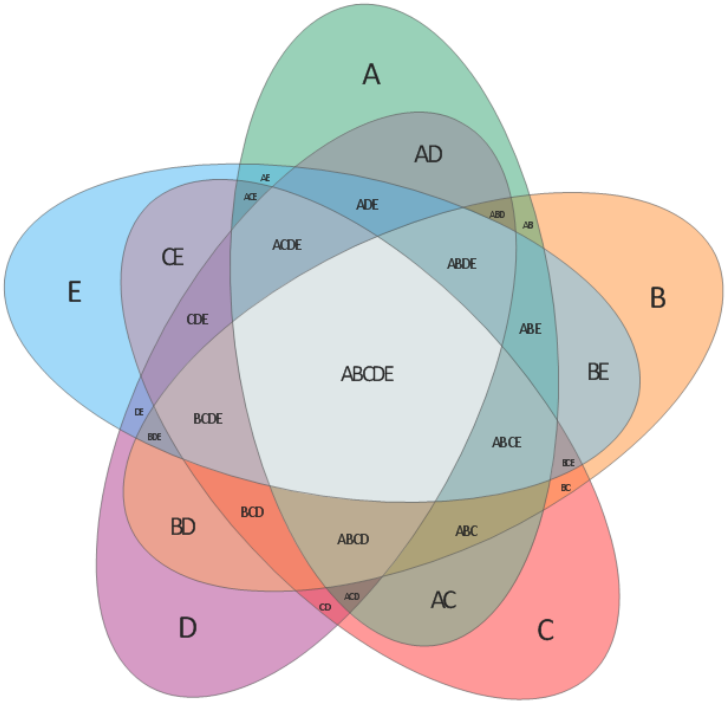
Mathematical Reasoning & Proofs

MAT 1362

Fall 2021



Alistair Savage

Department of Mathematics and Statistics

University of Ottawa

Contents

Preface

These are notes for the course *Mathematical Reasoning & Proofs* at the University of Ottawa. This is an introduction to rigorous mathematical reasoning and the concept of proof in mathematics. It is a course designed to prepare students for upper-level proof-based mathematics courses. We will discuss the axiomatic method and various methods of proof (proof by contradiction, mathematical induction, etc.). We do this in the context of some fundamental notions in mathematics that are crucial for upper-level mathematics courses. These include the basics of naive set theory, functions, and relations. We will also discuss, in a precise manner, the integers, integers modulo n, rational numbers, and real numbers. In addition, we will discuss concepts related to the real line, such as completeness, supremum, and the precise definition of a limit. In general, this course is designed to provide students with a solid theoretical foundation upon which to build in subsequent courses.

This course should be of interest to students who feel dissatisfied with mathematics courses in which computation is emphasized over proof and explanation. In MAT 1362, we will rarely perform computations based on standard techniques and algorithms, such as computing derivatives using the chain and product rules. Instead, we will focus on *why* certain mathematical statements are true and *why* given techniques work. This is often much more difficult than following an algorithm to perform a computation. However, it is much more rewarding and results in a deeper understanding of the material.

Acknowledgement: Significant portions of these notes closely follow the book The Art of Proof by Matthias Beck and Ross Geoghegan [BG10], which is the official course text.

Alistair Savage

Course website: `https://alistairsavage.ca/mat1362`

Chapter 1

Integers

In this chapter we discuss the integers. While you have encountered the integers in many previous courses, dating back to grade school, you probably took certain properties for granted. In this course, we will begin with some precise axioms and deduce other properties of the integers in a more rigorous way.

1.1 Axioms

We will discuss the concept of a set later, in Chapter 5. For now, we will use the word intuitively. A set S is a collections of things, called the *elements* or *members* of S. We write $a \in S$ to indicate that a is an element of S. A *binary operation* on a set S is a function that takes two elements of S as input and produces another element of S as output.

We will assume there is a set $\mathbb{Z}$, whose members we will call *integers*. This set comes with two binary operations:

- *addition*, denoted $+$, and
- *multiplication*, denoted $\cdot$.

We will often denote multiplication by *juxtaposition*. That is, we will write ab instead of $a \cdot b$.

We assume that $\mathbb{Z}$, together with these operations, satisfies the following five axioms, as well as Axioms 2.1 and 2.17 to be introduced in Chapter 2.

Axiom 1.1 (Commutativity, associativity, and distributivity)**.** For all integers a, b, and c, we have

(i) $a + b = b + a$, (*commutativity of addition*)

(ii) $(a + b) + c = a + (b + c)$, (*associativity of addition*)

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$, (*distributivity*)

(iv) $a \cdot b = b \cdot a$, (*commutativity of multiplication*)

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. (*associativity of multiplication*)

Axiom 1.2 (Additive identity)**.** There exists an integer 0 such that $a + 0 = a$ for all $a \in \mathbb{Z}$. This element 0 is called an *additive identity*, or an *identity element for addition*.

Axiom 1.3 (Multiplicative identity)**.** There exists an integer 1 such that $1 \neq 0$ and $a \cdot 1 = a$ for all $a \in \mathbb{Z}$. The element 1 is called a *multiplicative identity*, or an *identity element for multiplication*.

Axiom 1.4 (Additive inverse)**.** For each $a \in \mathbb{Z}$, there exists an integer, denoted $-a$, such that $a + (-a) = 0$. The element $-a$ is called the *additive inverse* of a.

Axiom 1.5 (Cancellation)**.** If $a, b, c \in \mathbb{Z}$, $a \cdot b = a \cdot c$, and $a \neq 0$, then $b = c$. This is called the *cancellation property*.

The symbol "=" means *equals*. When we write $a = b$ for elements a and b of some set S (e.g. $\mathbb{Z}$), we mean that a and b are *the same element*. This symbol has the following properties:

(i) $a = a$. (*reflexivity of equality*)

(ii) If $a = b$, then $b = a$. (*symmetry of equality*)

(iii) If $a = b$ and $b = c$, then $a = c$. (*transitivity of equality*)

(iv) If $a = b$, then a can be replaced by b in any statement or expression, without changing the meaning of that statement or expression. (In fact, the statement/expression is unchanged.) We call this the *replacement* property. For example, if $a, b, c \in \mathbb{Z}$ and $a = b$, then $a + c = b + c$.

The symbol $\neq$ means *is not equal to*. When we write $a \neq b$ for $a, b \in \mathbb{Z}$, we mean that a and b are not the same element of $\mathbb{Z}$. Note the following:

(i) The symbol $\neq$ is not reflexive. We never have $a \neq a$.

(ii) The symbol $\neq$ is symmetric. If $a, b \in \mathbb{Z}$ and $a \neq b$, then $b \neq a$.

(iii) The symbol $\neq$ is not transitive. For example, $1 \neq 2$ and $2 \neq 1$, but it is not true that $1 \neq 1$ (which is what transitivity would imply).

The symbol $\notin$ means *is not an element of*.

1.2 First consequences of the axioms

For now, we *only* assume Axioms 1.1–1.5. That is, we will not use any other properties of the integers that you may have learned in previous courses in mathematics. We will deduce other properties of the integers *from* these axioms. Once we have proved that some other statement is true, we may then use it in following statements. In general, we would like to assume as few axioms as possible, and show that other properties are *implied by* this small list of axioms. Note, for example, that we have *not* yet introduced the operation of subtraction. (We will see this in Section 1.3.)

Proposition 1.6. *If $a, b, c \in \mathbb{Z}$, then $(a+b)c = ac + bc$.*

Proof. Suppose $a, b, c \in \mathbb{Z}$. Then we have

$$\begin{aligned} (a+b)c &= c(a+b) && \text{Axiom 1.1(iv) (commutativity of multiplication)} \\ &= ca + cb && \text{Axiom 1.1(iii) (distributivity)} \\ &= ac + bc. && \text{Axiom 1.1(iv) (commutativity of multiplication)} \end{aligned}$$

□

Proposition 1.7. *If $a \in \mathbb{Z}$, then $0 + a = a$ and $1 \cdot a = a$.*

Proof. This proof of this proposition is left as an exercise (Exercise 1.2.1). □

Proposition 1.8. *If $a \in \mathbb{Z}$, then $(-a) + a = 0$.*

Proof. The proof of this proposition is left as an exercise (Exercise 1.2.2). □

Proposition 1.9. *If $a, b, c \in \mathbb{Z}$ and $a + b = a + c$, then $b = c$.*

Proof. Suppose $a, b, c \in \mathbb{Z}$. Then we have

$$\begin{aligned} & a + b = a + c \\ \implies & (-a) + (a+b) = (-a) + (a+c) && \text{replacement property} \\ \implies & ((-a) + a) + b = ((-a) + a) + c && \text{Axiom 1.1(ii) (associativity of addition)} \\ \implies & 0 + b = 0 + c && \text{Proposition 1.8} \\ \implies & b = c. && \text{Proposition 1.7} \end{aligned}$$

□

Above, we have used the symbol $\implies$. If P and Q are two statements, then $P \implies Q$ means that the statement P *implies* the statement Q or, equivalently, that Q follows logically from P. It can also be read "if P, then Q".

Proposition 1.10 (Uniqueness of the additive inverse)**.** *If $a, b \in \mathbb{Z}$ and $a + b = 0$, then $b = -a$. In other words, the element $-a$ mentioned in Axiom 1.4 is the* unique *additive inverse of a (i.e. every integer has* exactly one *additive inverse).*

Proof. Suppose $a, b \in \mathbb{Z}$. Then we have

$$\begin{aligned} & a + b = 0 \\ \implies & (-a) + (a+b) = (-a) + 0 && \text{replacement property} \\ \implies & (-a) + (a+b) = -a && \text{Axiom 1.2 (add. ident.)} \\ \implies & ((-a) + a) + b = -a && \text{Axiom 1.1(ii) (assoc. of add.)} \\ \implies & 0 + b = -a && \text{Proposition 1.8} \\ \implies & b = -a. && \text{Proposition 1.7} \end{aligned}$$

□

Proposition 1.10 is a good example of how we have tried to make the axioms as weak as possible. We could have worded Axiom 1.4 to say that every integer has a *unique* additive inverse. However, Proposition 1.10 shows that it is enough to state the weaker axiom that every integer has *at least one* additive inverse. The uniqueness of the additive inverse follows from the axioms.

Proposition 1.11. *Suppose $a, b, c, d \in \mathbb{Z}$. Then*

(i) $(a+b)(c+d) = (ac+bc)+(ad+bd)$,

(ii) $a+(b+(c+d)) = (a+b)+(c+d) = ((a+b)+c)+d$,

(iii) $a+(b+c) = (c+a)+b$,

(iv) $a(bc) = c(ab)$,

(v) $a(b+(c+d)) = (ab+ac)+ad$,

(vi) $(a(b+c))d = (ab)d+a(cd)$.

Proof. We will prove part (v) and leave the remaining parts as an exercise (Exercise 1.2.3). Suppose $a, b, c, d \in \mathbb{Z}$. Then we have

$$\begin{aligned} a(b+(c+d)) &= ab + a(c+d) && \text{Axiom 1.1(iii) (distributivity)} \\ &= ab + (ac+ad) && \text{Axiom 1.1(iii) (distributivity)} \\ &= (ab+ac)+ad. && \text{Axiom 1.1(ii) (assoc. of addition)} \end{aligned}$$

□

Proposition 1.12 (Uniqueness of the additive identity)**.** *Suppose $a \in \mathbb{Z}$. If a has the property that $b+a = b$ for all $b \in \mathbb{Z}$, then $a = 0$. In other words, the additive identity is unique.*

Proof. Suppose $a \in \mathbb{Z}$ has the property that $b+a = b$ for all $b \in \mathbb{Z}$. In particular, choosing $b = 0$, we have

$$\begin{aligned} & 0+a = 0 \\ \implies\ & a = 0. && \text{Proposition 1.7} \end{aligned}$$

□

Proposition 1.13. *Suppose $a \in \mathbb{Z}$. If a has the property that $b+a = b$ for* some *$b \in \mathbb{Z}$, then $a = 0$.*

Proof. Suppose $a \in \mathbb{Z}$ has the property that $b+a = b$ for some $b \in \mathbb{Z}$. By Axiom 1.4, b has an additive inverse $-b \in \mathbb{Z}$. Then

$$\begin{aligned} & b+a = b \\ \implies\ & (-b)+(b+a) = (-b)+b && \text{replacement property} \end{aligned}$$

$$\begin{aligned}
&\implies ((-b)+b)+a=(-b)+b && \text{Axiom 1.1(ii) (associativity of addition)}\\
&\implies 0+a=0 && \text{Proposition 1.8}\\
&\implies a=0. && \text{Proposition 1.7}
\end{aligned}$$

□

Note the difference between Propositions 1.12 and 1.13. In Proposition 1.12, the equation $b+a=b$ is assumed to hold for *all* $b\in\mathbb{Z}$, whereas in Proposition 1.13, it is assumed to hold only for *some* $b\in\mathbb{Z}$.

Proposition 1.14. *If $a\in\mathbb{Z}$, then $a\cdot 0=0=0\cdot a$.*

Proof. We have

$$\begin{aligned}
&0=0+0 && \text{Axiom 1.2 (additive identity)}\\
&\implies a\cdot 0=a\cdot(0+0) && \text{replacement}\\
&\implies a\cdot 0=a\cdot 0+a\cdot 0 && \text{Axiom 1.1(iii) (distributivity)}\\
&\implies a\cdot 0+\big(-(a\cdot 0)\big)=(a\cdot 0+a\cdot 0)+\big(-(a\cdot 0)\big) && \text{replacement}\\
&\implies a\cdot 0+\big(-(a\cdot 0)\big)=a\cdot 0+\Big(a\cdot 0+\big(-(a\cdot 0)\big)\Big) && \text{Axiom 1.1(ii) (assoc. of addition)}\\
&\implies 0=a\cdot 0+0 && \text{Axiom 1.4 (additive inverse)}\\
&\implies 0=a\cdot 0 && \text{Axiom 1.2 (additive identity).}
\end{aligned}$$

The equality $0=0\cdot a$ then follows from Axiom 1.1(iv) (commutativity of multiplication). □

If $a,b\in\mathbb{Z}$, we say that a *is divisible by* b (or that b *divides* a) if there exists $c\in\mathbb{Z}$ such that $a=bc$. We will write $b|a$ to indicate that a is divisible by b and $b\nmid a$ to indicate that a is not divisible by b.

How can we define even integers? Well, as you learn in grade school, even integers are integers that are divisible by 2. But what is 2? Neither our axioms nor anything we have proved up to this point discusses the integer 2. However, we can *define* 2 to be the integer $1+1$.

Proposition 1.15. *If a and b are even integers, then $a+b$ and ab are also even.*

Proof. Suppose a and b are even integers. Then, by definition, there exist $j,k\in\mathbb{Z}$ such that $a=2j$ and $b=2k$. Thus

$$\begin{aligned}
a+b&=2j+2k && \text{replacement property}\\
&=2(j+k) && \text{Axiom 1.1(iii) (distributivity)}
\end{aligned}$$

Since $j+k\in\mathbb{Z}$, this implies that $a+b$ is divisible by 2, hence is even.

We leave the proof that ab is even as an exercise (Exercise 1.2.4). □

Proposition 1.16. *(i) 0 is divisible by every integer.*

(ii) If $a\in\mathbb{Z}$ and $a\neq 0$, then $0\nmid a$.

Proof. (i) Suppose $m \in \mathbb{Z}$. Then $0 = m \cdot 0$ by Proposition 1.14. Thus, by the definition of divisibility, 0 is divisible by m.

(ii) Suppose $a \in \mathbb{Z}$ is divisible by 0. Then, by the definition of divisibility, there exists $k \in \mathbb{Z}$ such that $a = k \cdot 0$. But $k \cdot 0 = 0$ by Proposition 1.14. So $a = 0$. So we have proved that the only number divisible by zero is zero. It follows that, if $a \neq 0$, then $0 \nmid a$.

□

Proposition 1.17 (Uniqueness of the multiplicative identity)**.** *If $a \in \mathbb{Z}$ has the property that $ba = b$ for all $b \in \mathbb{Z}$, then $a = 1$.*

Proof. The proof of this proposition is left as an exercise (Exercise 1.2.5). □

Proposition 1.18. *If $a \in \mathbb{Z}$ has the property that, for some nonzero $b \in \mathbb{Z}$, $ba = b$, then $a = 1$.*

Proof. Suppose $a \in \mathbb{Z}$ has the given property. So there exists some nonzero $b \in \mathbb{Z}$ such that $ba = b$. Then

$$\begin{aligned} & ba = b && \\ \implies\ & b \cdot a = b \cdot 1 && \text{Axiom 1.3 (multiplicative identity)} \\ \implies\ & a = 1. && \text{Axiom 1.5 (cancellation)} \end{aligned}$$

□

Proposition 1.19. *For all $a, b \in \mathbb{Z}$, we have $(-a)b = -(ab)$.*

Proof. Suppose $a, b \in \mathbb{Z}$. Then

$$\begin{aligned} & a + (-a) = 0 && \text{Axiom 1.4 (additive inverse)} \\ \implies\ & (a + (-a))b = 0 \cdot b && \text{replacement property} \\ \implies\ & (a + (-a))b = 0 && \text{Prop. 1.14} \\ \implies\ & ab + (-a)b = 0 && \text{Prop. 1.6} \\ \implies\ & (-a)b = -(ab). && \text{Prop. 1.10} \end{aligned}$$

□

Proposition 1.20. *(i) For all $a \in \mathbb{Z}$, we have $-(-a) = a$.*

(ii) $-0 = 0$.

Proof. (i) Suppose $a \in \mathbb{Z}$. We have

$$\begin{aligned} & (-a) + \big(-(-a)\big) = 0 = (-a) + a && \text{Axiom 1.4 (additive inverse) and Prop. 1.8} \\ \implies\ & (-a) + \big(-(-a)\big) = (-a) + a && \text{transitivity of equality} \\ \implies\ & -(-a) = a. && \text{Prop. 1.9} \end{aligned}$$

(ii) We have

$$\begin{aligned} & 0+0=0 && \text{Axiom 1.2 (additive identity)} \\ \implies\ & -0=0. && \text{Proposition 1.10} \end{aligned}$$

□

Proposition 1.21. *For all $a, b \in \mathbb{Z}$, we have $(-a)(-b) = ab$. In particular, $(-1)(-1) = 1$.*

Proof. Suppose $a, b \in \mathbb{Z}$. Then

$$\begin{aligned} (-a)(-b) &= -\big(a(-b)\big) && \text{Prop 1.19} \\ &= -((-b)a) && \text{Axiom 1.1(iv) (commutativity of multiplication)} \\ &= -(-(ba)) && \text{Prop. 1.19} \\ &= -(-(ab)) && \text{Axiom 1.1(iv) (commutativity of multiplication)} \\ &= ab. && \text{Prop. 1.20(i)} \end{aligned}$$

□

Proposition 1.22. *Suppose $a, b \in \mathbb{Z}$. Then there exists a unique $c \in \mathbb{Z}$ such that $a + c = b$.*

Note that Proposition 1.22 asserts that there is *one and only one* c with the given property. Thus, this statement is asserting two things: that such an element c *exists* (the existence part of the statement) and that any two elements with the given property must be equal (the uniqueness part of the statement). Later, once we have discussed subtraction, the element c in Proposition 1.22 will be denoted $b - a$.

Proof of Proposition 1.22. To prove the existence part of the statement, we just need to find one element with the given property. In fact, $(-a) + b$ is such an element, since

$$\begin{aligned} a + \big((-a) + b\big) &= \big(a + (-a)\big) + b && \text{Axiom 1.1(ii) (associativity of addition)} \\ &= 0 + b && \text{Axiom 1.4 (additive inverse)} \\ &= b. && \text{Proposition 1.7} \end{aligned}$$

It remains to prove uniqueness. Suppose c_1 and c_2 are two elements with the given property. Then we have

$$\begin{aligned} & a + c_1 = b = a + c_2 && \\ \implies\ & a + c_1 = a + c_2 && \text{transitivity of equality} \\ \implies\ & c_1 = c_2. && \text{Proposition 1.9} \end{aligned}$$

□

Proposition 1.23. *If $a \in \mathbb{Z}$ satisfies $a \cdot a = a$, then $a = 0$ or $a = 1$.*

Proof. The proof of this proposition is left as an exercise (Exercise 1.2.6). □

Warning! You *cannot* start a proof with the statement you are trying to prove. Doing so results in circular reasoning, which is not valid. For example, in Proposition 1.23, you cannot start with the statement $a = 0$ or $a = 1$. Instead, you must deduce the statement you are trying to prove from statements you know to be true, or the hypotheses of the proposition. To illustrate how starting with the statement you are trying to prove can result in nonsense, consider the following invalid "argument":

$$\begin{aligned} & 1 = -1 \\ \implies & 1 \cdot 1 = (-1)(-1) \\ \implies & 1 = 1. \end{aligned}$$

We ended up with a true statement, but that does *not* mean that our original statement is true. Make sure you avoid this common pitfall.

Proposition 1.24. *If $a, b \in \mathbb{Z}$, then*

(i) $-(a + b) = (-a) + (-b)$,

(ii) $-a = (-1)a$, *and*

(iii) $(-a)b = a(-b) = -(ab)$.

Proof. The proof of this proposition is left as an exercise (Exercise 1.2.7). Note that some of part (iii) was proved in Proposition 1.19. □

Remark 1.25. In mathematics, the word "or", without further qualification, is always inclusive. For example, to say that "P or Q is true" means that P is true or Q is true or both P and Q are true.

Proposition 1.26. *If $a, b \in \mathbb{Z}$ satisfy $ab = 0$, then $a = 0$ or $b = 0$.*

Proof. Suppose $a, b \in \mathbb{Z}$ satisfy $ab = 0$. Then

$$a \cdot b = 0 = a \cdot 0.$$

We split the proof into two cases: $a = 0$ and $a \neq 0$.

Case 1: If $a = 0$, then the statement "$a = 0$ or $b = 0$" is true, and we are done.

Case 2: If $a \neq 0$, then, by Axiom 1.5, we can conclude that $b = 0$. Thus, the statement "$a = 0$ or $b = 0$" is again true. □

Base ten numbers. So far the only specific integers with names are 0, 1, and -1. It is useful to have names for some more integers. We define the *digits*

$$\begin{aligned} 2 &:= 1 + 1, \\ 3 &:= 2 + 1, \\ &\vdots \\ 9 &:= 8 + 1. \end{aligned}$$

We can then define numbers write in base ten notation, e.g. 11 and 56, as you learn in elementary school. This is discussed in detail in [BG10, Ch. 7], but we will omit such a discussion in this course.

Powers. Fix an integer b. We define the powers b^n for integers $n \geq 0$ as follows:

(i) We define $b^0 := 1$.

(ii) For $n > 0$, we define $b^n = \underbrace{bb \cdots b}_{n \text{ terms}}$.

Note that it follows from the above that $0^0 = 1$. We also have, for all $a \in \mathbb{Z}$ and integers $m, k \geq 0$,

- $a^m a^k = a^{m+k}$.
- $(a^m)^k = a^{mk}$.

Exercises.

1.2.1. Prove Proposition 1.7.

1.2.2. Prove Proposition 1.8.

1.2.3. Prove the remaining parts of Proposition 1.11.

1.2.4. Complete the proof of Proposition 1.15.

1.2.5. Prove Proposition 1.17.

1.2.6. Prove Proposition 1.23. *Hint*: Split the proof into two cases: $a = 0$ and $a \neq 0$.

1.2.7. Prove Proposition 1.24.

1.3 Subtraction

Although you are all familiar with subtraction of integers, we have not encountered this concept yet, since it is not mentioned in our axioms or in the results we have proven so far. We can now define the concept of subtraction precisely.

Definition 1.27 (Subtraction)**.** For $a, b \in \mathbb{Z}$, we define $a - b$ to be $a + (-b)$. This new binary operation $-$ will be called *subtraction*.

Proposition 1.28. *For all $a, b, c, d \in \mathbb{Z}$, we have*

(i) $(a - b) + (c - d) = (a + c) - (b + d)$,

(ii) $(a - b) - (c - d) = (a + d) - (b + c)$,

(iii) $(a - b)(c - d) = (ac + bd) - (ad + bc)$,

(iv) $a - b = c - d$ *if and only if* $a + d = b + c$,

(v) $(a - b)c = ac - bc$.

Proof. The proof of part (i) can be found in [BG10, Prop. 1.27]. We will prove part (iii) and leave the proofs of the other statements as an exercise (Exercise 1.3.1). We have

$$\begin{aligned}
(a-b)(c-d) &= \big(a+(-b)\big)\big(c+(-d)\big) && \text{def. of subtraction}\\
&= \big(ac+(-b)c\big)+\big(a(-d)+(-b)(-d)\big) && \text{Prop. 1.11(i)}\\
&= \big(ac+\big((-b)c+a(-d)\big)\big)+(-b)(-d) && \text{Prop. 1.11(ii)}\\
&= \big(ac+\big((-b)c+a(-d)\big)\big)+bd && \text{Prop. 1.21}\\
&= bd+\big(ac+\big((-b)c+a(-d)\big)\big) && \text{Axiom 1.1(i) (comm. of add.)}\\
&= (bd+ac)+\big((-b)c+a(-d)\big) && \text{Prop. 1.11(ii)}\\
&= (ac+bd)+\big((-b)c+a(-d)\big) && \text{Axiom 1.1(i) (comm. of add.)}\\
&= (ac+bd)+\big(-(bc)+(-(ad))\big) && \text{Prop. 1.19}\\
&= (ac+bd)+\big(-(bc+ad)\big) && \text{by Prop. 1.24(i)}\\
&= (ac+bd)-(bc+ad) && \text{def. of subtraction}\\
&= (ac+bd)-(ad+bc). && \text{Axiom 1.1(i) (comm. of add.)}
\end{aligned}$$

□

As you can see, writing out some proofs in detail, citing all the appropriate axioms and results, can become rather lengthy. As we begin to become familiar with the properties, we will often omit straightforward steps, so that we can focus on the important new ideas in a proof, instead of the small technical points that are similar to arguments we have done before. But it is important to realize that one *could* fill in all the details, justifying every step.

Remark 1.29. We have seen in this chapter that the arithmetic of integers, as defined by our axioms, behave as we learned in grade school. From now on, we will start to use the properties demonstrated in this chapter freely, often omitting some of the justifications. In particular, as in Proposition 1.11(ii), we see that we can move the parentheses in the addition of multiple integers however we like, leaving the result unchanged. Therefore, if $a, b, c, d \in \mathbb{Z}$, we can unambiguously write expressions like

$$a + b + c + d,$$

since the result of the additions is the same no matter how we group the terms.

Exercises.

1.3.1. Prove the remaining parts of Proposition 1.28.

Chapter 2

Natural numbers and induction

In this section we introduce the natural numbers and an ordering on the integers. We then see the important principles of mathematical induction and well-ordering.

2.1 Natural numbers

In Chapter 1, we introduced the integers. However, you may notice that none of our axioms or results so far have referred to *positive* or *negative* numbers, nor to the relations "greater than" or "less than". We introduce another axiom to deal with these notions.

Axiom 2.1 (Natural numbers)**.** There exists a subset $\mathbb{N}$ of $\mathbb{Z}$ with the following properties:

(i) If $a, b \in \mathbb{N}$, then $a + b \in \mathbb{N}$. (The subset $\mathbb{N}$ is closed under addition.)

(ii) If $a, b \in \mathbb{N}$, then $ab \in \mathbb{N}$. (The subset $\mathbb{N}$ is closed under multiplication.)

(iii) $0 \notin \mathbb{N}$.

(iv) For every $a \in \mathbb{Z}$, we have $a \in \mathbb{N}$ or $a = 0$ or $-a \in \mathbb{N}$.

We call the members of $\mathbb{N}$ *natural numbers* or *positive integers*. A *negative integer* is an integer that is not positive and not zero.

Remark 2.2. It is important to note that some references use the symbol $\mathbb{N}$ to denote a slightly different subset of $\mathbb{Z}$ than the one introduced above. Namely, they include 0 in the set of natural numbers. Keep this in mind when reading other sources, to avoid confusion.

The proof of our next proposition will involve *proof by contradiction*. This technique works as follows. Suppose we want to show that some statement P is true. Instead of showing this directly, we can show that the assumption that P is false leads to a logical contradiction (such as $1 = 0$). We implicitly use the *Law of the Excluded Middle*, which says that P must be either true or false. Thus, if its being false leads to a contradiction, it must be true.

Proposition 2.3. *For $a \in \mathbb{Z}$, one and only one of the following statements is true:*

- $a \in \mathbb{N}$,
- $-a \in \mathbb{N}$,
- $a = 0$.

Proof. Suppose $a \in \mathbb{Z}$. By Axiom 2.1(iv), at least one of the statements in the proposition is true. So it remains to prove that *at most* one is true.

First suppose $a = 0$. Then, by Proposition 1.20(ii), we have $-a = -0 = 0$. Therefore, by Axiom 2.1(iii), $a \notin \mathbb{N}$ and $-a \notin \mathbb{N}$.

It remains to prove that, if $a \neq 0$, then a and $-a$ cannot both be in $\mathbb{N}$. We prove this by contradiction. Therefore, we assume that the statement

$$a \text{ and } -a \text{ are not both in } \mathbb{N} \tag{2.1}$$

is false. This is equivalent to assuming that the statement

$$a \in \mathbb{N} \text{ and } -a \in \mathbb{N} \tag{2.2}$$

is true. Assuming this, Axiom 2.1(i), tells us that

$$a + (-a) \in \mathbb{N}.$$

However, by Axiom 1.4, we have $a + (-a) = 0$. Therefore, $0 \in \mathbb{N}$. But this contradicts Axiom 2.1(iii). Therefore, our assumption (2.2) must be false. Consequently, the statement (2.1) must be true, as desired. □

Proposition 2.4. *We have* $1 \in \mathbb{N}$.

Proof. Since $1 \neq 0$ (by the multiplicative identity axiom, Axiom 1.3), one and only one of $1 \in \mathbb{N}$ and $-1 \in \mathbb{N}$ is true by Proposition 2.3. If $-1 \in \mathbb{N}$, then by the closure of $\mathbb{N}$ under multiplication (Axiom 2.1(ii)), we have $1 = (-1)(-1) \in \mathbb{N}$, which would contradict Proposition 2.3. Thus $1 \in \mathbb{N}$. □

2.2 Ordering the integers

Now that we have introduced the natural numbers $\mathbb{N}$, we are able to introduce an order on the integers.

