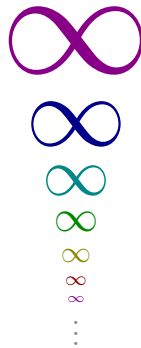# An infinite descent into pure mathematics

by Clive Newstead

Last updated on Wednesday 7th March 2018

Note to readers

Hello, and thank you for taking the time to read this quick introduction to the book! I would like to begin with an apology and a warning:

This book is still under development!

That is to say, there are some sections that are incomplete (notably Sections 6.2 and 6.3, and all of Chapter 8), as well as other sections which are currently much more terse than I would like them to be.

An up-to-date version of this book is be available from the following web page:

`http://infinitedescent.xyz`

As the book is undergoing constant changes, I advise that you do not print the notes in their entirety—if you must print them at all, then I suggest that you do it a few pages at a time, as required.

This book was designed with *inquiry* and *communication* in mind, as they are central to a good mathematical education. One of the upshots of this is that there are many exercises throughout the book, requiring a more active approach to learning, rather than passive reading. These exercises are a fundamental part of the book, and should be completed even if not required by the course instructor. Another upshot of these design principles is that solutions to exercises are not provided—a student seeking feedback on their solutions should speak to someone to get such feedback, be it another student, a teaching assistant or a course instructor.

Navigating the book

The material covered in Chapters 1 and 2 can be considered prerequisite for all subsequent material in the book; any introductory course in pure mathematics should cover at least these two chapters. The remaining chapters are a preview of other areas of pure mathematics. The dependencies between the sections in Chapters 3–8; dashed arrows indicate that a section is a *recommended*, rather than *required*, for another.
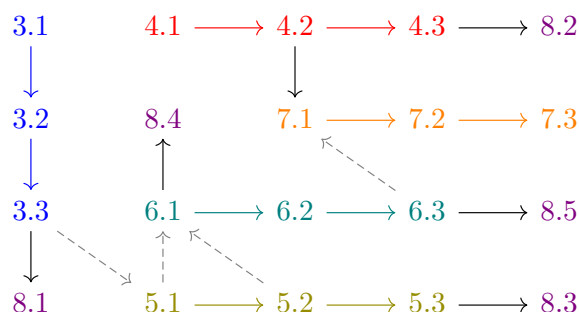
What the numbers, colours and symbols mean

Much of the material in this book is broken into enumerated items which, broadly speaking, fall into one of four categories: **results** (often followed by proofs), **definitions**, **examples** (including exercises for the reader), and **remarks**. These items are colour-coded as indicated in the previous sentence, and are enumerated according to their section—for example, Theorem 1.3.10 is in Section 1.3. Particularly important theorems, definitions and so on, appear in a ⊡box⊡.

You will also encounter the symbols □, ◁ and ⊛, whose meanings are as follows:

□ **End of proof.** It is standard in mathematical documents to identify when a proof has ended by drawing a small square or by writing '*Q.E.D.*' (The latter stands for *quod erat demonstrandum*, which is Latin for *what was to be shown*.)

◁ **End of item.** This is *not* a standard usage, and is included only to help you to identify when an item has finished and the main content of the book continues.

⊛ **Optional content.** Sections, exercises, results and proofs marked with this symbol can be skipped over. Usually this is because the content is very challenging, or is technical in a way that is mathematically necessary but educationally not very important.

Licence

Comments and corrections

Any feedback, be it from students, teaching assistants, instructors or any other readers, would be very much appreciated. Particularly useful are corrections of typographical errors, suggestions for alternative ways to describe concepts or prove theorems, and requests for new content (e.g. if you know of a nice example that illustrates a concept, or if there is a relevant concept you wish were included in the book). Such feedback can be sent to me by email (`cnewstead@cmu.edu`).

Contents

Acknowledgements

When I reflect on the time I have spent writing this book, I am overwhelmed by the number of people who have had some kind of influence on their content.

This book would never have come to exist were it not for Chad Hershock's course 38-801 *Evidence-Based Teaching in the Sciences* in Fall 2014. His course heavily influenced my approach to teaching, and it motivated me to write this book in the first place. Many of the pedagogical decisions I made when writing this book were informed by research that I was exposed to as a student in Chad's class.

I am extremely grateful to John Mackey for using this book for teaching 21-128 *Mathematical Concepts and Proofs* and 15-151 *Mathematical Foundations of Computer Science* in Fall 2016 and Fall 2017, and to David Offner and Mary Radcliffe for using it for teaching 21-127 *Concepts of Mathematics* in Spring 2017 and Spring 2018, respectively. Thanks to numerous discussions with John, David, Mary and their students over the course of these three semesters, the book has more than doubled in length, several sections have been restructured and improved, and dozens of typographical errors have been fixed.

Steve Awodey, my PhD advisor, has for a long time been a source of inspiration for me. Many of the choices I made when choosing how to present the material in this book are grounded in my desire to do mathematics *the right way*—it was this desire that led me to study category theory, and ultimately to become Steve's PhD student. I have learnt a great deal from him. Furthermore, I greatly appreciate his patience and flexibility in helping direct my research despite my busy teaching schedule and extracurricular interests (such as writing this book).

Perhaps unbeknownst to them, many insightful conversations with the following people have helped shape the material in this book in one way or another: Jeremy Avigad, Deb Brandon, Heather Dwyer, Thomas Forster, Will Gunther, Kate Hamilton, Jessica Harrell, Bob Harper, Brian Kell, Marsha Lovett, Ben Millwood, Ruth Poproski, Hilary Schuldt, Gareth Taylor, Katie Walsh, Emily Weiss and Andy Zucker.

The Department of Mathematical Sciences at Carnegie Mellon University has supporting me academically, professionally and financially throughout my PhD, and for presenting me with more opportunities than I could possibly have hoped for to develop as a teacher.

I would also like to thank everyone at the Eberly Center for Teaching Excellence and Educational Innovation at Carnegie Mellon University. I have been involved with the Eberly Center since my first semester as a graduate student in Fall 2013, originally as a client, and now in my third year working for them as a Graduate Teaching Fellow. During this time, I have learnt an incredible amount about teaching and learning and have transformed as a teacher. The Eberly Center's student-centred, evidence-based approach to the science of teaching and learning underlies everything I do as a teacher, including writing this book—its influence cannot be understated.

Finally, but importantly, I am grateful to the 800+ students who have already used this book to learn mathematics. Every time a student asks a question or points out an error, the book gets better. If you are a student using this book, please don't hesitate to send comments and corrections to me by email (`cnewstead@cmu.edu`).

<div align="right">

Clive Newstead
February 2018
Pittsburgh

</div>

Remark on originality

With a few exceptions mentioned below, this book was typed with my own ten fingers and without use of external resources.

Much of this book was written during the Fall 2016 semester, during which time I was a teaching assistant for John Mackey, who was using this book as course notes. I incorporated many of John's suggestions into the notes, particularly in Section 4.2 and throughout Chapter 7, and as a result, there is some overlap between the exercises in this book and the questions on his problem sheets.

Some fragments of the LaTeX code are adapted or copied directly from helpful posts made on the website *LaTeX Stack Exchange* (`http://tex.stackexchange.com`).

Chapter 1

Mathematical reasoning

1.1   Getting started

Before we can start proving things, we need to eliminate certain kinds of statements that we might try to prove. Consider the following statement:

This sentence is false.

Is it true or false? If you think about this for a couple of seconds then you'll get into a bit of a pickle.

Now consider the following statement:

The happiest donkey in the world.

Is it true or false? Well it's not even a sentence; it doesn't make sense to even *ask* if it's true or false!

Clearly we'll be wasting our time trying to write proofs of statements like the two listed above—we need to narrow our scope to statements that we might actually have a chance of proving (or perhaps refuting)! This motivates the following (informal) definition.

Definition 1.1.1

A **proposition** is a statement to which it is possible to assign a **truth value** ('true' or 'false'). If a proposition is true, a **proof** of the proposition is a logically valid argument demonstrating that it is true, which is pitched at such a level that a member of the intended audience can verify its correctness.

Thus the statements given above are not propositions because there is no possible way of assigning them a truth value. Note that, in Definition 1.1.1, all that matters is that it *makes sense* to say that it is true or false, regardless of whether it actually *is* true or false—the truth value of many propositions is unknown, even very simple ones.

Exercise 1.1.2

Think of an example of a true proposition, a false proposition, a proposition whose truth value you don't know, and a statement that is not a proposition.   ◁

Results in mathematical papers and textbooks may be referred to as *propositions*, but they may also be referred to as *theorems*, *lemmas* or *corollaries* depending on their intended usage.

- A **proposition** is an umbrella term which can be used for any result.

- A **theorem** is a key result which is particularly important.

- A **lemma** is a result which is proved for the purposes of being used in the proof of a theorem.

- A **corollary** is a result which follows from a theorem without much additional effort.

These are not precise definitions, and they are not meant to be—you could call every result a *proposition* if you wanted to—but using these words appropriately helps readers work out how to read a paper. For example, if you just want to skim a paper and find its key results, you'd look for results labelled as *theorems*.

It is not much good trying to prove results if we don't have anything to prove results about. With this in mind, we will now introduce the *number sets* and prove some results about them in the context of four topics, namely: division of integers, number bases, rational and irrational numbers, and polynomials. These topics will provide context for the rest of the material in Chapters 1 and 2.

We will not go into very much depth in this section. Rather, think of this as a warm-up exercise—a quick, light introduction, with more proofs to be provided in Chapter 1 and in future chapters.

Number sets

Later in this section, and then in much more detail in Section 2.2, we will encounter the notion of a *set*; a set can be thought of as being a collection of objects. This seemingly simple notion is fundamental to mathematics, and is so involved that we will not treat sets formally in the main body of the text—see Section B.2 for a formal viewpoint. For now, the following definition will suffice.

Definition 1.1.3 (to be revised in Definition 2.2.1)
A **set** is a collection of objects. The objects in the set are called **elements** of the set. If X is a set and x is an object, then we write $x \in X$ (LaTeX code: `x \in X`) to denote the assertion that x is an element of X.

The sets of concern to us first and foremost are the *number sets*—that is, sets whose elements are particular types of *number*. At this introductory level, many details will be

temporarily swept under the rug; we will work at a level of precision which is appropriate for our current stage, but still allows us to develop a reasonable amount of intuition.

In order to define the number sets, we will need three things: an infinite line, a fixed point on this line, and a fixed unit of length.

So here we go. Here is an infinite line:

The arrows indicate that it is supposed to extend in both directions without end. The points on the line will represent numbers (specifically, *real numbers*, a misleading term that will be defined in Definition 1.1.24). Now let's fix a point on this line, and label it '0':

$$0$$
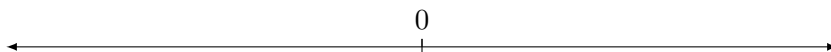
This point can be thought of as representing the number zero; it is the point against which all other numbers will be measured. Finally, let's fix a unit of length:

This unit of length will be used, amongst other things, to compare the extent to which the other numbers differ from zero.

Definition 1.1.4
The above infinite line, together with its fixed zero point and fixed unit length, constitute the (**real**) **number line**.

We will use the number line to construct five sets of numbers of interest to us:

- The set $\mathbb{N}$ of *natural numbers*—Definition 1.1.5;

- The set $\mathbb{Z}$ of *integers*—Definition 1.1.11;

- The set $\mathbb{Q}$ of *rational numbers*—Definition 1.1.23;

- The set $\mathbb{R}$ of *real numbers*—Definition 1.1.24; and

- The set $\mathbb{C}$ of *complex numbers*—Definition 1.1.30.

Each of these sets has a different character and is used for different purposes, as we will see both later in this section and throughout this book.

Natural numbers ($\mathbb{N}$)

The *natural numbers* are the numbers used for counting—they are the answers to questions of the form 'how many'—for example, I have *three* uncles, *one* dog and *zero* cats.

Counting is a skill humans have had for a very long time; we know this because there is evidence of people using tally marks tens of thousands of years ago. Tally marks provide one method of counting small numbers: starting with nothing, proceed through the objects you want to count one by one, and make a mark for every object. When you are finished, there will be as many marks as there are objects. We are taught from a young age to count with our fingers; this is another instance of making tally marks, where now instead of making a mark we raise a finger.

Making a tally mark represents an *increment* in quantity—that is, adding one. On our number line, we can represent an increment in quantity by moving to the right by the unit length. Then the distance from zero we have moved, which is equal to the number of times we moved right by the unit length, is therefore equal to the number of objects being counted.

Definition 1.1.5

The **natural numbers** are represented by the points on the number line which can be obtained by starting at 0 and moving right by the unit length any number of times:

$$
\begin{array}{ccccccc}
0 & 1 & 2 & 3 & 4 & 5 \\
\end{array}
$$
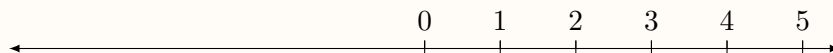
In more familiar terms, they are the *non-negative whole numbers*. We write $\mathbb{N}$ for the set of all natural numbers; thus, the notation '$n \in \mathbb{N}$' means that n is a natural number.

The natural numbers have very important and interesting mathematical structure, and are central to the material in Sections 1.3, 4.1 and 4.2. A more precise characterisation of the natural numbers will be provided in Section 1.3, and a mathematical construction of the set of natural numbers can be found in Definition B.2.3. Central to these more precise characterisations will be the notions of 'zero' and of 'adding one'—just like making tally marks.

Aside

Some authors define the natural numbers to be the *positive* whole numbers $(1, 2, 3, \ldots)$, excluding zero. We take 0 to be a natural number since our main use of the natural numbers will be for counting finite sets, and a set with nothing in it is certainly finite! That said, as with any mathematical definition, the choice about whether $0 \in \mathbb{N}$ or $0 \notin \mathbb{N}$ is a matter of taste or convenience, and is merely a convention—it is not something that can be proved

or refuted.   ◁

Number bases

Writing numbers down is something that may seem easy to you now, but it likely took you several years as a child to truly understand what was going on. Historically, there have been many different systems for representing numbers symbolically, called *numeral systems*. First came the most primitive of all, tally marks, appearing in the Stone Age and still being used for some purposes today. Thousands of years and hundreds of numeral systems later, there is one dominant numeral system, understood throughout the world: the **Hindu–Arabic numeral system**. This numeral system consists of ten symbols, called *digits*. It is a *positional* numeral system, meaning that the position of a symbol in a string determines its numerical value.

In English, the *Arabic numerals* are used as the ten digits:

$$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9$$

The right-most digit in a string is in the units place, and the value of each digit increases by a factor of ten moving to the left. For example, when we write '2812', the left-most '2' represents the number two thousand, whereas the last '2' represents the number two.

The fact that there are ten digits, and that the numeral system is based on powers of ten, is a biological accident corresponding with the fact that most humans have ten fingers. For many purposes, this is inconvenient. For example, ten does not have many positive divisors (only four)—this has implications for the ease of performing arithmetic; a system based on the number twelve, which has six positive divisors, might be more convenient. Another example is in computing and digital electronics, where it is more convenient to work in a *binary* system, with just two digits, which represent 'off' and 'on' (or 'low voltage' and 'high voltage'), respectively; arithmetic can then be performed directly using sequences of *logic gates* in an electrical circuit.

It is therefore worthwhile to have some understanding of positional numeral systems based on numbers other than ten. The mathematical abstraction we make leads to the definition of *base-b expansion*.

Definition 1.1.6

Let $b > 1$. The **base-b expansion** of a natural number n is the[a] string $d_r d_{r-1} \ldots d_0$ such that

- $n = d_r \cdot b^r + d_{r-1} \cdot b^{r-1} + \cdots + d_0 \cdot b^0$;

- $0 \leqslant d_i < b$ for each i; and

- If $n > 0$ then $d_r \neq 0$—the base-b expansion of zero is 0 in all bases b.

Certain number bases have names; for instance, the base-2, 3, 8, 10 and 16 expansions are respectively called *binary*, *ternary*, *octal*, *decimal* and *hexadecimal*.

---

[a]The use of the word 'the' is troublesome here, since it assumes that every natural number has only one base-b expansion. This fact actually requires proof—see Theorem 3.3.51.

Example 1.1.7

Consider the number 1023. Its decimal (base-10) expansion is 1023, since

$$1023 = 1 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$$

Its binary (base-2) expansion is 1111111111, since

$$1023 = 1 \cdot 2^9 + 1 \cdot 2^8 + 1 \cdot 2^7 + 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

We can express numbers in base-36 by using the ten usual digits 0 through 9 and the twenty-six letters A through Z; for instance, A represents 10, M represents 22 and Z represents 35. The base-36 expansion of 1023 is SF, since

$$1023 = 28 \cdot 36^1 + 15 \cdot 36^0 = \text{S} \cdot 36^1 + \text{F} \cdot 36^0$$

$\triangleleft$

Exercise 1.1.8

Find the binary, ternary, octal, decimal, hexadecimal and base-36 expansions of the number 21127, using the letters A–F as additional digits for the hexadecimal expansion and the letters A–Z as additional digits for the base-36 expansion. $\triangleleft$

We sometimes wish to specify a natural number in terms of its base-b expansion; we have some notation for this.

Notation 1.1.9

Let $b > 1$. If the numbers $d_0, d_1, \ldots, d_r$ are base-b digits (in the sense of Definition 1.1.6), then we write

$$d_r d_{r-1} \ldots d_{0\,(b)} = d_r \cdot b^r + d_{r-1} \cdot b^{r-1} + \cdots + d_0 \cdot b^0$$

for the natural number whose base-b expansion is $d_r d_{r-1} \ldots d_0$. If there is no subscript (b) and a base is not specified explicitly, the expansion will be assumed to be in base-10.

Example 1.1.10

Using our new notation, we have

$$1023 = 1111111111_{(2)} = 1101220_{(3)} = 1777_{(8)} = 1023_{(10)} = 3\mathrm{FF}_{(16)} = \mathrm{SF}_{(36)}$$

◁

Integers ($\mathbb{Z}$)

The *integers* can be used for measuring the difference between two instances of counting. For example, suppose I have five apples and five bananas. Another person, also holding apples and bananas, wishes to trade. After our exchange, I have seven apples and only one banana. Thus I have two more apples and four fewer bananas.

Since an increment in quantity can be represented by moving to the right on the number line by the unit length, a *decrement* in quantity can therefore be represented by moving to the *left* by the unit length. Doing so gives rise to the integers.

Definition 1.1.11

The **integers** are represented by the points on the number line which can be obtained by starting at 0 and moving in either direction by the unit length any number of times:

$$
\begin{array}{ccccccccccc}
-5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5
\end{array}
$$
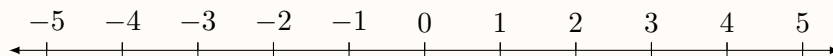
We write $\mathbb{Z}$ for the set of all integers; thus, the notation '$n \in \mathbb{Z}$' means that n is an integer.

The integers have such a fascinating structure that a whole chapter of this book is devoted to them—see Chapter 3. This is to do with the fact that, although you can add, subtract and multiply two integers and obtain another integer, the same is not true of division. This 'bad behaviour' of division is what makes the integers interesting. We will now see some basic results about division.

Division of integers

The motivation we will soon give for the definition of the rational numbers (Definition 1.1.23) is that the result of dividing one integer by another integer is not necessarily another integer. However, the result is *sometimes* another integer; for example, I can divide six apples between three people, and each person will receive an integral number of apples.

This makes division interesting: how can we measure the failure of one integer's divisibility by another? How can we deduce when one integer is divisible by another? What is the structure of the set of integers when viewed through the lens of division? This motivates Definition 1.1.12.

Definition 1.1.12 (to be repeated in Definition 3.1.4)

Let $a, b \in \mathbb{Z}$. We say b **divides** a, or that b is a **divisor** (or **factor**) of a, if $a = qb$ for some integer q.

Example 1.1.13

The integer 12 is divisible by 1, 2, 3, 4, 6 and 12, since

$$12 = 12 \cdot 1 = 6 \cdot 2 = 4 \cdot 3 = 3 \cdot 4 = 2 \cdot 6 = 1 \cdot 12$$

It is also divisible by the negatives of all of those numbers; for example, 12 is divisible by -3 since $12 = (-4) \cdot (-3)$. ◁

Exercise 1.1.14

Prove that 1 divides every integer, and that every integer divides 0. ◁

Using Definition 1.1.12, we can prove some general basic facts about divisibility.

Proposition 1.1.15

Let $a, b, c \in \mathbb{Z}$. If b divides a and c divides b, then c divides a.

Proof. Suppose that b divides a and c divides b. By Definition 1.1.12, it follows that

$$a = qb \quad \text{and} \quad b = rc$$

for some integers q and r. Using the second equation, we may substitute rc for b in the first equation, to obtain

$$a = q(rc)$$

But $q(rc) = (qr)c$, and qr is an integer, so it follows from Definition 1.1.12 that c divides a. □

Exercise 1.1.16

Let $a, b \in \mathbb{Z}$. Suppose that d divides a and d divides b. Prove that d divides $au + bv$, where u and v are any integers. ◁

It is not just interesting to know when one integer *does* divide another; however, proving that one integer *doesn't* divide another is much harder. Indeed, to prove that an integer b does not divide an integer a, we must prove that $b \neq qa$ for *any* integer q at all. We will look at methods for doing this in Section 1.2; these methods use the following extremely important result, which will underlie all of Chapter 3.

> **Theorem 1.1.17** (Division theorem, to be repeated in Theorem 3.1.1)
>
> Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There is exactly one way to write
>
> $$a = qb + r$$
>
> such that q and r are integers, and $0 \leqslant r < b$ (if $b > 0$) or $0 \leqslant r < -b$ (if $b < 0$).

The number q in Theorem 1.1.17 is called the **quotient** of a when divided by b, and the number r is called the **remainder**.

Example 1.1.18

The number 12 leaves a remainder of 2 when divided by 5, since $12 = 2 \cdot 5 + 2$.   ◁

Here's a slightly more involved example.

Proposition 1.1.19

Suppose an integer a leaves a remainder of r when divided by an integer b, and that $r > 0$. Then $-a$ leaves a remainder of $b - r$ when divided by b.

Proof. Suppose a leaves a remainder of r when divided by b. Then

$$a = qb + r$$

for some integer q. A bit of algebra yields

$$-a = -qb - r = -qb - r + (b - b) = -(q+1)b + (b - r)$$

Since $0 < r < b$, we have $0 < b - r < b$. Hence $-(q+1)$ is the quotient of $-a$ when divided by b, and $b - r$ is the remainder.   □

Exercise 1.1.20

Prove that if an integer a leaves a remainder of r when divided by an integer b, then a leaves a remainder of r when divided by $-b$.   ◁

We will finish this part on division of integers by connecting it with the material on number bases—we can use the division theorem (Theorem 1.1.17) to find the base-b expansion of a given natural number. It is based on the following observation: the natural number n whose base-b expansion is $d_r d_{r-1} \cdots d_1 d_0$ is equal to

$$d_0 + b(d_1 + b(d_2 + \cdots + b(d_{r-1} + bd_r)\cdots))$$

Moreover, $0 \leqslant d_i < b$ for all i. In particular n leaves a remainder of d_0 when divided by b. Hence

$$\frac{n - d_0}{b} = d_1 + d_2 b + \cdots + d_r b^{r-1}$$

The base-b expansion of $\frac{n-d_0}{b}$ is therefore

$$d_r d_{r-1} \cdots d_1$$

In other words, the remainder of n when divided by b is the last base-b digit of n, and then subtracting this number from n and dividing the result by b truncates the final digit. Repeating this process gives us d_1, and then d_2, and so on, until we end up with 0.

This suggests the following algorithm for computing the base-b expansion of a number n:

- **Step 1.** Let d_0 be the remainder when n is divided by b, and let $n_0 = \frac{n-d_0}{b}$ be the quotient. Fix $i = 0$.

- **Step 2.** Suppose n_i and d_i have been defined. If $n_i = 0$, then proceed to Step 3. Otherwise, define d_{i+1} to be the remainder when n_i is divided by b, and define $n_{i+1} = \frac{n_i - d_{i+1}}{b}$. Increment i, and repeat Step 2.

- **Step 3.** The base-b expansion of n, is

$$d_i d_{i-1} \cdots d_0$$

Example 1.1.21

We compute the base-17 expansion of 15213, using the letters A–G to represent the numbers 10 through 16.

- $15213 = 894 \cdot 17 + 15$, so $d_0 = 15 = \mathrm{F}$ and $n_0 = 894$.

- $894 = 52 \cdot 17 + 10$, so $d_1 = 10 = \mathrm{A}$ and $n_1 = 52$.

- $52 = 3 \cdot 17 + 1$, so $d_2 = 1$ and $n_2 = 3$.

- $3 = 0 \cdot 17 + 3$, so $d_3 = 3$ and $n_3 = 0$.

- The base-17 expansion of 15213 is therefore 31AF.

A quick verification gives

$$31\mathrm{AF}_{(17)} = 3 \cdot 17^3 + 1 \cdot 17^2 + 10 \cdot 17 + 15 = 15213$$

as desired. ◁

Exercise 1.1.22

Find the base-17 expansion of $408\,735\,787$ and the base-36 expansion of $1\,442\,151\,747$. ◁

Rational numbers ($\mathbb{Q}$)

Bored of eating apples and bananas, I buy a pizza which is divided into eight slices. A friend and I decide to share the pizza. I don't have much of an appetite, so I eat three slices and my friend eats five. Unfortunately, we cannot represent the proportion of the pizza each of us has eaten using natural numbers or integers. However, we're not far off: we can count the number of equal parts the pizza was split into, and of those parts, we can count how many we had. On the number line, this could be represented by splitting the unit line segment from 0 to 1 into eight equal pieces, and proceeding from there. This kind of procedure gives rise to the *rational numbers*.

Definition 1.1.23
The **rational numbers** are represented by the points at the number line which can be obtained by dividing any of the unit line segments between integers into an equal number of parts.

$$-5 \quad -4 \quad -3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5$$
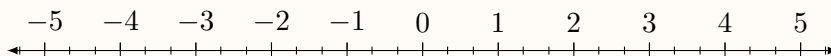
The rational numbers are those of the form $\frac{a}{b}$, where $a, b \in \mathbb{Z}$ and $b \neq 0$. We write $\mathbb{Q}$ for the set of all rational numbers; thus, the notation '$q \in \mathbb{Q}$' means that q is a rational number.

The rational numbers are a very important example of a type of algebraic structure known as a *field*—they are particularly central to algebraic number theory and algebraic geometry.

Real numbers ($\mathbb{R}$)

Quantity and change can be measured in the abstract using *real numbers*.

Definition 1.1.24
The **real numbers** are the points on the number line. We write $\mathbb{R}$ for the set of all real numbers; thus, the notation '$a \in \mathbb{R}$' means that a is a real number.

The real numbers are central to real analysis, a branch of mathematics introduced in Chapter 6. They turn the rationals into a *continuum* by 'filling in the gaps'—specifically, they have the property of *completeness*, meaning that if a quantity can be approximated with arbitrary precision by real numbers, then that quantity is itself a real number.

We can define the basic arithmetic operations (addition, subtraction, multiplication and division) on the real numbers, and a notion of ordering of the real numbers, in terms of the infinite number line.

- **Ordering.** A real number a is less than a real number b, written $a < b$, if a lies to the left of b on the number line. The usual conventions for the symbols $\leqslant$ (LaTeX code: `\le`), $>$ and $\geqslant$ (LaTeX code: `\ge`) apply, for instance '$a \leqslant b$' means that either $a < b$ or $a = b$.

- **Addition.** Suppose we want to add a real number a to a real number b. To do this, we *translate* a by b units to the right—if $b < 0$ then this amounts to translating a by an equivalent number of units to the left. Concretely, take two copies of the number line, one above the other, with the same choice of unit length; move the 0 of the lower number line beneath the point a of the upper number line. Then $a + b$ is the point on the upper number line lying above the point b of the lower number line.

  Here is an illustration of the fact that $(-3) + 5 = 2$:
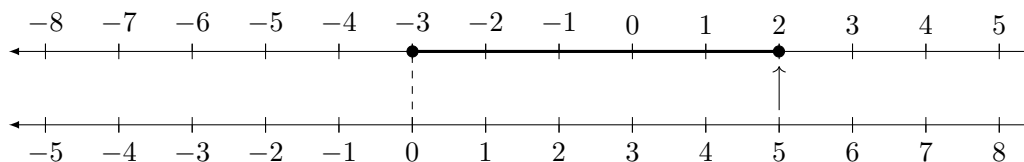
- **Multiplication.** This one is fun. Suppose we want to multiply a real number a by a real number b. To do this, we *scale* the number line, and perhaps *reflect* it. Concretely, take two copies of the number line, one above the other; align the 0 points on both number lines, and stretch the lower number line evenly until the point 1 on the lower number line is below the point a on the upper number line—note that if $a < 0$ then the number line must be reflected in order for this to happen. Then $a \cdot b$ is the point on the upper number line lying above b on the lower number line.

  Here is an illustration of the fact that $5 \cdot 4 = 20$.
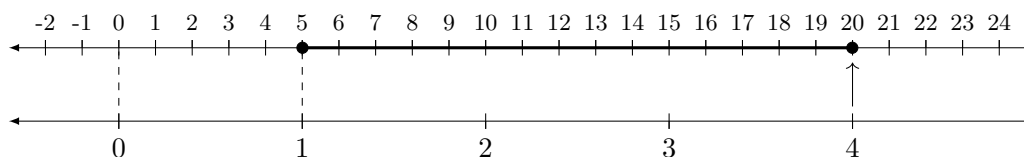
and here is an illustration of the fact that $(-5) \cdot 4 = -20$:
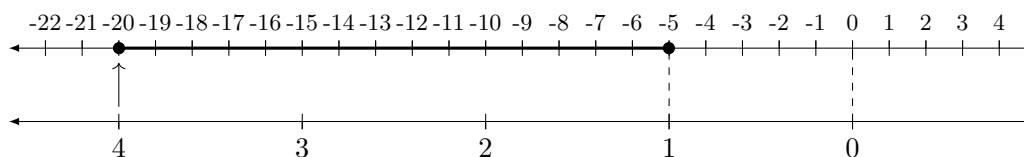
Exercise 1.1.25

Interpret the operations of subtraction and division as geometric transformations of the real number line.   ◁

We will take for granted the arithmetic properties of the real numbers in this section, waiting until Section 6.1 to sink our teeth into the details. For example, we will take for granted the basic properties of rational numbers, for instance

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Rational and irrational numbers

Before we can talk about irrational numbers, we should say what they are.

Definition 1.1.26
An **irrational number** is a real number that is not rational.

Unlike $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, there is no standard single letter expressing the irrational numbers. However, by the end of Section 2.2, we will be able to write the set of irrational numbers as $\mathbb{R} \setminus \mathbb{Q}$.

Note in particular that 'irrational' does not simply mean 'not rational'—that would imply that all complex numbers which are not real are irrational—rather, the term 'irrational' means 'real and not rational'.

Proving that a real number is *irrational* is not particularly easy. We will get our foot in the door by allowing ourselves to assume the following result, which is proved in Proposition 1.3.38.

Proposition 1.1.27
The real number $\sqrt{2}$ is irrational.   □

We can use the fact that $\sqrt{2}$ is irrational to prove some facts about the relationship between rational numbers and irrational numbers.

Proposition 1.1.28
Let a and b be irrational numbers. It is possible that ab be rational.

Proof. Let $a = b = \sqrt{2}$. Then a and b are irrational, and $ab = 2 = \frac{2}{1}$, which is rational. □

Exercise 1.1.29
Let r be a rational number and let a be an irrational number. Prove that it is possible that ra be rational, and it is possible that ra be irrational. ◁

Complex numbers ($\mathbb{C}$)

We have seen that multiplication by real numbers corresponds with scaling and reflection of the number line—scaling alone when the multiplicand is positive, and scaling with reflection when it is negative. We could alternatively interpret this reflection as a *rotation* by half a turn, since the effect on the number line is the same. You might then wonder what happens if we rotate by arbitrary angles, rather than only half turns.

What we end up with is a *plane* of numbers, not merely a line—see page 28. Moreover, it happens that the rules that we expect arithmetic operations to satisfy still hold—addition corresponds with translation, and multiplication corresponds with scaling and rotation. This resulting number set is that of the *complex numbers*.

Definition 1.1.30
The **complex numbers** are those obtained by the non-negative real numbers upon rotation by any angle about the point 0.

There is a particularly important complex number, i, which is the point in the complex plane exactly one unit above 0—this is illustrated on page 28. Multiplication by i has the effect of rotating the plane by a quarter turn anticlockwise. In particular, we have $i^2 = i \cdot i = -1$; the complex numbers have the astonishing property that square roots of *all* complex numbers exist (including all the real numbers).

In fact, every complex number can be written in the form $a + bi$, where $a, b \in \mathbb{R}$; this number corresponds with the point on the complex plane obtained by moving a units to the right and b units up, reversing directions as usual if a or b is negative. Arithmetic on the complex numbers works just as with the real numbers; in particular, using the fact that $i^2 = -1$, we obtain

$$(a + bi) + (c + di) = (a + c) + (b + d)i \quad \text{and} \quad (a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$$
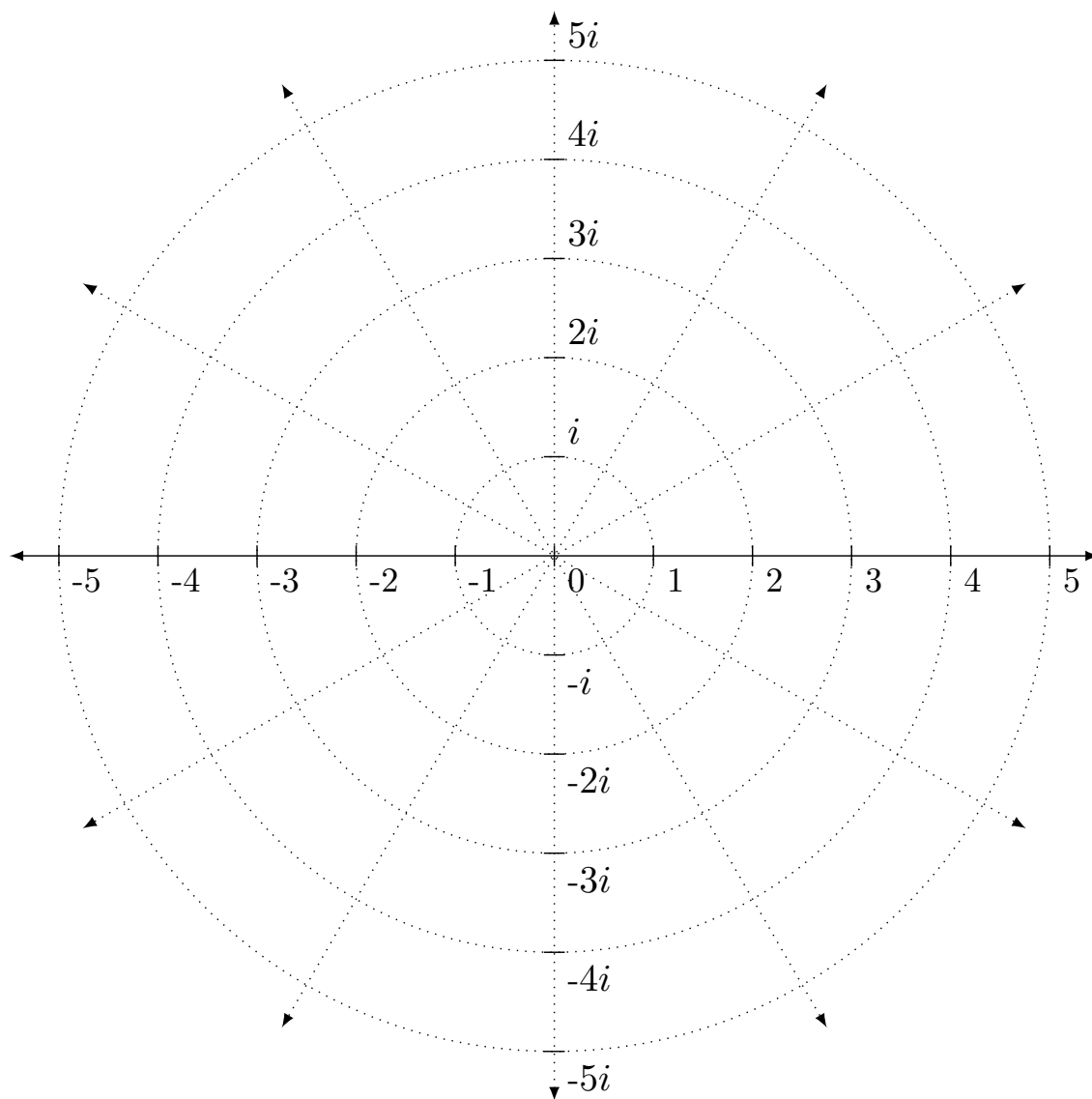
Figure 1.1: Illustration of the complex plane, with some points labelled.

We will discuss complex numbers further in the portion of this section on polynomials below, and in Sections B.2 and 8.4.

Polynomials

The integers, rational numbers, real numbers and complex numbers are all examples of *rings*, which means that they come equipped with nicely behaving notions of addition, subtraction and multiplication.

Definition 1.1.31
Let A be one $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. (More generally, A could be any ring—see Section 8.1.) A (**univariate**) **polynomial over** A in the **indeterminate** x is an expression of the form

$$a_0 + a_1 x + \cdots + a_n x^n$$

where $n \in \mathbb{N}$ and each $a_k \in A$. The numbers a_k are called the **coefficients** of the polynomial. If not all coefficients are zero, the largest value of k for which $a_k \neq 0$ is called the **degree** of the polynomial. By convention, the degree of the polynomial 0 is $-\infty$.

Polynomials of degree 1, 2 and 3 are called *linear*, *quadratic* and *cubic* polynomials, respectively.

Example 1.1.32
The following expressions are all polynomials:

$$3 \qquad 2x - 1 \qquad (3+i)x^2 - x$$

Their degrees are 0, 1 and 2, respectively. The first two are polynomials over $\mathbb{Z}$, and the third is a polynomial over $\mathbb{C}$. ◁

Exercise 1.1.33
Write down a polynomial of degree 4 over $\mathbb{R}$ which is not a polynomial over $\mathbb{Q}$. ◁

Notation 1.1.34
Instead of writing out the coefficients of a polynomial each time, we may write something like $p(x)$ or $q(x)$. The '(x)' indicates that x is the indeterminate of the polynomial. If α is a number[a] and $p(x)$ is a polynomial in indeterminate x, we write $p(\alpha)$ for the result of **substituting** α for x in the expression $p(x)$.

---

[a] When dealing with polynomials, we will typically reserve the letter x for the indeterminate variable, and use the Greek letters α, β, γ (LaTeX code: `\alpha, \beta, \gamma`) for numbers to be substituted into a polynomial.

Note that, if A is any of the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ and $p(x)$ is a polynomial over A, then $p(\alpha) \in A$ for all $\alpha \in A$.

Example 1.1.35

Let $p(x) = x^3 - 3x^2 + 3x - 1$. Then $p(x)$ is a polynomial over $\mathbb{Z}$ with indeterminate x. For any integer α, the value $p(\alpha)$ will also be an integer. For example

$$p(0) = 0^3 - 3 \cdot 0^2 + 3 \cdot 0 - 1 = -1 \quad \text{and} \quad p(3) = 3^3 - 3 \cdot 3^2 + 3 \cdot 3 - 1 = 8$$

◁

Definition 1.1.36

Let $p(x)$ be a polynomial. A **root** of $p(x)$ is a complex number α such that $p(\alpha) = 0$.

The *quadratic formula* (Theorem 1.2.6) tells us that the roots of the polynomial $x^2 + ax + b$, where $a, b \in \mathbb{C}$, are precisely the complex numbers

$$\frac{-a + \sqrt{a^2 - 4b}}{2} \quad \text{and} \quad \frac{-a - \sqrt{a^2 - 4b}}{2}$$

Note our avoidance of the symbol '$\pm$', which is commonly found in discussions of quadratic polynomials. The symbol '$\pm$' is dangerous because it may suppress the word 'and' or the word 'or', depending on context—this kind of ambiguity is not something that we will want to deal with when discussing the logical structure of a proposition in Sections 1.2 and 2.1.

Example 1.1.37

Let $p(x) = x^2 - 2x + 5$. The quadratic formula tells us that the roots of p are

$$\frac{2 + \sqrt{4 - 4 \cdot 5}}{2} = 1 + \sqrt{-4} = 1 + 2i \quad \text{and} \quad \frac{2 - \sqrt{4 - 4 \cdot 5}}{2} = 1 - \sqrt{-4} = 1 - 2i$$

The numbers $1 + 2i$ and $1 - 2i$ are related in that their real parts are equal and their imaginary parts differ only by a sign. Exercise 1.1.38 generalises this observation. ◁

Exercise 1.1.38

Let $\alpha = a + bi$ be a complex number, where $a, b \in \mathbb{R}$. Prove that α is the root of a quadratic polynomial over $\mathbb{R}$, and find the other root of this polynomial. ◁

The following exercise proves the well-known result which classifies the number of real roots of a polynomial over $\mathbb{R}$ in terms of its coefficients.

Exercise 1.1.39
Let $a, b \in \mathbb{R}$ and let $p(x) = x^2 + ax + b$. The value $\Delta = a^2 - 4b$ is called the **discriminant** of p. Prove that p has two roots if $\Delta \neq 0$ and one root if $\Delta = 0$. Moreover, if $a, b \in \mathbb{R}$, prove that p has no real roots if $\Delta < 0$, one real root if $\Delta = 0$, and two real roots if $\Delta > 0$. ◁

Example 1.1.40
Consider the polynomial $x^2 - 2x + 5$. Its discriminant is equal to $(-2)^2 - 4 \cdot 5 = -16$, which is negative. Exercise 1.1.39 tells us that it has two roots, neither of which are real. This was verified by Example 1.1.37, where we found that the roots of $x^2 - 2x + 5$ are $1 + 2i$ and $1 - 2i$.

Now consider the polynomial $x^2 - 2x - 3$. Its discriminant is equal to $(-2)^2 - 4 \cdot (-3) = 16$, which is positive. Exercise 1.1.39 tells us that it has two roots, both of which are real; and indeed

$$x^2 - 2x - 3 = (x + 1)(x - 3)$$

so the roots of $x^2 - 2x - 3$ are -1 and 3. ◁

1.2 Elementary proof techniques

There are many facets to mathematical proof, ranging from questions of how much detail to provide and what assumptions can be made, to questions of how to go about solving a particular problem and what steps are logically valid. This section provides some tools for answering the latter issues, but the proof techniques we will look at here are not exhaustive, by any means.

If this section is successful, then it will feel somewhat like all we are doing is stating the obvious. However, when it comes to writing your own proofs, this feeling of obviousness will likely disappear—it is when this happens that the usefulness of the proof techniques in this section will become apparent.

Assumptions and goals

Every mathematical proof is written in the context of certain *assumptions* being made, and certain *goals* to be achieved.

- **Assumptions** are the propositions which are known to be true, or which we are assuming to be true for the purposes of proving something. They include theorems that have already been proved, prior knowledge which is assumed of the reader, and assumptions which are explicitly made using words like 'suppose' or 'assume'.

- **Goals** are the propositions we are trying to prove in order to complete the proof of a result, or perhaps just a step in the proof.

With every phrase we write, our assumptions and goals change. This is perhaps best illustrated by example. In Example 1.2.1 below, we will examine the proof of Proposition 1.1.15 in detail, so that we can see how the words we wrote affected the assumptions and goals at each stage in the proof. We will indicate our assumptions and goals at any given stage using tables—the assumptions listed will only be those assumptions which are made explicitly; prior knowledge and previously proved theorems will be left implicit.

Example 1.2.1

The statement of Proposition 1.1.15 was as follows:

> Let $a, b, c \in \mathbb{Z}$. If b divides a and c divides b, then c divides a.

The set-up of the proposition instantly gives us our initial assumptions and goals:

Assumptions	Goals
$a, b, c \in \mathbb{Z}$	If b divides a and c divides b, then c divides a

We will now proceed through the proof, line by line, to see what effect the words we wrote had on the assumptions and goals.

Since our goal was an expression of the form 'if... then...', it made sense to start by assuming the 'if' statement, and using that assumption to prove the 'then' statement. As such, the first thing we wrote in our proof was:

> Suppose that b divides a and c divides b.

Our updated assumptions and goals are reflected in the following table.

Assumptions	Goals
$a, b, c \in \mathbb{R}$	c divides a
b divides a	
c divides b	

Our next step in the proof was to unpack the definitions of 'b divides a' and 'c divides b', giving us more to work with.

> Suppose that b divides a and c divides b. By Definition 1.1.12, it follows that
>
> $$a = qb \quad \text{and} \quad b = rc$$
>
> for some integers q and r.

This introduces two new variables q, r and allows us to replace the assumptions 'b divides a' and 'c divides b' with their definitions.

Assumptions	Goals
$a, b, c, q, r \in \mathbb{R}$	c divides a
$a = qb$	
$b = rc$	

At this point we have pretty much exhausted all of the assumptions we can make, and so our attention turns towards the goal—that is, we must prove that c divides a. At this

point, it helps to 'work backwards' by unpacking the goal: what does it mean for c to divide a? Well, by Definition 1.1.12, we need to prove that a is equal to some integer multiplied by c—this will be reflected in the following table of assumptions and goals.

Since we are now trying to express a in terms of c, it makes sense to use the equations we have relating a with b, and b with c, to relate a with c.

Suppose that b divides a and c divides b. By Definition 1.1.12, it follows that

$$a = qb \quad \text{and} \quad b = rc$$

for some integers q and r. Using the second equation, we may substitute rc for b in the first equation, to obtain

$$a = q(rc)$$

We are now very close, as indicated in the following table.

Assumptions	Goals
$a, b, c, q, r \in \mathbb{R}$	$a = [\text{some integer}] \cdot c$
$a = qb$	
$b = rc$	
$a = q(rc)$	

Our final step was to achieve the goal—namely, to express a as an integer multiplied by c:

Suppose that b divides a and c divides b. By Definition 1.1.12, it follows that

$$a = qb \quad \text{and} \quad b = rc$$

for some integers q and r. Using the second equation, we may substitute rc for b in the first equation, to obtain

$$a = q(rc)$$

But $q(rc) = (qr)c$, and qr is an integer,

Assumptions	Goals
$a, b, c, q, r \in \mathbb{R}$	$a = [\text{some integer}] \cdot c$
$a = qb$	
$b = rc$	
$a = q(rc)$	
$a = (qr)c$ and $qr \in \mathbb{Z}$	

It is helpful to the reader to declare when the goal has been achieved; this was the content of the final sentence.

> Suppose that b divides a and c divides b. By Definition 1.1.12, it follows that
>
> $$a = qb \quad \text{and} \quad b = rc$$
>
> for some integers q and r. Using the second equation, we may substitute rc for b in the first equation, to obtain
>
> $$a = q(rc)$$
>
> But $q(rc) = (qr)c$, and qr is an integer, so it follows from Definition 1.1.12 that c divides a.

$\triangleleft$

For the rest of this section, we will examine various proof techniques in the context of assumptions and goals. This will be made more precise when we study proof from a *symbolic* perspective in Section 2.1.

Conditional statements

One of the most common kinds of proposition that you will encounter in mathematics is that of a *conditional statement*—that is, one of the form 'if... then...'. As we saw in Example 1.2.1, these can be proved by assuming the statement after the word 'if', and deriving a proof of the statement after the word 'then'.

Proof tip
To prove a proposition of the form 'if P, then Q', assume the proposition P and then derive a proof of the proposition Q.

Assumptions	Goals		Assumptions	Goals
	if P, then Q	$\rightsquigarrow$	P	Q

$\triangleleft$

Proposition 1.1.15 was an example of a proposition containing a conditional statement. Proposition 1.2.2 below contains another example.

Proposition 1.2.2

Let x and y be real numbers. If x and $x + y$ are rational, then y is rational.

Proof of Proposition 1.2.2. Suppose x and $x + y$ are rational. Then there exist integers a, b, c, d with $b, d \neq 0$ such that

$$x = \frac{a}{b} \quad \text{and} \quad x + y = \frac{c}{d}$$

It then follows that

$$y = (x + y) - x = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}$$

Since $bc - ad$ and bd are integers, and $bd \neq 0$, it follows that y is rational. $\qquad \square$

The key phrase in the above proof was 'Suppose x and $x + y$ are rational.' This introduced the assumptions $x \in \mathbb{Q}$ and $x + y \in \mathbb{Q}$, and reduced our goal to that of deriving a proof that y is rational—this was the content of the rest of the proof.

Writing tip

A template for writing proofs of propositions of the form 'if P, then Q' is as follows:

Suppose [*write out P here*]. Then [*prove Q here*].

Words similar in meaning to 'suppose', such as 'assume', may also be used. $\qquad \triangleleft$

The following exercises, based on the topics we introduced in Section 1.1, are an opportunity for you to practise writing proofs of conditional statements.

Exercise 1.2.3

Let $p(x)$ be a polynomial over $\mathbb{C}$. Prove that if α is a root of $p(x)$, and $a \in \mathbb{C}$, then α is a root of $(x - a)p(x)$. $\qquad \triangleleft$

Another common kind of proposition is that of a *biconditional statement*; that is, one of the form 'P if and only if Q' (sometimes abbreviated in writing to 'P iff Q'). This abbreviates the longer expression, 'if P, then Q, and if Q, then P', and indicates that P and Q are in some sense *equivalent*. The statement 'if Q, then P' is called the **converse** of the statement 'if P, then Q'.

Proof tip

To prove a propositions of the form 'P if and only if Q', provide separate proofs of the propositions 'if P, then Q' and 'if Q, then P'.

Assumptions	Goals		Assumptions	Goals
	P if and only if Q	$\rightsquigarrow$		if P, then Q if Q, then P

◁

In writing, we may sometimes abbreviate 'if P, then Q' by writing '$P \Rightarrow Q$' (LATEX code: `P \Rightarrow Q`), and 'P if and only if Q' by '$P \Leftrightarrow Q$' (LATEX code: `P \Leftrightarrow Q`). These symbols will reappear from a formal point of view in Section 2.1.

Many examples of biconditional statements come from solving equations; indeed, to say that the values $\alpha_1, \ldots, \alpha_n$ are the solutions to a particular equation is precisely to say that

$$x \text{ is a solution} \quad \Leftrightarrow \quad x = \alpha_1 \text{ or } x = \alpha_2 \text{ or } \cdots \text{ or } x = \alpha_n$$

Example 1.2.4

We find all real solutions x to the equation

$$\sqrt{x - 3} + \sqrt{x + 4} = 7$$

Let's rearrange the equation to find out what the possible solutions may be.

$$
\begin{aligned}
\sqrt{x-3} + \sqrt{x+4} = 7 &\Rightarrow (x-3) + 2\sqrt{(x-3)(x+4)} + (x+4) = 49 && \text{squaring} \\
&\Rightarrow 2\sqrt{(x-3)(x+4)} = 48 - 2x && \text{rearranging} \\
&\Rightarrow 4(x-3)(x+4) = (48-2x)^2 && \text{squaring} \\
&\Rightarrow 4x^2 + 4x - 48 = 2304 - 192x + 4x^2 && \text{expanding} \\
&\Rightarrow 196x = 2352 && \text{rearranging} \\
&\Rightarrow x = 12 && \text{dividing by } 196
\end{aligned}
$$

You might be inclined to stop here. Unfortunately, all we have proved is that, given a real number x, *if* x solves the equation $\sqrt{x-3} + \sqrt{x+4} = 7$, *then* $x = 12$. This narrows down the set of possible solutions to just one candidate—but we still need to check the converse, namely that *if* $x = 12$, *then* x is a solution to the equation.

