $\cdot$, $\frac{1}{a}$.
- $\mathbb{R}$ is **totally ordered** under $\leq$:
  (10) For all $a \in \mathbb{R}$, $a \leq a$ (reflexivity).
  (11) For all $a, b, c \in \mathbb{R}$, if $a \leq b$ and $b \leq a$, then $a = b$ (antisymmetry).
  (12) For all $a, b, c \in \mathbb{R}$, if $a \leq b$ and $b \leq c$, then $a \leq c$ (transitivity).
  (13) For all $a, b \in \mathbb{R}$, $a \leq b$ or $b \leq a$ (comparability).
- $\mathbb{R}$ is an **ordered field**:
  (13) For all $a, b, c \in \mathbb{R}$, if $a \leq b$, then $a + c \leq b + c$.
  (14) For all $a, b \in \mathbb{R}$, if $a, b \geq 0$, then $ab \geq 0$.

We will now think of $\mathbb{Q} \subseteq \mathbb{R}$ as the elements of $\mathbb{R}$ that can be expressed as a quotient of two elements of $\mathbb{Z}$.

At each stage of development, from $\mathbb{N}$ to $\mathbb{Z}$ to $\mathbb{Q}$, we gained an additional property from the previous stage. Specifically, all elements of $\mathbb{Z}$ had additive inverses, while that was not true for $\mathbb{N}$, and all nonzero elements of $\mathbb{Q}$ had multiplicative inverses, while that was not true for $\mathbb{Z}$. But since $\mathbb{Q}$ satisfies the full list of axioms above, we have not yet found a property that $\mathbb{R}$ has that $\mathbb{Q}$ doesn't. That property involves bounds.

9.3. Completeness of $\mathbb{R}$.

Definition 9.3. Let S be a nonempty subset of $\mathbb{R}$. A **least upper bound** for S, or **supremum**, is a real number u such that

(1) $\forall s \in S$, $s \leq u$.

(2) If $u' < u$, then $\exists s' \in S$ such that $u' < s'$.

Part (1) says u is an upper bound for S, while part (2) says u is the least such. The supremum of S is denoted $\sup S$. Similarly, the **greatest lower bound**, or **infimum**, of S is denoted $\inf S$.

The supremum of any nonempty set of reals is unique, as is the infimum; see Problem 4. Also, $\sup S$ may or may not be an element of S; see Problem 6.

An essential difference between $\mathbb{Q}$ and $\mathbb{R}$ is that the latter satisfies the following axiom:

Axiom of Completeness. Every nonempty set of real numbers that is bounded above has a least upper bound.

In other words, if $\emptyset \neq S \subseteq \mathbb{R}$ and S has an upper bound, then $\sup S$ exists and is a real number. This is false if $\mathbb{R}$ is replaced by $\mathbb{Q}$, as Problem 6f shows. That is, a nonempty set of rationals that is bounded above need not have a rational least upper bound.

The Axiom of Completeness plays an essential role in Calculus. In particular, it is used to prove the Intermediate Value Theorem and the Extreme Value Theorem. The latter is then used to prove Rolle's Theorem, which is used to prove the Mean Value Theorem. The Mean Value Theorem is then used for a variety of results, such as the relationship between the sign of $f'(x)$ and the increasing/decreasing nature of $f(x)$.

In order to prove the Axiom of Completeness for $\mathbb{R}$, we will construct two rational Cauchy sequences, one increasing toward $\sup S$ and one decreasing toward $\sup S$. We will then show that these sequences are $\overset{\mathbb{R}}{\sim}$ equivalent, and show that their equivalence class is equal to the real number $\sup S$.

Proof. Assume $\emptyset \neq S \subseteq \mathbb{R}$ is bounded above. Let u be a rational upper bound for S and let l be a rational such that $\exists s \in S$ such that $l < s$ (we know such an s exists because $S \neq \emptyset$).

Define the rational sequences (l_n) and (u_n) recursively as follows:

Base. $l_0 = l$ and $u_0 = u$.

Recursive Step. Let $\text{avg}(l_n, u_n) = \frac{l_n + u_n}{2}$.

- If avg(l_n, u_n) is an upper bound for S, define $l_{n+1} = l_n$ and $u_{n+1} =$ avg(l_n, u_n).
- If avg(l_n, u_n) is not an upper bound for S, define $l_{n+1} =$ avg(l_n, u_n) and $u_{n+1} = u_n$.

Notice (l_n) and (u_n) are rational sequences, and (l_n) is increasing while (u_n) is decreasing. Furthermore, each element of (u_n) is an upper bound for S, while no element of (l_n) is an upper bound for S.