Definition 2.5 (Order on the integers)**.** For $a, b \in \mathbb{Z}$, we write $a < b$ (and say a is *less than* b) or $b > a$ (and say b is *greater than* a) if and only if

$$b - a \in \mathbb{N}.$$

We write $a \leq b$ (and say a is *less than or equal to* b) or $b \geq a$ (and say b is *greater than or equal to* a) if and only if

$$a < b \quad \text{or} \quad a = b.$$

Proposition 2.6 (Transitivity of $<$)**.** *Suppose $a, b, c \in \mathbb{Z}$. If $a < b$ and $b < c$, then $a < c$. In other words, the relation $<$ is transitive.*

Proof. Assume $a, b, c \in \mathbb{Z}$ such that $a < b$ and $b < c$. Thus, by definition, we have $b - a \in \mathbb{N}$ and $c - b \in \mathbb{N}$. Then, by Axiom 2.1(i)

$$c - a = (c - b) + (b - a) \in \mathbb{N}.$$

Thus, $a < c$. □

Proposition 2.7 ($\mathbb{N}$ has no largest element)**.** *For each $a \in \mathbb{N}$, there exists $b \in \mathbb{N}$ such that $b > a$.*

Proof. The proof of this proposition is left as an exercise (Exercise 2.2.1). □

Proposition 2.8. *If $a, b \in \mathbb{Z}$ satisfy $a \leq b \leq a$, then $a = b$.*

Proof. Suppose $a, b \in \mathbb{Z}$ satisfy $a \leq b \leq a$. Suppose, towards a contradiction, that $a \neq b$. Then $a < b < a$. By definition, this means that

$$b - a \in \mathbb{N} \quad \text{and} \quad a - b \in \mathbb{N}.$$

Then, by Axiom 2.1(i),

$$0 = (a - b) + (b - a) \in \mathbb{N}.$$

This contradicts Axiom 2.1(iii). Since the assumption $a \neq b$ leads to a contradiction, we must have $a = b$. □

Proposition 2.9. *Suppose $a, b, c, d \in \mathbb{Z}$.*

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

(ii) If $a < b$ and $c < d$, then $a + c < b + d$.

(iii) If $0 < a < b$ and $0 < c \leq d$, then $ac < bd$.

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

Proof. The proof of part (iii) can be found in [BG10, Prop. 2.7]. We will prove part (iv) and leave the proofs of the other parts as an exercise (Exercise 2.2.2).

Suppose $a, b, c \in \mathbb{Z}$ satisfy $a < b$ and $c < 0$. So $b - a \in \mathbb{N}$ and

$$-c = 0 + (-c) = 0 - c \in \mathbb{N}.$$

Thus, by Axiom 2.1(ii),

$$(b - a)(-c) \in \mathbb{N}.$$

Now,

$$(b - a)(-c) = b(-c) - a(-c) = ac - bc.$$

Therefore $ac - bc \in \mathbb{N}$, and so $bc < ac$. □

Proposition 2.10. *If $a, b \in \mathbb{Z}$, then exactly one of the following statements in true:*

- $a < b$,
- $a = b$,
- $a > b$.

Proof. The proof of this proposition is left as an exercise (Exercise 2.2.3). □

Proposition 2.11. *If $a \in \mathbb{Z}$ and $a \neq 0$, then $a^2 \in \mathbb{N}$. (Here a^2 means $a \cdot a$.)*

Proof. Suppose $a \in \mathbb{Z}$ and $a \neq 0$. By Axiom 2.1(iv), either $a \in \mathbb{N}$ or $-a \in \mathbb{N}$.

Case 1: Suppose $a \in \mathbb{N}$. Then $a^2 \in \mathbb{N}$ by Axiom 2.1(ii).

Case 2: Suppose $-a \in \mathbb{N}$. Then

$$a^2 = a \cdot a = (-a)(-a) \in \mathbb{N}$$

by Proposition 1.21 and Axiom 2.1(ii). □

Proposition 2.12. *There is no $a \in \mathbb{Z}$ satisfying $a^2 = -1$.*

Proof. We will prove this by contradiction. Suppose there is an $a \in \mathbb{Z}$ such that $a^2 = -1$. We split the proof into two cases:

Case 1: $a = 0$. Then $a^2 = 0 \cdot 0 = 0$, and so $0 = -1$. Adding 1 to both sides gives $1 = 0$, which contradicts Axiom 1.3.

Case 2: $a \neq 0$. In this case, Proposition 2.11 implies that $-1 = a^2 \in \mathbb{N}$. By Proposition 2.4, we also have $1 \in \mathbb{N}$. This contradicts Proposition 2.3.

In both cases, we arrived at a contradiction. This completes the proof by contradiction. □

Proposition 2.13. *If $a \in \mathbb{N}$ and $b \in \mathbb{Z}$ satisfy $ab \in \mathbb{N}$, then $b \in \mathbb{N}$.*

Proof. The proof of this proposition is left as an exercise (Exercise 2.2.4). □

Proposition 2.14. *Suppose $a, b, c, d \in \mathbb{Z}$.*

(i) $-a < -b$ *if and only if* $a > b$.

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

(iii) If $c < 0$ *and* $ac < bc$, *then* $b < a$.

(iv) If $a \leq b$ *and* $0 \leq c$, *then* $ac \leq bc$.

Proof. We prove part (iv) and leave the other parts as exercises (Exercise 2.2.5). Assume $a \leq b$ and $0 \leq c$. We split the proof into three cases.

Case 1: $c = 0$. Then $ac = 0$ and $bc = 0$. So $ac \leq bc$ is true since $0 \leq 0$.

Case 2: $c > 0$ and $a = b$. Then $ac = bc$ and so $ac \leq bc$ is true.

Case 3: $c > 0$ and $a < b$. Then we have $c \in \mathbb{N}$ and $b - a \in \mathbb{N}$. Therefore,

$$bc - ac = (b - a)c \in \mathbb{N},$$

by the closure of $\mathbb{N}$ under multiplication (Axiom 2.1(ii)). Therefore, $ac \leq bc$. □

If A and B are sets, we will write $A \subseteq B$ to mean that A is a subset of B. In other words $A \subseteq B$ means that

$$x \in A \implies x \in B.$$

Two sets are *equal*, written $A = B$, if

$$A \subseteq B \quad \text{and} \quad B \subseteq A.$$

If other words, $A = B$ means that

$$x \in A \iff x \in B.$$

(If P and Q are statements, then "$P \iff Q$" means "$P \implies Q$ *and* $Q \implies P$".) We write $A \subsetneq B$ if

$$A \subseteq B \quad \text{and} \quad A \neq B.$$

Note that this is *different* than the symbol $\not\subseteq$ which means "is not a subset of". Thus $A \not\subseteq B$ if and only if there is at least one element of A that is not an element of B.

It is best to avoid the symbol $\subset$ because of its ambiguity. Some authors use $\subset$ to mean $\subseteq$ and others use it to mean $\subsetneq$.

We will use the notation

$$\{n \in \mathbb{Z} : \text{some property of } n\}$$

to denote the set of integers satisfying a given property. For example $\{n \in \mathbb{Z} : n > 3\}$ is the set of all integers greater than 3. We will discuss sets in more detail later, in Chapter 5.

Proposition 2.15. *We have* $\mathbb{N} = \{n \in \mathbb{Z} : n > 0\}$.

Proof. We have

$$\begin{aligned} a \in \{n \in \mathbb{Z} : n > 0\} &\iff a \in \mathbb{Z} \text{ and } a > 0 \\ &\iff a \in \mathbb{Z} \text{ and } a = a - 0 \in \mathbb{N} \\ &\iff a \in \mathbb{N}. \end{aligned}$$

□

Exercises.

2.2.1. Prove Proposition 2.7.

2.2.2. Prove the remaining parts of Proposition 2.9.

2.2.3. Prove Proposition 2.10.

2.2.4. Prove Proposition 2.13. *Hint*: Consider three cases: $b < 0$, $b = 0$, and $b > 0$.

2.2.5. Prove the remaining parts of Proposition 2.14.

2.2.6. Prove that if $a, b, c \in \mathbb{Z}$ satisfy $a \leq b$ and $b \leq c$, then $a \leq c$. (In other words, the relation $\leq$ is transitive. Note that it follows from this that $\geq$ is also transitive.)

2.3 Induction

In this section we introduce an important method of proof: *mathematical induction*. This method is based on the natural numbers, and we need one further axiom before discussing induction. Before stating this axiom, we begin with a proposition.

Proposition 2.16. *(i)* $1 \in \mathbb{N}$.

(ii) $n \in \mathbb{N} \implies n + 1 \in \mathbb{N}$.

Proof. Part (i) was already proved in Proposition 2.4. Then part (ii) follows from Axiom 2.1(i). □

The new axiom states that $\mathbb{N}$ is the smallest subset of $\mathbb{Z}$ satisfying Proposition 2.16.

Axiom 2.17 (Induction Axiom)**.** Suppose a subset $A \subseteq \mathbb{Z}$ satisfies the following properties:

(i) $1 \in A$,

(ii) $n \in A \implies n + 1 \in A$.

Then $\mathbb{N} \subseteq A$.

Proposition 2.18. *Suppose $B \subseteq \mathbb{N}$ satisfies:*

(i) $1 \in B$,

(ii) $n \in B \implies n + 1 \in B$.

Then $B = \mathbb{N}$.

Proof. By hypothesis, $B \subseteq \mathbb{N}$. By Axiom 2.17, $\mathbb{N} \subseteq B$. Thus $B = \mathbb{N}$. □

Proposition 2.18 is the basis of the principle of induction.

Theorem 2.19 (Principle of mathematical induction: first form)**.** *Suppose that, for each $k \in \mathbb{N}$, we have a statement $P(k)$. Furthermore, suppose that*

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

(ii) for all $n \in \mathbb{N}$, $P(n) \implies P(n+1)$.

Then $P(k)$ is true for all $k \in \mathbb{N}$.

Proof. Assume that (i) and (ii) are true. Let

$$B := \{k \in \mathbb{N} : P(k) \text{ is true}\}.$$

Then $1 \in B$ by (i) and $n \in B \implies n+1 \in B$ by (ii). Therefore, by Proposition 2.18, $B = \mathbb{N}$. In other words, $P(k)$ is true for all $k \in \mathbb{N}$. □

Proofs that use Theorem 2.19 are called *proofs by induction*. In proofs by induction, statement (i) is often called the *base case* and statement (ii) is often called the *induction step*. While proving the induction step, we typically assume $P(n)$ is true and then show that $P(n+1)$ follows from this assumption. When doing this, $P(n)$ is called the *induction hypothesis*.

Example 2.20. We will prove by induction that $11^n - 6$ is divisible by 5 for every $n \in \mathbb{N}$. Let $P(k)$ be the statement

$$11^k - 6 \text{ is divisible by } 5.$$

Base case: $P(1)$ is the statement that $11^1 - 6$ is divisible by 5. Since $11^1 - 6 = 5$, this is clearly true.

Induction step: Suppose that $P(n)$ is true for some $n \in \mathbb{N}$. Thus, $11^n - 6$ is divisible by 5. Therefore, there exists $m \in \mathbb{Z}$ such that

$$11^n - 6 = 5m.$$

We want to show that $P(n+1)$ is true, that is, $11^{n+1} - 6$ is divisible by 5. We have

$$\begin{aligned} 11^{n+1} - 6 &= 11 \cdot 11^n - 6 \\ &= 11(5m+6) - 6 && \text{(by the induction hypothesis)} \\ &= 55m + 66 - 6 \\ &= 55m + 60 \\ &= 5(11m + 12). \end{aligned}$$

Thus, $11^{n+1} - 6$ is divisible by 5. In other words $P(n+1)$ is true. This completes our proof of the induction step.

Proposition 2.21. *For all $a \in \mathbb{N}$, we have $a \geq 1$.*

Proof. We prove the result by induction on a. Let $P(a)$ be the statement

$$a \geq 1.$$

Base case: The base case $P(1)$ is true because $1 \geq 1$.
Induction step: Suppose that, for some $m \in \mathbb{N}$, the statement $P(m)$ is true; so $m \geq 1$. Since

$$(m+1) - m = 1 \in \mathbb{N},$$

we have $m + 1 > m$, and so $m + 1 \geq m \geq 1$. Thus $m + 1 \geq 1$ by transitivity of $\geq$ (see Exercise 2.2.6). So $P(m + 1)$ is true, completing the proof of the inductive step. □

Proposition 2.22. *There is no integer a satisfying $0 < a < 1$.*

Proof. Suppose, towards a contradiction, that there is an integer a satisfying $0 < a < 1$. Since $a > 0$, we have $a \in \mathbb{N}$. Thus, by Proposition 2.21, we have $a \geq 1$. Since $a < 1$ implies that $a \leq 1$, we have

$$1 \leq a \leq 1.$$

Therefore, by Proposition 2.8, we have $a = 1$. Since $a < 1$, we obtain the inequality $1 < 1$, which means that $0 = 1 - 1 \in \mathbb{N}$. This contradicts Axiom 2.1(iii). Therefore, our original assumption is false. Thus, there is no integer a satisfying $0 < a < 1$. □

Corollary 2.23. *Suppose $b \in \mathbb{Z}$. There is no integer a satisfying $b < a < b + 1$.*

Proof. The proof of this corollary is left as an exercise (Exercise 2.3.2). □

Proposition 2.24. *Suppose $a, b \in \mathbb{N}$. If $b|a$, then $b \leq a$.*

Proof. We prove the result by contradiction. Suppose $a, b \in \mathbb{N}$, $b|a$, and $b > a$. By the definition of divisibility, there exists some $c \in \mathbb{Z}$ such that $a = bc$. Then the inequality $b > a$ is equivalent to $b > bc$. By Proposition 2.14(ii), we have $1 > c$. Then Proposition 2.22 and Proposition 2.10 imply that $c \leq 0$.

Case 1: $c = 0$. In this case, we have $a = b \cdot 0 = 0$, which contradicts the fact that $a \in \mathbb{N}$ (by Axiom 2.1(iii)).

Case 2: $c < 0$. In this case $-c = 0 - c \in \mathbb{N}$. Thus

$$-a = -(bc) = b(-c) \in \mathbb{N},$$

which contradicts the fact that $a \in \mathbb{N}$ (by Proposition 2.3).

In either case we arrive at a contradiction, and so our proof is complete. □

Example 2.25. Let us prove that $8^n - 3^n$ is divisible by 5 for all $n \in \mathbb{N}$. We will prove this by induction. Let

$$P(n) \quad \text{be the statement} \quad \text{“}8^n - 3^n \text{ is divisible by } 5\text{”}.$$

Since $8^1 - 3^1 = 8 - 3 = 5 = 5 \cdot 1$, we see that $P(1)$ is true.

Now assume that $P(n)$ is true for some $n \in \mathbb{N}$. So there exists $m \in \mathbb{Z}$ such that $8^n - 3^n = 5m$. Then

$$\begin{aligned} 8^{n+1} - 3^{n+1} &= 8^{n+1} - 3 \cdot 8^n + 3 \cdot 8^n - 3^{n+1} \\ &= 8 \cdot 8^n - 3 \cdot 8^n + 3 \cdot 8^n - 3 \cdot 3^n \\ &= (8-3) \cdot 8^n + 3 \cdot (8^n - 3^n) \\ &= 5 \cdot 8^n + 15m \\ &= 5 \cdot (8^n + 3m). \end{aligned}$$

Since $8^n + 3m \in \mathbb{Z}$, we see that 5 divides $8^{n+1} - 3^{n+1}$.

Sometimes we wish to start an induction at an integer other than 1.

Theorem 2.26 (Principle of mathematical induction: first form revisited)**.** *Suppose m is a fixed integer and that, for each $k \in \mathbb{Z}$ with $k \geq m$, we have a statement $P(k)$. Furthermore, suppose that*

(i) $P(m)$ is true, and

(ii) for all $n \geq m$, $P(n) \implies P(n+1)$.

Then $P(k)$ is true for all $k \geq m$.

Proof. If we set $Q(k) = P(k + m - 1)$ for all $k \in \mathbb{N}$, then this theorem is reduced to Theorem 2.19. See [BG10, Th. 2.25] for details. □

Example 2.27. We will prove that

$$3k^2 + 15k + 19 \geq 0 \text{ for all integers } k \geq -2.$$

Base case: When $k = -2$, we have $3(-2)^2 + 15(-2) + 19 = 12 - 30 + 19 = 1 \geq 0$. So the statement is true for $k = -2$.

Induction step: Suppose the statement is true for some $k \geq -2$. Then

$$\begin{aligned} 3(k+1)^2 + 15(k+1) + 19 &= 3(k^2 + 2k + 1) + 15k + 15 + 19 \\ &= 3k^2 + 21k + 37 \\ &= (3k^2 + 15k + 19) + (6k + 18) \\ &\geq 0 + 6k + 18 = 6k + 18. \end{aligned}$$

Now, we have

$$\begin{aligned} k \geq -2 &\implies 6k \geq -12 && \text{(by Prop. 2.14(iv))} \\ &\implies 6k + 18 \geq 6 \geq 0 && \text{(by Prop. 2.9(i))}. \end{aligned}$$

Thus

$$3(k+1)^2 + 15(k+1) + 19 \geq 0,$$

which completes the induction step.

Exercises.

2.3.1 ([BG10, Prop. 2.18]). Prove the following statements.

(i) For all $k \in \mathbb{N}$, $k^3 + 2k$ is divisible by 3.

(ii) For all $k \in \mathbb{N}$, $k^4 - 6k^3 + 11k^2 - 6k$ is divisible by 4.

(iii) For all $k \in \mathbb{N}$, $k^3 + 5k$ is divisible by 6.

2.3.2. Prove Corollary 2.23.

2.3.3 ([BG10, Prop. 2.27]). Prove that, for all integers $k \geq 2$, we have $k^2 < k^3$.

2.4 The well-ordering principle

Definition 2.28 (Smallest and greatest elements)**.** Suppose $A \subseteq \mathbb{Z}$ is nonempty. If there exists $m \in A$ such that

$$m \leq a \text{ for all } a \in A,$$

then we say m is a *smallest element* of A and write $m = \min(A)$. If there exists $M \in A$ such that

$$M \geq a \text{ for all } a \in A,$$

then we say M is a *greatest element* of A and write $M = \max(A)$.

Proposition 2.29. *Suppose $A \subseteq \mathbb{Z}$ is nonempty.*

(i) If A has a smallest element, then this element is unique. In other words, A has at most one *smallest element.*

(ii) If A has a greatest element, then this element is unique. In other words, A has at most one *greatest element.*

Proof. Suppose a and b are both smallest elements of A. Then $a \leq b$ and $b \leq a$. Thus, by Proposition 2.8, we have $a = b$. The proof of the second part of the proposition is analogous. □

Example 2.30. By Propositions 2.4 and 2.21, 1 is the smallest element of $\mathbb{N}$. On the other hand, by Proposition 2.7, $\mathbb{N}$ has no greatest element.

Example 2.31. The set of even integers has neither a smallest element nor a greatest element. However, the set of negative even integers has greatest element -2, but no smallest element.

Remark 2.32. We will always use the words *positive* and *negative* in the strict sense. So $a \in \mathbb{Z}$ is positive if $a > 0$ and negative if $a < 0$. We say $a \in \mathbb{Z}$ is *nonnegative* if $a \geq 0$.

Theorem 2.33 (Well-ordering principle)**.** *Every nonempty subset of* $\mathbb{N}$ *has a smallest element.*

Proof. Define the set

$$A := \{k \in \mathbb{N} : \text{every subset of } \mathbb{N} \text{ containing an integer } \leq k \text{ has a smallest element}\}.$$

If we prove that $A = \mathbb{N}$, then we have proved the theorem. We will prove by induction that A contains every natural number.

Base case: As seen in Example 2.30, 1 is a smallest element of $\mathbb{N}$. Therefore, if any subset of $\mathbb{N}$ contains 1, then 1 is its smallest element. Therefore, $1 \in A$.

Induction step: Assume $n \in A$ for some $n \in \mathbb{N}$. Suppose that $S \subseteq \mathbb{N}$ contains an integer $\leq n+1$. We want to prove that S has a smallest element. If S contains an integer $\leq n$, then S has a smallest element by the induction hypothesis. Otherwise (i.e. when S does not contain an integer $\leq n$), S must contain $n+1$ (by Corollary 2.23), and this integer is the smallest element of S. □

Proposition 2.34. *Suppose* A *is a nonempty subset of* $\mathbb{Z}$ *and* $b \in \mathbb{Z}$ *satisfies* $b \leq a$ *for all* $a \in A$*. (We say that* A *is* bounded below *by* b*.) Then* A *has a smallest element.*

Proof. Let A be a nonempty subset of $\mathbb{Z}$ and suppose $b \in \mathbb{Z}$ satisfies $b \leq a$ for all $a \in A$. Define a new set by

$$B := \{a + 1 - b : a \in A\}.$$

For all $a \in A$, we have $b \leq a$, so $b < a + 1$, and hence $a + 1 - b \in \mathbb{N}$. Thus, $B \subseteq \mathbb{N}$. Since A is nonempty, so is B. Therefore, by the well-ordering principle (Theorem 2.33), B has a smallest element c. Then, $c = d + 1 - b$ for some $d \in A$ (by the definition of B). For all $a \in A$, we have

$$a + 1 - b \in B \implies a + 1 - b \geq c = d + 1 - b \implies a \geq d.$$

Thus d is a smallest element of A. □

We will now use the well-ordering principle in a definition. First we need a proposition.

Proposition 2.35. *Suppose* a *and* b *are integers that are not both* 0*. Then the set*

$$S = \{k \in \mathbb{N} : k = ax + by \text{ for some } x, y \in \mathbb{Z}\}$$

is nonempty.

Proof. The proof of this proposition is left as an exercise (Exercise 2.4.1). □

Definition 2.36 (gcd)**.** Suppose $a, b \in \mathbb{Z}$. If a and b are not both zero, we define

$$\gcd(a, b) = \min\big(\{k \in \mathbb{N} : k = ax + by \text{ for some } x, y \in \mathbb{Z}\}\big).$$

(Since this set is nonempty by Proposition 2.35, it has a minimum element by Theorem 2.33.) If $a = b = 0$, we define $\gcd(0, 0) = 0$.

We will see later that $\gcd(a, b)$ is actually the greatest common divisor of a and b, justifying the notation (see Proposition 6.29).

Exercises.

2.4.1. Prove Proposition 2.35.

Chapter 3

Logic

We have already used logical argument in Chapters 1 and 2. One of our goals there was to introduce ourselves to the concept of mathematical proof before getting into the technicalities of logic. In the current chapter will examine some basic concepts of logic in more detail. This will allow us to be more precise in our mathematical arguments.

3.1 Quantifiers

The symbol $\exists$ is called the *existential quantifier*. It means *there exists* or *there exist*. The symbol $\forall$ is called the *universal quantifier*. It means *for all* or *for each* or *for every* or *whenever*.

Examples 3.1. (i) "$\exists m \in \mathbb{Z}$ such that $m > 5$" means "there exists an element $m \in \mathbb{Z}$ such that $m > 5$". (This statement is true.)

(ii) "$\forall m \in \mathbb{Z}$, $m < 5$" means "for all $m \in \mathbb{Z}$, we have $m < 5$". (This statement is false.)

(iii) Axiom 1.2 could be written: $\exists 0 \in \mathbb{Z}$ such that $\forall a \in \mathbb{Z}$, $a + 0 = a$.

(iv) Axiom 1.3 could be written: $\exists 1 \in \mathbb{Z}$ such that ($1 \neq 0$ and $\forall a \in \mathbb{Z}$, $a \cdot 1 = a$).

Statements with quantifiers consist of *quantified segments* of the form ($\exists \ldots$ such that) and/or ($\forall \ldots$) in a certain order, and then a *final statement* or assertion. For instance, in example (iii) above, we have

$$\underbrace{(\exists 0 \in \mathbb{Z} \text{ such that})(\forall a \in \mathbb{Z})}_{\text{quantified segments}} \underbrace{a + 0 = a}_{\text{final statement}} .$$

The order of quantifiers is *very* important. Consider the following statements:

(i) $(\forall a \in \mathbb{Z})(\exists b \in \mathbb{Z}$ such that$)$ $a + b = 0$

(ii) $(\exists b \in \mathbb{Z}$ such that$)(\forall a \in \mathbb{Z})$ $a + b = 0$

Statement (i) asserts that, for each integer a, there is an integer $b \in \mathbb{Z}$, *which could depend on* a, such that $a + b = 0$. This is true, since one can choose $b = -a$. On the other hand, statement (ii) asserts that there is some integer b such that $a + b = 0$ for *all* integers a. This is false, since there is no b that satisfies this condition for all a. So in statement (i), b may depend on a, whereas in statement (ii) it may not.

The particular variable used in a quantified statement is not important. For example,

$$(\forall a \in \mathbb{Z})(\exists b \in \mathbb{Z} \text{ such that}) \ a + b = 0 \quad \equiv \quad (\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z} \text{ such that}) \ m + n = 0,$$

where the symbol $\equiv$ denotes logical equivalence.

One can combine several consecutive $\forall$-phrases in a row. For example

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z}) \qquad \text{has the same meaning as} \qquad (\forall a, b \in \mathbb{Z}).$$

Similarly, one can combine several $\exists$-phrases:

$$(\exists a \in \mathbb{N})(\exists b \in \mathbb{N}) \qquad \text{has the same meaning as} \qquad (\exists a, b \in \mathbb{N}).$$

Examples 3.2. We can express many statements using quantifiers.

(i) "Every natural number is greater than -1" can be written as $(\forall n \in \mathbb{N})\ n > -1$.

(ii) "Every integer is the sum of two integers" can be written as $(\forall a \in \mathbb{Z})(\exists b, c \in \mathbb{Z} \text{ such that})\ b + c = a$.

(iii) "There exists a smallest natural number" can be written as $(\exists n \in \mathbb{N} \text{ such that})(\forall m \in \mathbb{N})\ n \leq m$.

Examples 3.3. (i) The statement "$(\forall x \in \mathbb{Z})(\exists y \in \mathbb{N} \text{ such that })\ x < y$" is true.

(ii) The statement "$(\exists y \in \mathbb{N} \text{ such that })(\forall x \in \mathbb{Z})\ x < y$" is false.

(iii) The statement "$(\forall x \in \mathbb{Z})\ x^2 \geq 0$" is true.

For all statements can often be rewritten as *if then* statements. For example

$$(\forall x \in \mathbb{Z})\ x^2 \geq 0 \qquad \text{is equivalent to} \qquad \text{if } x \in \mathbb{Z}, \text{ then } x^2 \geq 0.$$

The symbol $\nexists$ means *there does not exist*. For example, the statement

$$(\nexists a \in \mathbb{N} \text{ such that})(\forall b \in \mathbb{N})\ a > b$$

means that there is no natural number that is greater than all other natural numbers.

Uniqueness. The symbol $\exists!$ means *there exists a unique*. For example, Axiom 1.4 and Proposition 1.10 imply the statement

$$(\forall a \in \mathbb{Z})(\exists! b \in \mathbb{Z} \text{ such that})\ a + b = 0.$$

A statement of the form $(\exists! n \in \mathbb{N} \text{ such that})$ is actually two statements:

- *existence*: $(\exists n \in \mathbb{N} \text{ such that})$, and
- *uniqueness*: (if $n \in \mathbb{N}$ and $m \in \mathbb{N}$ both have the given property, then $n = m$).

Exercises.

3.1.1. Express each of the following statements using quantifiers. (Note that we make no claim as to the validity of these statements. We merely translate them.)

(i) There exists a largest integer.

(ii) There exists a smallest natural number.

(iii) Every integer is the sum of two integers.

(iv) Every integer is the square of an integer.

(v) The equation $x^2 + 5y^3 = 4$ has a unique integer solution (i.e. it has one and only one solution where x and y are integers).

3.1.2. For each of the following statements, decide whether it is true or false.

(i) $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z}$ such that$)\ x + y = 2$

(ii) $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{N}$ such that$)\ x + y = 2$

(iii) $(\exists x \in \mathbb{Z}$ such that$)(\forall y \in \mathbb{Z})\ x + y = 2$

(iv) $(\exists a \in \mathbb{Z}$ such that$)(\forall b \in \mathbb{Z})\ a + b = b$

(v) $(\forall b \in \mathbb{Z})(\exists a \in \mathbb{Z}$ such that$)\ a + b = b$

3.2 Implications

The symbol $\implies$ means *implies*. If P and Q are statements, then the following are equivalent:

- $P \implies Q$.
- P implies Q.
- If P, then Q.
- (not P) or Q.

Remark 3.4. It is important to note that if P is a false statement, then the implication $P \implies Q$ is true. This follows from the fact, mentioned above, that "$P \implies Q$" is equivalent to "(not P) or Q". For example, the statement

if 5 is an even number, then there is life on Mars

is true (regardless of whether or not there is life on Mars), since the statement "5 is an even number" is false.

To see that the implication $P \implies Q$ is equivalent to "(not P) or Q", we can compare their *truth tables*.

P	Q	$P \implies Q$	(not P) or Q
true	true	true	true
true	false	false	false
false	true	true	true
false	false	true	true

The *double implication* symbol $\iff$ means *if and only if*. If P and Q are statements, then the following are equivalent:

- $P \iff Q$.
- P if and only if Q.
- $(P \implies Q)$ and $(Q \implies P)$.
- Either P and Q are both false, or P are Q are both true.
- (P and Q) or ((not P) and (not Q)).

Examples 3.5. Suppose n is an integer.

(i) The statement (n is divisible by 2 $\iff$ n is even) is true.

(ii) The statement (n is divisible by 4 $\iff$ n is even) is false.

Converse. The *converse* of the implication $P \implies Q$ is the implication $Q \implies P$. **Important:** An implication and its converse are *not* equivalent in general. It is possible for one to be true, while the other is false. (It is also possible for both to be true or both to be false.)

Example 3.6. The statement

$$n \text{ is divisible by } 4 \implies n \text{ is even}$$

is true. However, its converse is

$$n \text{ is even} \implies n \text{ is divisible by } 4,$$

which is false.

Contrapositive. The *contrapositive* of an implication $P \implies Q$ is the implication (not Q) $\implies$ (not P). An implication and its contrapositive are equivalent. That is

$$P \implies Q \qquad \text{is equivalent to} \qquad (\text{not } Q) \implies (\text{not } P).$$

Example 3.7. The statement

$$n \text{ is divisible by } 4 \implies n \text{ is even}$$

is equivalent to its contrapositive

$$n \text{ is not even} \implies n \text{ is not divisible by } 4.$$

Sometimes the easiest way to prove a statement is to prove its contrapositive.

Exercises.

3.2.1. Give two examples of true mathematical statements whose converses are false. (Do not give examples that we have already seen.)

3.2.2. Try re-proving some of the if-then propositions in Chapters 1 and 2 by proving their contrapositives.

3.3 Negations

If P is a statement, then its *negation* is the statement (not P). For example, the negation of (n is even) is (n is not even). We will sometimes write $\neg P$ for "not P".

Negation of "and" and "or". Negation interchanges "and" and "or" in the following sense (sometimes called *De Morgan's laws*):

- $\neg(P \text{ or } Q) \equiv (\neg P \text{ and } \neg Q)$,
- $\neg(P \text{ and } Q) \equiv (\neg P \text{ or } \neg Q)$.

Example 3.8. Suppose P is some property that an integer may possess. Then the statement "$\exists! n \in \mathbb{Z}$ with property P" is equivalent to

$$(\exists n \in \mathbb{Z} \text{ with property } P) \text{ and } (\text{there is at most one integer with property } P).$$

Its negation is therefore

$$(\text{there is no } n \in \mathbb{Z} \text{ with property } P) \text{ or } (\text{there is more than one integer with property } P).$$

Negation of an implication. Since the implication $P \implies Q$ is equivalent to "$\neg P$ or Q", the negation of the implication $P \implies Q$ is "P and $\neg Q$". In other words,

$$\neg(P \implies Q) \equiv \neg(\neg P \text{ or } Q) \equiv (P \text{ and } \neg Q).$$

Negations involving quantifiers. Now suppose we want to find the negation of a statement involving the quantifiers $\forall$ and $\exists$. We write it in the form of quantified segments followed by a final statement. Then, to find the negation we do the following:

(i) We maintain the order of the quantified segments, but change every $(\forall \ldots)$ segment into a $(\exists \ldots$ such that$)$ segment.

(ii) Change each $(\exists \ldots$ such that$)$ segment into a $(\forall \ldots)$ segment.