As such, to finish off the proof, note that

$$\sqrt{12 - 3} + \sqrt{12 + 4} = \sqrt{9} + \sqrt{16} = 3 + 4 = 7$$

and so the value $x = 12$ is indeed a solution to the equation. ◁

The last step in Example 1.2.4 may have seemed a little bit silly; but Example 1.2.5 demonstrates that proving the converse when solving equations truly is necessary.

Example 1.2.5

We find all real solutions x to the equation

$$x + \sqrt{x} = 0$$

We proceed as before, rearranging the equation to find all possible solutions.

$$\begin{aligned}
x + \sqrt{x} = 0 &\Rightarrow x = -\sqrt{x} && \text{rearranging} \\
&\Rightarrow x^2 = x && \text{squaring} \\
&\Rightarrow x(x-1) = 0 && \text{rearranging} \\
&\Rightarrow x = 0 \text{ or } x = 1
\end{aligned}$$

Now certainly 0 is a solution to the equation, since

$$0 + \sqrt{0} = 0 + 0 = 0$$

However, 1 is *not* a solution, since

$$1 + \sqrt{1} = 1 + 1 = 2$$

Hence it is actually the case that, given a real number x, we have

$$x + \sqrt{x} = 0 \quad \Leftrightarrow \quad x = 0$$

Checking the converse here was vital to our success in solving the equation!   ◁

A slightly more involved example of a biconditional statement arising from the solution to an equation—in fact, a class of equations—is the proof of the quadratic formula.

Theorem 1.2.6 (Quadratic formula)

Let $a, b \in \mathbb{C}$. A complex number α is a root of the polynomial $x^2 + ax + b$ if and only if

$$\alpha = \frac{-a + \sqrt{a^2 - 4b}}{2} \quad \text{or} \quad \alpha = \frac{-a - \sqrt{a^2 - 4b}}{2}$$

Proof. First we prove that *if* α is a root, *then* α is one of the values given in the statement of the proposition. So suppose α be a root of the polynomial $x^2 + ax + b$. Then

$$\alpha^2 + a\alpha + b = 0$$

The algebraic technique of 'completing the square' tells us that

$$\alpha^2 + a\alpha = \left(\alpha + \frac{a}{2}\right)^2 - \frac{a^2}{4}$$

and hence

$$\left(\alpha + \frac{a}{2}\right)^2 - \frac{a^2}{4} + b = 0$$

Rearranging yields

$$\left(\alpha + \frac{a}{2}\right)^2 = \frac{a^2}{4} - b = \frac{a^2 - 4b}{4}$$

Taking square roots gives

$$\alpha + \frac{a}{2} = \frac{\sqrt{a^2 - 4b}}{2} \quad \text{or} \quad \alpha + \frac{a}{2} = \frac{-\sqrt{a^2 - 4b}}{2}$$

and, finally, subtracting $\frac{a}{2}$ from both sides gives the desired result.

The proof of the converse is Exercise 1.2.7. $\qquad\qquad\square$

Exercise 1.2.7

Complete the proof of the quadratic formula. That is, for fixed $a, b \in \mathbb{C}$, prove that if

$$\alpha = \frac{-a + \sqrt{a^2 - 4b}}{2} \quad \text{or} \quad \alpha = \frac{-a - \sqrt{a^2 - 4b}}{2}$$

then α is a root of the polynomial $x^2 + ax + b$. $\qquad\qquad\triangleleft$

Writing tip

A template for proving statements of the form 'P if and only if Q' is as follows.

> Suppose [*write out P here*]. Then [*prove Q here*].
>
> Conversely, suppose [*write out Q here*]. Then [*prove P here*].

Another template, which more clearly separates the two conditional statements, is as follows.

> - ($\Rightarrow$) Suppose [*write out P here*]. Then [*prove Q here*].
> - ($\Leftarrow$) Suppose [*write out Q here*]. Then [*prove P here*].

$\qquad\qquad\triangleleft$

Example 1.2.8

Let $n \in \mathbb{N}$. We will prove that n is divisible by 8 if and only if the number formed of the last three digits of the base-10 expansion of n is divisible by 8.

First, we will do some 'scratch work'. Let $d_r d_{r-1} \ldots d_0$ be the base-10 expansion of n. Then

$$n = d_r \cdot 10^r + d_{r-1} \cdot 10^{r-1} + \cdots + d_0$$

Define

$$n' = d_2 d_1 d_0 \quad \text{and} \quad n'' = n - n' = d_r d_{r-1} \ldots d_4 d_3 000$$

Now $n - n' = 1000 \cdot d_r d_{r-1} \ldots d_4 d_3$ and $1000 = 8 \cdot 125$, so it follows that 8 divides n''.

Our goal is now to prove that 8 divides n if and only if 8 divides n'.

- ($\Rightarrow$) Suppose 8 divides n. Since 8 divides n'', it follows from Exercise 1.1.16 that 8 divides $an + bn''$ for all $a, b \in \mathbb{Z}$. But

$$n' = n - (n - n') = n - n'' = 1 \cdot n + (-1) \cdot n''$$

so indeed 8 divides n', as required.

- ($\Leftarrow$) Suppose 8 divides n'. Since 8 divides n'', it follows from Exercise 1.1.16 that 8 divides $an' + bn''$ for all $a, b \in \mathbb{Z}$. But

$$n = n' + (n - n') = n' + n'' = 1 \cdot n' + 1 \cdot n''$$

so indeed 8 divides n, as required.

$\triangleleft$

Exercise 1.2.9
Prove that a natural number n is divisible by 3 if and only if the sum of its base-10 digits is divisible by 3. $\triangleleft$

Negation and contradiction

Frequently we are tasked with proving that a proposition is *not* true. For example, $\sqrt{2}$ is *not* rational, there is *not* an integer solution x to the equation $3x = 5$, and so on. One way to prove that a proposition is false is to assume that it is true, and use that assumption to derive nonsense. The nonsense we derive is more properly called a *contradiction*.

Definition 1.2.10
A **contradiction** is a proposition which is known or assumed to be false.

Proof tip
To prove a proposition of the form 'not P', assume that P is true and derive a contradiction.

Assumptions	Goals
	not P

$\rightsquigarrow$

Assumptions	Goals
P	[contradiction]

◁

The following proposition has a classic proof by contradiction.

Proposition 1.2.11
Let r be a rational number and let a be an irrational number. Then $r + a$ is irrational.

Proof. By Definition 1.1.26, we need to prove that $r + a$ is real and not rational. It is certainly real, since r and a are real, so it remains to prove that $r + a$ is not rational.

Suppose $r + a$ is rational. Since r is rational, it follows from Proposition 1.2.2 that a is rational, since
$$a = (r + a) - r$$
This contradicts the assumption that a is irrational. It follows that $r + a$ is not rational, and is therefore irrational. □

Writing tip
A template for proving statements of the form 'not P' (or, equivalently, 'P is false') is as follows.

> Suppose [*write out P here*]. Then [*derive a contradiction here*]. This contradicts [*write out the assumption or known fact that is contradicted*]. It follows that [*write out the assertion that P is false here*].

◁

Now you can try proving some elementary facts by contradiction.

Exercise 1.2.12
Let $x \in \mathbb{R}$. Prove by contradiction that if x is irrational then $-x$ and $\frac{1}{x}$ are irrational. ◁

Exercise 1.2.13
Prove by contradiction that there is no least positive real number. That is, prove that there is not a real number a such that $a \leqslant b$ for all positive real numbers b. ◁

A proof need not be a 'proof by contradiction' in its entirety—indeed, it may be that only a small portion of the proof uses contradiction. This is exhibited in the proof of the following proposition.

Proposition 1.2.14
Let a be an integer. Then a is odd[b] if and only if $a = 2b + 1$ for some integer b.

---

[b] For clarity's sake, we take 'even' to mean 'divisible by 2' and 'odd' to mean 'not even'.

Proof. Suppose a is odd. By the division theorem (Theorem 1.1.17), either $a = 2b$ or $a = 2b + 1$, for some $b \in \mathbb{Z}$. If $a = 2b$, then 2 divides a, contradicting the assumption that a is odd; so it must be the case that $a = 2b + 1$.

Conversely, suppose $a = 2b+1$. Then a leaves a remainder of 1 when divided by 2. However, by the division theorem, the even numbers are precisely those that leave a remainder of 0 when divided by 2. It follows that a is not even, so is odd. $\square$

Proofs involving cases

The situation often arises where you know that (at least) one of several facts is true, but you don't know *which* of the facts is true. The solution is to do whatever you're trying to do in all the possible cases—then it doesn't matter which case you fall into!

Proof tip

To use an assumption of the form 'P or Q' when proving a proposition R, split into cases based on whether P is true or Q is true—in both cases, prove that P is true.

Assumptions	Goals		Assumptions	Goals
P or Q	R	$\rightsquigarrow$		if P, then R
				if Q, then R

$\triangleleft$

As you might guess, this proof technique generalises to more than two cases. The proof of Proposition 1.2.15 below splits into three cases.

Proposition 1.2.15

Let $n \in \mathbb{Z}$. Then n^2 leaves a remainder of 0 or 1 when divided by 3.

Proof. Let $n \in \mathbb{Z}$. By the division theorem, one of the following must be true for some $k \in \mathbb{Z}$:

$$n = 3k \quad \text{or} \quad n = 3k + 1 \quad \text{or} \quad n = 3k + 2$$

- Suppose $n = 3k$. Then
$$n^2 = (3k)^2 = 9k^2 = 3 \cdot (3k^2)$$
  So n^2 leaves a remainder of 0 when divided by 3.

- Suppose $n = 3k + 1$. Then
$$n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$$

So n^2 leaves a remainder of 1 when divided by 3.

- Suppose $n = 3k + 2$. Then

$$n^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$$

So n^2 leaves a remainder of 1 when divided by 3.

In all cases, n^2 leaves a remainder of 0 or 1 when divided by 3. □

Writing tip

The following is a template for proving a proposition R by using an assumption of the form 'P or Q'.

There are two possible cases.

- Suppose [*write out P here*]. Then [*prove R here*].
- Suppose [*write out Q here*]. Then [*prove R here*].

In both cases, R is true.

A similar template can be used for proofs requiring more than two cases. ◁

Exercise 1.2.16

Let n be an integer. Prove that n^2 leaves a remainder of 0, 1 or 4 when divided by 5. ◁

Exercise 1.2.17

Let $a, b \in \mathbb{R}$ and suppose $a^2 - 4b \neq 0$. Let α and β be the (distinct) roots of the polyonomial $x^2 + ax + b$. Prove that there is a real number c such that either $\alpha - \beta = c$ or $\alpha - \beta = ci$. ◁

A particularly useful proof principle which allows us to prove propositions by splitting into cases is the *law of excluded middle*.

Definition 1.2.18
The **law of excluded middle** is the assertion that every proposition is either true or it is false. Put otherwise, it says that if P is any proposition, then the proposition 'P or not P' is true.

We can therefore use the law of excluded middle to prove facts by splitting into two cases, based on whether a particular proposition is true or false. The law of excluded middle is an example of a *nonconstructive* proof technique—whilst this matter is not an issue in

mainstream mathematics, it can lead to issues in computer science when not kept in check. This matter will not concern us in the main body of the text, but will be discussed in Section B.3.

The proof of Proposition 1.2.19 below makes use of the law of excluded middle.

Proposition 1.2.19
Let $a, b \in \mathbb{Z}$. If ab is even, then either a is even or b is even (or both).

Proof. Suppose $a, b \in \mathbb{Z}$ with ab even.

- Suppose a is even—then we're done.

- Suppose a is odd. Suppose that b is also odd. Then we can write

$$a = 2k + 1 \quad \text{and} \quad b = 2\ell + 1$$

for some integers k, ℓ. This implies that

$$ab = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(\underbrace{2k\ell + k + \ell}_{\in \mathbb{Z}}) + 1$$

so that ab is odd. This contradicts the assumption that ab is even, and so b must in fact be even.

In both cases, either a or b is even. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Exercise 1.2.20
Reflect on the proof of Proposition 1.2.19. Where in the proof did we use the law of excluded middle? Where in the proof did we use proof by contradiction? What was the contradiction in this case? Prove Proposition 1.2.19 twice more, once using contradiction and not using the law of excluded middle, and once using the law of excluded middle and not using contradiction. $\qquad\qquad\triangleleft$

Exercise 1.2.21
Let a and b be irrational numbers. Prove that it is possible that a^b be rational. $\qquad\qquad\triangleleft$

Reducing a goal to another goal

As indicated above, a huge number of mathematical results take the form 'if P, then Q'. We've already seen a few, and there are dozens more to come! The reason why we prove results of this form is because they are useful—any time we know P is true, we also know that Q is true! In particular, if Q is what we're trying to prove, and we know that P implies Q, then we reduce the problem of proving Q to that of proving P.

Proof tip

To prove a proposition Q using an assumption of the form 'if P, then Q', simply prove that P is true.

Assumptions	**Goals**
if P, then Q	Q

$\rightsquigarrow$

Assumptions	**Goals**
if P, then Q	P

$\triangleleft$

The following is a very simple example of using a conditional statement in a proof.

Proposition 1.2.22

The number $\frac{1}{\sqrt{2}}$ is irrational.

Proof. We proved in Exercise 1.2.12 that, for any real number x, if x is irrational, then $-x$ and $\frac{1}{x}$ are irrational. Since $\sqrt{2}$ is irrational, it follows that $\frac{1}{\sqrt{2}}$ is irrational. $\qquad\square$

Writing tip

The following is a template for proving a proposition Q by using an assumption of the form 'if P, then Q'.

> Since [*write out $P \Rightarrow Q$ here*], in order to prove [*write out Q here*], it suffices to prove [*write out P here*]. To this end, [*prove P here*].

$\triangleleft$

Example 1.2.23

Section 1.3 is devoted to *induction principles*, which are proof techniques used to prove that a given statement is true of all natural numbers. For example, induction can be used to prove that

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

is true for all natural numbers n. Induction principles reduce the problem of proving a statement is true of all natural numbers to the problem of proving a *base case* and an *induction step* (to be defined in Section 1.3).

Thus, from a mathematical perspective, induction principles are nothing more than statements of the form

> if [*base case*] and [*induction step*], then [*statement is true for all natural numbers*]

We will not explore induction any further here, as it is on its way very soon! $\triangleleft$

Dealing with variables

We have made heavy use of variables already in this book, and we will not stop any time soon. The notion of a variable may seem like a simple concept, but it actually has many technicalities associated with it—a whole field, called *nominal theory*, has emerged within mathematical logic and theoretical computer science in order to deal with variables in a systematic way. We won't need to go into quite that amount of detail; instead, we will just need to focus on two aspects:

- the *range* of a variable, which tells us what kind of thing it refers to; and

- the *quantification* of a variable, which tells us how many things it refers to.

Definition 1.2.24
Let x be a variable. The **range** (or **domain of discourse**) of x is the set of objects which x refers to.

In mathematical writing, all variables should have a range, which is either explicitly mentioned or is clear from context.

Example 1.2.25
Consider the following statement.

> If x^2 is rational, then x is rational.

As stated, this statement *looks* like it is false; for example, letting $x = \sqrt{2}$, we can see that $x^2 = 2$, which is rational, but x is irrational. However, this is poorly written, since the range of x is not indicated—indeed, if we're told in advance that x refers to an integer, then the statement is automatically true, since all integers are rational; the counterexample above doesn't work in this case, since $\sqrt{2}$ is not an integer.

Here is a better way of writing it.

> Let x be a real number. If x^2 is rational, then x is rational.

The first sentence here indicates to the reader what kind of object the variable x refers to. As we expected in the first place, this is now a *false* statement—but it's a well-written false statement! ◁

Exercise 1.2.26

Consider the following statement:

> Let x be an integer. If $x = 2k + 1$, then x is odd.

Re-word the statement to specify the range of k. With the range of k that you specified, is the statement true or is it false? Would a different choice of range change its truth or falsity? ◁

Unfortunately simply specifying the range of a variable is not sufficient to give statements mathematical meaning and can lead to ambiguity.

Example 1.2.27

Consider the following statement:

$$x + y \text{ is even}, \quad x, y \in \mathbb{Z}$$

The range of the variables x and y is specified—namely, they refer to integers—but we're left wondering whether the statement '$x + y$ is even' is true. It's certainly *sometimes* true, but it can also be false—specifically, it's true if x and y are both even or both odd, and false otherwise. ◁

As Example 1.2.27 demonstrates, simply stating the range of variables is not sufficient. This is where *quantification* comes in. We will focus on two kinds of quantification, namely *universal* and *existential* quantification.

Universal quantification is a means of saying that the variable can take any value in its range—typically, we universally quantify a variable by using the words 'all' or 'every'. In Section 2.1 we will describe universal quantification more precisely.

Proof tip

To prove a proposition of the form 'for all $x \in X$, P', take an element $x \in X$, and prove P for that value of x, knowing nothing about x, other than the assumption that x is an element of X.

Assumptions	Goals
	for all $x \in X$, P

$\rightsquigarrow$

Assumptions	Goals
$x \in X$	P

◁

Proposition 1.2.28

Every integer greater than one has at least four divisors.

Proof. Let $n \in \mathbb{Z}$, and suppose $n > 1$. Then the numbers $-n$, -1, 1 and n are all distinct, and moreover

$$n = (-1) \cdot (-n) = (-n) \cdot (-1) = n \cdot 1 = 1 \cdot n$$

so they all divide n. □

Writing tip

A template for proving statements of the form 'for all x, P' is as follows.

> Let $x \in X$. Then [*prove P for x here, using no assumptions about x other than the fact that x is an element of X*].

Other words can be used instead of 'let', such as 'take' or 'fix', or even 'suppose'. ◁

Proposition 1.2.29

The base-10 expansion of the square of every natural number ends in one of the digits 0, 1, 4, 5, 6 or 9.

Proof. Fix $n \in \mathbb{N}$, and let

$$n = d_r d_{r-1} \dots d_0$$

be its base-10 expansion. Write

$$n = 10m + d_0$$

where $m \in \mathbb{N}$—that is, m is the natural number obtained by removing the final digit from n. Then

$$n^2 = 100m^2 + 20md_0 + d_0^2 = 10m(10m + 2d_0) + d_0^2$$

Hence the final digit of n^2 is equal to the final digit of d_0^2. But the possible values of d_0^2 are

$$0 \quad 1 \quad 4 \quad 9 \quad 25 \quad 36 \quad 49 \quad 64 \quad 81$$

all of which end in one of the digits 0, 1, 4, 5, 6 or 9. □

Exercise 1.2.30

Prove that every linear polynomial over $\mathbb{Q}$ has a rational root. ◁

Exercise 1.2.31

Prove that, for all real numbers x and y, if x and y are irrational, then $x + y$ and $x - y$ are not both rational. ◁

Sometimes we seek to prove results about existence in mathematics—this just requires us to find *one* thing making a statement true. *Existential quantification* is a means of expressing that there is at least one value a variable can take which makes a statement true. We typically existentially quantify a variable using words like 'there exist' or 'there is'.

Proof tip

To prove a proposition of the form 'there exists $x \in X$ such that P', find a value of $x \in X$ making P true, specify such a value of x, and then prove that P is true for the specified value of x.

Assumptions	Goals		Assumptions	Goals
	there exists $x \in X$ such that P	$\leadsto$	$x = [\textit{specified value}]$	P

$\triangleleft$

Proposition 1.2.32

Let $a \in \mathbb{R}$. The cubic polynomial

$$x^3 + (1 - a^2)x - a$$

has a real root.

Proof. Let $p(x) = x^3 + (1 - a^2)x - a$. Define $x = a$; then

$$p(x) = p(a) = a^3 + (1 - a^2)a - a = a^3 + a - a^3 - a = 0$$

Hence a is a root of $p(x)$. Since a is real, $p(x)$ has a real root. $\square$

Writing tip

A template for proving statements of the form 'there exists x such that P' is as follows.

> Define x by [*define x here*]. Then [*prove P for the specified value of x here*].

Other words can be used instead of 'let', such as 'take' or 'fix', or even 'suppose'. $\triangleleft$

Exercise 1.2.33

Prove that there is a real number which is irrational but whose square is rational. $\triangleleft$

Exercise 1.2.34

Prove that there is an integer which is divisible by zero. $\triangleleft$

Statements may involve many variables, which could be universally or existentially quantified, or any combination of the above. In these cases, variables appearing later in a statement can depend on variables appearing earlier in the statement.

We now revisit Example 1.2.27, this time with quantified variables, and look at how the choice of quantifier affects its truth values.

Example 1.2.35

Consider the statement '$x + y$ is even', where x and y are variables ranging over the integers. There are four ways of quantifying x and y, each yielding a statement with a different meaning:

(a) For all integers x, and all integers y, $x + y$ is even;

(b) For all integers x, there exists an integer y such that $x + y$ is even;

(c) There exists an integer x such that, for all integers y, $x + y$ is even;

(d) There exists an integer x and an integer y such that $x + y$ is even.

Statement (a) is false. If it were true, then it would imply that $0 + 1$ is even; but that is nonsense!

Statement (b) is true. To see this, let $x \in \mathbb{Z}$. We split into cases based on whether x is even or odd.

- If x is even, then by letting $y = 0$, we see that $x + y = x$ is even.

- If x is odd, then by letting $y = 1$, we see that $x + y = x + 1$ is even.

In any case, there is an integer y such that $x + y$ is even, as required.   ◁

Exercise 1.2.36

Prove that (c) is false and (d) is true in Example 1.2.35.   ◁

Exercise 1.2.37

Prove that, for all real numbers x, there exists a real number y such that $x + y \in \mathbb{Q}$.   ◁

1.3 Induction on the natural numbers

We defined the natural numbers in Definition 1.1.5; to reiterate, they are the non-negative whole numbers

$$0, 1, 2, 3, \ldots$$

and we denote the set of natural numbers by $\mathbb{N}$. This was an *informal* definition: it assumed that we have an inherent notion in our minds of what a number line is, what 0 is, and so on. And we probably *do* have such an inherent notion in our minds; it's so ingrained that you wouldn't think twice about what I mean when I write $3 + 15$ or 7×12, even though I haven't defined what $+$ or $\times$ mean (or even what 3, 15, 7 and 12 mean).

This informal approach gets us into some trouble if we really want to be precise about what we're doing, and so Definition 1.1.5 won't suffice. However, we can pin down what it is that the natural numbers 'should be' by writing down some basic properties that they should satisfy—these properties are called *axioms*. The approach we take is to characterise the natural numbers in terms of the number 0 and the operation of 'adding 1', which we call the *successor operation*. A set with a notion of zero and a notion of successor can be thought of as a set of natural numbers provided it satisfies following five axioms, called the *Peano axioms*.

Axioms 1.3.1 (Peano axioms)

(a) $\mathbb{N}$ contains a **zero element**, denoted 0;

(b) If $n \in \mathbb{N}$ then there is an element $n^+ \in \mathbb{N}$, called the **successor** of n;

(c) Zero is not a successor; that is, $n^+ \neq 0$ for all $n \in \mathbb{N}$;

(d) For all $m, n \in \mathbb{N}$, if $m^+ = n^+$, then $m = n$;

(e) If X is a set such that

    (i) $0 \in X$; and

    (ii) for all $n \in \mathbb{N}$, if $n \in X$, then $n^+ \in X$;

  then every natural number is an element of X.

Most of these properties are reasonably self-explanatory. For example, we can interpret (c) as saying that there isn't a natural number n such that $n + 1 = 0 \ldots$ if there were, then we'd have $n = -1$ but -1 isn't a natural number. And (d) says that if $m + 1 = n + 1$ then $m = n$; this makes sense because we should be able to 'subtract 1' from both sides of the equation.

The property that requires some discussion is (e). In slightly more human terms, it says: if a set X contains 0 and the successors of all its elements, then it contains all the natural numbers. Why should this be so? Well, we know $0 \in X$. Since X contains successors of all its elements, it contains $0 + 1$, which is 1; and so it contains $1 + 1$, which is 2; and so it contains $2 + 1$, which is 3; ... and so on.

From the five Peano axioms, we can recover everything we know about the natural numbers. For instance:

- **Numerals.** Define $1 = 0^+$, $2 = 1^+$ $(= 0^{++})$, $3 = 2^+$ $(= 0^{+++})$, and so on. Thus the symbols $0, 1, 2, 3, 4, \dots$ (called *numerals*) are given meaning by saying that n is the nth iterated successor of 0.

- **Addition.** We can define addition by declaring $m + 0 = m$ and $m + (n^+) = (m+n)^+$. Thus, for instance,

$$m + 1 = m + (0^+) = (m + 0)^+ = m^+$$

  and, then

$$m + 2 = m + (1^+) = (m + 1)^+ = m^{++}$$

  and so on.

- **Multiplication.** We can define multiplication as iterated addition. Precisely, define $m \times 0 = 0$ and $m \times (n^+) = (m \times n) + m$ (L^AT_EX code: `\times`).

- **Exponentiation.** We can define exponentiation as iterated multiplication. Precisely, define $m^0 = 1$ and $m^{n^+} = (m^n) \times m$.

- **Order.** If you think about it, $m \leqslant n$ (L^AT_EX code: `\le`) really just means that there is some non-negative number you can add to m to obtain n. Thus we can define '$m \leqslant n$' to mean

$$m + k = n \text{ for some } k \in \mathbb{N}$$

  and then we can define '$m < n$' to mean '$m \leqslant n$ and $m \neq n$'.

The way we defined addition and multiplication is called **recursion**: we defined how they act on zero, and how they act on a successor $n + 1$ in terms of how they act on n.

Example 1.3.2

We prove that $2 \times 2 = 4$ using the recursive definitions of addition and multiplication.

$$
\begin{aligned}
2 \times 2 &= (2 \times 1) + 2 && \text{by definition of } \times, \text{ since } 2 = 1^+ \\
&= ((2 \times 0) + 2) + 2 && \text{by definition of } \times, \text{ since } 1 = 0^+ \\
&= (0 + 2) + 2 && \text{by definition of } \times \\
&= ((0 + 1) + 1) + 2 && \text{by definition of } +, \text{ since } 2 = 1^+ \\
&= (1 + 1) + 2 && \text{since } 0 + 1 = 0^+ = 1 \\
&= 2 + 2 && \text{since } 1 + 1 = 1^+ = 2 \\
&= (2 + 1) + 1 && \text{by definition of } +, \text{ since } 2 = 1^+ \\
&= 3 + 1 && \text{since } 2 + 1 = 2^+ = 3 \\
&= 4 && \text{since } 3 + 1 = 3^+ = 4
\end{aligned}
$$

Note that, in order to shorten the proof, we used the fact proved earlier, that $m + 1 = m^+$ for all m, on the fifth, sixth, eighth and ninth lines. ◁

Exercise 1.3.3
Using the recursive definitions of addition, multiplication and exponentiation, prove that $2^2 = 4$. ◁

We will not go through the long, arduous process of proving everything we need from the Peano axioms, as that would take a long time, and would not be very enlightening. Before moving on, we will make some more recursive definitions that will be useful to us as we progress through the book.

Definition 1.3.4
For each $i \in \mathbb{N}$ let x_i be a real number.

- The **indexed sum** $\sum_{i=1}^{n} x_i$ is defined recursively for $n \in \mathbb{N}$ by

$$
\sum_{i=1}^{0} x_i = 0 \quad \text{and} \quad \sum_{i=1}^{n+1} x_i = \left(\sum_{i=1}^{n} x_i \right) + x_{n+1}
$$

- The **indexed product** $\prod_{i=1}^{n} x_i$ is defined recursively for $n \in \mathbb{N}$ by

$$
\prod_{i=1}^{0} x_i = 1 \quad \text{and} \quad \prod_{i=1}^{n+1} x_i = \left(\prod_{i=1}^{n} x_i \right) \cdot x_{n+1}
$$

Example 1.3.5

Let $x_i = i^2$ for each $i \in \mathbb{N}$. Then

$$\sum_{i=1}^{5} x_i = 1 + 4 + 9 + 16 + 25 = 55$$

and

$$\prod_{i=1}^{5} x_i = 1 \cdot 4 \cdot 9 \cdot 16 \cdot 25 = 14400$$

◁

Exercise 1.3.6

Let $x_1, x_2 \in \mathbb{R}$. Working strictly from the definitions of indexed sum and indexed product, prove that

$$\sum_{i=1}^{2} x_i = x_1 + x_2 \quad \text{and} \quad \prod_{i=1}^{2} x_i = x_1 \cdot x_2$$

◁

The remainder of this section concerns *induction* on the natural numbers. This is a class of proof techniques which are used for proving statements about natural numbers—Definition 1.3.7 makes this notion slightly more precise, and is a particular instance of a *logical formula*, which will be introduced in Definition 2.1.37 (and again formally in Definition B.1.3).

Definition 1.3.7

A **statement about natural numbers** is an expression involving a variable, such that when a natural number is substituted for the variable in the expression, it becomes a proposition (in the sense of Definition 1.1.1). We will denote statements about natural numbers as $p(n)$, $q(m)$, and so on; the letter in parentheses denotes the variable.

Example 1.3.8

Let $p(n)$ be the statement

$$2n + 1 \text{ is divisible by } 3$$

This is a statement about natural numbers. The proposition $p(1)$ says

$$2 \cdot 1 + 1 \text{ is divisible by } 3$$

which is true, since $2 \cdot 1 + 1 = 3 = 1 \cdot 3$. The proposition $p(2)$ says

$$2 \cdot 2 + 1 \text{ is divisible by } 3$$

which is false, since $2 \cdot 2 + 1 = 5 = 1 \cdot 3 + 2$, which leaves a remainder of 2 when divided by 3. For a given natural number n, the proposition $p(3n)$ says

$$2 \cdot (3n) + 1 \text{ is divisible by } 3$$

which will be seen to be false in the following exercise. ◁

Exercise 1.3.9
Letting $p(n)$ be the statement as in Example 1.3.8. Prove that $p(3n + 1)$ is true for all $n \in \mathbb{N}$, and that $p(3n)$ and $p(3n + 2)$ are both false for all $n \in \mathbb{N}$. ◁

Weak induction

The first induction principle we encounter says that natural numbers behave like dominoes. Imagine an infinitely long line of dominoes—one for each natural number—and suppose we want to prove a statement about natural numbers, say $p(n)$. Proving $p(n)$ will correspond to the nth domino falling; hence proving $p(n)$ for all $n \in \mathbb{N}$ corresponds to *all* the dominoes falling.

How do we make all the dominoes fall? Well we knock down domino 0, and from there everything is taken care of: domino 0 knocks down domino 1; then domino 1 knocks down domino 2; and so on. For $n \in \mathbb{N}$, domino n knocks down domino $n + 1$.

From a more mathematical perspective, what this means is: we prove $p(0)$; then $p(1)$ will follow from the fact that $p(0)$ is true; and $p(2)$ will follow from the fact that $p(1)$ is true; and so on. For $n \in \mathbb{N}$, $p(n + 1)$ will follow from the fact that $p(n)$ is true. In other words, provided we can prove $p(0)$ is true, and that $p(n) \Rightarrow p(n + 1)$ for each n, we've made all the dominos fall over and hence proved the proposition for all natural numbers.

Sometimes a statement might be false for a few natural numbers, but true after a certain point. For example $3n < 2^n$ is true when $n = 0$, false when $n = 1, 2, 3$, and then true for all $n \geqslant 4$. This isn't a problem—if all we want to do is prove that it is true for $n \geqslant 4$, we just knock over domino 4 first instead of domino 0!

Now let's be more precise about what we mean, and prove that we're correct.

Theorem 1.3.10 (Weak induction principle)

Let $p(n)$ be a statement about natural numbers, and let $b \in \mathbb{N}$. If

   (i) $p(b)$ is true; and

  (ii) For all $n \geqslant b$, if $p(n)$ is true, then $p(n+1)$ is true;

then $p(n)$ is true for all $n \geqslant b$.

Proof. First suppose $b = 0$. Let X be the set of all natural numbers n for which $p(n)$ is true. For a natural number n, the proposition $n \in X$ is equivalent to the proposition $p(n)$. Thus, respectively, the hypotheses of the theorem state:

   (i) $0 \in X$; and

  (ii) For all $n \in \mathbb{N}$, if $n \in X$, then $n + 1 \in X$;

So by Axiom 1.3.1(e), every natural number is an element of X. Hence $p(n)$ is true for all $n \in \mathbb{N}$.

The case when $b > 0$ is left for the reader in Exercise 1.3.13.   □

Proof tip

To prove a statement $p(n)$ is true for all natural numbers $n \geqslant b$, you can:

- (**Base case**) Prove $p(b)$ is true;

- (**Induction step**) Fix $n \geqslant b$, and assume that $p(n)$ is true; from this assumption alone, derive $p(n+1)$.

The assumption $p(n)$ is called the **induction hypothesis**.

This whole process is called **proof by** (**weak**) **induction** (**on** n). We won't usually use the word 'weak' unless we really need to specify it. Usually we'll also omit 'on n' unless there is more than one variable at play, in which case we will specify.   ◁

Example 1.3.11

We will prove that $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all natural numbers n, by induction.[c] Note that since we're proving it for *all* natural numbers, our base case has $b = 0$.

Let $p(n)$ be the assertion that $0 + 1 + \cdots + n = \frac{n(n+1)}{2}$.

---

[c] The LATEX code for $\frac{a}{b}$ is `\frac{a}{b}`.

- (**BC**) We prove $p(0)$ is true. Now, $p(0)$ is the expression $0 = \frac{0(0+1)}{2}$. Since the right-hand side evaluates to 0, $p(0)$ is true.

- (**IS**) Let $n \in \mathbb{N}$ and suppose $p(n)$ is true, i.e. assume

$$0 + 1 + \cdots + n = \frac{n(n+1)}{2} \qquad\qquad\text{—}(\mathbf{IH})$$

We prove that this implies $p(n+1)$, which is the formula

$$0 + 1 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}$$

We proceed by calculation:

$$
\begin{aligned}
0 + 1 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) & \text{by } (\mathbf{IH}) \\
&= (n+1)\left(\frac{n}{2} + 1\right) & \text{by factorisation} \\
&= (n+1)\left(\frac{n}{2} + \frac{2}{2}\right) & \text{since } \frac{2}{2} = 1 \\
&= \frac{(n+1)(n+2)}{2} & \text{combining fractions}
\end{aligned}
$$

Hence $p(n)$ implies $p(n+1)$. By induction, we're done. ◁

Writing tip

Proofs by induction all follow the same format, so it is good to get into some good habits. These good habits make your proof more readable and better structured, and they help you to avoid silly mistakes. With reference to Example 1.3.11, here are some tips for writing proofs by induction of your own:

- **Labelling the steps.** Clearly labelling the base case and induction step helps the reader identify what part of the proof is being done. I used **BC** and **IS** to signify which is which; you are of course welcome to develop your own convention.

- **Writing down the induction hypothesis.** Writing down the induction hypothesis $p(n)$ explicitly—which I labelled by **IH**—makes it very clear what it is you are assuming. You can then refer back to it later in your proof—as I did in the first line of the calculation—to specify when you have used it.

- **Writing down the goal of the induction step.** When proving the induction step, it is common to fall down the trap of forgetting what you are actually trying to prove. Writing down $p(n+1)$ explicitly, prefixed by something like 'we need to prove ...', gives you something to look back on as you complete your proof.

- **Saying when you're done.** When you have proved $p(n + 1)$ is true, it is a good idea to conclude the proof by summarising what you did. A quick statement like 'hence $p(n)$ implies $p(n + 1)$, so by induction, we're done' will suffice.

◁

Example 1.3.12
We'll prove that $n^3 - n$ is divisible by 3 for all $n \in \mathbb{N}$. Thus, the statement $p(n)$ to be proved is $n^3 - n$, and the base case is when $n = 0$.

- (**BC**) We need to prove that $0^3 - 0$ is divisible by 3. Well $0^3 - 0 = 0 = 3 \times 0$, so $0^3 - 0$ is divisible by 3.

- (**IS**) Let $n \in \mathbb{N}$ and suppose that $n^3 - n$ is divisible by 3. Specifically, the induction hypothesis is:
$$n^3 - n = 3k \text{ for some } k \in \mathbb{N} \qquad\qquad \text{—(\textbf{IH})}$$
We need to prove that $(n + 1)^3 - (n + 1)$ is divisible by 3; in other words, we need to find some natural number ℓ such that
$$(n + 1)^3 - (n + 1) = 3\ell$$

Expanding the brackets, we obtain:
$$
\begin{aligned}
(n + 1)^3 - (n + 1) &= (n^3 + 3n^2 + 3n + 1) - n - 1 &&\text{expand brackets} \\
&= n^3 - n + 3n^2 + 3n + 1 - 1 &&\text{rearrange terms} \\
&= n^3 - n + 3n^2 + 3n &&\text{since } 1 - 1 = 0 \\
&= 3k + 3n^2 + 3n &&\text{by (\textbf{IH})} \\
&= 3(k + n^2 + n) &&\text{factorise}
\end{aligned}
$$

Thus we have expressed $(n+1)^3 - (n+1)$ in the form 3ℓ for a natural number ℓ; specifically, $\ell = k + n^2 + n$. By induction, we're done. ◁

The following exercise completes the proof of the weak induction principle, where the base case is allowed to be nonzero.

Exercise 1.3.13
Prove the weak induction principle (Theorem 1.3.10) in the case when $b > 0$. ◁

Example 1.3.14
Let $p(n)$ be the statement $3n < 2^n$. We prove $p(n)$ is true for all $n \geqslant 4$ by induction.

- (**BC**) $p(4)$ is the statement $3 \cdot 4 < 2^4$. This is true, since $12 < 16$.

- (**IS**) Suppose $n \geqslant 4$ and that $p(n)$ is true, i.e. that $3n < 2^n$ (**IH**). We want to prove $3(n+1) < 2^{n+1}$. Well

$$
\begin{aligned}
3(n+1) = 3n + 3 \qquad & \text{expand brackets} \\
< 2^n + 3 \qquad & \text{by (\textbf{IH})} \\
< 2^n + 16 \qquad & \text{since } 3 < 16 \\
= 2^n + 2^4 \qquad & \text{since } 2^4 = 16 \\
\leqslant 2^n + 2^n \qquad & \text{since } n \geqslant 4 \\
= 2 \cdot 2^n \qquad & \text{since } x + x = 2x \\
= 2^{n+1} \qquad & \text{using laws of indices}
\end{aligned}
$$

So we have proved $3(n+1) < 2^{n+1}$, as required.

Hence $p(n)$ implies $p(n+1)$, so by induction, we're done.   ◁

Note that the proof in Example 1.3.14 says nothing about the truth or falsity of $p(n)$ for $n = 0, 1, 2, 3$. In order to assert that these cases are false, you need to show them individually; indeed:

- $3 \times 0 = 0$ and $2^0 = 1$, hence $p(0)$ is true;

- $3 \times 1 = 3$ and $2^1 = 2$, hence $p(1)$ is false;

- $3 \times 2 = 6$ and $2^2 = 4$, hence $p(2)$ is false;

- $3 \times 3 = 9$ and $2^3 = 9$, hence $p(3)$ is false.

So we deduce that $p(n)$ is true when $n = 0$ or $n \geqslant 4$, and false otherwise.

Exercise 1.3.15
Use weak induction to prove that

$$
\sum_{k=0}^{n} 2^k = 2^{n+1} - 1
$$

for all $n \in \mathbb{N}$.   ◁

Sometimes a 'proof' by induction might appear to be complete nonsense. The following is a classic example of a 'fail by induction':

Example 1.3.16

The following argument supposedly proves that every horse is the same colour.

- (**BC**) Suppose there is just one horse. This horse is the same colour as itself, so the base case is immediate.

- (**IS**) Suppose that every collection of n horses is the same colour (**IH**). Let X be a set of $n + 1$ horses. Removing the first horse from X, we see that the last n horses are the same colour by (**IH**). Removing the last horse from X, we see that the first n horses are the same colour. Hence all the horses in X are the same colour.

By induction, we're done.   ◁

Exercise 1.3.17

Write down the statement $p(n)$ that Example 1.3.16 attempted to prove for all $n \geqslant 1$. Convince yourself that the proof of the base case is correct, then write down—with quantifiers— exactly the proposition that the induction step is meant to prove. Explain why the argument in the induction step failed to prove this proposition.   ◁

Writing tip

There are several ways to avoid situations like that of Example 1.3.16 by simply putting more thought into writing the proof. Some tips are:

- **State $p(n)$ explicitly.** In the statement 'all horses are the same colour' it is not clear exactly what the induction variable is. However, we could have said:

  Let $p(n)$ be the statement 'every set of n horses has the same colour'.

- **Refer to the base case b in the induction step.** In Example 1.3.16, our induction hypothesis simply stated 'assume every set of n horses has the same colour'. Had we instead said:

  Let $n \geqslant 1$ and assume every set of n horses has the same colour.

  We may have spotted the error in what was to come.

                                                                                                            ◁

What follows are a couple more examples of proofs by weak induction.

Example 1.3.18

Given any $n \in \mathbb{N}$,

$$\sum_{k=0}^{n} k^3 = \left(\sum_{k=0}^{n} k\right)^2$$

We proved in Example 1.3.11 that $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$, thus it suffices to prove that

$$\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

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

We proceed by induction.

- **(BC)** We need to prove that $0^3 = \frac{0^2(0+1)^2}{4}$. This is true since both sides of the equation are equal to 0.

- **(IS)** Fix $n \in \mathbb{N}$ and suppose that $\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$. We need to prove that $\sum_{k=0}^{n+1} k^3 = \frac{(n+1)^2(n+2)^2}{4}$. This is true since:

$$
\begin{aligned}
\sum_{i=0}^{n+1} k^3 &= \sum_{i=0}^{n} k^3 + (n+1)^3 && \text{by definition of sum} \\
&= \frac{n^2(n+1)^2}{4} + (n+1)^3 && \text{by (\textbf{IH})} \\
&= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} && (algebra) \\
&= \frac{(n+1)^2(n^2 + 4(n+1))}{4} && (algebra) \\
&= \frac{(n+1)^2(n+2)^2}{4} && (algebra)
\end{aligned}
$$

By induction, the result follows. ◁

Example 1.3.19

We will prove the correctness of the following formula for the sum of an *arithmetic progression*, that is a sequence of finite length such that the difference between consecutive terms is constant.

Specifically, let $a, d \in \mathbb{R}$. We will prove that

$$\sum_{k=0}^{n} (a + kd) = \frac{(n+1)(2a + nd)}{2}$$

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

We proceed by induction.

- (**BC**) We need to prove that $\sum_{k=0}^{0}(a+kd) = \frac{(0+1)(2a+0d)}{2}$. This is true, since

$$\sum_{k=0}^{0}(a+kd) = a + 0d = a = \frac{2a}{2} = \frac{1 \cdot (2a)}{2} = \frac{(0+1)(2a+0d)}{2}$$

- (**IS**) Fix $n \in \mathbb{N}$ and suppose that $\sum_{k=0}^{n}(a+kd) = \frac{(n+1)(2a+nd)}{2}$. We need to prove:

$$\sum_{k=0}^{n+1}(a+kd) = \frac{(n+2)(2a+(n+1)d)}{2}$$

This is true, since

$$\sum_{k=0}^{n+1}(a+kd)$$

$$= \sum_{k=0}^{n}(a+kd) + (a+(n+1)d) \qquad \text{by definition of sum}$$

$$= \frac{(n+1)(2a+nd)}{2} + (a+(n+1)d) \qquad \text{by (\textbf{IH})}$$

$$= \frac{(n+1)(2a+nd) + 2a + 2(n+1)d}{2} \qquad (\textit{algebra})$$

$$= \frac{(n+1) \cdot 2a + (n+1) \cdot nd + 2a + 2(n+1)d}{2} \qquad (\textit{algebra})$$

$$= \frac{2a(n+1+1) + (n+1)(nd+2d)}{2} \qquad (\textit{algebra})$$

$$= \frac{2a(n+2) + (n+1)(n+2)d}{2} \qquad (\textit{algebra})$$

$$= \frac{(n+2)(2a+(n+1)d)}{2} \qquad (\textit{algebra})$$

By induction, the result follows. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \triangleleft$

Strong induction

Sometimes it is clear that a statement can *almost* be proved by induction, but a snag appears; for example, in the following example, the truth of $p(n+1)$ seems to depend not on just $p(n)$, but also on $p(n-1)$:

Example 1.3.20

Define a sequence of numbers $(a_n)_{n \in \mathbb{N}}$ recursively by:

$$a_0 = 0, \quad a_1 = 1, \quad a_n = 3a_{n-1} - 2a_{n-2} \text{ for all } n \geqslant 2$$

Thus, continuing the sequence, we have

$$a_2 = 3 \cdot 1 - 2 \cdot 0 = 3, \quad a_3 = 3 \cdot 3 - 2 \cdot 1 = 7, \quad a_4 = 15, \quad \dots$$

Looking at the sequence $(0, 1, 3, 7, 15, \dots)$, you might hypothesise that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$. And you would be correct! So let's try and prove that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$ by induction.

The statement is demonstrably true for $n = 0, 1$, since

$$a_0 = 0 = 1 - 1 = 2^0 - 1 \quad \text{and} \quad a_1 = 1 = 2 - 1 = 2^1 - 1$$

Fix $n \geqslant 1$ and suppose $a_n = 2^n - 1$. If this implies that $a_{n+1} = 2^{n+1} - 1$, we'll be done by induction: indeed, induction gives that $p(n)$ is true for all $n \geqslant 1$, and we checked the case $n = 0$ separately.

So let's see what happens. Since $n \geqslant 1$, we have $n + 1 \geqslant 2$, so we can apply the recursive formula for a_{n+1}:

$$a_{n+1} = 3a_n - 2a_{n-1}$$

Here's where we get stuck: our induction hypothesis only tells us that $a_n = 2^n - 1$, so that

$$a_{n+1} = 3(2^n - 1) - 2a_{n-1}$$

but it doesn't tell us anything at all about a_{n-1}. We need to express a_{n-1} in terms of n in order to get a reasonable formula for a_{n+1}. ⊠ ◁

This example illustrates why weak induction is called 'weak'. But all is not lost: using the technique of weak induction, we can prove a principle of *strong induction*. The induction step in strong induction assumes not just the truth of the proposition for *one* prior step, but its truth of *all* prior steps.

Despite its name, strong induction is no stronger than weak induction; the two principles are equivalent. In fact, we'll prove the strong induction principle *by weak induction*!

Corollary 1.3.21 (Strong induction principle)

Let $p(x)$ be a statement about natural numbers and let $b \in \mathbb{N}$. If

  (i) $p(b)$ is true; and

  (ii) For all $n \in \mathbb{N}$, if $p(k)$ is true for all $b \leqslant k \leqslant n$, then $p(n+1)$ is true;

then $p(n)$ is true for all $n \geqslant b$.

Proof. We'll prove this using weak induction. For each n, let $q(n)$ be the statement

$$\text{`}p(k)\text{ is true for all }b \leqslant k \leqslant n\text{'}$$

Notice that $q(n)$ implies $p(n)$ for all $n \geqslant b$—to see this, let $k = n$ in the statement of $q(n)$. Thus if we can prove that $q(n)$ is true for all n, then we've proved that $p(n)$ is true for all n.

- (**BC**) $q(b)$ is equivalent to $p(b)$, since the only natural number k with $b \leqslant k \leqslant b$ is b itself; hence $q(b)$ is true by (i);

- (**IS**) Let $n \geqslant b$ and suppose $q(n)$ is true. By (ii), $p(n+1)$ is true. Since $q(n)$ is true, $p(k)$ is true for all $b \leqslant k \leqslant n$. Combining these facts, $p(k)$ is true for all $b \leqslant k \leqslant n+1$, which is precisely the statement that $q(n+1)$ is true.

By induction, $q(n)$ is true for all $n \geqslant b$. Hence $p(n)$ is true for all $n \geqslant b$. □

Proof tip

To prove a statement $p(n)$ is true for all natural numbers $n \geqslant b$ (where b is some fixed natural number):

- (**Base case**) Prove $p(b)$ is true;

- (**Induction step**) Fix $n \geqslant b$, and assume that $p(k)$ is true for all $b \leqslant k \leqslant n$; from this assumption alone, derive $p(n+1)$.

The assumption that $p(k)$ is true for all $b \leqslant k \leqslant n$ is called the **induction hypothesis**.

This whole process is called **proof by (strong) induction (on n)**. We won't usually use the word 'strong' unless we really need to specify it. Usually we'll also omit 'on n' unless there is more than one variable at play, in which case we will specify.   ◁

Strong induction is very well suited to proving formulae for sequences where subsequent terms are defined in terms of more than one previous term, as the next few examples demonstrate.

Example 1.3.22

Recall from Example 1.3.20 that we defined the sequence

$$a_0 = 0, \quad a_1 = 1, \quad a_n = 3a_{n-1} - 2a_{n-2} \text{ for all } n \geqslant 2$$

and we wished to prove that $a_n = 2^n - 1$ for all $n \in \mathbb{N}$. We have proved that it's true when $n = 0$, and will show that it's true for $n \geqslant 1$ by strong induction on n.

- (**BC**) We have already proved that $a_1 = 2^1 - 1$.

- (**IS**) Let $n \in \mathbb{N}$, and assume that $a_k = 2^k - 1$ for all $1 \leqslant k \leqslant n$. Since $a_0 = 2^0 - 1$, this in fact holds for all $k \leqslant n$.

  We need to prove that this assumption implies that $a_{n+1} = 2^{n+1} - 1$. Well, $n \geqslant 1$, so $n + 1 \geqslant 2$ and we can apply the recursive formula to a_{n+1}. Thus

$$\begin{aligned}
a_{n+1} &= 3a_n - 2a_{n-1} && \text{by definition of } a_{n+1} \\
&= 3(2^n - 1) - 2(2^{n-1} - 1) && \text{since } p(k) \text{ holds for all } k \leqslant n \\
&= 3 \cdot 2^n - 3 - 2 \cdot 2^{n-1} + 2 && \text{expand brackets} \\
&= 3 \cdot 2^n - 3 - 2^n + 2 && \text{laws of indices} \\
&= 2 \cdot 2^n - 1 && \text{simplifying} \\
&= 2^{n+1} - 1 && \text{laws of indices}
\end{aligned}$$

So we're done by strong induction. ◁

Example 1.3.23
Define a sequence recursively by $a_0 = 4$, $a_1 = 9$ and $a_n = 5a_{n-1} - 6a_{n-2}$ for all $n \geqslant 2$.