By construction, the distance between u_{n+1} and l_{n+1} is half of the distance between u_n and l_n for all n. It follows that $|u_n - l_n| = \frac{1}{2^n}|u_0 - l_0|$ for all n. Since, for all $m > n$, $l_n \leq l_m \leq u_n$ and $l_n \leq u_m \leq u_n$, we also have

$$\begin{aligned} |u_m - u_n| &\leq |u_n - l_n| \text{ and} \\ |l_m - l_n| &\leq |u_n - l_n|. \end{aligned}$$

Since $|u_n - l_n| = \frac{1}{2^n}|u_0 - l_0|$ and $\frac{1}{2^n} \to 0$, it follows that

- Both (l_n) and (u_n) are Cauchy, and
- $(l_n) \overset{\mathbb{R}}{\sim} (u_n)$.

We assert that $[(u_n)] =$ sup S. Since u_n is an upper bound for S for all n, $[(u_n)]$ is an upper bound for S. Suppose there is some real number α such that $\alpha < [(u_n)] = [(l_n)]$ and α is an upper bound for S. Since (l_n) is an increasing sequence, $\exists k \in \mathbb{Z}_+$ such that $\alpha < l_k$. But no element of (l_n) is an upper bound for S, so α isn't either. Thus $[(u_n)] =$ sup S, as asserted.

Therefore the Axiom of Completeness holds for $\mathbb{R}$.

□

9.4. **Topological Notions.** The open intervals utilized in real analysis are a special case of the notion of an open neighborhood in any "topological space" that has a distance function defined on it.

Definition 9.4. Let $x \in \mathbb{R}$ and let $\epsilon > 0$. The **ϵ-neighborhood of x** or **ϵ-ball about x** is the set

$$B_\epsilon(x) = \{y \in \mathbb{R} \mid |x - y| < \epsilon\}.$$

Thus $B_\epsilon(x)$ consists of points within ϵ of x on the real number line, i.e., elements of the open interval $(x - \epsilon, x + \epsilon)$. Notice this definition applies to any set X that contains a notion of distance (known as a **metric**):

$$B_\epsilon(x) = \{y \in X \mid d(x, y) < \epsilon\},$$

where $d(x, y)$ denotes the distance between x and y. Using the usual notion of distance in Euclidean 3-space, an ϵ-ball about x actually *looks* like a ball; it is the interior of a sphere.

We have yet another version of the Archimedean Principle:

Archimedean Principle. For every real number x there is a positive integer n such that $n > x$.

Proof. (By contradiction.) If not, then there is some real number x such that $\forall n \in \mathbb{Z}_+$, $n \leq x$. Thus $\mathbb{Z}_+$ has an upper bound. By the Axiom of Completeness, $\mathbb{Z}_+$ has a least upper bound, say $\alpha \in \mathbb{R}$. Since $\alpha - 1$ is *not* an upper bound for $\mathbb{Z}_+$, $\exists k \in \mathbb{Z}_+$ such that $k > \alpha - 1$. But then $\alpha < k + 1 \in \mathbb{Z}_+$, a contradiction. □

We will use this to prove a fundamental property of the rationals and the reals: between any two real numbers there exists a rational number.

Theorem 9.3. *Let $x \in \mathbb{R}$ and let $\epsilon > 0$. Then $\exists q \in \mathbb{Q}$ such that $q \in B_\epsilon(x)$.*

Proof. Let x and ϵ be given. We need to show there is some rational number in the interval $(x - \epsilon, x + \epsilon)$. By the Archimedean Principle, $\exists n \in \mathbb{Z}_+$ such that $n > \frac{1}{\epsilon}$, that is, $0 < \frac{1}{n} < \epsilon$.

Let $S = \{\frac{i}{n} \mid i \in \mathbb{Z}\}$. Then $S \subseteq \mathbb{Q}$ and the distance between any two successive elements of S, $\frac{i}{n}$ and $\frac{i+1}{n}$, is $\frac{i+1}{n} - \frac{i}{n} = \frac{1}{n} < \epsilon$. But the distance between $x + \epsilon$ and $x - \epsilon$ is 2ϵ, so at least one element of S must lie in $B_\epsilon(x)$. □

An equivalent formulation of Theorem 9.3 (see Problem 7) is that between any two real numbers, there is a rational number. Since this holds for *any* two real numbers, it follows that *between any two irrational numbers, there exists a rational number*. In fact, it is also true that between any two real numbers, there is an irrational number (Problem 8). Since this holds for *any* two real numbers, it follows that *between any two rational numbers, there exists a irrational number*.

So, we have

(1) Between any two irrational numbers, there exists a rational number.
(2) Between any two rational numbers, there exists a irrational number.
(3) The rational numbers are countably infinite[10].
(4) The irrational numbers are uncountable.

This is an example of a situation where finite intuition can be misleading for an infinite problem.

[10] That is, there is a bijection from $\mathbb{N}$ to $\mathbb{Q}$.