(iii) Negate the final statement.

Example 3.9. Axiom 1.2 can be written as

$$(\exists b \in \mathbb{Z} \text{ such that})(\forall a \in \mathbb{Z})\ a + b = a.$$

(We have replaced the quantified variable 0 by b, which does not change the meaning of the implication.) Its negation is

$$(\forall b \in \mathbb{Z})(\exists a \in \mathbb{Z} \text{ such that})\ a + b \neq a.$$

Examples 3.10. (i) The negation of "every differentiable function is continuous" is "there exists a differentiable function that is not continuous".

(ii) The negation of "none of Paul's Facebook posts are interesting" is "there exists a Facebook post by Paul that is interesting".

(iii) The negation of

$$(\forall \varepsilon > 0)\ (\exists \delta > 0 \text{ such that})\ (\forall x \in \mathbb{R})\ (|x - a| < \delta \implies |f(x) - f(a)| < \varepsilon)$$

is

$$(\exists \varepsilon > 0 \text{ such that})\ (\forall \delta > 0)\ (\exists x \in \mathbb{R} \text{ such that})\ (|x - a| < \delta \text{ and } |f(x) - f(a)| \geq \varepsilon).$$

(The first statement is the definition of continuity at the point a.)

Exercises.

3.3.1. Negate the following statements.

(i) Every polynomial has a real root.

(ii) Steve is blond and Samantha is tall.

(iii) $\forall x \in \mathbb{Z},\ \exists! y \in \mathbb{Z}$ such that $xy = 3$.

(iv) That cow is neither large nor pink.

(v) If $f(x, y) > 0$, then $x > 0$ or $y \leq 0$.

(vi) The quotient group G/N is finite if and only if G is finite.

(vii) For each $L \in \mathbb{N}$, there exists $N \in \mathbb{N}$ such that $x_N > L$.

Chapter 4

Finite series and strong induction

In this chapter we will introduce some common mathematical notions such as summation notation, product notation, and factorials. We will then prove the important Binomial Theorem and introduce a second form of mathematical induction.

4.1 Preliminaries

An *(infinite) sequence* is a list of integers x_j for $j \in \mathbb{N}$. We denote such a sequence by $(x_j)_{j=1}^{\infty}$. (Later we will see that a sequence is a function with domain $\mathbb{N}$. See Example 5.21.) It is possible that the indices (i.e. the subscripts) do not start at 1, but rather at some other integer m. In that case, we write $(x_j)_{j=m}^{\infty}$. A *finite sequence* $(x_j)_{j=m}^{M}$ is a list of numbers

$$x_m, x_{m+1}, x_{m+2}, \ldots, x_{M-1}, x_M.$$

(Here $m, M \in \mathbb{Z}$ with $m \leq M$.)

Example 4.1. If we define $x_j = j^2 - 5$, then $x_1 = -4$, $x_2 = -1$, $x_3 = 4$, etc. The number x_k is called the k-th *term* of the sequence.

Some sequences are defined *recursively*.

Example 4.2. Consider a sequence $(x_j)_{j=1}^{\infty}$ defined as follows.

(i) Define $x_1 = 1$.

(ii) Assuming x_n is defined, define $x_{n+1} = 2x_n - 3$.

Then, in this sequence, we have $x_1 = 1$, $x_2 = -1$, $x_3 = -5$, $x_4 = -13$, etc.

Note that the sequence of Example 4.1 was defined directly. Given any k, we can immediately compute x_k. On the other hand, the sequence of Example 4.2 was defined recursively. In order to compute the k-th term, we must compute all the terms before it.

Example 4.3. Define a sequence $(x_n)_{n=1}^{\infty}$ recursively as follows:

$$x_1 = -4,$$

$$x_{n+1} = 3x_n - 8 \text{ for } n \geq 1.$$

Let's prove that x_n is even for all $n \in \mathbb{N}$.

Base case: When $n = 1$, we have $x_1 = -4 = 2(-2)$. So x_1 is divisible by 2, hence is even.

Induction step: Suppose x_n is even for some $n \geq 1$. Thus, we have $x_n = 2m$ for some $m \in \mathbb{Z}$. Then

$$x_{n+1} = 3x_n - 8 = 3(2m) - 8 = 2(3m - 4).$$

Since $m \in \mathbb{Z}$, we have $3m - 4 \in \mathbb{Z}$. Thus x_{n+1} is divisible by 2, hence is even. This completes the proof of the induction step.

Summation and product notation. If $(x_j)_{j=m}^n$ is a finite sequence of integers, we define

$$\sum_{j=m}^{n} x_j = x_m + x_{m+1} + \cdots + x_n,$$

$$\prod_{j=m}^{n} x_j = x_m x_{m+1} \cdots x_n.$$

(If $m = n$, we interpret these as $\sum_{j=m}^m x_j = x_m$ and $\prod_{j=m}^m x_j = x_m$.)

We let

$$\mathbb{Z}_{\geq 0} := \{n \in \mathbb{Z} : n \geq 0\}$$

denote the set of nonnegative integers..

Factorial. For $n \in \mathbb{Z}_{\geq 0}$ we define $n!$ (read "n factorial") as follows:

(i) We define $0! := 1$.

(ii) For $n > 0$, we define $n! = \prod_{j=1}^n j = 1 \cdot 2 \cdot \cdots \cdot n$.

Exercises.

4.1.1 ([BG10, Proj. 4.3]). Suppose m is a natural number. Define the following sequence:

(i) Define $x_1 = m$.

(ii) Assuming x_n is defined, define

$$x_{n+1} = \begin{cases} \frac{x_n}{2} & \text{if } x_n \text{ is even,} \\ x_n + 1 & \text{otherwise.} \end{cases}$$

Does this sequence eventually take on the value 1, no matter what value of $m \in \mathbb{N}$ was chosen to start with? Try to prove your assertion.

4.1.2 ([BG10, Prop. 4.7]). Prove that, for all $k \in \mathbb{N}$:

(i) $5^{2k} - 1$ is divisible by 24;

(ii) $2^{2k+1} + 1$ is divisible by 3;

(iii) $10^k + 3 \cdot 4^{k+2} + 5$ is divisible by 9.

4.1.3 ([BG10, Prop. 4.8]). Prove that, for all $k \in \mathbb{N}$, $4^k > k$.

4.1.4 ([BG10, Proj. 4.9]). Determine for which natural numbers k the inequality $k^2 < 2^k$ holds. Prove your answer.

4.1.5. Prove that $2^n < n!$ for $n \geq 4$.

4.1.6. Define a sequence $(x_n)_{n=1}^{\infty}$ recursively as follows:

$$\begin{aligned} x_1 &= 12, \\ x_{n+1} &= 2x_n + 6 \text{ for } n \geq 1. \end{aligned}$$

Prove that x_n is divisible by 3 for all $n \in \mathbb{N}$.

4.1.7. Define a sequence $(x_n)_{n=1}^{\infty}$ recursively as follows:

$$\begin{aligned} x_1 &= 10, \\ x_{n+1} &= x_n^2 + 3x_n - 5 \text{ for } n \geq 1. \end{aligned}$$

Prove that x_n is divisible by 5 for all $n \in \mathbb{N}$.

4.2 Finite series

We will now work out some examples of sums that can be explicitly computed, as well as stating some useful properties of sums.

Recall that if $a, b \in \mathbb{Z}$ and a divides b, then there exists $c \in \mathbb{Z}$ such that $ac = b$. We denote this c by $\frac{b}{a}$. Note that this implies that $\frac{b}{a}$ is an integer and (for now) is *only* defined when a divides b. We have not yet introduced the concept of rational numbers.

Proposition 4.4. *Suppose $n \in \mathbb{N}$.*

(i) $\displaystyle\sum_{j=1}^{n} j = \frac{n(n+1)}{2}.$

(ii) $\displaystyle\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$

Proof. We will prove the first equality, and leave the second as an exercise. We prove the first equality by induction on n. If $n = 1$, we have

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

which proves the base case.

Now assume the result is true for some $n \in \mathbb{N}$. Then we have

$$\begin{aligned}
\sum_{j=1}^{n+1} j &= \left(\sum_{j=1}^{n} j\right) + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{n^2 + 3n + 2}{2} \\
&= \frac{(n+1)(n+2)}{2} \\
&= \frac{(n+1)\big((n+1)+1\big)}{2}.
\end{aligned}$$

This completes the proof of the induction step. □

Proposition 4.5. *For $x \in \mathbb{Z}$ with $x \neq 1$, and $n \in \mathbb{Z}_{\geq 0}$, we have*

$$\sum_{j=0}^{n} x^j = \frac{1 - x^{n+1}}{1 - x}.$$

Proof. Fix $x \in \mathbb{Z}$, $x \neq 1$. We will prove that

$$(1-x)\sum_{j=0}^{k} x^j = 1 - x^{k+1}$$

by induction on $k \geq 0$. The base case $k = 0$ says that

$$(1-x)\sum_{j=0}^{0} x^j = 1 - x,$$

which is true since $\sum_{j=0}^{0} x^j = x^0 = 1$.

For the induction step, we assume the result holds for k equal to some $n \in \mathbb{Z}_{\geq 0}$. Thus, we assume that $(1-x)\sum_{j=0}^{n} x^j = 1 - x^{n+1}$. Then

$$(1-x)\sum_{j=0}^{n+1} x^j = (1-x)\left(\sum_{j=0}^{n} x^j + x^{n+1}\right)$$

$$= (1-x)\sum_{j=0}^{n} x^j + (1-x)x^{n+1} = 1 - x^{n+1} + x^{n+1} - x^{n+2} = 1 - x^{n+2},$$

where we used the induction hypothesis in the second-to-last step. □

The following propositions provide some useful arithmetic properties of sums.

Proposition 4.6. *(i) Suppose $a \in \mathbb{Z}$ and let $(x_j)_{j=m}^{M}$ be a finite sequence in $\mathbb{Z}$. Then*

$$a \cdot \left(\sum_{j=m}^{M} x_j \right) = \sum_{j=m}^{M} (ax_j).$$

(ii) If $a \in \mathbb{Z}$, then for all $n \in \mathbb{N}$,

$$\sum_{j=1}^{n} a = na.$$

In particular, $\sum_{j=1}^{n} 1 = n$.

Proof. (i) We have

$$a \cdot \left(\sum_{j=m}^{M} x_j \right) = a \cdot (x_m + x_{m+1} + \cdots + x_M) = ax_m + ax_{m+1} + \cdots + ax_M = \sum_{j=m}^{M} (ax_j).$$

(ii) We have

$$\sum_{j=1}^{n} a = \underbrace{a + a + \cdots + a}_{n \text{ terms}} = (\underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}})a = na.$$ □

Proposition 4.7. *Suppose $a, b, c \in \mathbb{Z}$ satisfy $a \leq b < c$. Furthermore, suppose $(x_j)_{j=a}^{c}$ and $(y_j)_{j=a}^{c}$ are finite sequences in $\mathbb{Z}$.*

(i) $\displaystyle\sum_{j=a}^{c} x_j = \sum_{j=a}^{b} x_j + \sum_{j=b+1}^{c} x_j.$

(ii) $\displaystyle\sum_{j=a}^{b} (x_j + y_j) = \sum_{j=a}^{b} x_j + \sum_{j=a}^{b} y_j.$

Proof. (i) We have

$$\sum_{j=a}^{c} x_j = (x_a + \cdots + x_b) + (x_{b+1} + \cdots + x_c) = \sum_{j=a}^{b} x_j + \sum_{j=b+1}^{c} x_j.$$

(ii) We have

$$\sum_{j=a}^{b} (x_j + y_j) = (x_a + y_a) + \cdots + (x_b + y_b) = (x_a + \cdots + x_b) + (y_a + \cdots + y_b) = \sum_{j=a}^{b} x_j + \sum_{j=a}^{b} y_j.$$

□

The following proposition shows how we can shift the summation index without altering a sum.

Proposition 4.8. *Suppose $(x_j)_{j=m}^M$ is a finite sequence in $\mathbb{Z}$ and that $r \in \mathbb{Z}$. Then*

$$\sum_{j=m}^{M} x_j = \sum_{j=m+r}^{M+r} x_{j-r}.$$

Proof. We have

$$\sum_{j=m}^{M} x_j = x_m + x_{m+1} + \cdots + x_M = x_{(m+r)-r} + x_{(m+r+1)-r} + \cdots + x_{(M+r)-r} = \sum_{j=m+r}^{M+r} x_{j-r}. \quad \square$$

Finally, we prove a useful result about inequalities for finite sums.

Proposition 4.9. *Suppose $(x_j)_{j=m}^M$ and $(y_j)_{j=m}^M$ are finite sequences in $\mathbb{Z}$ such that $x_j \leq y_j$ for all $m \leq j \leq M$. Then*

$$\sum_{j=m}^{M} x_j \leq \sum_{k=m}^{M} y_j.$$

Proof. Let $P(M)$ be the statement that

$$\sum_{j=m}^{M} x_j \leq \sum_{k=m}^{M} y_j$$

for all finite sequences $(x_j)_{j=m}^M$ and $(y_j)_{j=m}^M$ in $\mathbb{Z}$ such that $x_j \leq y_j$ for all $m \leq j \leq M$. We will prove that $P(M)$ is true for all $M \geq m$ by induction on M.

First note that $P(m)$ is the statement $x_m \leq y_m$, which is true by assumption. Now suppose that $P(M)$ is true for some $M \geq m$. Then

$$\sum_{j=1}^{M+1} x_j = \sum_{j=1}^{M} x_j + x_{M+1} \leq \sum_{j=1}^{M} y_j + y_{M+1} = \sum_{j=1}^{M+1} y_j.$$

This completes the proof of the induction step. $\square$

Exercises.

4.2.1 ([BG10, Proj. 4.12]). Find and prove a formula for $\sum_{j=1}^{k} j^3$.

4.2.2. Prove by induction that

$$\sum_{i=1}^{k} (3i - 2) = \frac{k(3k-1)}{2} \quad \text{for all } k \in \mathbb{N}.$$

4.2.3. Prove by induction that

$$\sum_{k=3}^{n} \frac{2}{k^2 - 3k + 2} = \frac{2n-4}{n-1} \quad \text{for all } n \in \mathbb{Z},\ n \geq 3.$$

(Strictly speaking, this question involves rational numbers, which we haven't seen yet. But you can do arithmetic with them just like you have in previous math courses.)

4.3 The Binomial Theorem

Theorem 4.10. *Suppose $k, m \in \mathbb{Z}_{\geq 0}$, with $m \leq k$. Then $k!$ is divisible by $m!(k-m)!$.*

Proof. We will prove this result by induction. However, since the statement involves two parameters, we have to be careful about how we set up the induction. For each $k \in \mathbb{Z}_{\geq 0}$, we let $P(k)$ be the statement

$$\text{for all } 0 \leq m \leq k,\ k! \text{ is divisible by } m!(k-m)!.$$

Then, to prove the theorem, it suffices to prove that $P(k)$ is true for all $k \in \mathbb{Z}_{\geq 0}$. We will do this by induction on k.

The base case is when $k = 0$. Then the condition $0 \leq m \leq k$ forces $m = 0$, and so we only need to note that $k! = 0! = 1$ is divisible by $m!(k-m)! = 0!0! = 1 \cdot 1 = 1$.

Now we assume that $P(n)$ is true for some $n \in \mathbb{Z}_{\geq 0}$, and we need to show that $P(n+1)$ is true. If $m = 0$, then $m!(n+1-m)! = 0!(n+1)! = (n+1)!$, which clearly divides $(n+1)!$. Similarly, if $m = n+1$, then $m!(n+1-m)! = (n+1)!0! = (n+1)!$, which divides $(n+1)!$. So it remains to consider the cases where $1 \leq m \leq n$.

Fix m satisfying $1 \leq m \leq n$. We have assumed that $P(n)$ is true. Using the $m-1$ and m cases of $P(n)$, there exist integers a and b such that

$$n! = a(m-1)!(n-m+1)! \quad \text{and} \quad n! = b(m!)(n-m)!.$$

Then

$$\begin{aligned}
(n+1)! &= n!(n+1) \\
&= n!(m+n+1-m) \\
&= n!m + n!(n+1-m) \\
&= a(m-1)!(n-m+1)!m + b(m!)(n-m)!(n+1-m) \\
&= (a+b)(m!)(n-m+1)!,
\end{aligned}$$

which implies that $m!(n+1-m)!$ divides $(n+1)!$, completing the proof of the induction step. □

By Theorem 4.10, $\frac{k!}{m!(k-m)!}$ is an integer for $0 \leq m \leq k$. We define

$$\binom{k}{m} = \frac{k!}{m!(k-m)!},$$

which we read as "k choose m" (since one can show that it is equal to the number of ways of choosing m objects from a collection of k objects) and call it a *binomial coefficient*.

Corollary 4.11. *For $1 \leq m \leq n$, we have*

$$\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}.$$

Proof. In the proof of the Theorem 4.10 we obtained the equality

$$(n+1)! = n!m + n!(n+1-m).$$

Dividing both sides by $m!(n+1-m)!$ gives

$$\begin{aligned} & \frac{(n+1)!}{m!(n+1-m)!} = \frac{n!m}{m!(n+1-m)!} + \frac{n!(n+1-m)}{m!(n+1-m)!} \\ \implies & \frac{(n+1)!}{m!(n+1-m)!} = \frac{n!}{(m-1)!(n+1-m)!} + \frac{n!}{m!(n-m)!}, \end{aligned}$$

which is precisely the corollary. (Note that, while we have not yet discussed division, the steps above are justified by the fact that the Binomial Theorem tells us that the fractions above are actually integers. So we are simply using properties of divisibility of integers.) □

Corollary 4.11 tells us that the binomial coefficients can be obtained from *Pascal's triangle*.

$$\begin{array}{ccccccccccccc} & & & & & & 1 & & & & & & \\ & & & & & 1 & & 1 & & & & & \\ & & & & 1 & & 2 & & 1 & & & & \\ & & & 1 & & 3 & & 3 & & 1 & & & \\ & & 1 & & 4 & & 6 & & 4 & & 1 & & \\ & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\ 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\ & & & & & & \vdots & & & & & & \end{array}$$

If we number the rows from the top, starting at zero, then the m-th entry in the k-th row is $\binom{k}{m}$. Each entry not on the outside edge is the sum of its two neighbours in the previous row. You may have learned in high school that

$$\begin{aligned} (a+b)^2 &= a^2 + 2ab + b^2, \\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3. \end{aligned}$$

Here is the general form, allowing you to write a similar formula for any exponent.

Theorem 4.12 (Binomial Theorem for integers)**.** *If $a, b \in \mathbb{Z}$ and $k \in \mathbb{Z}_{\geq 0}$, then*

$$(a+b)^k = \sum_{m=0}^{k} \binom{k}{m} a^m b^{k-m}.$$

Proof. We prove the result by induction on k. For the base case, we have

$$(a+b)^0 = 1 = \binom{0}{0} a^0 b^0.$$

Now assume that, for some $n \in \mathbb{Z}_{\geq 0}$, we have

$$(a+b)^n = \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m}.$$

Then

$$\begin{aligned}
&\sum_{m=0}^{n+1} \binom{n+1}{m} a^m b^{n+1-m} \\
&\quad = \binom{n+1}{0} a^0 b^{n+1} + \sum_{m=1}^{n} \binom{n+1}{m} a^m b^{n+1-m} + \binom{n+1}{n+1} a^{n+1} b^0 && \text{(by Prop. 4.7(i))} \\
&\quad = b^{n+1} + \sum_{m=1}^{n} \left(\binom{n}{m-1} + \binom{n}{m} \right) a^m b^{n+1-m} + a^{n+1} && \text{(by Cor. 4.11)} \\
&\quad = b^{n+1} + \sum_{m=1}^{n} \binom{n}{m-1} a^m b^{n+1-m} + \sum_{m=1}^{n} \binom{n}{m} a^m b^{n+1-m} + a^{n+1} && \text{(by Prop. 4.7(ii))} \\
&\quad = b^{n+1} + \sum_{m=0}^{n-1} \binom{n}{m} a^{m+1} b^{n+1-(m+1)} + \sum_{m=1}^{n} \binom{n}{m} a^m b^{n+1-m} + a^{n+1} && \text{(by Prop. 4.8 with } r=1) \\
&\quad = \sum_{m=0}^{n} \binom{n}{m} a^{m+1} b^{n+1-(m+1)} + \sum_{m=0}^{n} \binom{n}{m} a^m b^{n+1-m} && \text{(by Prop. 4.7(i))} \\
&\quad = a \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m} + b \sum_{m=0}^{n} \binom{n}{m} a^m b^{n-m} && \text{(by Prop. 4.6(i))} \\
&\quad = a(a+b)^n + b(a+b)^n && \text{(by the induction hypothesis)} \\
&\quad = (a+b)^{n+1},
\end{aligned}$$

completing the proof of the induction step. □

Theorem 4.12 justifies the term *binomial coefficient*, since the integers $\binom{k}{m}$ are the *coefficients* of the expansion of a power of a *binomial*.

Corollary 4.13. *For $k \in \mathbb{Z}_{\geq 0}$, we have*

$$\sum_{m=0}^{k} \binom{k}{m} = 2^k.$$

Proof. Take $a = b = 1$ in Theorem 4.12. □

Exercises.

4.3.1 (Leibniz's formula [BG10, Proj. 4.23]). Consider an operation denoted by $'$ that is applied to functions (denoted u, v, w). Assume that the operation $'$ satisfies the following axioms:

$$\begin{aligned}(u+v)' &= u' + v',\\ (uv)' &= uv' + u'v,\\ (cu)' &= cu', \text{ where } c \text{ is a constant.}\end{aligned}$$

Define $w^{(k)}$ recursively by

(i) $w^{(0)} = w$.

(ii) Assuming $w^{(n)}$ is defined (where $n \in \mathbb{Z}_{\geq 0}$), define $w^{(n+1)} = \left(w^{(n)}\right)'$.

Prove that

$$(uv)^{(k)} = \sum_{m=0}^{k} \binom{k}{m} u^{(m)} v^{(k-m)}.$$

(Of course, you know an operation with these properties, namely, the derivative. However, no calculus is needed to prove the above statement.)

4.4 Strong induction

There is a second form of induction, sometimes called *strong induction*.

Theorem 4.14 (Principle of mathematical induction—second form)**.** *For each $k \in \mathbb{N}$, let $P(k)$ be a statement. Assume that*

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

(ii) if $P(j)$ is true for all integers j such that $1 \leq j \leq n$, then $P(n+1)$ is true.

Then $P(k)$ is true for all $k \in \mathbb{N}$.

Proof. This can be proved by proving the statement "$P(j)$ is true for all integers j such that $1 \leq j \leq k$" by induction (the first form of induction) on k. We leave the details as an exercise (Exercise 4.4.1). □

Note the difference between Theorem 4.14 and Theorem 2.19. In Theorem 2.19, one only assumes $P(n)$ in the induction step. However, in Theorem 4.14, one assumes $P(j)$ for all $1 \leq j \leq n$. Of course, one can start the induction at any integer (as opposed to 1).

The *Fibonacci numbers* $(f_j)_{j=1}^{\infty}$ are defined by

$$f_1 = 1, \qquad f_2 = 1, \qquad \text{and}$$

$$f_n = f_{n-1} + f_{n-2} \qquad \text{for } n \geq 3.$$

Using strong induction, one can obtain an explicit formula for the Fibonacci numbers—one that gives the n-th Fibonacci number directly, without computing it recursively. The formula involves irrational numbers, which we will discuss in more detail later. However, since this is a such a classic example, we will assume for now that we know about irrational numbers.

Proposition 4.15. *For $k \in \mathbb{N}$, we have*

$$f_k = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^k - \left(\frac{1-\sqrt{5}}{2} \right)^k \right). \tag{4.1}$$

Proof. Let

$$a = \frac{1+\sqrt{5}}{2} \qquad \text{and} \qquad b = \frac{1-\sqrt{5}}{2}.$$

Since the recursive formula defining the Fibonacci numbers is not valid until $n \geq 3$, we need to check two bases cases. We leave it as an exercise to check that (4.1) gives $f_1 = 1$ and $f_2 = 1$, as desired.

Now we assume that the formula (4.1) holds for all $1 \leq k \leq n$ for some $n \geq 2$. We will need the computations

$$a + 1 = \frac{3+\sqrt{5}}{2} = \frac{1+2\sqrt{5}+5}{4} = a^2,$$
$$b + 1 = \frac{3-\sqrt{5}}{2} = \frac{1-2\sqrt{5}+5}{4} = b^2.$$

Then we have

$$\begin{aligned} f_{n+1} &= f_n + f_{n-1} \\ &= \frac{1}{\sqrt{5}}(a^n - b^n) + \frac{1}{\sqrt{5}}(a^{n-1} - b^{n-1}) \\ &= \frac{1}{\sqrt{5}}(a^n + a^{n-1} - b^n - b^{n-1}) \\ &= \frac{1}{\sqrt{5}}(a^{n-1}(a+1) - b^{n-1}(b+1)) \\ &= \frac{1}{\sqrt{5}}(a^{n-1}a^2 - b^{n-1}b^2) \\ &= \frac{1}{\sqrt{5}}(a^{n+1} - b^{n+1}), \end{aligned}$$

completing the induction proof. □

You might wonder where the formula (4.1) comes from. We see from the proof that the key property of a and b is that $a^2 = a + 1$ and $b^2 = b + 1$. In fact, the recursion relation $f_n = f_{n-1} + f_{n-2}$ leads to the quadratic equation $x^2 = x + 1$, and a and b are precisely the two roots of this equation.

Exercises.

4.4.1. Prove Theorem 4.14.

4.4.2 ([BG10, Proj. 4.26]). A sequence $(x_j)_{j=0}^{\infty}$ satisfies

$$x_1 = 1, \quad \text{and for all } m \geq n \geq 0, \quad x_{m+n} + x_{m-n} = \frac{1}{2}(x_{2m} + x_{2n}).$$

Find a formula for x_j. Prove that your formula is correct.

4.4.3 ([BG10, Prop. 4.30]). Prove that, for all $k, m \in \mathbb{N}$, where $m \geq 2$, we have

$$f_{m+k} = f_{m-1}f_k + f_m f_{k+1}.$$

4.4.4 ([BG10, Prop. 4.31]). Prove that, for all $k \in \mathbb{N}$, we have

$$f_{2k+1} = f_k^2 + f_{k+1}^2.$$

4.4.5 ([BG10, Prop. 4.32]). Prove that, for all $k, m \in \mathbb{N}$, f_{mk} is divisible by f_m.

4.4.6 ([BG10, Proj. 4.33]). How many ways are there to order the numbers $1, 2, \ldots, 20$ in a row so that the first number is 1, the last number is 20, and each pair of consecutive numbers differ by at most 2?

Chapter 5

Naive set theory

In this section we discuss some important basic concepts in set theory. Since everything in mathematics is, in some sense, built from sets, the notion of a set is fundamental.

5.1 Subsets and equality

As we mentioned before, a *set* is a collection of things, called its *elements* or *members*. We write $x \in A$ to indicate that x is a member of the set A and we write $x \notin A$ to indicate that x is not a member of the set A.

It is important to note that for each x, the only options are $x \in A$ and $x \notin A$. In particular, an object cannot be an element of a set more than once and the order of elements is irrelevant. For instance, the sets

$$\{2, 2, 3\} \qquad \text{and} \qquad \{2, 3\} \qquad \text{and} \qquad \{3, 2\}$$

are the same. They both contain the natural numbers 2 and 3 and nothing else.

In Section 2.2, we introduced the symbols $\subseteq$, $\subsetneq$, and $\not\subseteq$. In particular

$$(A \subseteq B) \qquad \text{if and only if} \qquad (x \in A \implies x \in B).$$

We will also sometimes write $B \supseteq A$ to mean $A \subseteq B$.

Proposition 5.1. *Suppose A, B, and C are sets.*

(i) $A \subseteq A$. (Set containment is reflexive.)

(ii) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$. (Set containment is transitive.)

Proof. (i) Since $x \in A \implies x \in A$ is clearly true, we have $A \subseteq A$.

(ii) Suppose $A \subseteq B$ and $B \subseteq C$. We want to show that $x \in A \implies x \in C$. Indeed, we have

$$\begin{aligned} x \in A &\implies x \in B && \text{(since } A \subseteq B\text{)} \\ &\implies x \in C. && \text{(since } B \subseteq C\text{)} \end{aligned}$$

□

We also discussed the notion of set equality in Section 2.2. In particular, the following statements are equivalent for two sets A and B:

- $A = B$.
- $x \in A \iff x \in B$.
- $A \subseteq B$ and $B \subseteq A$.

Example 5.2. Define

$$A = \{3n + 1 : n \in \mathbb{Z}\} \qquad \text{and} \qquad B = \{3m + 10 : m \in \mathbb{Z}\}.$$

We will prove that $A = B$. We do this by proving that $A \subseteq B$ and $B \subseteq A$.

First we prove that $A \subseteq B$. To do this, we need to prove that $x \in A \implies x \in B$. So suppose $x \in A$. Then there exists $n \in \mathbb{Z}$ such that $x = 3n + 1$. Thus

$$x = 3n + 1 = 3n - 9 + 10 = 3(n - 3) + 10.$$

Therefore, if we take $m = n - 3$, we have $m \in \mathbb{Z}$ and $x = 3m + 10$. So $x \in B$. This completes the proof that $x \in A \implies x \in B$, hence that $A \subseteq B$.

Next we prove that $B \subseteq A$. So we need to prove that $x \in B \implies x \in A$. So suppose $x \in B$. Then there exists $m \in \mathbb{Z}$ such that $x = 3m + 10$. Thus

$$x = 3m + 10 = 3m + 9 + 1 = 3(m + 3) + 1.$$

Therefore, if we let $n = m + 3$, we have $n \in \mathbb{Z}$ and $x = 3n + 1$. So $x \in A$. This completes the proof that $x \in B \implies x \in A$, hence that $B \subseteq A$.

Proposition 5.3. *Suppose A, B, and C are sets.*

(i) $A = A$. (Set equality is reflexive.)

(ii) If $A = B$, then $B = A$. (Set equality is symmetric.)

(iii) If $A = B$ and $B = C$, then $A = C$. (Set equality is transitive.)

Proof. The proof of this proposition is left as an exercise (Exercise 5.1.2). □

The *empty set*, denoted $\varnothing$, is the set with no elements. That is, it is the set such that $x \in \varnothing$ is never true, no matter what x is. The following proposition implies that there is only one empty set.

Proposition 5.4. *Suppose $\varnothing_1$ and $\varnothing_2$ have the property that $x \in \varnothing_1$ is never true and $x \in \varnothing_2$ is never true. Then $\varnothing_1 = \varnothing_2$.*

Proof. Assume that $\varnothing_1$ and $\varnothing_2$ have the given properties. The statement $\varnothing_1 = \varnothing_2$ is equivalent to the statement

$$x \in \varnothing_1 \iff x \in \varnothing_2$$

This is clearly true, since both sides are false for all x. □

Proposition 5.5. *The empty set is a subset of every set. That is, for every set S, we have $\varnothing \subseteq S$.*

Proof. Suppose S is a set. Then the inclusion $\varnothing \subseteq S$ is equivalent to the implication

$$x \in \varnothing \implies x \in S,$$

which is true, since the hypothesis is always false. See Remark 3.4. □

Exercises.