We will prove that $a_n = 3 \cdot 2^n + 3^n$ for all $n \in \mathbb{N}$.

We proceed by strong induction for $n \geqslant 1$, treating the $n = 0$ case as a second base case.

- (**BC**) The result holds when $n = 0$ and when $n = 1$, since

$$a_0 = 4 = 3 \cdot 2^0 + 3^0 \qquad \text{and} \qquad a_1 = 9 = 3 \cdot 2^1 + 3^1$$

- (**IS**) Fix $n \geqslant 1$ and suppose that $a_k = 3 \cdot 2^k + 3^k$ for all $k \leqslant n$. We need to prove that $a_{n+1} = 3 \cdot 2^{n+1} + 3^{n+1}$. Well,

$$\begin{aligned}
a_{n+1} &= 5a_n - 6a_{n-1} && \text{by definition of the sequence} \\
&= 5(3 \cdot 2^n + 3^n) - 6(3 \cdot 2^{n-1} + 3^{n-1}) && \text{by the induction hypothesis} \\
&= (5 \cdot 3 \cdot 2 - 6 \cdot 3)2^{n-1} + (5 \cdot 3 - 6)3^{n-1} && (\textit{algebra}) \\
&= 12 \cdot 2^{n-1} + 9 \cdot 3^{n-1} && (\textit{algebra}) \\
&= 3 \cdot 2^2 \cdot 2^{n-1} + 3^2 \cdot 3^{n-1} && (\textit{algebra}) \\
&= 3 \cdot 2^{n+1} + 3^{n+1} && (\textit{algebra})
\end{aligned}$$

  Hence the result we sought to prove is true.

By induction, it follows that $a_n = 3 \cdot 2^n + 3^n$ for all $n \in \mathbb{N}$. ◁

Example 1.3.24

Define a sequence recursively by

$$b_0 = 1 \quad \text{and} \quad b_{n+1} = 1 + \sum_{k=0}^{n} b_k \text{ for all } n \in \mathbb{N}$$

We will prove by strong induction that $b_n = 2^n$ for all $n \in \mathbb{N}$.

- (**BC**) By definition of the sequence we have $b_0 = 1 = 2^0$.

- (**IS**) Fix $n \in \mathbb{N}$, and suppose that $b_k = 2^k$ for all $k \leqslant n$. We need to show that $b_{n+1} = 2^{n+1}$. This is true, since

$$
\begin{aligned}
b_{n+1} &= 1 + \sum_{k=0}^{n} b_k && \text{by the recursive formula for } b_{n+1} \\
&= 1 + \sum_{k=0}^{n} 2^k && \text{by the induction hypothesis} \\
&= 1 + (2^{n+1} - 1) && \text{by Exercise 1.3.15} \\
&= 2^{n+1}
\end{aligned}
$$

By induction, it follows that $b_n = 2^n$ for all $n \in \mathbb{N}$.   ◁

A first look at binomials and factorials

In Section 4.2, two kinds of natural number will turn out to be extremely useful, namely *factorials* and *binomial coefficients*. These numbers allow us to count the number of elements of certain kinds of sets, and correspond with the 'real-world' processes of *permutation* and *selection*, respectively. Everything we do here will be re-defined and re-proved *combinatorially* in Section 3.2. In this section, we will overlook the combinatorial nature, and instead characterise them recursively. We will prove that the combinatorial and recursive definitions of binomial coefficients and factorials are equivalent in Section 4.2.

Definition 1.3.25 (to be redefined in Definition 4.2.24)

Let $n \in \mathbb{N}$. The **factorial** of n, written $n!$, is defined recursively by

$$0! = 1 \quad \text{and} \quad (n+1)! = (n+1) \cdot n! \text{ for all } n \geqslant 0$$

Put another way, we have

$$n! = \prod_{i=1}^{n} i$$

for all $n \in \mathbb{N}$—recall 1.3.4 to see why these definitions are really just two ways of wording the same thing.

Exercise 1.3.26
Prove that

$$\prod_{i=0}^{n-1} (3i+1)(3i+2) = \frac{(3n)!}{3^n n!}$$

for all $n \in \mathbb{N}$. ◁

Definition 1.3.27 (to be redefined in Definition 4.2.18)
Let $n, k \in \mathbb{N}$. The **binomial coefficient** $\binom{n}{k}$ (LATEX code: `\binom{n}{k}`) (read 'n choose k') is defined recursively for $n, k \in \mathbb{N}$ by

$$\binom{k}{0} = 1, \quad \binom{0}{k+1} = 0, \quad \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

This definition gives rise to an algorithm for computing binomial coefficients: they fit into a diagram known as **Pascal's triangle**, with each binomial coefficient computed as the sum of the two lying above it (with zeroes omitted):

$$
\begin{array}{ccccccccc}
& & & & \binom{0}{0} & & & & \\
& & & \binom{1}{0} & & \binom{1}{1} & & & \\
& & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
& \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} \\
\binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5} \\
\vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}
=
\begin{array}{ccccccccc}
& & & & 1 & & & & \\
& & & 1 & & 1 & & & \\
& & 1 & & 2 & & 1 & & \\
& 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
1 & 5 & & 10 & & 10 & & 5 & & 1 \\
\vdots & \vdots & \vdots & \vdots &
\end{array}
$$

Exercise 1.3.28
Write down the next two rows of Pascal's triangle. ◁

We can prove lots of identities concerning binomial coefficients and factorials by induction.

Example 1.3.29
We prove that $\sum_{i=0}^{n} \binom{n}{i} = 2^n$ by induction on n.

- (**BC**) We need to prove $\binom{0}{0} = 1$ and $2^0 = 1$. These are both true by the definitions of binomial coefficients and exponents.

- (**IS**) Fix $n \geqslant 0$ and suppose that

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n$$

We need to prove

$$\sum_{i=0}^{n+1} \binom{n+1}{i} = 2^{n+1}$$

This is true, since

$$\sum_{i=0}^{n+1} \binom{n+1}{i}$$

$$= \binom{n+1}{0} + \sum_{i=1}^{n+1} \binom{n+1}{i} \qquad \text{splitting the sum}$$

$$= 1 + \sum_{j=0}^{n} \binom{n+1}{j+1} \qquad \text{letting } j = i - 1$$

$$= 1 + \sum_{j=0}^{n} \left(\binom{n}{j} + \binom{n}{j+1} \right) \qquad \text{by Definition 1.3.27}$$

$$= 1 + \sum_{j=0}^{n} \binom{n}{j} + \sum_{j=0}^{n} \binom{n}{j+1} \qquad \text{separating the sums}$$

Now $\sum_{j=0}^{n} \binom{n}{j} = 2^n$ by the induction hypothesis. Moreover, reindexing the sum using $k = j + 1$ yields

$$\sum_{j=0}^{n} \binom{n}{j+1} = \sum_{k=1}^{n+1} \binom{n}{k} = \sum_{k=1}^{n} \binom{n}{k} + \binom{n}{n+1}$$

By the induction hypothesis, we have

$$\sum_{k=1}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} - \binom{n}{0} = 2^n - 1$$

and $\binom{n}{n+1} = 0$, so that $\sum_{j=0}^{n} \binom{n}{j+1} = 2^n - 1$.

Putting this together, we have

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

so the induction step is finished.

By induction, we're done. ◁

Exercise 1.3.30

Prove by induction on $n \geqslant 1$ that

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$$

◁

Theorem 1.3.31

Let $n, k \in \mathbb{N}$. Then

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{if } k \leqslant n \\ 0 & \text{if } k > n \end{cases}$$

Proof. We proceed by induction on n.

- (**BC**) When $n = 0$, we need to prove that $\binom{0}{k} = \frac{0!}{k!(-k)!}$ for all $k \leqslant 0$, and that $\binom{0}{k} = 0$ for all $k > 0$.

  If $k \leqslant 0$ then $k = 0$, since $k \in \mathbb{N}$. Hence we need to prove

  $$\binom{0}{0} = \frac{0!}{0!0!}$$

  But this is true since $\binom{0}{0} = 1$ and $\frac{0!}{0!0!} = \frac{1}{1 \times 1} = 1$.

  If $k > 0$ then $\binom{0}{k} = 0$ by Definition 1.3.27.

- (**IS**) Fix $n \in \mathbb{N}$ and suppose that $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ for all $k \leqslant n$ and $\binom{n}{k} = 0$ for all $k > n$.

We need to prove that, for all $k \leqslant n + 1$, we have

$$\binom{n+1}{k} = \frac{(n+1)!}{k!(n+1-k)!}$$

and that $\binom{n+1}{k} = 0$ for all $k > n + 1$.

So fix $k \in \mathbb{N}$. There are four possible cases: either (i) $k = 0$, or (ii) $0 < k \leqslant n$, or (iii) $k = n + 1$, or (iv) $k > n + 1$. In cases (i), (ii) and (iii), we need to prove the factorial formula for $\binom{n+1}{k}$; in case (iv), we need to prove that $\binom{n+1}{k} = 0$.

(i) Suppose $k = 0$. Then $\binom{n+1}{0} = 1$ by Definition 1.3.27, and

$$\frac{(n+1)!}{k!(n+1-k)!} = \frac{(n+1)!}{0!(n+1)!} = 1$$

   since $0! = 1$. So $\binom{n+1}{0} = \frac{(n+1)!}{0!(n+1)!}$.

(ii) If $0 < k \leqslant n$ then $k = \ell + 1$ for some natural number $\ell < n$. Then $\ell + 1 \leqslant n$, so we can use the induction hypothesis to apply factorial formula to both $\binom{n}{\ell}$ and $\binom{n}{\ell+1}$. Hence

$$\binom{n+1}{k}$$
$$= \binom{n+1}{\ell+1} \qquad\qquad \text{since } k = \ell + 1$$
$$= \binom{n}{\ell} + \binom{n}{\ell+1} \qquad\qquad \text{by Definition 1.3.27}$$
$$= \frac{n!}{\ell!(n-\ell)!} + \frac{n!}{(\ell+1)!(n-\ell-1)!} \qquad\qquad \text{by induction hypothesis}$$

   Now note that

$$\frac{n!}{\ell!(n-\ell)!} = \frac{n!}{\ell!(n-\ell)!} \cdot \frac{\ell+1}{\ell+1} = \frac{(n+1)!}{(\ell+1)!(n-\ell)!} \cdot (\ell+1)$$

   and

$$\frac{n!}{(\ell+1)!(n-\ell-1)!} = \frac{n!}{(\ell+1)!(n-\ell-1)!} \cdot \frac{n-\ell}{n-\ell} = \frac{n!}{(\ell+1)!(n-\ell)!} \cdot (n-\ell)$$

Piecing this together, we have

$$\frac{n!}{\ell!(n-\ell)!} + \frac{n!}{(\ell+1)!(n-\ell-1)!}$$

$$= \frac{n!}{(\ell+1)!(n-\ell)!} \cdot [(\ell+1) + (n-\ell)]$$

$$= \frac{n!(n+1)}{(\ell+1)!(n-\ell)!}$$

$$= \frac{(n+1)!}{(\ell+1)!(n-\ell)!}$$

so that $\binom{n}{\ell+1} = \frac{(n+1)!}{(\ell+1)!(n-\ell)!}$. Now we're done; indeed,

$$\frac{(n+1)!}{(\ell+1)!(n-\ell)!} = \frac{(n+1)!}{k!(n+1-k)!}$$

since $k = \ell + 1$.

(iii) If $k = n + 1$, then

$$\binom{n+1}{k} = \binom{n+1}{n+1} \qquad\qquad \text{since } k = n+1$$

$$= \binom{n}{n} + \binom{n}{n+1} \qquad\qquad \text{by Definition 1.3.27}$$

$$= \frac{n!}{n!0!} + 0 \qquad\qquad\qquad \text{by induction hypothesis}$$

$$= 1$$

and $\frac{(n+1)!}{(n+1)!0!} = 1$, so again the two quantities are equal.

(iv) If $k > n + 1$, then $k = \ell + 1$ for some $\ell > n$, and so by Definition 1.3.27 and the induction hypothesis we have

$$\binom{n+1}{k} = \binom{n+1}{\ell+1} \stackrel{\text{IH}}{=} \binom{n}{\ell} + \binom{n}{\ell+1} = 0 + 0 = 0$$

$\square$

On first reading, this proof is long and confusing, especially in the induction step where we are required to split into four cases. We will give a much simpler proof in Section 4.2 (see Theorem 1.3.31), where we prove the statement *combinatorially* by putting the elements of two sets in one-to-one correspondence.

We can use 1.3.31 to prove useful identities involving binomial coefficients.

Example 1.3.32
Let $n, k, \ell \in \mathbb{N}$ with $\ell \leqslant k \leqslant n$ then

$$\binom{n}{k}\binom{k}{\ell} = \binom{n}{\ell}\binom{n-\ell}{k-\ell}$$

Indeed:

$$\binom{n}{k}\binom{k}{\ell}$$

$$= \frac{n!}{k!(n-k)!} \cdot \frac{k!}{\ell!(k-\ell!)} \qquad\qquad \text{by Theorem 1.3.31}$$

$$= \frac{n!k!}{k!\ell!(n-k)!(k-\ell)!} \qquad\qquad \text{combine fractions}$$

$$= \frac{n!}{\ell!(n-k)!(k-\ell)!} \qquad\qquad \text{cancel } k!$$

$$= \frac{n!(n-\ell)!}{\ell!(n-k)!(k-\ell)!(n-\ell)!} \qquad\qquad \text{multiply by } \frac{(n-\ell)!}{(n-\ell)!}$$

$$= \frac{n!}{\ell!(n-\ell!)} \cdot \frac{(n-\ell)!}{(k-\ell)!(n-k)!} \qquad\qquad \text{separate fractions}$$

$$= \frac{n!}{\ell!(n-\ell!)} \cdot \frac{(n-\ell)!}{(k-\ell)!((n-\ell)-(k-\ell))!} \qquad \text{rearranging}$$

$$= \binom{n}{\ell}\binom{n-\ell}{k-\ell} \qquad\qquad \text{by Theorem 1.3.31}$$

$\triangleleft$

Exercise 1.3.33
Proof that $\binom{n}{k} = \binom{n}{n-k}$ for all $n, k \in \mathbb{N}$ with $k \leqslant n$. $\triangleleft$

A very useful application of binomial coefficients in elementary algebra is to the binomial theorem.

Theorem 1.3.34 (Binomial theorem)
Let $n \in \mathbb{N}$ and $x, y \in \mathbb{R}$. Then

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Proof. In the case when $y = 0$ we have $y^{n-k} = 0$ for all $k < n$, and so the equation reduces to

$$x^n = x^n y^{n-n}$$

which is true, since $y^0 = 1$. So for the rest of the proof, we will assume that $y \neq 0$.

We will now reduce to the case when $y = 1$; and extend to arbitrary $y \neq 0$ afterwards.

We prove $(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$ by induction on n.

- (**BC**) $(1 + x)^0 = 1$ and $\binom{0}{0} x^0 = 1 \cdot 1 = 1$, so the statement is true when $n = 0$.

- (**IS**) Fix $n \in \mathbb{N}$ and suppose that

$$(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \qquad\qquad \text{---}(\mathbf{IH})$$

We need to show that $(1 + x)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^k$. Well,

$$
\begin{aligned}
& (1 + x)^{n+1} \\
&= (1 + x)(1 + x)^n && \text{by laws of indices} \\
&= (1 + x) \cdot \sum_{k=0}^{n} \binom{n}{k} x^k && \text{by (\textbf{IH})} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^k + x \cdot \sum_{k=0}^{n} \binom{n}{k} x^k && \text{by expanding } (x + 1) \\
&= \sum_{k=0}^{n} \binom{n}{k} x^k + \sum_{k=0}^{n} \binom{n}{k} x^{k+1} && \text{distributing } x \\
&= \sum_{k=0}^{n} \binom{n}{k} x^k + \sum_{k=1}^{n+1} \binom{n}{k-1} x^k && k \to k - 1 \text{ in second sum} \\
&= \binom{n}{0} x^0 + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right) x^k + \binom{n}{n} x^{n+1} && \text{splitting the sums} \\
&= \binom{n}{0} x^0 + \sum_{k=1}^{n} \binom{n+1}{k} x^k + \binom{n}{n} x^{n+1} && \text{by Definition 1.3.27} \\
&= \binom{n+1}{0} x^0 + \sum_{k=1}^{n} \binom{n+1}{k} x^k + \binom{n+1}{n+1} x^{n+1} && \text{see } (*) \text{ below} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k
\end{aligned}
$$

The step labelled $(*)$ holds because

$$\binom{n}{0} = 1 = \binom{n+1}{0} \qquad \text{and} \qquad \binom{n}{n} = 1 = \binom{n+1}{n+1}$$

By induction, we've shown that $(1+x)^n = \sum_{i=0}^{n} \binom{n}{k} x^k$ for all $n \in \mathbb{N}$.

When $y \neq 0$ is not necessarily equal to 1, we have that

$$(x+y)^n = y^n \cdot \left(1 + \frac{x}{y}\right)^n = y^n \cdot \sum_{k=0}^{n} \binom{n}{k} \left(\frac{x}{y}\right)^k = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

The middle equation follows by what we just proved; the leftmost and rightmost equations are simple algebraic rearrangements. $\qquad\square$

Example 1.3.35
In Example 1.3.29 we saw that

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

This follows quickly from the binomial theorem, since

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot 1^k \cdot 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}$$

Likewise, in Exercise 1.3.30 you proved that the alternating sum of binomial coefficients is zero; that is, for $n \in \mathbb{N}$, we have

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

The proof is greatly simplified by applying the binomial theorem. Indeed, by the binomial theorem, we have

$$0 = 0^n = (-1+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k=0}^{n} (-1)^k \binom{n}{k}$$

Both of these identities can be proved much more elegantly, quickly and easily using *enumerative combinatorics*. This will be the topic covered in Section 4.2. $\qquad\triangleleft$

Well-ordering principle

In a way that we will make precise in Section 5.2, the underlying reason why we can perform induction and recursion on the natural numbers is because of the way they are ordered. Specifically, the natural numbers satisfy the *well-ordering principle*: if a set of natural numbers has at least one element, then it has a least element. This sets the natural numbers apart from the other number sets; for example, $\mathbb{Z}$ has no least element, since if $a \in \mathbb{Z}$ then $a - 1 \in \mathbb{Z}$ and $a - 1 < a$.

Definition 1.3.36
Let X be a set. If X has at least one element, then we say X is **inhabited** (or **nonempty**[a]); otherwise, we say X is **empty**.

---

[a]The word 'nonempty' means 'doesn't not have elements', which is a bit silly.

Theorem 1.3.37 (Well-ordering principle)
Let X be a set of natural numbers. If X is inhabited, then X has a least element.

Strategy. Under the assumption that X is a set of natural numbers, the proposition we want to prove has the form $p \Rightarrow q$. Namely

$$X \text{ is inhabited} \quad \Rightarrow \quad X \text{ has a least element}$$

Assuming X is inhabited doesn't really give us much to work with, so let's try the contrapositive:

$$X \text{ has no least element} \quad \Rightarrow \quad X \text{ is empty}$$

The assumption that X has no least element *does* give us something to work with. Under this assumption we need to deduce that X is empty.

We will do this by 'forcing X up' by strong induction. Certainly $0 \notin X$, otherwise it would be the least element. If none of the numbers $0, 1, \ldots, n$ are elements of X then neither can $n + 1$ be, since if it were then *it* would be the least element of X. Let's make this argument formal.

Proof. Let X be a set of natural numbers containing no least element. We prove by strong induction that $n \notin X$ for all $n \in \mathbb{N}$.

- (**BC**) $0 \notin X$ since if $0 \in X$ then 0 is the least element of X.

- (**IS**) Suppose $k \notin X$ for all $0 \leqslant k \leqslant n$. If $n+1 \in X$ then $n+1$ is the least element of X; indeed, if $\ell < n+1$ then $0 \leqslant \ell \leqslant n$, so $\ell \notin X$ by the induction hypothesis. This contradicts the assumption that X has no least element, so $n+1 \notin X$.

By strong induction, $n \notin X$ for each $n \in \mathbb{N}$. Since X is a set of natural numbers, and it contains no natural numbers, it follows that X is empty. $\qquad\square$

Aside

In Section 5.2 we will encounter more general sets with a notion of 'less than', for which any inhabited subset has a 'least' element. Any such set has an induction principle, the proof of which is more or less identical to the proof of Corollary 1.3.21. This has powerful applications in computer science, where it can be used to formally verify that a computer program containing various loops will terminate: termination of a program corresponds to a particular set having a 'least' element. $\qquad\triangleleft$

The following proof that $\sqrt{2}$ is irrational is a classic application of the well-ordering principle.

Proposition 1.3.38

The number $\sqrt{2}$ is irrational.

To prove Proposition 1.3.38 we will use the following two lemmas. The first lemma we prove uses the well-ordering principle to prove that fractions can be 'cancelled to lowest terms'.

Lemma 1.3.39

Let q be a positive rational number. There is a pair of nonzero natural numbers a, b such that $q = \frac{a}{b}$ and such that the only natural number which divides both a and b is 1.

Proof. First note that we can express q as the ratio of two nonzero natural numbers, since q is a positive rational number. By the well-ordering principle, there is a *least* natural number a such that $q = \frac{a}{b}$ for some positive $b \in \mathbb{N}$.

Suppose that some natural number d other than 1 divides both a and b. Note that $d \neq 0$, since if $d = 0$ then that would imply $a = 0$. Since $d \neq 1$, it follows that $d \geqslant 2$.

Since d divides a and b, there exist natural numbers a', b' such that $a = a'd$ and $b = b'd$. Moreover, $a', b' > 0$ since $a, b, d > 0$. It follows that

$$q = \frac{a}{b} = \frac{a'd}{b'd} = \frac{a'}{b'}$$

But $d \geqslant 2$, and hence

$$a' = \frac{a}{d} \leqslant \frac{a}{2} < a$$

contradicting minimality of a. Hence our assumption that some natural number d other than 1 divides both a and b was false—it follows that the only natural number dividing both a and b is 1. □

The next lemma is a technical result that will allow us to derive a contradiction in our proof that $\sqrt{2}$ is irrational.

Lemma 1.3.40

Let $a \in \mathbb{Z}$. If a^2 is even then a is even.

Proof. We prove the contrapositive; that is, we prove that if a is odd then a^2 is odd.

Odd numbers are precisely those of the form $2k + 1$, where $k \in \mathbb{Z}$. So suppose $a = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Letting $\ell = 2k^2 + 2k$ we see that $a^2 = 2\ell + 1$, and since $\ell \in \mathbb{Z}$, it follows that a^2 is odd.

By contraposition, if a^2 is even then a is even. □

We are now ready to prove that $\sqrt{2}$ is irrational.

Proof of Proposition 1.3.38. Suppose $\sqrt{2}$ is rational. Since $\sqrt{2} > 0$, this means that we can write

$$\sqrt{2} = \frac{a}{b}$$

where a and b are both positive natural numbers. By Lemma 1.3.39, we may assume that the only natural number dividing a and b is 1.

Multiplying the equation $\sqrt{2} = \frac{a}{b}$ and squaring yields

$$a^2 = 2b^2$$

Hence a^2 is even. By Lemma 1.3.40, a is even, so we can write $a = 2c$ for some $c > 0$. Then $a^2 = (2c)^2 = 4c^2$, and hence

$$4c^2 = 2b^2$$

Dividing by 2 yields

$$2c^2 = b^2$$

77

and hence b^2 is even. By Lemma 1.3.40 again, b is even.

But if a and b are both even, the natural number 2 divides both a and b. This contradicts the fact that the only natural number dividing both a and b is 1. Hence our assumption that $\sqrt{2}$ is rational is incorrect, and $\sqrt{2}$ is irrational.   □

Writing tip

In the proof of Proposition 1.3.38 we could have separately proven that a^2 being even implies a is even, and that b^2 being even implies b is even. This would have required us to repeat the same proof twice, which is somewhat tedious! Proving auxiliary results (lemmas) separately and then applying them in theorems can improve the readability of the main proof, particularly when the auxiliary results are particularly technical. Doing so also helps emphasise the important steps.   ◁

Exercise 1.3.41

What goes wrong in the proof of Proposition 1.3.38 if we try instead to prove that $\sqrt{4}$ is irrational?   ◁

Exercise 1.3.42

Prove that $\sqrt{3}$ is irrational.   ◁

Chapter 2

Logic, sets and functions

2.1 Symbolic logic

Symbolic logic arises from the observation that propositions—that is, results about mathematical objects—can themselves be treated as mathematical objects. So that we can study propositions in an abstract setting, we will represent propositions by symbols, typically the letters p, q, r and s. (It is rare that we will speak about more than four propositions at the same time; if we need to, we'll just use more letters!) We call these **propositional variables**: they are 'propositional' because they represent propositions, and they are 'variables' because we will make no assumptions about their truth value (unless explicitly stated).

This symbolic approach will allow us to decompose complex propositions into simpler ones and investigate their logical structure, which in turn will help us work out how to structure our proofs.

For example, consider the following:

> Let n be an integer. If n is prime and $n > 2$ then n is odd.

The three statements 'n is prime', '$n > 2$' and 'n is odd' are all propositions in their own right, despite the fact that they all appear in a more complex proposition. We can really examine the logical structure of the proposition by replacing these simpler propositions with symbols. Referring to 'n is prime' as p, '$n > 2$' as q, and 'n is odd' as r, the structure of the second proposition is:

> If p and q, then r.

Thus the propositions p, q, r are tied together by language, namely the word 'and' and the construction 'if–then'. Soon we will give precise definitions of what these words mean; in the abstract setting they are called *logical operators*.

Looking at the logical structure of complex propositions allows us to make an educated guess about how to proceed with a proof of the statement if it is true. Indeed, it is a safe bet that in order to prove 'if p and q, then r', you should derive r from the assumption that p and q are both true.

The value of reducing statements to symbolic expressions is that it forces us to remove ambiguity and gives a clear-cut and precise way of knowing when we've done what we set out to do.

Logical operators

A *logical operator*, intuitively speaking, is a rule that constructs a new proposition out of other propositions. For example, as we saw in Section 1.2, from propositions p, q we can construct several new propositions off the bat:

$$\text{`}p \text{ and } q\text{'} \qquad \text{`}p \text{ or } q\text{'} \qquad \text{`if } p, \text{ then } q\text{'} \qquad \text{`}p \text{ is false'}$$

These constructions correspond with the logical operators of *conjunction*, *disjunction*, *implication* and *negation*, respectively—and there are many more where they came from!

Relying on our understanding of the English language to interpret what these logical operators mean will cause us some trouble; the next few pages introduce the most commonly used logical operators, together with their precise definitions. To get us started, we will need the definition of a *propositional formula*; these are the symbolic expressions which represent propositions built from smaller propositions using logical operators.

Definition 2.1.1
A **propositional formula** is an expression built from **propositional variables** $p, q, r, s, \dots$ and **logical operators** (to be defined individually below).

Intuitively, propositional variables will refer to basic propositions, such as '3 is odd', and propositional formulae will refer to more complex propositions, such as '3 is odd and 6 is not a perfect square'.

Conjunction ('and', $\wedge$)

Conjunction is the logical operator which makes precise what we mean when we say 'and'.

Definition 2.1.2
Let p and q be propositions. The **conjunction** of p and q, denoted $p \wedge q$ (read: 'p and q') (LaTeX code: `\wedge`) is a proposition which is true if both p and q are true, and false otherwise.

Aside
Strictly speaking, the definitions of logical operators should be given in terms of *propositional variables*, rather than propositions themselves; these truth values then extend *inductively* to general propositional formulae, in a sense to be made precise in Section 5.3.

These propositional formulae only *represent* propositions—the latter cannot be treated formally because they are statements in natural language, not mathematical objects. This perspective is confusing on first exposure, so we will simplify matters by blurring the distinction between propositional variables, propositional formulae and propositions. ◁

It is not always obvious when conjunction is being used; sometimes it sneaks in without the word 'and' ever being mentioned! Be on the look-out for occasions like this, such as in the following exercise.

Example 2.1.3

We can express the proposition '7 is an integer greater than 5' in the form $p \wedge q$, by letting p represent the proposition '7 is an integer' and let q represent the proposition '7 is greater than 5'. In order to prove that 7 is an integer greater than 5, we would need to give a proof that 7 is an integer, and a proof that 7 is greater than 5. ◁

Exercise 2.1.4

Express the proposition 'Clive is a mathematician who lives in Pittsburgh' in the form $p \wedge q$, for propositions p and q. ◁

The truth value of a propositional formula is determined by the truth values of the propositional variables it contains. As such, the truth value of $p \wedge q$ is defined in terms of the truth values of p and of q. An easy way to specify this information isusing a **truth table**, which tells us the truth value of $p \wedge q$ for all possible assignments of truth values to p and q:

p	q	$p \wedge q$		
✓	✓	✓	←	$p \wedge q$ is true when p is true and q is true
✓	×	×	←	$p \wedge q$ is false when p is true and q is false
×	✓	×	←	$p \wedge q$ is false when p is false and q is true
×	×	×	←	$p \wedge q$ is false when p is false and q is false

Here ✓ (LATEX code: `\checkmark`) denotes 'true' and × (LATEX code: `\times`) denotes 'false'.[a] There is a row for each possible assignment of 'true' (✓) or 'false' (×) to the propositional variables, and a column for each variable and the proposition we're interested in.

Disjunction ('or', ∨)

Disjunction is the logical operator that makes precise what we mean by 'or'.

---

[a] Instead of ✓,×, some authors use ⊤,⊥ (LATEX code: `\top,\bot`) or T, F or $1, 0$.

The word 'or' is especially context-dependent in English: if you say to me, 'you can have a slice of cake or you can have a chocolate bar,' does that mean I can have both, or not? We remove this ambiguity with the following definition; and to clarify, with this definition of 'or', I *can* have both the cake and the chocolate bar. Yummy.

> **Definition 2.1.5**
> Let p and q represent propositions. The **disjunction** of p and q, denoted $p \vee q$ (read: 'p or q') (LaTeX code: `\vee`) is the proposition which is true if at least one of p or q is true, and false otherwise.

Exercise 2.1.6
Using Definition 2.1.5, write down a truth table for $p \vee q$ (see page 82 for how it was done for $p \wedge q$). ◁

The real power of truth tables comes when investigating how logical operators interact with each other.

Example 2.1.7
Given propositions p, q, r, when is $(p \wedge q) \vee (p \wedge r)$ true? It's not immediately obvious, but we can work it out by breaking it down into its component parts, namely the propositions $p \wedge q$ and $p \wedge r$; we'll call these **auxiliary propositions**. We can then make a column for each variable, each auxiliary proposition, and the main proposition, to find its truth values.

p	q	r	$p \wedge q$	$p \wedge r$	$(p \wedge q) \vee (p \wedge r)$
✓	✓	✓	✓	✓	✓
✓	✓	✗	✓	✗	✓
✓	✗	✓	✗	✓	✓
✓	✗	✗	✗	✗	✗
✗	✓	✓	✗	✗	✗
✗	✓	✗	✗	✗	✗
✗	✗	✓	✗	✗	✗
✗	✗	✗	✗	✗	✗

variables   auxiliary prop$^\text{n}$s   main proposition

We can then read off the table precisely when $(p \wedge q) \vee (p \wedge r)$ is true, by comparing the entries in its column with the corresponding truth values of p, q, r. ◁

Aside
If you haven't already mixed up $\wedge$ and $\vee$, you probably will soon, so here's a way of remembering which is which:

mac n cheese

If you forget whether it's $\wedge$ or $\vee$ that means 'and', just write it in place of the 'n' in 'mac n cheese':

$$\text{mac} \wedge \text{cheese} \qquad\qquad \text{mac} \vee \text{cheese}$$

Clearly the first looks more correct, so $\wedge$ means 'and'. (For any Brits among you, the mnemonic 'fish n chips' works just as well.) ◁

Exercise 2.1.8
Write a truth table for the proposition $p \wedge (q \vee r)$. Compare it with the truth table for $(p \wedge q) \vee (p \wedge r)$. What do you notice? ◁

Hopefully, if you did the previous exercise correctly, you'll have noticed that the column for $p \wedge (q \vee r)$ is identical to the column for $(p \wedge q) \vee (p \wedge r)$. So in some sense, these two propositions are 'the same'.

Definition 2.1.9
Two propositional formulae depending on the same propositional variables are **logically equivalent** if they have the same truth value as each other, no matter what the assignment of truth values to their propositional variables.

Proof tip
To prove that two propositions are logically equivalent, you can draw a truth table containing both propositions; if their columns are identical, then they are logically equivalent. ◁

Example 2.1.10
The propositional formulae $p \wedge (q \wedge r)$ and $(p \wedge q) \wedge r$ are equivalent. To prove this, we'll combine the truth tables for both propositions, with auxiliary columns for the propositions $q \wedge r$ and $p \wedge q$.

p	q	r	$q \wedge r$	$p \wedge (q \wedge r)$	$p \wedge q$	$(p \wedge q) \wedge r$
✓	✓	✓	✓	✓	✓	✓
✓	✓	✕	✕	✕	✓	✕
✓	✕	✓	✕	✕	✕	✕
✓	✕	✕	✕	✕	✕	✕
✕	✓	✓	✓	✕	✕	✕
✕	✓	✕	✕	✕	✕	✕
✕	✕	✓	✕	✕	✕	✕
✕	✕	✕	✕	✕	✕	✕

Evidently the two propositional formulae are equivalent since their columns are identical. Indeed, $p \wedge (q \wedge r)$ and $(p \wedge q) \wedge r$ are both true if all three of p, q and r are true, and they're both false if one or more of p, q or r is false. ◁

Negation ('not', ¬)

So far we only officially know how to prove that true propositions are true. The negation operator makes precise what we mean by 'not', which allows us to prove that false propositions are false.

Definition 2.1.11
Let p be a proposition. The **negation** of p, denoted $\neg p$ (read: 'not p') (LATEX code: `\neg`) is the proposition which is true if p is false, and false if p is true.

The truth table for the negation operator is very simple, since it is defined in terms of only one propositional variable:

p	$\neg p$
✓	✗
✗	✓

Example 2.1.12
What follows is the truth table for $p \wedge (\neg q)$ (read 'p and not q'); we include a column for $\neg q$ because it appears inside the proposition.

p	q	$\neg q$	$p \wedge (\neg q)$
✓	✓	✗	✗
✓	✗	✓	✓
✗	✓	✗	✗
✗	✗	✓	✗

◁

Theoretically we could stop here: the three operators we've seen, $\wedge$, $\vee$ and $\neg$, can be used to give any combination of truth values to a compound proposition, in *any* number of variables![b] For example, try the following exercise:

---

[b] Proving this claim and investigating other 'complete sets' of operators would make a nice final project!

Exercise 2.1.13

Using only two variables p, q and the operators $\wedge, \vee, \neg$, write down a propositional formula whose truth table column is:

p	q	???
✓	✓	✗
✓	✗	✓
✗	✓	✓
✗	✗	✗

Did you use all three of the permitted logical operators? If so, find another equivalent propositional formula defined using only two of the operators. We will encounter this later as the *exclusive disjunction* operator, see Definition 2.1.21.   ◁

The following theorem is our first big result of the course. It is a pair of dual results which relate conjunction, disjunction and negation. Informally the result says:

- Saying 'neither p nor q is true' is the same as saying 'both p and q are false';

- Saying 'p and q are not both true' is the same as saying 'at least one of p and q is false'.

Let's make this precise:

Theorem 2.1.14 (De Morgan's laws for logical operators)

Let p and q be propositions. Then

(a) $\neg(p \vee q)$ is logically equivalent to $(\neg p) \wedge (\neg q)$;

(b) $\neg(p \wedge q)$ is logically equivalent to $(\neg p) \vee (\neg q)$.

Proof. (a) The following truth table demonstrates that $\neg(p \vee q)$ and $(\neg p) \wedge (\neg q)$ have the same truth value for any assignment of truth values to p and q; hence they are logically equivalent.

p	q	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$(\neg p) \wedge (\neg q)$
✓	✓	✓	✗	✗	✗	✗
✓	✗	✓	✗	✗	✓	✗
✗	✓	✓	✗	✓	✗	✗
✗	✗	✗	✓	✓	✓	✓

The proof of (b) mimics the proof of (a) and is left as an exercise. □

Corollary 2.1.15

(a) The operator $\wedge$ can be expressed in terms of $\vee$ and $\neg$;

(b) The operator $\vee$ can be expressed in terms of $\wedge$ and $\neg$.

Proof. (a) First note that, if p is any proposition, then p is equivalent to $\neg(\neg p)$, which we'll write simply $\neg\neg p$. This is demonstrated by the following truth table

p	$\neg p$	$\neg\neg p$
✓	✗	✓
✗	✓	✗

Therefore, given any propositions p and q,

- $p \wedge q$ is equivalent to $(\neg\neg p) \wedge (\neg\neg q)$;

- ...which is equivalent to $\neg((\neg p) \vee (\neg q))$ by De Morgan's laws applied to the propositions $\neg p$ and $\neg q$.

Since $p \wedge q$ is equivalent to $\neg((\neg p) \vee (\neg q))$, which contains only the operators $\neg$ and $\vee$, the result has been shown.

The proof of (b) mimics the proof of (a) and is left as an exercise. □

This means that just *two* operators, say $\wedge$ and $\neg$, suffice for expressing all other possible operators! However, there is no real virtue in being stingy with our operators; after all, the whole point of everything we're doing is to communicate mathematical ideas. The propositional formula

$$\neg((\neg p) \vee (\neg q))$$

is a lot harder to read and *much* harder to understand than the expression

$$p \wedge q$$

So we'll keep $\wedge$ for now, and we'll go one step further: there is one especially crucial operator that we have not yet defined, namely *implication*.

Implication ('if...then...', $\Rightarrow$)

The implication operator makes precise what we mean when we say 'if p, then q' or 'p implies q'. The definition of the implication operator might seem unnatural at first, but this will be discussed as an aside after the definition has been given.

Definition 2.1.16

Let p and q be propositions. The proposition $p \Rightarrow q$ (read: 'if p then q', or 'p implies q') (LATEX code: `\Rightarrow`) is *false* if p is true and q is false, and true otherwise.

The truth table for the implication operator is as follows:

p	q	$p \Rightarrow q$
✓	✓	✓
✓	✗	✗
✗	✓	✓
✗	✗	✓

Exercise 2.1.17

Use a truth table to show that $p \Rightarrow q$ is equivalent to $(\neg p) \vee q$.   ◁

Exercise 2.1.18

Let p and q be propositional variables. Find a propositional formula which is equivalent to $\neg(p \Rightarrow q)$, using only the operators $\wedge$, $\vee$ and $\neg$. How could you use this equivalence to prove that an implication $p \Rightarrow q$ is false?   ◁

Aside

The biggest source of confusion for most people about the implication operator is why $p \Rightarrow q$ is true whenever p is false, even if q is also false.

The reason behind this confusion is that people tend to think of implication in terms of *causation*, i.e. that $p \Rightarrow q$ is a statement asserting 'q is true because of p'. This is *not* what 'implies' means here! The statement $p \Rightarrow q$ says nothing about the truth value of q *unless* we know that p is true.

Think of it this way: $p \Rightarrow q$ means that I can give you a proof of q so long as you can give me a proof of p. If p has no proofs, my job is done before I even started! The only way I can fail is if you have a proof of p but I have no proof of q.   ◁

Other operators (⇔, ⊕ ...)

There are many other operators we can define, but we will focus on just two more.

Definition 2.1.19

Let p and q be propositions. The proposition $p \Leftrightarrow q$ (read 'p if and only if q') (LaTeX code: `\Leftrightarrow`) is true when p and q have the same truth value, and false otherwise. The operator $\Leftrightarrow$ is called the **biconditional operator**.

Exercise 2.1.20

Show that $p \Leftrightarrow q$ is logically equivalent to $(p \Rightarrow q) \wedge (q \Rightarrow p)$. ◁

Definition 2.1.21

Let p and q be propositions. The proposition $p \oplus q$ (read 'p or q but not both') (LaTeX code: `\oplus`) is true when p and q have different truth values, and false otherwise. The operator $\oplus$ is called the **exclusive disjunction operator**.

Computer scientists and logicians often refer to $\oplus$ as 'xor' or 'exclusive or'.

Proof principles

In Section 1.2, we saw how to prove statements using the techniques of *proof by contradiction* and the *law of excluded middle*. We are now in a position to make these proof techniques precise from a symbolic perspective. For good measure, we will now also introduce another useful technique, called *proof by contraposition*.

Definition 2.1.22

The **law of excluded middle** is the assertion that $p \vee (\neg p)$ is true for all propositions p.

In Section 1.2, we attributed the usefulness of the law of excluded middle to the fact that we can prove a proposition is true by splitting into cases based on whether another proposition is true.

Exercise 2.1.23

Let p, q, r be propositions. Prove that $(p \vee q) \Rightarrow r$ is logically equivalent to $(p \Rightarrow r) \wedge (q \Rightarrow r)$. ◁

The following corollary is the technical result underpinning the reason why the law of excluded middle is so useful in proofs.

Corollary 2.1.24
Let p and q be propositions. If $p \Rightarrow q$ and $\neg p \Rightarrow q$ are true, then q is true.

Proof. By Exercise 2.1.23, it suffices to show that if $(p \vee \neg p) \Rightarrow q$ is true, then q is true. By the law of the excluded middle, $p \vee \neg p$ is true, and hence $(p \vee \neg p) \Rightarrow q$ is true if and only if q is true. But this is precisely what we wanted to prove. $\qquad\square$

Proof by contradiction can also be proved to be a valid proof technique by considering truth tables.

Theorem 2.1.25 (Principle of contradiction)
Let p and q be propositions, and suppose that q is false. If $p \Rightarrow q$ is true, then p is false.

Proof. Consider the truth table of the proposition $p \Rightarrow q$:

p	q	$p \Rightarrow q$
✓	✓	✓
✓	✗	✗
✗	✓	✓
✗	✗	✓

The only row in which q is false and $p \Rightarrow q$ is true is the fourth row, in which p is false. $\quad\square$

We won't dwell on these proof techniques, since we already saw them in Section 1.1. However, there is a very useful proof technique that we haven't seen yet, called *proof by contraposition*. This is particularly useful for when you're trying to prove an implication and can't quite get it to work.

Definition 2.1.26
Let p and q be propositions. The **contrapositive** of the proposition $p \Rightarrow q$ is the proposition $(\neg q) \Rightarrow (\neg p)$.

Theorem 2.1.27 (Principle of contraposition)
Let p and q be propositions. Then $p \Rightarrow q$ is logically equivalent to $(\neg q) \Rightarrow (\neg p)$.

Proof. Consider the following truth table:

p	q	$p \Rightarrow q$	$\neg q$	$\neg p$	$(\neg q) \Rightarrow (\neg p)$
✓	✓	✓	✗	✗	✓
✓	✗	✗	✓	✗	✗
✗	✓	✓	✗	✓	✓
✗	✗	✓	✓	✓	✓

Since the third and sixth columns are identical, the two propositions are logically equivalent.

□

Proof tip

To prove an implication $p \Rightarrow q$, you can instead prove the implication $\neg q \Rightarrow \neg p$; that is, assuming that q is false, show that p must be false. We then say $p \Rightarrow q$ is true 'by contraposition'. ◁

Example 2.1.28

Fix two natural numbers m and n. We will prove that if $mn > 64$, then either $m > 8$ or $n > 8$. Letting p be the proposition '$mn > 64$', q be the proposition '$m > 8$' and r be the proposition '$n > 8$', the statement 'if $mn > 64$, then either $m > 8$ or $n > 8$' becomes

$$p \Rightarrow (q \vee r)$$

By contraposition, this is equivalent to

$$\neg(q \vee r) \Rightarrow \neg p$$

By de Morgan's laws, this is equivalent to

$$((\neg q) \wedge (\neg r)) \Rightarrow \neg p$$

Let's spell this out. The proposition $\neg p$ means $mn \leqslant 64$, and the proposition $(\neg q) \wedge (\neg r)$ means that $m \leqslant 8$ and $n \leqslant 8$. So what we need to prove is:

If $m \leqslant 8$ and $n \leqslant 8$ then $mn \leqslant 64$.

Well this is certainly true! If you multiply two natural numbers which are less than or equal to 8, then their product must be less than or equal to 8^2, which is equal to 64. ◁

Corollary 2.1.29

Let p and q be propositions. Then $p \Leftrightarrow q$ is equivalent to

$$(p \Rightarrow q) \wedge ((\neg p) \Rightarrow (\neg q))$$

Proof. Left as an exercise. You can prove it directly, or apply reasoning you've already acquired to the result of Theorem 2.1.27.   □

The logical equivalence set up by Corollary 2.1.29 is useful in proofs of some biconditional statements.

Whilst the contrapositive of an implication $p \Rightarrow q$ is equivalent to $p \Rightarrow q$, its *converse* is not.

Definition 2.1.30
Let p and q be propositions. The **converse** of the proposition $p \Rightarrow q$ is the proposition $q \Rightarrow p$.

Exercise 2.1.31
Demonstrate by truth table that, for propositional variables p and q, the propositions $p \Rightarrow q$ and $q \Rightarrow p$ are *not* logically equivalent. Provide an example of an implication and its converse that demonstrate this.   ◁

✴ Tautologies

There are many instances when a proposition expressed in terms of propositional variables is true no matter what truth values are assigned to the variables.

Example 2.1.32
Let p be a proposition. The following propositions are all true, regardless of whether p is true or false:
$$p \Rightarrow p, \quad p \Leftrightarrow (p \wedge p), \quad p \Leftrightarrow (p \vee p)$$

◁

Definition 2.1.33
A **tautology** is a propositional formula which is true regardless of the truth values assigned to its variables.

Example 2.1.34
Let p and q be propositions. We'll prove that

$$p \Rightarrow (q \Rightarrow p)$$

is a tautology by looking at its truth table:

p	q	$q \Rightarrow p$	$p \Rightarrow (q \Rightarrow p)$
✓	✓	✓	✓
✓	✗	✓	✓
✗	✓	✗	✓
✗	✗	✓	✓

The column for $p \Rightarrow (q \Rightarrow p)$ has ✓ in every row, so is a tautology.

An alternative proof is as follows. The only way that $p \Rightarrow (q \Rightarrow p)$ can be *false* is if p is true and $q \Rightarrow p$ is false. But if p is true then $q \Rightarrow p$ is necessarily true, so this is impossible. ◁

Exercise 2.1.35
How might fact proved in Exercise 2.1.34, that $p \Rightarrow (q \Rightarrow p)$ is a tautology, be useful in a proof of a conditional statement? Where did we use this in the proof of Proposition 1.2.19? ◁

Exercise 2.1.36
Let p, q, r be propositions. Prove that

$$[p \Rightarrow (q \Rightarrow r)] \Rightarrow [(p \Rightarrow q) \Rightarrow (p \Rightarrow r)]$$

is a tautology. ◁

Free and bound variables

If all we have to work with is propositions then our ability to do mathematical reasoning will be halted pretty quickly. For example, consider the following statement:

$$x \text{ is divisible by } 7$$

This statement seems like the kind of thing we should probably be able to work with if we're doing mathematics. It makes sense if x is a whole number, such as 28 or 41; but it doesn't make sense at all if x is a parrot called Alex.[c] In any case, even when it does make sense, its truth depends on the value of x; indeed, '28 is divisible by 7' is a true proposition, but '41 is divisible by 7' is a false proposition.

This means that the statement 'x is divisible by 7' isn't a proposition—*quel horreur*! But it *almost* is a proposition: if we know that x refers somehow to a whole number, then it

---

[c] Alex the parrot is the only non-human animal to have ever been observed to ask an existential question; he died in September 2007. It is unlikely that Alex was divisible by 7, even when he was alive.

becomes a proposition as soon as a particular numerical value of x is specified. Such a symbol x is called a **free variable** or **parameter**. To indicate that a statement p contains x as a free variable, we will write $p(x)$. When we replace x by a specific value, say 28, we write $p(28)$; this is called **substitution** of a value for a variable.

Some statements might have several free variables. For example, the statement '$y = x + 3$' is a true proposition when $x = 3$ and $y = 6$, but it's a false proposition when $x = 1$ and $y = 2$. What really matters is that we have a notion of what it is appropriate to use as values of x and y—namely, they should be numbers—and that whenever we use such values, what comes out is a proposition. To indicate that a statement p contains x and y as free variables, we will write $p(x, y)$.

Definition 2.1.37

A **logical formula** is a statement containing some number of **free variables**, each with a specified **range**, such that the statement becomes a proposition when values for all the variables are substituted from their respective ranges.

Example 2.1.38

As mentioned before, the statement $p(x)$ defined by 'x is divisible by 7' is a logical formula with one free variable x, whose range is the set $\mathbb{Z}$ of integers. Then, for example, $p(28)$ is a true proposition and $p(41)$ is a false proposition.   ◁

Exercise 2.1.39

Write down a logical formula $p(x, y)$ with two free variables x, y with range $\mathbb{Z}$. Is the proposition $p(3, 7)$ true or false? For what values of $y \in \mathbb{Z}$ is $p(0, y)$ true?   ◁

We can obtain propositions from logical formulae in ways other than simply substituting for a variable. For example, the assertion that *every* substitution for a variable makes the formula true, is in itself a proposition. This can be done using *quantifiers*.

Universal quantifier ($\forall$)

The universal quantifier makes precise what we mean when we say 'for all', or '$p(x)$ is always true no matter what value x takes'.

Definition 2.1.40

Let $p(x)$ be a logical formula with free variable x, whose range is a set X. The proposition '$\forall x \in X, p(x)$' (read 'for all x in X, $p(x)$') (LATEX code: `\forall`) is true if $p(x)$ is true no matter what value of x is substituted from X, and false otherwise. The symbol $\forall$ is called the **universal quantifier**.

Note that the fact that the variable x ranges over the set X is built into the notation '$\forall x \in X$'.

Exercise 2.1.41

Let $p(x)$ be the formula 'x is divisible by 7', where x ranges over the integers. Write out the propositions $\forall x \in \mathbb{Z}$, $p(x)$ and $\forall x \in \mathbb{Z}$, $\neg p(x)$ in English. ◁

Example 2.1.42

Consider the proposition

> For all integers n, if n is even then $n + 1$ is odd.

This proposition takes the form

$$\forall n \in \mathbb{Z}, \ (p(n) \Rightarrow q(n))$$

where $p(n)$ is the statement 'n is even' and $q(n)$ is the statement '$n + 1$ is odd'.

A proof would proceed as follows:

  (i) Let n be an (arbitrary) integer.

 (ii) Assume that n is even.

(iii) From the above two assumptions, derive the fact that $n + 1$ is odd.

Step (i) is introduction of the variable n. For the rest of the proof we may treat n as if it's any old integer, but whatever we say about n must be true no matter what value n takes. Having introduced n, we now need to prove $p(n) \Rightarrow q(n)$.