Problems. 1. Fill in the details of the proof of Theorem 9.1.

2. Fill in the details of the proof of Theorem 9.2.

3. Let $x, y \in \mathbb{R}$. Prove if $\forall \epsilon > 0$, $x < y + \epsilon$, then $x \leq y$.

4. Let $S \subseteq \mathbb{R}$ be nonempty. Prove sup S is unique if it exists.

5. Prove if $a =$ sup A and $b =$ sup B, then $a + b$ is an upper bound for $C = \{x + y \in \mathbb{R} \mid x \in A \text{ and } y \in B\}$.

6. Find the supremum and infimum of each of the following subsets $S \subseteq \mathbb{R}$ if possible, and state whether they are elements of S.
   (a) $\{1, 2, 3\}$.
   (b) $\{\frac{n}{n+1} \mid n \in \mathbb{Z}_+\}$.
   (c) $\{\frac{2n+1}{n+1} \mid n \in \mathbb{Z}_+\}$.
   (d) $[0, \infty)$.
   (e) $[0, 4)$.
   (f) $\{q \in \mathbb{Q} \mid 0 \leq q \leq \sqrt{2}\}$.

7. Use Theorem 9.3 to prove $\forall x, y \in \mathbb{R}$ with $x < y$, $\exists q \in \mathbb{Q}$ such that $x < q < y$.

8. (a) Prove the product of a rational number and an irrational number is irrational. (Hint: Proof by contradiction.)
   (b) Given $x, y \in \mathbb{R}$ with $x < y$, use Problem 7 to show $\exists q \in \mathbb{Q}$ such that $\frac{x}{\sqrt{2}} < q < \frac{y}{\sqrt{2}}$.
   (c) Conclude $q\sqrt{2}$ is irrational.
   (d) Since $x < q\sqrt{2} < y$, conclude that there is an irrational number between any two real numbers.

9. We know that $|a - b|$ is the distance between the numbers a and b on the number line. So we could define a distance function $d(a, b) = |a - b|$ on $\mathbb{R} = \mathbb{R}^1$.
   (a) Draw the set $\{x \in \mathbb{R} \mid d(x, 0) = 1\}$.
   (b) We can also define the usual distance of points in the plane, $\mathbb{R}^2$, using the distance formula:

$$d((x_1, y_1), (x_2, y_2)) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

   Draw the set $\{(x, y) \in \mathbb{R}^2 \mid d((x, y), (0, 0)) = 1\}$.

10. There are other ways to measure “distance.” Here is another measure of distance in $\mathbb{R}^2$:

$$\rho((x_1, y_1), (x_2, y_2)) = \max\{|x_2 - x_1|, |y_2 - y_1|\}.$$

Draw the set $\{(x, y) \in \mathbb{R}^2 \mid \rho((x, y), (0, 0)) = 1\}$.

A. The Basics of Logic

This chapter reviews the usual basic notions of propositional logic and quantifiers.

Definition A.1. A **proposition** or **statement** is a sentence that is either true or false. Given propositions p and q, compound propositions can be formed using the following logical operations (each given by its defining truth table):

Negation ($\sim$):

p	$\sim p$
T	F
F	T

Disjunction ($\vee$):

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

Conjunction ($\wedge$):

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

Implication ($\Rightarrow$):

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Biconditional ($\Leftrightarrow$):

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Think of propositions p, q, r, etc. as "logical variables" that can take on the "logical values" T and F in logical expressions containing $\sim$, $\vee$, $\Rightarrow$, etc. Compare this with the "real variables" x, y, z, etc. that can take on any "real value" in algebraic expressions containing $+$, $\cdot$, etc.

Definition A.2. 1. Two compound propositions are **logically equivalent** if they have the same truth value regardless of the truth values of their constituent propositions.

2. A compound proposition is a **tautology** if it is always true, regardless of the truth values of its constituent propositions.
3. A compound proposition is a **contradiction** if it is always false, regardless of the truth values of its constituent propositions.

DeMorgan's Laws state that the negation of a conjunction is a disjunction and vice-versa. More precisely, the negation of the proposition "$p \vee q$" is the proposition "$(\sim p) \wedge (\sim q)$" and the negation of the proposition "$p \wedge q$" is the proposition "$(\sim p) \vee (\sim q)$."

Definition A.3. Let $p \Rightarrow q$ be an implication. Its **hypothesis** is p, its **conclusion** is q, its **converse** is $q \Rightarrow p$ and its **contrapositive** is $(\sim q) \Rightarrow (\sim p)$. An implication is logically equivalent to its contrapositive but **not** to its converse. The negation of $p \Rightarrow q$ is $p \wedge (\sim q)$. (See Problem 2.)