5.1.1 ([BG10, Proj. 5.3]). Consider the following sets:

$$\begin{aligned} A &= \{3x : x \in \mathbb{N}\}, \\ B &= \{3x + 21 : x \in \mathbb{N}\}, \\ C &= \{x + 7 : x \in \mathbb{N}\}, \\ D &= \{3x : x \in \mathbb{N} \text{ and } x > 7\}, \\ E &= \{x : x \in \mathbb{N}\}, \\ F &= \{3x - 21 : x \in \mathbb{N}\}, \\ G &= \{x : x \in \mathbb{N} \text{ and } x > 7\}. \end{aligned}$$

Determine which of the following set equalities are true. If a statement is true, prove it. If it is false, explain why the set equality does not hold. (Not all of the sets are used in this exercise. These sets will play a role in Exercise 5.2.1.)

(i) $D = E$.

(ii) $C = G$.

(iii) $D = B$.

5.1.2. Prove Proposition 5.3.

5.1.3 ([BG10, Proj. 5.5]). Are the following sets equal?

(i) $S = \{m : m \in \mathbb{N}\}$ and $T_m = \{m\}$ for a specified $m \in \mathbb{N}$.

(ii) $U = \{my : y \in \mathbb{Z},\ m \in \mathbb{N},\ my > 0\}$ and $V_m = \{my : y \in \mathbb{Z},\ my > 0\}$ for a specified $m \in \mathbb{N}$.

(iii) V_m and $W_m = \{my : y \in \mathbb{Z},\ y > 0\}$ for a specified $m \in \mathbb{N}$.

Find the simplest possible way of writing each of these sets.

5.2 Intersections and unions

The *intersection* of two sets A and B is

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

In other words,

$$(x \in A \cap B) \iff (x \in A \text{ and } x \in B).$$

If $A \cap B = \varnothing$, we say that A and B are *disjoint*.

The *union* of A and B is

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

In other words,

$$(x \in A \cup B) \iff (x \in A \text{ or } x \in B).$$

Examples 5.6. (i) $\{1, 2, 5\} \cup \{2, 8, 9\} = \{1, 2, 5, 8, 9\}$ and $\{1, 2, 5\} \cap \{2, 8, 9\} = \{2\}$.

(ii) $\{-n : n \in \mathbb{Z},\ n \geq 0\} \cup \mathbb{N} = \mathbb{Z}$.

(iii) $\{n \in \mathbb{N} : n \text{ is even }\} \cap \{n \in \mathbb{N} : n \text{ is divisible by } 4\} = \{n \in \mathbb{N} : n \text{ is divisible by } 4\}$

(iv) If $A = \{2n : n \in \mathbb{Z}\}$ and $B = \{2n + 1 : n \in \mathbb{Z}\}$, then $A \cup B = \mathbb{Z}$ and $A \cap B = \varnothing$. In particular, A and B are disjoint.

(v) $\{n \in \mathbb{Z} \colon n \geq 3\} \cap \{n \in \mathbb{Z} \colon n \text{ is even}\} = \{2n \colon n \in \mathbb{N},\ n \geq 2\}$.

If A and B are sets, then their *set difference* is

$$A - B = \{x \colon x \in A \text{ and } x \notin B\}.$$

The set difference is also sometimes written as $A \setminus B$. The *symmetric difference* of A and B is

$$A \Delta B = (A - B) \cup (B - A).$$

It is clear from the definition that $A \Delta B = B \Delta A$, which is why this is called the *symmetric* difference. (Note that $A - B$ is not equal to $B - A$ in general.)

If $A \subseteq X$, then the *complement* of A in X is $X - A$. If the larger set X is clear from the context, then we sometimes write $A^{\complement}$ for the complement of A in X. But it is important to note that the notation $A^{\complement}$ does not make sense unless we have some larger set X in mind.

Examples 5.7. (i) An integer is said to be *odd* if is it not even. Thus, the set of odd integers is the complement in $\mathbb{Z}$ of the set of even integers:

$$\mathbb{Z} - \{n \in \mathbb{Z} : n \text{ is even}\} = \{n \in \mathbb{Z} : n \text{ is odd}\}.$$

(ii) $\mathbb{Z} - \mathbb{N} = \{n \in \mathbb{Z} : n \leq 0\}$ and $\mathbb{N} - \mathbb{Z} = \varnothing$.

(iii) $\{n \in \mathbb{Z} : n \leq 0\} \Delta \{n \in \mathbb{Z} : n \geq 0\} = \{n \in \mathbb{Z} : n \neq 0\}$.

Proposition 5.8. *Suppose $A, B \subseteq X$. Then*

$$A \subseteq B \iff B^{\complement} \subseteq A^{\complement}.$$

Proof. Suppose $A \subseteq B$. Then

$$\begin{aligned} x \in B^{\complement} &\iff (x \in X) \text{ and } (x \notin B) \\ &\implies (x \in X) \text{ and } (x \notin A) \qquad \text{(since } x \in A \text{ would imply } x \in B\text{)} \\ &\implies x \in A^{\complement}. \end{aligned}$$

So $B^{\complement} \subseteq A^{\complement}$.

To prove the reverse implication, first note that, for any $Y \subseteq X$, we have $\left(Y^{\complement}\right)^{\complement} = Y$ (Exercise 5.2.3). Thus, by what we have already proved,

$$B^{\complement} \subseteq A^{\complement} \implies \left(A^{\complement}\right)^{\complement} \subseteq \left(B^{\complement}\right)^{\complement} \implies A \subseteq B. \qquad \square$$

Theorem 5.9 (De Morgan's laws)**.** *Suppose $A, B \subseteq X$.*

(i) $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$.

(ii) $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$.

Proof. We will prove (ii) and leave the proof of (i) as an exercise (Exercise 5.2.4). For $x \in X$, we have

$$\begin{aligned} x \in (A \cup B)^{\complement} &\iff \neg(x \in A \cup B) \\ &\iff \neg(x \in A \text{ or } x \in B) \\ &\iff x \notin A \text{ and } x \notin B \\ &\iff x \in A^{\complement} \text{ and } x \in B^{\complement} \\ &\iff x \in A^{\complement} \cap B^{\complement}. \end{aligned}$$

Thus $x \in (A \cup B)^{\complement} \iff x \in A^{\complement} \cap B^{\complement}$, and so $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$. $\square$

If A, B, and C are sets, we have

$$(A \cup B) \cup C = A \cup (B \cup C) \quad \text{and} \quad (A \cap B) \cap C = A \cap (B \cap C).$$

(We leave this as an exercise for you to verify.) In other words, the operations of union and intersection are associative. Therefore, as for addition (see Remark 1.29), we can unambiguously write expressions like

$$A \cup B \cup C \cup D \quad \text{and} \quad A \cap B \cap C \cap D,$$

since the result is the same no matter how we group the terms.

In fact, one can form even more arbitrary unions and intersections. If I is some set (which we think of as an index set) and, for each $i \in I$, A_i is a set. Then

$$\bigcup_{i \in I} A_i = \{x : x \in A_i \text{ for some } i \in I\} \quad \text{and} \quad \bigcap_{i \in I} A_i = \{x : x \in A_i \text{ for all } i \in I\}.$$

Example 5.10. (i) For $i \in \mathbb{Z}$, define $A_i = \{n : n \in \mathbb{Z},\ n \geq i\}$. Then

$$\bigcap_{i\in\mathbb{Z}} A_i = \varnothing, \qquad \bigcup_{i\in\mathbb{Z}} A_i = \mathbb{Z}.$$

(ii) We have

$$\bigcap_{m\in\mathbb{N}} \{n : n \in \mathbb{N},\ n \leq m\} = \{1\}, \qquad \bigcup_{m\in\mathbb{N}} \{n : n \in \mathbb{N},\ n \leq m\} = \mathbb{N}$$

A special case of the arbitrary unions and intersections defined above is when we have finitely many sets $A_1, A_2, \ldots, A_k$ for some $k \in \mathbb{N}$. Then

$$\bigcup_{i=1}^{k} A_i = \{x : x \in A_i \text{ for some } i \in \{1, 2, \ldots, k\}\} \quad \text{and}$$
$$\bigcap_{i=1}^{k} A_i = \{x : x \in A_i \text{ for all } i \in \{1, 2, \ldots, k\}\}.$$

Union and intersection are also commutative:

$$A \cup B = B \cup A \quad \text{and} \quad A \cap B = B \cap A.$$

We even have a type of distributivity for union and intersection. Our proofs of these properties will use the following logical facts: If P, Q, and R are statements, then

$$P \text{ and } (Q \text{ or } R) \iff (P \text{ and } Q) \text{ or } (P \text{ and } R)$$

and

$$P \text{ or } (Q \text{ and } R) \iff (P \text{ or } Q) \text{ and } (P \text{ or } R).$$

In other words, *and* is distributive over *or*, and *or* is distributive over *and*.

Proposition 5.11. *Suppose A, B, and C are sets. Then*

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

Proof. We have

$$\begin{aligned} x \in C \cap (A \cup B) &\iff x \in C \text{ and } x \in A \cup B \\ &\iff x \in C \text{ and } (x \in A \text{ or } x \in B) \\ &\iff (x \in C \text{ and } x \in A) \text{ or } (x \in C \text{ and } x \in B) \\ &\iff x \in C \cap A \text{ or } x \in C \cap B \\ &\iff x \in (C \cap A) \cup (C \cap B). \end{aligned}$$

□

Proposition 5.12. *Suppose A, B, and C are sets. Then*

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

Proof. We have

$$\begin{aligned} x \in C \cup (A \cap B) &\iff x \in C \text{ or } x \in A \cap B \\ &\iff x \in C \text{ or } (x \in A \text{ and } x \in B) \\ &\iff (x \in C \text{ or } x \in A) \text{ and } (x \in C \text{ or } x \in B) \\ &\iff (x \in C \cup A) \text{ and } (x \in C \cup B) \\ &\iff x \in (C \cup A) \cap (C \cup B). \end{aligned}$$

□

Proposition 5.11 says that intersection is distributive over union and Proposition 5.12 says that union is distributive over intersection.

Example 5.13. Suppose

$$A = \{1, 2, 4, 5\}, \quad B = \{2, 3, 5, 6\}, \quad C = \{4, 5, 6, 7\}.$$

Then

$$C \cup (A \cap B) = \{4, 5, 6, 7\} \cup \{2, 5\} = \{2, 4, 5, 6, 7\},$$

but

$$(C \cup A) \cap (C \cup B) = \{1, 2, 4, 5, 6, 7\} \cap \{2, 3, 4, 5, 6, 7\} = \{2, 4, 5, 6, 7\}.$$

Thus, $C \cup (A \cap B) = (C \cup A) \cap (C \cup B)$.

Exercises.

5.2.1 ([BG10, Proj. 5.11]). Consider the sets from Exercise 5.1.1. Determine which of the following set equalities are true. If a statement is true, prove it. If it is false, explain why the set equality does not hold.

(i) $A \cap E = B$.

(ii) $A \cap C = B$.

(iii) $E \cap F = A$.

5.2.2 ([BG10, Proj. 5.12]). Determine which of the following statements are true for all sets A, B, and C. If a double implication fails, determine whether one or the other of the possible implications holds. If a statement is true, prove it. If it is false, provide a counterexample.

(i) $C \subseteq A$ and $C \subseteq B \iff C \subseteq (A \cup B)$.

(ii) $C \subseteq A$ or $C \subseteq B \iff C \subseteq (A \cup B)$.

(iii) $C \subseteq A$ and $C \subseteq B \iff C \subseteq (A \cap B)$.

(iv) $C \subseteq A$ or $C \subseteq B \iff C \subseteq (A \cap B)$.

5.2.3. Suppose $Y \subseteq X$. Prove that $\left(Y^{\complement}\right)^{\complement} = Y$

5.2.4. Prove Theorem 5.9(i).

5.2.5 ([BG10, Proj. 5.16]). For each of the following assertions, prove it is true for all sets A, B, and C, or provide a counterexample.

(i) $A - (B \cup C) = (A - B) \cup (A - C)$.

(ii) $A \cap (B - C) = (A \cap B) - (A \cap C)$.

5.3 Cartesian products

Suppose A and B are sets. We define a new set

$$A \times B := \{(a, b) \colon a \in A,\ b \in B\},$$

called the *Cartesian product* of A and B. We call (a, b) an *ordered pair*. Note that (a, b) is *not* the same as the set $\{a, b\}$. In a set, the order of elements is not relevant, so $\{a, b\} = \{b, a\}$ for all a and b. However, equality of ordered pairs is given by

$$(a, b) = (c, d) \iff a = c \text{ and } b = d.$$

Thus $(a, b) = (b, a)$ if and only if $a = b$.

Example 5.14. If $A = \{1, 2\}$ and $B = \{2, 3\}$, then

$$A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3)\}.$$

Example 5.15. The Cartesian product $\mathbb{N} \times \mathbb{N}$ is the set of all ordered pairs of natural numbers. For example, $(3, 5) \in \mathbb{N} \times \mathbb{N}$.

Example 5.16. We will learn about the set $\mathbb{R}$ of real numbers in Section 7. Then $\mathbb{R} \times \mathbb{R}$ is the *Cartesian plane* you have likely seen in previous math courses.

Proposition 5.17. *If A and B are nonempty sets such that $A \neq B$, then $A \times B \neq B \times A$.*

Proof. Suppose A and B are nonempty sets, with $A \neq B$. Then either $A \not\subseteq B$ or $B \not\subseteq A$. Suppose $A \not\subseteq B$. Then there exists an element $a \in A$ such that $a \notin B$. Since B is not empty, there exists some $b \in B$. Then $(a, b) \in A \times B$, but $(a, b) \notin B \times A$, since $a \notin B$. The case where $B \not\subseteq A$ is analogous. □

Remark 5.18. Note $\varnothing \times A = \varnothing = A \times \varnothing$, for any set A. This is why we needed the hypothesis that A and B are nonempty in Proposition 5.17.

Proposition 5.19. *Let A, B, and C be sets.*

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

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

Proof. We will prove part (i) and leave the proof of part (ii) as an exercise (Exercise 5.3.1). We have

$$\begin{aligned}(x,y) \in A \times (B \cup C) &\iff x \in A \text{ and } y \in (B \cup C)\\ &\iff x \in A \text{ and } (y \in B \text{ or } y \in C)\\ &\iff (x \in A \text{ and } y \in B) \text{ or } (x \in A \text{ and } y \in C)\\ &\iff (x,y) \in A \times B \text{ or } (x,y) \in A \times C\\ &\iff (x,y) \in (A \times B) \cup (A \times C).\end{aligned}$$

□

Exercises.

5.3.1. Prove Proposition 5.19(ii).

5.3.2 ([BG10, Proj. 5.21]). For each of the following statements, prove that it is true for all sets A, B, C, and D, or give a counterexample.

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

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

5.4 Functions

We now turn our attention to the important concept of a function. You have all seen functions in previous math classes. You probably thought of a function in the following way. A function consists of

- a set A called the *domain* of the function;
- a set B called the *codomain* of the function;
- a "rule" f that "assigns" to each $a \in A$ an element $f(a) \in B$.

We denote such a function $f\colon A \to B$.

Example 5.20. Consider the function $f\colon \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = n^2 + 2$ for all $n \in \mathbb{Z}$. The domain of f is $\mathbb{Z}$ and the codomain is also $\mathbb{Z}$. Note that, while f must assign some element of the codomain to every element of the domain, it is *not* the case that every element of the codomain is equal to $f(n)$ for some element n of the domain. For instance, for the above function f, there is no $n \in \mathbb{Z}$ such that $f(n) = -1$. The functions

- $f\colon \mathbb{Z} \to \mathbb{Z}$, $f(n) = n^2 + 2$ for all $n \in \mathbb{Z}$, and
- $f\colon \mathbb{Z} \to \mathbb{N}$, $f(n) = n^2 + 2$ for all $n \in \mathbb{Z}$,

are *different* functions, even though their domains are equal and the "rule" is the same. The domain and the codomain are part of the function. So if two functions have different codomains, they are different functions.

Example 5.21. Every sequence $(x_j)_{j=1}^{\infty}$ is really a function with domain $\mathbb{N}$, where we have just written x_j instead of $f(j)$.

The above definition of a function is rather vague. In particular what do the words "rule" and "assign" mean? To give a more precise definition of a function, we think of it in terms of its graph. The *graph* of $f\colon A \to B$ is

$$\Gamma(f) = \{(a,b) \in A \times B : b = f(a)\} = \{(a, f(a)) : a \in A\} \subseteq A \times B.$$

If you think about the way you have drawn graphs (say, in calculus), you can convince yourself that this definition corresponds to what you have seen before.

Definition 5.22 (Function)**.** A *function* with *domain* A and *codomain* B is a subset Γ of $A \times B$ such that for each $a \in A$, there is one and only one $b \in B$, such that $(a,b) \in \Gamma$. If $(a,b) \in \Gamma$, we write $b = f(a)$.

Remark 5.23. If you think about our precise definition of a function (Definition 5.22), it corresponds to what you might have called the "vertical line test" for functions in calculus.

Example 5.24. A binary operation on a set A is a function $f\colon A \times A \to A$. For example, addition is a binary operation on $\mathbb{Z}$. So it is a function plus$\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. However, we usually write $m + n$ instead of plus(m,n).

Exercises.

5.4.1. Which of the following are functions?

(i) $\{(a, a^2) : a \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$

(ii) $\{(a, a^2) : a \in \mathbb{N}\} \subseteq \mathbb{N} \times \mathbb{N}$

(iii) $\{(a^2, a) : a \in \mathbb{Z}\} \subseteq \{n^2 : n \in \mathbb{Z}\} \times \mathbb{Z}$

(iv) $\{(a^2, a) : a \in \mathbb{N}\} \subseteq \{n^2 : n \in \mathbb{N}\} \times \mathbb{N}$.

5.5 Russell's paradox and axiomatic set theory

You may wonder why this chapter of the notes is called *naive* set theory. It is because we have implicitly assumed that, given any property P, we can define a set

$$\{x : x \text{ has property } P\}.$$

However, this leads to problems. Consider the set

$$R = \{x : x \text{ is a set and } x \notin x\}.$$

Then we ask the question

$$\text{is } R \in R?$$

Well, if $R \in R$, then $R \notin R$ is false, and so, by the definition of R, we have $R \notin R$. On the other hand, if $R \notin R$, then, by the definition of R, we have $R \in R$. Thus, we see that

$$R \in R \iff R \notin R.$$

This is a contradiction known as *Russell's paradox*.

It is possible to fix Russell's paradox. The fix involves reworking our concept of a set and starting from a very specific list of axioms about what we are and are not allowed to do with sets. This is called *axiomatic set theory*, and is beyond the scope of this course. The canonical axiomatic set theory is called *ZFC*, named after Ernst Zermelo, Abraham Fraenkel, and the Axiom of Choice.

In this course, the problems related to Russell's paradox are not an issue. All of the sets that we discuss can be shown to exist in ZFC. Thus, we will remain "naive" and ignore this issue.

Chapter 6

Equivalence relations and modular arithmetic

In this chapter we discuss the concept of a relation and, in particular, of an equivalence relation, a concept that is ubiquitous in mathematics. We then turn our attention to a particular family of equivalence relations that give rise to *modular arithmetic*.

6.1 Equivalence relations

Definition 6.1 (Relation)**.** A *relation* on a set A is a subset of $A \times A$. If $R \subseteq A \times A$ is a relation on A, we usually write xRy to indicate that $(x, y) \in R$ and we say that x *is related to* y by the relation R. So

$$xRy \iff (x, y) \in R.$$

We often use other symbols instead of R, such as $\sim, \approx, \equiv, <, \leq, >, \geq, \prec, \succ$, etc.

Example 6.2. Some examples of relations on $\mathbb{Z}$ are:

- equality ($=$),
- less than ($<$),
- less than or equal to ($\leq$),
- divides (i.e. a divides b).

For example, formally speaking, the relation $\leq$ is the subset of $\mathbb{Z} \times \mathbb{Z}$ given by

$$\{(a, b) : b - a \in \mathbb{N} \text{ or } a = b\}.$$

Example 6.3. The graph $\Gamma(f)$ of a function $f\colon A \to A$ is a special case of a relation, for which there is exactly one $(x, y) \in \Gamma(f)$ for each $x \in A$.

Definition 6.4 (Equivalence relation, equivalence class)**.** A relation $\sim$ on a set A is an *equivalence relation* if it has the following three properties:

- $a \sim a$ for all $a \in A$. (*Reflexivity*)
- If $a \sim b$, then $b \sim a$. (*Symmetry*)
- If $a \sim b$ and $b \sim c$, then $a \sim c$. (*Transitivity*)

If $\sim$ is an equivalence relation on A, then the *equivalence class* of $a \in A$ is

$$[a] := \{b \in A : b \sim a\}.$$

Sometimes, when we wish to emphasize the particular equivalence relation (for instance, when we are working with more than one), we write $[a]_\sim$ instead of $[a]$.

Examples 6.5. (i) The relation $=$ on $\mathbb{Z}$ is an equivalence relation.

(ii) The relation $\leq$ on $\mathbb{Z}$ is not an equivalence relation, since it is not symmetric (e.g. $1 \leq 2$, but $2 \not\leq 1$).

(iii) The relation $=$ on subsets of $\mathbb{Z}$ (i.e. set equality) is an equivalence relation.

(iv) The relation $\subseteq$ on subsets of $\mathbb{Z}$ is not an equivalence relation since it is not symmetric.

Note that, in (iii) and (iv), the relation is on the set

$$A = \{X : X \subseteq \mathbb{Z}\}$$

of subsets of $\mathbb{Z}$

Proposition 6.6. *Suppose $\sim$ is an equivalence relation on a set A, and $a, b \in A$. Then*

(i) $a \in [a]$, and

(ii) $a \sim b \iff [a] = [b]$.

Proof. (i) Since $\sim$ is an equivalence relation, it is reflexive. Thus $a \sim a$. So $a \in [a]$.

(ii) Suppose $a \sim b$. We will prove that $[a] = [b]$ by showing the two inclusions $[a] \subseteq [b]$ and $[b] \subseteq [a]$.

Suppose $c \in [a]$. Then $c \sim a$. Thus, by transitivity of $\sim$, we have $c \sim b$, and so $c \in [b]$. Therefore, $[a] \subseteq [b]$.

Now suppose $c \in [b]$. Then $c \sim b$. By symmetry of $\sim$, we then have $b \sim a$ (since $a \sim b$). Then, by transitivity of $\sim$, we have $c \sim a$, and so $c \in [a]$. Therefore, $[b] \subseteq [a]$.

Conversely, suppose $[a] = [b]$. By part (i), we have $a \in [a] = [b]$, so $a \in [b]$. Hence $a \sim b$. □

We say that a is a *representative* of the equivalence class $[a]$. Representatives of a given equivalence class are not unique in general. By Proposition 6.6(ii), b is a representative of the equivalence class $[a]$ if and only if $a \sim b$ (which is equivalent to $b \in [a]$).

Proposition 6.6 implies that for each $a \in A$, there is a unique equivalence class (namely $[a]$) containing a. In fact, the equivalence classes of an equivalence relation on A subdivide the set A in a certain sense, as we shall now explain.

Proposition 6.7. *Suppose $\sim$ is an equivalence relation on a set A. Then, for all $a, b \in A$, we have*

$$[a] = [b] \quad \text{or} \quad [a] \cap [b] = \varnothing.$$

Proof. Suppose $a, b \in A$. If $[a] \cap [b] = \varnothing$, we are done. So assume $[a] \cap [b] \neq \varnothing$. Then there exists an element $c \in [a] \cap [b]$. Thus, $a \sim c \sim b$, which implies that $a \sim b$. Therefore, by Proposition 6.6(ii), we have $[a] = [b]$. □

Definition 6.8 (Partition)**.** A *partition* of a set A is a set Π, whose elements are nonempty subsets of A such that

- $P_1, P_2 \in \Pi,\ P_1 \neq P_2 \implies P_1 \cap P_2 = \varnothing$, and
- every $a \in A$ belongs to some $P \in \Pi$.

Equivalently, a set Π of nonempty subsets of A is a partition of A if every element of A belongs to a unique element of Π.

Intuitively, a partition of a set A is a subdivision of A into disjoint subsets.

Example 6.9. Let P_1 be the set of even integers and let P_2 be the set of odd integers. Then $\Pi = \{P_1, P_2\}$ is a partition of $\mathbb{Z}$.

The next proposition says that equivalence relations and partitions are two ways of viewing the same idea.

Proposition 6.10. *(i) Suppose $\sim$ is an equivalence relation on A. Then the set Π of equivalence classes of $\sim$ is partition of A.*

(ii) Suppose Π is a partition of A. Then the relation $\sim$ defined by

$$a \sim b \iff a \text{ and } b \text{ lie in the same element of } \Pi$$

is an equivalence relation on A.

Proof. Part (i) is Proposition 6.6(i) and Proposition 6.7. To prove part (ii), let Π be a partition of A. Define a relation $\sim$ on A by

$$a \sim b \iff a \text{ and } b \text{ lie in the same element of } \Pi.$$

Reflexivity: Suppose $a \in A$. Then $a \in P$ for some $P \in \Pi$. Thus $a \sim a$.

Symmetry: Suppose $a, b \in A$ and $a \sim b$. Then a and b lie in the same element of Π. Thus we also have $b \sim a$.

Transitivity: Suppose $a, b, c \in A$, $a \sim b$, and $b \sim c$. Then a and b lie in some $P \in \Pi$. Also, b and c lie in some $P' \in \Pi$. Since b can only lie in one element of Π, we have $P = P'$. Hence a and c both lie in P, so that $a \sim c$. □

The *absolute value* of an integer x is defined to be

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

Example 6.11. Consider the relation on $\mathbb{Z}$ defined by

$$x \sim y \iff |x| = |y|.$$

- *Reflexivity*: For all $x \in \mathbb{Z}$, $|x| = |x|$, so $x \sim x$.
- *Symmetry*: For all $x, y \in \mathbb{Z}$,

$$x \sim y \implies |x| = |y| \implies |y| = |x| \implies y \sim x.$$

- *Transitivity*: For $x, y, z \in \mathbb{Z}$,

$$x \sim y \text{ and } y \sim z \implies |x| = |y| = |z| \implies x \sim z.$$

Thus $\sim$ is an equivalence relation. The equivalence class of $x \in \mathbb{Z}$ is the set $\{x, -x\}$. The set

$$\Pi = \{\{x, -x\} : x \in \mathbb{Z}\}$$

is a partition of $\mathbb{Z}$.

Example 6.12. Consider the relation on $\mathbb{Z} \times \mathbb{Z}$ defined by

$$(x, y) \sim (v, w) \iff 2x - 3y = 2v - 3w.$$

- *Reflexivity*: For all $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, we have $2x - 3y = 2x - 3y$, so $(x, y) \sim (x, y)$.
- *Symmetry*: $(x, y) \sim (v, w) \implies 2x - 3y = 2v - 3w \implies 2v - 3w = 2x - 3y \implies (v, w) \sim (x, y)$.
- *Transitivity*: Suppose $(x, y) \sim (v, w)$ and $(v, w) \sim (u, z)$. Then $2x - 3y = 2v - 3w$ and $2v - 3w = 2u - 3z$. Hence $2x - 3y = 2u - 3z$, and so $(x, y) \sim (u, z)$.

Thus $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}$. The equivalence classes are sets

$$\{(x, y) \in \mathbb{Z} \times \mathbb{Z} : 2x - 3y = n\}, \quad n \in \mathbb{Z}.$$

That is, they are the points with integer coordinates that lie on a fixed line $2x - 3y = n$ in the plane.

Exercises.

6.1.1 ([BG10, Proj. 6.7]). For each of the following relations defined on $\mathbb{Z}$, determine whether it is an equivalence relation. If it is, determine the equivalence classes.

(i) $x \sim y$ if $x < y$.

(ii) $x \sim y$ if $x \leq y$.

(iii) $x \sim y$ if $|x| = |y|$.

(iv) $x \sim y$ if $x \neq y$.

(v) $x \sim y$ if $xy > 0$.

(vi) $x \sim y$ if ($x|y$ or $y|x$).

6.1.2 ([BG10, Proj. 6.8]). Prove that each of the following relations defined on $\mathbb{Z} \times \mathbb{Z}$ is an equivalence relation. Determine the equivalence classes for each relation.

(i) $(x, y) \sim (v, w)$ if $x^2 + y^2 = v^2 + w^2$.

(ii) $(x, y) \sim (v, w)$ if $y - x^2 = w - v^2$.

(iii) $(x, y) \sim (v, w)$ if $xy = vw$.

(iv) $(x, y) \sim (v, w)$ if $x + 2y = v + 2w$.

6.1.3 ([BG10, Proj. 6.9]). On $\mathbb{Z} \times (\mathbb{Z} - \{0\})$ we define the relation $(m_1, n_1) \sim (m_2, n_2)$ if $m_1 n_2 = n_1 m_2$.

(i) Show that this is an equivalence relation.

(ii) For two equivalence classes $[(m_1, n_1)]$ and $[(m_2, n_2)]$, we define two binary operations $\oplus$ and $\odot$ via

$$[(m_1, n_1)] \oplus [(m_2, n_2)] = [(m_1 n_2 + m_2 n_1, n_1 n_2)]$$

and

$$[(m_1, n_1)] \odot [(m_2, n_2)] = [(m_1 m_2, n_1 n_2)].$$

What properties do the binary operations have? For example, which axioms of the integers are satisfied?

6.2 The division algorithm

In Section 6.3, we will discuss an important equivalence relation. We first need a theorem about division of integers.

Theorem 6.13 (The Division Algorithm)**.** *Suppose $n \in \mathbb{N}$. For every $m \in \mathbb{Z}$, there exist unique $q, r \in \mathbb{Z}$ such that*

$$m = qn + r \quad \textit{and} \quad 0 \leq r \leq n - 1.$$

The integer q is called the quotient *and r is called the* remainder *upon division of m by n.*

Proof. Fix $n \in \mathbb{N}$. Let us first prove the existence part of the theorem. We first consider the $m \geq 0$ case by induction. For the base case $m = 0$, we can set $q = r = 0$.

For the induction step, assume there exist $q, r \in \mathbb{Z}$ such that

$$m = qn + r \qquad \text{and} \qquad 0 \leq r \leq n - 1.$$

Case 1: $r < n - 1$. Then set $q' = q$ and $r' = r + 1$, so that

$$m + 1 = q'n + r' \qquad \text{and} \qquad 0 \leq r' \leq n - 1.$$

Case 2: $r = n - 1$. Then set $q' = q + 1$ and $r' = 0$, so that

$$m + 1 = qn + r + 1 = (q + 1)n = q'n + r' \qquad \text{and} \qquad 0 \leq r' \leq n - 1.$$

In both cases, we found integers q' and r' with the required properties, completing the proof of the induction step.

Now consider the case $m < 0$. Since $-m > 0$ we can find, by the first part of our proof, integers q and r such that

$$-m = qn + r \qquad \text{and} \qquad 0 \leq r \leq n - 1.$$

Case 1: $r = 0$. Then $m = (-q)n + 0$ is the required expression for m.

Case 2: $r > 0$. Then

$$m = -qn - r = (-q - 1)n + (n - r)$$

is the required expression, since $0 < n - r < n$.