Step (ii) uses our proof strategy for proving implications: prove the proposition to the right of the $\Rightarrow$ symbol from the assumption that what is to the left of the $\Rightarrow$ symbol is true. This means that for the remainder of the proof, we may assume that n is even.

Step (iii) finishes off the proof. ◁

Common error

Consider the following (non-)proof of the proposition $\forall n \in \mathbb{Z}$, $n^2 \geqslant 0$.

> Let n be an arbitrary integer, say $n = 17$. Then $17^2 = 289 \geqslant 0$, so the statement is true.

The error made here is that the *writer* has picked an arbitrary value of n, not the *reader*. (In fact, the above argument actually proves $\exists n \in \mathbb{Z}$, $n^2 \geqslant 0$; see below.)

Your proof should make no assumptions about the value of n other than its range. Here is a correct proof:

> Let n be an arbitrary integer. Either $n \geqslant 0$ or $n < 0$. If $n \geqslant 0$ then $n^2 \geqslant 0$, since the product of two nonnegative numbers is nonnegative; if $n < 0$ then $n^2 \geqslant 0$, since the product of two negative numbers is positive.

$\triangleleft$

Existential quantifier ($\exists$)

The existential quantifier makes precise what we mean when we say 'there exists', or '$p(x)$ is true for some value of x in its range'.

Definition 2.1.43
Let $p(x)$ be a logical formula with free variable x, ranging over a set X. The proposition '$\exists x \in X$, $p(x)$' (read 'there exists x in X such that $p(x)$') (LaTeX code: `\exists`) is true if $p(x)$ is true for at least one substitution of the variable x from X. The symbol $\exists$ is called the **existential quantifier**.

Exercise 2.1.44
Let $p(x)$ be the formula 'x is divisible by 7', where x ranges over the integers. Write out the propositions $\exists x$, $p(x)$ and $\exists x$, $\neg p(x)$ in English. For each, either prove that it is true, or prove that it is false. $\triangleleft$

Example 2.1.45
Consider the proposition

> There exists a natural number which is odd and greater than 3.

This proposition takes the form $\exists n \in \mathbb{N}, (p(n) \wedge q(n))$, where $p(n)$ is the statement 'n is odd' and $q(n)$ is the statement 'n is greater than 3'.

A proof would proceed by finding a particular value of n such that $p(n)$ and $q(n)$ are both true. Well, we know that 5 is odd, and 5 is certainly greater than 3! This means that $p(5) \wedge q(5)$ is true. Since we've proved the proposition for a value of n, we now know that $\exists n \in \mathbb{N}, (p(n) \wedge q(n))$ is true. $\triangleleft$

From now on, if a variable's range is irrelevant or is clear from context, we will simply omit reference to its range. For example, if it is clear that the variable n refers to an integer, we will write $\forall n,\ p(n)$ and $\exists n,\ p(n)$ instead of $\forall n \in \mathbb{Z},\ p(n)$ and $\exists n \in \mathbb{Z},\ p(n)$, respectively.

Quantifiers behave in an interesting way with the negation operator. Intuitively this makes sense: for example, to show 'x is even' isn't true for *all* x, it suffices to find a single x for which 'x is even' is false. Thus, we can disprove $\forall x, (x \text{ is even})$ by proving $\exists x, (x \text{ is not even})$. This will be useful when cooking up proof strategies.

> **Theorem 2.1.46** (De Morgan's laws for quantifiers)
> Let $p(x)$ be a logical formula. Then
> (a) $\neg(\exists x,\ p(x))$ is logically equivalent to $\forall x, (\neg p(x))$;
>
> (b) $\neg(\forall x,\ p(x))$ is logically equivalent to $\exists x, (\neg p(x))$.

Proof. (a) We need to show that $\forall x, (\neg p(x))$ is true when $\neg(\exists x,\ p(x))$ is true, and false when it is false.

Suppose $\neg(\exists x,\ p(x))$ is true. Then $\exists x,\ p(x)$ is false, which means it is not the case that at least one value of x makes $p(x)$ true. Since no values of x make $p(x)$ true, this must mean that *all* values of x make $\neg p(x)$ true. So from the assumption that x takes any value whatsoever, we know that $\neg p(x)$ is true. Hence $\forall x, (\neg p(x))$ is true.

Conversely, suppose $\neg(\exists x,\ p(x))$ is false. Then $\exists x,\ p(x)$ is true, so there is some fixed value of x making $p(x)$ true. Therefore it is not the case that $\neg p(x)$ is true for all values of x: if x takes this special value then $p(x)$ is true, so $\neg p(x)$ is false! Hence $\forall x, (\neg p(x))$ is false.

The proof of (b) mimics the proof of (a) and is left to the reader. $\qquad \square$

Bound variables

When a variable is quantified, we say it is **bound**. Bound variables behave differently from free variables in a number of ways, for example

- Propositions cannot have free variables, but they can have bound variables.

- It is possible to substitute a value for a free variable, but not for a bound variable.

Example 2.1.47

Consider the following formula, in which the variables x, y, z all have range $\mathbb{Z}$:

$$\forall x \in \mathbb{Z},\ \exists y \in \mathbb{Z},\ x^2 + y^2 + z^2 = 1$$

In this formula, the variables x and y are bound, but the variable z is free. To see this, note that we *can* substitute for z; substituting 2 for z yields:

$$\forall x,\ \exists y,\ x^2 + y^2 + 2^2 = 1$$

which is a false proposition. However we cannot substitute for x or y; trying to substitute 2 for x yields:

$$\forall 2,\ \exists y,\ 2^2 + y^2 + z^2 = 1$$

which *must* be nonsense: the phrase 'for all 2, ...' doesn't even make sense!   ◁

Exercise 2.1.48

For each of the following formulae, where all variables range over the integers, write down the formula using quantifiers and specify which variables are free and which are bound:

(a) If n is prime and $n > 2$ then n is odd.

(b) There exist x and y such that $ax + by = 1$.

(c) No integer value of x satisfies $0x = 1$.

◁

Quantifier alternation

Compare the following two statements:

  (i) For every door, there is a key that can unlock it.

 (ii) There is a key that can unlock every door.

Letting the variables x and y refer to doors and keys, respectively, and letting $p(x, y)$ be the statement 'door x can be unlocked by key y', we can formulate these statements as:

  (i) $\forall x,\ \exists y,\ p(x, y)$

 (ii) $\exists y,\ \forall x,\ p(x, y)$

This is a typical 'real-world' example of what is known as *quantifier alternation*—the two statements differ only by the order of the front-loaded quantifiers, and yet they say very different things. Statement (i) requires every door to be unlockable, but the keys might be different for different doors; statement (ii), however, implies the existence of some kind of 'master key' that can unlock all the doors.

Here's another example with a more mathematical nature:

Exercise 2.1.49

Let $p(x, y)$ be the statement '$x + y$ is even'.

- Prove that $\forall x \in \mathbb{Z}$, $\exists y \in \mathbb{Z}$, $p(x, y)$ is true.

- Prove that $\exists y \in \mathbb{Z}$, $\forall x \in \mathbb{Z}$, $p(x, y)$ is false.

$\triangleleft$

In both of the foregoing examples, you might have noticed that the '$\forall\exists$' statement says something *weaker* than the '$\exists\forall$' statement—in some sense, it is easier to make a $\forall\exists$ statement true than it is to make an $\exists\forall$ statement true.

This idea is formalised in Theorem 2.1.50 below, which despite its abstract nature, has an extremely simple proof.

Theorem 2.1.50

Let $p(x, y)$ be a logical formula. Then

$$\exists y, \, \forall x, \, p(x, y) \Rightarrow \forall x, \, \exists y, \, p(x, y)$$

Proof. Suppose $\exists y, \forall x, p(x, y)$ is true. We need to prove that $\forall x, \exists y, p(x, y)$ is true.

Using our assumption $\exists y, \forall x, p(x, y)$, we may choose y^* such that $\forall x, p(x, y^*)$ is true.

Now to prove $\forall x, \exists y, p(x, y)$, fix x. We need to find y such that $p(x, y)$ is true. But $p(x, y^*)$ is true by our above assumption! So we're done. $\qquad\square$

Statements of the form $\exists y, \forall x, p(x, y)$ imply some kind of *uniformity*: a value of y making $\forall x, p(x, y)$ true can be thought of as a 'one size fits all' solution to the problem of proving $p(x, y)$ for a given x. Later in your studies, it is likely that you will encounter the word 'uniform' many times—it is precisely this notion of quantifier alternation that the word 'uniform' refers to.

2.2   Sets and set operations

With a system of logical notation under our belt, we're now ready to introduce the notion of a *set* with a notch more precision than in Section 1.1. At their core, sets seem extremely simple—a set is just collections of objects—except this characterisation of a set leads to logical inconsistencies.[d]   We overcome these inconsistencies by restricting ourselves to working inside a *universe* $\mathcal{U}$, which we consider to be a set which is so big that it contains all of the mathematical objects that we want to talk about. This definition seems circular— Section B.2 aims to clear up this confusion.

Definition 2.2.1

A **set** is a collection of **elements** from a specified **universe of discourse**. The collection of everything in the universe of discourse is called the **universal set** (or just **universe**), denoted $\mathcal{U}$ (LaTeX code: `\mathcal{U}`).
The formula $x \in X$ (LaTeX code: `\in`) denotes the statement that x is an element of X, where the range of x is the universe of discourse. We write $x \notin X$ (LaTeX code: `\not\in`) to mean $\neg(x \in X)$, i.e. that x is not an element of X.

This definition seems a bit weird—and it is—so if you're confused, then don't worry, as we will avoid reference to it as much as possible. The only property of $\mathcal{U}$ that we'll need is that if we speak about *any* mathematical object at all, except for $\mathcal{U}$ itself, then this mathematical object is an element of $\mathcal{U}$ (rather than just floating around in space without being an element of anything).

Example 2.2.2
In Section 1.1, we introduced five sets: the empty set $\varnothing$, the set $\mathbb{N}$ of natural numbers, the set $\mathbb{Z}$ of integers, the set $\mathbb{Q}$ of rational numbers, the set $\mathbb{R}$ of real numbers and the set $\mathbb{C}$ of complex numbers.   ◁

Exercise 2.2.3
Which of the following propositions are true, and which are false?

$$\frac{1}{2} \in \mathbb{Z} \qquad \frac{1}{2} \in \mathbb{Q} \qquad \mathbb{Z} \in \mathbb{Q} \qquad \mathbb{Z} \in \mathcal{U} \qquad \frac{1}{2} \in \mathcal{U}$$

◁

Another fundamental example of a set is the *empty set*.

Definition 2.2.4
The **empty set**, denoted $\varnothing$ (LaTeX code: `\varnothing`), is the set with no elements.

---

[d]Read about *Russell's paradox* for more information.

The empty set may seem trivial—and it is—but owing to its canonicity, it arises all over the place, and will be especially important when we come to talk about functions and cardinality in Section 4.3.

Exercise 2.2.5

Let $p(x)$ be any formula. Show that the proposition $\forall x, (x \in \varnothing \Rightarrow p(x))$ is true. What does the proposition $\forall x, (x \in \varnothing \Rightarrow x \neq x)$ mean in English? Is it true? ◁

Specifying a set

One way of defining a set is simply to describe it in words, like we have done up to now. There are other, more concise ways, of specifying sets, which also remove such ambiguity from the process.

Lists. One way is simply to provide a **list** the elements of the set. To specify that the list denotes a set, we enclose the list with curly brackets $\{,\}$ (LaTeX code: \{,\}). For example, the following is a specification of a set X, whose elements are the natural numbers between 0 and 5 (inclusive):

$$X = \{0, 1, 2, 3, 4, 5\}$$

Implied lists. Sometimes a list might be too long to write out—maybe even infinite—or the length of the list might depend on a variable. In these cases it will be convenient to use an **implied list**, in which some elements of the list are written, and the rest are left implicit by writing an ellipsis '...' (LaTeX code: \dots). For example, the statement

$$X = \{1, 4, 9, \ldots, n^2\}$$

means that X is the set whose elements are all the square numbers from 1 to n^2, where n is some number. Implied lists can be ambiguous, since they rely on the reader's ability to infer the pattern being followed, so use with caution!

Set-builder notation. In general, implied lists can be ambiguous, so in practice they are avoided unless the implied list is very simple, such as a set of consecutive numbers like $\{3, 4, \ldots, 9\}$. In fact, many sets can't even be listed in this way.

To get around this, we can use *set-builder notation*, which is a means of specifying a set in terms of the properties its elements satisfy. Given a set X, the set of elements of X satisfying some property $p(x)$ is denoted

$$\{x \in X \mid p(x)\}$$

The bar '|' (LaTeX code: `\mid`) separates the variable name from the formula that they make true. Some authors use a colon '$\{x \in X : p(x)\}$' or semicolon '$\{x \in X; p(x)\}$' instead.[e]

Example 2.2.6

The set of all even integers can be written as

$$\{n \in \mathbb{Z} \mid n \text{ is even}\} = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$$

For comparison, the set of all even natural numbers can be written as

$$\{n \in \mathbb{N} \mid n \text{ is even}\} = \{0, 2, 4, 6, \ldots\}$$

$\triangleleft$

Proof tip

When a set X is expressed in set-builder notation, say $X = \{x \mid p(x)\}$, then the statement $x \in X$ is true precisely when $p(x)$ is true. In other words, to prove $x \in X$, you can prove $p(x)$. Likewise, to prove $x \notin X$, you can prove $\neg p(x)$. $\triangleleft$

Exercise 2.2.7

Express the set of all integers which are perfect squares in set-builder notation and as an implied list. $\triangleleft$

You're probably tired of worrying about ranges and universes—and so am I. We can use the language of set theory to avoid them completely by specifying the ranges of the variables we use as soon as they appear. For example, given a set X:

- The proposition $\forall x \in X,\ p(x)$ means that x has range X and $\forall x,\ p(x)$. It is equivalent to $\forall x,\ x \in X \Rightarrow p(x)$, so long as the range of x contains all the elements of X.

- The proposition $\exists x \in X,\ p(x)$ means that x has range X and $\exists x,\ p(x)$. It is equivalent to $\exists x,\ x \in X \wedge p(x)$, so long as the range of x contains all the elements of X.

- The set $\{x \in X \mid p(x)\}$ denotes the set $\{x \mid p(x)\}$, where the range of x is X.

From now on, this is the style that we will use, and the universe $\mathcal{U}$ will be assumed to include all the mathematical objects that we define or need.

We can also use set-builder notation to specify the form of the elements of a set. For example, the set

$$Z = \{3x + 2 \mid x \text{ is an integer}\}$$

---

[e]When $X = \mathcal{U}$, we abbreviate this by simply writing $\{x \mid p(x)\}$ instead of $\{x \in \mathcal{U} \mid p(x)\}$.

denotes the set of things of the form $3x + 2$ where x is an integer. Thus

$$Z = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$

From now on our universe of discourse will, unless otherwise specified, include all mathematical objects that we define. With this in mind, there are some very important sets to be defined.

Subsets and set equality

Much of the discussion above concerned when an element of one set is or is not an element of another. For example, every integer is a rational number; that is

$$\forall n, \, (n \in \mathbb{Z} \Rightarrow n \in \mathbb{Q})$$

We can say this more concisely by saying that $\mathbb{Z}$ is a *subset* of $\mathbb{Q}$.

Definition 2.2.8

Let X and Y be sets. We say X is a *subset* of Y if $\forall x \in X$, $x \in Y$, or equivalently, if

$$\forall x, \, (x \in X \Rightarrow x \in Y)$$

We abbreviate this proposition by writing $X \subseteq Y$ (LaTeX code: `\subseteq`), and we write $X \nsubseteq Y$ (LaTeX code: `\nsubseteq`) for its negation.

Note that we could also

Proof tip

A proof that X is a subset of Y typically proceeds as follows. Let $x \in X$ be arbitrary; then knowing nothing about x other than the fact that $x \in X$, prove that $x \in Y$. ◁

Exercise 2.2.9

Let X be a set. Prove that $\varnothing \subseteq X$ and that $X \subseteq X$. ◁

Example 2.2.10

We know from Section 1.1 that there is a chain of subsets given by:

$$\varnothing \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

◁

The following proposition proves a property of subsethood known as *transitivity*—we'll revisit this property in Sections 5.1 and 5.2.

Proposition 2.2.11
Let X, Y, Z be sets. If $X \subseteq Y$ and $Y \subseteq Z$, then $X \subseteq Z$.

Strategy. The result we want to prove is an implication. Thus we *assume* $X \subseteq Y$ and $Y \subseteq Z$, and our *goal* is to derive that $X \subseteq Z$. Spelling this out slightly more, the goal is to derive $\forall x,\, x \in X \Rightarrow x \in Z$; so we can introduce a variable x and assume that $x \in X$. Then our goal is to use our assumptions to prove that $x \in Z$. Well, $X \subseteq Y$ means $\forall x,\, x \in X \Rightarrow x \in Y$. Since we're assuming $x \in X$, substituting it into this assumption yields that $x \in Y$. Likewise, the assumption that $Y \subseteq Z$ yields that $x \in Z$.

Proof. Suppose that $X \subseteq Y$ and $Y \subseteq Z$. We need to prove that every element of X is an element of Z. So let $x \in X$. Since $X \subseteq Y$, it follows that $x \in Y$; and since $Y \subseteq Z$, it follows that $x \in Z$. Hence $X \subseteq Z$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

Aside
Notice how in the proof of Proposition 2.2.11 we omitted many of the details of the thought process that went into coming up with the proof: decomposing the logical structure of the proposition to be proved, spelling out what our goal is at every step, and so on. We left enough of an argument to convince a mathematically literate reader that we're correct, but kept it concise enough that attention is drawn to the important steps. $\qquad\qquad\triangleleft$

Definition 2.2.12
Let X be a set. The **power set** of X, denoted $\mathcal{P}(X)$ (L^ATEX code: `\mathcal{P}`), is the set of all subsets of X.

Example 2.2.13
There are four subsets of $\{1, 2\}$, namely

$$\varnothing, \quad \{1\}, \quad \{2\}, \quad \{1, 2\}$$

so $\mathcal{P}(X) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\triangleleft$

Exercise 2.2.14
Write out the elements of $\mathcal{P}(\{1, 2, 3\})$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\triangleleft$

Exercise 2.2.15
Let X be a set. Show that $\varnothing \in \mathcal{P}(X)$ and $X \in \mathcal{P}(X)$. $\qquad\qquad\qquad\triangleleft$

Exercise 2.2.16
Write out the elements of $\mathcal{P}(\varnothing)$, $\mathcal{P}(\mathcal{P}(\varnothing))$ and $\mathcal{P}(\mathcal{P}(\mathcal{P}(\varnothing)))$. $\qquad\qquad\triangleleft$

Power sets are often a point of confusion because they bring the property of being a *subset* of one set to that of being an *element* of another, in the sense that for all sets U and X we have

$$U \subseteq X \quad \Leftrightarrow \quad U \in \mathcal{P}(X)$$

This distinction looks easy to grasp, but when the sets U and X look alike, it's easy to fall into various traps. Here's a simple example.

Example 2.2.17
It is true that $\varnothing \subseteq \varnothing$, but false that $\varnothing \in \varnothing$. Indeed,

- $\varnothing \subseteq \varnothing$ means $\forall x \in \varnothing$, $x \in \varnothing$; but propositions of the form $\forall x \in \varnothing$, $p(x)$ are always true, as discussed in Exercise 2.2.5.

- The empty set has no elements; if $\varnothing \in \varnothing$ were true, it would mean that $\varnothing$ had an element (that element being $\varnothing$). So it must be the case that $\varnothing \notin \varnothing$.

$\triangleleft$

The following exercise is intended to help you overcome similar potential kinds of confusion by means of practice. Try to think precisely about what the definitions involved are.

Exercise 2.2.18
Write out the elements of $\mathcal{P}(\varnothing)$ and of $\mathcal{P}(\mathcal{P}(\varnothing))$. Determine, with proof, whether or not each of the following statements is true:

$$\mathcal{P}(\varnothing) \in \mathcal{P}(\mathcal{P}(\varnothing)), \quad \mathcal{P}(\varnothing) \subseteq \mathcal{P}(\mathcal{P}(\varnothing)), \quad \varnothing \in \{\{\varnothing\}\}, \quad \varnothing \subseteq \{\{\varnothing\}\}, \quad \{\varnothing\} \in \{\{\varnothing\}\}$$

$\triangleleft$

Set equality

Discussion 2.2.19
Let X and Y be sets. What should it mean to say that X and Y are equal? Try to provide a precise definition of equality of sets before reading on. $\triangleleft$

There are different possible notions of 'sameness' for sets: maybe $X = Y$ when X and Y have the same elements (this is called *extensional equality*), or maybe $X = Y$ when they're described by the same criteria (this is called *intensional equality*). In mathematics, it is more useful to know when two sets have the same elements, regardless of how they are described; so we take extensional equality as our notion of sameness for sets. This doesn't

mean intensional equality should be ignored—if you want to implement mathematics in a computer, the sets' *descriptions* have a much more important role to play.

Definition 2.2.20

Let X and Y be sets. We say X is *equal* to Y if $X \subseteq Y$ and $Y \subseteq X$, and we write $X = Y$. If $X \subseteq Y$ and $X \neq Y$ then we say X is a **proper subset** of Y and write $X \subsetneqq Y$ (LaTeX code: `\subsetneqq`).

Example 2.2.21

Let $E = \{n \in \mathbb{Z} \mid n \text{ is even}\}$. Then:

- $E \subsetneqq \mathbb{Z}$. Indeed, $E \subseteq \mathbb{Z}$ since every element of E is an element of $\mathbb{Z}$ by definition; but $E \neq \mathbb{Z}$ since, for instance, $1 \in \mathbb{Z}$ but $1 \notin E$.

- $\mathbb{N} \nsubseteq E$ since, for instance, $1 \in \mathbb{N}$ but $1 \notin E$.

- $E \nsubseteq \mathbb{N}$ since, for instance, $-2 \in E$ but $-2 \notin \mathbb{N}$.

$\triangleleft$

Exercise 2.2.22

Define a set X such that:

$$\mathbb{N} \subsetneqq X \quad \wedge \quad X \subsetneqq \mathbb{Q} \quad \wedge \quad X \nsubseteq \mathbb{Z} \quad \wedge \quad \mathbb{Z} \nsubseteq X$$

$\triangleleft$

Proof tip

To prove $X = Y$, you can prove that $X \subseteq Y$ and $Y \subseteq X$. This proof strategy is called *double-containment*. More specifically, such a proof is split into two parts:

(i) Let $x \in X$; from this assumption alone, prove that $x \in Y$.

(ii) Let $x \in Y$; from this assumption alone, prove that $x \in X$.

$\triangleleft$

Set operations

In Example 2.2.21 we defined E to be the set of all even integers. What if we wanted to talk about the set of all even natural numbers instead? It would be nice if there was some expression in terms of E and $\mathbb{N}$ to denote this set. This is where *set operations* come in.

Intersection (∩)

The *intersection* of two sets is the set of things which are elements of both sets.

Definition 2.2.23

Let X and Y be sets. The (**pairwise**) **intersection** of X and Y, denoted $X \cap Y$ (LATEX code: \cap), is defined by

$$X \cap Y = \{x \mid x \in X \wedge x \in Y\}$$

Example 2.2.24

Let E be the set of all even integers. Then $E \cap \mathbb{N}$ refers to the set of things which are both even integers and natural numbers... in other words, it is the set of even natural numbers. ◁

Exercise 2.2.25

Write down the elements of the set

$$\{0, 1, 4, 7\} \cap \{1, 2, 3, 4, 5\}$$

◁

Proof tip

To prove $x \in X \cap Y$ you can give two proofs: one that $x \in X$ and one that $x \in Y$. For example, if $X = \{x \mid p(x)\}$ and $Y = \{x \mid q(x)\}$, then $X \cap Y = \{x \mid p(x) \wedge q(x)\}$. ◁

Example 2.2.26

Let $X = \{x \in \mathbb{Z} \mid x \geqslant 5\}$ and $Y = \{x \in \mathbb{N} \mid x \leqslant 10\}$. Then

$$X \cap Y = \{x \in \mathbb{Z} \mid 5 \leqslant x \leqslant 10\} = \{5, 6, 7, 8, 9, 10\}$$

◁

Exercise 2.2.27

Let X and Y be sets. Prove that $X \subseteq Y$ if and only if $X \cap Y = X$. ◁

Union (∪)

The *union* of two sets is the set of things which are elements of at least one of the sets.

Definition 2.2.28

Let X and Y be sets. The (**pairwise**) **union** of X and Y, denoted $X \cup Y$ (LATEX code: \cup), is defined by
$$X \cup Y = \{x \mid x \in X \vee x \in Y\}$$

Example 2.2.29
Let E be the set of even integers and O be the set of odd integers. Since every integer is either even or odd, $E \cup O = \mathbb{Z}$. Note that $E \cap O = \varnothing$, thus $\{E, O\}$ is an example of a *partition* of $\mathbb{Z}$; see Definition 4.2.36. ◁

Exercise 2.2.30
Write down the elements of the set

$$\{0, 1, 4, 7\} \cup \{1, 2, 3, 4, 5\}$$

◁

The union operation allows us to define the following class of sets that will be particularly useful for us when studying counting principles in Section 4.2.

Definition 2.2.31
Define $[n]$ recursively for $n \in \mathbb{N}$ by

$$[0] = \varnothing \quad \text{and} \quad [n+1] = [n] \cup \{n+1\} \text{ for all } n \in \mathbb{N}$$

Exercise 2.2.32
Prove that if $n > 0$ then the elements of $[n]$ are the natural numbers from 1 up to n (inclusive). In implied list notation, this is to say that

$$[n] = \{1, 2, \ldots, n\}$$

whenever $n \geqslant 1$. ◁

Exercise 2.2.33
Let X and Y be sets. Prove that $X \subseteq Y$ if and only if $X \cup Y = Y$. ◁

Example 2.2.34
Let X, Y, Z be sets. We prove that $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.

- ($\subseteq$) Let $x \in X \cap (Y \cup Z)$. Then $x \in X$, and either $x \in Y$ or $x \in Z$. If $x \in Y$ then $x \in X \cap Y$, and if $x \in Z$ then $x \in X \cap Z$. In either case, we have $x \in (X \cap Y) \cup (X \cap Z)$.

- ($\supseteq$) Let $x \in (X \cap Y) \cup (X \cap Z)$. Then either $x \in X \cap Y$ or $x \in X \cap Z$. In both cases we have $x \in X$ by definition of intersection. In the first case we have $x \in Y$, and in the second case we have $x \in Z$; in either case, we have $x \in Y \cup Z$, so that $x \in X \cap (Y \cup Z)$.

◁

Exercise 2.2.35
Let X, Y, Z be sets. Prove that $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$. ◁

Relative complement (\\) and complement ($-^c$)

> **Definition 2.2.36**
> Let X and Y be sets. The **relative complement** of Y in X, denoted $X \setminus Y$ (LaTeX code: \setminus), is defined by
> $$X \setminus Y = \{x \in X \mid x \notin Y\}$$
> If X is a set then the **complement** of X, denoted X^c (LaTeX code: X^c), is simply the relative complement of X in the universal set: $X^c = \mathcal{U} \setminus X$.

Example 2.2.37
Let E be the set of all even integers. Then $n \in \mathbb{Z} \setminus E$ if and only if n is an integer and n is not an even integer; that is, if and only if n is odd. Thus $\mathbb{Z} \setminus E$ is the set of all odd integers.

Moreover, $n \in \mathbb{N} \setminus E$ if and only if n is a natural number and n is not an even integer. Since the even integers which are natural numbers are precisely the even natural numbers, $\mathbb{N} \setminus E$ is precisely the set of all odd natural numbers. ◁

Exercise 2.2.38
Write down the elements of the set

$$\{0, 1, 4, 7\} \setminus \{1, 2, 3, 4, 5\}$$

◁

Exercise 2.2.39
Let X and Y be sets. Prove that $X \subseteq Y$ if and only if $Y \setminus (Y \setminus X) = X$. ◁

Comparison with logical operators and quantifiers

The astute reader will have noticed some similarities between set operations and the logical operators and quantifiers that we saw in Section 2.1. Indeed, this can be summarised in the following table. In each row, the expressions in both columns are equivalent, where p denotes '$x \in X$', q denotes '$x \in Y$', and $r(i)$ denotes '$x \in X_i$':

sets	logic
$x \in X \cap Y$	$p \wedge q$
$x \in X \cup Y$	$p \vee q$
$x \in X^c$	$\neg p$
$x \in X \setminus Y$	$p \wedge (\neg q)$

This translation between logic and set theory does not stop there; in fact, as the following theorem shows, De Morgan's laws for the logical operators $\wedge$ and $\vee$ also carry over to the set operations $\cap$ and $\cup$.

Theorem 2.2.40 (De Morgan's laws for sets—pairwise version)
Let X, Y, Z be sets. Then
(a) $Z \setminus (X \cup Y) = (Z \setminus X) \cap (Z \setminus Y)$;

(b) $Z \setminus (X \cap Y) = (Z \setminus X) \cup (Z \setminus Y)$.

Proof of (a). Let $x \in Z \setminus (X \cup Y)$. Then $x \in Z$ and $x \notin X \cup Y$. The formula $x \notin X \cup Y$ says precisely

$$\neg(x \in X \vee x \in Y)$$

By de Morgan's laws for logical operators (Theorem 2.1.14), this is equivalent to

$$x \notin X \wedge x \notin Y$$

Since $x \in Z$ and $x \notin X$, we have $x \in Z \setminus X$. Since $x \in Z$ and $x \notin Y$, we have $x \in Z \setminus Y$. Hence, by definition of intersection, it follows that $x \in (Z \setminus X) \cap (Z \setminus Y)$.

Hence $Z \setminus (X \cup Y) \subseteq (Z \setminus X) \cap (Z \setminus Y)$.

The proof of $(Z \setminus X) \cap (Z \setminus Y) \subseteq Z \setminus (X \cup Y)$ is similar, and is left as an exercise, as is the proof of (b). $\qquad \square$

The following exercise derives perhaps a more familiar statement of de Morgan's laws for sets.

Exercise 2.2.41
Let X and Y be sets. Prove that

$$(X \cup Y)^c = X^c \cap Y^c \quad \text{and} \quad (X \cap Y)^c = X^c \cup Y^c$$

$\triangleleft$

Product ($\times$)

Definition 2.2.42
Let X and Y be sets. The (**Cartesian**) **product** of X and Y, denoted $X \times Y$ (LaTeX code: `\times`), is the set of all **ordered pairs** (x, y), where $x \in X$ and $y \in Y$. That is,

$$X \times Y = \{(x, y) \mid x \in X \wedge y \in Y\}$$

Example 2.2.43

If you have ever taken calculus, you will probably be familiar with the set $\mathbb{R} \times \mathbb{R}$.

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

Formally, this is the set of ordered pairs of real numbers. Geometrically, if we interpret $\mathbb{R}$ as an infinite line, the set $\mathbb{R} \times \mathbb{R}$ is the (real) plane: an element $(x,y) \in \mathbb{R} \times \mathbb{R}$ describes the point in the plane with coordinates (x,y).

We can investigate this further. For example, the following set:

$$\mathbb{R} \times \{0\} = \{(x,0) \mid x \in \mathbb{R}\}$$

is precisely the x-axis. We can describe graphs as subsets of $\mathbb{R} \times \mathbb{R}$. Indeed, the graph of $y = x^2$ is given by

$$G = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\} = \{(x, x^2) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$$

◁

Exercise 2.2.44

Write down the elements of the set $\{1,2\} \times \{1,3,4\}$. ◁

Exercise 2.2.45

Let X be a set. Prove that $X \times \varnothing = \varnothing$. ◁

Exercise 2.2.46

Let X, Y and Z be sets. Is it true that $X \times Y = Y \times X$? Is it true that $(X \times Y) \times Z = X \times (Y \times Z)$? ◁

Aside

Aaand breathe! All this new notation can be overwhelming at first, but it will be worth it in the end. This chapter was all about teaching you a new language—new symbols, new terminology—because without it, our future pursuits will be impossible. If you're stuck now, then don't worry: you'll soon get the hang of it, especially when we start using this new language in context. You can, of course, refer back to the results in this chapter for reference at any point in the future. ◁

2.3   Functions

One way of studying interactions between sets is by studying *functions* between them, which we will define informally in Definition 2.3.9. Functions are mathematical objects which assign, to each element of one set, exactly one element of another. Almost every branch of mathematics studies functions, be it directly or indirectly, and almost every application of mathematics arises from a translation of the abstract notion of a function to the real world. Just one example of this is the theory of computation—functions provide precisely the language necessary to describe the deterministic input-output behaviour of algorithms.

Existence and uniqueness

When discussing functions, it is useful to isolate the logical principles at work. To do so, it will help us to introduce a new quantifier '∃!'.

Definition 2.3.1

Let $p(x)$ be a logical formula. The proposition '$\exists! x,\, p(x)$' (read 'there exists a unique x such that $p(x)$') (LaTeX code: `\exists!`) is true if $p(x)$ is true for exactly one value of x. The symbol $\exists!$ is called the **unique existential quantifier**.

Example 2.3.2

There is only one set with no elements, namely the empty set. Symbolically, we could write

$$\exists! X \in \mathcal{U},\, (X \text{ is a set} \wedge \forall x \in \mathcal{U},\, x \notin X)$$

◁

Example 2.3.3

Every positive real number has a unique positive square root. We can write this symbolically as

$$\forall a \in \mathbb{R},\, (a > 0 \Rightarrow \exists! b \in \mathbb{R},\, (b > 0 \wedge b^2 = a))$$

Reading this from left to right, this says: for every real number a, if a is positive, then there exists a unique real number b, which is positive and whose square is a.   ◁

Exercise 2.3.4

The following propositions are all true. For each of the propositions, write it out using the $\exists!$ quantifier, and consider how you might prove it. Do you notice any patterns in your proof techniques?

(a) For each real number a, the equation $x^2 + 2ax + a^2 = 0$ has exactly one real solution x.

(b) There is a unique real number a for which the equation $x^2 + a^2 = 0$ has a real solution x.

(c) There is a unique natural number with exactly one positive divisor.

<div align="right">◁</div>

The following exercise shows that the $\exists!$ quantifier is really just shorthand for a more complicated expression.

Exercise 2.3.5

Let $p(x)$ be a logical formula. Prove that the following are equivalent:

(a) $\exists! x,\ p(x)$

(b) $[\exists x,\ p(x)] \wedge [\forall y,\ \forall z,\ (p(y) \wedge p(z) \Rightarrow y = z)]$

(c) $\exists x,\ (p(x) \wedge \forall y,\ (p(y) \Rightarrow y = x))$

<div align="right">◁</div>

The expressions (b) and (c) in Exercise 2.3.5 is particularly informative, as they breaks down a proof of existence and uniqueness into two chunks.

Proof tip

A proof of a statement of the form $\exists! x,\ p(x)$ can be split into two proofs:

- **Existence.** Prove $\exists x,\ p(x)$. That is, find a value of x making $p(x)$ true.

- **Uniqueness.** Either...

    ◇ ...prove $\forall y,\ \forall z,\ (p(y) \wedge p(z) \Rightarrow y = z)$. That is, fix y, z and assume that $p(y)$ and $p(z)$ are true. Derive that it must be the case that $y = z$.

  ...or...

    ◇ ...prove $\forall y,\ (p(y) \Rightarrow y = x)$. That is, fix y and assume that $p(y)$ is true. Derive that it must be the case that $y = x$, where x is as in your proof of existence.

<div align="center">113</div>

From these two parts, you can conclude that $\exists! x,\, p(x)$ is true.

Note that you only need to use *one* of the above techniques for proving uniqueness; the first corresponds to (b) in Exercise 2.3.5, and the second corresponds to (c). ◁

Example 2.3.6

An example of this proof structure in action is in a proof of the statement in part (a) of Exercise 2.3.4, that is, for each real number a there exists a unique x such that $x^2 + 2ax + a^2 = 0$.

Fix $a \in \mathbb{R}$. We prove existence and uniqueness of an element $x \in \mathbb{R}$ for which $x^2 + 2ax + a^2 = 0$ separately.

- (**Existence**) Let $x = -a$. Then

$$x^2 + 2ax + a^2 = (-a)^2 + 2a(-a) + a^2 = a^2 - 2a^2 + a^2 = 0$$

  so a solution exists.

- (**Uniqueness**) Fix $y \in \mathbb{R}$ and suppose that $y^2 + 2ay + a^2 = 0$. We will prove that is must be the case that $y = -a$. Well, factorising the expression yields $(y + a)^2 = 0$. If $y + a$ were nonzero then its square would also be nonzero, hence $y + a = 0$. Therefore, $y = -a$, as required.

Hence $x = -a$ is the unique solution to the equation $x^2 + 2ax + a^2 = 0$. ◁

This followed pattern (c) from Exercise 2.3.5. The following follows pattern (b).

Example 2.3.7

We prove Exercise 2.3.3, namely that for each real $a > 0$ there is a unique $b > 0$ such that $b^2 = a$. So first fix $a > 0$.

- (**Existence**) The real number $\sqrt{a}$ is positive and satisfies $(\sqrt{a})^2 = a$ by definition. Its existence will be deferred to a later time, but an informal argument for its existence could be provided using 'number line' arguments as in Section 1.1.

- (**Uniqueness**) Let $y, z > 0$ be real numbers such that $y^2 = a$ and $z^2 = a$. Then $y^2 = z^2$. Rearranging and factorising yields

$$(y - z)(y + z) = 0$$

  so either $y - z = 0$ or $y + z = 0$. If $y + z = 0$ then $z = -y$, and since $y > 0$, this means that $z < 0$. But this contradicts the assumption that $z > 0$. As such, it must be the case that $y - z = 0$, and hence $y = z$, as required.

$\triangleleft$

Exercise 2.3.8

Prove the statements in parts (b) and (c) of Exercise 2.3.4. $\triangleleft$

The unique existence quantifier clarifies the process of solving equations: when solving equations, there are typically two steps:

- **Step 1.** Start with the equation, and derive some set of potential solutions.

- **Step 2.** For each of the potential solutions, check whether each solves the equation—the set of those that *do* is precisely the set of all solutions to the equation.

In the case when an equation has a unique solution, and this solution is the only one which is derived algebraically from the equation, we recognise 'Step 1' as being a proof of *uniqueness* of a solution, and 'Step 2' as a proof of *existence* of a solution.

To wit, let's revisit the equation

$$x^2 + 2ax + a^2 = 0$$

from Example 2.3.6, where a and x refer to real numbers. We established that, for a given real number a, there is a unique real solution x. Instead of proving existence and uniqueness seprately, we could have instead solved this equation using a sequence of reversible steps:

$$
\begin{aligned}
x^2 + 2ax + a^2 = 0 &\Leftrightarrow (x + a)^2 = 0 &&\text{by factorising} \\
&\Leftrightarrow x + a = 0 &&\text{since 0 is the only square root of 0} \\
&\Leftrightarrow x = -a &&\text{rearranging}
\end{aligned}
$$

Working from top to bottom, this says *if* there is a solution x, *then* it is equal to $-a$. Working from bottom to top, this says that $-a$ is a solution. Thus the 'bottom to top' direction proves existence, and the 'top to bottom' direction proves uniqueness.

Functions

You might have come across the notion of a *function* before now. In schools, functions are often introduced as being like *machines*—they have inputs and outputs, and on a given input they always return the same output. For instance, there is a function which takes integers as inputs and gives integers as outputs, which on the input x returns the integer $x + 3$.

This, however, is clearly not a precise definition. A next approximation to a precise defin-
ition of a function might look something like this:

Definition 2.3.9

Let X and Y be sets. A **function** f from X to Y is a mathematical object which assigns
to each element of X exactly one element of Y. Given $x \in X$, the element of Y associated
with x by f is denoted $f(x)$, and is called the **value** of f at x. We write
$$f : X \to Y \quad (\text{\LaTeX code: } \texttt{f : X \textbackslash to Y})$$
to denote that f is a function from X to Y. We say X is the **domain** (or **source**) of f
and Y is the **codomain** (or **target**) of f.

This is better—for instance, we're now talking about sets (and not mysterious 'machines'),
which we have explored with in Section 2.2. Moreover, this definition establishes the
relationship between functions and the $\exists!$ quantifier: indeed, to say that f assigns to each
element of X a unique element of Y is to say precisely that

$$\forall x \in X, \exists! y \in Y, \, y = f(x)$$

Functions arise whenever there is a true proposition of the form $\forall x \in X, \exists! y \in Y, \, p(x, y)$—
this defines a function $f : X \to Y$ which assigns to each $x \in X$ the unique $y \in Y$ such that
$p(x, y)$ is true. In other words, $\forall x \in X, \, p(x, f(x))$ is true! We can use this to generate
some examples.

Example 2.3.10

Example 2.3.3 said that every positive real number has a unique positive square root; we
proved this in Example 2.3.7. What this means is that there is a function

$$r : \mathbb{R}^{>0} \to \mathbb{R}^{>0} \qquad \text{where } \mathbb{R}^{>0} = \{x \in \mathbb{R} \mid x > 0\}$$

defined by letting $r(x)$ be the (unique) positive square root of x, for each $x \in \mathbb{R}^{>0}$. That
is, we have a function r defined by $r(x) = \sqrt{x}$. $\triangleleft$

Exercise 2.3.11

Recall Exercise 2.3.4. Which of the statements (a), (b) or (c) is of the form $\forall x \in X, \exists! y \in$
$Y, \, p(x, y)$? For each statement of this form, determine the domain and codomain of the
corresponding function, and write an expression defining this function. $\triangleleft$

There are many ways to specify a function $f : X \to Y$. Before we move too far in this
direction, it is worth noting a very important point regarding what should be written in
the specification of a function.

Writing tip

When specifying a function, make sure that you specify its **domain** and its **codomain** and, if you use any variables, make sure they're all **quantified**! ◁

With this in mind, let's look at a few ways of specifying a function.

- **Lists.** If X is finite, then we can specify a function $f : X \to Y$ by simply listing the values of f at all possible elements $x \in X$. For example, we can define a function

  $$f : \{1, 2, 3\} \to \{\mathsf{red}, \mathsf{yellow}, \mathsf{green}, \mathsf{blue}, \mathsf{purple}\}$$

  by declaring

  $$f(1) = \mathsf{red}, \quad f(2) = \mathsf{purple}, \quad f(3) = \mathsf{green}$$

  Note that the function is at this point completely specified: we know its values at all elements of the domain $\{1, 2, 3\}$. It doesn't matter that some of the elements of the codomain (yellow and blue) are unaccounted for—all that matters is that each element of the domain is associated with exactly one element of the codomain.

  Unfortunately, most of the sets that we work with will be infinite, or of an unspecified finite size; in these cases, simply writing a list of values isn't sufficient. Fortunately for us, there are other ways of specifying functions.

- **Formulae.** In many cases, particularly when the domain X and codomain Y are number sets, we can define a function by giving a formula for the value of $f(x)$ for each $x \in X$. For example, we can define a function $f : \mathbb{R} \to \mathbb{R}$ by letting

  $$f(x) = x^2 + 3 \text{ for all } x \in \mathbb{R}$$

- **By cases.** It will at times be convenient to define a function using different specifications for different elements of the domain. A very simple example is the *absolute value function* $|-| : \mathbb{R} \to \mathbb{R}$, defined for $x \in \mathbb{R}$

  $$|x| = \begin{cases} x & \text{if } x \geqslant 0 \\ -x & \text{if } x \leqslant 0 \end{cases}$$

  Here we have split into two cases based on the conditions $x \geqslant 0$ and $x \leqslant 0$.

  When specifying a function $f : X \to Y$ by cases, it is important that the conditions be:

  - ◇ **exhaustive**: given $x \in X$, at least one of the conditions on X must hold; and
  - ◇ **compatible**: if any $x \in X$ satisfies more than one condition, the specified value must be the same no matter which condition is picked.

117

For the absolute value function defined above, these conditions are satisfied. Indeed, for $x \in \mathbb{R}$, it is certainly the case that $x \geqslant 0$ or $x \leqslant 0$, so the conditions are exhaustive. Moreover, given $x \in \mathbb{R}$, if both $x \geqslant 0$ and $x \leqslant 0$, then $x = 0$—so we need to check that the specification yields the same value when $x = 0$ regardless of which condition we pick. The $x \geqslant 0$ condition yields the value 0, and the $x \leqslant 0$ condition yields the value -0, which is equal to 0—so the conditions are compatible. We could have used $x < 0$ instead of $x \leqslant 0$; in this case the conditions are *mutually exclusive*, so certainly compatible because they do not overlap.

- **Algorithms.** You might, on first exposure to functions, have been taught to think of a function as a *machine* which, when given an *input*, produces an *output*. This 'machine' is defined by saying what the possible inputs and outputs are, and then providing a list of instructions (an *algorithm*) for the machine to follow, which on any input produces an output—and, moreover, if fed the same input, the machine always produces the same output.

  For example, we might instruct a machine to take rational numbers as inputs and give rational numbers as outputs, and to follow the following sequence of steps on a given input

  $$\text{multiply by } 2 \to \text{add } 5 \to \text{square the result} \to \text{divide by } 6$$

  This 'machine' defines a function $M : \mathbb{Q} \to \mathbb{Q}$ which, in equation form, is specified by

  $$M(x) = \frac{(2x + 5)^2}{6} \text{ for all } x \in \mathbb{Q}$$

  In our more formal set-up, therefore, we can define a function $M : I \to O$ by specifying:

  - ◇ a set I of all **inputs**;
  - ◇ a set O of potential **outputs**; and
  - ◇ a deterministic[f] algorithm which describes how an input $x \in I$ is transformed into an output $M(x) \in O$.

  That is, the domain is the set I of all possible 'inputs', the codomain is a set O containing all the possible 'outputs', and the function M is a rule specifying how an input is associated with the corresponding output.

  For now, we will use algorithmic specifications of functions only sparingly—this is because it is much harder to make formal what is meant by an 'algorithm', and it is important to check that a given algorithm is deterministic.

---

[f]The word 'deterministic' just means that the algorithm always produces the same output on a single input.

- **Graphs.** Given sets X and Y, each function $X \to Y$ is uniquely determined by its *graph* (see Definition 2.3.12), which is a particular subset of $X \times Y$, thought of as the set of all 'input-output' pairs of the function—this equivalence will be the content of Theorem 2.3.15. The elements of the graph G of a function f are pairs (x, y), with $x \in X$ and $y \in Y$, and the assertion that $(x, y) \in G$ will be equivalent to the assertion that $f(x) = y$.

Definition 2.3.12

Let $f : X \to Y$ be a function. The **graph** of f is the subset $\mathrm{Gr}(f) \subseteq X \times Y$ (LATEX code: `\mathrm{Gr}`) defined by

$$\mathrm{Gr}(f) = \{(x, f(x)) \mid x \in X\} = \{(x, y) \in X \times Y \mid y = f(x)\}$$

Example 2.3.13

Given a (sufficiently well-behaved) function $f : \mathbb{R} \to \mathbb{R}$, we can represent $\mathrm{Gr}(f) \subseteq \mathbb{R} \times \mathbb{R}$ by plotting it on a pair of axes using Cartesian coordinates in the usual way. For example, if f is defined by $f(x) = \frac{x}{2}$ for all $x \in \mathbb{R}$, then its graph

$$\mathrm{Gr}(f) = \left\{ \left(x, \frac{x}{2}\right) \mid x \in \mathbb{R} \right\}$$

can be represented by graph plot in Figure 2.1.
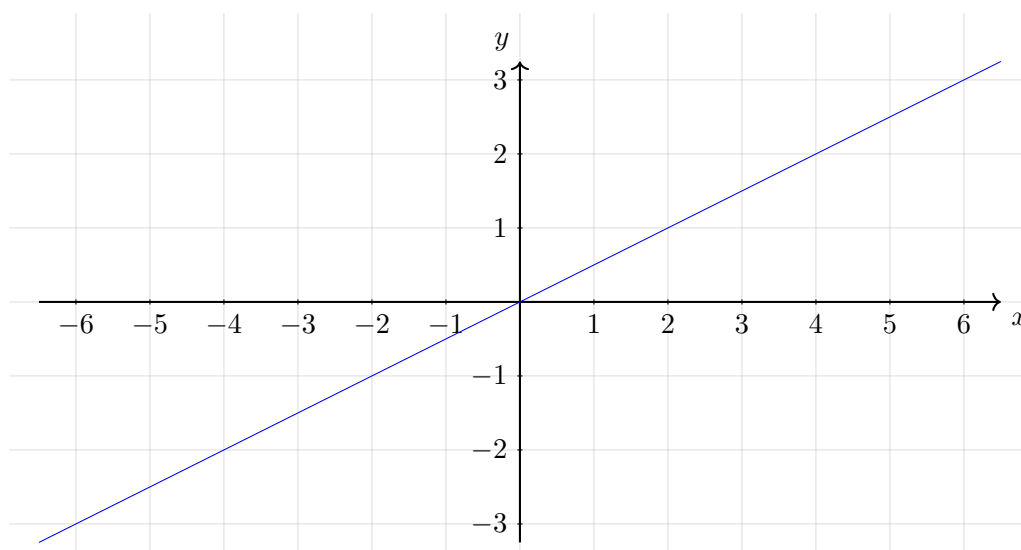
Figure 2.1: Graph (in blue) of the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \frac{x}{2}$ for all $x \in \mathbb{R}$

◁

Exercise 2.3.14

Find a function $f : \mathbb{Z} \to \mathbb{Z}$ whose graph is equal to the set

$$\{\dots, (-2, -5), (-1, -2), (0, 1), (1, 4), (2, 7), (3, 10), \dots\}$$

◁

Well-definedness

We must be careful when specifying functions that what we write really *does* define a function! This correctness of specification is known as *well-definedness*.

There are three things to check when it comes to well-definedness of a function $f : X \to Y$, namely *totality*, *existence* and *uniqueness*:

- **Totality.** A value $f(x)$ should be specified for each $x \in X$.

- **Existence.** For each $x \in X$, the specified value $f(x)$ should actually exist, and should be an element of Y.

- **Uniqueness.** For each $x \in X$, the specified value $f(x)$ should refer to only one element of Y. That is, if $x = x' \in X$ then we should have $f(x) = f(x')$. This issue usually arises when elements of X can be described in different ways.

When specifying a function, you should justify each of these components of well-definedness unless they are extremely obvious. You will probably find that, in most cases, the only component in need of justification is uniqueness, but keep all three in mind.

Theorem 2.3.15 below provides a way of verifying that a function is well-defined by characterising their graphs.

Theorem 2.3.15

Let X and Y be sets. A subset $G \subseteq X \times Y$ is the graph of a function if and only if

$$\forall x \in X, \exists! y \in Y, (x, y) \in G$$

Proof. ($\Rightarrow$). Suppose $G \subseteq X \times Y$ is the graph of a function, say $G = \mathrm{Gr}(f)$ for some $f : X \to Y$. Then for each $x \in X$, it follows from well-definedness of f that $f(x)$ is the unique element $y \in Y$ for which $(x, y) \in G$. That is, $(x, f(x)) \in G$, and if $y \in Y$ with $(x, y) \in G$, then $y = f(x)$.