Definition A.4. There are two **quantifiers** for logical variables:

1. The **universal** quantifier, $\forall$, which is read "for each," "for all," "for every," etc.
2. The **existential** quantifier, $\exists$, which is read "for some," "for at least one," "there exists," etc.

The negation of a universal quantifier is an existential quantifier, and vice versa. More precisely, the negation of the proposition "$\forall x, P(x)$" is the proposition "$\exists x$ such that $(\sim P(x))$", and the negation of the proposition "$\exists x$ such that $P(x)$" is the proposition "$\forall x, (\sim P(x))$".

Problems. 1. Provide an example that shows an implication is not logically equivalent to its converse.

2. Use truth tables to prove the negation of $p \Rightarrow q$ is $p \wedge (\sim q)$. Notice this shows that THE NEGATION OF AN IMPLICATION IS NOT AN IMPLICATION.
3. Find the hypothesis, conclusion, converse, contrapositive, and negation of the following implication:

   If today is Monday, then this class is algebra or this class is analysis.
4. Use truth tables to prove $p \Rightarrow (q \vee r)$ is logically equivalent to $(p \wedge (\sim q)) \Rightarrow r$. (This is a handy logical equivalence.) Use this to rewrite the following statement:

   If $x \otimes y \in P$, then $x \in P$ or $y \in P$.
5. Use the logical equivalence in Problem 4 and some basic algebra to prove the following:

   Let x be a real number. If $x^2 > 1$, then $x > 1$ or $x < -1$.
6. Negate each of the following:
   (a) All cows have four legs.
   (b) Some sheep have three legs.
   (c) For all x, there exists a y such that $xy > 0$ or $x \geq y$.
   (d) If $x^2 \geq 9$, then $x \geq 3$ or $x \leq -3$.
   (e) If $x^2 \leq 9$, then $-3 \leq x \leq 3$.

(f) $\forall \epsilon, \exists \delta$ such that $|x - c| < \delta \Rightarrow |f(x) - L| < \epsilon$. (Recall this is the definition of the limit of a function from Calculus I.)

(g) If f is continuous on $[a, b]$ and differentiable on (a, b), then there exists $c \in (a, b)$ such that $f'(c) = \dfrac{f(b) - f(a)}{b - a}$. (This is the Mean-Value Theorem from Calculus I.)

(h) All monkeys are curious, but no monkey is as curious as George. (This is from the children's book "Curious George flies a kite," by H.A. Rey and Margaret Rey.)

B. The Basics of Sets

This chapter contains a brief review of operations on sets and the power set of a set. Parallels are drawn between certain operations on sets and certain operations on propositions. Russell's famous paradox is briefly discussed. Most of this should be review, with the exception Russell's paradox and the union/intersection of an indexed family of sets.

We assume the notions of a **set**, an **element** of a set, a **universe of discourse**, and the **empty** set $\emptyset$. A set can be defined by (i) naming all its members, such as $X = \{a, b, c, d\}$, or (ii) by means of a particular property, such as $X = \{x \in U \mid x \text{ possesses property } P\}$, or (iii) via **recursion** (that is, inductively) in some cases. The relationship between subsets of a common universal set can be illustrated with a **Venn diagram.** If X is a finite set, we denote the number of elements of X by $|X|$.

Definition B.1. A set B is a **subset** of a set A, denoted by $B \subseteq A$, if every element of B is an element of A. More specifically, $B \subseteq A$ provided $x \in B \Rightarrow x \in A$. $A = B$ if $A \subseteq B$ and $B \subseteq A$. B is a **proper** subset of A if $B \subseteq A$ but $B \neq A$.

The above definition is more important than it at first seems. Remember it when asked to show that one set is a subset of another, or when asked to show two sets are equal.

Definition B.2. Let U be the universe of discourse, let $A \subseteq U$, and let $B \subseteq U$. Then the notions of **union**, **intersection**, **difference**, **complement** are given by

$$\begin{aligned}
&A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\} \\
&A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\} \\
&A - B = \{x \in A \mid x \notin B\} \qquad\qquad \text{(Note: it is not assumed } B \subseteq A.\text{)} \\
&A' = \{x \in U \mid x \notin A\} = U - A.
\end{aligned}$$

There are more general notions of intersection and union:

Definition B.3. Let U be the universe of discourse, let $\Lambda \neq \emptyset$ and let $\mathcal{A} = \{A_\alpha \mid \alpha \in \Lambda\}$ be an indexed family of sets. Then

$$\bigcup \mathcal{A} = \bigcup_{\alpha \in \Lambda} A_\alpha = \{x \in U \mid \exists \beta \in \Lambda \text{ such that } x \in A_\beta\}$$

$$\bigcap \mathcal{A} = \bigcap_{\alpha \in \Lambda} A_\alpha = \{x \in U \mid \forall \alpha \in \Lambda,\ x \in A_\alpha\}$$

Definition B.4. If X is a set, then the **power set** of X, denoted $\mathcal{P}(X)$ or 2^X, is the set of all subsets of X, i.e., $\mathcal{P}(X) = \{A \mid A \subseteq X\}$.