It remains to prove the uniqueness part of the theorem. Suppose that $m \in \mathbb{Z}$ and

$$q_1 n + r_1 = m = q_2 n + r_2 \quad \text{for some } q_1, q_2, r_1, r_2 \in \mathbb{Z},\ 0 \leq r_1, r_2 \leq n - 1.$$

Then we have

$$(q_1 - q_2)n = r_2 - r_1. \tag{6.1}$$

Thus, $r_2 - r_1$ is divisible by n. But since $0 \leq r_1, r_2 \leq n - 1$, we have

$$1 - n \leq r_2 - r_1 \leq n - 1.$$

Since the only multiple of n between $1 - n$ and $n - 1$ is 0, we have $r_2 - r_1 = 0$, so that $r_1 = r_2$. Then (6.1) implies that $q_1 = q_2$ as well. □

Examples 6.14. (i) For $n = 3$ and $m = 11$, we obtain $q = 3$ and $r = 2$ since $11 = 3 \cdot 3 + 2$.

(ii) For $n = 5$ and $m = -26$, we obtain $q = -6$ and $r = 4$ since $-26 = (-6) \cdot 5 + 4$.

Exercises.

6.2.1. Prove the following statements.

(i) An integer $m \in \mathbb{Z}$ is odd if and only if there exists $q \in \mathbb{Z}$ such that $m = 2q + 1$.

(ii) For every $n \in \mathbb{Z}$, n is even or $n + 1$ is even.

(iii) An integer $m \in \mathbb{Z}$ is even if and only if m^2 is even.

6.3 The integers modulo n

In this section, we discuss an important, and frequently encountered, concept in mathematics: the integers modulo n.

For a fixed $n \in \mathbb{N}$, we define a relation $\equiv$ on $\mathbb{Z}$ by

$$x \equiv y \iff x - y \text{ is divisible by } n.$$

The natural number n is called the *modulus*. When we wish to make the modulus explicit, we write

$$x \equiv y \mod n.$$

If $x \equiv y \mod n$, we say that x and y are *equivalent modulo n* or *congruent modulo n* (or sometimes simply *equivalent/congruent mod n*). Note that $x \equiv y \mod 1$ for all $x, y \in \mathbb{Z}$, and so equivalence modulo 1 is not so interesting. For this reason, we usually assume $n \geq 2$.

Example 6.15. Suppose $n = 2$. Then $x \equiv y \mod 2$ if and only if $x - y$ is even, i.e. x and y are either both even or both odd. In this case, we say that x and y have the same *parity*.

Example 6.16. Fix the modulus 7. Then $2 \equiv 16$, since $2 - 16 = -14$ is divisible by 7. Similarly, we have

$$0 \equiv -7 \equiv 7 \equiv 14, \quad 1 \equiv -6 \equiv 8 \equiv 701, \quad 5 \equiv 7005.$$

Example 6.17. Suppose $n \in \mathbb{N}$ and $m \in \mathbb{Z}$. By the Division Algorithm (Theorem 6.13), we have

$$m = qn + r \quad \text{for some } q, r \in \mathbb{Z},\ 0 \leq r \leq n - 1.$$

Then $m - r = qn$ is divisible by n, and so $m \equiv r \mod n$.

Proposition 6.18. *Fix a modulus $n \in \mathbb{N}$.*

(i) Equivalence modulo n (i.e. $\equiv$) is an equivalence relation.

(ii) The equivalence relation $\equiv$ has exactly n distinct equivalence classes, namely

$$[0], [1], \ldots, [n - 1].$$

Proof. To prove (i), we need to check that $\equiv$ is reflexive, symmetric, and transitive.

Reflexivity: For $a \in \mathbb{Z}$, we have $a - a = 0$, which is divisible by n, hence $a \equiv a$.

Symmetry: Suppose $a \equiv b$. Then n divides $a-b$. So there exists $j \in \mathbb{Z}$, such that $a-b = jn$. Then $b - a = -jn = (-j)n$ is also divisible by n, and so $b \equiv a$.

Transitivity: Suppose $a \equiv b$ and $b \equiv c$. Then n divides both $a - b$ and $b - c$. So there exist $j, k \in \mathbb{Z}$ such that

$$a - b = jn \quad \text{and} \quad b - c = kn.$$

Then

$$a - c = (a - b) + (b - c) = jn + kn = (j + k)n$$

is divisible by n, hence $a \equiv c$.

To prove (ii), we need to show that the equivalence classes $[0], [1], \ldots, [n-1]$ are distinct, and that every integer lies in one of them.

If $m \in \mathbb{Z}$, then Example 6.17 shows that $m \in [r]$ for some $0 \leq r \leq n-1$. So every integer lies in one of the given classes.

It remains to show that the given equivalence classes are distinct. So suppose $0 \leq m, k \leq n - 1$ and $[m] = [k]$ (i.e. n divides $m - k$). We want to show that this implies $m = k$. Now,

$$0 \leq m, k \leq n - 1 \implies -n + 1 \leq m - k \leq n - 1,$$

and the only number between $-n + 1$ and $n - 1$ divisible by n is 0. Thus $m - k = 0$, and hence $m = k$, as desired. □

The set of equivalence classes for the relation of equivalence modulo n is called the *set of integers modulo* n, and is denoted by $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$.

Example 6.19. We have

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}.$$

Example 6.20. By Proposition 6.18, for any integer a, its equivalence class modulo n is equal to one of the classes

$$[0], [1], \ldots, [n - 1].$$

Example 6.17 tells us how to find out which one: we have $[a] = [r]$, where r is the remainder upon division of a by n. For example, if $n = 5$, then we have

$$31 = 6 \cdot 5 + 1,$$

and so $[31] = [1]$. Similarly,

$$[26] = [1], \quad [-1] = [4], \quad [12] = [2], \quad [35] = [0].$$

(The basic idea is that we add or subtract multiples of n until the representative lies in the range $0, 1, \ldots, n - 1$.) If $n = 3$, we have

$$[-2] = [1], \quad [33] = [0], \quad [20] = [2].$$

Proposition 6.21. *Fix a modulus $n \in \mathbb{N}$. If $a \equiv a'$ and $b \equiv b'$, then*

$$a + b \equiv a' + b' \quad \textit{and} \quad ab \equiv a'b'.$$

Proof. Fix a modulus n. Suppose $a \equiv a'$ and $b \equiv b'$. Then there exist $k, \ell \in \mathbb{Z}$ such that

$$a - a' = kn \quad \text{and} \quad b - b' = \ell n.$$

Then

$$(a + b) - (a' + b') = (a - a') + (b - b') = kn + \ell n = (k + \ell)n,$$

and so $a + b \equiv a' + b'$. Furthermore,

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b' = a\ell n + knb' = (a\ell + kb')n,$$

and so $ab \equiv a'b'$. □

The above proposition allows us to define two operations on $\mathbb{Z}_n$. Namely, we define *addition* $\oplus$ and *multiplication* $\odot$ on $\mathbb{Z}_n$ by

$$[a] \oplus [b] = [a + b] \quad \text{and} \quad [a] \odot [b] = [ab].$$

Remark 6.22. It is important that you understand *why* we needed Proposition 6.21 in order to be able to define the above operations. Remember that $[a] = [a'] \iff a \equiv a'$ and $[b] = [b'] \iff b \equiv b'$ (by Proposition 6.6(ii)). Our definition of $\oplus$ then says that the sum of the classes $[a] = [a']$ and $[b] = [b']$ is

$$[a] \oplus [b] = [a + b]$$

and *also* that it is

$$[a'] \oplus [b'] = [a' + b'].$$

So if it is not true that $[a + b] = [a' + b']$, then the operation $\oplus$ is not well defined, since we are defining it to be two different things (i.e. there is a conflict in our definition). Luckily, Proposition 6.21 tells us precisely that $[a + b] = [a' + b']$.

To further illustrate this point, suppose we tried to define a function

$$f \colon \mathbb{Z}_5 \to \mathbb{Z}, \quad f([n]) = n.$$

Then, since $[1] = [6]$, we should have $f([1]) = f([6])$. But $f([1]) = 1 \neq 6 = f([6])$. So, in fact, this function is *not* well-defined.

Remark 6.23. Many texts simply reuse the notation $+$ and $\cdot$ for addition and multiplication in $\mathbb{Z}_n$. (In fact, this is the most common convention.) We use the notation $\oplus$ and $\odot$ to make it explicit that these are operations on a different set ($\mathbb{Z}_n$ as opposed to $\mathbb{Z}$).

Example 6.24. Fix a modulus $n \in \mathbb{N}$. By Proposition 6.18(ii), for every $a \in \mathbb{Z}$, the equivalence class $[a]$ must be equal to one of the classes $[0], [1], \ldots, [n-1]$. When doing computations in modular arithmetic, we usually write our final answer in this form. (See Example 6.20.) For example,

(i) If $n = 4$, we have $[3] \oplus [2] = [3 + 2] = [5] = [1]$.

(ii) If $n = 5$, we have $[4] \odot [3] = [4 \cdot 3] = [12] = [2]$.

(iii) If $n = 2$, then

$$[235] \odot [35423] \odot [24] = [1] \odot [1] \odot [0] = [1 \cdot 1 \cdot 0] = [0].$$

Proposition 6.25. *Fix an integer $n \geq 2$. Addition and multiplication in $\mathbb{Z}_n$ are commutative, associative, and distributive. Also, the set $\mathbb{Z}_n$ has an additive identity $[0]$, a multiplicative identity $[1]$, and additive inverses (the additive inverse of $[a]$ being $[-a]$). In other words, Axioms 1.1–1.4 hold with $\mathbb{Z}$ replaced everywhere by $\mathbb{Z}_n$.*

Proof. We will prove three of these statements, and leave the rest as exercises.

Addition in $\mathbb{Z}_n$ is commutative: Choose two arbitrary elements $[a], [b] \in \mathbb{Z}_n$. Then we have

$$\begin{aligned} [a] \oplus [b] &= [a + b] && \text{by the definition of } \oplus \\ &= [b + a] && \text{commutativity of addition in } \mathbb{Z} \\ &= [b] \oplus [a]. && \text{by the definition of } \oplus \end{aligned}$$

Thus addition in $\mathbb{Z}_n$ is commutative.

Multiplication is distributive over addition in $\mathbb{Z}_n$: Choose three arbitrary elements $[a], [b], [c] \in \mathbb{Z}_n$. Then we have

$$\begin{aligned} [a] \odot ([b] \oplus [c]) &= [a] \odot [b + c] && \text{by the definition of } \oplus \\ &= [a(b + c)] && \text{by the definition of } \odot \\ &= [ab + ac] && \text{distributivity in } \mathbb{Z} \\ &= [ab] \oplus [ac] && \text{by the definition of } \oplus \\ &= [a] \odot [b] \oplus [a] \odot [c]. && \text{by the definition of } \odot \end{aligned}$$

Thus distributivity holds in $\mathbb{Z}_n$.

The element $[0] \in \mathbb{Z}_n$ is an additive identity: Choose an arbitrary element $[a] \in \mathbb{Z}_n$. Then we have

$$\begin{aligned} [a] \oplus [0] &= [a + 0] && \text{by the definition of } \oplus \\ &= [a]. && \text{since 0 is an additive identity for } \mathbb{Z} \end{aligned}$$

Thus, for all $[a] \in \mathbb{Z}_n$, we have $[a] \oplus [0] = [a]$. So $[0]$ is an additive identity for $\mathbb{Z}_n$.

The remaining statements are left as an exercise (Exercise 6.3.3). □

Exercises.

6.3.1. Perform the following computations in $\mathbb{Z}_n$ for the given value of n. In each case, write your final answer in the standard form: $[0], [1], [2], \ldots, [n-1]$. You should not have to use a calculator.

(i) $[3] \oplus [4]$, $n = 5$.

(ii) $[0] \oplus [4]$, $n = 8$.

(iii) $[3667] \oplus [6991]$, $n = 3$.

(iv) $[2] \odot [3]$, $n = 6$.

(v) $[2] \odot [3]$, $n = 5$.

(vi) $[5] \odot [6]$, $n = 7$.

(vii) $[503259] \odot [32485]$, $n = 2$.

6.3.2. For each of the following questions, write your answer in the standard form: $[0], [1], [2], \ldots, [n-1]$, where n is the modulus.

(i) What is the additive inverse of $[3]$ in $\mathbb{Z}_7$?

(ii) What is the additive inverse of $[3]$ in $\mathbb{Z}_6$?

(iii) What is the additive inverse of $[5]$ in $\mathbb{Z}_{21}$?

(iv) Is there an element $[a]$ of $\mathbb{Z}_7$ such that $[a] \odot [3] = [1]$? If so, find it. If not, prove that no such element exists.

(v) Is there an element $[a]$ of $\mathbb{Z}_{12}$ such that $[a] \odot [3] = [1]$? If so, find it. If not, prove that no such element exists.

6.3.3. Complete the proof of Proposition 6.25.

6.3.4. Fix a modulus n. Suppose $a, b \in \mathbb{Z}$ satisfy $0 < b < n$ and $[a] \odot [b] = [0]$. Prove that $[a]$ cannot have a multiplicative inverse. In other words, show that there is no $[c] \in \mathbb{Z}_n$ such that $[c] \odot [a] = [1]$.

6.3.5. Prove that there are no integers x, y, z such that

$$9x^6 + 13y^5 + 4y^2 + 3z^6 = 0 \quad \text{and} \quad -6x^4 - 2y^5 + y^2 - 3z^8 = 1.$$

Hint: Prove the result by contradiction. Assume the equations have a solution and then do some computations modulo 3 to arrive at a contradiction.

6.3.6. (i) Without using induction, prove that the following statement is true:

$$\forall\, a \in \mathbb{Z} \ \left(a^2 \text{ is divisible by 4 or } a^2+3 \text{ is divisible by 4}\right).$$

Hint: Use modular arithmetic.

(ii) Is the statement

$$\left(\forall\, a \in \mathbb{Z},\ a^2 \text{ is divisible by 4}\right) \text{ or } \left(\forall\, a \in \mathbb{Z},\ a^2+3 \text{ is divisible by 4}\right)$$

true? Justify your answer.

6.4 Prime numbers

Definition 6.26 (Prime number, composite number, factor)**.** An integer $n \geq 2$ is *prime* if it is divisible only by ± 1 and $\pm n$. If an integer $n \geq 2$ is not prime, it is *composite*. If $n = q_1 q_2 \cdots q_k$ for some $q_1, q_2, \ldots, q_k \in \mathbb{Z}$, then the $q_1, q_2, \ldots, q_k$ are called *factors* of n, and the expression $n = q_1 q_2 \cdots q_k$ is called a *factorization* of n.

Proposition 6.27. *Every integer $n \geq 2$ can be factored into primes.*

Proof. We prove the result by induction on n. The base case is when $n = 2$, which is already prime.

For the induction step, assume that $n \geq 3$ and that any integer less than n (and ≥ 2) can be factored into primes. If n is prime, we are done. Otherwise, there exist $a, b \in \mathbb{N}$, $a, b \geq 2$, such that $n = ab$. Then $a, b < n$ and so, by the induction hypothesis, a and b can each be written as a product of primes. This gives a prime factorization of n. □

Proposition 6.28. *There are infinitely many prime numbers.*

Proof. We prove the result by contradiction. Suppose there are finitely many primes $p_1, p_2, \ldots, p_n$. Then consider the number

$$q = p_1 p_2 \cdots p_n + 1.$$

The remainder upon division of q by p_i is 1, for all $1 \leq i \leq n$. Thus, q is not divisible by any prime number. Therefore q does not have a prime factorization, contradicting Proposition 6.27. □

Recall, from Definition 2.36 that, for $m, n \in \mathbb{Z}$, not both zero, we define $\gcd(m, n)$ to be the smallest element of the set

$$S = \{k \in \mathbb{N} : k = mx + ny \text{ for some } x, y \in \mathbb{Z}\}.$$

When $m = n = 0$, the set S is empty, in which case we define $\gcd(0, 0) = 0$.

Proposition 6.29. *Suppose $m, n \in \mathbb{Z}$.*

(i) $\gcd(m, n)$ *divides both m and n.*

(ii) If m and n are not both zero, then $\gcd(m,n) > 0$.

(iii) Every integer that divides both m and n also divides $\gcd(m,n)$.

Proof. The proof of this proposition can be found in [BG10, Prop. 6.29]. □

Propositions 6.29 and 2.24 imply that $\gcd(m,n)$ is the largest integer that divides both m and n. Thus $\gcd(m,n)$ is the *greatest common divisor* of m and n, justifying the notation.

Proposition 6.30. *For all $k, m, n \in \mathbb{Z}$, we have*

$$\gcd(km, kn) = |k| \gcd(m,n).$$

Proof. If $k = 0$, then

$$\gcd(km, kn) = \gcd(0,0) = 0 = 0 \gcd(m,n).$$

Now assume $k \neq 0$. Let

$$S = \{j \in \mathbb{N} : j = mx + ny \text{ for some } x, y \in \mathbb{Z}\}$$

and

$$T = \{j \in \mathbb{N} : j = kmx + kny \text{ for some } x, y \in \mathbb{Z}\}.$$

Set $g = \gcd(m,n)$ and $h = \gcd(km, kn)$. So g is the smallest element of S and h is the smallest element of T. Our goal is to prove that $|k|g = h$.

Since $g \in S$, there exist integers x_1 and y_1 such that $g = mx_1 + ny_1$. Therefore,

$$|k|g = m(|k|x_1) + n(|k|y_1) = mk(\pm x_1) + nk(\pm y_1)$$

is an element of T. (Here we use the fact that $|k|$ is equal to either k or $-k$.) Since h is the *smallest* element of T, this implies that $|k|g \geq h$.

On the other hand, $h \in T$, and so there exist integers x_2 and y_2 such that

$$h = kmx_2 + kny_2 = \pm|k|(mx_2 + ny_2).$$

So $|k|$ divides h, and the integer $\frac{h}{|k|} = \pm(mx_2 + ny_2) = m(\pm x_2) + n(\pm y_2)$ in an element of S. Since g is the *smallest* element of S, we have $g \leq \frac{h}{|k|}$, and so $|k|g \leq h$.

The two inequalities imply that $|k|g = h$. □

Proposition 6.31 (Euclid's lemma)**.** *Suppose p is a prime and $m, n \in \mathbb{N}$. If $p|mn$, then $p|m$ or $p|n$.*

Proof. Suppose p divides mn. If p divides m, we are done. So consider the case that p does not divide m. We need to show that p divides n. Since p is prime and does not divide m, we have $\gcd(m,p) = 1$. By Proposition 6.30, we have

$$\gcd(mn, pn) = n \gcd(m,p) = n.$$

Then, by Proposition 6.29(iii), since p divides both mn and pn, we can conclude that p also divides n. □

Corollary 6.32. *Suppose $k \in \mathbb{N}$, p is a prime, and $m_1, \ldots, m_k \in \mathbb{N}$. If $p|m_1 m_2 \cdots m_k$, then $p|m_i$ for some $1 \leq i \leq k$.*

Proof. Let $P(k)$ be the statement

$$\forall m_1, m_2, \ldots, m_k \in \mathbb{N},\ (p|m_1 m_2 \cdots m_k) \implies (p|m_i \text{ for some } 1 \leq i \leq k).$$

We prove that $P(k)$ is true for all $k \geq 1$ by induction on k.

Base case: Consider the case $k = 1$. The statement $P(1)$ is

$$\forall m_1 \in \mathbb{N},\ (p|m_1) \implies (p|m_1),$$

which is clearly true.

Induction step: Assume that $P(n)$ is true for some $n \in \mathbb{N}$. We will show that $P(n+1)$ is true. Suppose $m_1, \ldots, m_{n+1} \in \mathbb{N}$ and p divides

$$m_1 m_2 \cdots m_{n+1} = (m_1 m_2 \cdots m_n) m_{n+1}.$$

Then, by Proposition 6.31, $p|m_1 \cdots m_n$ or $p|m_{n+1}$. In the first case, the induction hypothesis implies that $p|m_i$ for some $1 \leq i \leq n$. Thus, in either case, we have $p|m_i$ for some $1 \leq i \leq n+1$. This completes the proof of the induction step. □

By Proposition 6.27 every integer $n \geq 2$ has a prime factorization. Our next goal is to show that, in fact, such a prime factorization is *unique*. Of course, one can always re-order the factors in any factorization. For example,

$$30 = 2 \cdot 3 \cdot 5 = 3 \cdot 2 \cdot 5.$$

So the best we can hope for is that prime factorizations are unique up to such re-ordering (i.e. that any two prime factorizations of the same integer $n \geq 2$ differ only by re-ordering).

Theorem 6.33. *Every integer $n \geq 2$ has a unique (up to re-ordering) prime factorization.*

Proof. A prime factorization *exists* by Proposition 6.27. It remains to show the uniqueness part of the theorem. We will do this by induction on n.

Base case: When $n = 2$, the only factorization is simply the expression 2 itself, since there is no other way to write 2 as a product of primes (since there are no primes less than 2).

Induction step: Now consider $n \geq 3$ and suppose that every integer less than n (and ≥ 2) has a unique prime factorization. Suppose n has two prime factorizations

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_j.$$

Then, by Corollary 6.32, p_1 divides q_i for some $1 \leq i \leq j$. But since q_i is prime, this implies that $p_1 = q_i$ (since p_1 cannot equal ± 1 or $-q_i$, and those are the only other factors of q_i). So we have

$$\frac{n}{p_1} = p_2 p_3 \cdots p_k = q_1 q_2 \cdots q_{i-1} q_{i+1} \cdots q_j.$$

By the induction hypothesis, these two prime factorizations of $\frac{n}{p_1}$ are equal, up to re-ordering. Therefore, the two given prime factorizations of n are equal, up to re-ordering. □

Proposition 6.34. *If p is prime and $0 < r < p$, then $\binom{p}{r}$ is divisible by p.*

Proof. The proof of this proposition can be found in [BG10, Prop. 6.34]. □

Theorem 6.35 (Fermat's Little Theorem)**.** *If $m \in \mathbb{Z}$ and p is prime, then*

$$m^p \equiv m \mod p.$$

Proof. Fix a prime p. If $p = 2$, then Fermat's Little Theorem says that m^2 is even if and only if m is even, which was Proposition 6.2.1(iii). So we assume $p > 2$.

Let $P(k)$ be the statement

$$k^p \equiv k \mod p.$$

We will first prove that $P(m)$ is true for all $m \geq 0$. (We will deal with the case $m < 0$ after.)

Base case: Since $0^p - 0 = 0 - 0 = 0$ is divisible by p, we have $0^p \equiv 0$.

Induction step: We assume that $P(m)$ is true for some $m \geq 0$ and show that $P(m+1)$ is true. By the Binomial Theorem (Theorem 4.12), we have

$$(m+1)^p = \sum_{\ell=0}^{p} \binom{p}{\ell} m^\ell 1^{p-\ell} = \sum_{\ell=0}^{p} \binom{p}{\ell} m^\ell.$$

By Proposition 6.34, $\binom{p}{\ell} \equiv 0 \mod p$ for $0 < \ell < p$. Therefore,

$$(m+1)^p = \sum_{\ell=0}^{p} \binom{p}{\ell} m^\ell \equiv \binom{p}{0} m^0 + \binom{p}{p} m^p = 1 + m^p \equiv 1 + m \mod p,$$

where we used the induction hypothesis in the last step. This completes the proof of the induction step. (Note that the string of "equations" above involves both $=$ and $\equiv$. But since equality implies equivalence mod p, the corresponding string, where we replace all $=$ symbols by $\equiv$ symbols is also true. Then we use transitivity of $\equiv$ to conclude that $(m+1)^p \equiv 1+m$.)

It remains to prove the statement for $m < 0$. Suppose $m < 0$. Define $n = -m$. Then $n > 0$ and so, by the above, we have $n^p \equiv n \mod p$. Since p is odd, we have

$$m^p = (-n)^p = (-1)^p n^p = -n^p \equiv -n = m.$$

Thus the result also holds for $m < 0$. □

Corollary 6.36. *Suppose $m \in \mathbb{Z}$ and let p be a prime that does not divide m. Then*

$$m^{p-1} \equiv 1 \mod p.$$

Proof. By Theorem 6.35, we have $m^p \equiv m$. In other words, p divides $m^p - m = m(m^{p-1} - 1)$. Since p does not divide m, we can conclude that p divides $m^{p-1} - 1$ by Proposition 6.31. Thus $m^{p-1} \equiv 1$. □

Remark 6.37. Fermat's Little Theorem is the mathematics that underpins the theory of RSA encryption. So your bank account information is secure when you check your balance online because of Fermat's Little Theorem.

Exercises.

6.4.1 ([BG10, Proj. 6.27]). For which $n \geq 2$ does $\mathbb{Z}_n$ satisfy the cancellation property (Axiom 1.5)? Prove your assertion.

6.4.2. Let $m, n \in \mathbb{N}$. Suppose m divides n, and p is a prime factor of n that is not a prime factor of m. Prove that m divides $\frac{n}{p}$. *Hint*: Use prime factorizations.

6.4.3. Given $a, b \in \mathbb{N}$, we can write them as products of primes

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \quad \text{and} \quad b = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k},$$

where the $p_1, \ldots, p_k$ are distinct prime numbers, and the exponents are elements of $\mathbb{Z}_{\geq 0}$. (We allow the exponent zero so that we can write the prime factorizations of a and b using the same set of primes—using an exponent of zero if a particular prime does not appear in one of the factorizations. This also allows us to consider the case $a = 1$ or $b = 1$, in which case all of the corresponding exponents are zero.) Prove that a divides b if and only if $n_i \leq m_i$ for all $1 \leq i \leq k$.

6.4.4. Suppose p is a prime number. Prove that, for all $x \in \mathbb{Z}$,

$$3x^{p^2} - 5x^{p^3} + 2x$$

is divisible by p.

6.4.5. Suppose that $a, b \in \mathbb{N}$ have prime factorizations

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \quad \text{and} \quad b = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k},$$

where the $p_1, \ldots, p_k$ are distinct prime numbers, and the exponents are elements of $\mathbb{Z}_{\geq 0}$. Define

$$\mathrm{GCD}(a, b) = p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k}$$

where, for $1 \leq i \leq k$, we define ℓ_i to be the minimum of n_i and m_i. (Note the difference between this and the definition of $\gcd(a, b)$.)

(i) Prove that $\mathrm{GCD}(a, b)$ divides $\gcd(a, b)$. *Hint*: Use Proposition 6.29(iii).

(ii) Prove that $\gcd(a, b)$ divides $\mathrm{GCD}(a, b)$. *Hint*: Use Proposition 6.29(i).

(iii) Prove that $\mathrm{GCD}(a, b) = \gcd(a, b)$.

Chapter 7

Real numbers

In this chapter, we will introduce the real numbers. As was the case for the integers, you have likely encountered real numbers before. However, we will take a more rigorous approach. Namely, we will start from a precise list of axioms, and we will assume that a set $\mathbb{R}$ exists that satisfies these axioms. Many of the axioms are the same as those we saw for the integers. However, there are some important differences.

7.1 Axioms

We will assume that there is a set, denoted $\mathbb{R}$, with binary operations $+$ (*addition*) and $\cdot$ (*multiplication*) satisfying Axioms 7.1–7.5, 7.13 and 7.35. The elements of $\mathbb{R}$ are called *real numbers*.

Axiom 7.1 (Commutativity, associativity, and distributivity)**.** For all $x, y, z \in \mathbb{R}$, we have

(i) $x + y = y + x$, (*commutativity of addition*)

(ii) $(x + y) + z = x + (y + z)$, (*associativity of addition*)

(iii) $x \cdot (y + z) = x \cdot y + x \cdot z$, (*distributivity*)

(iv) $x \cdot y = y \cdot x$, (*commutativity of multiplication*)

(v) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. (*associativity of multiplication*)

As we did for the integers, we will often denote multiplication by *juxtaposition*. That is, we will write xy instead of $x \cdot y$.

Axiom 7.2 (Additive identity)**.** There exists a real number 0 satisfying $\forall x \in \mathbb{R},\ x + 0 = x$. This element 0 is called an *additive identity*, or an *identity element for addition*.

Axiom 7.3 (Multiplicative identity)**.** There exists a real number 1 such that $1 \neq 0$ and $\forall x \in \mathbb{R},\ x \cdot 1 = x$. The element 1 is called a *multiplicative identity*, or an *identity element for multiplication*.

Axiom 7.4 (Additive inverse)**.** For each $x \in \mathbb{R}$, there exists a real number, denoted $-x$, such that $x + (-x) = 0$. The element $-x$ is called an *additive inverse* of x.

Axiom 7.5 (Multiplicative inverse)**.** For each $x \in \mathbb{R} - \{0\}$, there exists a real number, denoted x^{-1}, such that $x \cdot x^{-1} = 1$. The element x^{-1} is called a *multiplicative inverse* of x.

Remark 7.6. Although we use the same notation 0 and 1 for the additive and multiplicative identities of the real numbers $\mathbb{R}$ as we did for the corresponding elements of the integers $\mathbb{Z}$, these are *a priori* different elements since we have not discussed any relationship between $\mathbb{Z}$ and $\mathbb{R}$. Later, in Section 8.2, we will discuss how we can view $\mathbb{Z}$ as a subset of $\mathbb{R}$, and then the 0 of $\mathbb{Z}$ will correspond to the 0 of $\mathbb{R}$, and similarly for 1. This explains our use of the same notation.

Proposition 7.7. *For each $x \in \mathbb{R} - \{0\}$, there exists a* unique *real number y such that $xy = 1$.*

Proof. Suppose $x \in \mathbb{R} - \{0\}$. By Axiom 7.5, there exists a real number y such that $xy = 1$. It remains to show that this element is unique. Suppose z is another real number such $xz = 1$. Then we have

$$y = y \cdot 1 = y(xz) = (yx)z = (xy)z = 1 \cdot z = z \cdot 1 = z.$$

Thus, the element with the given property is unique. □

Proposition 7.7 justifies calling x^{-1} *the* (as opposed to *a*) multiplicative inverse of x.

Corollary 7.8. *For $x \in \mathbb{R}$, $x \neq 0$, we have $(x^{-1})^{-1} = x$.*

Proof. Suppose $x \in \mathbb{R}$ with $x \neq 0$. Then

$$x^{-1}x = xx^{-1} = 1.$$

Therefore, x is a multiplicative inverse of x^{-1}. Since the multiplicative inverse is unique by Proposition 7.7, we must have $(x^{-1})^{-1} = x$. □

Remark 7.9. Since addition and multiplication of real numbers is associative, we can omit the parentheses when writing the addition or multiplication of more than two elements. For instance, if $w, x, y, z \in \mathbb{R}$, we have unambiguously write expressions like

$$w + x + y + z \quad \text{and} \quad wxyz,$$

since the results of the additions and multiplications is the same no matter how we group the terms. See Remark 1.29.