($\Leftarrow$). Suppose $G \subseteq X \times Y$ is satisfies $\forall x \in X$, $\exists! y \in Y$, $(x, y) \in G$. Define a function $f : X \to Y$ by, for each $x \in X$, defining the value $f(x)$ to be the unique element $y \in Y$ for which $(x, y) \in G$. Well-definedness of f is then immediate from our assumption of the existence and uniqueness of such a value of y for each $x \in X$. $\qquad\square$

Example 2.3.16
The set G defined by

$$G = \{(1, \mathsf{red}), (2, \mathsf{red}), (3, \mathsf{green})\}$$

is the graph of a function $f : \{1, 2, 3\} \to \{\mathsf{red}, \mathsf{green}, \mathsf{blue}\}$. The function f is defined by

$$f(1) = \mathsf{red}, \quad f(2) = \mathsf{red}, \quad f(3) = \mathsf{green}$$

However, G is *not* the graph of a function $\{1, 2, 3, 4\} \to \{\mathsf{red}, \mathsf{green}, \mathsf{blue}\}$, since G contains no elements of the form $(4, y)$ for $y \in \{\mathsf{red}, \mathsf{green}, \mathsf{blue}\}$. Moreover, the set G' defined by

$$G' = \{(1, \mathsf{red}), (2, \mathsf{red}), (2, \mathsf{blue}), (3, \mathsf{green})\}$$

does not define the graph of a function $\{1, 2, 3\} \to \{\mathsf{red}, \mathsf{green}, \mathsf{blue}\}$, since there is not a *unique* element of the form $(2, y)$ in G'—rather, there are two of them! $\qquad\triangleleft$

Exercise 2.3.17
For each of the following specifications of sets X, Y, G, determine whether or not G is the graph of a function from X to Y.

(a) $X = \mathbb{R}$, $Y = \mathbb{R}$, $G = \{(a, a^2) \mid a \in \mathbb{R}\}$;

(b) $X = \mathbb{R}$, $Y = \mathbb{R}$, $G = \{(a^2, a) \mid a \in \mathbb{R}\}$;

(c) $X = \mathbb{R}^{\geqslant 0}$, $Y = \mathbb{R}^{\geqslant 0}$, $G = \{(a^2, a) \mid a \in \mathbb{R}\}$, where $\mathbb{R}^{\geqslant 0} = \{x \in \mathbb{R} \mid x \geqslant 0\}$;

(d) $X = \mathbb{Q}$, $Y = \mathbb{Q}$, $G = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid xy = 1\}$.

(e) $X = \mathbb{Q}$, $Y = \mathbb{Q}$, $G = \{(a, a) \mid a \in \mathbb{Z}\}$;

$\triangleleft$

Aside
In light of Theorem 2.3.15, some people choose to define functions $X \to Y$ as particular subsets of $X \times Y$—that is, they identify functions with their graphs. This is particularly useful when studying the logical foundations of mathematics. We avoid this practice here, because it is not conceptually necessary, and it would preclude other possible ways of encoding functions. $\qquad\triangleleft$

We will now look at some more examples (and non-examples) of functions.

Example 2.3.18

Example 2.3.3 gives a prime example of a function: it says that for every positive real number a there is a unique positive real number b such that $b^2 = a$. This unique b is precisely the positive square root $\sqrt{a}$ of a. Writing $\mathbb{R}^{>0}$ for the set of positive real numbers, we have thus established that taking the positive square root defines a function $\mathbb{R}^{>0} \to \mathbb{R}^{>0}$.   ◁

There is a class of functions called *identity functions* that, despite being very simple, are so important that we will give them a numbered definition!

Definition 2.3.19

Let X be a set. The **identity function** on X is the function $\mathrm{id}_X : X \to X$ (LaTeX code: `\mathrm{id}_X`) defined by $\mathrm{id}_X(x) = x$ for all $x \in X$.

You should convince yourself that the specification of id_X given in Definition 2.3.19 is well-defined.

Another interesting example of a function is the *empty function*, which is useful in coming up with counterexamples and proving combinatorial identities (see Section 4.2).

Definition 2.3.20

Let X be a set. The **empty function** with codomain X is the (unique!) function $\varnothing \to X$. It has no values, since there are no elements of its domain.

Again, you should convince yourself that this specification is well-defined. Conceptually, convincing yourself of this is not easy; but writing down the proof of well-definedness is extremely easy—you will find that there is simply nothing to prove!

Example 2.3.21

Define $f : \mathbb{R} \to \mathbb{R}$ by the equation $f(x)^2 = x$ for all $x \in \mathbb{R}$. This is not well-defined for a few reasons. First, if $x < 0$ then there is no real number y such that $y^2 = x$, so for $x < 0$ there are no possible values of $f(x)$ in the codomain of f, so *existence* fails. Second, if $x > 0$ then there are in fact *two* real numbers y such that $y^2 = x$, namely the positive square root $\sqrt{x}$ and the negative square root $-\sqrt{x}$. The specification of f does not indicate which of these values to take, so *uniqueness* fails.

Notice that the function $r : \mathbb{R}^{>0} \to \mathbb{R}^{>0}$ from Example 2.3.10 *is* (well-)defined by the equation $r(x)^2 = x$ for all $x \in \mathbb{R}^{>0}$. This illustrates why it is very important to specify the domain and codomain when defining a function.   ◁

Exercise 2.3.22
Which of the following specifications of functions are well-defined?

(a) $g : \mathbb{Q} \to \mathbb{Q}$ defined by the equation $(x + 1)g(x) = 1$ for all $x \in \mathbb{Q}$;

(b) $h : \mathbb{N} \to \mathbb{Q}$ defined by $(x + 1)h(x) = 1$ for all $x \in \mathbb{N}$;

(c) $k : \mathbb{N} \to \mathbb{N}$ defined by $(x + 1)k(x) = 1$ for all $x \in \mathbb{N}$;

(d) $\ell : \mathbb{N} \to \mathbb{N}$ defined by $\ell(x) = \ell(x)$ for all $x \in \mathbb{N}$.

Under what conditions on sets X and Y is a function $i : X \cup Y \to \{0, 1\}$ defined by

$$i(z) = \begin{cases} 0 & \text{if } z \in X \\ 1 & \text{if } z \in Y \end{cases}$$

well-defined? ◁

Composition of functions

In our section on sets, we talked about various operations that can be performed on sets—union, intersection, and so on. There are also operations on functions, by far the most important of which is *composition*. To understand how composition works, let's revisit the algorithmically defined function $M : \mathbb{Q} \to \mathbb{Q}$ from page 118:

multiply by $2 \to$ add $5 \to$ square the result $\to$ divide by 6

The function M is, in some sense, a *sequence* of functions, performed one-by-one until the desired result is reached. This is precisely *composition of functions*.

Definition 2.3.23
Given functions $f : X \to Y$ and $g : Y \to Z$, their **composite** $g \circ f$ (LaTeX code: `g \circ f`) (read 'g composed with f' or 'g after f' or even just 'g f') is the function $g \circ f : X \to Z$ defined by
$$(g \circ f)(x) = g(f(x)) \text{ for all } x \in X$$

Intuitively, $g \circ f$ is the function resulting from first applying f, and then applying g, to the given input.

Common error

Function composition is in some sense written 'backwards': in the expression $g \circ f$, the function which is applied *first* is written *last*—there is a good reason for this: the argument to the function is written after the function! However, this mis-match often trips students up on their first exposure to function composition, so be careful!   ◁

Example 2.3.24

The function M from page 118 can be defined as the composite

$$M = ((k \circ h) \circ g) \circ f$$

where

- $f : \mathbb{Q} \to \mathbb{Q}$ is defined by $f(x) = 2x$ for all $x \in \mathbb{Q}$;

- $g : \mathbb{Q} \to \mathbb{Q}$ is defined by $g(x) = x + 5$ for all $x \in \mathbb{Q}$;

- $h : \mathbb{Q} \to \mathbb{Q}$ is defined by $h(x) = x^2$ for all $x \in \mathbb{Q}$;

- $k : \mathbb{Q} \to \mathbb{Q}$ is defined by $k(x) = \frac{x}{6}$ for all $x \in \mathbb{Q}$.

◁

Exercise 2.3.25

Let $f, g, h, k : \mathbb{Q} \to \mathbb{Q}$ be as in Exercise 2.3.24. Compute equations defining the following composites:

(a) $f \circ g$;

(b) $g \circ f$;

(c) $((f \circ g) \circ h) \circ k$;

(d) $f \circ (g \circ (h \circ k))$;

(e) $(g \circ g) \circ (g \circ g)$.

◁

Example 2.3.26

Let $f : X \to Y$ be any function. Then

$$\mathrm{id}_Y \circ f = f = f \circ \mathrm{id}_X$$

To see this, let $x \in X$. Then

$$
\begin{aligned}
(\mathrm{id}_Y \circ f)(x) &= \mathrm{id}_Y(f(x)) && \text{by definition of composition} \\
&= f(x) && \text{by definition of } \mathrm{id}_Y \\
&= f(\mathrm{id}_X(x)) && \text{by definition of } \mathrm{id}_X \\
&= (f \circ \mathrm{id}_X)(x) && \text{by definition of composition}
\end{aligned}
$$

Equality of the three functions in question follows. ◁

Exercise 2.3.27
Prove that composition of functions is *associative*, that is, if $f : X \to Y$, $g : Y \to Z$ and $h : Z \to W$ are functions, then

$$
h \circ (g \circ f) = (h \circ g) \circ f : X \to W
$$

As a consequence of associativity, when we want to compose more than two functions, it doesn't matter what order we compose the functions in. As such, we can just write $h \circ g \circ f$. ◁

Exercise 2.3.28
Let $f : X \to Y$ and $g : Z \to W$ be functions, and suppose that $Y \subsetneq Z$. Note that there is a function $h : X \to W$ defined by $h(x) = g(f(x))$ for all $x \in X$. Write h as a composite of functions involving f and g. ◁

Images and preimages

> **Definition 2.3.29**
> Let $f : X \to Y$ be a function and let $U \subseteq X$. The **image of U under f** is the subset $f[U] \subseteq Y$ (also written $f_*(U)$ (LaTeX code: `f_*`) or even just $f(U)$) is defined by
>
> $$
> f[U] = \{f(x) \mid x \in U\} = \{y \in Y \mid \exists x \in U, \, y = f(x)\}
> $$
>
> That is, $f[U]$ is the set of values that the function f takes when given inputs from U. The **image of f** is the image of the entire domain, i.e. the set $f[X]$.

Example 2.3.30
Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. The image of f is the set $\mathbb{R}^{\geqslant 0}$ of all nonnegative real numbers. Let's prove this:

- $(f[\mathbb{R}] \subseteq \mathbb{R}^{\geqslant 0})$. Let $y \in f[\mathbb{R}]$. Then $y = x^2$ for some $x \in \mathbb{R}$. But $x^2 \geqslant 0$, so we must have $y \in \mathbb{R}^{\geqslant 0}$, as required.

- ($\mathbb{R}^{\geqslant 0} \subseteq f[\mathbb{R}]$). Let $y \in \mathbb{R}^{\geqslant 0}$. Then $\sqrt{y} \in \mathbb{R}$, and $y = (\sqrt{y})^2 = f(\sqrt{y})$. Hence $y \in f[\mathbb{R}]$, as required.

We have shown by double containment that $f[\mathbb{R}] = \mathbb{R}^{\geqslant 0}$. ◁

Exercise 2.3.31

For each of the following functions f and subsets U of their domain, describe the image $f[U]$.

(a) $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = 3n$, with $U = \mathbb{N}$;

(b) $f : X \to X \times X$ (where X is any set) defined by $f(x) = (x, x)$ with $U = X$;

(c) $f : \{a, b, c\} \to \{1, 2, 3\}$ defined by $f(a) = 1$, $f(b) = 3$ and $f(c) = 1$, with $U = \{a, b, c\}$.

◁

Exercise 2.3.32

Prove that $f[\varnothing] = \varnothing$ for all functions f. ◁

Example 2.3.33

Let $f : X \to Y$ be a function and let $U, V \subseteq X$. Then $f[U \cap V] \subseteq f[U] \cap f[V]$. To see this, let $y \in f[U \cap V]$. Then $y = f(x)$ for some $x \in U \cap V$. By definition of intersection, $x \in U$ and $x \in V$. Since $x \in U$ and $y = f(x)$, we have $y \in f[U]$; likewise, since $x \in V$, we have $y \in f[V]$. But then by definition of intersection, we have $y \in f[U] \cap f[V]$. ◁

Exercise 2.3.34

Let $f : X \to Y$ be a function and let $U, V \subseteq X$. We saw in Example 2.3.33 that $f[U \cap V] \subseteq f[U] \cap f[V]$. Determine which of the following is true, and for each, provide a proof of its truth or falsity:

(a) $f[U] \cap f[V] \subseteq f[U \cap V]$;

(b) $f[U \cup V] \subseteq f[U] \cup f[V]$;

(c) $f[U] \cup f[V] \subseteq f[U \cup V]$.

◁

> **Definition 2.3.35**
>
> Let $f : X \to Y$ be a function and let $V \subseteq Y$. The **preimage of V under f** is the subset $f^{-1}[V]$ (LATEX code: `f^{-1}`) (also written $f^*(V)$ (LATEX code: `f^*`)) is defined by
>
> $$f^{-1}[V] = \{x \in X \mid f(x) \in V\} = \{x \in X \mid \exists y \in V,\, f(x) = y\}$$
>
> That is, $f^{-1}[V]$ is the set of all the elements of its domain X that the function f sends to elements of V.

Example 2.3.36

Let $f : \mathbb{Z} \to \mathbb{Z}$ be the function defined by $f(x) = x^2$ for all $x \in X$. Then

- $f^{-1}[\{1, 4, 9\}] = \{-3, -2, -1, 1, 2, 3\}$;

- $f^{-1}[\{1, 2, 3, 4, 5, 6, 7, 8, 9\}] = \{-3, -2, -1, 1, 2, 3\}$ too, since the other elements of [9] are not perfect squares, and hence not of the form $f(x)$ for $x \in \mathbb{Z}$;

- $f^{-1}[\mathbb{N}] = \mathbb{Z}$, since for any $x \in \mathbb{Z}$ we have $f(x) \geqslant 0$, so that $f(x) \in \mathbb{N}$.

◁

Example 2.3.37

Let $f : X \to Y$ be a function, let $U \subseteq X$ and let $V \subseteq Y$. Then $f[U] \subseteq V$ if and only if $U \subseteq f^{-1}[V]$. The proof is as follows.

($\Rightarrow$). Suppose $f[U] \subseteq V$; we'll prove $U \subseteq f^{-1}[V]$. So fix $x \in U$. Then $f(x) \in f[U]$ by definition of image. But then $f(x) \in V$ by our assumption that $f[U] \subseteq V$, and so $x \in f^{-1}[V]$ by definition of preimage. Since x was arbitrarily chosen from U, it follows that $U \subseteq f^{-1}[V]$.

($\Leftarrow$). Suppose $U \subseteq f^{-1}[V]$; we'll prove $f[U] \subseteq V$. So fix $y \in f[U]$. Then $y = f(x)$ for some $x \in U$ by definition of image. But then $x \in f^{-1}[V]$ by our assumption that $U \subseteq f^{-1}[V]$, and so $f(x) \in V$ by definition of preimage. But $y = f(x)$, so $y \in V$, and since y was arbitrarily chosen, it follows that $f[U] \subseteq V$. ◁

The following exercise demonstrates that preimages interact very nicely with the basic set operations (intersection, union and relative complement):

Exercise 2.3.38

Let $f : X \to Y$ be a function and let $U, V \subseteq Y$. Prove that

$$f^{-1}[U \cap V] = f^{-1}[U] \cap f^{-1}[V] \quad \text{and} \quad f^{-1}[U \cup V] = f^{-1}[U] \cup f^{-1}[V] \quad \text{and} \quad f^{-1}[Y \backslash U] = X \backslash f^{-1}[U]$$

◁

Exercise 2.3.39

Let $f : X \to Y$ be a function. Prove that $f^{-1}[\varnothing] = \varnothing$ and $f^{-1}[Y] = X$.   ◁

Exercise 2.3.40

Let $f : X \to Y$ be a function. Provide a proof of the truth or falsity of each of the following statements:

- $U \subseteq f^{-1}[f[U]]$ for all $U \subseteq X$;

- $f^{-1}[f[U]] \subseteq U$ for all $U \subseteq X$;

- $V \subseteq f[f^{-1}[V]]$ for all $V \subseteq Y$;

- $f[f^{-1}[V]] \subseteq V$ for all $V \subseteq Y$.

◁

Chapter 3

Number theory

3.1   Division

This section introduces the notion of *divisibility*. As we have already mentioned, it is not always the case that one integer can divide another. As you read through this section, note that we never use fractions; everything we do is *internal* to $\mathbb{Z}$, and does not require that we 'spill over' to $\mathbb{Q}$ at any point. This will help you when you study ring theory in the future, and is a good practice to mimic in your own work.

The following theorem, called the division theorem, is the crux of everything that is to follow.

Theorem 3.1.1 (Division theorem)
Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leqslant r < |b|$$

Strategy.   Let's look at the simple case when $a \geqslant 0$ and $b > 0$. We can always find q, r such that $a = qb + r$, for example $q = 0$ and $r = a$. Moreover, by increasing q we can reduce r, since

$$qb + r = (q + 1)b + (r - b)$$

We will keep doing this until the 'remainder' is as small as it can be without being negative. As an example, consider the case when $a = 14$ and $b = 5$. This procedure gives

$$
\begin{aligned}
14 &= 0 \times 5 + 14 \\
&= 1 \times 5 + 9 \\
&= 2 \times 5 + 4 \qquad\qquad\qquad \leftarrow \text{least nonnegative remainder} \\
&= 3 \times 5 + (-1) \\
&= \cdots
\end{aligned}
$$

This procedure shows that in this case we should take $q = 2$ and $r = 4$, since $14 = 2 \times 5 + 4$ and $0 \leqslant 4 < |5|$.

We can show that such a descending sequence of remainders terminates using the well-ordering principle, and then we must argue that the quotient and remainder that we obtain are unique.

⊛ *Proof.* We may assume that $b > 0$: if not, replace b by $-b$ and q by $-q$. We may also assume that $a \geqslant 0$. Otherwise, replace a by $-a$, q by $-(q + 1)$ and r by $b - r$.

Thus, what follows assumes that $a \geqslant 0$ and $b > 0$.

- **Existence.** We prove that such integers q, r exist by the well-ordering principle. Namely, we define a sequence $(r_n)_{n \in \mathbb{N}}$ such that $a = nb + r_n$ and $r_0 > r_1 > r_2 > \cdots$, and use this sequence to find the values of q, r.

  ◇ Let $r_0 = a$. Then $a = 0b + r_0$, as required.

  ◇ Suppose r_n has been defined, and let $r_{n+1} = r_n - b$. Then

  $$
  \begin{aligned}
  (n+1)b + r_{n+1} &= (n+1)b + r_n - b \\
  &= nb + b + r_n - b \\
  &= nb + r = a
  \end{aligned}
  $$

  Since $b > 0$, we must have $r_{n+1} < r_n$ for all n.

  Let $R = \mathbb{N} \cap \{r_n \mid n \in \mathbb{N}\}$. That is, R is the set of terms of the sequence which are non-negative. Since $r_0 = a \geqslant 0$, we have that $r_0 \in R$ and hence R is inhabited. By the well-ordering principle, R has a least element r_k for some $k \in \mathbb{N}$.

  Define $q = k$ and $r = r_k$. By construction we have $a = qb + r$ and $r \geqslant 0$, so it remains to show that $r < b$. Well, if $r \geqslant b$ then $r - b \geqslant 0$, but $r - b = r_{k+1}$, so this would imply $r_{k+1} \in R$, contradicting minimality of r. Hence $r < b$, so q, r are as required.

- **Uniqueness.** Suppose q', r' also satisfy $a = q'b + r'$ and $0 \leqslant r' < b$. If we can show that $r' = r$ then this proves that $q = q'$: indeed, if $qb + r = q'b + r$ then we can subtract r and then divide by b, since $b > 0$.

  First note that $q' \geqslant 0$. If $q' < 0$ then $q' \leqslant -1$, so

  $$
  a = q'b + r' \leqslant -b + r'
  $$

  and hence $r' \geqslant a + b \geqslant b$ since $a \geqslant 0$. This contradicts the assumption that $r < b$. So $q' \geqslant 0$.

  Since $q' \geqslant 0$, we also know that $a = q'b + r_{q'}$, and hence $r' = r_{q'} \in R$. By minimality of r we have $r \leqslant r'$. It remains to show that $r = r'$. If not then $r < r'$. Thus

  $$
  qb + r = q'b + r' > q'b + r \quad \Rightarrow \quad qb > q'b \quad \Rightarrow \quad q > q'
  $$

  and hence $q = q' + t$ for some $t \geqslant 1$. But then

  $$
  q'b + r' = a = qb + r = (q' + t)b + r = q'b + (tb + r)
  $$

  so $r' = tb + r \geqslant b$, contradicting $r' < b$. So $r = r'$ as desired, and hence $q = q'$.

At long last, we are done. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ □

Definition 3.1.2

Let $a, b \in \mathbb{Z}$ with $b \neq 0$, and let q, r be the unique integers such that

$$a = qb + r \quad \text{and} \quad 0 \leqslant r < |b|$$

We say q is the **quotient** and r is the **remainder** of a divided by b.

Example 3.1.3

Some examples of division include:

$$14 = 2 \times 5 + 4, \qquad -14 = -3 \times 5 + 1, \qquad 15 = 3 \times 5 + 0$$

$\triangleleft$

Definition 3.1.4

Let $a, b \in \mathbb{Z}$. We say b **divides** a, or that b is a **divisor** (or **factor**) of a, if there exists $q \in \mathbb{Z}$ such that $a = qb$. To denote the fact that b divides a we write $b \mid a$ (LaTeX code: `\mid`). For the negation $\neg(b \mid a)$ write $b \nmid a$ (LaTeX code: `\nmid`).

Thus, when $b \neq 0$, saying $b \mid a$ is equivalent to saying that the remainder of a divided by b is 0.

Example 3.1.5

5 divides 15 since $15 = 3 \times 5$. However, 5 does not divide 14: we know that the remainder of 14 divided by 5 is 4, not 0—and it can't be both since we proved in the division theorem that remainders are unique! $\triangleleft$

Exercise 3.1.6

Show that if $a \in \mathbb{Z}$ then $1 \mid a$, $-1 \mid a$ and $a \mid 0$. For which integers a does $a \mid 1$? For which integers a does $0 \mid a$? $\triangleleft$

We now introduce the very basic notion of a *unit*. This notion is introduced to rule out trivialities. Units become interesting when talking about general rings, but in $\mathbb{Z}$, the units are very familiar.

Definition 3.1.7

Let $u \in \mathbb{Z}$. We say u is a **unit** if $u \mid 1$; that is, u is a unit if there exists $v \in \mathbb{Z}$ such that $uv = 1$.

Proposition 3.1.8

The only units in $\mathbb{Z}$ are 1 and -1.

Proof. First note that 1 and -1 are units, since $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = 1$. Now suppose that $u \in \mathbb{Z}$ is a unit, and let $v \in \mathbb{Z}$ be such that $uv = 1$. Certainly $u \neq 0$, since $0v = 0 \neq 1$. If $u > 1$ or $u < -1$ then $v = \frac{1}{u} \notin \mathbb{Z}$. So we must have $u \in \{-1, 1\}$. $\qquad \square$

Exercise 3.1.6 shows that -1, 0 and 1 are, from the point of view of divisibility, fairly trivial. For this reason, most of the results we discuss regarding divisibility will concern **non-zero non-units**, i.e. all integers except -1, 0 or 1.

Greatest common divisors

> **Definition 3.1.9**
> Let $a, b \in \mathbb{Z}$. An integer d is a **greatest common divisor** of a and b if:
>
> (a) $d \mid a$ and $d \mid b$;
>
> (b) If q is another integer such that $q \mid a$ and $q \mid b$, then $q \mid d$.

Example 3.1.10
2 is a greatest common divisor of 4 and 6; indeed:

(a) $4 = 2 \times 2$, and $6 = 3 \times 2$, so $2 \mid 4$ and $2 \mid 6$;

(b) Suppose $q \mid 4$ and $q \mid 6$. The divisors of 4 are $\pm 1, \pm 2, \pm 4$ and the divisors of 6 are ± 1, ± 2, ± 3, ± 6. Since q divides both, it must be the case that $q \in \{-2, -1, 1, 2\}$; in any case, $q \mid 2$.

Likewise, -2 is a greatest common divisor of 4 and 6. ◁

Exercise 3.1.11
There are two greatest common divisors of 6 and 15; find both. ◁

We will now prove that greatest common divisors *exist*—that is, any two integers have a greatest common divisor—and that they are *unique up to sign*.

> **Theorem 3.1.12**
> Every pair of integers a, b has a greatest common divisor.

Proof. First note that if $a = b = 0$, then 0 is a greatest common divisor for a and b. Moreover, we may take a, b to be non-negative, since divisibility is insensitive to sign. So suppose that $a, b \geqslant 0$ and that a, b are not both zero.

133

Define a set $X \subseteq \mathbb{Z}$ by

$$X = \{au + bv \mid u, v \in \mathbb{Z}, \ au + bv > 0\}$$

That is, X is the set of positive integers of the form $au + bv$.

X is inhabited. To see this, note that $a^2 > 0$ or $b^2 > 0$ since $a \neq 0$ or $b \neq 0$, so letting $u = a$ and $v = b$ in the expression $au + bv$, we see that

$$au + bv = a^2 + b^2 > 0 \quad \Rightarrow \quad a^2 + b^2 \in X$$

By the well-ordering principle, X has a least element d, and by definition of X there exist $u, v \in \mathbb{Z}$ such that $d = au + bv$.

We will prove that d is a greatest common divisor for a and b.

- $d \mid a$. If $a = 0$, then this is immediate, so suppose that $a > 0$. Let $q, r \in \mathbb{Z}$ be such that

  $$a = qd + r \qquad \text{and} \qquad 0 \leqslant r < d$$

  Now $a = a \cdot 1 + b \cdot 0$, so $a \in X$, and hence $d \leqslant a$.

  $$r = a - qd = a - q(au + bv) = a(1 - qu) + b(-qv)$$

  If $r > 0$ then this implies that $r \in X$; but this would contradict minimality of d, since $r < d$. So we must have $r = 0$ after all.

- $d \mid b$. The proof of this is identical to the proof that $d \mid a$.

- Suppose q is an integer dividing both a and b. Then $q \mid au + bv$ by Exercise 1.1.16. Since $au + bv = d$, we have $q \mid d$.

So d is a greatest common divisor of a and b after all. $\qquad\qquad\qquad\qquad\qquad\square$

Exercise 3.1.13
Let $a, b \in \mathbb{Z}$. If d and d' are two greatest common divisors of a and b, then either $d = d'$ or $d = -d'$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\triangleleft$

Aside
A consequence of Theorem 3.1.12 and Exercise 3.1.13 is that every pair of integers has a unique non-negative greatest common divisor! Written symbolically, we can say

$$\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}, \ \exists! d \in \mathbb{Z}, \ \begin{pmatrix} d \geqslant 0 \text{ and } d \text{ is a greatest} \\ \text{common divisor for } a \text{ and } b \end{pmatrix}$$

As discussed in Section 2.3, since this is a formula of the form 'for all ... there exists a unique ...', this defines a function gcd : $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. We won't explicitly refer to the fact that gcd is a function; rather, we'll just concern ourselves with its values, as in Notation 3.1.14. ◁

Exercise 3.1.13 justifies our use of the following notation to refer to greatest common divisors.

Notation 3.1.14
Let $a, b \in \mathbb{Z}$. Denote by $\gcd(a, b)$ (LaTeX code: `\mathrm{gcd}`) the (unique!) non-negative greatest common divisor of a and b.

Example 3.1.15
In Example 3.1.10, we saw that both 2 and -2 are greatest common divisors of 4 and 6. Using Notation 3.1.14, we can now write $\gcd(4, 6) = 2$. ◁

Exercise 3.1.16
For each $n \in \mathbb{Z}$, let $D_n \subseteq \mathbb{Z}$ be the set of divisors of n. Prove that $D_a \cap D_b = D_{\gcd(a,b)}$ for all $a, b \in \mathbb{Z}$. ◁

Our goal for the rest of this subsection is to investigate the behaviour of greatest common divisors, find out how to compute them, and look into the implications they have for solutions to certain kinds of equations.

Theorem 3.1.17
Let $a, b, q, r \in \mathbb{Z}$, and suppose that $a = qb + r$. Then

$$\gcd(a, b) = \gcd(b, r)$$

Proof. Let $d = \gcd(a, b)$. We check that d satisfies the conditions required to be a greatest common divisor of b and r.

Note that $d \mid a$ and $d \mid b$, so let $s, t \in \mathbb{Z}$ be such that $a = sd$ and $b = td$.

- $d \mid b$ by definition, and $d \mid r$ since

$$r = a - qb = sd - qtd = (s - qt)d$$

- Suppose $d' \mid b$ and $d' \mid r$; say $b = ud'$ and $r = vd'$ with $u, v \in \mathbb{Z}$. Then $d' \mid a$, since

$$a = qb + r = qud' + vd' = (qu + v)d'$$

so $d' \mid d$ since $d = \gcd(a, b)$.

135

So d is a greatest common divisor of b and r. Since $d > 0$, the result is shown.   □

Combined with the division theorem (Theorem 3.1.1), Theorem 3.1.17 gives a relatively fast algorithm for computing the greatest common divisor of two integers, known as the **Euclidean algorithm**.

Proof tip

Euclidean algorithm. Let $a, b \in \mathbb{Z}$. To find $\gcd(a, b)$, proceed as follows.

- Set $r_0 = |a|$ and $r_1 = |b|$.

- Given r_{n-2} and r_{n-1}, define r_n to be the remainder of r_{n-2} divided by r_{n-1}.

- Stop when $r_n = 0$; then $r_{n-1} = \gcd(a, b)$.

◁

Example 3.1.18

We will find the greatest common divisor of 148 and 28.

$$148 = 5 \times 28 + 8$$
$$28 = 3 \times 8 + 4$$
$$8 = 2 \times \boxed{4} + 0 \qquad\qquad\qquad \leftarrow \text{Stop!}$$

Hence $\gcd(148, 28) = 4$. Here the sequence of remainders is given by:

$$r_0 = 148, \quad r_1 = 28, \quad r_2 = 8, \quad r_3 = 4, \quad r_4 = 0$$

◁

Example 3.1.19

The Euclidean algorithm works surprisingly quickly, even for relatively large numbers. Consider the problem of computing $\gcd(1311, 5757)$ for example:

$$5757 = 4 \times 1311 + 513$$
$$1311 = 2 \times 513 + 285$$
$$513 = 1 \times 285 + 228$$
$$285 = 1 \times 228 + 57$$
$$228 = 4 \times \boxed{57} + 0 \qquad\qquad\qquad \leftarrow \text{Stop!}$$

Hence $\gcd(1311, 5757) = 57$. Here the sequence of remainders is given by:

$$r_0 = 5757, \quad r_1 = 1311, \quad r_2 = 513, \quad r_3 = 285, \quad r_4 = 228, \quad r_5 = 57, \quad r_6 = 0$$

◁

Example 3.1.20

Here's an example where one of the numbers is negative: we compute the value of $\gcd(-420, 76)$:

$$-420 = (-6) \times 76 + 36$$
$$76 = 2 \times 36 + 4$$
$$36 = 9 \times \boxed{4} + 0 \qquad\qquad\qquad \leftarrow \text{Stop!}$$

Hence $\gcd(-420, 76) = 4$. ◁

Exercise 3.1.21

Use the Euclidean algorithm to compute the greatest common divisors of the following pairs of integers

$$(12, 9), \quad (100, 35), \quad (7125, 1300), \quad (1010, 101010), \quad (-4, 14)$$

◁

The following theorem will be useful when we study modular arithmetic in Section 3.3; it is called a 'lemma' for historical reasons, and is really an important result in its own right.

Theorem 3.1.22 (Bézout's lemma)

Let $a, b, c \in \mathbb{Z}$, and let $d = \gcd(a, b)$. The equation

$$ax + by = c$$

has a solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ if and only if $d \mid c$.

Proof. ($\Rightarrow$) Write $a = a'd$ and $b = b'd$, for $a', b' \in \mathbb{Z}$. If there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$, then

$$c = ax + by = a'dx + b'dy = (a'x + b'y)d$$

and so $d \mid c$.

($\Leftarrow$) Suppose $d \mid c$, and let $c = kd$ for some $k \in \mathbb{Z}$.

If $c = 0$, then a solution is $x = y = 0$. If $c < 0$, then $ax + by = c$ if and only if $a(-x) + b(-y) = -c$; so we may assume that $c > 0$.

We proved in Theorem 3.1.12 that a greatest common divisor of a and b is a least element of the set

$$X = \{au + bv \mid u, v \in \mathbb{Z}, \ au + bv > 0\}$$

So let $u, v \in \mathbb{Z}$ be such that $au + bv = d$. Then

$$a(ku) + b(kv) = k(au + bv) = kd = c$$

and so letting $x = ku$ and $y = kv$, we see that the equation $ax + by = c$ has a solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. $\square$

Bézout's lemma completely characterises when the equation $ax + by = c$ has a solution. An easy generalisation of Bézout's lemma provides a complete characterisation of when solutions to **linear Diophantine equations** exist, that is equations of the form

$$ax + by = c$$

where $a, b, c \in \mathbb{Z}$. We will soon develop an algorithm for computing *all* solutions to these equations.

Example 3.1.23
Here are some examples of applications of Bézout's lemma.

- Consider the equation $1311x + 5757y = 12963$. We computed in Example 3.1.19 that $\gcd(1311, 5757) = 57$. But $57 \nmid 12963$ since $12963 = 227 \times 57 + 24$. By Bézout's lemma, the equation $1311x + 5757y = 12963$ has no integer solutions.

- For fixed z, the equation $4u + 6v = z$ has solutions exactly when z is even, since $\gcd(4, 6) = 2$.

- For fixed a, b, the equation $au + bv = 0$ always has solution. Indeed, setting $u = b$ and $v = -a$ gives a solution; but we knew one had to exist since by Exercise 3.1.6 we know that $d \mid 0$ for all $d \in \mathbb{Z}$.

$\triangleleft$

Exercise 3.1.24
Which of the following equations have solutions?

(a) $12u + 9v = -18$

(b) $12u + 9v = 1$

(c) $100u + 35v = 125$

(d) $7125u + 1300v = 0$

(e) $1010u + 101010v = 1010101010101010$

(f) $14u - 4v = 12$

◁

Coprimality

> **Definition 3.1.25**
> Let $a, b \in \mathbb{Z}$. We say a and b are **coprime** (or **relatively prime**), and write $a \perp b$ (L​A​T​E​X code: `\perp`) (read 'a is coprime to b'), if $\gcd(a, b) = 1$.

Example 3.1.26
$4 \perp 9$. To see this, note that if $d \mid 4$ then $d \in \{-4, -2, -1, 1, 2, 4\}$, and if $d \mid 9$ then $d \in \{-9, -3, -1, 1, 3, 9\}$. Hence if $d \mid 4$ and $d \mid 9$, then $d = 1$ or $d = -1$. It follows that $\gcd(4, 9) = 1$. ◁

Exercise 3.1.27
Which integers in the set $[15]$ are coprime to 15? ◁

Proposition 3.1.28
Let $a, b \in \mathbb{Z}$. The following are equivalent:

(1) a and b are coprime;

(2) If $d \in \mathbb{Z}$ with $d \mid a$ and $d \mid b$, then d is a unit.

Proof. We prove that condition (1) implies condition (2), and vice versa.

- (1)$\Rightarrow$(2). Suppose a and b are coprime, and fix $d \in \mathbb{Z}$ with $d \mid a$ and $d \mid b$. Then $d \mid \gcd(a, b) = 1$, so d is a unit.

- (2)$\Rightarrow$(1). Suppose condition (2) above holds. We prove that 1 satisfies the conditions required to be a greatest common divisor of a and b. The fact that $1 \mid a$ and $1 \mid b$ is automatic; and the fact that if $d \mid a$ and $d \mid b$ implies $d \mid 1$ is precisely the condition (2) that we are assuming.

Hence the two conditions are equivalent. □

Proposition 3.1.29
Let a and b be integers, not both zero, and let $d = \gcd(a, b)$. The integers $\frac{a}{d}$ and $\frac{b}{d}$ are coprime.

Exercise 3.1.30
Prove Proposition 3.1.29.   ◁

The following corollary is a specialisation of Bézout's lemma to the case when a and b are coprime.

Corollary 3.1.31
Let $a, b \in \mathbb{Z}$. The equation $au + bv = 1$ has a solution if and only if a and b are coprime. Moreover, if a and b are coprime, then the equation $au + bv = z$ has a solution for all $z \in \mathbb{Z}$.

Proof. By Bézout's lemma (Theorem 3.1.22), the equation $au + bv = 1$ has a solution if and only if $\gcd(a, b) \mid 1$. But the only positive divisor of 1 is 1, so a solution exists if and only if $\gcd(a, b) = 1$, which is precisely the assertion that a and b are coprime.

If a and b are coprime, then $1 = \gcd(a, b) \mid z$ for all $z \in \mathbb{Z}$. So by Bézout's lemma again, the equation $au + bv = z$ has a solution for all $z \in \mathbb{Z}$.   □

A useful consequence of Bézout's lemma is the following result:

Proposition 3.1.32
Let $a, b, c \in \mathbb{Z}$. If a and b are coprime and $a \mid bc$, then $a \mid c$.

Proof. By Bézout's lemma (Theorem 3.1.22) there exist integers u and v such that $au + bv = 1$. Multiplying by c gives $acu + bcv = c$. Since $a \mid bc$, we can write $bc = ka$ for some $k \in \mathbb{Z}$, and so $acu + kav = c$. But then

$$(cu + kv)a = c$$

which proves that $a \mid c$.   □

Linear Diophantine equations

We have now seen two important results:

- The **Euclidean algorithm**, which was a procedure for computing the greatest common divisor of two integers.

- **Bézout's lemma**, which provides a necessary and sufficient condition for equations of the form $ax + by = c$ to have an integer solution.

We will now develop the **reverse Euclidean algorithm**, which provides a method for computing a solutions to (bivariate) linear Diophantine equations, when such a solution exists. Then we will prove a theorem that characterises *all* integer solutions in terms of a given solution.

Example 3.1.33

Suppose we want to find integers x and y such that $327x + 114y = 18$. Running the Euclidean algorithm yields that $\gcd(327, 114) = 3$ — see below. For reasons soon to become apparent, we rearrange each equation to express the remainder on its own.

$$327 = 2 \times 114 + 99 \qquad \Rightarrow \qquad 99 = 327 - 2 \times 114 \qquad (1)$$
$$114 = 1 \times 99 + 15 \qquad \Rightarrow \qquad 15 = 114 - 1 \times 99 \qquad (2)$$
$$99 = 6 \times 15 + 9 \qquad \Rightarrow \qquad 9 = 99 - 6 \times 15 \qquad (3)$$
$$15 = 1 \times 9 + 6 \qquad \Rightarrow \qquad 6 = 15 - 1 \times 9 \qquad (4)$$
$$9 = 1 \times 6 + 3 \qquad \Rightarrow \qquad 3 = 9 - 1 \times 6 \qquad (5)$$
$$6 = 2 \times 3 + 0$$

We can then express 3 in the form $327u + 114v$ by successively substituting the equations into each other:

- Equation (5) expresses 3 as a linear combination of 6 and 9. Substituting equation (4) yields:
$$3 = 9 - 1 \times (15 - 1 \times 9) \quad \Rightarrow \quad 3 = 2 \times 9 - 1 \times 15$$

- This now expresses 3 as a linear combination of 9 and 15. Substituting equation (3) yields:
$$3 = 2 \times (99 - 6 \times 15) - 1 \times 15 \quad \Rightarrow \quad 3 = (-13) \times 15 + 2 \times 99$$

- This now expresses 3 as a linear combination of 15 and 99. Substituting equation (2) yields:
$$3 = (-13) \times (114 - 1 \times 99) + 2 \times 99 \quad \Rightarrow \quad 3 = 15 \times 99 - 13 \times 114$$

- This now expresses 3 as a linear combination of 99 and 114. Substituting equation (1) yields:
$$3 = 15 \times (327 - 2 \times 114) - 13 \times 114 \quad \Rightarrow \quad 3 = (-43) \times 114 + 15 \times 327$$

Now that we've expressed 3 as a linear combination of 114 and 327, we're nearly done: we know that $18 = 6 \times 3$, so multiplying through by 6 gives

$$18 = (-258) \times 114 + 90 \times 327$$

Hence $(x, y) = (90, -258)$ is a solution to the equation $327x + 114y = 18$. ◁

Proof tip

Let $a, b \in \mathbb{Z}$ and let $d = \gcd(a, b)$. To find integers x, y such that $ax + by = d$:

   (i) Run the Euclidean algorithm on the pair (a, b), keeping track of all quotients and remainders.

  (ii) Rearrange each equation of the form $r_{n-2} = q_n r_{n-1} + r_n$ to isolate r_n.

 (iii) Substitute for the remainders r_k in reverse order until $\gcd(a, b)$ is expressed in the form $ax + by$ for some $x, y \in \mathbb{Z}$.

This process is called the **reverse Euclidean algorithm**.   ◁

Exercise 3.1.34

Find a solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ to the equation $630x + 385y = 4340$.   ◁

Now that we have a procedure for computing *one* solution to the equation $ax + by = c$, we need to come up with a procedure for computing *all* solutions. This can be done by proving the following theorem.

Theorem 3.1.35

Let $a, b, c \in \mathbb{Z}$, where a and b are not both zero. Suppose that x_0 and y_0 are integers such that $ax_0 + by_0 = c$. Then, $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is another solution to the equation $ax + by = c$ if and only if

$$x = x_0 + k \cdot \frac{b}{\gcd(a, b)} \qquad \text{and} \qquad y = y_0 - k \cdot \frac{a}{\gcd(a, b)}$$

for some $k \in \mathbb{Z}$.

Thus, as soon as we've found one solution $(x, y) = (x_0, y_0)$ to the equation $ax + by = c$, this theorem tells us what all other solutions must look like.

Proof of Theorem 3.1.35. We prove the two directions separately.

($\Rightarrow$). First suppose that (x_0, y_0) is an integer solution to the equation $ax + by = c$. Let $k \in \mathbb{Z}$ and let

$$x = x_0 + k \cdot \frac{b}{\gcd(a, b)} \qquad \text{and} \qquad y = y_0 - k \cdot \frac{a}{\gcd(a, b)}$$

Then

$$ax + by$$

$$= a\left(x_0 + k \cdot \frac{b}{\gcd(a,b)}\right) + b\left(y_0 - k \cdot \frac{a}{\gcd(a,b)}\right) \qquad \text{by definition of } x \text{ and } y$$

$$= (ax_0 + by_0) + ak \cdot \frac{b}{\gcd(a,b)} - kb \cdot \frac{a}{\gcd(a,b)} \qquad \text{rearranging}$$

$$= (ax_0 + by_0) + \frac{kab - kab}{\gcd(a,b)} \qquad \text{combining the fractions}$$

$$= ax_0 + by_0 \qquad \text{since } kab - kab = 0$$

$$= c \qquad \text{since } (x_0, y_0) \text{ is a solution}$$

so (x, y) is indeed a solution to the equation.

($\Leftarrow$). First suppose that $a \perp b$. Fix a solution (x_0, y_0) to the equation $ax + by = c$, and let (x, y) be another solution. Then

$$a(x - x_0) + b(y - y_0) = (ax_0 + by_0) - (ax + by) = c - c = 0$$

so that

$$a(x - x_0) = b(y_0 - y)$$

Now a and b are coprime, so by Proposition 3.1.32, we have $a \mid y_0 - y$ and $b \mid x - x_0$. Let $k, \ell \in \mathbb{Z}$ be such that $x - x_0 = kb$ and $y_0 - y = \ell a$. Then substituting into the above equation yields

$$a \cdot kb = b \cdot \ell a$$

and hence $(k - \ell)ab = 0$. Since $ab \neq 0$, we have $k = \ell$, so that

$$x = x_0 + kb \quad \text{and} \quad y = y_0 - ka$$

Now we drop the assumption that $a \perp b$. Let $\gcd(a, b) = d \geqslant 1$. We know that $d \mid c$, by Bézout's lemma (Theorem 3.1.22), and so

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$$

is another linear Diophantine equations, and moreover $\frac{a}{d} \perp \frac{b}{d}$ by Proposition 3.1.29. By what we proved above, we have

$$x = x_0 + k \cdot \frac{b}{d} \quad \text{and} \quad y = y_0 - k \cdot \frac{a}{d}$$

for some $k \in \mathbb{Z}$. But this is exactly what we sought to prove! $\qquad \square$

Example 3.1.36

We know that $(x, y) = (90, -258)$ is a solution to the equation $327x + 114y = 18$, and

$$\frac{327}{\gcd(327, 114)} = \frac{327}{3} = 109 \qquad \text{and} \qquad \frac{114}{\gcd(327, 114)} = \frac{114}{3} = 38$$

so this theorem tells us that $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is a solution to the equation $327x + 114y = 18$ if and only if

$$x = 90 + 38k \qquad \text{and} \qquad y = -258 - 109k$$

for some $k \in \mathbb{Z}$.   ◁

Exercise 3.1.37

Find all integers x, y such that

$$630x + 385y = 4340$$

◁

Least common multiples

You would be forgiven for wondering why so much of the foregoing section was devoted to greatest common divisors, with no mention of least common multiples. We will now give the latter some attention.

> **Definition 3.1.38**
>
> Let $a, b \in \mathbb{Z}$. An integer m is a **least common multiple** of a and b if:
>
> (a) $a \mid m$ and $b \mid m$;
>
> (b) If n is another integer such that $a \mid n$ and $b \mid n$, then $m \mid n$.

In a sense that can be made precise, the definition of least common multiple is *dual* to that of greatest common divisor (Definition 3.1.9).[a] This means that many properties of greatest common divisors have corresponding 'dual' properties, which hold of least common multiples. As such, we will not say much here about least common multiples, and that which we *do* say is in the form of exercises.

Exercise 3.1.39

Let $a, b \in \mathbb{Z}$. Prove that a and b have a least common multiple. Furthermore, prove that least common multiples are unique up to sign, in the sense that if m, m' are two least common multiples of a and b, then $m = m'$ or $m = -m'$.   ◁

---

[a]Specifically, we refer here to the dual of a *preorder*, i.e. a reflexive, transitive relation—see Chapter 5 for more on this!

As with greatest common divisors, Exercise 3.1.39 justifies the following definition.

Definition 3.1.40

Given $a, b \in \mathbb{Z}$, denote by $\mathrm{lcm}(a, b)$ (LaTeX code: `\mathrm{lcm}`) the non-negative least common multiple of a and b.

Exercise 3.1.41

Let $a, b \in \mathbb{Z}$. Prove that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = |ab|$. ◁

3.2   Prime numbers

Thinking of divisibility as a way of *breaking down* an integer, for example $12 = 2 \times 2 \times 3$, our goal now is to show that:

- There are numbers which are *atomic*, in the sense that they can't be broken down any further by division;

- . . . and every non-zero non-unit can be written as a product of these atomic numbers;

- . . . *and* this product is essentially unique.

There are a couple of fairly vague terms used here: 'atomic' and 'essentially unique'. We will soon make these precise; the atomic numbers will be the *irreducible* and *prime* numbers (two notions which coincide for the integers), and 'essentially unique' will mean unique up to reordering and multiplication by units.

Primes and irreducibles

Definition 3.2.1
Let p be a non-zero non-unit. We say p is **prime** if for all $a, b \in \mathbb{Z}$, if $p \mid ab$ then $p \mid a$ or $p \mid b$.

Example 3.2.2
Here are some examples of prime and non-prime numbers:

- 2 is prime. Suppose not; then there exist $a, b \in \mathbb{Z}$ such that $2 \mid ab$ but 2 divides neither a nor b. Thus a and b are both odd, meaning that ab is odd. . . but this contradicts the assumption that $2 \mid ab$.

- 6 is not prime. Indeed, $6 \mid 2 \times 3$ but 6 divides neither 2 nor 3.

◁

Exercise 3.2.3
Using Definition 3.2.1, prove that 3 and 5 are prime and that 4 is not prime.   ◁

Recall the definition of binomial coefficients (Definition 1.3.27).

Example 3.2.4

Let $k \in \mathbb{Z}$ with $0 < k < 5$. We'll show that $5 \mid \binom{5}{k}$.

Well, by Theorem 1.3.31 we know that

$$5! = \binom{5}{k} k!(5-k)!$$

By Theorem 1.3.31, we have

$$\underbrace{5 \times 4!}_{=5!} = \binom{5}{k} \times \underbrace{1 \times \cdots \times k}_{=k!} \times \underbrace{1 \times \cdots \times (5-k)}_{=(5-k)!}$$

Since 5 is prime, it must divide one of the factors on the right-hand side of this equation. Thus, either 5 divides $\binom{5}{k}$, or it divides ℓ for some $1 \leqslant \ell \leqslant k$ or $1 \leqslant \ell \leqslant 5 - k$. But $k < 5$ and $5 - k < 5$, so it cannot divide any of these values of ℓ—if it did, it would imply $5 \leqslant \ell \leqslant k$ or $5 \leqslant \ell \leqslant 5 - k$, which is nonsense. Hence 5 must divide $\binom{5}{k}$. ◁

Exercise 3.2.5

Let $p \in \mathbb{Z}$ be a positive prime and let $0 < k < p$. Show that $p \mid \binom{p}{k}$. ◁

Aside

Most people are introduced to primes with a definition along the lines of 'p is prime if p has exactly two positive divisors'. We have avoided this to elucidate the fact that the integers together with their arithmetic structure are the canonical example of a mathematical object called a *ring*. The notion of a *prime element* can be defined in any ring as in Definition 3.2.1. Secondly, these two definitions are equivalent in $\mathbb{Z}$, but not in all rings. ◁

Definition 3.2.6

Let a be a non-zero non-unit. We say a is **reducible** if $a = mn$ for some non-units m, n; otherwise it is **irreducible**.

Proposition 3.2.7

A non-zero non-unit p is irreducible if and only if the only divisors of p are p, $-p$, 1 and -1.

Proof. Suppose p is irreducible and that $a \mid p$. Then $p = ab$ for some $b \in \mathbb{Z}$. Since p is irreducible, either a or b is a unit. If a is a unit then $b = \pm p$, and if b is a unit then $a = \pm p$. So the only divisors of p are ± 1 and $\pm p$.