If X is a finite set, then $|\mathcal{P}(X)| = 2^{|X|}$, which is why $\mathcal{P}(X)$ is sometimes denoted 2^X. This can be proven by induction or by realizing $\mathcal{P}(X)$ as the set of all functions from X to a set with two elements, and counting them. See Problem 8 and Problem 9.

Definition B.5. (1) The **Cartesian product** of the sets X and Y is the set

$$X \times Y = \{(x, y) \mid x \in X \text{ and } y \in Y\}.$$

(2) More generally, the Cartesian product of the sets $S_1, S_2, \ldots, S_n$ is the set

$$\prod_{i=1}^{n} S_i = S_1 \times S_2 \times \cdots \times S_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in S_i\}.$$

It pays to think of $X \times Y$ as a sort of rectangular structure. In particular, when both sets are finite, $|X \times Y| = |X||Y|$.

There is an analogy between the logical operations and the set operations above. In particular,

Logical operation	Set operation
$\sim p$	A'
$p \vee q$	$A \cup B$
$p \wedge q$	$A \cap B$
$p \Rightarrow q$	$A \subseteq B$
$p \Leftrightarrow q$	$A = B$

The above is called "naive set theory" because it is not a rigorous, axiomatic structure. While everything above seems quite reasonable, the system can lead to a contradiction. This was famously attributed to Bertrand Russell (British philosopher, logician, mathematician, historian, socialist, pacifist, and social critic) in 1901, and is known as **Russell's paradox**. Here is a common form of it:

> Let $M = \{x \mid x \notin x\}$. (That is, M is the set of all sets that are not members of themselves[11].) Since M is a set, there are two possibilities: either $M \in M$ or $M \notin M$. But
>
> If $M \notin M$, then **by definition of** M, $M \in M$.

[11] For example, take the set of all squares. That set is not itself a square, and therefore is not a member of the set of all squares. On the other hand, if we take the complementary set that contains all non-squares, that set is itself not a square and so should be one of its own members.

If $M \in M$, then **by definition of** M, $M \notin M$.

Thus $M \in M$ iff $M \notin M$.

Problem 14 contains a more popular version of Russell's paradox.

This uncomfortable paradox was ultimately avoided by using one of two axiomatic systems for set theory: Gödel-Bernays set theory or Zermelo-Fraenkel set theory. (ZFC set theory consists of the latter together with the Axiom of Choice.) A foundations topics course is recommended for a solid treatment of these systems.

Problems. 1. T (true) or F (false)?

T **F** $\{a, b\} \subseteq \{\{a, b\}, a, b\}$.

T **F** $\{a, b\} \in \{\{a, b\}, a, b\}$.

T **F** $\{a\} \in \{\{a, b\}, a, b\}$.

T **F** $\emptyset \in \{\{a, b\}, a, b\}$.

T **F** $\emptyset \subseteq \{\{a, b\}, a, b\}$.

T **F** $\emptyset \in \emptyset$

T **F** $\emptyset \subseteq \emptyset$

T **F** $\emptyset \in \{\emptyset\}$

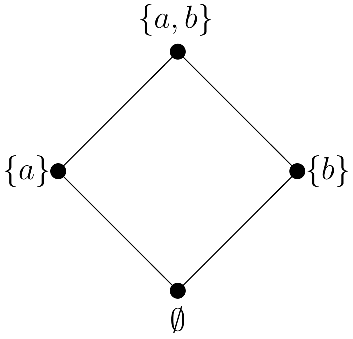
T **F** $\emptyset \subseteq \{\emptyset\}$

T **F** $\emptyset \in \{\emptyset, \{\emptyset\}\}$

T **F** $\{\emptyset\} \in \{\emptyset, \{\emptyset\}\}$

T **F** $\{\{\emptyset\}\} \subseteq \{\emptyset, \{\emptyset\}\}$

2. Suppose A and B are both subsets of a set containing 100 elements. If $|A| = 55$ and $|B| = 40$, what is the largest $|A \cup B|$ could be? The smallest? What is the largest $|A \cap B|$ could be? The smallest? Venn diagrams might help.
3. Suppose you try an experiment where you roll a pair of 6-sided dice. Then the set of equally-likely outcomes is $\{1, 2, 3, 4, 5, 6\} \times \{1, 2, 3, 4, 5, 6\}$. Draw a Cartesian graph of this set of outcomes, and show why a total of seven is the most likely outcome of your experiment.
4. The four subsets of the set $\{a, b\}$ can be arranged in a "lattice diagram" in the shape of a square, as shown below. Each edge represents a subset relation as you go up. (For example, $\{a\} \subseteq \{a, b\}$ below.) In a similar way, draw a lattice diagram in the shape of a cube for the eight subsets of the set $\{a, b, c\}$.