Proposition 7.10. *For all $x, y \in \mathbb{R} - \{0\}$, we have $(xy)^{-1} = x^{-1}y^{-1}$.*

Proof. Suppose $x, y \in \mathbb{R} - \{0\}$. By Axiom 7.5, x and y have multiplicative inverses x^{-1} and y^{-1}, respectively. We have

$$\begin{aligned} & (xy)^{-1}xy = 1 \\ \implies & (xy)^{-1}xyy^{-1} = y^{-1} \\ \implies & (xy)^{-1}x \cdot 1 = y^{-1} \\ \implies & (xy)^{-1}x = y^{-1} \end{aligned}$$

$$\begin{aligned} &\implies (xy)^{-1}xx^{-1} = y^{-1}x^{-1} \\ &\implies (xy)^{-1} \cdot 1 = x^{-1}y^{-1} \\ &\implies (xy)^{-1} = x^{-1}y^{-1}. \end{aligned}$$

□

Proposition 7.11. *Suppose $x, y, z \in \mathbb{R}$ and $x \neq 0$. If $xy = xz$, then $y = z$.*

Proof. Assume $x, y, z \in \mathbb{R}$, $x \neq 0$, and $xy = xz$. By Axiom 7.5, x has a multiplicative inverse x^{-1}. Then

$$\begin{aligned} &xy = xz \\ &\implies x^{-1}xy = x^{-1}xz \\ &\implies xx^{-1}y = xx^{-1}z \\ &\implies 1 \cdot y = 1 \cdot z \\ &\implies y \cdot 1 = z \cdot 1 \\ &\implies y = z. \end{aligned}$$

□

Remark 7.12. You should compare Axioms 7.1–7.5 to Axioms 1.1–1.5. Replacing $\mathbb{Z}$ by $\mathbb{R}$,

- Axiom 1.1 becomes Axiom 7.1,
- Axiom 1.2 becomes Axiom 7.2,
- Axiom 1.3 becomes Axiom 7.3, and
- Axiom 1.4 becomes Axiom 7.4.

However, Axioms 1.5 and 7.5 are different. Nevertheless, Proposition 7.11 shows us that Axiom 1.5 holds for $\mathbb{R}$ as well (i.e. Axiom 7.5 is stronger than Axiom 1.5). Therefore, any proposition we proved for $\mathbb{Z}$ using only axioms Axioms 1.1–1.5 also holds for $\mathbb{R}$, with an identical proof. In particular all of the propositions of Section 1.2 hold with $\mathbb{Z}$ replaced by $\mathbb{R}$. We will refer to the $\mathbb{R}$ analogues of these propositions by appending "for $\mathbb{R}$". For example, we may say "by Proposition 1.9 for $\mathbb{R}$".

Subtraction. As for the integers, we define *subtraction* in $\mathbb{R}$ by

$$x - y := x + (-y), \quad x, y \in \mathbb{R}.$$

Then Proposition 1.28 also holds with $\mathbb{Z}$ replaced by $\mathbb{R}$.

Division. We have not yet discussed division in this course, because division is not very well behaved for the integers. (More precisely, given two random integers, it is unlikely that you can divide one by the other and obtain an integer.) However, we can define *division* in $\mathbb{R}$. If $x, y \in \mathbb{R}$ and $x \neq 0$, we define

$$\frac{y}{x} := yx^{-1}.$$

Precisely, division is a function

$$\text{division}\colon \mathbb{R} \times (\mathbb{R} - \{0\}) \to \mathbb{R}, \quad \text{division}(y, x) = yx^{-1}.$$

Note that

$$\frac{1}{x} = 1 \cdot x^{-1} = x^{-1}.$$

Exercises.

7.1.1. Using only Axioms 7.1–7.5 and the definition of division, show that you can add "fractions" with common denominators the way you learn in grade school. More precisely, show that, for all $a, b, c \in \mathbb{R}$ with $c \neq 0$,

$$\frac{a}{c} + \frac{b}{c} = \frac{a+b}{c}.$$

7.1.2. Suppose $a, b, c, d \in \mathbb{R}$ and $b, d \neq 0$. Show that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}.$$

Show all your steps.

7.1.3. Suppose $x \in \mathbb{R}$ and $x \neq 0$. Prove that $(-x)^{-1} = -x^{-1}$

7.1.4. Suppose $a, b \in \mathbb{R}$ and $b \neq 0$. Prove that

$$\frac{-a}{b} = -\frac{a}{b} = \frac{a}{-b}.$$

7.1.5. Prove that zero does not have a multiplicative inverse.

7.2 Positive real numbers and ordering

In our discussion of the natural numbers, after introducing Axioms 1.1–1.5 and proving some propositions that result from these axioms, we added an axiom (Axiom 2.1) that guaranteed the existence of the set $\mathbb{N}$ of natural numbers. This resulted in an ordering on the integers. We now introduce an analogue of Axiom 2.1 for $\mathbb{R}$. Just as $\mathbb{N}$ turned out to be the set of positive integers, its analogue for $\mathbb{R}$ will be the set of positive real numbers.

Axiom 7.13. There exists a subset $\mathbb{R}_{>0} \subseteq \mathbb{R}$ with the following properties:

(i) If $x, y \in \mathbb{R}_{>0}$, then $x + y \in \mathbb{R}_{>0}$. (The subset $\mathbb{R}_{>0}$ is closed under addition.)

(ii) If $x, y \in \mathbb{R}_{>0}$, then $xy \in \mathbb{R}_{>0}$. (The subset $\mathbb{R}_{>0}$ is closed under multiplication.)

(iii) $0 \notin \mathbb{R}_{>0}$.

(iv) For every $x \in \mathbb{R}$, we have $x \in \mathbb{R}_{>0}$ or $x = 0$ or $-x \in \mathbb{R}_{>0}$.

The elements of $\mathbb{R}_{>0}$ are called *positive real numbers*. A real number that is neither positive nor zero is a *negative real number*.

Note that Axiom 7.13 is the same as Axiom 2.1, but with $\mathbb{Z}$ and $\mathbb{N}$ replaced by $\mathbb{R}$ and $\mathbb{R}_{>0}$, respectively.

Proposition 7.14. *(i) For $x \in \mathbb{R}$, one and only one of the following statements is true:*

- $x \in \mathbb{R}_{>0}$,
- $-x \in \mathbb{R}_{>0}$,
- $x = 0$.

(ii) We have $1 \in \mathbb{R}_{>0}$.

Proof. The proof of part (i) is the same as the proof of Proposition 2.3, but with $\mathbb{Z}$ and $\mathbb{N}$ replaced by $\mathbb{R}$ and $\mathbb{R}_{>0}$, respectively. Similarly, the proof of part (ii) is the same as that of Proposition 2.4. □

We now define an ordering on the set of real numbers, just as we did for the integers.

Definition 7.15 (Order on the real numbers)**.** For $x, y \in \mathbb{R}$, we write $x < y$ (and say x is *less than* y) or $y > x$ (and say y is *greater than* x) if and only if

$$y - x \in \mathbb{R}_{>0}.$$

We write $x \leq y$ (and say x is *less than or equal to* y) or $y \geq x$ (and say y is *greater than or equal to* x) if and only if

$$x < y \quad \text{or} \quad x = y.$$

Remark 7.16. Note that Definition 7.15 is the same as Definition 2.5, but with $\mathbb{Z}$ and $\mathbb{N}$ replaced by $\mathbb{R}$ and $\mathbb{R}_{>0}$, respectively. Therefore, many of the propositions concerning the ordering on $\mathbb{Z}$ that we proved in Section 2.2 also hold with $\mathbb{Z}$ and $\mathbb{N}$ replaced by $\mathbb{R}$ and $\mathbb{R}_{>0}$, with an identical proof. In particular, Propositions 2.6–2.15 all hold for $\mathbb{R}$. Again (see Remark 7.12) we will refer to the $\mathbb{R}$ analogues of these propositions by appending "for $\mathbb{R}$".

Proposition 7.17. *(i) Suppose $x \in \mathbb{R}$, $x \neq 0$. Then $x \in \mathbb{R}_{>0}$ if and only if $\frac{1}{x} \in \mathbb{R}_{>0}$.*

(ii) Suppose $x, y \in \mathbb{R}_{>0}$. If $x < y$, then $0 < \frac{1}{y} < \frac{1}{x}$.

Proof. (i) Suppose $x \in \mathbb{R}_{>0}$. By Axiom 7.13(iv), we have $\frac{1}{x} \in \mathbb{R}_{>0}$ or $\frac{1}{x} = 0$ or $-\frac{1}{x} \in \mathbb{R}_{>0}$. We will show that the latter two cases lead to a contradiction. First assume that $\frac{1}{x} = 0$. Then

$$1 = x \cdot \frac{1}{x} = x \cdot 0 = 0,$$

where, in the last equality we used Proposition 1.14 for $\mathbb{R}$. But the equality $1 = 0$ contradicts Axiom 7.3. Next, assume that $-\frac{1}{x} \in \mathbb{R}_{>0}$. Then

$$-1 = -\left(x \cdot \frac{1}{x}\right) = x \cdot \left(-\frac{1}{x}\right) \in \mathbb{R}_{>0},$$

by the closure of $\mathbb{R}_{>0}$ under multiplication (Axiom 7.13(ii)). But this contradicts Proposition 7.14. So we must have $\frac{1}{x} \in \mathbb{R}_{>0}$.

Conversely, suppose $x^{-1} = \frac{1}{x} \in \mathbb{R}_{>0}$. Then, by the above, $x = (x^{-1})^{-1} \in \mathbb{R}_{>0}$.

(ii) Now suppose $x, y \in \mathbb{R}_{>0}$ satisfy $x < y$. Then $x^{-1}, y^{-1} \in \mathbb{R}_{>0}$ by part (i), and hence $x^{-1}y^{-1} \in \mathbb{R}_{>0}$ by the closure of $\mathbb{R}_{>0}$ under multiplication (Axiom 7.13(ii)). Therefore, we have

$$x < y \implies x^{-1}y^{-1}x < x^{-1}y^{-1}y \implies y^{-1} < x^{-1},$$

where, in the first implication, we used Proposition 2.9(iii) for $\mathbb{R}$.

□

Example 7.18. We will prove that, for all $x \in \mathbb{R}$,

$$x^4 < 2x^5 \iff x > \frac{1}{2}. \tag{7.1}$$

Let's split into two cases: $x = 0$ and $x \neq 0$.

Case 1: Suppose $x = 0$. Then $x^4 = 0^4 = 0$ and $2x^5 = 2 \cdot 0^5 = 0$. Thus, the statement $x^4 < 2x^5$ is false since $0 \not< 0$. Since the statement $0 > \frac{1}{2}$ is also false, the double implication (7.1) is true.

Case 2: Suppose $x \neq 0$. Since $x^4 = (x^2)^2$, Proposition 2.11 for $\mathbb{R}$ implies that $x^4 \in \mathbb{R}_{>0}$. Therefore, $(x^4)^{-1} \in \mathbb{R}_{>0}$ by Proposition 7.17. Similarly, $\frac{1}{2} \in \mathbb{R}_{>0}$. Thus

$$\begin{aligned}
x^4 < 2x^5 &\implies (x^4)^{-1}x^4 < (x^4)^{-1}2x^5 && \text{(Proposition 2.9(iii) for } \mathbb{R}) \\
&\implies 1 < 2x \\
&\implies \frac{1}{2} \cdot 1 < \frac{1}{2} \cdot 2x && \text{(Proposition 2.9(iii) for } \mathbb{R}) \\
&\implies \frac{1}{2} < x.
\end{aligned}$$

For the other implication, we have

$$\begin{aligned}
x > \frac{1}{2} &\implies 2x > 2 \cdot \frac{1}{2} && \text{(Proposition 2.9(iii) for } \mathbb{R}) \\
&\implies 2x > 1 \\
&\implies x^4 \cdot 2x > x^4 \cdot 1 && \text{(Proposition 2.9(iii) for } \mathbb{R}) \\
&\implies 2x^5 > x^4.
\end{aligned}$$

For later use, we define

$$\mathbb{R}_{\geq 0} := \mathbb{R}_{>0} \cup \{0\} = \{x \in \mathbb{R} : x \geq 0\}.$$

Exercises.

7.2.1 ([BG10, Prop. 8.41]). Let $x \in \mathbb{R}$. Prove that $x^2 < x^3$ if and only if $x > 1$.

7.2.2. Recall that we defined $2 := 1 + 1 \in \mathbb{Z}$. Prove that there is no integer $n \in \mathbb{Z}$ such that $2n = 1$. Therefore, unlike $\mathbb{R}$, the set $\mathbb{Z}$ of integers does not have multiplicative inverses of all nonzero elements. *Hint*: Try a proof by contradiction, using Proposition 2.21.

7.2.3. Suppose $x, y \in \mathbb{R}$. Prove that

$$xy \in \mathbb{R}_{>0} \iff (x, y \in \mathbb{R}_{>0}) \text{ or } (-x, -y \in \mathbb{R}_{>0}).$$

7.2.4. Prove that, for all $x \in \mathbb{R}$,

$$x^2 - 4 > 0 \iff x < -2 \text{ or } x > 2.$$

7.2.5. Suppose $x, y \in \mathbb{R}$ and $x \neq 0$. Prove that

$$\frac{y}{x} \in \mathbb{R}_{>0} \iff (x, y \in \mathbb{R}_{>0}) \text{ or } (-x, -y \in \mathbb{R}_{>0}).$$

7.3 The real numbers versus the integers

As we have discussed, Axioms 1.1–1.4 for $\mathbb{Z}$ are identical to Axioms 7.1–7.4. Similarly, Axiom 2.1 and Axiom 7.13 are identical.

However, Axiom 1.5 (cancellation) and Axiom 7.5 are different. We showed in Proposition 7.11 that Axiom 7.5 implies Axiom 1.5 (with $\mathbb{Z}$ replaced by $\mathbb{R}$). However, the converse implication is false. For example, the integer 2 does not have a multiplicative inverse in $\mathbb{Z}$. Thus, Axiom 7.5 does *not* hold with $\mathbb{R}$ replaced by $\mathbb{Z}$. This is therefore a difference between $\mathbb{Z}$ and $\mathbb{R}$.

Another important difference between $\mathbb{Z}$ and $\mathbb{R}$ concerns the ordering. By Proposition 2.21, the set $\mathbb{N}$ of natural numbers has a smallest element, namely 1. The analogous statement for $\mathbb{R}$ is false. Before proving this (Theorem 7.20), we prove a lemma.

Lemma 7.19. *We have* $0 < \frac{1}{2} < 1$.

Proof. Since $2 = 1+1 \in \mathbb{R}_{>0}$ by the closure of $\mathbb{R}_{>0}$ under addition (Axiom 7.13(i)), it follows from Proposition 7.17(i) that $0 < \frac{1}{2}$. Since $2 - 1 = (1 + 1) - 1 = 1 \in \mathbb{R}_{>0}$, we have $1 < 2$. Therefore, by Proposition 7.17(ii), we have $\frac{1}{2} < \frac{1}{1} = 1$.

Alternate proof: We can also prove that $\frac{1}{2} < 1$ by contradiction. Suppose $1 \leq \frac{1}{2}$. Then we have

$$0 < 1 < 2 \quad \text{and} \quad 0 < 1 \leq \frac{1}{2}.$$

By Proposition 2.9(iii) for $\mathbb{R}$, we then have

$$1 \cdot 1 < 2 \cdot \frac{1}{2} \implies 1 < 1 \implies 0 = 1 - 1 \in \mathbb{R}_{>0},$$

which contradicts Axiom 7.13(iii). □

Theorem 7.20. *The set* $\mathbb{R}_{>0}$ *of positive real numbers does not have a smallest element.*

Proof. We will prove the result by contradiction. Suppose x is a smallest element of $\mathbb{R}_{>0}$. Then (using Lemma 7.19) we have

$$0 < \frac{1}{2} < 1 \quad \text{and} \quad 0 < x \leq x.$$

By Proposition 2.9(iii) for $\mathbb{R}$, we then have

$$\frac{1}{2} \cdot x < x.$$

However, by the closure of $\mathbb{R}_{>0}$ under multiplication (Axiom 7.13(ii)), we have $\frac{1}{2} \cdot x \in \mathbb{R}_{>0}$. This contradicts our assumption that x is a smallest element of $\mathbb{R}_{>0}$. □

Another important difference between $\mathbb{Z}$ and $\mathbb{R}$ concerns "gaps" between numbers. The integers have gaps. For instance, by Proposition 2.22, there is no integer between 0 and 1. In contrast, the real numbers have no such gaps, as the following theorem shows.

Theorem 7.21. *For all $x, y \in \mathbb{R}$ such that $x < y$, there exists a $z \in \mathbb{R}$ such that $x < z < y$.*

Proof. Suppose $x, y \in \mathbb{R}$ satisfy $x < y$. We will show that $z = \frac{x+y}{2}$ satisfies $x < z < y$. First,

$$z - x = \frac{x+y}{2} - 1 \cdot x = \frac{x+y}{2} - \frac{1}{2} \cdot 2 \cdot x = \frac{1}{2}(x + y - 2x) = \frac{1}{2}(y - x) \in \mathbb{R}_{>0},$$

by closure of $\mathbb{R}_{>0}$ under multiplication (Axiom 7.13(ii)), since $\frac{1}{2} \in \mathbb{R}_{>0}$ (by Lemma 7.19) and $y - x \in \mathbb{R}_{>0}$ by assumption. Thus $x < z$. Second,

$$y - z = 1 \cdot y - \frac{x+y}{2} = \frac{1}{2} \cdot 2 \cdot y - \frac{x+y}{2} = \frac{1}{2}(2y - (x+y)) = \frac{1}{2}(y - x) \in \mathbb{R}_{>0},$$

and so $z < y$. □

The final axiom for $\mathbb{Z}$, Axiom 2.17 has no analogue for $\mathbb{R}$. On the other hand, we will introduce one final axiom for $\mathbb{R}$ which has no analogue for $\mathbb{Z}$.

Exercises.

7.3.1 ([BG10, Proj. 8.44]). Construct a subset $A \subseteq \mathbb{R}$ that satisfies

(i) $1 \in A$ and

(ii) if $n \in A$, then $n + 1 \in A$,

yet for which $\mathbb{R}_{>0}$ is not a subset of A.

7.4 Upper and lower bounds

Before introducing our last axiom for $\mathbb{R}$, we begin with some definitions.

Definition 7.22 (Bounded sets, supremum, infimum)**.** Let $A \subseteq \mathbb{R}$ such that $A \neq \varnothing$.

(i) The set A is *bounded above* if there exists $b \in \mathbb{R}$ such that $\forall a \in A,\ a \leq b$. Any real number b with this property is called an *upper bound* for A.

(ii) The set A is *bounded below* if there exists $b \in \mathbb{R}$ such that $\forall a \in A,\ b \leq a$. Any real number b with this property is called a *lower bound* for A.

(iii) The set A is *bounded* if it is both bounded above and bounded below.

(iv) A *least upper bound*, or *supremum*, for A is an upper bound that is less than or equal to every upper bound for A.

(v) A *greatest lower bound*, or *infimum*, for A is a lower bound that is greater than or equal to every lower bound for A.

The next proposition shows that suprema and infima are unique, if they exist.

Proposition 7.23. *Suppose A is a nonempty subset of $\mathbb{R}$.*

(i) If x_1 and x_2 are least upper bounds for A, then $x_1 = x_2$.

(ii) If x_1 and x_2 are greatest lower bounds for A, then $x_1 = x_2$.

Proof. We will prove the first statement, since the proof of the second is analogous. Suppose x_1 and x_2 are least upper bounds for A. Then, since x_1 is an upper bound for A and x_2 is a *least* upper bound, we have $x_2 \leq x_1$. Similarly, we have $x_1 \leq x_2$. Thus $x_1 = x_2$. □

For a nonempty subset A of $\mathbb{R}$, the least upper bound (supremum) of A is denoted by $\sup(A)$ (or $\sup A$) and the greatest upper bound (infimum) of A is denoted by $\inf(A)$ (or $\inf A$). Keep in mind that, for an arbitrary nonempty set $A \subseteq \mathbb{R}$, $\inf A$ and/or $\sup A$ may not exist, as we will see.

Example 7.24. We will show that $\inf \mathbb{R}_{>0} = 0$. Since $0 < x$ for all $x \in \mathbb{R}_{>0}$, we have that 0 is a lower bound for R. It remains to show that 0 is the *greatest* lower bound. We do this by contradiction. Suppose $y \in \mathbb{R}$ is a lower bound for $\mathbb{R}_{>0}$ and $0 < y$. Then, by Theorem 7.21, there exists $z \in \mathbb{R}$ such that $0 < z < y$. But then $z \in \mathbb{R}_{>0}$ does *not* satisfy $y \leq z$. This contradicts the fact that y is a lower bound for $\mathbb{R}_{>0}$.

Example 7.25. We have $\inf \mathbb{R}_{\geq 0} = 0$. The proof is almost identical to that of Example 7.24.

Examples 7.24 and 7.25 illustrate an important point: the supremum or infimum of a set A (if it exists) may or may not be an element of A. In addition, infima and suprema may not exist, as the following example illustrates.

Proposition 7.26. *The set $\mathbb{R}_{>0}$ has no upper bound.*

Proof. We prove the result by contradiction. Suppose x is an upper bound for $\mathbb{R}_{>0}$. Then, since $1 \in \mathbb{R}_{>0}$ by Proposition 7.14(ii), we have

$$x \geq 1 > 0 \implies x > 0 \implies x \in \mathbb{R}_{>0}.$$

Thus $x + 1 \in \mathbb{R}_{>0}$ by closure of $\mathbb{R}_{>0}$ under addition (Axiom 7.13(i)). Since

$$(x + 1) - x = 1 \in \mathbb{R}_{>0},$$

we have $x + 1 > x$. This contradicts the assumption that x is an upper bound for $\mathbb{R}_{>0}$. □

Example 7.27. Consider the set

$$A = \{x^{-1} : x \in \mathbb{R}_{>0}\}.$$

We will show that $\inf(A) = 0$.

To prove this, first note that, by Proposition 7.17, $x^{-1} > 0$ for all $x \in \mathbb{R}_{>0}$. Thus 0 is a lower bound for A.

It remains to show that it is the *greatest* lower bound. We will prove this by contradiction. Suppose y is another lower bound such that $0 < y$. Then, by Theorem 7.21, there exists $z \in \mathbb{R}$ such that $0 < z < y$. Let $x = z^{-1}$. Then, by Proposition 7.17, $x \in \mathbb{R}_{>0}$ and so, by Corollary 7.8, we have $z = x^{-1} \in A$. But this contradicts the assumption that y is a lower bound for A (since $z < y$). Therefore, $0 = \inf(A)$.

Example 7.28. Let us find the supremum of the set

$$A = \left\{2 - \frac{3}{x} : x \in \mathbb{R}_{>0}\right\}.$$

We will prove that

$$\sup A = 2.$$

To prove this, we first show that 2 is a upper bound for A. Indeed

$$\begin{aligned} x \in \mathbb{R}_{>0} &\implies x > 0 \\ &\implies \frac{1}{x} > 0 && \text{(Prop. 7.17(i))} \\ &\implies \frac{-3}{x} < 0 && \text{(Prop. 2.9(iv) for } \mathbb{R}) \\ &\implies 2 - \frac{3}{x} < 2. && \text{(Prop. 2.9(i) for } \mathbb{R}) \end{aligned}$$

Since every element of A is of the form $2 - \frac{3}{x}$ for some $x \in \mathbb{R}_{>0}$, the above argument implies that 2 is an upper bound for A.

Now we must show that 2 is the *least* upper bound for A. We prove this by contradiction. Suppose A has an upper bound b with $b < 2$. Thus $2 - b \in \mathbb{R}_{>0}$. Since b is an upper bound for A, we have, for all $x \in \mathbb{R}_{>0}$,

$$2 - \frac{3}{x} < b \implies \frac{3}{x} > 2 - b$$

$$\implies \frac{x}{3} < \frac{1}{2-b} \qquad \text{(Prop. 7.17(ii))}$$
$$\implies x < \frac{3}{2-b}. \qquad \text{(Prop. 2.9(iii))}$$

This implies that $\mathbb{R}_{>0}$ is bounded above by $\frac{3}{2-b}$, contradicting Proposition 7.26.

Example 7.29. Let us show that the set

$$A = \left\{ 2 - \frac{3}{x} : x \in \mathbb{R}_{>0} \right\}.$$

of Example 7.28 has no lower bound, and hence no infimum. We prove this by contradiction. Suppose b were a lower bound for A. Then, in particular, we have $b \leq 2 - \frac{3}{4} < 2$. So

$$\begin{aligned} & b \leq 2 - \frac{3}{x} \quad \text{for all } x \in \mathbb{R}_{>0} \\ \implies & \frac{3}{x} \leq 2 - b \quad \text{for all } x \in \mathbb{R}_{>0} \\ \implies & \frac{3}{2-b} \leq x \quad \text{for all } x \in \mathbb{R}_{>0}. \qquad (\text{since } x \in \mathbb{R}_{>0},\ 2-b \in \mathbb{R}_{>0}) \end{aligned}$$

However, since $\frac{3}{2-b} > 0$, we can find $x \in \mathbb{R}_{>0}$ such that $x < \frac{3}{2-b}$ by Theorem 7.20. Thus we have arrived at a contradiction, as desired.

Examples 7.30. (i) The set $\{x \in \mathbb{R} : x < 0\}$ has supremum 0, but no infimum.

(ii) The set $\{x \in \mathbb{R} : x \leq 0\}$ has supremum 0, but no infimum.

(iii) The set $\mathbb{R}$ has no supremum and no infimum.

(iv) The set $\{x \in \mathbb{R} : 0 \leq x \leq 1\}$ has infimum 0 and supremum 1.

(v) The set $\{x \in \mathbb{R} : 0 < x \leq 1\}$ has infimum 0 and supremum 1.

(vi) The set $\{x \in \mathbb{Z} : 0 < x\}$ has infimum 1, but no supremum. (Technically speaking, we have not defined infima and suprema for subsets of $\mathbb{Z}$, but the definitions are the same. Furthermore, we will discuss in Section 8.2 how we can view $\mathbb{Z}$ as a subset of $\mathbb{R}$.)

Definition 7.31 (Maximum, minimum)**.** Suppose $A \subseteq \mathbb{R}$.

(i) An element $b \in A$ is the *maximum* or *largest* element of A if $\forall a \in A,\ a \leq b$. If this is the case, we write $b = \max(A)$.

(ii) An element $b \in A$ is the *minimum* or *smallest* element of A if $\forall a \in A,\ b \leq a$. If this is the case, we write $b = \min(A)$.

Note the important difference between Definition 7.31 and parts (i) and (ii) of Definition 7.22. In the definition of upper/lower bounds, the bound is an element of $\mathbb{R}$, whereas in Definition 7.31, the maximum/minimum element is required to be an element of the set A itself.

Proposition 7.32. *Suppose $A \subseteq \mathbb{R}$ is nonempty.*

(i) If A has a supremum and $\sup(A) \in A$, then A also has a largest element and $\sup(A) = \max(A)$. Conversely, if A has a largest element then A has a supremum, $\max(A) = \sup(A)$, and $\sup(A) \in A$.

(ii) If A has an infimum and $\inf(A) \in A$, then A also has a smallest element and $\inf(A) = \min(A)$. Conversely, if A has a smallest element then A has an infimum, $\min(A) = \inf(A)$, and $\inf(A) \in A$.

Proof. We will prove the first statement, since the proof of the second is analogous. Suppose A has a supremum b and $b \in A$. Then, by the definition of supremum, we have $\forall a \in A,\ a \leq b$. Thus $b = \max(A)$.

Conversely, suppose A has a largest element b. Then $b \in A$ and $\forall a \in A,\ a \leq b$. Thus b is an upper bound for A. We prove that b is a supremum by contradiction. Suppose that b is not the *least* upper bound. Then there exists an upper bound c for A with $c < b$. But since $b \in A$, this contradicts the fact that c is an upper bound for A. Therefore, b must be the least upper bound of A, i.e. $b = \sup(A)$. Therefore $\sup(A) = b = \max(A) \in A$. □

Proposition 7.32 essentially says that greatest elements of a set A are simply suprema that are contained in A. Similarly smallest elements of A are simply infima that are contained in A. It follows from this and Proposition 7.23 that greatest and smallest elements, if they exist, are unique.

Example 7.33. Consider the set

$$A = \left\{ 2 - \frac{3}{x} : x \in \mathbb{R}_{>0} \right\}.$$

of Examples 7.28 and 7.29.

We showed in Example 7.28 that $\sup A = 2$. By Proposition 7.32(i), if A had a largest element, it would be 2. But $2 \notin A$ since, as shown in Example 7.28, all elements of A are strictly less than 2. Thus A does not have a largest element.

In addition, we showed in Example 7.29 that A does not have an infimum. Thus, by Proposition 7.32(ii), it also does not have a smallest element.

Examples 7.34. Let us take another look at the sets of Examples 7.30.

(i) The set $\{x \in \mathbb{R} : x < 0\}$ has no maximum and no minimum.

(ii) The set $\{x \in \mathbb{R} : x \leq 0\}$ has maximum 0 and no minimum.

(iii) The set $\mathbb{R}$ has no maximum and no minimum.

(iv) The set $\{x \in \mathbb{R} : 0 \leq x \leq 1\}$ has minimum 0 and maximum 1.

(v) The set $\{x \in \mathbb{R} : 0 < x \leq 1\}$ has maximum 1 and no minimum.

Here is our final axiom for the real numbers.

Axiom 7.35 (Completeness axiom)**.** Every nonempty subset of $\mathbb{R}$ that is bounded above has a least upper bound.

Proposition 7.36. *Suppose that $A \subseteq B \subseteq \mathbb{R}$, that A and B are nonempty, and that B is bounded above. Then* $\sup(A) \leq \sup(B)$.

Proof. Since B is bounded above and $A \subseteq B$, we know that A is also bounded above. Thus, by Axiom 7.35, $\sup(A)$ and $\sup(B)$ exist. By definition, we have $b \leq \sup(B)$ for all $b \in B$. Since $A \subseteq B$, this implies that $a \leq \sup(B)$ for all $a \in A$. Therefore, $\sup(B)$ is an upper bound for A. Since $\sup(A)$ is the *least* upper bound, we have $\sup(A) \leq \sup(B)$. □

We now define *intervals*. For $x, y \in \mathbb{R}$, we define

$$\begin{aligned}
[x, y] &:= \{z \in \mathbb{R} : x \leq z \leq y\}, \\
(x, y] &:= \{z \in \mathbb{R} : x < z \leq y\}, \\
[x, y) &:= \{z \in \mathbb{R} : x \leq z < y\}, \\
(x, y) &:= \{z \in \mathbb{R} : x < z < y\}, \\
(-\infty, y] &:= \{z \in \mathbb{R} : z \leq y\}, \\
(-\infty, y) &:= \{z \in \mathbb{R} : z < y\}, \\
[x, \infty) &:= \{z \in \mathbb{R} : x \leq z\}, \\
(x, \infty) &:= \{z \in \mathbb{R} : x < z\}, \\
(-\infty, \infty) &:= \mathbb{R}.
\end{aligned}$$

Remark 7.37. (i) Note that ∞ and $-\infty$ are *not* real numbers. We are using these symbols just as part of the notation.

(ii) The text [BG10] requires that $x < y$ for the above intervals. However, this is not necessary. For instance, when $x = y$, we have

$$[x, x] = \{x\}, \quad [x, x) = (x, x] = (x, x) = \varnothing,$$

and when $x > y$, we have

$$[x, y] = [x, y) = (x, y] = (x, y) = \varnothing.$$

(iii) We use the same notation for the interval (x, y) and the point $(x, y) \in \mathbb{R}^2$, so there is some potential chance for confusion. It should be clear from the context whether we are referring to an interval or a point in $\mathbb{R}^2$.

Proposition 7.38. *Every nonempty subset of* $\mathbb{R}$ *that is bounded below has a greatest lower bound.*

Proof. Suppose A is a nonempty subset of $\mathbb{R}$ that is bounded below. Therefore, there exists an $m \in \mathbb{R}$ such that $\forall x \in A,\ m \leq x$. Define

$$B = \{-x : x \in A\}.$$

We will show that B is bounded above by $-m$. Indeed,

$$x \in B \implies -x \in A \implies m \leq -x \implies x \leq -m.$$

Thus, $\forall x \in B, x \leq -m$, as desired. Therefore, by Axiom 7.35, B has a least upper bound y.