Conversely, suppose that the only divisors of p are ± 1 and $\pm p$, and let $a, b \in \mathbb{Z}$ with $p = ab$. We want to prove that a or b is a unit. Since $a \mid p$, we have $a \in \{1, -1, p, -p\}$. If $a = \pm 1$, then a is a unit; if $a = \pm p$, then $b = \pm 1$, so that b is a unit. In any case, either a or b is a unit, and hence p is irreducible. □

Example 3.2.8

A couple of examples of reducible and irreducible numbers are:

- 2 is irreducible: if $2 = mn$ then either m or n is even, otherwise we'd be expressing an even number as the product of two odd numbers. We may assume m is even, say $m = 2k$; then $2 = 2kn$, so $kn = 1$ and hence n is a unit.

- 6 is reducible since $6 = 2 \times 3$ and both 2 and 3 are non-zero non-units.

◁

Exercise 3.2.9

Prove that if $p \in \mathbb{Z}$ is prime then p is irreducible.   ◁

Lemma 3.2.10

Let $a \in \mathbb{Z}$ be a non-zero non-unit. Then there are irreducibles $p_1, \ldots, p_n$ such that $a = p_1 \times \cdots \times p_n$.

Proof. We may assume $a > 0$, since if $a < 0$ we can just multiply by -1.

We proceed by strong induction on $a \geqslant 2$. The base case has $a = 2$ since we consider only non-units.

- (**BC**) We have shown that 2 is irreducible, so setting $p_1 = 2$ yields a product of primes.

- (**IS**) Let $a \geqslant 2$ and suppose that each integer k with $2 \leqslant k \leqslant a$ has an expression as a product of irreducibles. If $a + 1$ is irreducible then we're done; otherwise we can write $a + 1 = st$, where $s, t \in \mathbb{Z}$ are non-zero non-units. We may assume further that s and t are positive. Moreover, $s < a + 1$ and $t < a + 1$ since $s, t \geqslant 2$.

  By the induction hypothesis, s and t have expressions as products of irreducibles. Write
  $$s = p_1 \times \cdots \times p_m, \qquad t = q_1 \times \cdots \times q_n$$

  This gives rise to an expression of a as a product of irreducibles:
  $$a = st = \underbrace{p_1 \times \cdots \times p_m}_{=s} \times \underbrace{q_1 \times \cdots \times q_n}_{=t}$$

By induction, we're done.   □

> **Theorem 3.2.11**
> Let $p \in \mathbb{Z}$. Then p is prime if and only if p is irreducible.

Proof. We prove the two directions separately.

- **Prime $\Rightarrow$ irreducible.** This was Exercise 3.2.9.

- **Irreducible $\Rightarrow$ prime.** Suppose p is irreducible. Let $a, b \in \mathbb{Z}$ and suppose $p \mid ab$. We need to show that $p \mid a$ or $p \mid b$. It suffices to show that if $p \nmid a$ then $p \mid b$.

  So suppose $p \nmid a$. Let $d = \gcd(p, a)$. Since $d \mid p$ and p is irreducible, we must have $d = 1$ or $d = p$ by Proposition 3.2.7. Since $p \nmid a$ and $d \mid a$, we must therefore have $d = 1$.

  By Bézout's lemma (Theorem 3.1.22), there exist $u, v \in \mathbb{Z}$ such that $au + pv = 1$. Multiplying by b gives $abu + pbv = b$. Since $p \mid ab$, there exists $k \in \mathbb{Z}$ such that $pk = ab$. Then
  $$b = abu + pbv = pku + pbv = p(ku + bv)$$
  so $p \mid b$, as required.

So we're done. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Since primes and irreducibles are the same thing in $\mathbb{Z}$, we will refer to them as 'primes', unless we need to emphasise a particular aspect of them.

Prime factorisation

Having described prime numbers in two ways, each of which emphasises their nature of being 'unbreakable' by multiplication, we will extend Lemma 3.2.10 to prove that every integer can be expressed as a product of primes in an essentially unique way.

> **Theorem 3.2.12** (Fundamental theorem of arithmetic)
> Let $a \in \mathbb{Z}$ be a non-zero non-unit. There exist primes $p_1, \ldots, p_k \in \mathbb{Z}$ such that
> $$a = p_1 \times \cdots \times p_k$$
> Moreover, this expression is essentially unique: if $a = q_1 \times \cdots \times q_\ell$ is another expression of a as a product of primes, then $k = \ell$ and, re-ordering the q_i if necessary, for each i there is a unit u_i such that $q_i = u_i p_i$.

Proof. We showed that such a factorisation exists in Lemma 3.2.10, with the word 'prime' replaced by the word 'irreducible'. It remains to prove (essential) uniqueness.

Let k be least such that there is an expression of a as a product of k primes, namely $a = p_1 \times \cdots \times p_k$. Let $a = q_1 \times \cdots \times q_\ell$ be any other such expression. We prove by induction on k that $\ell = k$ and, after re-ordering if necessary, for each i there is a unit u_i such that $q_i = u_i p_i$.

- (**BC**) If $k = 1$ then $a = p_1$ is itself prime. Then we have $p_1 = q_1 \times \cdots \times q_\ell$. Since p_1 is prime, $p_1 \mid q_j$ for some j; by swapping q_1 and q_j we may take $j = 1$, so that $p_1 \mid q_1$. By irreducibility of q_1 we have $q_1 = u_1 p_1$ for some unit u_1.

- (**IS**) Let $k \geqslant 1$ and suppose that any integer which can be expressed as a product of k primes is (essentially) uniquely expressible in such a way. Suppose a has an expression as a product of $k + 1$ primes, and that $k + 1$ is the least such number. Suppose also that
$$a = p_1 \times \cdots \times p_k \times p_{k+1} = q_1 \times \cdots \times q_\ell$$
Note that $\ell \geqslant k + 1$. Since p_{k+1} is prime we must have $p_{k+1} \mid q_j$ for some j; by swapping q_j and q_ℓ if necessary, we may take $j = \ell$, so that $p_{k+1} \mid q_\ell$. As before, $q_\ell = u_{k+1} p_{k+1}$ for some unit u_{k+1}. Dividing through by p_{k+1} gives

$$p_1 \times \cdots \times p_k = q_1 \times \cdots \times q_{\ell-1} \times u_{k+1}$$

Replacing $q_{\ell-1}$ by $q_{\ell-1} u_{k+1}$, which is still prime, we can apply the induction hypothesis to obtain $k = \ell - 1$, so $k + 1 = \ell$, and, after reordering if necessary $q_i = u_i p_i$ for all $i \leqslant k$. Since this also holds for $i = k + 1$, we're done.

By induction, we're done. ☐

Example 3.2.13
Here are some examples of numbers written as products of primes:

- $12 = 2 \times 2 \times 3$. We could also write this as $2 \times 3 \times 2$ or $(-2) \times (-3) \times 2$, and so on.

- $53 = 53$ is an expression of 53 as a product of primes.

- $-1000 = 2 \times 5 \times (-2) \times 5 \times 2 \times 5$.

◁

Exercise 3.2.14
Express the following numbers as products of primes:

$$16 \qquad -240 \qquad 5050 \qquad 111111 \qquad -123456789$$

◁

To make things slightly more concise, we introduce a standard way of expressing a number as a product of primes:

Definition 3.2.15
The **canonical prime factorisation** of a non-zero non-unit $a \in \mathbb{Z}$ is the expression in the form

$$a = up_1^{j_1} \cdots p_r^{j_r}$$

where:

- $u = 1$ if $a > 0$, and $u = -1$ if $a < 0$;

- The numbers p_i are all positive primes;

- $p_1 < p_2 < \cdots < p_r$;

- $j_i \geqslant 1$ for all i.

We call j_i the **multiplicity** of p_i in the factorisation of a, and we call u the **sign** of a.

Typically we omit u if $u = 1$, and just write a minus sign $(-)$ if $u = -1$.

Example 3.2.16
The canonical prime factorisations of the integers given in Example 3.2.13 are:

- $12 = 2^2 \cdot 3$.

- $53 = 53$.

- $-1000 = -2^3 \cdot 5^3$.

◁

Exercise 3.2.17
Write out the canonical prime factorisations of the numbers from Exercise 3.2.14, which were:

$$16 \qquad -240 \qquad 5050 \qquad 111111 \qquad -123456789$$

◁

The following exercise provides another tool for computing reastgreatest common divisors of pairs of integers by looking at their prime factorisations.

Exercise 3.2.18

Let $p_1, p_2, \ldots, p_r$ be distinct primes, and let $k_i, \ell_i \in \mathbb{N}$ for all $1 \leqslant i \leqslant r$. Define

$$m = p_1^{k_1} \times p_2^{k_2} \times \cdots \times p_r^{k_r} \quad \text{and} \quad n = p_1^{\ell_1} \times p_2^{\ell_2} \times \cdots \times p_r^{\ell_r}$$

Prove that

$$\gcd(m, n) = p_1^{u_1} \times p_2^{u_2} \times \cdots \times p_r^{u_r}$$

where $u_i = \min\{k_i, \ell_i\}$ for all $1 \leqslant i \leqslant r$.   ◁

Example 3.2.19

We use Exercise 3.2.18 to compute the greatest common divisor of 17640 and 6468.

First we compute the prime factorisations of 17640 and 6468:

$$17640 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2 \quad \text{and} \quad 6468 = 2^2 \cdot 3 \cdot 7^2 \cdot 11$$

It now follows from Exercise 3.2.18 that

$$\begin{aligned} \gcd(17640, 6468) &= 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^2 \cdot 11^0 \\ &= 4 \cdot 3 \cdot 1 \cdot 49 \cdot 1 \\ &= 588 \end{aligned}$$

◁

Distribution of primes

So far we have seen several examples of prime numbers; to name a few, we've seen 2, 3, 5 and 53. It might seem like the prime numbers go on forever, but proving this is less than obvious.

Exercise 3.2.20

Let P be an inhabited finite set of positive prime numbers and let m be the product of all the elements of P. That is, for some $n \geqslant 1$ let

$$P = \{p_1, \ldots, p_n\} \quad \text{and} \quad m = p_1 \times \cdots \times p_n$$

where each $p_k \in P$ is a positive prime. Using the fundamental theorem of arithmetic, show that $m + 1$ has a positive prime divisor which is not an element of P.   ◁

Theorem 3.2.21

There are infinitely many primes.

Proof. We prove that there are infinitely many *positive* prime numbers—the result then follows immediately. Let P be the set of all positive prime numbers. Then P is inhabited, since $2 \in P$, for example. If P were finite, then by Exercise 3.2.20, there would be a positive prime which is not an element of P—but P contains all positive primes, so that is impossible. Hence there are infinitely many positive primes. □

This is one proof of many, which is due to Euclid around 2300 years ago. We might hope that a proof of the infinitude of primes gives some insight into how the primes are *distributed*. That is, we might ask questions like: how frequently do primes occur? How fast does the sequence of primes grow? How likely is there to be a prime number in a given set of integers?

As a starting point, Euclid's proof gives an algorithm for writing an infinite list of primes:

- Let $p_1 = 2$; we know that 2 is prime;

- Given $p_1, \ldots, p_n$, let p_{n+1} be the smallest positive prime factor of $p_1 \times \cdots \times p_n + 1$.

The first few terms produced would be:

- $p_1 = 2$ by definition;

- $2 + 1 = 3$, which is prime, so $p_2 = 3$;

- $2 \times 3 + 1 = 7$, which is prime, so $p_3 = 7$;

- $2 \times 3 \times 7 + 1 = 43$, which is prime, so $p_4 = 43$;

- $2 \times 3 \times 7 \times 43 + 1 = 1807 = 13 \times 139$, so $p_5 = 13$;

- $2 \times 3 \times 7 \times 43 \times 13 + 1 = 23479 = 53 \times 443$, so $p_6 = 53$;

- … and so on.

The sequence obtained, called the *Euclid–Mullin sequence*, is a bit bizarre:

$$2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, \ldots$$

Big primes like 38709183810571 often appear before small primes like 11. It remains unknown whether or not every positive prime number appears in this list!

The chaotic nature of this sequence makes it difficult to extract information about how the primes are distributed: the numbers $p_1 \times \cdots \times p_n + 1$ grow very quickly—indeed, it must

be the case that $p_1 \times \cdots \times p_n + 1 > 2^n$ for all n—so the upper bounds for the sequence grow at least exponentially.

Another proof of the infinitude of primes that gives a (slightly) tighter bound can be obtained using the following exercise.

Exercise 3.2.22

Let $n \in \mathbb{Z}$ with $n > 2$. Prove that the set $\{k \in \mathbb{Z} \mid n < k < n!\}$ contains a prime number. ◁

3.3 Modular arithmetic

It turns out that much arithmetic can be done by considering only the *remainders* of integers when divided by a fixed integer. Here is a simple example:

Example 3.3.1

Suppose a_1 has remainder r_1 and a_2 has remainder r_2 when divided by 7. That is, there exist $q_1, q_2 \in \mathbb{Z}$ such that

$$a_1 = 7q_1 + r_1 \qquad \text{and} \qquad a_2 = 7q_2 + r_2$$

Then $a_1 + a_2$ has the same remainder as $r_1 + r_2$ when divided by 7. Indeed, suppose $a_1 + a_2 = 7q + r$, where $0 \leqslant r < 7$. Then

$$\begin{aligned}
r_1 + r_2 &= (a_1 - 7q_1) + (a_2 - 7q_2) \\
&= (a_1 + a_2) + 7(-q_1 - q_2) \\
&= (7q + r) + 7(-q_1 - q_1) \\
&= 7(q - q_1 - q_2) + r
\end{aligned}$$

An example of this in action: $41 = 5 \times 7 + 6$ and $240 = 34 \times 7 + 2$, so the remainders of 41 and 240 when divided by 7 are 6 and 2, respectively. Now

$$41 + 240 = 281 = 40 \times 7 + 1 \qquad \text{and} \qquad 6 + 2 = 8 = 1 \times 7 + 1$$

which demonstrates that $41 + 240$ and $6 + 2$ have the same remainder when divided by 7. ◁

In this section we will study the extent to which we can do arithmetic with integers knowing only their remainders upon division by a given integer.

Definition 3.3.2

Fix $n \in \mathbb{Z}$. Given integers $a, b \in \mathbb{Z}$, we say a is **congruent** to b **modulo** n, and write

$$a \equiv b \bmod n \text{ (\LaTeX\ code: } \texttt{a \textbackslash equiv b \textbackslash bmod\{n\}} \text{)}$$

if $n \mid a - b$. If a is not congruent to b modulo n, write

$$a \not\equiv b \bmod n \text{ (\LaTeX\ code: } \texttt{\textbackslash not\textbackslash equiv} \text{)}$$

The number n is called the **modulus** of the congruence.

Convention 3.3.3

When talking about modular arithmetic, we will restrict our attention to *positive* integers. This is because for any integers a, b, n we have

$$a \equiv b \bmod n \quad \Leftrightarrow \quad a \equiv b \bmod (-n)$$

and $a \equiv b \bmod 0$ if and only if $a = b$. Thus, whenever we write 'mod$n$' or specify that a variable n is a 'modulus', it is implicit that n is an integer and $n > 0$. This will shorten some of our proofs.   ◁

Example 3.3.4

Some examples of congruence modulo n are as follows:

- $16 \equiv 30 \bmod 2$ since $30 - 16 = 14$, which is a multiple of 2.

- $44 \equiv 20 \bmod 6$ since $20 - 44 = -24$, which is a multiple of 6.

◁

Exercise 3.3.5

Show that if $a, b \in \mathbb{Z}$ with $a, b \geqslant 0$ then $a \equiv b \bmod 10$ if and only if the decimal expressions of a and b end in the same digit. What happens when a and b are allowed to be negative?   ◁

It is important from the outset to point out that, although congruence is written with a symbol that looks like that of equality ('$\equiv$' vs. '$=$'), we can only treat congruence like equality inasmuch as we have proved we can. Specifically, the ways in which congruence *can* be treated like equality will be proved in two theorems:

- Theorem 3.3.6 tells us that congruence satisfies three extremely basic properties of equality.[b] One useful consequence of this is that it is valid to use strings of congruences, for example

$$-5 \equiv 18 \equiv 41 \equiv 64 \bmod 23 \quad \Rightarrow \quad -5 \equiv 64 \bmod 23$$

- Theorem 3.3.9 tells us that we can treat congruence like equality for the purposes of addition, multiplication and subtraction. Thus it will be valid to write things like

$$x \equiv 7 \bmod 12 \quad \Rightarrow \quad 2x + 5 \equiv 19 \bmod 12$$

---

[b] Using the language of Definition 5.1.31, Theorem 3.3.6 says precisely that congruence is an *equivalence relation*.

and we'll be able to replace values by congruent values in congruences, provided they're only being added, subtracted or multiplied. For example, from the knowledge that $2^{60} \equiv 1 \bmod 61$ and $60! \equiv -1 \bmod 61$, we will be able to deduce

$$2^{60} \cdot 3 \equiv 60! \cdot x \bmod 61 \quad \Rightarrow \quad 3 \equiv -x \bmod 61$$

Don't let these properties shared by congruence and equality lull you into a false sense of security! We will soon see that for other purposes, such as division and various other algebraic operations, congruence does *not* behave like equality.

Theorem 3.3.6

Let $a, b, c \in \mathbb{Z}$ and let n be a modulus. Then

(a) $a \equiv a \bmod n$;

(b) If $a \equiv b \bmod n$, then $b \equiv a \bmod n$;

(c) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.

Proof.

(a) Note that $a - a = 0$, which is divisible by n since $0 = 0 \times n$, and hence $a \equiv a \bmod n$.

(b) Suppose $a \equiv b \bmod n$. Then $n \mid a - b$, so that $a - b = kn$ for some $k \in \mathbb{Z}$. Hence $b - a = -kn$, and so $n \mid b - a$, so that $b \equiv a \bmod n$ as required.

(c) Suppose $a \equiv b \bmod n$ and $b \equiv c \bmod n$. Then $n \mid a - b$ and $n \mid b - c$, so there exist $k, \ell \in \mathbb{Z}$ such that
$$a - b = kn \quad \text{and} \quad b - c = \ell n$$
Hence $a - c = (a - b) + (b - c) = (k + \ell)n$, so that $n \mid a - c$. Hence $a \equiv c \bmod n$, as required.

$\square$

There is a slightly simpler characterisation of congruence modulo n, as seen in Proposition 3.3.7 below.

Proposition 3.3.7

Fix a modulus n and let $a, b \in \mathbb{Z}$. The following are equivalent:

(i) a and b leave the same remainder when divided by n;

(ii) $a = b + kn$ for some $k \in \mathbb{Z}$;

(iii) $a \equiv b \bmod n$.

Proof. We prove (i) $\Leftrightarrow$ (iii) and (ii) $\Leftrightarrow$ (iii).

- (i) $\Rightarrow$ (iii). Suppose a and b leave the same remainder when divided by n, and let $q_1, q_2, r \in \mathbb{Z}$ be such that

$$a = q_1 n + r, \quad b = q_2 n + r \quad \text{and} \quad 0 \leqslant r < n$$

  Then $a - b = (q_1 - q_2)n$, which proves that $n \mid a - b$, and so $a \equiv b \bmod n$.

- (iii) $\Rightarrow$ (i). Suppose that $a \equiv b \bmod n$, so that $b - a = qn$ for some $q \in \mathbb{Z}$. Write

$$a = q_1 n + r_1, \quad b = q_2 n + r_2 \quad \text{and} \quad 0 \leqslant r_1, r_2 < n$$

  We may further assume that $r_1 \leqslant r_2$. (If not, swap the roles of a and b—this is fine, since $n \mid b - a$ if and only if $n \mid a - b$.) Now we have

$$\begin{aligned} b - a = qn &\Rightarrow (q_2 n + r_2) - (q_1 n + r_1) = qn \\ &\Rightarrow (q_2 - q_1 - q)n + (r_2 - r_1) = 0 \qquad \text{rearranging} \end{aligned}$$

  since $0 \leqslant r_1 \leqslant r_2 < n$ we have $0 \leqslant r_2 - r_1 < n$, so that $r_2 - r_1$ is the remainder of 0 when divided by n. That is, $r_2 - r_1 = 0$, so $r_1 = r_2$. Hence a and b have the same remainder when divided by n.

- (ii) $\Leftrightarrow$ (iii). We unpack the definitions of (ii) and (iii) to see that they are equivalent. Indeed

$$\begin{aligned} \text{(ii)} &\Leftrightarrow a = b + kn \text{ for some } k \in \mathbb{Z} \\ &\Leftrightarrow a - b = kn \text{ for some } k \in \mathbb{Z} \qquad \text{rearranging} \\ &\Leftrightarrow n \mid a - b \qquad\qquad\qquad\quad \text{by definition of divisibility} \\ &\Leftrightarrow a \equiv b \bmod n \qquad\qquad\quad\ \text{by definition of congruence} \\ &\Leftrightarrow \text{(iii)} \end{aligned}$$

$\square$

Discussion 3.3.8
Where in the proof of Proposition 3.3.7 did we rely on the convention that the modulus n is positive? Is the result still true if n is negative? $\triangleleft$

The following theorem tells us that, in a very limited sense, the $\equiv$ symbol can be treated as a $=$ symbol for the purposes of doing addition, subtraction and multiplication. Emphatically, it does *not* say that we can treat '$\equiv$' like '$=$' for the purposes of doing *division*.

Theorem 3.3.9 (Modular arithmetic)

Fix a modulus n, and let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ be such that

$$a_1 \equiv b_1 \bmod n \qquad \text{and} \qquad a_2 \equiv b_2 \bmod n$$

Then the following congruences hold:

(a) $a_1 + a_2 \equiv b_1 + b_2 \bmod n$;

(b) $a_1 a_2 \equiv b_1 b_2 \bmod n$;

(c) $a_1 - a_2 \equiv b_1 - b_2 \bmod n$.

Proof. By Definition 3.3.2 that $n \mid a_1 - b_1$ and $n \mid a_2 - b_2$, so there exist $q_1, q_2 \in \mathbb{Z}$ such that

$$a_1 - b_1 = q_1 n \qquad \text{and} \qquad a_2 - b_2 = q_2 n$$

This implies that

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) = q_1 n + q_2 n = (q_1 + q_2) n$$

so $n \mid (a_1 + a_2) - (b_1 + b_2)$. This proves (a).

The algebra for (b) is slightly more involved:

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= (q_1 n + b_1)(q_2 n + b_2) - b_1 b_2 \\ &= q_1 q_2 n^2 + b_1 q_2 n + b_2 q_1 n + b_1 b_2 - b_1 b_2 \\ &= q_1 q_2 n^2 + b_1 q_2 n + b_2 q_1 n \\ &= (q_1 q_2 n + b_1 q_2 + b_2 q_1) n \end{aligned}$$

This shows that $n \mid a_1 a_2 - b_1 b_2$, thus proving (b).

Now (a) and (b) together imply (c). Indeed, we know that $-1 \equiv -1 \bmod n$ and $b_1 \equiv b_2 \bmod n$, so by (b) we have $-b_1 \equiv -b_2 \bmod n$. We also know that $a_1 \equiv a_2 \bmod n$, and hence $a_1 - b_1 \equiv a_2 - b_2 \bmod n$ by (a). $\qquad \square$

Theorem 3.3.9 allows us to perform algebraic manipulations with congruences as if they were equations, provided all we're doing is adding, multiplying and subtracting.

Example 3.3.10

We will solve the congruence $3x - 5 \equiv 2x + 3 \bmod 7$ for x:

$$3x - 5 \equiv 2x + 3 \bmod 7$$

$\Leftrightarrow$	$x - 5 \equiv 3 \bmod 7$	$(\Rightarrow)$ subtract $2x$	$(\Leftarrow)$ add $2x$
$\Leftrightarrow$	$x \equiv 8 \bmod 7$	$(\Rightarrow)$ add 5	$(\Leftarrow)$ subtract 5
$\Leftrightarrow$	$x \equiv 1 \bmod 7$	since $8 \equiv 1 \bmod 7$	

So the integers x for which $3x - 5$ and $2x + 3$ leave the same remainder when divided by 7, are precisely the integers x which leave a remainder of 1 when divided by 7:

$$3x - 5 \equiv 2x + 3 \bmod 7 \qquad \Leftrightarrow \qquad x = 7q + 1 \text{ for some } q \in \mathbb{Z}$$

$\triangleleft$

Exercise 3.3.11

For which integers x does the congruence $5x + 1 \equiv x + 8 \bmod 3$ hold? Characterise such integers x in terms of their remainder when divided by 3. $\triangleleft$

So far this all feels like we haven't done very much: we've just introduced a new symbol $\equiv$ which behaves just like equality... but does it really? The following exercises should expose some more ways in which congruence *does* behave like equality, and some in which it *doesn't*.

Exercise 3.3.12

Fix a modulus n. Is it true that

$$a \equiv b \bmod n \quad \Rightarrow \quad a^k \equiv b^k \bmod n$$

for all $a, b \in \mathbb{Z}$ and $k \in \mathbb{N}$? If so, prove it; if not, provide a counterexample. $\triangleleft$

Exercise 3.3.13

Fix a modulus n. Is it true that

$$k \equiv \ell \bmod n \quad \Rightarrow \quad a^k \equiv a^\ell \bmod n$$

for all $k, \ell \in \mathbb{N}$ and $a \in \mathbb{Z}$? If so, prove it; if not, provide a counterexample. $\triangleleft$

Exercise 3.3.14

Fix a modulus n. Is it true that

$$qa \equiv qb \bmod n \quad \Rightarrow \quad a \equiv b \bmod n$$

for all $a, b, q \in \mathbb{Z}$ with $q \not\equiv 0 \bmod n$? If so, prove it; if not, provide a counterexample. $\triangleleft$

Common error

The false sense of security that Theorem 3.3.9 induces often leads students new to all this to the belief that $\equiv$ and $=$ are interchangeable concepts. This is emphatically *not* the case. In particular:

- Fractions don't make sense in modular arithmetic; for instance, it is invalid to say $2x \equiv 1 \bmod 5$ implies $x \equiv \frac{1}{2} \bmod 5$.

- Square roots don't make sense in modular arithmetic; for instance, it is invalid to say $x^2 \equiv 3 \bmod 4$ implies $x \equiv \pm\sqrt{3} \bmod 4$.

- Numbers in exponents cannot be replaced by congruent numbers; for instance, it is invalid to say $x^3 \equiv 2^3 \bmod 4$ implies $x \equiv 2 \bmod 4$.

$\triangleleft$

Multiplicative inverses

We made a big deal about the fact that fractions don't make sense in modular arithmetic. That is, it is invalid to say

$$2x \equiv 1 \bmod 5 \quad \Rightarrow \quad x \equiv \frac{1}{2} \bmod 5$$

Despite this, we can still make sense of 'division', provided we change what we mean when we say 'division'. Indeed, the congruence $2x \equiv 1 \bmod 5$ has a solution:

$$2x \equiv 1 \bmod 5$$
$$\Leftrightarrow \quad 6x \equiv 3 \bmod 5 \qquad (\Rightarrow) \text{ multiply by 3} \qquad (\Leftarrow) \text{ subtract 3}$$
$$\Leftrightarrow \quad x \equiv 3 \bmod 5 \qquad \text{since } 6 \equiv 1 \bmod 5$$

Here we didn't divide by 2, but we still managed to cancel the 2 by instead multiplying through by 3. For the purposes of solving the equation this had the same effect as division by 2 would have had if we were allowed to divide. The key here was that $2 \times 3 \equiv 1 \bmod 5$.

> **Definition 3.3.15**
> Fix a modulus n. Given $a \in \mathbb{Z}$, a **multiplicative inverse** for a modulo n is an integer u such that $au \equiv 1 \bmod n$.

Example 3.3.16

Some examples of multiplicative inverses are as follows:

- 2 is a multiplicative inverse of itself modulo 3, since $2 \times 2 \equiv 4 \equiv 1 \bmod 3$.

- 2 is a multiplicative inverse of 3 modulo 5, since $2 \times 3 \equiv 6 \equiv 1 \bmod 5$.

- 7 is also a multiplicative inverse of 3 modulo 5, since $3 \times 7 \equiv 21 \equiv 1 \bmod 5$.

- 3 has no multiplicative inverse modulo 6. Indeed, suppose $u \in \mathbb{Z}$ with $3u \equiv 1 \bmod 6$. Then $6 \mid 3u - 1$, so $3u - 1 = 6q$ for some $q \in \mathbb{Z}$. But then

$$1 = 3u - 6q = 3(u - 2q)$$

  which implies that $3 \mid 1$, which is nonsense.

$\triangleleft$

Knowing when multiplicative inverses exist is very important for solving congruences: if u is a multiplicative inverse for a modulo n, then we can solve equations of the form $ax \equiv b \bmod n$ extremely easily:

$$ax \equiv b \bmod n \quad \Rightarrow \quad x \equiv ub \bmod n$$

Exercise 3.3.17
For $n = 7, 8, 9, 10, 11, 12$, either find a multiplicative inverse for 6 modulo n, or show that no multiplicative inverse exists. Can you spot a pattern? $\triangleleft$

Some authors write a^{-1} to denote multiplicative inverses. We refrain from this, since it suggests that multiplicative inverses are unique—but they're not, as you'll see in the following exercise.

Exercise 3.3.18
Let n be a modulus and let $a \in \mathbb{Z}$. Suppose that u is a multiplicative inverse for a modulo n. Prove that, for all $k \in \mathbb{Z}$, $u + kn$ is a multiplicative inverse for a modulo n. $\triangleleft$

Proposition 3.3.19
Let $a \in \mathbb{Z}$ and let n be a modulus. Then a has a multiplicative inverse modulo n if and only if $a \perp n$.

Proof. Note that a has a multiplicative inverse u modulo n if and only if there is a solution (u, v) to the equation $au + nv = 1$. Indeed, $au \equiv 1 \bmod n$ if and only if $n \mid au - 1$, which occurs if and only if there is some $q \in \mathbb{Z}$ such that $au - 1 = nq$. Setting $q = -v$ and rearranging yields the desired equivalence.

By Bézout's lemma (Theorem 3.1.22), such a solution (u, v) exists if and only if $\gcd(a, n) \mid 1$. This occurs if and only if $\gcd(a, n) = 1$, i.e. if and only if $a \perp n$. $\square$

Proof tip

To solve a congruence of the form $ax \equiv b \bmod n$ when $a \perp n$, first find a multiplicative inverse u for a modulo n, and then simply multiply through by u to obtain $x \equiv ub \bmod n$. ◁

Corollary 3.3.20

Let $a, p \in \mathbb{Z}$, where p is a positive prime. If $p \nmid a$ then a has a multiplicative inverse modulo p.

Proof. Suppose $p \nmid a$, and let $d = \gcd(a, p)$. Since $d \mid p$ and p is prime we have $d = 1$ or $d = p$. Since $d \mid a$ and $p \nmid a$ we can't have $d = p$; therefore $d = 1$. By Proposition 3.3.19, a has a multiplicative inverse modulo p. □

Example 3.3.21

11 is prime, so each of the integers a with $1 \leqslant a \leqslant 10$ should have a multiplicative inverse modulo 11. And indeed, the following are all congruent to 1 modulo 11:

$$1 \times 1 = 1 \quad 2 \times 6 = 12 \quad 3 \times 4 = 12 \quad 4 \times 3 = 12 \quad 5 \times 9 = 45$$
$$6 \times 2 = 12 \quad 7 \times 8 = 56 \quad 8 \times 7 = 56 \quad 9 \times 5 = 45 \quad 10 \times 10 = 100$$

◁

Exercise 3.3.22

Find all integers x such that $25x - 4 \equiv 4x + 3 \bmod 13$. ◁

Orders and totients

For any modulus n, there are only finitely many possible remainders modulo n. A nice consequence of this finiteness is that, when $a \perp n$, we can choose some power of a to be its multiplicative inverse, as proved in the following exercise.

Exercise 3.3.23

Let n be a modulus and let $a \in \mathbb{Z}$ with $a \perp n$. Prove that there exists $k \geqslant 1$ such that $a^k \equiv 1 \bmod n$. ◁

Exercise 3.3.23, together with the well-ordering principle, justify the following definition.

Definition 3.3.24

Let n be a modulus and let $a \in \mathbb{Z}$ with $a \perp n$. The **order** of a modulo n is the least $k \geqslant 1$ such that $a^k \equiv 1 \bmod n$.

Note that this definition makes sense by Exercise 3.3.23 and the well-ordering principle.

Example 3.3.25

The powers of 7 modulo 100 are:

- $7^1 = 7$, so $7^1 \equiv 7 \bmod 100$;

- $7^2 = 49$, so $7^2 \equiv 49 \bmod 100$;

- $7^3 = 343$, so $7^3 \equiv 43 \bmod 100$;

- $7^4 = 2401$, so $7^4 \equiv 1 \bmod 100$.

Hence the order of 7 modulo 100 is 4, and 7^3 and 43 are multiplicative inverses of 7 modulo 100.   ◁

Our focus turns to computing specific values of k such that $a^k \equiv 1 \bmod n$, whenever $a \in \mathbb{Z}$ and $a \perp n$. We first focus on the case when n is prime; then we develop the machinery of *totients* to study the case when n is not prime.

Lemma 3.3.26

Let $a, b \in \mathbb{Z}$ and let $p \in \mathbb{Z}$ be a positive prime. Then $(a + b)^p \equiv a^p + b^p \bmod p$.

Proof. By the binomial theorem (Theorem 1.3.34), we have

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

By Exercise 3.2.5, $p \mid \binom{p}{k}$ for all $0 < k < p$, and hence $\binom{p}{k} a^k b^{p-k} \equiv 0 \bmod p$ for all $0 < k < p$. Thus

$$(a + b)^p \equiv \binom{p}{0} a^0 b^{p-0} + \binom{p}{p} a^p b^{p-p} \equiv a^p + b^p \bmod p$$

as desired.   □

Theorem 3.3.27 (Fermat's little theorem)

Let $a, p \in \mathbb{Z}$ with p a positive prime. Then $a^p \equiv a \bmod p$.

Proof. We may assume that $a \geqslant 0$, otherwise replace a by its remainder modulo p.

We will prove that $a^p \equiv a \bmod p$ by induction on a.

- (**BC**) Since $p > 0$ we have $0^p = 0$, hence $0^p \equiv 0 \bmod p$.

- (**IS**) Fix $a \geqslant 0$ and suppose $a^p \equiv a \bmod p$. Then $(a+1)^p \equiv a^p + 1^p \bmod p$ by Lemma 3.3.26. Now $a^p \equiv a \bmod p$ by the induction hypothesis, and $1^p = 1$, so we have $(a+1)^p \equiv a + 1 \bmod p$.

By induction, we're done. □

Corollary 3.3.28

Let $a, p \in \mathbb{Z}$ with p a positive prime and $p \nmid a$. then $a^{p-1} \equiv 1 \bmod p$.

Proof. Since $p \nmid a$, it follows that $a \perp p$. Fermat's little theorem (Theorem 3.3.27) tells us that $a^{|p|} \equiv a \bmod p$. By Proposition 3.3.19, a has a multiplicative inverse b modulo p. Hence

$$a^p b \equiv ab \bmod p$$

But $a^p b \equiv a^{p-1} ab \bmod p$, and $ab \equiv 1 \bmod p$, so we get

$$a^{p-1} \equiv 1 \bmod p$$

as required. □

This can be useful for computing remainders of humongous numbers when divided by smaller primes.

Example 3.3.29

We compute the remainder of 2^{1000} when divided by 7. By Fermat's little theorem (Theorem 3.3.27), we know that $2^7 \equiv 2 \bmod 7$. Since $7 \nmid 2$, it follows that 2 has a multiplicative inverse modulo 7, so we can cancel it from both sides to obtain $2^6 \equiv 1 \bmod 7$. Now $1000 = 166 \times 6 + 4$, so

$$2^{1000} \equiv 2^{166 \times 6 + 4} \equiv (2^6)^{166} \cdot 2^4 \equiv 2^4 \equiv 16 \equiv 2 \bmod 7$$

so the remainder of 2^{1000} when divided by 7 is 2. ◁

Exercise 3.3.30

Find the remainder of 3^{244886} when divided by 13. ◁

Unfortunately, the hypothesis that p is prime in Fermat's little theorem is necessary. For example, 6 is not prime, and $5^{6-1} = 5^5 = 3125 = 520 \times 6 + 5$, so $5^5 \equiv 5 \bmod 6$.

Definition 3.3.31

Let $n \in \mathbb{Z}$. The **totient** of n is the natural number $\varphi(n)$ (LaTeX code: `\varphi(n)`), which is the number of integers from 1 up to $|n|$ which are coprime to n.[a]

---

[a]More succinctly, we have $\varphi(n) = |\{k \in [|n|] \mid k \perp n\}|$, where the notation $|X|$ is defined in Definition 4.1.39.

Example 3.3.32

Here are some examples of totients:

- The elements of $[6]$ which are coprime to 6 are 1 and 5, so $\varphi(6) = 2$.

- If p is a positive prime, then every element of $[p]$ is coprime to p except for p itself. Hence if p is a positive prime then $\varphi(p) = p - 1$. More generally, if p is prime then $\varphi(p) = |p| - 1$.

◁

Exercise 3.3.33

Prove that if p is a positive prime and $k \geqslant 1$ then

$$\varphi(p^k) = p^k - p^{k-1}$$

◁

Theorem 3.3.34 (Euler's theorem)

Let n be a modulus and let $a \in \mathbb{Z}$ with $a \perp n$. Then

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Proof. By definition of totient, the set X defined by

$$X = \{k \in [n] \mid k \perp n\}$$

has $\varphi(n)$ elements. List the elements as

$$X = \{x_1, x_2, \ldots, x_{\varphi(n)}\}$$

Note that $ax_i \perp n$ for all i, so let y_i be the (unique) element of X such that $ax_i \equiv y_i \bmod n$.

Note that if $i \neq j$ then $y_i \neq y_j$. We prove this by contraposition; indeed, since $a \perp n$, by Proposition 3.3.19, a has a multiplicative inverse, say b. Then

$$y_i \equiv y_j \bmod n \ \Rightarrow \ ax_i \equiv ax_j \bmod n \ \Rightarrow \ bax_i \equiv bax_j \bmod n \ \Rightarrow \ x_i \equiv x_j \bmod n$$

and $x_i \equiv x_j \bmod n$ if and only if $i = j$. Thus

$$X = \{x_1, x_2, \ldots, x_{\varphi(n)}\} = \{y_1, y_2, \ldots, y_{\varphi(n)}\}$$

This means that the product of the 'x_i's is equal to the product of the 'y_i's, and hence

$$x_1 \cdot \ldots \cdot x_{\varphi(n)}$$
$$\equiv y_1 \cdot \ldots \cdot y_{\varphi(n)} \bmod n \qquad\qquad \text{since } \{x_1, \ldots\} = \{y_1, \ldots\}$$
$$\equiv (ax_1) \cdot \ldots \cdot (ax_{\varphi(n)}) \bmod n \qquad \text{since } y_i \equiv ax_i \bmod n$$
$$\equiv a^{\varphi(n)} \cdot x_1 \cdot \ldots \cdot x_{\varphi(n)} \bmod n \qquad \text{rearranging}$$

Since each x_i is coprime to n, we can cancel the x_i terms (by multiplying by their multiplicative inverses) to obtain

$$a^{\varphi(n)} \equiv 1 \bmod n$$

as required. □

Example 3.3.35
Some examples of Euler's theorem in action are as follows:

- We have seen that $\varphi(6) = 2$, and we know that $5 \perp 6$. And, indeed,

$$5^{\varphi(6)} = 5^2 = 25 = 4 \times 6 + 1$$

  so $5^{\varphi(6)} \equiv 1 \bmod 6$.

- By Exercise 3.3.33, we have

$$\varphi(121) = \varphi(11^2) = 11^2 - 11^1 = 121 - 11 = 110$$

  Moreover, given $a \in \mathbb{Z}$, $a \perp 121$ if and only if $11 \nmid a$. Hence $a^{110} \equiv 1 \bmod 121$ whenever $11 \nmid a$.

◁

Wilson's theorem

We conclude this chapter on number theory with *Wilson's theorem*, which is a nice result that completely characterises prime numbers in the sense that we can tell when a number is prime by computing the remainder of $(n-1)!$ when divided by n.

Let's test a few numbers first:

n	$(n-1)!$	remainder	n	$(n-1)!$	remainder
2	1	1	9	40320	0
3	2	2	10	362880	0
4	6	2	11	3628800	10
5	24	4	12	39916800	0
6	120	0	13	479001600	12
7	720	6	14	6227020800	0
8	5040	0	15	87178291200	0

It's tempting to say that an integer $n > 1$ is prime if and only if $n \nmid (n-1)!$, but this isn't true since it fails when $n = 4$. But it's extremely close to being true.

Theorem 3.3.36 (Wilson's theorem)

Let $n > 1$ be a modulus. Then n is prime if and only if $(n-1)! \equiv -1 \bmod n$.

The following sequence of exercises will piece together into a proof of Wilson's theorem.

Exercise 3.3.37

Let $n \in \mathbb{Z}$ be composite. Prove that if $n > 4$, then $n \mid (n-1)!$. ◁

Exercise 3.3.38

Let p be a positive prime and let $a \in \mathbb{Z}$. Prove that, if $a^2 \equiv 1 \bmod p$, then $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$. ◁

Exercise 3.3.38 implies that the only elements of $[p-1]$ that are their own multiplicative inverses are 1 and $p-1$; this morsel of information allows us to deduce result in the following exercise.

Exercise 3.3.39

Let p be a positive prime. Prove that $(p-1)! \equiv -1 \bmod p$. ◁

Proof of Wilson's theorem (Theorem 3.3.36). Let $n > 1$ be a modulus.

- If n is prime, then $(n-1)! \equiv -1 \bmod n$ by Exercise 3.3.39.

- If n is composite, then either $n = 4$ or $n > 4$. If $n = 4$ then

$$(n-1)! = 3! = 6 \equiv 2 \bmod 4$$

  and so $(n-1)! \not\equiv -1 \bmod n$. If $n > 4$, then

$$(n-1)! \equiv 0 \bmod n$$

  by Exercise 3.3.37.

Hence $(n-1)! \equiv -1 \bmod n$ if and only if n is prime, as desired. $\qquad \square$

Since Wilson's theorem completely characterises the positive prime numbers, we could have defined 'n is prime', for $n > 1$, to mean that $(n-1)! \equiv -1 \bmod n$. We don't do this because, although this is an interesting result, it is not particularly useful in applications. We might even hope that Wilson's theorem gives us an easy way to test whether a number is prime, but unfortunately even this is a bust: computing the remainder $(n-1)!$ on division by n is not particularly efficient.

However, there are some nice applications of Wilson's theorem, which we will explore now.

Example 3.3.40

We'll compute the remainder of $3^{45} \cdot 44!$ when divided by 47. Note that $3^{45} \cdot 44!$ is equal to a monstrous number with 76 digits; I don't recommend doing the long division! Anyway...

- 47 is prime, so we can apply both Fermat's little theorem (Theorem 3.3.27) and Wilson's theorem (Theorem 3.3.36).

- By Fermat's little theorem, we know that $3^{46} \equiv 1 \bmod 47$. Since $3 \cdot 16 = 48 \equiv 1 \bmod 47$, we have

$$3^{45} \equiv 3^{45} \cdot (3 \cdot 16) \equiv 3^{46} \cdot 16 \equiv 16 \bmod 47$$

- By Wilson's theorem, we have $46! \equiv -1 \bmod 47$. Now

  ◇ $46 \equiv -1 \bmod 47$, so 46 is its own multiplicative inverse modulo 47.
  ◇ The extended Euclidean algorithm yields $45 \cdot 23 \equiv 1 \bmod 47$.

  So we have

$$44! = 44! \cdot (45 \cdot 23) \cdot (46 \cdot 46) \equiv 46! \cdot 23 \cdot 46 \equiv (-1) \cdot 23 \cdot (-1) \equiv 23 \bmod 47$$

Putting this information together yields

$$3^{45} \cdot 44! \equiv 16 \cdot 23 = 368 \equiv 39 \bmod 47$$

So the remainder left when $3^{45} \cdot 44!$ is divided by 47 is 39. $\qquad \triangleleft$

Exercise 3.3.41

Let p be an odd positive prime. Prove that

$$\left[\left(\frac{p-1}{2} \right)! \right]^2 \equiv (-1)^{\frac{p+1}{2}} \bmod p$$

$\triangleleft$

Chinese remainder theorem

We introduce the Chinese remainder theorem with an example.

Example 3.3.42

We find all integer solutions x to the system of congruences

$$x \equiv 2 \bmod 5 \quad \text{and} \quad x \equiv 4 \bmod 8$$

Note that $x \equiv 4 \bmod 8$ if and only if $x = 4 + 8k$ for some $k \in \mathbb{Z}$. Now, for all $k \in \mathbb{Z}$ we have

$$x \equiv 2 \bmod 5$$
$$\Leftrightarrow 4 + 8k \equiv 2 \bmod 5 \qquad \text{since } x = 4 + 8k$$
$$\Leftrightarrow 8k \equiv -2 \bmod 5 \qquad \text{subtracting } 4$$
$$\Leftrightarrow 3k \equiv 3 \bmod 5 \qquad \text{since } 8 \equiv -2 \equiv 3 \bmod 5$$
$$\Leftrightarrow k \equiv 1 \bmod 5 \qquad \text{multiplying by a multiplicative inverse for 3 modulo 5}$$

So $4 + 8k \equiv 2 \bmod 5$ if and only if $k = 1 + 5\ell$ for some $\ell \in \mathbb{Z}$.

Combining this, we see that x satisfies both congruences if and only if

$$x = 4 + 8(1 + 5\ell) = 12 + 40\ell$$

for some $\ell \in \mathbb{Z}$.

Hence the integers x for which both congruences are satisfied are precisely those integers x such that $x \equiv 12 \bmod 40$. ◁

Exercise 3.3.43

Find all integer solutions x to the system of congruences:

$$\begin{cases} x \equiv -1 \bmod 4 \\ x \equiv 1 \bmod 9 \\ x \equiv 5 \bmod 11 \end{cases}$$

Express your solution in the form $x \equiv a \bmod n$ for suitable $n > 0$ and $0 \leqslant a < n$. ◁

Exercise 3.3.44

Let m, n be coprime moduli and let $a, b \in \mathbb{Z}$. Let $u, v \in \mathbb{Z}$ be such that

$$mu \equiv 1 \bmod n \quad \text{and} \quad nv \equiv 1 \bmod m$$

In terms of a, b, m, n, u, v, find an integer x such that

$$x \equiv a \bmod m \quad \text{and} \quad x \equiv b \bmod n$$

◁

Exercise 3.3.45

Let m, n be coprime moduli and let $x, y \in \mathbb{Z}$. Prove that if $x \equiv y \bmod m$ and $x \equiv y \bmod n$, then $x \equiv y \bmod mn$. ◁

Theorem 3.3.46 (Chinese remainder theorem)

Let m, n be moduli and let $a, b \in \mathbb{Z}$. If m and n are coprime, then there exists an integer solution x to the simultaneous congruences

$$x \equiv a \bmod m \quad \text{and} \quad x \equiv b \bmod n$$

Moreover, if $x, y \in \mathbb{Z}$ are two such solutions, then $x \equiv y \bmod mn$.

Proof. Existence of a solution x is precisely the content of Exercise 3.3.44.

Now let $x, y \in \mathbb{Z}$ be two solutions to the two congruences. Then

$$\begin{cases} x \equiv a \bmod m \\ y \equiv a \bmod m \end{cases} \quad \Rightarrow \quad x \equiv y \bmod m$$

$$\begin{cases} x \equiv b \bmod n \\ y \equiv b \bmod n \end{cases} \quad \Rightarrow \quad x \equiv y \bmod n$$

so by Exercise 3.3.45, we have $x \equiv y \bmod mn$, as required. □

We now generalise the Chinese remainder theorem to the case when the moduli m, n are not assumed to be coprime. There are two ways we could make this generalisation: either we could reduce the more general version of the theorem to the version we proved in Theorem 3.3.46, or we could prove the more general version from scratch. We opt for the latter approach, but you might want to consider what a 'reductive' proof would look like.

Theorem 3.3.47

Let m, n be moduli and let $a, b \in \mathbb{Z}$. There exists an integer solution x to the system of congruences

$$x \equiv a \bmod m \quad \text{and} \quad x \equiv b \bmod n$$

if and only if $a \equiv b \bmod \gcd(m, n)$.
Moreover, if $x, y \in \mathbb{Z}$ are two such solutions, then $x \equiv y \bmod \operatorname{lcm}(m, n)$

Proof. Let $d = \gcd(m, n)$, and write $m = m'd$ and $n = n'd$ for some $m', n' \in \mathbb{Z}$.

We prove that an integer solution x to the system of congruences exists if and only if $a \equiv b \bmod d$.

- ($\Rightarrow$) Suppose an integer solution x to the system of congruences exists. Then there exist integers k, ℓ such that

$$x = a + mk = b + n\ell$$

  But $m = m'd$ and $n = n'd$, so we have $a + m'dk = b + n'd\ell$, and so

$$a - b = (n'\ell - m'k)d$$

  so that $a \equiv b \bmod d$, as required.

- ($\Leftarrow$) Suppose $a \equiv b \bmod d$, and let $t \in \mathbb{Z}$ be such that $a - b = td$. Let $u, v \in \mathbb{Z}$ be solutions to the congruence $mu + nv = d$, which exists by Bézout's lemma (Theorem 3.1.22). Note also that, since $m = m'd$ and $n = n'd$, dividing through by d yields $m'u + n'v = 1$.

  Define

$$x = an'v + bm'u$$

  Now we have

$$
\begin{aligned}
x &= an'v + bm'u && \text{by definition of } x \\
&= an'v + (a - td)m'u && \text{since } a - b = td \\
&= a(m'u + n'v) - tdm'u && \text{rearranging} \\
&= a - tdm'u && \text{since } m'u + n'v = 1 \\
&= a - tum && \text{since } m = m'd
\end{aligned}
$$

  so $x \equiv a \bmod m$. Likewise

$$
\begin{aligned}
x &= an'v + bm'u && \text{by definition of } x \\
&= (b + td)n'v + bm'u && \text{since } a - b = td \\
&= b(m'u + n'v) + tdn'v && \text{rearranging} \\
&= b + tdn'v && \text{since } m'u + n'v = 1 \\
&= b + tvn && \text{since } n = n'd
\end{aligned}
$$

  so $x \equiv b \bmod n$.

  Hence $x = an'v + bm'u$ is a solution to the system of congruences.