5. Let A, B and C be sets. Use Venn diagrams to illustrate the following:
   (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (c) $A - (B \cup C) = (A - B) \cap (A - C)$
   (d) $A - (B \cap C) = (A - B) \cup (A - C)$
6. For each $n \in \mathbb{Z}_+$, let A_n be the closed interval $[-n, \frac{1}{n}]$. Let $\mathcal{A} = \{A_n \mid n \in \mathbb{Z}_+\}$. Find $\bigcup_{n \in \mathbb{Z}^+} A_n$ and $\bigcap_{n \in \mathbb{Z}^+} A_n$.
7. Find $\mathcal{P}(\emptyset)$, $\mathcal{P}(\mathcal{P}(\emptyset))$, and $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$.
8. Let X be a finite set. For each $A \subseteq X$, define the function $f_A : X \to \{0,1\}$ by

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

For $X = \{a, b, c\}$, fill in the table below with the appropriate outputs.

x	$f_\emptyset(x)$	$f_{\{a\}}(x)$	$f_{\{b\}}(x)$	$f_{\{c\}}(x)$	$f_{\{a,b\}}(x)$	$f_{\{a,c\}}(x)$	$f_{\{b,c\}}(x)$	$f_X(x)$
a								
b								
c								

Are there any other functions $f : \{a, b, c\} \to \{0, 1\}$?

9. Let X be a finite set, let $A \subseteq X$, and let $f_A : X \to \{0,1\}$ be the function defined in Problem 8.
   (a) If $|X| = n$, how many such functions are there? Why?
   (b) Generalize the idea in Problem 8 to argue that the number of subsets of X is 2^n.

10. In Problem 8, write the output columns as vectors in $\mathbb{R}^3$. For example, the columnn under $f_{\{a\}}(x)$ would be written $(1, 0, 0)$. Plot each of these eight points in the $x - y - z$ coordinate system. Observe that the resulting points form the vertex of a cube which can be realized as the same cube in Problem 4.
11. The type of proofs by induction that you were asked to do probably involved some kind of equation like "$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$," as if that equation dropped out of the sky. But in reality, this pattern emerged after looking at some examples, and the equation resulted from a general description of that pattern.

    We have seen that for a finite set X, $|\mathcal{P}(X)| = 2^{|X|}$. In Problem 9, we showed this by counting functions $X \to \{0, 1\}$. This can also be done by induction, and the following illustrates the pattern that is required for the inductive step.

    (a) Write $\mathcal{P}(\{a\})$.
    (b) Write $\mathcal{P}(\{a, b\})$ as the union of $\mathcal{P}(\{a\})$ and another set with the same size.
    (c) Write $\mathcal{P}(\{a, b, c\})$ as the union of $\mathcal{P}(\{a, b\})$ and another set with the same size.
    (d) Write $\mathcal{P}(\{a, b, c, d\})$ as the union of $\mathcal{P}(\{a, b, c\})$ and another set with the same size.

    Notice that each set has twice as many elements as the set above it. **That** is why the number of subsets of a set with n elements is 2^n, and **that** is where that formula comes from ... noticing the pattern from examples.
12. In Calculus, you learned the following: "If $f(x)$ is differentiable, then $f(x)$ is continuous." Illustrate this implication with a Venn diagram, where the universe of discourse is the set of all functions of x. Show how this same diagram illustrates the contrapositive of that statement.
13. If $A = \{a, b, c, \ldots, x, y, z\}$ and $D = \{0, 1, 2, \ldots, 8, 9\}$, what is $|A \times D|$? Prove or disprove: $A \times D = D \times A$.
14. Here is the Barber paradox:

    > Suppose there is a town with just one male barber; and that every man in the town keeps himself clean-shaven: either by shaving themselves or by being shaved by the lone barber. It seems reasonable to imagine that the barber obeys the following rule: He shaves all and only those men in town who do not shave themselves.
    >
    > Under this scenario, we can ask the following question: Does the barber shave himself?

    Explain the paradox.

C. Relations and Functions

In this chapter, we discuss relations, and define equivalence relations, partial orders, and functions. Inverses and inverse images of sets under functions are defined, as well as special types of functions. Topics new to the student might include inverse images of sets under functions, partial orders, and the Axiom of Choice; the last of these is only briefly mentioned, and its understanding is not essential for subsequent chapters.

Definition C.1. Let X and Y be nonempty sets. A **relation** from X to Y is a subset $\mathcal{R} \subseteq X \times Y$. The statement "$(x, y) \in \mathcal{R}$" is sometimes denoted "$x\mathcal{R}y$." A relation from X to X is called a **relation on** X.