We will show that $-y$ is a greatest lower bound for A. Since

$$x \in A \implies -x \in B \implies -x \leq y \implies x \geq -y,$$

we see that $-y$ is a lower bound for A. It remains to show that $-y$ is the *greatest* lower bound for A. Suppose z is another lower bound for A. Then, as above, $-z$ is an upper bound for B. Since y is the *least* upper bound for B, we have $y \leq -z$. Therefore $-y \geq z$. It follows that $-y$ is a greatest lower bound for A. □

Exercises.

7.4.1. Suppose that $A \subseteq \mathbb{R}$ has supremum M. Show that the set

$$B = \{5 - 2x : x \in A\}$$

has infimum $5 - 2M$.

7.4.2. Suppose A and B are nonempty subsets of $\mathbb{R}$ that are bounded above. Furthermore, suppose that $A \cap B \neq \varnothing$. Show that $A \cap B$ is bounded above and that

$$\sup(A \cap B) \leq \min\{\sup A, \sup B\}.$$

7.4.3. Suppose A is a subset of $\mathbb{R}$ with a maximum and minimum element, such that $\max A = \min A$. Prove that A has exactly one element.

7.4.4. Suppose $a, b \in \mathbb{R}$ with $a < b$. Prove that

$$\inf(a, b) = a \quad \text{and} \quad \sup(a, b) = b.$$

(Recall that $(a, b) = \{x \in \mathbb{R} : a < x < b\}$.)

7.4.5. Find the supremum and infimum of the set

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

or show that they do not exist.

Chapter 8

Injections, surjections, and bijections

In this chapter will we examine some important types of functions. Namely we will consider functions that are injective, surjective, or both. We will then discuss how we can identify the set of integers as a subset of the set of real numbers in a way that preserves all of the important operations and relations that we have discussed.

8.1 Injections, surjections, and bijections

Definition 8.1 (Injective, injection)**.** A function $f\colon A \to B$ is said to be *injective* (or to be an *injection*, or to be *one-to-one*) if

$$\forall x, y \in A,\ x \neq y \implies f(x) \neq f(y).$$

Equivalently (taking the contrapositive) f is injective if

$$\forall x, y \in A,\ f(x) = f(y) \implies x = y.$$

Example 8.2. If $c \in \mathbb{R}$, $c \neq 0$, then the function

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = cx,$$

is injective. To prove this, suppose $x, y \in \mathbb{R}$. Then

$$f(x) = f(y) \implies cx = cy \implies x = y,$$

where the last implication follows from Proposition 7.11 (alternatively, multiply both sides by c^{-1}). Thus f is injective.

Example 8.3. The function

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2,$$

is *not* injective. To prove that a function f is not injective, it is enough to find two elements x and y of the domain such that $x \neq y$ and $f(x) = f(y)$. In this case, we have $1 \neq -1$, but $f(1) = 1 = f(-1)$. Thus f is not injective.

Definition 8.4 (Surjective, surjection, image)**.** A function $f\colon A \to B$ is *surjective* (or is a *surjection*, or is *onto*) if

$$\forall b \in B\ \exists a \in A \text{ such that } f(a) = b.$$

For any subset $S \subseteq A$, the *image of S under f* is the set

$$f(S) := \{f(a) : a \in S\} \subseteq B.$$

The *image* of f is $f(A)$. In other words, the image of f is the image of the domain of f under f. Thus, f is surjective if and only if $f(A) = B$ (i.e. the image of f is equal to the codomain of f).

Example 8.5. The function

$$f\colon \mathbb{Z} - \{0\} \to \mathbb{N}, \quad f(x) = |x|,$$

is surjective. To prove this, note that, for all $x \in \mathbb{N}$, we have $f(x) = |x| = x$.

Definition 8.6 (Bijective, bijection)**.** A function is *bijective* (or is a *bijection*) if it is both injective and surjective.

Example 8.7. For any nonempty set A, we have the *identity function*

$$\mathrm{id}_A\colon A \to A, \quad \mathrm{id}_A(a) = a \text{ for all } a \in A.$$

This function is bijective.

Example 8.8. Consider the function

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = \frac{x}{3} + 1.$$

We will show that this function is bijective. Suppose $x, y \in \mathbb{R}$. Then

$$f(x) = f(y) \implies \frac{x}{3} + 1 = \frac{y}{3} + 1 \implies \frac{x}{3} + 1 - 1 = \frac{y}{3} + 1 - 1$$
$$\implies \frac{x}{3} = \frac{y}{3} \implies 3 \cdot \frac{x}{3} = 3 \cdot \frac{y}{3} \implies x = y.$$

So f is injective.

It remains to prove that f is surjective. Let $y \in \mathbb{R}$. We wish to find $x \in \mathbb{R}$ such that $f(x) = y$. Note that

$$f(x) = y \iff \frac{x}{3} + 1 = y \iff x = 3(y - 1).$$

Since $3(y-1) \in \mathbb{R}$ (by closure of $\mathbb{R}$ under addition and multiplication), it lies in the domain of f. We have

$$f\big(3(y-1)\big) = \frac{3(y-1)}{3} + 1 = y - 1 + 1 = y.$$

Therefore f is surjective.

Examples 8.9. (i) The function $f\colon \{0\} \to \{2, 5, -4\}$ given by $f(0) = -4$, is injective but not surjective.

(ii) The function $f\colon \{1, 2\} \to \{1\}$ given by $f(1) = f(2) = 1$ is surjective but not injective.

(iii) The function $f\colon \{1, 2\} \to \{1, 8\}$ given by $f(1) = f(2) = 8$ is neither surjective nor injective.

(iv) The function $f\colon \{-1, 1\} \to \{-2, 13\}$ given by $f(-1) = -2$, $f(1) = 13$, is bijective.

(v) The function $f\colon \mathbb{Z} \to \mathbb{Z}_{\geq 0}$, $f(n) = n^2$, is not injective since, for example $f(1) = 1 = f(-1)$. It is also not surjective, since, for example, there is no $n \in \mathbb{Z}$ such that $f(n) = 3$.

(vi) The function $f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$, $f(n) = n^2$, is injective but not surjective.

(vii) The function $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $f(x) = 3x$, is bijective.

(viii) The function $f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $f(x) = 3x + 1$ is injective, but not surjective. (For instance, its image does not contain 0.)

If $f\colon A \to B$ and $g\colon B \to C$, then their *composite* is the function

$$g \circ f\colon A \to C, \quad (g \circ f)(a) = g(f(a)) \text{ for all } a \in A.$$

Composition is the operation that takes two functions and returns their composite (i.e. the composite function is the result of composition).

Example 8.10. Define

$$f\colon \{1, 2, 3\} \to \{2, 4\}, \quad f(1) = f(2) = 4,\ f(3) = 2,$$
$$g\colon \{2, 4\} \to \{1, 8, 10\}, \quad g(2) = 8,\ g(4) = 10.$$

Then

$$g \circ f\colon \{1, 2, 3\} \to \{1, 8, 10\}$$

is given by

$$(g \circ f)(1) = g(f(1)) = g(4) = 10,$$
$$(g \circ f)(2) = g(f(2)) = g(4) = 10,$$
$$(g \circ f)(3) = g(f(3)) = g(2) = 8.$$

Example 8.11. If $f\colon A \to B$, then

$$\mathrm{id}_B \circ f = f \quad \text{and} \quad f \circ \mathrm{id}_A = f.$$

Proposition 8.12. *Suppose $f\colon A \to B$ and $g\colon B \to C$. So $g \circ f\colon A \to C$.*

(i) If f and g are both injective, then $g \circ f$ is injective.

(ii) If f and g are both surjective, then $g \circ f$ is surjective.

(iii) If f and g are both bijective, then $g \circ f$ is bijective.

Proof. (i) Suppose f and g are both injective. For $a_1, a_2 \in A$, we have

$$\begin{aligned} & (g \circ f)(a_1) = (g \circ f)(a_2) \\ \implies\ & g(f(a_1)) = g(f(a_2)) \\ \implies\ & f(a_1) = f(a_2) && \text{since } g \text{ is injective} \\ \implies\ & a_1 = a_2. && \text{since } f \text{ is injective} \end{aligned}$$

(ii) Suppose f and g are both surjective. Let $c \in C$. Since g is surjective, there exists $b \in B$ such that $g(b) = c$. Then, since f is surjective, there exists $a \in A$ such that $f(a) = b$. Then

$$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

Thus, for all $c \in C$, there exists $a \in A$ such that $(g \circ f)(a) = c$. So $g \circ f$ is surjective.

(iii) This follows from the previous two parts, by the definition of bijectivity. □

Definition 8.13 (Inverse functions)**.** Suppose $f\colon A \to B$.

(i) A *left inverse* of f is a function $g\colon B \to A$ such that

$$g \circ f = \mathrm{id}_A.$$

(ii) A *right inverse* of f is a function $g\colon B \to A$ such that

$$f \circ g = \mathrm{id}_B.$$

(iii) A *two-sided inverse* (or simply *inverse*) of f is a function that is both a left inverse and a right inverse of f.

Example 8.14. Consider the functions

$$\begin{aligned} f\colon \mathbb{Z}_{\geq 0} \to \mathbb{Z}, \quad f(x) = x, \\ g\colon \mathbb{Z} \to \mathbb{Z}_{\geq 0}, \quad g(x) = |x|. \end{aligned}$$

Then, for all $x \in \mathbb{Z}_{\geq 0}$, we have

$$(g \circ f)(x) = g(f(x)) = g(x) = |x| = x.$$

Thus

$$g \circ f = \mathrm{id}_{\mathbb{Z}_{\geq 0}},$$

and so g is a left inverse of f and f is a right inverse of g. However, $f \circ g \neq \mathrm{id}_{\mathbb{Z}}$ since, for example

$$(f \circ g)(-1) = f(g(-1)) = f(1) = 1 \neq -1 = \mathrm{id}_{\mathbb{Z}}(-1).$$

Therefore, g is *not* a right inverse of f and f is *not* a left inverse of g.

Example 8.15. Consider the functions

$$f\colon \mathbb{R} \to \mathbb{R}, \quad f(x) = 3x + 1,$$
$$g\colon \mathbb{R} \to \mathbb{R}, \quad g(x) = \frac{x-1}{3}.$$

Then

$$f \circ g = \mathrm{id}_{\mathbb{R}} \quad \text{and} \quad g \circ f = \mathrm{id}_{\mathbb{R}}.$$

Thus f is an inverse of g and g is an inverse of f.

Proposition 8.16. *Suppose f is a function.*

(i) The function f is injective if and only if f has a left inverse.

(ii) The function f is surjective if and only if f has a right inverse.

(iii) The function f is bijective if and only if f has an inverse.

Proof. (i) Suppose $f\colon A \to B$ is injective. Fix an $a_0 \in A$ and define a function $g\colon B \to A$ by

$$g(b) = \begin{cases} a & \text{if } b \text{ is in the image of } f \text{ and } f(a) = b, \\ a_0 & \text{otherwise.} \end{cases}$$

The function g is well-defined since f is injective, so if b is in the image of f, there is *exactly one* $a \in A$ such that $f(a) = b$. By construction we have $g \circ f = \mathrm{id}_A$, and so g is a left inverse of f.

Conversely, assume that $f\colon A \to B$ has a left inverse $g\colon B \to A$. Then, for $a_1, a_2 \in A$, we have

$$f(a_1) = f(a_2) \implies g(f(a_1)) = g(f(a_2)) \implies (g \circ f)(a_1) = (g \circ f)(a_2)$$
$$\implies \mathrm{id}_A(a_1) = \mathrm{id}_A(a_2) \implies a_1 = a_2.$$

Thus, f is injective.

(ii) Suppose $f\colon A \to B$ is surjective. We define a function $g\colon B \to A$ as follows. For each $b \in B$, choose an $a \in A$ such that $f(a) = b$ (which we can do since f is surjective) and define $g(b) = a$. Then, for all $b \in B$, we have

$$(f \circ g)(b) = f(g(b)) = f(a) = b,$$

and so g is a right inverse of f.

Conversely, suppose that $f\colon A \to B$ has a right inverse $g\colon B \to A$. Then, for all $b \in B$, we have

$$f(g(b)) = (f \circ g)(b) = \mathrm{id}_B(b) = b,$$

and so b is in the image of f. Since b was arbitrary, this proves that f is surjective.

(iii) Suppose $f\colon A \to B$ is bijective. Then we can define a function $g\colon B \to A$ as follows. For each b, there exists exactly one $a \in A$ such that $f(a) = b$ (since f is bijective). We define $g(b) = a$. Then, by construction, $(f \circ g)(b) = b$ for all $b \in B$, and $(g \circ f)(a) = a$ for all $a \in A$. So g is an inverse of f.

Conversely, suppose that f has an inverse. Then f is injective by (i) and surjective by (ii). Hence f is bijective. □

Proposition 8.17. *Suppose f has left inverse g and right inverse h. Then $g = h$, and so f is invertible with inverse g.*

Proof. Suppose $f\colon A \to B$ has left inverse $g\colon B \to A$ and right inverse $h\colon B \to A$. Then

$$g = g \circ \mathrm{id}_B = g \circ f \circ h = \mathrm{id}_A \circ h = h.$$ □

Corollary 8.18. *If a function is bijective, then its inverse is unique.*

Proof. Suppose f has two inverses g and h. Then g is a left inverse of f and h is a right inverse of f. Thus, the result follows from Proposition 8.17. □

Proposition 8.19. *Suppose A and B are sets. There exists an injection from A to B if and only if there exists a surjection from B to A.*

Proof. Suppose $f\colon A \to B$ is an injection. Then, by Proposition 8.16(i), f has a left inverse $g\colon B \to A$. So

$$g \circ f = \mathrm{id}_A. \tag{8.1}$$

This implies that g has a right inverse, and thus g is surjective by Proposition 8.16(ii). Similarly, if $g\colon B \to A$ is surjective, then g has a right inverse $f\colon A \to B$ satisfying (8.1). Thus f has a left inverse, hence f is injective. □

Exercises.

8.1.1. Define the function

$$g\colon \mathbb{R}_{\geq 0} \to \mathbb{R}, \quad g(x) = -3x + 4.$$

(i) Prove that g is injective.

(ii) What is the image of g? Write your answer as an interval and justify your answer.

(iii) Is g surjective?

8.1.2. Consider the function

$$f\colon \mathbb{R} \to \mathbb{R}_{\geq 0}, \quad f(x) = |2x + 3|.$$

(i) Is f injective? Justify your answer.

(ii) Is f surjective? Justify your answer.

(iii) Does f have a left inverse? If it does, give one and show that it is indeed a left inverse. Otherwise, justify why f does not have a left inverse.

(iv) Does f have a right inverse? If it does, give one and show that it is indeed a right inverse. Otherwise, justify why f does not have a right inverse.

8.1.3. Consider the function

$$f\colon \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, \quad f(x) = \frac{x}{3} + 1.$$

(i) Is f injective? Justify your answer.

(ii) Is f surjective? Justify your answer.

(iii) Does f have a left inverse? If it does, give one and show that it is indeed a left inverse. Otherwise, justify why f does not have a left inverse.

(iv) Does f have a right inverse? If it does, give one and show that it is indeed a right inverse. Otherwise, justify why f does not have a right inverse.

8.1.4. (i) Suppose $f\colon A \to B$ and $g\colon B \to C$ are functions, and that g is surjective. Does it follow that $g \circ f$ is surjective? If yes, give a proof. If not, give a counterexample.

(ii) Suppose $f\colon A \to B$ and $g\colon B \to C$ are functions, and that f is injective. Does it follow that $g \circ f$ is injective? If yes, give a proof. If not, give a counterexample.

(iii) Suppose $f\colon A \to B$ and $g\colon B \to C$ are functions such that $g \circ f$ is injective. Does it follow that f is injective? If yes, give a proof. If not, give a counterexample.

(iv) Suppose $f\colon A \to B$ and $g\colon B \to C$ are functions such that $g \circ f$ is surjective. Does it follow that g is surjective? If yes, give a proof. If not, give a counterexample.

8.1.5. Suppose that A and B are nonempty subsets of $\mathbb{R}$, and that $f\colon A \to B$ is a function satisfying

$$\forall a_1, a_2 \in A,\ \big(a_1 < a_2 \implies f(a_1) < f(a_2)\big).$$

(Such a function is said to be *strictly increasing*.) Prove that f is injective.

8.1.6. (i) Give an example of a function with two different left inverses.

(ii) Give an example of a function with two different right inverses.

8.1.7. (i) Suppose $f\colon A \to B$ and $g\colon B \to C$ both have left inverses. Prove that $g \circ f$ has a left inverse.

(ii) Suppose $f\colon A \to B$ and $g\colon B \to C$ both have right inverses. Prove that $g \circ f$ has a right inverse.

(iii) Suppose $f\colon A \to B$ and $g\colon B \to C$ both have inverses. Prove that $g \circ f$ has an inverse.

8.2 Embedding $\mathbb{Z}$ in $\mathbb{R}$

We introduced the set $\mathbb{Z}$ of integers and the set $\mathbb{R}$ of real numbers axiomatically. That is, we assumed that there existed sets with binary operations of addition and multiplication satisfying certain axioms. Because of this approach, there is *a priori* no connection between $\mathbb{Z}$ and $\mathbb{R}$. For example, the additive identity of $\mathbb{Z}$ is not related to the additive identity of $\mathbb{R}$ (and similarly for the multiplicative identities). For this reason, in this section we will denote the additive and multiplicative identities of $\mathbb{Z}$ by $0_{\mathbb{Z}}$ and $1_{\mathbb{Z}}$, and the additive and multiplicative identities of $\mathbb{R}$ by $0_{\mathbb{R}}$ and $1_{\mathbb{R}}$.

We will now briefly outline how we can view $\mathbb{Z}$ as a subset of $\mathbb{R}$ in a way that respects the operations of addition and multiplication. Further details can be found in [BG10, §9.2].

Definition 8.20 (Embedding of $\mathbb{Z}$ in $\mathbb{R}$)**.** We define a function $e\colon \mathbb{Z} \to \mathbb{R}$ as follows:

(i) We first define e on $\mathbb{Z}_{\geq 0}$ recursively. We define $e(0_{\mathbb{Z}}) = 0_{\mathbb{R}}$ and, assuming $e(n)$ is defined for some $n \in \mathbb{Z}_{\geq 0}$, we define

$$e(n + 1_{\mathbb{Z}}) := e(n) + 1_{\mathbb{R}}.$$

(ii) Then we define e on negative integers. For $k \in \mathbb{Z}$ with $k < 0$, we define

$$e(k) := -e(-k).$$

Proposition 8.21. *The function $e\colon \mathbb{Z} \to \mathbb{R}$ defined in Definition 8.20 has the following properties.*

(i) $e(1_{\mathbb{Z}}) = 1_{\mathbb{R}}$.

(ii) For all $k \in \mathbb{Z}$, $e(-k) = -e(k)$. (The function e preserves additive inverses.)

(iii) For all $m, k \in \mathbb{Z}$, we have $e(m+k) = e(m)+e(k)$. (The function e preserves addition.)

(iv) For all $m, k \in \mathbb{Z}$, we have $e(mk) = e(m)e(k)$. (The function e preserves multiplication.)

(v) For all $m, k \in \mathbb{Z}$, we have $m < k \iff e(m) < e(k)$. (The function e preserves order.)

(vi) e is injective.

Proof. See [BG10, §9.2]. □

By Proposition 8.21, the image $e(\mathbb{Z})$ of e is a subset of $\mathbb{R}$ that behaves exactly like $\mathbb{Z}$. In other words, e is a bijection between $\mathbb{Z}$ and a subset of $\mathbb{R}$, and this bijection preserves addition, multiplication, additive inverses, and order. Therefore, from now on, we will identify $\mathbb{Z}$ with this subset of $\mathbb{R}$ by identifying $n \in \mathbb{Z}$ with $e(n) \in \mathbb{R}$. In this way, we will think of $\mathbb{Z}$ as being a subset of $\mathbb{R}$.

Chapter 9

Limits

In this chapter, we introduce and discuss the concept of a *limit*. This is a crucial concept in mathematics, especially in the field of *analysis*, which includes differential and integral calculus. While limits are often treated in a intuitive way in calculus courses, we will work with the precise definition.

9.1 Unboundedness of the integers

In Proposition 2.7, we saw that $\mathbb{N}$ has no largest element. However, that does not immediately imply that $\mathbb{N}$ is not bounded above as a subset of $\mathbb{R}$, since we have not yet ruled out the possibility that there is some real number that is larger than all natural numbers.

Proposition 9.1. *The set $\mathbb{N}$ of natural numbers, considered as a subset of $\mathbb{R}$, is not bounded above.*

Proof. We prove the result by contradiction. Suppose $\mathbb{N}$ is bounded above. Then, by Axiom 7.35, $\mathbb{N}$ has a least upper bound u. Consider the interval

$$\left(u - \frac{1}{2}, u\right] = \left\{x \in \mathbb{R} : u - \frac{1}{2} < x \leq u\right\}.$$

If this interval did not contain any natural number, then $u - \frac{1}{2}$ would be an upper bound for $\mathbb{N}$, contradicting the assumption that u is a *least* upper bound. So there is some $n \in \mathbb{N}$ such that $n \in (u - \frac{1}{2}, u]$. Then

$$u - \frac{1}{2} < n \implies u < n + \frac{1}{2} < n + 1.$$

However, $n + 1 \in \mathbb{N}$, since $1 \in \mathbb{N}$ (by Proposition 2.4) and $\mathbb{N}$ is closed under addition (Axiom 2.1(i)), this contradicts our assumption that u is an upper bound. □

Corollary 9.2. *The set $\mathbb{Z}$ of integers is neither bounded above nor bounded below.*

Proof. Since $\mathbb{N} \subseteq \mathbb{Z}$, any upper bound for $\mathbb{Z}$ would also be an upper bound for $\mathbb{N}$, contradicting Proposition 9.1.

Now suppose, towards a contradiction, that $\mathbb{Z}$ is bounded below by b. Then, for all $n \in \mathbb{N}$, we have

$$-n \in \mathbb{Z} \implies b \leq -n \implies n \leq -b,$$

and so $\mathbb{N}$ would be bounded above by $-b$, again contradicting Proposition 9.1. □

Proposition 9.3. *For every $\varepsilon \in \mathbb{R}_{>0}$, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \varepsilon$.*

Proof. Suppose $\varepsilon \in \mathbb{R}_{>0}$. Then $\frac{1}{\varepsilon} \in \mathbb{R}_{>0}$ by Proposition 7.17(i). Therefore, by Proposition 9.1, there exist $n \in \mathbb{N}$ such that $n > \frac{1}{\varepsilon}$. Then, by Proposition 7.17(ii), we have $\frac{1}{n} < \varepsilon$. □

Exercises.

9.1.1. Consider the set

$$A = \left\{ 5 + \frac{3}{2n} : n \in \mathbb{N} \right\}$$

(i) Find the infimum of A or prove that it does not exist.

(ii) Find the minimum element of A or prove that it does not exist.

(iii) Find the maximum element of A or prove that it does not exist.

(iv) Find the supremum of A or prove that it does not exist.

9.2 Absolute value

We define the *absolute value* of real numbers just as we did for the integers in Section 6.1. Namely, for $x \in \mathbb{R}$, we define

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

So $|x| \in \mathbb{R}_{\geq 0}$ for all $x \in \mathbb{R}$.

Proposition 9.4. *For all $x, y \in \mathbb{R}_{\geq 0}$, we have*

$$x < y \iff x^2 < y^2.$$

Proof. Let $x, y \in \mathbb{R}_{\geq 0}$.

First suppose that $x < y$ so that $y - x \in \mathbb{R}_{>0}$. If $x = 0$, this implies that $y \in \mathbb{R}_{>0}$, and thus

$$y^2 > 0 = x^2$$

by Axiom 7.13(ii). On the other hand, if $x > 0$, then we have $y > x > 0$, and so $x + y \in \mathbb{R}_{>0}$ by Axiom 7.13(i). Thus

$$y^2 - x^2 = (y - x)(y + x) \in \mathbb{R}_{>0}$$

by Axiom 7.13(ii). So $x^2 < y^2$.

Conversely, suppose that $x^2 < y^2$, so that

$$(y - x)(y + x) = y^2 - x^2 \in \mathbb{R}_{>0}.$$

We cannot have $x = y = 0$, since this would imply $x^2 = 0 = y^2$. Thus, at least one of x and y is positive, and hence $x + y \in \mathbb{R}_{>0}$. Thus

$$y - x = \frac{y^2 - x^2}{y + x} \in \mathbb{R}_{>0},$$

and so $x < y$. □

Proposition 9.5. *For all $x \in \mathbb{R}$, we have $|x|^2 = x^2$.*

Proof. This proof is left as an exercise (Exercise 9.2.1). □

Proposition 9.6. *For all $x, y \in \mathbb{R}$, we have:*

(i) $|x| = 0$ *if and only if* $x = 0$,

(ii) $|xy| = |x|\,|y|$,

(iii) $-|x| \leq x \leq |x|$,

(iv) $|x + y| \leq |x| + |y|$ *(the* triangle inequality*)*,

(v) if $-y < x < y$, *then* $|x| < |y|$.

Proof. (i) See [BG10, Prop. 10.8(i)].

(ii) If $x, y \geq 0$, then $xy \geq 0$, and so

$$|xy| = xy = |x|\,|y|.$$

If $x \geq 0$ and $y < 0$, then $xy \leq 0$ and so

$$|xy| = -xy = x(-y) = |x|\,|y|.$$

The remaining cases, where $x < 0$, $y \geq 0$, and where $x, y < 0$ are similar and are left as an exercise.

(iii) If $x \geq 0$, then $|x| = x$ and so

$$-|x| = -x \leq 0 \leq x = |x| \implies -|x| \leq x \leq |x|.$$

On the other hand, if $x < 0$, then $|x| = -x$ and so

$$-|x| = -(-x) = x < 0 \leq |x| \implies -|x| \leq x \leq |x|.$$

(iv) We have

$$\begin{aligned} |x+y|^2 &= (x+y)^2 && \text{(by Proposition 9.5)} \\ &= x^2 + 2xy + y^2 \\ &= |x|^2 + 2xy + |y|^2 && \text{(by Proposition 9.5)} \\ &\leq |x|^2 + |2xy| + |y|^2 && \text{(by part (iii))} \\ &= |x|^2 + 2|x|\,|y| + |y|^2 && \text{(by part (ii))} \\ &= (|x| + |y|)^2. \end{aligned}$$

Thus, by Proposition 9.4, we have $|x+y| \leq |x| + |y|$.

(v) Suppose $-y < x < y$. Then, in particular, we have $-y < y$, which implies that $y > 0$ and so $|y| = y$. If $x \geq 0$, then

$$|x| = x < y = |y|.$$

On the other hand, if $x < 0$, then

$$|x| = -x < y = |y|,$$

where the inequality $-x < y$ follows from the assumption that $-y < x$. □

Proposition 9.7. *Suppose $x \in \mathbb{R}$ satisfies $0 \leq x \leq 1$. Furthermore suppose $m, n \in \mathbb{N}$ such that $m \geq n$. Then $x^m \leq x^n$.*

Proof. Let $0 \leq x \leq 1$ and fix $n \in \mathbb{N}$. Let $P(m)$ be the statement

$$x^m \leq x^n.$$

We will prove by induction on m that $P(m)$ is true for all $m \geq n$.

The base case, when $m = n$ is clearly true since $x^n \leq x^n$. Now suppose $k \geq n$ and $P(k)$ is true. Since $0 \leq x \leq 1$, we have $x^n \cdot x \leq x^n \cdot 1 = x^n$. So

$$x^{k+1} = x^k \cdot x \leq x^n \cdot x \leq x^n,$$

where the first inequality follows from the induction hypothesis. □

Exercises.

9.2.1. Prove Proposition 9.5. *Hint*: Consider the two cases $x < 0$ and $x \geq 0$.

9.2.2 ([BG10, Prop. 10.7]). Let $x, y \in \mathbb{R}$. Prove that $|x| < |y|$ if and only if $x^2 < y^2$.

9.2.3. Prove that for all $n \in \mathbb{N}$ and $x_1, x_2, \ldots, x_n \in \mathbb{R}$,

$$\left| \sum_{i=1}^{n} x_i \right| \leq \sum_{i=1}^{n} |x_i|.$$

9.3 Distance

In this section, we briefly discuss the idea of the distance between two real numbers. For $x, y \in \mathbb{R}$, we define the *distance* between x and y to be $|x - y|$. This matches our intuition of thinking of real numbers as points on the real line.

Proposition 9.8 (Properties of distance)**.** *Suppose* $x, y, z \in \mathbb{R}$.

(i) $|x - y| = 0 \iff x = y$. *(Distance satisfies the* separation *property.)*

(ii) $|x - y| = |y - x|$. *(Distance is* symmetric.*)*

(iii) $|x - z| \leq |x - y| + |y - z|$. *(The* triangle inequality.*)*

(iv) $|x - y| \geq \big||x| - |y|\big|$.

Proof. (i) By Proposition 9.6(i), we have

$$|x - y| = 0 \iff x - y = 0 \iff x = y.$$

(ii) By Proposition 9.6(ii), we have

$$|x - y| = |(-1)(y - x)| = |-1|\,|y - x| = 1 \cdot |y - x| = |y - x|.$$

(iii) By Proposition 9.6(iv), we have

$$|x - z| = |(x - y) + (y - z)| \leq |x - y| + |y - z|.$$

(iv) Switching the roles of x and y if necessary, we may assume that $|x| \geq |y|$. Then $\big||x| - |y|\big| = |x| - |y|$. Taking $z = 0$ in part (iii), we have

$$|x| = |x - 0| \leq |x - y| + |y - 0| = |x - y| + |y|,$$

and so

$$|x - y| \geq |x| - |y| = \big||x| - |y|\big|.$$

□

Proposition 9.9. *Let* $z \in \mathbb{R}_{\geq 0}$. *Then*

$$z = 0 \iff \forall \varepsilon \in \mathbb{R}_{>0},\ z < \varepsilon.$$

Proof. If $z = 0$, then $z < \varepsilon$ for all $\varepsilon \in \mathbb{R}_{>0}$. Now assume $z \neq 0$. Then $z > 0$. Thus, by Theorem 7.21, there exists an $\varepsilon \in \mathbb{R}$, such that $0 < \varepsilon < z$. Therefore, the statement $\forall \varepsilon \in \mathbb{R}_{>0},\ z < \varepsilon$ is false. □

Corollary 9.10. *For* $x, y \in \mathbb{R}$, *we have*

$$x = y \iff \forall \varepsilon > 0,\ |x - y| < \varepsilon.$$

Proof. We have

$$\begin{aligned} x = y &\iff |x - y| = 0 && \text{(Proposition 9.8(i))} \\ &\iff \forall \varepsilon > 0,\ |x - y| < \varepsilon. && \text{(Proposition 9.9 with } z = |x - y|) \end{aligned}$$

□

Exercises.

9.3.1. Prove that, for all $x, y \in \mathbb{R}$, we have $|x - y| \leq |x| + |y|$.

9.3.2. Suppose $z \in \mathbb{R}_{\geq 0}$. Prove that

$$z = 0 \iff \forall n \in \mathbb{N},\ z < \frac{1}{n}.$$

9.4 Limits

We are now ready to give the precise definition of the limit of a sequence.