We now prove that if x, y are two integer solutions to the system of congruences, then they are congruent modulo $\mathrm{lcm}(a, b)$. First note that we must have

$$x \equiv y \bmod m \quad \text{and} \quad x \equiv y \bmod n$$

so that $x = y + km$ and $x = y + \ell n$ for some $k, \ell \in \mathbb{Z}$. But then

$$x - y = km = \ell n$$

Writing $m = m'd$ and $n = n'd$, we see that $km'd = \ell n'd$, so that $km' = \ell n'$. But m', n' are coprime by Proposition 3.1.29, and hence $m' \mid \ell$ by Proposition 3.1.32. Write $\ell = \ell'm'$ for some $\ell' \in \mathbb{Z}$. Then we have

$$x - y = \ell n = \ell'm'n$$

and hence $x \equiv y \bmod m'n$. But $m'n = \operatorname{lcm}(m, n)$ by Exercise 3.1.41. $\qquad \square$

This theorem is in fact *constructive*, in that it provides an algorithm for finding all integer solutions x to a system of congruences

$$x \equiv a \bmod m \quad \text{and} \quad x \equiv b \bmod n$$

as follows:

- Use the Euclidean algorithm to compute $d = \gcd(m, n)$.

- If $d \nmid a - b$ then there are no solutions, so stop. If $d \mid a - b$, then proceed to the next step.

- Use the extended Euclidean algorithm to compute $u, v \in \mathbb{Z}$ such that $mu + nv = d$.

- The integer solutions x to the system of congruences are precisely those of the form

$$x = \frac{anv + bmu + kmn}{d} \quad \text{for some } k \in \mathbb{Z}$$

Exercise 3.3.48
Verify that the algorithm outlined above is correct. Use it to compute the solutions to the system of congruences
$$x \equiv 3 \bmod 12 \quad \text{and} \quad x \equiv 15 \bmod 20$$

<div align="right">◁</div>

⊛Exercise 3.3.49
Generalise the Chinese remainder theorem to systems of arbitrarily (finitely) many congruences. That is, given $r \in \mathbb{N}$, find precisely the conditions on moduli $n_1, n_2, \ldots, n_r$ and integers $a_1, a_2, \ldots, a_r$ such that an integer solution exists to the congruences

$$x \equiv a_1 \bmod n_1, \quad x \equiv a_2 \bmod n_2, \quad \cdots \quad x_r \equiv a_r \bmod n_r$$

Find an explicit formula for such a value of x, and find a suitable modulus n in terms of $n_1, n_2, \ldots, n_r$ such that any two solutions to the system of congruences are congruent modulo n. ◁

Exercise 3.3.50
Prove that gaps between consecutive primes can be made arbitrarily large. That is, prove that for all $n \in \mathbb{N}$, there exists an integer a such that the numbers

$$a, \; a+1, \; a+2, \; \ldots, \; a+n$$

are all composite.   ◁

Application: tests for divisibility

The language of modular arithmetic provides a practical setting for proving tests for divisibility using number bases. Number bases were introduced in Section 1.1, and we gave a preliminary definition in Definition 1.1.6 of what a number base is. Our first job will be to justify why this definition makes sense at all—that is, we need to prove that every natural number *has* a base-b expansion, and moreover, that it only has one of them. Theorem 3.3.51 says exactly this.

Theorem 3.3.51
Let $n \in \mathbb{N}$ and let $b \in \mathbb{N}$ with $b \geqslant 2$. Then there exist unique $r \in \mathbb{N}$ and $d_0, d_1, \ldots, d_r \in \{0, 1, \ldots, b-1\}$ such that

$$n = \sum_{i=0}^{r} d_i b^i$$

and such that $d_r \neq 0$, except $n = 0$, in which case $r = 0$ and $d_0 = 0$.

Proof. We proceed by strong induction on n.

- (**BC**) We imposed the requirement that if $n = 0$ then $r = 0$ and $d_0 = 0$; and this evidently satisfies the requirement that $n = \sum_{i=0}^{r} d_i b^i$.

- (**IS**) Fix $n \geqslant 0$ and suppose that the requirements of the theorem are satisfied for all the natural numbers up to and including n.

  By the division theorem (Theorem 3.1.1), there exist unique $u, v \in \mathbb{N}$ such that

  $$n + 1 = ub + v \quad \text{and} \quad v \in \{0, 1, \ldots, b-1\}$$

  Since $b \geqslant 2$, we have $u < n+1$, and so $u \leqslant n$. It follows from the induction hypothesis that there exist unique $r \in \mathbb{N}$ and $d_1, \ldots, d_r \in \{0, 1, \ldots, b-1\}$ such that

  $$u = \sum_{i=0}^{r} d_{i+1} b^i$$

and $d_r \neq 0$. Writing $d_0 = v$ yields

$$n = ub + v = \sum_{i=0}^{r} d_{i+1} b^{i+1} + d_0 = \sum_{i=0}^{r} d_i b^i$$

Since $d_r \neq 0$, this proves existence.

For uniqueness, suppose that there exists $s \in \mathbb{N}$ and $e_0, \ldots, e_s \in \{0, 1, \ldots, b-1\}$ such that

$$n + 1 = \sum_{j=0}^{s} e_j b^j$$

and $e_s \neq 0$. Then

$$n + 1 = \left(\sum_{j=1}^{s} e_j b^{j-1} \right) b + e_0$$

so by the division theorem we have $e_0 = d_0 = v$. Hence

$$u = \frac{n + 1 - v}{b} = \sum_{j=1}^{s} e_j b^{j-1} = \sum_{i=1}^{r} d_i b^{j-1}$$

so by the induction hypothesis, it follows that $r = s$ and $d_i = e_i$ for all $1 \leqslant i \leqslant r$. This proves uniqueness.

By induction, we're done. $\qquad\square$

We now re-state the definition of base-b expansion, confident in the knowledge that this definition makes sense.

> **Definition 3.3.52**
> Let $n \in \mathbb{N}$. The **base-b expansion** of n is the unique string $d_r d_{r-1} \ldots d_0$ such that the conditions in Theorem 3.3.51 are satisfied. The base-2 expansion is also known as the **binary expansion**, and the base-10 expansion is called the **decimal expansion**.

Example 3.3.53
Let $n \in \mathbb{N}$. Then n is divisible by 3 if and only if the sum of the digits in the decimal expansion of n is divisible by 3. Likewise, n is divisible by 9 if and only if the sum of the digits in the decimal expansion n is divisible by 9.

We prove this for divisibility by 3. Let

$$n = d_r d_{r-1} \cdots d_1 d_0$$

be the decimal expansion of n, and let $s = \sum_{i=0}^{r} d_i$ be the sum of the digits of n.

Then we have

$$n \equiv \sum_{i=0}^{r} d_i 10^i \bmod 3 \qquad\qquad \text{since } n = \sum_{i} d_i 10^i$$

$$\equiv \sum_{i=0}^{r} d_i 1^i \bmod 3 \qquad\qquad \text{since } 10 \equiv 1 \bmod 3$$

$$\equiv \sum_{i=0}^{r} d_i \qquad\qquad\qquad \text{since } 1^i = 1 \text{ for all } i$$

$$\equiv s \qquad\qquad\qquad\qquad \text{by definition of } s$$

Since $n \equiv s \bmod 3$, it follows that n is divisible by 3 if and only if s is divisible by 3.   ◁

Exercise 3.3.54
Let $n \in \mathbb{N}$. Prove that n is divisible by 5 if and only if the final digit in the decimal expansion of n is 5 or 0.

More generally, fix $k \geqslant 1$ and let m be the number whose decimal expansion is given by the last k digits of that of n. Prove that n is divisible by 5^k if and only if m is divisible by 5^k. For example, we have

$$125 \mid 9\,550\,828\,230\,495\,875 \quad \Leftrightarrow \quad 125 \mid 875$$

◁

Exercise 3.3.55
Let $n \in \mathbb{N}$. Prove that n is divisible by 11 if and only if the *alternating sum* of the digits of n is divisible by 11. That is, prove that if the decimal expansion of n is $d_r d_{r-2} \cdots d_0$, then

$$11 \mid n \quad \Leftrightarrow \quad 11 \mid d_0 - d_1 + d_2 - \cdots + (-1)^r d_r$$

◁

Exercise 3.3.56
Let $n \in \mathbb{N}$. Find a method for testing if n is divisible by 7 based on the decimal expansion of n.   ◁

Application: public-key cryptography

Public-key cryptography is a method of encryption and decryption that works according to the following principles:

- Encryption is done using a *public key* that is available to anyone.

- Decryption is done using a *private key* that is only known to the recipient.

- Knowledge of the private key should be extremely difficult to derive from knowledge of the public key.

Specifically, suppose that Alice wants to securely send Bob a message. As the recipient of the message, Bob has a public key and a private key. So:

- Bob sends the *public key* to Alice.

- Alice uses the public key to encrypt the message.

- Alice sends the encrypted message, which is visible (but encrypted) to anyone who intercepts it.

- Bob keeps the private key secret, and uses it upon receipt of the message to decrypt the message.

Notice that, since the public key can only be used to *encrypt* messages, a hacker has no useful information upon intercepting the message or the public key.

RSA encryption is an algorithm which provides one means of doing public-key cryptography using the theory of modular arithmetic. It works as follows.

Step 1. Let p and q be distinct positive prime numbers, and let $n = pq$. Then $\varphi(n) = (p-1)(q-1)$.

Step 2. Choose $e \in \mathbb{Z}$ with $1 < e < \varphi(n)$ and $e \perp \varphi(n)$. The pair (n, e) is called the **public key**.

Step 3. Choose $d \in \mathbb{Z}$ with $de \equiv 1 \bmod \varphi(n)$. The pair (n, d) is called the **private key**.

Step 4. To encrypt a message M (which is encoded as an integer), compute $K \in [n]$ such that $K \equiv M^e \bmod n$. Then K is the encrypted message.

Step 5. The original message M can be recovered since $M \equiv K^d \bmod n$.

Computing the private key (n, d) from the knowledge of (n, e) would allow a hacker to decrypt an encrypted message. However, doing so is typically very difficult when the prime factors of n are large. So if we choose p and q to be very large primes—which we can

do without much hassle at all—then it becomes computationally infeasible for a hacker to compute the private key.

Example. Suppose I want to encrypt the message M, which I have encoded as the integer 32. Let $p = 13$ and $q = 17$. Then $n = 221$ and $\varphi(n) = 192$. Let $e = 7$, and note that $7 \perp 192$. Now $7 \times 55 \equiv 1 \bmod 192$, so we can define $d = 55$.

- The public key is $(221, 7)$, which Bob sends to Alice. Now Alice can encrypt the message:

$$32^7 \equiv 59 \bmod 221$$

  Alice then sends Bob the encrypted message 59.

- The private key is $(221, 55)$, so Bob can decrypt the message:

$$59^{55} \equiv 32 \bmod 221$$

  so Bob has received Alice's message 32.

Exercise 3.3.57
Prove that the RSA algorithm is correct. Specifically, prove:

(a) If $n = pq$, for distinct positive primes p and q, then $\varphi(n) = (p-1)(q-1)$;

(b) Given $1 < e < \varphi(n)$ with $e \perp \varphi(n)$, there exists $d \in \mathbb{Z}$ with $de \equiv 1 \bmod \varphi(n)$.

(c) Given $M, K \in \mathbb{Z}$ with $K \equiv M^e \bmod n$, it is indeed the case that $K^d \equiv M \bmod n$.

◁

Chapter 4

Finite and infinite sets

4.1   Functions revisited

To motivate some of the definitions to come, look at the dots (•) and stars (⋆) below. Are there more dots or more stars?

• • • • • • • • • • • • • • • • • • • •

⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆ ⋆
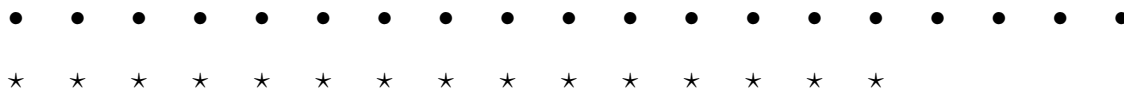
Pause for a second and think about how you knew the answer to this question.

Indeed, there are more dots than stars. There are a couple of ways to arrive at this conclusion:

 (i) You could count the number of dots, count the number of stars, and then compare the two numbers; or

 (ii) You could notice that the dots and the stars are evenly spaced, but that the line of dots is longer than the line of stars.

It is likely that you chose method (ii). In fact, it is likely that you haven't even counted the number of dots or the number of stars yet—and you don't need to! We can conclude that there are more dots than stars by simply pairing up dots with stars—we eventually run out of stars, and there are still dots left over, so there must have been more dots than stars.

Injectivity

One way of formalising this act of pairing up stars with dots mathematically is to define a function $f : S \to D$ from the set S of stars to the set D of dots, where the value of f at each star is the dot that it is paired with. We of course must do this in such a way that each dot is paired with at most one star:
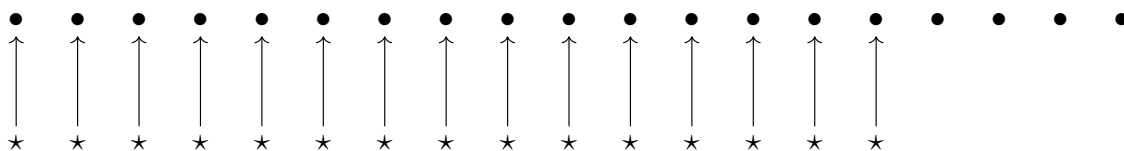
It is a property of this function—called *injectivity*—that allows us to deduce that there are more dots than stars.

Intuitively, a function $f : X \to Y$ is injective if it puts the elements of X in one-to-one correspondence[a] with the elements of a subset of Y—just like how the stars are in one-to-one correspondence with a subset of the dots in the example above.

Definition 4.1.1
A function $f : X \to Y$ is **injective** (or **one-to-one**) if

$$f(x) = f(x') \ \Rightarrow \ x = x' \quad \text{for all } x, x' \in X$$

An injective function is said to be an **injection**.

Proof tip
The definition of injectivity makes it easy to see how to prove that a function $f : X \to Y$ is injective: let $x, x' \in X$, assume that $f(x) = f(x')$, then derive $x = x'$. ◁

By contraposition, $f : X \to Y$ being injective is equivalent to saying that if $x, x' \in X$ and $x \neq x'$, then $f(x) \neq f(x')$.

The following is a very simple example from elementary arithmetic:

Example 4.1.2
Define $f : \mathbb{Z} \to \mathbb{Z}$ by letting $f(x) = 2x + 1$ for all $x \in \mathbb{Z}$. We'll prove that f is injective. Fix $x, x' \in \mathbb{Z}$, and assume that $f(x) = f(x')$. By definition of f, we have $2x + 1 = 2x' + 1$. Subtracting 1 yields $2x = 2x'$, and dividing by 2 yields $x = x'$. Hence f is injective. ◁

The following example is slightly more sophisticated.

Proposition 4.1.3
Let $f : X \to Y$ and $g : Y \to Z$ be functions. If f and g are injective, then $g \circ f$ is injective.

Proof. Let $x, x' \in X$. We need to prove that

$$(g \circ f)(x) = (g \circ f)(x') \quad \Rightarrow \quad x = x'$$

So assume $(g \circ f)(x) = (g \circ f)(x')$. By definition of function composition, this implies that $g(f(x)) = g(f(x'))$. By injectivity of g, we have $f(x) = f(x')$; and by injectivity of f, we have $x = x'$. □

---

[a] In fact, some authors use the term 'one-to-one' to mean 'injective'.

Exercise 4.1.4

Let $f : X \to Y$ and $g : Y \to Z$ be functions. Prove that if $g \circ f$ is injective, then f is injective. ◁

Exercise 4.1.5

Write out what it means to say a function $f : X \to Y$ is *not* injective, and say how you would prove that a given function is not injective. Give an example of a function which is not injective, and use your proof technique to write a proof that it is not injective. ◁

Exercise 4.1.6

For each of the following functions, determine whether it is injective or not injective.

- $f : \mathbb{N} \to \mathbb{Z}$, defined by $f(n) = n^2$ for all $n \in \mathbb{N}$.

- $g : \mathbb{Z} \to \mathbb{N}$, defined by $g(n) = n^2$ for all $n \in \mathbb{Z}$.

- $h : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, defined by $h(x, y, z) = 2^x \cdot 3^y \cdot 5^z$ for all $x, y, z \in \mathbb{N}$.

◁

Surjectivity

Let's revisit the rows of dots and stars that we saw earlier. Beforehand, we made our idea that there are more dots than stars formal by proving the existence of an injection $f : S \to D$ from the set S of stars to the set D of dots.

However, we could have drawn the same conclusion instead from defining a function $D \to S$, which in some sense *covers* the stars with dots—that is, every star is paired up with at least one dot.
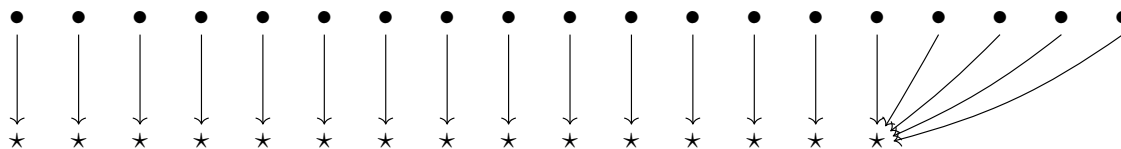
This property is called *surjectivity*—a function $f : X \to Y$ is surjective if every element of Y is a value of f. This is made precise in Definition 4.1.7.

> **Definition 4.1.7**
> A function $f : X \to Y$ is **surjective** (or **onto**) if
> $$\forall y \in Y, \ \exists x \in X, \ f(x) = y$$
> A surjective function is said to be a **surjection**.

Proof tip

To prove that a function $f : X \to Y$ is surjective, prove that each element $y \in Y$ is a value of f. That is, fix $y \in Y$, and demonstrate that there exist some $x \in X$ such that $f(x) = y$. ◁

Example 4.1.8

Fix $n \in \mathbb{N}$ with $n > 0$, and define a function function $r : \mathbb{Z} \to \{0, 1, \ldots, n - 1\}$ by letting $r(a)$ be the remainder of a when divided by n. This function is surjective, since for each $k \in \{0, 1, \ldots, n - 1\}$ we have $r(k) = k$. ◁

Exercise 4.1.9

For each of the following pairs of sets (X, Y), determine whether the function $f : X \to Y$ defined by $f(x) = 2x + 1$ is surjective.

(a) $X = \mathbb{Z}$ and $Y = \{x \in \mathbb{Z} \mid x \text{ is odd}\}$;

(b) $X = \mathbb{Z}$ and $Y = \mathbb{Z}$;

(c) $X = \mathbb{Q}$ and $Y = \mathbb{Q}$;

(d) $X = \mathbb{R}$ and $Y = \mathbb{R}$.

◁

Exercise 4.1.10

Let $f : X \to Y$ be a function. Find a subset $V \subseteq Y$ and a surjection $g : X \to V$ agreeing with f (that is, such that $g(x) = f(x)$ for all $x \in X$). ◁

Exercise 4.1.11

Let $f : X \to Y$ be a function. Prove that f is surjective if and only if $Y = f[X]$ ◁

Exercise 4.1.12

Let $f : X \to Y$ be a function. Prove that there is a set Z and functions

$$p : X \to Z \quad \text{and} \quad i : Z \to Y$$

such that p is surjective, i is injective, and $f = i \circ p$. ◁

Bijectivity

Bijective functions formalise the idea of putting sets into one-to-one correspondence—each element of one set is paired with exactly one element of another.

Definition 4.1.13
A function $f : X \to Y$ is **bijective** if it is injective and surjective. A bijective function is said to be a **bijection**.

Proof tip
To prove that a function f is bijective, prove that it is injective and surjective. ◁

Example 4.1.14
Let $D \subseteq \mathbb{Q}$ be the set of *dyadic rational numbers*, that is

$$D = \left\{ x \in \mathbb{Q} \;\middle|\; x = \frac{a}{2^n} \text{ for some } a \in \mathbb{Z} \text{ and } n \in \mathbb{N} \right\}$$

Let $k \in \mathbb{N}$, and define $f : \mathbb{D} \to \mathbb{D}$ by $f(x) = \frac{x}{2^k}$. We will prove that f is a bijection.

- (**Injectivity**) Fix $x, y \in D$ and suppose that $f(x) = f(y)$. Then $\frac{x}{2^k} = \frac{y}{2^k}$, so that $x = y$, as required.

- (**Surjectivity**) Fix $y \in D$. We need to find $x \in D$ such that $f(x) = y$. Well certainly if $2^k y \in D$ then we have

$$f(2^k y) = \frac{2^k y}{2^k} = y$$

  so it suffices to prove that $2^k y \in D$. Since $y \in D$, we must have $y = \frac{a}{2^n}$ for some $n \in \mathbb{N}$.

  ◇ If $k \leqslant n$ then $n - k \in \mathbb{N}$ and so $2^k y = \frac{a}{2^{n-k}} \in D$.

  ◇ If $k > n$ then $k - n > 0$ and $2^k y = 2^{k-n} a \in \mathbb{Z}$; but $\mathbb{Z} \subseteq D$ since if $a \in \mathbb{Z}$ then $a = \frac{a}{2^0}$. So again we have $2^k y \in D$.

  In any case we have $2^k y \in D$ and $f(2^k y) = y$, so that f is surjective.

Since f is both injective and surjective, it is bijective. ◁

Exercise 4.1.15
Let X be a set. Prove that the identity function $\mathrm{id}_X : X \to X$ is a bijection. ◁

Exercise 4.1.16
Let $m, n \in \mathbb{N}$. Find a bijection $[m] \times [n] \to [mn]$. ◁

Exercise 4.1.17

Let $f : X \to Y$ and $g : Y \to Z$ be bijections. Prove that $g \circ f$ is a bijection. ◁

We will soon see a way to characterise injections, surjections and bijections in terms of other functions, called *inverses*. Before we do that, though, we will make precise our intuition that an injection $X \to Y$ tells us that X has at most as many elements as Y, that a surjection $X \to Y$ tells us that X has at least as many elements as Y, and that a bijection $X \to Y$ tells us that X has exactly as many elements as Y.

Inverses

Recall Definition 4.1.1, which says that a function $f : X \to Y$ is injective if, for all $x, x' \in X$, if $f(x) = f(x')$ then $x = x'$.

Exercise 4.1.18

Let $f : X \to Y$ be a function. Prove that f is injective if and only if

$$\forall y \in f[X], \exists! x \in X, y = f(x)$$

◁

Thinking back to Section 2.3, you might notice that this means that the logical formula '$y = f(x)$' defines a function $f[X] \to X$—specifically, if f is injective then there is a function $g : f[X] \to X$ which is (well-)defined by the equation $x = g(f(x))$. Thinking of f as an *encoding* function, we then have that g is the corresponding *decoding* function—decoding is possible by injectivity of f. (If f were not injective then distinct elements of X might have the same encoding, in which case we're stuck if we try to decode them!)

Exercise 4.1.19

Define a function $e : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $e(m, n) = 2^m \cdot 3^n$. Prove that e is injective. We can think of e as encoding *pairs* of natural numbers as single natural numbers—for example, the pair $(4, 1)$ is encoded as $2^4 \cdot 3^1 = 48$. For each of the following natural numbers k, find the pairs of natural numbers encoded by e as k:

$$1 \qquad 24 \qquad 7776 \qquad 59049 \qquad 396718580736$$

◁

In Exercise 4.1.19, we were able to decode any natural number of the form $2^m \cdot 3^n$ for $m, n \in \mathbb{N}$. This process of decoding yields a function

$$d : \{k \in \mathbb{N} \mid k = 2^m \cdot 3^n \text{ for some } m, n \in \mathbb{N}\} \to \mathbb{N} \times \mathbb{N}$$

What would happen if we tried to decode a natural number not of the form $2^m \cdot 3^n$ for $m, n \in \mathbb{N}$, say 5 or 100? Well... it doesn't really matter! All we need to be true is that $d(e(m,n)) = (m,n)$ for all $(m,n) \in \mathbb{N} \times \mathbb{N}$; the value of d on other natural numbers is irrelevant.

Definition 4.1.20

Let $f : X \to Y$ be a function. A **left inverse** (or **post-inverse**) for f is a function $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$.

Example 4.1.21

Let $e : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be as in Exercise 4.1.19. Define a function $d : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ by

$$d(k) = \begin{cases} (m,n) & \text{if } k = 2^m \cdot 3^n \text{ for some } m, n \in \mathbb{N} \\ (0,0) & \text{otherwise} \end{cases}$$

Note that d is well-defined by the fundamental theorem of arithmetic (Theorem 3.2.12). Moreover, given $m, n \in \mathbb{N}$, we have

$$d(e(m,n)) = d(2^m \cdot 3^n) = (m,n)$$

and so d is a left inverse for e.   ◁

Exercise 4.1.22

Let $f : X \to Y$ be a function with $X \neq \varnothing$. Prove that f is injective if and only if f has a left inverse.   ◁

What about surjections? Definition 4.1.7 said that a function $f : X \to Y$ is surjective if

$$\forall y \in Y, \exists x \in X, f(x) = y$$

This isn't quite of the form $\forall y \in Y, \exists! x \in X, p(y,x)$—we assume a value of x making '$f(x) = y$' true *exists*, but we don't assume that it is *unique*. However, we can be cunning[b]—just make an arbitrary (but fixed) choice amongst the y values that work!

Definition 4.1.23

Let $f : X \to Y$ be a function. A **right inverse** (or **pre-inverse**) for f is a function $g : Y \to X$ such that $f \circ g = \mathrm{id}_Y$.

Example 4.1.24

Define $f : \mathbb{R} \to \mathbb{R}^{\geq 0}$ by $f(x) = x^2$. Note that f is surjective, since for each $y \in \mathbb{R}^{\geq 0}$ we have $\sqrt{y} \in \mathbb{R}$ and $f(\sqrt{y}) = y$. However f is not injective; for instance

$$f(-1) = 1 = f(1)$$

Here are three right inverses for f:

---

[b] We can only be cunning if we accept the *axiom of choice*—see Appendix B.2 for more details!

- The positive square root function $g : \mathbb{R}^{\geqslant 0} \to \mathbb{R}$ defined by $g(y) = \sqrt{y}$ for all $y \in \mathbb{R}^{\geqslant 0}$. Indeed, for each $y \in \mathbb{R}^{\geqslant 0}$ we have

$$f(g(y)) = f(\sqrt{y}) = (\sqrt{y})^2 = y$$

- The negative square root function $h : \mathbb{R}^{\geqslant 0} \to \mathbb{R}$ defined by $h(y) = -\sqrt{y}$ for all $y \in \mathbb{R}^{\geqslant 0}$. Indeed, for each $y \in \mathbb{R}^{\geqslant 0}$ we have

$$f(h(y)) = f(-\sqrt{y}) = (-\sqrt{y})^2 = y$$

- The function $k : \mathbb{R}^{\geqslant 0} \to \mathbb{R}$ defined by

$$k(y) = \begin{cases} \sqrt{y} & \text{if } 2n \leqslant y < 2n + 1 \text{ for some } n \in \mathbb{N} \\ -\sqrt{y} & \text{otherwise} \end{cases}$$

Note that k is well-defined, and again $f(k(y)) = y$ for all $y \in \mathbb{R}^{\geqslant 0}$ since no matter what value $k(y)$ takes, it is equal to either $\sqrt{y}$ or $-\sqrt{y}$.

There are many more right inverses for f—in fact, there are infinitely many more! ◁

Exercise 4.1.25
Prove that a function $f : X \to Y$ is surjective if and only if it has a right inverse. ◁

Exercises 4.1.22 and 4.1.25 establish that a function $f : X \to Y$ is...

- *injective* if and only if it has a *left inverse* (provided X is inhabited);

- *surjective* if and only if it has a *right inverse*.

It seems logical that we might be able to classify bijections as being those functions which have a left inverse and a right inverse. We can actually say something stronger—the left and right inverse can be taken to be the same function! (In fact, Proposition 4.1.30 establishes that they are necessarily the same function.)

Definition 4.1.26
Let $f : X \to Y$ be a function. A (**two-sided**) **inverse** for f is a function $g : Y \to X$ which is both a left inverse and a right inverse for f.

It is customary to simply say 'inverse' rather than 'two-sided inverse'.

Example 4.1.27

Let D be the set of dyadic rational numbers, as defined in Example 4.1.14. There, we defined a function $f : D \to D$ defined by $f(x) = \frac{x}{2^k}$ for all $x \in D$, where k is some fixed natural number. We find an inverse for f.

Define $g : D \to D$ by $g(x) = 2^k x$. Then

- g is a left inverse for f. To see this, note that for all $x \in D$ we have

$$g(f(x)) = g(\frac{x}{2^k}) = 2^k \cdot \frac{x}{2^k} = x$$

- g is a right inverse for f. To see this, note that for all $y \in D$ we have

$$f(g(y)) = f(2^k y) = \frac{2^k y}{2^k} = y$$

Since g is a left inverse for f and a right inverse for f, it is a two-sided inverse for f.   ◁

Exercise 4.1.28

The following functions have two-sided inverses. For each, find its inverse and prove that it is indeed an inverse.

(a) $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \frac{2x+1}{3}$.

(b) $g : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ defined by $g(X) = \mathbb{N} \setminus X$.

(c) $h : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $h(m, n) = 2^m(2n + 1) - 1$ for all $m, n \in \mathbb{N}$.

                                                                                                ◁

Exercises 4.1.22 and 4.1.25 can be pieced together to prove the following result.

Exercise 4.1.29

Let $f : X \to Y$ be a function. Prove that f is bijective if and only if f has an inverse.   ◁

Common error

When proving a function $f : X \to Y$ is bijective by finding an inverse $g : Y \to X$, it is important to check that g is *both* a left inverse *and* a right inverse for f. If you only prove that g is a left inverse for f, for example, then you have only proved that f is injective!   ◁

As indicated above, if a function has both a left and a right inverse, then they must be equal.

Proposition 4.1.30

Let $f : X \to Y$ be a function and suppose $\ell : Y \to X$ is a left inverse for f and $r : Y \to X$ is a right inverse for f. Then $\ell = r$.

Proof. The proof is deceptively simple:

$$\begin{aligned}
\ell &= \ell \circ \mathrm{id}_Y && \text{by definition of identity functions} \\
&= \ell \circ (f \circ r) && \text{since } r \text{ is a right inverse for } f \\
&= (\ell \circ f) \circ r && \text{by Exercise 2.3.27} \\
&= \mathrm{id}_X \circ r && \text{since } \ell \text{ is a left inverse for } f \\
&= r && \text{by definition of identity functions}
\end{aligned}$$

$\square$

It follows from Proposition 4.1.30 that, for any function $f : X \to Y$, any two inverses for f are equal—that is, every bijective function has a *unique* inverse!

Notation 4.1.31

Let $f : X \to Y$ be a function. Write $f^{-1} : Y \to X$ to denote the (unique) inverse for f, if it exists.

Proposition 4.1.32

Let $f : X \to Y$ be a bijection. A function $g : Y \to X$ is a left inverse for f if and only if it is a right inverse for f.

Proof. We will prove the two directions separately.

- ($\Rightarrow$) Suppose $g : Y \to X$ is a left inverse for f—that is, $g(f(x)) = x$ for all $x \in X$. We prove that $f(g(y)) = y$ for all $y \in Y$, thus establishing that g is a right inverse for f. So let $y \in Y$. Since f is a bijection, it is in particular a surjection, so there exists $x \in X$ such that $y = f(x)$. But then

$$\begin{aligned}
f(g(y)) &= f(g(f(x))) && \text{since } y = f(x) \\
&= f(x) && \text{since } g(f(x)) = x \\
&= y && \text{since } y = f(x)
\end{aligned}$$

So indeed g is a right inverse for f.

- ($\Leftarrow$) Suppose $g : Y \to X$ is a right inverse for f—that is, $f(g(y)) = y$ for all $y \in Y$. We prove that $g(f(x)) = x$ for all $x \in X$, thus establishing that g is a left inverse for

f. So let $x \in X$. Letting $y = f(x)$, we have $f(g(y)) = y$ since g is a right inverse for f. This says precisely that $f(g(f(x))) = f(x)$, since $y = f(x)$. By injectivity of f, we have $g(f(x)) = x$, as required.

$\square$

Exercise 4.1.33
Let $f : X \to Y$ be a bijection. Prove that $f^{-1} : Y \to X$ is a bijection. ◁

Exercise 4.1.34
Let $f : X \to Y$ and $g : Y \to Z$ be bijections. Prove that $g \circ f : X \to Z$ is a bijection, and write an expression for its inverse in terms of f^{-1} and g^{-1}. ◁

First look at counting

We'll very soon (Section 4.2) make heavy use of functions to count the number of elements of a finite set. Before we do that, let's look at how injections, surjections and bijections can be used to compare sizes of particular finite sets—namely, those of the form $[n]$ for $n \in \mathbb{N}$, as defined in Definition 2.2.31.

When we used dots and stars to motivate the definitions of injective and surjective functions, we suggested the following intuition:

- If there is an injection $f : X \to Y$, then X has 'at most as many elements as Y'; and

- If there is a surjection $g : X \to Y$, then X has 'at least as many elements as Y'.

Let's make this intuition formal in the case when X and Y are sets of the form $[n]$ for $n \in \mathbb{N}$.

Theorem 4.1.35
Let $m, n \in \mathbb{N}$.

(a) If there exists an injection $f : [m] \to [n]$, then $m \leqslant n$.

(b) If there exists a surjection $g : [m] \to [n]$, then $m \geqslant n$.

(c) If there exists a bijection $h : [m] \to [n]$, then $m = n$.

Let's think about how we might prove part (a); part (b) is left as an exercise, and part (c) follows immediately from (a), (b) and the definition of a bijection. The intuition behind

(a) is clear: if we can pair up the natural numbers from 1 up to m with a subset of the numbers from 1 up to n, then n should be at least as large as m.

Our hypothesis is that an injection $f : [m] \to [n]$ *exists*—but, unfortunately for us, we have no control over what values this function takes. If it were as simple as $f(k) = k$ for all $k \in [m]$, then this would be an incredibly easy result to prove. But it might be the case that, say, $f(1) = 3$, and $f(2) = 5$, and $f(3) = 2$, and $f(4) = 1$, and so on.

Since we're working with natural numbers (m and n), let's use the canonical technique for proving results about natural numbers—induction! We'll proceed by induction on n, but you could think about how you might prove the claim by induction on m.

Proof of Theorem 4.1.35(a). We'll prove the following statement by induction on $n \in \mathbb{N}$:

> For all $m \in \mathbb{N}$, if there exists an injection $f : [m] \to [n]$, then $m \leqslant n$.

- (**Base case**) Fix $m \in \mathbb{N}$ and suppose there exists an injection $f : [m] \to [0]$. We need to prove that $m \leqslant 0$, or equivalently that $m = 0$, since m can't be negative.

  Well, if $m \geqslant 1$, then $1 \in [m]$, and so $f(1) \in [0]$. But $[0] = \varnothing$, so this would imply that the empty set has an element, which is nonsense. So $m < 1$, and hence $m = 0$.

- (**Induction step**) Fix $n \in \mathbb{N}$ and suppose that, for all $m \in \mathbb{N}$, if there exists an injection $f : [m] \to [n]$, then $m \leqslant n$. This assumption is our induction hypothesis.

  Now fix $m \in \mathbb{N}$ and suppose there is an injection $f : [m] \to [n+1]$. We need to prove that $m \leqslant n + 1$.

  We can use our induction hypothesis to prove that things are $\leqslant n$, so we need to prove $m - 1 \leqslant n$. But the number to the left-hand side of the $\leqslant$ symbol must be a natural number—so let's consider the case when $m = 0$ separately. Well, if $m = 0$ then $0 \leqslant n + 1$. (That was easy!) So let's now assume that $m \geqslant 1$, so that $m - 1 \in \mathbb{N}$.

  In order to use the induction hypothesis to prove $m - 1 \leqslant n$, we need to find an injection $[m - 1] \to [n]$. We're given an injection $f : [m] \to [n + 1]$, so let's use this to construct an injection $g : [m - 1] \to [n]$. There are two cases to consider:

  ◇ Suppose $f(k) \neq n + 1$ for all $k \in [m - 1]$. Then we can define $g : [m - 1] \to [n]$ by $g(k) = f(k)$ for all $k \in [m - 1]$. Injectivity of g then follows immediately from injectivity of f: indeed, given $k, \ell \in [m - 1]$, we have

  $$g(k) = g(\ell) \quad \Rightarrow \quad f(k) = f(\ell) \quad \Rightarrow \quad k = \ell$$

  where the second implication follows from injectivity of f.

⋄ Suppose $f(r) = n + 1$ for some $r \in [m-1]$. Since f is injective, we have $f(k) \neq n + 1$ for all $k \neq r$; in particular, $f(m) \neq n + 1$. We'll define $g : [m-1] \to [n]$ to be the same as f, except it exchanges the values at r and at m. This ensures that $g(k) \in [n]$ for all $k \in [m-1]$. Specifically, for $k \in [m-1]$, define

$$g(k) = \begin{cases} f(k) & \text{if } k \neq r \\ f(m) & \text{if } k = r \end{cases}$$

We just noted that g defines a function $[m-1] \to [n]$. Now let's prove that g is injective.

Fix $k, \ell \in [m-1]$ and suppose $g(k) = g(\ell)$. We'll split into some cases and prove that $k = \ell$ in each case:

* Suppose $k \neq r$ and $\ell \neq r$. Then $g(k) = f(k)$ and $g(\ell) = f(\ell)$, so $f(k) = f(\ell)$ and $k = \ell$ by injectivity of f.
* Suppose $k = r$ or $\ell = r$. (We may in fact assume $k = r$, otherwise swap the roles of k and ℓ in what follows.) Then $g(k) = g(r) = f(m)$ by definition of g. Moreover, we know that $g(\ell) = f(t)$ for some $t \in [m]$ and, by definition of g, we must have $t = \ell$ (if $t \neq r$) or $t = m$. But then $f(t) = f(m)$, so $t = m$ by injectivity of f, so $\ell = r = k$.

Either way, we have $k = \ell$. So g is injective. Now that we've proved that there exists an injective function $g : [m-1] \to [n]$, it follows from the induction hypothesis that $m - 1 \leqslant n$, and so $m \leqslant n + 1$ as required.

This completes the inductive step, so the theorem is proved. □

Exercise 4.1.36
Prove part (b) of Theorem 4.1.35.   ◁

Exercise 4.1.37
Let $m, n \in \mathbb{N}$ with $m \leqslant n$. Does there exist an injection $[m] \to [n]$? Does there exist a surjection $[n] \to [m]$? Prove your answers.   ◁

Proposition 4.1.35 showed us that we can compare natural numbers m and n by determining if there is an injection, surjection or bijection $[m] \to [n]$. We can use this result, together with our intuition, to motivate the definition of what it is for a set to be *finite*. Intuitively, a set is finite if we can label its elements using the elements of $[n]$ for some $n \in \mathbb{N}$. This labelling process can be formalised using bijections. Exercise 4.1.38 shows that this n is unique.

Exercise 4.1.38
Let X be a set and let $m, n \in \mathbb{N}$. Prove that, if there exist bijections $f : [m] \to X$ and $g : [n] \to X$, then $m = n$.   ◁

> **Definition 4.1.39**
> A set X is **finite** if there is a bijection $[n] \to X$ for some $n \in \mathbb{N}$, called the **size** of X. Write $|X|$ for the size of X. If X is not finite we say it is **infinite**.

In more intuitive terms: a set X is finite if the number of elements of X is a natural number; the size X is simply the number of elements of X.

Example 4.1.40
Let $X = \{\text{cat}, \text{dog}, \text{rabbit}, \text{horse}, \text{sheep}\}$. Then $|X| = 5$. To see this, define $f : [5] \to X$ by

$$f(1) = \text{cat}, \quad f(2) = \text{dog}, \quad f(3) = \text{rabbit}, \quad f(4) = \text{horse}, \quad f(5) = \text{sheep}$$

Then f is a bijection, as can easily be checked by noting that the function $g : X \to 5$ defined by

$$g(\text{cat}) = 1, \quad g(\text{dog}) = 2, \quad g(\text{rabbit}) = 3, \quad g(\text{horse}) = 4, \quad g(\text{sheep}) = 5$$

is an inverse for f. ◁

Example 4.1.41
For each $n \in \mathbb{N}$ the set $[n]$ is finite, and $|[n]| = n$. This is because the identity function $\text{id}_{[n]} : [n] \to [n]$ is a bijection. ◁

Exercise 4.1.42
Let X be a finite set with $|X| = n > 1$. Let $x \in X$ and let $y \notin X$. Prove that

$$|X \setminus \{x\}| = n - 1 \quad \text{and} \quad |X \cup \{y\}| = n + 1$$

Demonstrate that the hypotheses that $x \in X$ and $y \notin X$ are necessary—in other words, find a set X with $|X| = n > 1$ and elements x, y such that $|X \setminus \{x\}| \neq n - 1$ and $|X \cup \{y\}| \neq n + 1$. ◁

The following exercise is straightforward to prove, but is extremely powerful. We will make heavy use of it in Section 4.2, where it can be used to prove combinatorial identities.

Exercise 4.1.43
Let X and Y be finite sets. Prove that if there exists a bijection $h : X \to Y$, then $|X| = |Y|$. ◁

We conclude this section by proving that not all sets are finite—specifically, we'll prove that $\mathbb{N}$ is infinite. *Intuitively* this seems extremely easy: of *course* $\mathbb{N}$ is infinite! But in mathematical practice, this isn't good enough: we need to use our definition of 'infinite' to prove that $\mathbb{N}$ is infinite. Namely, we need to prove that there is no bijection $[n] \to \mathbb{N}$ for any $n \in \mathbb{N}$. We will use Lemma 4.1.44 below in our proof.

Lemma 4.1.44

Every inhabited finite set of natural numbers has a greatest element.

Proof. We'll prove by induction on $n \geqslant 1$ that, for all sets X with $|X| = n$, X has a greatest element.

- (**BC**) Fix a set X with $|X| = 1$. then $X = \{x\}$ for some $x \in \mathbb{N}$. Since x is the only element of X, it is certainly the greatest element!

- (**IS**) Let $n \in \mathbb{N}$ and suppose that every set of natural numbers of size n has a greatest element (**IH**).

  Let $X = \{x_1, x_2, \ldots, x_n, x_{n+1}\}$ be a set with $n + 1$ elements. We wish to show that X has a greatest element.

  To do this, let $Y = X \setminus \{x_{n+1}\}$. Then $|Y| = n$, so by (**IH**) it has a greatest element, say x_i. If $x_i > x_{n+1}$ then x_i is the greatest element of X; otherwise, x_{n+1} is the greatest element of X. In either case, X has a greatest element.

By induction, we're done. $\square$

Theorem 4.1.45

The set $\mathbb{N}$ is infinite.

Proof. We proceed by contradiction. Suppose $\mathbb{N}$ is finite. Then $|\mathbb{N}| = n$ for some $n \in \mathbb{N}$, and hence $\mathbb{N}$ is either empty (nonsense) or, by Lemma 4.1.44, it has a greatest element g. But $g + 1 \in \mathbb{N}$ since every natural number has a successor, contradicting maximality of g. Hence $\mathbb{N}$ is infinite. $\square$

4.2   Counting principles

Recall from Definition 4.1.39 that a set X is *finite* if there is a bijection $[n] \to X$ for some $n \in \mathbb{N}$; moreover, this n is unique, and is called the *size* of X, which we denote by $|X|$.

The main portion of this section focuses on the problem of computing $|X|$ given a description of X. The field of mathematics that concerns itself with this problem is called *enumerative combinatorics*.

The next few results allow us to deduce that subsets, binary intersections, binary unions and binary products of finite sets are finite.

Proposition 4.2.1

Let $i : U \to X$ be an injection. If X is finite, then U is finite, and moreover $|U| \leqslant |X|$.

Proof. We prove by induction on n that, for all finite sets X of size n, and all injections $i : U \to X$, the set U is finite and $|U| \leqslant n$.

- (**BC**) Suppose $|X| = 0$. Then $X = \varnothing$. The only function whose codomain is the empty set is the empty function $\varnothing \to \varnothing$; in other words, if $i : U \to \varnothing$ is an injection, then $U = \varnothing$. Hence U is finite and $|U| = 0 \leqslant 0$ as required.

- (**IS**) Fix $n \geqslant 0$ and suppose that, for any set Y with $|Y| = n$, and any injection $j : V \to Y$, we have V finite and $|V| \leqslant n$.

  Let X be a set with $|X| = n + 1$, and let $f : [n + 1] \to X$ be a bijection.

  Fix an injection $i : U \to X$. For simplicity of notation, write $X' = X \setminus \{f(n + 1)\}$. Note that $|X'| = n$ by Exercise 4.1.42.

  We split into cases based on whether or not $f(n + 1) \in i[U]$.

  $\diamond$ If $f(n+1) \notin i[U]$, then there is a function $i' : U \to X'$ defined by $i'(x) = i(x)$ for all $x \in U$. Moreover, this function is injective, since if $x, y \in U$ and $i'(x) = i'(y)$, then $i(x) = i(y)$ by definition of i', and so $x = y$ by injectivity of i. Moreover $|X'| = n$, so the induction hypothesis applies to the injection $i' : U \to X'$. It follows that U is finite and

  $$|U| \leqslant |X'| = n < n + 1 = |X|$$

  as required.

  $\diamond$ If $f(n + 1) \in i[U]$, then there is some $u_\star \in U$ such that $i(u_\star) = f(n + 1)$. Write $U' = U \setminus \{u_\star\}$, and define $i' : U' \to X'$ by $i'(x) = i(x)$ for all $x \in U'$. Again i' is injective, and $|X'| = n$, so the induction hypothesis yields that U' is finite

and $|U'| \leqslant n$; say $|U'| = k \in \mathbb{N}$. But then $|U| = k + 1$ by Exercise 4.1.42, and $k + 1 \leqslant n + 1$ since $k \leqslant n$.

In either case, we've proved that U is finite and $|U| \leqslant |X|$, so the induction step is complete.

By induction, it follows that any injection with finite codomain has a finite domain. $\qquad\square$

Exercise 4.2.2
Let X be a finite set. Prove that every subset $U \subseteq X$ is finite. $\qquad\triangleleft$

Exercise 4.2.3
Let X and Y be finite sets. Prove that $X \cap Y$ is finite. $\qquad\triangleleft$

Exercise 4.2.4
Let X be a finite set and let $U \subseteq X$. Prove that $X \setminus U$ is finite, and moreover $|X \setminus U| = |X| - |U|$. $\qquad\triangleleft$

Proposition 4.2.5
Let X and Y be finite sets. Then $X \cup Y$ is finite, and moreover

$$|X \cup Y| = |X| + |Y| - |X \cap Y|$$

Proof. We will prove this in the case when X and Y are disjoint. The general case, when X and Y are not assumed to be disjoint, will be Exercise 4.2.6.

If $X = \varnothing$ then $X \cup Y = Y$ and $X \cap Y = \varnothing$, so that

$$|X \cup Y| = |Y| \quad \text{and} \quad |X| + |Y| - |X \cap Y| = 0 + |Y| - 0 = |Y|$$

so the result is proved. The proof is similar when $Y = \varnothing$. So for the remainder of the proof, we assume that both X and Y are inhabited.

Let $m = |X| > 0$ and $n = |Y| > 0$, and let $f : [m] \to X$ and $g : [n] \to Y$ be bijections.

Since X and Y are disjoint, we have $X \cap Y = \varnothing$. Define $h : [m + n] \to X \cup Y$ as follows; given $k \in [m + n]$, let

$$h(k) = \begin{cases} f(k) & \text{if } k \leqslant m \\ g(k - m) & \text{if } k > m \end{cases}$$

Note that h is well-defined: the cases $k \leqslant m$ and $k > m$ are mutually exclusive, they cover all possible cases, and $k - m \in [n]$ for all $m + 1 \leqslant k \leqslant n$ so that $g(k - m)$ is defined. It is then straightforward to check that h has an inverse $h^{-1} : X \cup Y \to [m + n]$ defined by

$$h^{-1}(z) = \begin{cases} f^{-1}(z) & \text{if } z \in X \\ g^{-1}(z) + m & \text{if } z \in Y \end{cases}$$

Well-definedness of h^{-1} relies fundamentally on the assumption that $X \cap Y = \varnothing$, as this is what ensures that the cases $x \in X$ and $x \in Y$ are mutually exclusive.

Hence $|X \cup Y| = m + n = |X| + |Y|$, which is as required since $|X \cap Y| = 0$. $\qquad\square$

Exercise 4.2.6
The following steps complete the proof of Proposition 4.2.5:

(a) Given sets A and B, prove that the sets $A \times \{0\}$ and $B \times \{1\}$ are disjoint, and find bijections $A \to A \times \{0\}$ and $B \to B \times \{1\}$. Write $A \sqcup B$ (LaTeX code: `\sqcup`) to denote the set $(A \times \{0\}) \cup (B \times \{1\})$. The set $A \sqcup B$ is called the **disjoint union** of A and B.

(b) Prove that, if A and B are finite then $A \sqcup B$ is finite and

$$|A \sqcup B| = |A| + |B|$$

(c) Let X and Y be sets. Find a bijection

$$(X \cup Y) \sqcup (X \cap Y) \to X \sqcup Y$$

(d) Complete the proof of Proposition 4.2.5—that is, prove that if X and Y are finite sets, not necessarily disjoint, then $X \cup Y$ is finite and

$$|X \cup Y| = |X| + |Y| - |X \cap Y|$$

$\triangleleft$

Proposition 4.2.7
Let X and Y be finite sets. Then $X \times Y$ is finite, and moreover

$$|X \times Y| = |X| \cdot |Y|$$

Proof. If $X = \varnothing$ or $Y = \varnothing$, then $X \times Y = \varnothing$, so that $|X| = |Y| = |X \times Y| = 0$ and the result is immediate. As such, we assume for the rest of the proof that X and Y are both inhabited.

Let X and Y be sets with $|X| = m > 0$ and $|Y| = n > 0$, and let $f : [m] \to X$ and $g : [n] \to Y$ be bijections. Define a function $h : [m] \times [n] \to X \times Y$ by

$$h(k, \ell) = (f(k), g(\ell))$$

for each $k \in [m]$ and $\ell \in [n]$. It is easy to see that this is a bijection, with inverse defined by

$$h^{-1}(x,y) = (f^{-1}(x), g^{-1}(y))$$

for all $x \in X$ and $y \in Y$. By Exercise 4.1.16 there is a bijection $p : [mn] \to [m] \times [n]$, and by Exercise 4.1.17 the composite $h \circ p : [mn] \to X \times Y$ is a bijection. Hence $|X \times Y| = mn$. $\square$

In summary, we have shown that if X and Y are finite sets, then so are $X \cup Y$, $X \cap Y$, $X \times Y$, any subset $U \subseteq X$, and more generally any set U for which there exists an injection $U \to X$.

Indexed unions, intersections and products — finite version

Since we will be dealing with arbitrary finite collections of sets, it will help us to introduce some new notation to make notation more concise. For example, writing

$$X_1 \cup X_2 \cup \cdots \cup X_n$$

again and again will be cumbersome.

Definition 4.2.8

Let $n \in \mathbb{N}$ and, for each $i \in [n]$, let X_i be a set. We define. . .