Two common ways to represent a relation from one finite set to another are

(1) A Cartesian graph, which simply indicates which elements of $X \times Y$ are in $\mathcal{R}$.
(2) A directed graph, consisting of vertices for each element of $X \cup Y$, and a directed edge from $x \in X$ to $y \in Y$ iff $x\mathcal{R}y$.

If X and Y are finite, then the number of relations from X to Y is the same as the number of subsets of $X \times Y$, which is $2^{|X||Y|}$, which gets big fast. So we'd like to isolate some special types of relations.

Definition C.2. Let $\mathcal{R}$ be a relation on X. Then $\mathcal{R}$ is

(1) **reflexive** provided $\forall a \in X$, $a\mathcal{R}a$.
(2) **symmetric** provided $\forall a, b \in X$, if $a\mathcal{R}b$, then $b\mathcal{R}a$.
(3) **transitive** provided $\forall a, b, c \in X$, if $a\mathcal{R}b$ and $b\mathcal{R}c$, then $a\mathcal{R}c$.
(4) **antisymmetric** provided $\forall a, b \in X$, if $a\mathcal{R}b$ and $b\mathcal{R}a$, then $a = b$.

Definition C.3. A relation $\mathcal{R}$ on X is

(1) an **equivalence relation** if it is reflexive, symmetric, and transitive.
(2) a **partial order** if it is reflexive, antisymmetric, and transitive.

A common symbol for a generic equivalence relation is $\sim$, as in $x \sim y$, rather than $x\mathcal{R}y$. A common symbol for a partial order is $\leq$, as in $x \leq y$, rather than $x\mathcal{R}y$. Notice it does not follow from the definition of partial order that for all $a, b \in X$, either $a \leq b$ or $b \leq a$; that is, there may exist elements that are not **comparable**.

Definition C.4. Let $\sim$ be an equivalence relation on X, and let $a \in X$. The **equivalence class** of a is the set

$$[a] = \{b \in X \mid a \sim b\}.$$

Thus the equivalence class of a consists of all the elements equivalent to a under $\sim$. *Any* element of $[a]$ – not just a – is a **representative** of $[a]$. Think of the set of equivalence classes of X under $\sim$ as the set of piles of equivalent elements.

It is immediate that the set of equivalence classes forms a **partition** of X into disjoint cells (the equivalence classes). Conversely, if you first partition X into disjoint cells and declare that two elements are equivalent iff they are in the same cell, then you get an equivalence relation.

In order to introduce the notion of a function, we return to the more general case of relations from one set to another.

Definition C.5. A relation $\mathcal{R}$ from X to Y is a **function** provided

(1) $\forall x \in X$, $\exists y \in Y$ such that $x\mathcal{R}y$.
(2) If $x\mathcal{R}y_1$ and $x\mathcal{R}y_2$, then $y_1 = y_2$.

The set X is called the **domain** and the set Y called the **range**. The first property simply says every element in X is related to some element of Y, and you probably know the second property as the "vertical line test." As you know, functions are usually denoted by letters such as f, g, ϕ, etc., and we write $f(x) = y$ rather than xfy. We also write $x \mapsto y$.

Definition C.6. Let $f : X \to Y$ be a function.

(1) The **image** of f is

$$\text{Im } f = \{y \in Y \mid \exists x \in X \text{ such that } y = f(x)\}.$$

(2) If $A \subseteq X$, then the **image of** A **under** f is the set

$$f(A) = \{y \in Y \mid \exists a \in A \text{ such that } y = f(a)\}.$$

(3) If $A \subseteq X$, then the **restriction of** f **to** A is the function $f|_A : A \to Y$ given by $a \mapsto f(a)$.
(4) If $B \subseteq Y$, the **inverse image of** B **under** f is

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

This is sometimes called the **pre-image** of B.
(5) If $g : Y \to Z$ is another function, the **composition** $g \circ f : X \to Z$ is given by $x \mapsto g(f(x))$.
(6) f is an **injection** if $\forall a, b \in X$, $[f(a) = f(b) \Rightarrow a = b]$.
(7) f is a **surjection** if $\forall y \in Y$, $\exists x \in X$ such that $y = f(x)$.
(8) f is a **bijection** if it is both an injection and a surjection.

The following cannot be proven or disproven. We will assume it.

Axiom of Choice. Given any collection $\mathcal{A}$ of pairwise disjoint nonempty sets, there exists a set $C \subseteq \bigcup \mathcal{A}$ having exactly one element in common with each set in $\mathcal{A}$. (i.e., $\forall A \in \mathcal{A}$, $C \cap A \neq \emptyset$ and if $x, y \in C \cap A$, then $x = y$.)