Definition 9.11 (Limit of a sequence)**.** Let $(x_k)_{k=1}^{\infty}$ be a sequence in $\mathbb{R}$ and $L \in \mathbb{R}$. We say that $(x_k)_{k=1}^{\infty}$ *converges to* L if

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N} \text{ such that } \forall n \geq N,\ |x_n - L| < \varepsilon,$$

or, equivalently, if

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N} \text{ such that } \big(n \geq N \implies |x_n - L| < \varepsilon\big).$$

When $(x_k)_{k=1}^{\infty}$ converges to L, we call L the *limit* of the sequence (x_k) and we write

$$\lim_{k \to \infty} x_k = L.$$

We say that a sequence *converges* if there exists some L such that the sequence converges to L. If no such L exists, then we say the sequence *diverges*. Thus, the sequence (x_k) diverges if

$$\forall L \in \mathbb{R}\ \exists \varepsilon > 0 \text{ such that } \forall N \in \mathbb{N}\ \exists n \geq N \text{ such that } |x_n - L| \geq \varepsilon.$$

It can take some time to get used to the formal definition of a limit, but it is important that you master this concept. Intuitively, the sequence (x_k) converges to L if, given any distance ε, the terms of sequence are eventually within a distance ε of L.

Proposition 9.12. *We have*

$$\lim_{k \to \infty} \frac{1}{k} = 0.$$

Proof. Let $\varepsilon > 0$. By Proposition 9.1, there exists $N \in \mathbb{N}$ with $N > \frac{1}{\varepsilon}$. Then, for all $n \geq N$, we have

$$\left| \frac{1}{n} - 0 \right| = \frac{1}{n} \leq \frac{1}{N} < \varepsilon$$

Hence $\lim_{k \to \infty} \frac{1}{k} = 0$. □

Example 9.13. We will prove that

$$\lim_{k\to\infty} \frac{2k-3}{k} = 2.$$

First note that, for $n > 0$, we have

$$\left|\frac{2n-3}{n} - 2\right| = \left|\frac{2n-3}{n} - \frac{2n}{n}\right| = \left|\frac{-3}{n}\right| = \frac{3}{n}.$$

Fix $\varepsilon > 0$. By Proposition 9.1, there exists $N \in \mathbb{N}$ with $N > \frac{3}{\varepsilon}$. Then, for all $n \geq N$, we have

$$\left|\frac{2n-3}{n} - 2\right| = \frac{3}{n} \leq \frac{3}{N} < \varepsilon,$$

as desired.

Example 9.14. We will prove that

$$\lim_{k\to\infty} \frac{3k^2+8k-5}{4k^2+1} = \frac{3}{4}.$$

First note that

$$\left|\frac{3n^2+8n-5}{4n^2+1} - \frac{3}{4}\right| = \left|\frac{3n^2+8n-5}{4n^2+1} - \frac{3\left(n^2+\frac{1}{4}\right)}{4\left(n^2+\frac{1}{4}\right)}\right| = \left|\frac{8n-\frac{23}{4}}{4n^2+1}\right|.$$

Now, when $n \geq 1$, we have $8n \geq 8 > \frac{23}{4}$. Also, $0 < 4n^2 < 4n^2+1$. Thus,

$$\left|\frac{8n-\frac{23}{4}}{4n^2+1}\right| = \frac{8n-\frac{23}{4}}{4n^2+1} \leq \frac{8n}{4n^2} = \frac{2}{n}.$$

Now suppose $\varepsilon > 0$. By Proposition 9.1, there exists $N \in \mathbb{N}$ with $N > \frac{2}{\varepsilon}$. Then, for all $n \geq N$, we have

$$\left|\frac{3n^2+8n-5}{4n^2+1} - \frac{3}{4}\right| \leq \frac{2}{n} \leq \frac{2}{N} < \varepsilon,$$

as desired.

Example 9.15. We will show that the sequence $(x_k)_{k=1}^{\infty}$ given by $x_k = 2k+1$ diverges. So we need to show that it does not converge to *any* real number. Let $L \in \mathbb{R}$. We will prove by contradiction that the sequence does not converge to L.

Suppose that $\lim_{k\to\infty} x_k = L$. For $k \geq |L|$, we have, by the triangle inequality,

$$|x_k - L| + |L| \geq |x_k| = |2k+1| = 2k+1 \geq 2|L|+1,$$

and so

$$|x_k - L| \geq |L| + 1.$$

Therefore, if $\varepsilon \leq |L|+1$, no matter which $N \in \mathbb{N}$ we choose, we can always choose an n greater than both $|L|$ and N, and then we have

$$|x_n - L| \geq |L| + 1 \geq \varepsilon.$$

So the sequence (x_k) does not converge to L.

Proposition 9.16 (Uniqueness of limits)**.** *If a sequence converges, then its limit is unique. In other words, if a sequence $(x_k)_{k=1}^{\infty}$ converges to L_1 and to L_2, then $L_1 = L_2$.*

Proof. Suppose (x_k) converges to both L_1 and L_2. Choose $\varepsilon > 0$. Then there exists a natural number N_1 such that

$$n \geq N_1 \implies |x_n - L_1| < \frac{\varepsilon}{2}.$$

Similarly, there exists a natural number N_2 such that

$$n \geq N_2 \implies |x_n - L_2| < \frac{\varepsilon}{2}.$$

Let $N = \max\{N_1, N_2\}$. Then, for $n \geq N$, we have

$$|x_n - L_1| < \frac{\varepsilon}{2} \quad \text{and} \quad |x_n - L_2| < \frac{\varepsilon}{2},$$

and so, by the triangle inequality, we have

$$|L_1 - L_2| \leq |L_1 - x_n| + |x_n - L_2| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Since our choice of $\varepsilon > 0$ was arbitrary, we conclude from Corollary 9.10 that $L_1 = L_2$. □

Proposition 9.17. *Suppose $r \in \mathbb{N}$ and $(x_k)_{k=1}^{\infty}$ is a sequence of real numbers. Then $(x_k)_{k=1}^{\infty}$ converges to L if and only if $(x_{k+r})_{k=1}^{\infty}$ converges to L*

Proof. Suppose $\lim_{k\to\infty} x_k = L$. Let $\varepsilon > 0$. Then there exists $N \in \mathbb{N}$ such that

$$n \geq N \implies |x_n - L| < \varepsilon.$$

But then, for all $n \geq N$, we have $n + r > n \geq N$ and so

$$|x_{n+r} - L| < \varepsilon.$$

So $\lim_{k\to\infty} x_{k+r} = L$. The reverse implication is left as Exercise 9.4.9. □

Proposition 9.17 tells us that we can always ignore some finite number of terms at the beginning of a sequence when computing limits.

Proposition 9.18 (Bernoulli's inequality)**.** *For $x \in \mathbb{R}_{\geq 0}$ and $k \in \mathbb{Z}_{\geq 0}$, we have*

$$(1 + x)^k \geq 1 + kx.$$

Proof. The statement is clearly true for $k = 0$ and $k = 1$, so we assume $k \geq 2$. Although we only proved the Binomial Theorem for the integers (Theorem 4.12), the same proof shows that it also holds for $a, b \in \mathbb{R}$. Thus we have

$$(1 + x)^k = \sum_{m=0}^{k} \binom{k}{m} x^m = 1 + kx + \sum_{m=2}^{k} \binom{k}{m} x^m \geq 1 + kx.$$ □

Proposition 9.19. *If $x \in \mathbb{R}$ with $|x| < 1$, then $\lim_{k\to\infty} x^k = 0$.*

Proof. The case $x = 0$ is easy (see Proposition 9.25(i)), so we assume $0 < |x| < 1$. Then for $N \geq 0$, by Proposition 9.18, we have

$$\left(\frac{1}{|x|}\right)^N = \left(1 + \frac{1-|x|}{|x|}\right)^N \geq 1 + \left(\frac{1-|x|}{|x|}\right) N > \left(\frac{1-|x|}{|x|}\right) N. \tag{9.1}$$

Now suppose $\varepsilon > 0$. By Proposition 9.1, there exists a natural number N such that

$$N > \frac{|x|}{1-|x|}\,\frac{1}{\varepsilon}. \tag{9.2}$$

Then, for $n \geq N$, we have

$$\begin{aligned} |x^n - 0| &= |x|^n \\ &\leq |x|^N && \text{(by Proposition 9.7)} \\ &< \frac{|x|}{1-|x|}\,\frac{1}{N} && \text{(by (9.1))} \\ &< \varepsilon. && \text{(by (9.2))} \end{aligned}$$

□

Definition 9.20 (Bounded, increasing, decreasing, monotonic sequence)**.** Suppose $(x_k)_{k=1}^{\infty}$ is a sequence.

(i) The sequence is *bounded* if there exist $\ell, u \in \mathbb{R}$ such that $\forall k \in \mathbb{N}$, $\ell \leq x_k \leq u$. Equivalently, it is bounded if there exists $\ell \in \mathbb{R}$ such that $\forall k \in \mathbb{N}$, $|x_k| \leq \ell$.

(ii) The sequence is *increasing* if $x_{k+1} \geq x_k$ for all $k \in \mathbb{N}$.

(iii) The sequence is *decreasing* if $x_{k+1} \leq x_k$ for all $k \in \mathbb{N}$.

(iv) The sequence is *monotonic* if it is either increasing or decreasing.

Theorem 9.21. *Every monotonic bounded sequence converges.*

Proof. We will prove that every decreasing bounded sequence converges. The proof for increasing bounded sequences is analogous and can be found in [BG10, Th. 10.19].

Suppose $(x_k)_{k=1}^{\infty}$ is decreasing and bounded. Then the set

$$A = \{x_k : k \in \mathbb{N}\} \subseteq \mathbb{R}$$

is bounded. Thus, by Proposition 7.38, it has a greatest lower bound s. We will show that $\lim_{k\to\infty} x_k = s$.

Let $\varepsilon > 0$. Then $s + \varepsilon > s$, and so $s + \varepsilon$ is *not* a lower bound for A. Thus, there exists some $N \in \mathbb{N}$ such that $x_N < s + \varepsilon$. Since the sequence is decreasing, we have $x_n \leq x_N$ for all $n \geq N$. Therefore, for $n \geq N$, we have

$$s - \varepsilon < s \leq x_n \leq x_N < s + \varepsilon,$$

and so $|x_n - s| < \varepsilon$ by Proposition 9.6(v). □

Note that increasing sequences are always bounded below (by the first term), so they are bounded if and only if they are bounded above. Similarly, decreasing sequences are bounded if and only if they are bounded below.

Examples 9.22. (i) The sequence $\left(4+\frac{1}{n}\right)_{n=1}^{\infty}$ is decreasing and bounded below by 4. Therefore it converges.

(ii) The sequence $\left(8-\frac{2}{3k^2+5}\right)_{k=1}^{\infty}$ is increasing and bounded above by 8. Therefore it converges.

Proposition 9.23. *Suppose the sequence $(x_k)_{k=1}^{\infty}$ converges to L.*

(i) If $(x_k)_{k=1}^{\infty}$ is increasing, then $x_k \leq L$ for all $k \in \mathbb{N}$.

(ii) If $(x_k)_{k=1}^{\infty}$ is decreasing, then $x_k \geq L$ for all $k \in \mathbb{N}$.

Proof. We will prove part (i), since the proof of part (ii) is analogous.

Assume $(x_k)_{k=1}^{\infty}$ is increasing and $\lim_{k\to\infty} x_k = L$. We will prove the result by contradiction. Assume there exists $m \in \mathbb{N}$ such that $x_m > L$. Let $\varepsilon = x_m - L$. Then for any $N \in \mathbb{N}$, let $n = \max\{N, m\}$. So, in particular, $n \geq N$. Since the sequence is increasing, we have $x_n \geq x_m > L$. But then

$$|x_n - L| = x_n - L \geq x_m - L = \varepsilon.$$

Thus the sequence $(x_k)_{k=1}^{\infty}$ does not converge to L, which is a contradiction. □

Proposition 9.24. *Every convergent sequence is bounded.*

Proof. Suppose $(x_k)_{k=1}^{\infty}$ converges. Taking $\varepsilon = 1$ in the definition of a limit, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, we have $|x_n - L| < 1$. Note that

$$|x_n - L| < 1 \implies |x_n| - |L| \leq \big||x_n| - |L|\big| \leq |x_n - L| < 1 \implies |x_n| < |L| + 1,$$

where, in the second inequality after the first implication, we used Proposition 9.8(iv). Now let

$$M = \max\{|x_1|, |x_2|, \ldots, |x_{N-1}|, |L| + 1\},$$

which exists since the maximum of any finite set exists. Then we have $|x_k| \leq M$ for all $k \in \mathbb{N}$, and so the sequence is bounded. □

Proposition 9.25 (Arithmetic of limits)**.** *Suppose $\lim_{k\to\infty} a_k = A$, $\lim_{k\to\infty} b_k = B$, and $c \in \mathbb{R}$.*

(i) $\lim_{k\to\infty} c = c$.

(ii) $\lim_{k\to\infty}(ca_k) = cA$.

(iii) $\lim_{k\to\infty}(a_k + b_k) = A + B$.

(iv) $\lim_{k\to\infty}(a_k b_k) = AB$.

(v) If $A \neq 0$, then $\lim_{k\to\infty} \frac{1}{a_k} = \frac{1}{A}$.

Proof. We will prove parts (i), (iii), and (v). The proofs of the other parts can be found in [BG10, Prop. 10.23].

Proof of (i): For any $\varepsilon > 0$, we have $|c - c| = 0 < \varepsilon$, and so we can take any $N \in \mathbb{N}$ in the definition of a limit (Definition 9.11).

Proof of (iii): Let $\varepsilon > 0$. Then there exists $N_1 \in \mathbb{N}$ such that

$$n \geq N_1 \implies |a_n - A| < \frac{\varepsilon}{2},$$

and there exists $N_2 \in \mathbb{N}$ such that

$$n \geq N_2 \implies |b_n - B| < \frac{\varepsilon}{2}.$$

Define $N = \max\{N_1, N_2\}$. Then, for all $n \geq N$, we have

$$\begin{aligned} |(a_n + b_n) - (A + B)| &= |(a_n - A) + (b_n - B)| \\ &\leq |a_n - A| + |b_n - B| \qquad \text{(by the triangle inequality)} \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Proof of (v): Suppose $A \neq 0$. Choose $N_1 \in \mathbb{N}$ such that, for $n \geq N_1$, we have $|a_n - A| < \frac{|A|}{2}$. Note that

$$|a_n - A| < \frac{|A|}{2} \implies |A| - |a_n| \leq \big||A| - |a_n|\big| \leq |A - a_n| < \frac{|A|}{2} \implies \frac{|A|}{2} < |a_n|,$$

where, in the second inequality after the first implication, we used Proposition 9.8(iv). Thus, for all $n \geq N_1$, we have

$$0 < \frac{|A|}{2} < |a_n| \implies 0 < \frac{1}{|a_n|} < \frac{2}{|A|}.$$

Thus, for $n \geq N_1$,

$$\left|\frac{1}{a_n} - \frac{1}{A}\right| = \left|\frac{A - a_n}{A a_n}\right| = \frac{|A - a_n|}{|A|\,|a_n|} \leq \frac{2}{|A|^2}|A - a_n|.$$

Now let $\varepsilon > 0$. Since $\lim_{k\to\infty} a_k = A$, we can choose $N_2 \in \mathbb{N}$ such that

$$n \geq N_2 \implies |A - a_n| < \frac{|A|^2}{2}\varepsilon.$$

Define $N = \max\{N_1, N_2\}$. Then, for $n \geq N$, we have

$$\left|\frac{1}{a_n} - \frac{1}{A}\right| \leq \frac{2}{|A|^2}|A - a_n| < \frac{2}{|A|^2}\frac{|A|^2}{2}\varepsilon = \varepsilon. \qquad \square$$

Proposition 9.25 is extremely useful, since it allows us to compute new limits from old ones.

Proposition 9.26. *For $\ell \in \mathbb{N}$, we have*

$$\lim_{k\to\infty} \frac{1}{k^\ell} = 0.$$

Proof. We prove the result by induction on ℓ. The base case $\ell = 1$ is Proposition 9.12. Now assume $n \in \mathbb{N}$ and the result holds for $\ell = n$. Then, by Proposition 9.25(iv), we have

$$\lim_{k\to\infty} \frac{1}{k^{n+1}} = \left(\lim_{k\to\infty} \frac{1}{k}\right)\left(\lim_{k\to\infty} \frac{1}{k^n}\right) = 0 \cdot 0 = 0,$$

and so the result also holds for $\ell = n+1$. This completes the proof of the induction step. □

Example 9.27. We have

$$\begin{aligned}\lim_{k\to\infty} \frac{4k^2 - 5k + 2}{3k^2} &= \lim_{k\to\infty} \left(\frac{4k^2}{3k^2} + \frac{-5k}{3k^2} + \frac{2}{3k^2}\right) \\ &= \lim_{k\to\infty} \left(\frac{4}{3}\right) - \frac{5}{3}\left(\lim_{k\to\infty} \frac{1}{k}\right) + \frac{2}{3}\left(\lim_{k\to\infty} \frac{1}{k^2}\right) = \frac{4}{3} + 0 + 0 = \frac{4}{3}.\end{aligned}$$

Example 9.28. Consider the sequence $\left((-1)^k\right)_{k=1}^\infty$. This sequence is bounded since $|(-1)^k| \leq 1$ for all $k \in \mathbb{N}$. However, this sequence does *not* converge. We prove this by contradiction. Suppose $\lim_{k\to\infty}(-1)^k = L$. Then there exists $N \in \mathbb{N}$ such that

$$\forall n \geq N,\ |(-1)^n - L| < \frac{1}{2}.$$

Since $2N, 2N+1 > N$, we then have, by the triangle inequality,

$$2 = \left|(-1)^{2N} - (-1)^{2N+1}\right| \leq \left|(-1)^{2N} - L\right| + \left|L - (-1)^{2N+1}\right| < \frac{1}{2} + \frac{1}{2} = 1,$$

which is a contradiction.

Example 9.29. Consider the sequences $(a_k)_{k=1}^\infty$ and $(b_k)_{k=1}^\infty$, where

$$a_k = 2 - k \qquad \text{and} \qquad b_k = k.$$

Neither of these sequences is bounded, hence both sequences diverge by Proposition 9.24. However, $(a_k + b_k)_{k=1}^\infty$ is the constant sequence $(2)_{k=1}^\infty$, which converges to 2 by Proposition 9.25(i).

Exercises.

9.4.1. Using the definition of a limit directly, find

$$\lim_{k\to\infty} \frac{8}{3k}.$$

9.4.2. Using the definition of a limit directly, find

$$\lim_{k\to\infty} \frac{2k^2+3k-1}{5k^2+5}.$$

9.4.3. Suppose $(x_k)_{k=1}^{\infty}$, $(y_k)_{k=1}^{\infty}$, and $(z_k)_{k=1}^{\infty}$ are sequences satisfying

$$x_k \le y_k \le z_k \quad \text{for all } k \in \mathbb{N}.$$

Furthermore, suppose that $\lim_{k\to\infty} x_k = L = \lim_{k\to\infty} z_k$ for some $L \in \mathbb{R}$. Prove that $\lim_{k\to\infty} y_k = L$.

9.4.4. A function $f\colon \mathbb{R} \to \mathbb{R}$ is said to be *increasing* if

$$\forall x, y \in \mathbb{R},\ \big(x \le y \implies f(x) \le f(y)\big).$$

Prove that if $(x_k)_{k=1}^{\infty}$ is an increasing sequence and $f\colon \mathbb{R} \to \mathbb{R}$ is an increasing function whose image is bounded, then the sequence $(f(x_k))_{k=1}^{\infty}$ converges.

9.4.5. Let $(x_k)_{k=1}^{\infty}$ be a sequence and let $L \in \mathbb{R}$.

(i) Prove that if $\lim_{k\to\infty} x_k = L$, then $\lim_{k\to\infty} |x_k| = |L|$.

(ii) Give an example of a sequence $(x_k)_{k=1}^{\infty}$ that diverges, but for which the sequence $(|x_k|)_{k=1}^{\infty}$ converges.

9.4.6. Using any results we have proved, find

$$\lim_{k\to\infty} \frac{3k^3+8k^2-3k-11}{6k^3}.$$

9.4.7. Define a sequence $\{x_k\}_{k=1}^{\infty}$ by

$$x_k = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ 1 & \text{if } k \text{ is even.} \end{cases}$$

Prove that the sequence $\{x_k\}_{k=1}^{\infty}$ diverges.

9.4.8. Consider the sequence $(a_k)_{k=1}^{\infty}$, where $a_k = (-1)^k$. Find a sequence $(b_k)_{k=1}^{\infty}$ such that the sequence $(a_k + b_k)_{k=1}^{\infty}$ converges.

9.4.9. Complete the proof of Proposition 9.17 by showing that if $(x_{k+r})_{k=1}^{\infty}$ converges to L, then $(x_k)_{k=1}^{\infty}$ converges to L.

9.5 Square roots

The completeness axiom (Axiom 7.35) allows us to prove the existence of certain real numbers, such as square roots. For any $r \in \mathbb{R}_{>0}$, we define the *square root* of r to be

$$\sqrt{r} := \sup\{x \in \mathbb{R} : x^2 < r\}.$$

We define $\sqrt{0} := 0$.

Theorem 9.30. *For $r \in \mathbb{R}_{>0}$, the real number $\sqrt{r}$ is well-defined, positive, and $(\sqrt{r})^2 = r$.*

Sketch of proof. We will consider the case $r = 2$. The proof for other values of r is similar. We first prove that $\sqrt{2}$ is well-defined. Let

$$A = \{x \in \mathbb{R} : x^2 < 2\}.$$

So we want to show that $\sup A$ exists. Since $1^2 = 1 < 2$, we see that A is nonempty. Now,

$$x \geq 2 \implies x^2 \geq 4 > 2.$$

Thus, $x < 2$ for all $x \in A$. So A is bounded above. Therefore, by the completeness axiom (Axiom 7.35), the set A has a supremum. So $\sqrt{2}$ is well-defined.

It remains to prove that $(\sqrt{2})^2 = 2$. This involves showing that the assumptions $(\sqrt{2})^2 < 2$ or $(\sqrt{2})^2 > 2$ lead to contradictions, using the definition of supremum. See [BG10, Th. 10.25] for details. □

Remark 9.31. Note that $-\sqrt{2}$ is also a number whose square is equal to 2. The notation $\sqrt{2}$ means the *positive* square root.

Proposition 9.32. *Suppose $r \in \mathbb{R}_{\geq 0}$. Then the number $\sqrt{r}$ is unique. More precisely, if $x \in \mathbb{R}_{\geq 0}$ satisfies $x^2 = r$, then $x = \sqrt{r}$.*

Proof. First consider the case $r = 0$. By Axiom 7.13(ii), if $x > 0$, then $x^2 > 0$. Thus, $x = 0 = \sqrt{0}$ is the only solution to $x^2 = 0$ with $x \in \mathbb{R}_{\geq 0}$.

Now suppose $r > 0$ and $x \in \mathbb{R}_{\geq 0}$ satisfies $x^2 = r = (\sqrt{r})^2$. Then

$$0 = x^2 - (\sqrt{r})^2 = (x - \sqrt{r})(x + \sqrt{r}).$$

Since $x + \sqrt{r} > 0$, this implies that $x - \sqrt{r} = 0$, and so $x = \sqrt{r}$. □

Proposition 9.33. *If $r \in \mathbb{R}$, $r < 0$, then there is no $x \in \mathbb{R}$ such that $x^2 = r$.*

Proof. If $x = 0$, then $x^2 = 0 \neq r$. On the other hand, if $x \neq 0$, then by Proposition 2.11 for $\mathbb{R}$, we have $x^2 > 0$. Thus $x^2 \neq r$. □

Proposition 9.33 says that negative real numbers do not have real square roots. In future courses you will discuss the *complex numbers*. It will turn out that, when working over the complex numbers, *all* square roots exist. In particular, negative real numbers have square roots in the complex numbers.

Chapter 10

Rational and irrational numbers

In this chapter, we briefly discuss the concept of rational numbers, which are numbers that can be written as a quotient of two integers. We also consider irrational numbers.

10.1 Rational numbers

Definition 10.1. A real number $r \in \mathbb{R}$ is *rational* if $r = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$, $n \neq 0$. A real number that is not rational is *irrational*. The set of all rational numbers is denoted $\mathbb{Q}$.

Proposition 10.2. *We have $\mathbb{Z} \subseteq \mathbb{Q}$.*

Proof. For $n \in \mathbb{Z}$, we have $n = \frac{n}{1} \in \mathbb{Q}$. □

Proposition 10.3. *Any rational number $r \in \mathbb{Q}$ can be written in the form $r = \frac{m}{n}$ where $n > 0$ and m and n have no common factors (other than ± 1).*

Sketch of proof. Let $r \in \mathbb{Q}$. By definition $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$, $b \neq 0$. If $b < 0$, then we write $r = \frac{-a}{-b}$ and the denominator is positive. Thus, we can assume the denominator is positive. Then we factor the numerator and denominator as products of primes and cancel all common prime factors. □

When r is written in the form $r = \frac{m}{n}$ where $n > 0$ and m and n have no common factors, we say that the representation $\frac{m}{n}$ is in *lowest terms*.

Proposition 10.4. *Suppose $r, s \in \mathbb{Q}$. Then*

(i) $r + s \in \mathbb{Q}$,

(ii) $rs \in \mathbb{Q}$,

(iii) $-r \in \mathbb{Q}$,

(iv) $r - s \in \mathbb{Q}$,

(v) if $r \neq 0$, then $r^{-1} \in \mathbb{Q}$.

Proof. We can write $r = \frac{a}{b}$ and $s = \frac{c}{d}$ for some $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$. Then

$$r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad + bc}{bd} \in \mathbb{Q}.$$

This proves part (i). The proof of the remaining parts is left as an exercise. □

Theorem 10.5. *Suppose $x, y \in \mathbb{R}$ with $x < y$. Then there exists $r \in \mathbb{Q}$ such that $x < r < y$.*

Proof. If $x = 0$, then, by Proposition 9.3, we can find $n \in \mathbb{N}$ such that $x = 0 < \frac{1}{n} < y$.

Now assume $x > 0$. By Proposition 9.3, there exists $m \in \mathbb{N}$ such that $\frac{1}{m} < y - x$. Also, since $\mathbb{N}$ is unbounded, there exists $n \in \mathbb{N}$ with $n > mx$. By the well-ordering principle (Theorem 2.33), we can choose this n to be minimal, so that $n - 1 \leq mx < n$. Dividing by m, we have

$$\frac{n}{m} - \frac{1}{m} \leq x < \frac{n}{m}.$$

The left-hand inequality above implies

$$\frac{n}{m} \leq x + \frac{1}{m} < x + (y - x) = y.$$

Therefore we have

$$x < \frac{n}{m} < y,$$

as desired.

Now suppose $x < 0$. If $y > 0$, then we can simply take $r = 0$. Therefore, we assume $y \leq 0$. So we have $0 \leq -y < -x$. By the above, there is a rational number r such that $-y < r < -x$. Then $-r$ is also rational (by Proposition 10.4) and we have $x < -r < y$, as desired. □

Theorem 10.5 says that the rational numbers are *dense* in the real numbers. (The word *dense* is a term in the field of topology and applies in a more general context.)

Corollary 10.6. *There is no smallest positive rational number.*

Proof. We prove the result by contradiction. Suppose a is a smallest positive rational number. So $0 < a$. Then, by Theorem 10.5, there exists some $r \in \mathbb{Q}$ such that $0 < r < a$. This contradicts the fact that a is a smallest positive rational number. □

Exercises.

10.1.1 ([BG10, Prop. 11.2]). Let $x, y, z, w \in \mathbb{R}$ with $y \neq 0$ and $w \neq 0$. Prove that if $\frac{x}{y} = \frac{z}{w}$, then $xw = zy$.

10.1.2 ([BG10, Prop. 11.3]). Prove that if $x, y, z \in \mathbb{R}$ with $y \neq 0$ and $z \neq 0$, then $\frac{xz}{yz} = \frac{x}{y}$.

10.1.3 ([BG10, Prop. 11.5]). Let $m, n, s, t \in \mathbb{Z}$ be such that $n, t \neq 0$, and m and n do not have any common factors. Prove that if $\frac{m}{n} = \frac{s}{t}$, then m divides s and n divides t.

10.1.4 ([BG10, Prop. 11.7]). The rational number $\frac{m}{n} \in \mathbb{Q}$ is positive (i.e. $\frac{m}{n} \in \mathbb{R}_{>0}$) if and only if either $m > 0$ and $n > 0$, or $m < 0$ and $n < 0$.

10.2 Irrational numbers

While we already know rational numbers exist (e.g. the integers are rational numbers), we have not yet proven that any irrational numbers exist.

Proposition 10.7. *The real number $\sqrt{2}$ is irrational.*

Proof. We will prove the result by contradiction. By Proposition 10.3, we can write $\sqrt{2} = \frac{m}{n}$, where $m, n \in \mathbb{Z}$ have no common factors (other than ± 1). Then we have

$$\frac{m^2}{n^2} = \left(\frac{m}{n}\right)^2 = (\sqrt{2})^2 = 2 \implies m^2 = 2n^2.$$

Thus, 2 divides m^2. Then, by Euclid's Lemma (Proposition 6.31), 2 divides m. So there exists some $a \in \mathbb{Z}$ such that $2a = m$. Note that

$$2a = m \implies 2^2a^2 = m^2 = 2n^2 \implies 2a^2 = n^2.$$

So 2 divides n^2. Again, by Euclid's Lemma (Proposition 6.31), 2 divides n. But then 2 is a common factor of m and n, contradicting our assumption that m and n have no common factors. □

In fact, Proposition 10.7 can be generalized. An integer n is said to be a *perfect square* if $n = m^2$ for some $m \in \mathbb{Z}$. Then we have the following result.

Theorem 10.8. *If $a \in \mathbb{N}$ is not a perfect square, then $\sqrt{a}$ is irrational.*

Proof. The proof of this result is left as an exercise. *Hint*: Follow the argument in the proof of Proposition 10.7 using a prime factor of a. □

Example 10.9. The real number $\sqrt{2} + \sqrt{3}$ is irrational. We can prove this by contradiction. Suppose $\sqrt{2} + \sqrt{3} \in \mathbb{Q}$. Then

$$\left(\sqrt{2} + \sqrt{3}\right)^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} \in \mathbb{Q}.$$

So $5 + 2\sqrt{6} = a$ for some $a \in \mathbb{Q}$. But then $\sqrt{6} = \frac{a-5}{2} \in \mathbb{Q}$ by Proposition 10.4, contradicting Theorem 10.8.

Note that $\mathbb{Q}$ does *not* satisfy the completeness axiom (Axiom 7.35). For example, the set

$$\{r \in \mathbb{Q} : r^2 < 2\}$$

is bounded above by a rational number (say, by 2), but has no least upper bound in $\mathbb{Q}$. Of course, it has a least upper bound in $\mathbb{R}$, namely $\sqrt{2}$. Similarly, the irrational numbers do not satisfy the completeness axiom.

Exercises.

10.2.1 ([BG10, Prop. 11.13]). Let m and n be nonzero integers. Prove that $\frac{m}{n}\sqrt{2}$ is irrational.

Index

Bibliography

[BG10] Matthias Beck and Ross Geoghegan. *The Art of Proof*. Undergraduate Texts in Mathematics. Springer, 2010. http://dx.doi.org/10.1007/978-1-4419-7023-7.