There are many versions of the Axiom of Choice. Perhaps the easiest one to understand is the existence of a "choice function" $f : \mathcal{A} \to \bigcup \mathcal{A}$ that "chooses" one element from each set in $\mathcal{A}$. In other words, the Axiom of Choice states that, given a collection of disjoint sets, you can *choose* exactly one element from each set. This is, of course, obvious in the case where this collection is finite.

Definition C.7. For any set X, the **identity function** on X is the function $\mathbb{1}_X : X \to X$ given by $x \mapsto x$. Another notation is id_X.

Lastly, operations like addition and multiplication are actually functions.

Definition C.8. A **binary operation** on a set X is a function $X \times X \to X$.

Problems. 1. Let $X = \{1, 2, 3, \ldots\}$. Define the binary operation $+$ on X as $+ : X \times X \to X$, given by $(a, b) \mapsto a + b$. Find the images of $(2, 1)$, $(5, 7)$, and $(0, 3)$.

2. Define $f(x) = x^2$, as in Calculus. Find $f([1, 3])$ and $f^{-1}([-1, 4])$.
3. Let $X = \{1, 2, 3, 4, 5, 6\}$, and let $\mathcal{R}$ be the relation on X given by $a\mathcal{R}b$ provided a divides b. Give the Cartesian graph and the directed graph associated to $\mathcal{R}$.
4. Let $f : X \to Y$ be a function. Define $\sim$ on X by $a \sim b$ provided $f(a) = f(b)$. Prove $\sim$ is an equivalence relation on X.
5. Let $f(x) = \sin x$, as in Calculus, and let $\sim$ be as in Problem 4. Find $[0]$, the equivalence class of 0 under $\sim$.
6. The reflexive, symmetric, and transitive properties are independent of each other. Let
   $X = \{a, b, c\}$. Draw a directed graph that represents a relation on X that is:
   (a) Reflexive, but neither symmetric nor transitive.
   (b) Symmetric, but neither reflexive nor transitive.
   (c) Transitive, but neither reflexive nor symmetric.
7. Determine the number of equivalence relations on a set with three elements. Hint: Since there is a one-to-one correspondence between the set of equivalence relations and the set of partitions, figure out how many partitions there are.

8. Start with a set with three elements and take its power set. Partially order this power set by inclusion, i.e. $X \leq Y$ if $X \subseteq Y$. Give the directed graph associated to this partial order. Hint: It looks cool if you stick it on a cube.
9. Let X be the set of students in this class born in the United States, and let Y be the set of the 50 U.S. states. Let $f : X \to Y$ be the function that sends student x to the state in which s/he was born.
   (a) Do you think f is an injection? Why?
   (b) Do you think f is a surjection? Why?
   (c) Do you think f is a bijection? Why?
   (d) Describe, in English, $f(\{\text{Jackie, Joe, Morgan}\})$.
   (e) Describe, in English, $f^{-1}(\text{Pennsylvania})$.
10. Let $\mathbb{1}_X$ and $\mathbb{1}_Y$ be the identity functions on X and Y, respectively (as in Definition C.7), and let $f : X \to Y$ be a function. Prove $f \circ \mathbb{1}_X = f$ and $\mathbb{1}_Y \circ f = f$. (This is why these are called identity functions; they act as the identity under composition.)
11. Let $f : X \to Y$ be a function and $A \subseteq X$. Prove $A \subseteq f^{-1}(f(A))$.
12. Let $f : X \to Y$ be a function and $B \subseteq Y$. Prove $f(f^{-1}(B)) \subseteq B$.
13. Prove the composition of two injections is an injection.
14. Prove the composition of two surjections is a surjection.
15. If X is a finite set, then there is obviously no surjection $f : X \to \mathcal{P}(X)$, since $\mathcal{P}(X)$ has more elements than X. If X is infinite, there is also no surjection $f : X \to \mathcal{P}(X)$, but the same argument doesn't hold, since you can't "count" the elements of either set. But here is a clever argument that proves there is no such surjection:

   Proof. (By contradiction.) Suppose $f : X \to \mathcal{P}(X)$ is a surjection. Define

$$A = \{x \in X \mid x \notin f(x)\}.$$

   (For example, if $f : \{a, b\} \to \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ is given by $f(a) = \{b\}$ and $f(b) = \{a, b\}$, then $a \notin f(a)$ and $b \in f(b)$.)

   Since $A \subseteq X$, $A \in \mathcal{P}(X)$. Since f is a surjection, $\exists a \in X$ such that

$$f(a) = A = \{x \in X \mid x \notin f(x)\}.$$

   Show we have a contradiction. Specifically, if $a \in A$ then $a \notin A$, and if $a \notin A$, then $a \in A$.

Department of Mathematics & Statistics, James Madison University, Harrisonburg, VA 22807, USA
Email address: vanwykla@jmu.edu