- . . . the **indexed union** of $\{X_i \mid i \in [n]\}$ is the set $\bigcup_{i=1}^{n} X_i$ defined by

$$\bigcup_{i=1}^{n} X_i = \{x \mid x \in X_i \text{ for some } i \in [n]\}$$

- . . . the **indexed intersection** of $\{X_i \mid i \in [n]\}$ is the set $\bigcap_{i=1}^{n} X_i$ defined by

$$\bigcap_{i=1}^{n} X_i = \{x \mid x \in X_i \text{ for all } i \in [n]\}$$

- . . . the **indexed product** of $\{X_i \mid i \in [n]\}$ is the set $\prod_{i=1}^{n} X_i$ defined by

$$\prod_{i=1}^{n} X_i = \{(x_1, x_2 \ldots, x_n) \mid x_i \in X_i \text{ for each } i \in [n]\}$$

The notation $(x_1, x_2 \ldots, x_n)$ refers to an **ordered n-tuple**; formally, this is a function $x : [n] \to \bigcup_{i=1}^{n} X_i$ such that $x(i) \in X_i$ for all $i \in [n]$—then x_i is just shorthand for $x(i)$. But for our purposes, it will suffice to think of $(x_1, \ldots, x_n)$ as simply being an ordered list of n elements, with the ith component of the list being an element of X_i.

We write $X^n = \prod_{i=1}^{n} X$. For example, $\mathbb{N}^4$ is the set of ordered sequences of natural numbers of length 4, such as $(1, 5, 7, 3)$ or $(2, 2, 2, 2)$.

In Section 4.3 we will generalise Definition 4.2.8 even further to define indexed unions, intersections and products of arbitrary families of sets, not just finite ones. Everything we do now generalises to that scenario, but it is instructive to work in the finite case first.

Example 4.2.9

If X_1 and X_2 are sets, then $\{X_1, X_2\}$ is a family of sets indexed by the index set $I = \{1, 2\}$. Then $x \in \bigcap_{i \in I} X_i$ if and only if $x \in X_1$ and $x \in X_2$. This proves that

$$\bigcap_{i=1}^{2} X_i = X_1 \cap X_2$$

In other words, pairwise intersection is a special case of indexed intersection. The proof that $\bigcup_{i=1}^{2} X_i = X_1 \cup X_2$ is similar. ◁

Example 4.2.10

Let X_i be a set for all $i \in \mathbb{N}$. Notice that according to our definition we have

$$\bigcup_{i=1}^{0} X_i = \varnothing$$

since, for given x, we have $x \in \bigcup_{i=1}^{0} X_i$ if and only if $x \in X_i$ for some $i \in [0]$; since $[0] = \varnothing$, there are no such values of i, and so the expression $x \in \bigcup_{i=1}^{0} X_i$ can never be true.

Moreover, given $n \in \mathbb{N}$ we have

$$\bigcup_{i=1}^{n+1} X_i = \left(\bigcup_{i=1}^{n} X_i \right) \cup X_{n+1}$$

This is because, for given x, we have

$$x \in \bigcup_{i=1}^{n+1} X_i \Leftrightarrow x \in X_i \text{ for some } i \in [n+1]$$

$$\Leftrightarrow x \in X_i \text{ for some } i \in [n], \text{ or } x \in X_{n+1}$$

$$\Leftrightarrow x \in \bigcup_{i=1}^{n} X_i \text{ or } x \in X_{n+1}$$

$$\Leftrightarrow x \in \left(\bigcup_{i=1}^{n} X_i \right) \cup X_{n+1}$$

This yields an inductive proof that, when $n \geqslant 1$, we have

$$\bigcup_{i=1}^{n} X_i = X_1 \cup X_2 \cup \cdots \cup X_n$$

$\triangleleft$

Exercise 4.2.11

Let X_i be a set for each $i \in \mathbb{N}$. Prove that

$$\bigcap_{i=1}^{0} X_i = \mathcal{U} \quad \text{and} \quad \bigcap_{i=1}^{n+1} X_i = \left(\bigcap_{i=1}^{n} X_i \right) \cap X_{n+1} \text{ for all } n \in \mathbb{N}$$

where $\mathcal{U}$ is the universe. Deduce that if $n \geqslant 1$ then

$$\bigcap_{i=1}^{n} X_i = X_1 \cap X_2 \cap \cdots \cap X_n$$

$\triangleleft$

To tie up this portion on finite indexed families of sets, we note a new version of de Morgan's laws for sets which generalises the version you saw in Theorem 2.2.40. This theorem will be generalised even further in Theorem 4.3.5.

Theorem 4.2.12 (de Morgan's laws for sets (finite version))

Let $n \in \mathbb{N}$. For each $i \in [n]$ let X_i be a set, and let Z be a set. Then

(a) $Z \setminus (\bigcup_{i=1}^{n} X_i) = \bigcap_{i=1}^{n} (Z \setminus X_i)$;

(b) $Z \setminus (\bigcap_{i=1}^{n} X_i) = \bigcup_{i=1}^{n} (Z \setminus X_i)$.

Exercise 4.2.13

Prove Theorem 4.2.12 by induction on n, using Theorem 2.2.40 for the induction step. ◁

Exercise 4.2.14

Let $n \in \mathbb{N}$ and let X_i be a set for each $i \in [n+1]$. Note that the elements of $\prod_{i=1}^{n+1} X_i$ are ordered $(n+1)$-tuples, and that the elements of $(\prod_{i=1}^{n} X_i) \times X_{n+1}$ are *ordered pairs*, the first component of which is an ordered n-tuple. Prove that these are essentially the same thing, by showing that the function

$$f : \prod_{i=1}^{n+1} X_i \to \left(\prod_{i=1}^{n} X_i \right) \times X_{n+1}$$

defined by

$$f(x_1, x_2, \ldots, x_n, x_{n+1}) = ((x_1, x_2, \ldots, x_n), x_{n+1})$$

for all $x_i \in X_i$ and $i \in [n+1]$, is a bijection. ◁

Binomials and factorials revisited

We defined binomial coefficients $\binom{n}{k}$ and factorials $n!$ *recursively* in Section 1.3, and proved elementary facts about them by induction. We will now re-define them *combinatorially*— that is, we give them meaning in terms of sizes of particular finite sets. We will prove that the combinatorial and recursive definitions are equivalent, and prove facts about them using combinatorial arguments.

The reasons for doing so are manifold. The combinatorial definitions allow us to reason about binomials and factorials with direct reference to descriptions of finite sets, which will be particularly useful when we prove identities about them using *counting in two ways*. Moreover, the combinatorial definitions remove the seeming arbitrary nature of the recursive definitions—for example, they provide a reason why it makes sense to define $0! = 1$ and $\binom{0}{0} = 1$.

Definition 4.2.15

Let X be a set and let $k \in \mathbb{N}$. A k-**element subset** of X is a subset $U \subseteq X$ such that $|U| = k$. The set of all k-element subsets of X is denoted $\binom{X}{k}$ (read: 'X choose k') (LaTeX code: `\binom{X}{k}`).

Intuitively, $\binom{X}{k}$ is the set of ways of picking k elements from X, without repetitions, in such a way that order doesn't matter. (If order mattered, the elements would be *sequences* instead of *subsets*.)

Example 4.2.16

We find $\binom{[4]}{k}$ for all $k \in \mathbb{N}$.

- $\binom{[4]}{0} = \{\varnothing\}$ since the only set with 0 elements is $\varnothing$;

- $\binom{[4]}{1} = \{\{1\}, \{2\}, \{3\}, \{4\}\}$;

- $\binom{[4]}{2} = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\}$;

- $\binom{[4]}{3} = \{\{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}\}$;

- $\binom{[4]}{4} = \{\{1,2,3,4\}\}$;

- If $k \geqslant 5$ then $\binom{[4]}{k} = \varnothing$, since by Exercise 4.2.2, no subset of $[4]$ can have more than 4 elements.

$\triangleleft$

Proposition 4.2.17

If X is a finite set, then $\mathcal{P}(X) = \bigcup_{k \leqslant |X|} \binom{X}{k}$.

Proof. Let $U \subseteq X$. By Exercise 4.2.2, U is finite and $|U| \leqslant |X|$. Thus $U \in \binom{X}{|U|}$, and hence $U \in \bigcup_{k \leqslant |X|} \binom{X}{k}$. This proves that $\mathcal{P}(X) \subseteq \bigcup_{k \leqslant |X|} \binom{X}{k}$.

The fact that $\bigcup_{k \leqslant |X|} \binom{X}{k} \subseteq \mathcal{P}(X)$ is immediate, since elements of $\binom{X}{k}$ are defined to be subsets of X, and hence elements of $\mathcal{P}(X)$. $\square$

Definition 4.2.18

Let $n, k \in \mathbb{N}$. Denote by $\binom{n}{k}$ (read: 'n choose k') (LaTeX code: `\binom{n}{k}`) the number of k-element subsets of a set of size n. That is, we define $\binom{n}{k} = \left| \binom{[n]}{k} \right|$. The numbers $\binom{n}{k}$ are called **binomial coefficients**.[a]

---

[a]Some authors use the notation $_n\mathrm{C}_k$ or $^n\mathrm{C}_k$ instead of $\binom{n}{k}$. We avoid this, as it is unnecessarily clunky.

Intuitively, $\binom{n}{k}$ is the number of ways of selecting k things from n, without repetitions, in such a way that order doesn't matter.

The value behind this notation is that it allows us to express huge numbers in a concise and meaningful way. For example,

$$\binom{4000}{11} = 103\,640\,000\,280\,154\,258\,645\,590\,429\,564\,000$$

Although these two numbers are equal, their *expressions* are very different; the expression on the left is meaningful, but the expression on the right is completely meaningless out of context.

Writing tip
When expressing the sizes of finite sets described combinatorially, it is best to *avoid* evaluating the expression; that is, leave in the powers, products, sums, binomial coefficients and factorials! The reason for this is that performing the calculations takes the meaning away from the expressions. ◁

Example 4.2.19
In Example 4.2.16 we proved that:

$$\binom{4}{0} = 1, \quad \binom{4}{1} = 4, \quad \binom{4}{2} = 6, \quad \binom{4}{3} = 4, \quad \binom{4}{4} = 1$$

and that $\binom{4}{k} = 0$ for all $k \geqslant 5$. ◁

Exercise 4.2.20
Fix $n \in \mathbb{N}$. Prove that $\binom{n}{0} = 1$, $\binom{n}{1} = n$ and $\binom{n}{n} = 1$. ◁

Definition 4.2.21
Let X be a set. A **permutation** of X is a bijection $X \to X$. Denote the set of all permutations of X by S_X (L&ATEX code: S_X),[a] and write $S_{[n]} = S_n$ for $n \in \mathbb{N}$.

---
[a]The 'S' comes from 'symmetry'. The set S_X comes with the natural structure of a *group*.

Example 4.2.22
There are six permutations of the set $[3]$. Representing each $f \in S_{[3]}$ by the ordered triple $(f(1), f(2), f(3))$, these permutations are thus given by

$$(1,2,3), \ (1,3,2), \ (2,1,3), \ (2,3,1), \ (3,1,2), \ (3,2,1)$$

For example, $(2,3,1)$ represents the permutation $f : [3] \to [3]$ defined by $f(1) = 2$, $f(2) = 3$ and $f(3) = 1$. ◁

Exercise 4.2.23
List all the permutations of the set $[4]$.   ◁

Definition 4.2.24
Let $n \in \mathbb{N}$. Denote by $n!$ (read: 'n factorial') the number of permutations of a set of size n. That is, $n! = |S_n|$. The numbers $n!$ are called **factorials**.

Example 4.2.25
Example 4.2.22 shows that $3! = 6$.   ◁

Counting products and partitions

We saw in Proposition 4.2.7 and Proposition 4.2.5 that, given two finite sets X and Y, the product $X \times Y$ and the union $X \cup Y$ are finite. We also found formulae for their size. The *multiplication principle* (Theorem 4.2.26) and *addition principle* (Theorem 4.2.37) generalise these formulae, extending to products and (disjoint) unions of any finite number of finite sets.

Theorem 4.2.26 (Multiplication principle (independent version))
Let $\{X_1, \ldots, X_n\}$ be a family of finite sets, with $n \geqslant 1$. Then $\prod_{i=1}^{n} X_i$ is finite, and

$$\left| \prod_{i=1}^{n} X_i \right| = |X_1| \cdot |X_2| \cdot \cdots \cdot |X_n|$$

Proof. We proceed by induction on n.

- (**BC**) When $n = 1$, an element of $\prod_{i=1}^{1} X_i$ is 'officially' 1-ary sequence (x_1) with $x_1 \in X_1$. This is the same as an element of X_1: it is easy to check that the assignments $(x_1) \mapsto x_1$ and $x_1 \mapsto (x_1)$ define mutually inverse (hence bijective) functions between $\prod_{i=1}^{1} X_i$ and X_1, and so

$$\left| \prod_{i=1}^{1} X_i \right| = |X_1|$$

- (**IS**) Fix $n \in \mathbb{N}$, and suppose that

$$\left| \prod_{i=1}^{n} X_i \right| = |X_1| \cdot |X_2| \cdot \cdots \cdot |X_n|$$

for all sets X_i for $i \in [n]$. This is our induction hypothesis.

Now let $X_1, \dots, X_n, X_{n+1}$ be sets. We define a function

$$F : \prod_{i=1}^{n+1} X_i \to \left(\prod_{i=1}^{n} X_i \right) \times X_{n+1}$$

by letting $F((x_1, \dots, x_n, x_{n+1})) = ((x_1, \dots, x_n), x_{n+1})$. It is again easy to check that F is a bijection, and hence

$$\left| \prod_{i=1}^{n+1} X_i \right| = \left| \prod_{i=1}^{n} X_i \right| \cdot |X_{n+1}|$$

by Proposition 4.2.7. Applying the induction hypothesis, we obtain the desired result, namely

$$\left| \prod_{i=1}^{n+1} X_i \right| = |X_1| \cdot |X_2| \cdot \dots \cdot |X_n| \cdot |X_{n+1}|$$

By induction, we're done. □

The multiplication principle is also known as the *rule of product*.

Problem-solving tip

The multiplication principle allows us to count the number of elements of a finite set X by devising a *procedure* for counting all of its elements exactly once. If this procedure has n steps, where $n \in \mathbb{N}$, then the procedure establishes a bijection

$$X \to \prod_{i=1}^{n} S_i$$

where S_i is the set of possible outcomes of the ith step in the procedure. If there are n_i possible outcomes of the ith step in the procedure, this therefore implies that

$$|X| = \prod_{i=1}^{n} n_i$$

◁

Example 4.2.27

You go to an ice cream stand selling the following flavours:

vanilla, strawberry, chocolate, rum and raisin, mint choc chip, toffee crunch

You can have your ice cream in a tub, a regular cone or a *choco-cone.* You can have one, two or three scoops. We will compute how many options you have.

To select an ice cream, you follow the following procedure:

- **Step 1.** Choose a flavour. There are 6 ways to do this.

- **Step 2.** Choose whether you'd like it in a tub, regular cone or choco-cone. There are 3 ways to do this.

- **Step 3.** Choose how many scoops you'd like. There are 3 ways to do this.

Hence there are $6 \times 3 \times 3 = 54$ options in total. $\triangleleft$

This may feel informal, but really what we are doing is establishing a bijection. Letting X be the set of options, the above procedure defines a bijection

$$X \to F \times C \times S$$

where F is the set of flavours, $C = \{\text{tub}, \text{regular cone}, \text{choco-cone}\}$ and $S = [3]$ is the set of possible numbers of scoops.

Example 4.2.28
We will prove that $|\mathcal{P}(X)| = 2^{|X|}$ for all finite sets X.[c]

Let X be a finite set and let $n = |X|$. Write

$$X = \{x_k \mid k \in [n]\} = \{x_1, x_2, \ldots, x_n\}$$

Intuitively, specifying an element of $\mathcal{P}(X)$—that is, a subset $U \subseteq X$—is equivalent to deciding, for each $k \in [n]$, whether $x_k \in U$ or $x_k \notin U$ ('in or out'), which in turn is equivalent to specifying an element of $\{\text{in}, \text{out}\}^n$.

For example, taking $X = [7]$, the subset $U = \{1, 2, 6\}$ corresponds with the choices

$$1 \text{ in}, \ 2 \text{ in}, \ 3 \text{ out}, \ 4 \text{ out}, \ 5 \text{ out}, \ 6 \text{ in}, \ 7 \text{ out}$$

and hence the element $(\text{in}, \text{in}, \text{out}, \text{out}, \text{out}, \text{in}, \text{out}) \in \{\text{in}, \text{out}\}^7$.

This defines a function $i : \mathcal{P}(X) \to \{\text{in}, \text{out}\}^n$. This function is injective, since different subsets determine different sequences; and it is surjective, since each sequence determines a subset.

---

[c]Some authors write 2^X to refer to the power set of a set X. This is justified by Exercise 4.2.28.

The above argument is sufficient for most purposes, but since this is the first bijective proof we have come across, we now give a more formal presentation of the details.

Define a function
$$i : \mathcal{P}(X) \to \{\text{in}, \text{out}\}^n$$
by letting the kth component of $i(U)$ be 'in' if $x_k \in U$ or 'out' if $x_k \notin U$, for each $k \in [n]$.

We prove that i is a bijection.

- i **is injective.** To see this, take $U, V \subseteq X$ and suppose $i(U) = i(V)$. We prove that $U = V$. So fix $x \in X$ and let $k \in [n]$ be such that $x = x_k$. Then

$$
\begin{aligned}
x \in U &\Leftrightarrow \text{the } k^{\text{th}} \text{ component of } i(U) \text{ is 'in'} && \text{by definition of } i \\
&\Leftrightarrow \text{the } k^{\text{th}} \text{ component of } i(V) \text{ is 'in'} && \text{since } i(U) = i(V) \\
&\Leftrightarrow x \in V && \text{by definition of } i
\end{aligned}
$$

  so indeed we have $U = V$, as required.

- i **is surjective.** To see this, let $v \in \{\text{in}, \text{out}\}^n$, and let

$$U = \{x_k \mid \text{the } k^{\text{th}} \text{ component of } v \text{ is 'in'}\}$$

  Then $i(U) = v$, since for each $k \in [n]$ we have $x_k \in U$ if and only if the kth component of v is 'in', which is precisely the definition of $i(U)$.

Hence
$$|\mathcal{P}(X)| = |\{\text{in}, \text{out}\}|^n = 2^n$$
as required. ◁

Exercise 4.2.29
Let X and Y be finite sets, and recall that Y^X denotes the set of functions from X to Y. Prove that $|Y^X| = |Y|^{|X|}$. ◁

Example 4.2.30
We count the number of ways we can shuffle a standard deck of cards in such a way that the colour of the cards alternate between red and black.

A procedure for choosing the order of the cards is as follows:

(i) Choose the colour of the first card. There are 2 such choices. This then determines the colours of the remaining cards, since they have to alternate.

(ii) Choose the order of the red cards. There are 26! such choices.

(iii) Choose the order of the black cards. There are 26! such choices.

By the multiplication principle, there are $2 \cdot (26!)^2$ such rearrangements. This number is huge, and in general there is no reason to write it out. Just for fun, though:

$$2 \cdot (26!)^2 = 325\,288\,005\,235\,264\,929\,014\,077\,766\,819\,257\,214\,042\,112\,000\,000\,000\,000$$

◁

Exercise 4.2.31
Since September 2001, car number plates on the island of Great Britain have taken the form XX NN XXX, where each X can be any letter of the alphabet except for 'I', 'Q' or 'Z', and NN is the last two digits of the year.[d] How many possible number plates are there? Number plates of vehicles registered in the region of Yorkshire begin with the letter 'Y'. How many Yorkshire number plates can be issued in a given year?   ◁

A sight modification to the multiplication principle allows sets later in the product to depend somehow on those appearing earlier. Thinking of the elements of a product as steps in a counting procedure, this means that later steps can depend on the outcome of earlier steps, which will turn out to be extremely useful!

Corollary 4.2.32 (Multiplication principle (dependent version))
Let $n \geqslant 1$ and for each $i \in [n]$ let $k_i \in \mathbb{N}$. Define a family of sets $X_i(x_1, \ldots, x_{i-1})$ for $i \in [n]$ inductively as follows:

- Let X_1 be a finite set of size k_1;

- Let $i < n$ and suppose $X_i(x_1, \ldots, x_{i-1})$ has been defined. For each $x_i \in X_i(x_1, \ldots, x_{i-1})$, let $X_{i+1}(x_1, \ldots, x_{i-1}, x_i)$ be a finite set of size k_{i+1}.

Then for each choice of sequence $(x_1, x_2, \ldots, x_n)$, with $x_i \in X_i(x_1, \ldots, x_{i-1})$ for each $i \in [n]$, the set
$$X = \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i(x_1, x_2, \ldots, x_{i-1}) \text{ for all } i \in [n]\}$$

is finite, and moreover
$$|X| = \prod_{i=1}^{n} k_i$$

---

[d]This is a slight simplification of what is really the case, but let's not concern ourselves with *too* many details!

Proof. We proceed by induction on $n \geqslant 1$.

- (**BC**) When $n = 1$, this result says precisely that if X_1 is a finite set of size k_1, then X_1 is a finite set of size k_1. This is true.

- (**IS**) Fix $n \geqslant 1$ and suppose that the theorem is true for n.

  For $i \leqslant n+1$, let sets $X_i(x_1, \ldots, x_{i-1})$ be defined as in the statement of the theorem, and let

  $$X = \{(x_1, x_2, \ldots, x_n, x_{n+1}) \mid x_i \in X_i(x_1, x_2, \ldots, x_{i-1}) \text{ for all } i \in [n+1]\}$$

  We prove that X is finite and $|X| = \prod_{i=1}^{n+1} k_i$.

  Let $X' = \{(x_1, x_2, \ldots, x_n) \mid x_i \in X_i(x_1, x_2, \ldots, x_{i-1}) \text{ for all } i \in [n]\}$. By the induction hypothesis, we know that $|X'| = \prod_{i=1}^{n} k_i$. Now there is an evident bijection

  $$X \to \bigcup_{(x_1, \ldots, x_n) \in X'} \{(x_1, x_2, \ldots, x_n)\} \times X_{n+1}(x_1, \ldots, x_n)$$

  given by the correspondence between

  $$(x_1, x_2, \ldots, x_n, x_{n+1}) \quad \text{and} \quad ((x_1, x_2, \ldots, x_n), x_{n+1})$$

  for all $i \in [n+1]$ and $x_i \in X_i(x_1, \ldots, x_{i-1})$. Moreover the sets $\{(x_1, x_2, \ldots, x_n)\} \times X_{n+1}(x_1, \ldots, x_n)$ are pairwise disjoint. Hence by the addition principle (to be proved soon—see Theorem 4.2.37), we have

  $$|X| = \sum_{(x_1, \ldots, x_n) \in X'} |\{(x_1, x_2, \ldots, x_n)\} \times X_{n+1}(x_1, \ldots, x_n)|$$

  But for all $(x_1, \ldots, x_n) \in X'$, we have

  $$
  \begin{aligned}
  &|\{(x_1, x_2, \ldots, x_n)\} \times X_{n+1}(x_1, \ldots, x_n)| \\
  &= |\{(x_1, x_2, \ldots, x_n)\}| \cdot |X_{n+1}(x_1, \ldots, x_n)| \qquad \text{by Proposition 4.2.7} \\
  &= 1 \cdot k_{n+1} \qquad\qquad\qquad\qquad\qquad\qquad \text{by definition of } X_{n+1}(\cdots) \\
  &= k_{n+1}
  \end{aligned}
  $$

and hence

$$\sum_{(x_1,\ldots,x_n)\in X'} |\{(x_1, x_2, \ldots, x_n)\} \times X_{n+1}(x_1, \ldots, x_n)|$$

$$= \sum_{(x_1,\ldots,x_n)\in X'} k_{n+1} \qquad\qquad \text{as we just saw}$$

$$= |X'| \cdot k_{n+1} \qquad\qquad \text{since terms in sum are constant}$$

$$= \left(\prod_{i=1}^{n} k_i\right) \cdot k_{n+1} \qquad\qquad \text{by the induction hypothesis}$$

$$= \prod_{i=1}^{n+1} k_i$$

as required.

By induction, we're done. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Example 4.2.33
We prove that there are six bijections $[3] \to [3]$. We can specify a bijection $f : [3] \to [3]$ according to the following procedure.

- **Step 1.** Choose the value of $f(1)$. There are 3 choices.

- **Step 2.** Choose the value of $f(2)$. The values $f(2)$ can take depend on the chosen value of $f(1)$.

  ◇ If $f(1) = 1$, then $f(2)$ can be equal to 2 or 3.
  ◇ If $f(1) = 2$, then $f(2)$ can be equal to 1 or 3.
  ◇ If $f(1) = 3$, then $f(2)$ can be equal to 1 or 2.

  In each case, there are 2 choices for the value of $f(2)$.

- **Step 3.** Choose the value of $f(3)$. The values $f(3)$ can take depend on the values of $f(1)$ and $f(2)$. We could split into the (six!) cases based on the values of $f(1)$ and $f(2)$ chosen in Steps 1 and 2; but we won't. Instead, note that $\{f(1), f(2)\}$ has two elements, and by injectivity $f(3)$ must have a distinct value, so that $[3] \setminus \{f(1), f(2)\}$ has one element. This element must be the value of $f(3)$. Hence there is only possible choice of $f(3)$.

By the multiplication principle, there are $3 \times 2 \times 1 = 6$ bijections $[3] \to [3]$. $\qquad$ ◁

Exercise 4.2.34

Count the number of injections $[3] \to [4]$. ◁

The *addition principle* says that if we can *partition* a set into smaller chunks, then the size of the set is the sum of the sizes of the chunks. We will first make this notion of 'partition' precise.

Definition 4.2.35

Sets X and Y are **disjoint** if $X \cap Y = \varnothing$. More generally, given $n \in \mathbb{N}$, a collection of sets $X_1, X_2, \ldots, X_n$ is **pairwise disjoint** if $X_i \cap X_j = \varnothing$ for all $i, j \in [n]$ with $i \neq j$.

Definition 4.2.36

A (**finite**) **partition** of a set X is, for some $n \in \mathbb{N}$, a collection $\{U_i \mid i \in [n]\}$ of subsets of X such that:

(i) Each U_i is inhabited;

(ii) The sets $U_1, U_2, \ldots, U_n$ are pairwise disjoint; and

(iii) $\bigcup_{i=1}^{n} U_i = X$.

Theorem 4.2.37 (Addition principle)

Let X be a set and let $\{U_1, \ldots, U_n\}$ be a partition of X for some $n \in \mathbb{N}$, such that each set U_i is finite. Then X is finite, and

$$|X| = |U_1| + |U_2| + \cdots + |U_n|$$

Exercise 4.2.38

Prove Theorem 4.2.37. The proof follows the same pattern as that of the multiplication principle (Theorem 4.2.26). Be careful to make sure you identify where you use the hypothesis that the sets U_i are pairwise disjoint! ◁

Problem-solving tip

The addition principle allows us to count the number of elements of a finite set by finding a *partition* of X, say $\{U_1, U_2, \ldots, U_n\}$. If $|U_i| = n_i$ for each $1 \leqslant i \leqslant n$, then this means that

$$|X| = \sum_{i=1}^{n} n_i$$

◁

Example 4.2.39

We will count the number of inhabited subsets of $[7]$ which either contain only even numbers, or contain only odd numbers.

Let O denote the set of inhabited subsets of $[7]$ containing only odd numbers, and let E denote the set of inhabited subsets of $[7]$ containing only even numbers. Note that $\{O, E\}$ forms a partition of the set we are counting, and so our set has $|O| + |E|$ elements.

- An element of O must be a subset of $\{1, 3, 5, 7\}$. By Example 4.2.28 there are $2^4 = 16$ such subsets. Thus the number of *inhabited* subsets of $[7]$ containing only odd numbers is 15, since we must exclude the empty set. That is, $|O| = 15$.

- A subset containing only even numbers must be a subset of $\{2, 4, 6\}$. Again by Example 4.2.28 there are $2^3 = 8$ such subsets. Hence there are 7 inhabited subsets of $[7]$ containing only even numbers. That is, $|E| = 7$.

Hence there are $15 + 7 = 22$ inhabited subsets of $[7]$ containing only even or only odd numbers. And here they are:

$$\begin{array}{cccccccc}
\{1\} & \{3\} & \{5\} & \{7\} & \{1,3\} & \{2\} & \{4\} & \{6\} \\
\{1,5\} & \{1,7\} & \{3,5\} & \{3,7\} & \{5,7\} & \{2,4\} & \{2,6\} & \{4,6\} \\
\{1,3,5\} & \{1,3,7\} & \{1,5,7\} & \{3,5,7\} & \{1,3,5,7\} & \{2,4,6\} & &
\end{array}$$

◁

Exercise 4.2.40

Pick your favourite integer $n > 1000$. For this value of n, how many inhabited subsets of $[n]$ contain either only even or only odd numbers? (You need not evaluate exponents.)   ◁

We now consider some examples of finite sets which use both the multiplication principle and the addition principle.

Example 4.2.41

A city has $6n$ inhabitants. The favourite colour of n of the inhabitants is orange, the favourite colour of $2n$ of the inhabitants is pink, and the favourite colour of $3n$ of the inhabitants is turquoise. The city government wishes to form a committee with equal representation from the three colour preference groups to decide how the new city hall should be painted. We count the number of ways this can be done.

Let X be the set of possible committees. First note that

$$X = \bigcup_{k=0}^{n} X_k$$

where X_k is the set of committees with exactly k people from each colour preference group. Indeed, we must have $k \leqslant n$, since it is impossible to have a committee with more than n people from the orange preference group.

Moreover, if $k \neq \ell$ then $X_k \cap X_\ell = \varnothing$, since if $k \neq \ell$ then a committee cannot simultaneously have exactly k people and exactly ℓ people from each preference group.

By the addition principle, we have

$$|X| = \sum_{k=0}^{n} |X_k|$$

We count X_k for fixed k using the following procedure:

- **Step 1.** Choose k people from the orange preference group to be on the committee. There are $\binom{n}{k}$ choices.

- **Step 2.** Choose k people from the pink preference group to be on the committee. There are $\binom{2n}{k}$ choices.

- **Step 3.** Choose k people from the turquoise preference group to be on the committee. There are $\binom{3n}{k}$ choices.

By the multiplication principle, it follows that $|X_k| = \binom{n}{k}\binom{2n}{k}\binom{3n}{k}$. Hence

$$|X| = \sum_{k=0}^{n} \binom{n}{k}\binom{2n}{k}\binom{3n}{k}$$

◁

Exercise 4.2.42
In Example 4.2.41, how many ways could a committee be formed with a *representative* number of people from each colour preference group? That is, the proportion of people on the committee which prefer any of the three colours should be equal to the corresponding proportion of the population of the city.

◁

Counting in two ways

Counting in two ways (also known as *double counting*) is a proof technique that allows us to prove that two natural numbers are equal by establishing they are two expressions for the size of the same set. (More generally, by Exercise 4.1.43, we can relate them to the sizes of two sets which are in bijection.)

The proof of Proposition 4.2.43 illustrates this proof very nicely. We proved it already by induction in Exercise 1.3.29; the combinatorial proof we now provide is much shorter and cleaner.

Proposition 4.2.43

Let $n \in \mathbb{N}$. Then $2^n = \sum_{k=0}^{n} \binom{n}{k}$.

Proof. We know that $|\mathcal{P}([n])| = 2^n$ by Example 4.2.28 and that $\mathcal{P}([n]) = \bigcup_{k=0}^{n} \binom{[n]}{k}$ by Proposition 4.2.17. Moreover, the sets $\binom{[n]}{k}$ are pairwise disjoint, so by the addition principle it follows that

$$2^n = |\mathcal{P}([n])| = \left| \bigcup_{k=0}^{n} \binom{[n]}{k} \right| = \sum_{k=0}^{n} \left| \binom{[n]}{k} \right| = \sum_{k=0}^{n} \binom{n}{k}$$

$\square$

Proof tip

To prove that two natural numbers m and n are equal, we can find sets X and Y such that $|X| = m$, $|Y| = n$ and either $X = Y$ or there is a bijection $X \to Y$. This proof technique is called **counting in two ways**, and is very useful for proving identities regarding numbers that have a combinatorial interpretation (especially binomial coefficients and factorials, which will be introduced later). ◁

The next example counts elements of *different* sets and puts them in bijection to establish an identity.

Proposition 4.2.44

Let $n, k \in \mathbb{N}$ with $n \geqslant k$. Then

$$\binom{n}{k} = \binom{n}{n-k}$$

Proof. First note that $\binom{n}{k} = \left| \binom{[n]}{k} \right|$ and $\binom{n}{n-k} = \left| \binom{[n]}{n-k} \right|$, so it suffices to find a bijection $f : \binom{[n]}{k} \to \binom{[n]}{n-k}$. Intuitively, this bijection arises because choosing k elements from $[n]$ to *put into* a subset is equivalent to choosing $n - k$ elements from $[n]$ to *leave out of* the subset. Specifically, we define

$$f(U) = [n] \setminus U \text{ for all } U \in \binom{[n]}{k}$$

Note first that f is well-defined, since if $U \subseteq [n]$ with $|U| = k$, then $[n] \setminus U \subseteq [n]$ and $|[n] \setminus U| = |[n]| - |U| = n - k$ by Exercise 4.2.4. We now prove f is a bijection:

- **f is injective.** Let $U, V \subseteq [n]$ and suppose $[n] \setminus U = [n] \setminus V$. Then for all $k \in [n]$, we have

$$
\begin{aligned}
k \in U &\Leftrightarrow k \notin [n] \setminus U && \text{by definition of set difference} \\
&\Leftrightarrow k \notin [n] \setminus V && \text{since } [n] \setminus U = [n] \setminus V \\
&\Leftrightarrow k \in V && \text{by definition of set difference}
\end{aligned}
$$

  so $U = V$, as required.

- **f is surjective.** Let $V \in \binom{[n]}{n-k}$. Then $|[n] \setminus V| = n - (n - k) = k$ by Exercise 4.2.4, so that $[n] \setminus V \in \binom{[n]}{k}$. But then

$$
f([n] \setminus V) = [n] \setminus ([n] \setminus V) = V
$$

  by Exercise 2.2.39.

Since f is a bijection, we have

$$
\binom{n}{k} = \left| \binom{[n]}{k} \right| = \left| \binom{[n]}{n-k} \right| = \binom{n}{n-k}
$$

as required. $\qquad\square$

We put a lot of detail into this proof. A slightly less formal proof might simply say that $\binom{n}{k} = \binom{n}{n-k}$ since choosing k elements from $[n]$ to put into a subset is equivalent to choosing $n - k$ elements from $[n]$ to leave out of the subset. This would be fine as long as the members of the intended audience of your proof could reasonably by expected to construct the bijection by themselves.

The proof of Proposition 4.2.45 follows this more informal format.

Proposition 4.2.45
Let $n, k, \ell \in \mathbb{N}$ with $n \geqslant k \geqslant \ell$. Then

$$
\binom{n}{k}\binom{k}{\ell} = \binom{n}{\ell}\binom{n-\ell}{k-\ell}
$$

Proof. Let's home in on the left-hand side of the equation. By the multiplication principle, $\binom{n}{k}\binom{k}{\ell}$ is the number of ways of selecting a k-element subset of $[n]$ and an ℓ-element subset of $[k]$. Equivalently, it's the number of ways of selecting a k-element subset of $[n]$ and then an ℓ-element subset *of the k-element subset that we just selected*. To make this slightly more concrete, let's put it this way:

$\binom{n}{k}\binom{k}{\ell}$ is the number of ways of painting k balls red from a bag of n balls, and painting ℓ of the red balls blue. This leaves us with ℓ blue balls and $k - \ell$ red balls.

Now we need to find an equivalent interpretation of $\binom{n}{\ell}\binom{n-\ell}{k-\ell}$. Well, suppose we pick the ℓ elements to be coloured blue first. To make up the rest of the k-element subset, we now have to select $k - \ell$ elements, and there are now $n - \ell$ to choose from. Thus

$\binom{n}{\ell}\binom{n-\ell}{k-\ell}$ is the number of ways of painting ℓ balls from a bag of n balls blue, and painting $k - \ell$ of the remaining balls red.

Thus, both numbers represent the number of ways of painting ℓ balls blue and $k - \ell$ balls red from a bag of n balls. Hence they are equal. $\qquad\square$

Exercise 4.2.46
Make the proof of Proposition 4.2.45 more formal by defining a bijection between sets of the appropriate sizes. $\qquad\triangleleft$

Exercise 4.2.47
Provide a combinatorial proof that if $n, k \in \mathbb{N}$ with $n \geqslant k$, then

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

Deduce that the combinatorial definition of binomial coefficients (Definition 4.2.18) is equivalent to the recursive definition (Definition 1.3.27). $\qquad\triangleleft$

The following proposition demonstrates that the combinatorial definition of factorials (Definition 4.2.24) is equivalent to the recursive definition (Definition 1.3.25).

Proposition 4.2.48
$0! = 1$ and if $n \in \mathbb{N}$ then $(n+1)! = (n+1) \cdot n!$.

Proof. The only permutation of $\varnothing$ is the empty function $e : \varnothing \to \varnothing$. Hence $S_0 = \{e\}$ and $0! = |S_0| = 1$.

Let $n \in \mathbb{N}$. A permutation of $[n+1]$ is a bijection $f : [n+1] \to [n+1]$. Specifying such a bijection is equivalent to carrying out the following procedure:

- Choose the (unique!) element $k \in [n+1]$ such that $f(k) = n + 1$. There are $n + 1$ choices for k.

- Choose the values of f at each $\ell \in [n+1]$ with $\ell \neq k$. This is equivalent to finding a bijection $[n+1] \setminus \{k\} \to [n]$. Since $|[n+1] \setminus \{k\}| = |[n]| = n$, there are $n!$ such choices.

By the multiplication principle, we have

$$(n+1)! = |S_{n+1}| = (n+1) \cdot n!$$

so we're done. $\square$

We now revisit Theorem 1.3.31; this time, our proof will be combinatorial, rather than inductive.

Theorem 4.2.49

Let $n, k \in \mathbb{N}$. Then

$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!(n-k)!} & \text{if } k \leqslant n \\ 0 & \text{if } k > n \end{cases}$$

Proof. Suppose $k > n$. By Exercise 4.2.2, if $U \subseteq [n]$ then $|U| \leqslant n$. Hence if $k > n$, then $\binom{[n]}{k} = \varnothing$, and so $\binom{n}{k} = 0$, as required.

Now suppose $k \leqslant n$. We will prove that $n! = \binom{n}{k} \cdot k! \cdot (n-k)!$; the result then follows by dividing through by $k!(n-k)!$. We prove this equation by counting the number of elements of S_n.

A procedure for defining an element of S_n is as follows:

(i) Choose which elements will appear in the first k positions of the list. There are $\binom{n}{k}$ such choices.

(ii) Choose the order of these k elements. There are $k!$ such choices.

(iii) Choose the order of the remaining $n - k$ elements. There are $(n-k)!$ such choices.

By the multiplication principle, $n! = \binom{n}{k} \cdot k! \cdot (n-k)!$. $\square$

Note that the proof of Theorem 4.2.49 relied only on the combinatorial definitions of binomial coefficients and factorials; we didn't need to know how to compute them at

all! The proof was *much* shorter, cleaner and, in some sense, more meaningful, than the inductive proof we gave in Section 1.3—see Theorem 1.3.31.

We conclude this section with some more examples and exercises in which counting in two ways can be used.

Exercise 4.2.50

Let $n, k \in \mathbb{N}$ with $k \leqslant n + 1$. Prove that

$$k \binom{n}{k} = (n - k + 1) \binom{n}{k - 1}$$

◁

Example 4.2.51

Let $m, n, k \in \mathbb{N}$. We prove that

$$\sum_{\ell=0}^{k} \binom{m}{\ell} \binom{n}{k - \ell} = \binom{m + n}{k}$$

by finding a procedure for counting the number of k-element subsets of an appropriate $(m + n)$-element set. Specifically, let X be a set containing m cats and n dogs. Then $\left| \binom{m+n}{k} \right|$ is the number of k-element subsets $U \subseteq X$. We can specify such a subset according to the following procedure.

- **Step 1.** Split into cases based on the number ℓ of cats in U. Note that we must have $0 \leqslant \ell \leqslant k$, since the number of cats must be a natural number and cannot exceed k as $|U| = k$. Moreover, these cases are mutually exclusive. Hence by the addition principle we have

$$\binom{m + n}{k} = \sum_{\ell=0}^{k} a_\ell$$

  where a_ℓ is the number of subsets of X containing ℓ cats and $k - \ell$ dogs.

- **Step 2.** Choose ℓ cats from the m cats in X to be elements of U. There are $\binom{[m]}{\ell}$ such choices.

- **Step 3.** Choose $k - \ell$ dogs from the n dogs in X to be elements of U. There are $\binom{[n]}{k-\ell}$ such choices.

The multiplication principle shows that $a_\ell = \binom{m}{\ell} \binom{n}{k-\ell}$. Hence

$$\binom{m + n}{k} = \sum_{\ell=0}^{k} \binom{m}{\ell} \binom{n}{k - \ell}$$

as required.   ◁

Exercise 4.2.52

Let $n \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

◁

Exercise 4.2.53

Let $n, m \in \mathbb{N}$ with $m \leqslant n$. Prove that

$$\sum_{k=m}^{n} \binom{n}{k}\binom{k}{m} = 2^{n-m}\binom{n}{m}$$

◁

Exercise 4.2.54

Given natural numbers n, a, b, c with $a + b + c = n$, define the **trinomial coefficient** $\binom{n}{a, b, c}$ to be the number of ways of partitioning $[n]$ into three sets of sizes a, b and c, respectively. That is, $\binom{n}{a, b, c}$ is the size of the set

$$\left\{ (A, B, C) \;\middle|\; \begin{array}{c} A \subseteq [n], \quad B \subseteq [n], \quad C \subseteq [n], \\ |A| = a, \quad |B| = b, \quad |C| = c, \\ \text{and } A \cup B \cup C = [n] \end{array} \right\}$$

By considering trinomial coefficients, prove that if $a, b, c \in \mathbb{N}$, then $(a + b + c)!$ is divisible by $a! \cdot b! \cdot c!$.

◁

Here is one nice application of counting in two ways and the multiplication principle to number theory. We will make use of this in the proof of Theorem 5.3.7, which provides a general formula for the totient of an integer.

Theorem 4.2.55 (Multiplicativity of Euler's totient function)
Let $m, n \in \mathbb{Z}$ and let $\varphi : \mathbb{Z} \to \mathbb{N}$ be Euler's totient function (see Definition 3.3.31). If m and n are coprime, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. Since $\varphi(-k) = \varphi(k)$ for all $k \in \mathbb{Z}$, we may assume that $m \geqslant 0$ and $n \geqslant 0$. Moreover, if $m = 0$ or $n = 0$, then $\varphi(m)\varphi(n) = 0$ and $\varphi(mn) = 0$, so the result is immediate. Hence we may assume that $m > 0$ and $n > 0$.

Given $k \in \mathbb{Z}$, define

$$C_k = \{a \in [k] \mid a \perp k\}$$

By definition of Euler's totient function, we thus have $|C_k| = \varphi(k)$ for all $k \in \mathbb{Z}$. We will define a bijection

$$f : C_m \times C_n \to C_{mn}$$

using the Chinese remainder theorem (Theorem 3.3.46).

Given $a \in C_m$ and $b \in C_n$, let $f(a, b)$ be the element $x \in [mn]$ such that

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$$

- **f is well-defined.** We check the properties of totality, existence and uniqueness.

  ◇ **Totality.** We have accounted for all the elements of $C_m \times C_n$ in our specification of f.

  ◇ **Existence.** By the Chinese remainder theorem, there exists $x \in \mathbb{Z}$ such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$. By adding an appropriate integer multiple of mn to x, we may additionally require $x \in [mn]$. It remains to check that $x \perp mn$.

  So let $d = \gcd(x, mn)$. If $d > 1$, then there is a positive prime p such that $p \mid x$ and $p \mid mn$. But then $p \mid m$ or $p \mid n$, meaning that either $p \mid \gcd(x, m)$ or $p \mid \gcd(x, n)$. But $x \equiv a \bmod m$, so $\gcd(x, m) = \gcd(a, m)$; and likewise $\gcd(x, n) = \gcd(b, n)$. So this contradicts the assumption that $a \perp m$ and $b \perp n$. Hence $x \perp mn$ after all.

  ◇ **Uniqueness.** Suppose $x, y \in C_{mn}$ both satisfy the two congruences in question. By the Chinese remainder theorem, we have $x \equiv y \bmod mn$, and hence $x = y + kmn$ for some $k \in \mathbb{Z}$. Since $x, y \in [mn]$, we have

  $$|k|mn = |kmn| = |x - y| \leqslant mn - 1 < mn$$

  This implies $|k| < 1$, so that $k = 0$ and $x = y$.

  so f is well-defined.

- **f is injective.** Let $a, a' \in C_m$ and $b, b' \in C_n$, and suppose that $f(a, b) = f(a', b')$. Then there is an element $x \in C_{mn}$ such that

  $$\begin{cases} x \equiv a \bmod m \\ x \equiv a' \bmod m \\ x \equiv b \bmod n \\ x \equiv b' \bmod n \end{cases}$$

  Hence $a \equiv a' \bmod m$ and $b \equiv b' \bmod n$. Since $a, a' \in [m]$ and $b, b' \in [n]$, we must have $a = a'$ and $b = b'$.

- **f is surjective.** Let $x \in C_{mn}$. Let $a \in [m]$ and $b \in [n]$ be the (unique) elements such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$, respectively. If $a \in C_m$ and $b \in C_n$, then we'll have $f(a,b) = x$ by construction, so it remains to check that $a \perp m$ and $b \perp n$.

  Suppose $d \in \mathbb{Z}$ with $d \mid a$ and $d \mid m$. We prove that $d = 1$. Since $x \equiv a \bmod m$, we have $d \mid x$ by Theorem 3.1.17. Since $m \mid mn$, we have $d \mid mn$. By definition of greatest common divisors, it follows that $d \mid \gcd(x, mn)$. But $\gcd(x, mn) = 1$, so that d is a unit, and so $a \perp m$ as required.

  The proof that $b \perp n$ is similar.

It was a lot of work to check that it worked, but we have defined a bijection $f : C_m \times C_n \to C_{mn}$. By the multiplication principle, we have

$$\varphi(m)\varphi(n) = |C_m| \cdot |C_n| = |C_m \times C_n| = |C_{mn}| = \varphi(mn)$$

as required. $\qquad \square$

Exercise 4.2.56
Let $n \in \mathbb{Z}$ and let $p > 0$ be prime. Prove that if $p \mid n$, then $\varphi(pn) = p \cdot \varphi(n)$. Deduce that $\varphi(p^k) = p^k - p^{k-1}$ for all prime $p > 0$ and all $k \geqslant 1$. $\quad \triangleleft$

Theorem 4.2.57 (Formula for Euler's totient function)
Let n be a nonzero integer. Then

$$\varphi(n) = |n| \cdot \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

where the product is indexed over positive primes p dividing n

---

Proof. Since $\varphi(n) = \varphi(-n)$ for all $n \in \mathbb{Z}$, we may assume that $n > 0$. Moreover

$$\varphi(1) = 1 = 1 \cdot \prod_{p \mid 1} \left(1 - \frac{1}{p}\right)$$

Note that the product here is empty, and hence equal to 1, since there are no positive primes p which divide 1. So now suppose $n > 1$.

Using the fundamental theorem of arithmetic (Theorem 3.2.12), we can write

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

for primes $0 < p_1 < p_2 < \cdots < p_r$ and natural numbers $k_1, k_2, \ldots, k_r \geqslant 1$.

By repeated application of Theorem 4.2.55, we have

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{k_i})$$

By Exercise 4.2.56, we have

$$\varphi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i-1} = p_i^{k_i}\left(1 - \frac{1}{p_i}\right)$$

Combining these two results, it follows that

$$\varphi(n) = \prod_{i=1}^{r} p_i^{k_i}\left(1 - \frac{1}{p_i}\right) = \left(\prod_{i=1}^{r} p_i^{k_i}\right)\left(\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)\right) = n \cdot \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

which is as required.   □

Inclusion–exclusion principle

The addition principle is useful only for counting unions of *pairwise disjoint* sets, i.e. sets that do not overlap. We saw in Proposition 4.2.5 how to compute the size of a union of two sets which *do* overlap:

$$|X \cup Y| = |X| + |Y| - |X \cap Y|$$

So far so good. But what if we have three or four sets instead of just two?

Exercise 4.2.58
Let X, Y, Z be sets. Show that

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|$$

Let W be another set. Derive a similar formula for $|W \cup X \cup Y \cup Z|$.   ◁

The inclusion–exclusion principle generalises Exercise 4.2.58 to arbitary finite collections of finite sets.

Theorem 4.2.59 (Inclusion–exclusion principle)
Let $n \geqslant 2$ and let $X_1, X_2, \ldots, X_n$ be sets. Then

$$\left|\bigcup_{i=1}^{n} X_i\right| = \sum_{J \subseteq [n]} (-1)^{|J|+1} \left|\bigcap_{j \in J} X_j\right|$$

where for the purposes of the formula we take $\bigcap_{j \in \varnothing} X_j = \varnothing$.

Proof. We proceed by induction.

- (**BC**) The proof for the case $n = 2$ was Proposition 4.2.5.

- (**IS**) Fix $n \geqslant 2$ and suppose, for any sets $X_1, X_2, \ldots, X_n$, that

$$\left| \bigcup_{i=1}^{n} X_i \right| = \sum_{J \subseteq [n]} (-1)^{|J|+1} \left| \bigcap_{j \in J} X_j \right| \qquad\qquad -(\textbf{IH})$$

We need to prove that, for any sets $X_1, X_2, \ldots, X_n, X_{n+1}$, that

$$\left| \bigcup_{i=1}^{n+1} X_i \right| = \sum_{J \subseteq [n+1]} (-1)^{|J|+1} \left| \bigcap_{j \in J} X_j \right|$$

Write $U = \bigcup_{i=1}^{n} X_i$. We know that

$$|U \cup X_{n+1}| = |U| + |X_{n+1}| - |U \cap X_{n+1}| \qquad\qquad -(\star)$$

Now by (**IH**) we know $|U|$ straight away:

$$|U| = \sum_{J \subseteq [n]} (-1)^{|J|+1} \left| \bigcap_{j \in J} X_j \right|$$

This covers the sizes of all the $J \subseteq [n+1]$ for which $n+1 \notin J$.

Note that $U \cap X_{n+1} = \bigcap_{i=1}^{n} X_i \cap X_{n+1}$. Applying (**IH**) again we get

$$- |U \cap X_{n+1}|$$

$$= - \sum_{J \subseteq [n]} (-1)^{|J|+1} \left| \left(\bigcap_{j \in J} X_j \right) \cap X_{n+1} \right| \qquad \text{by (\textbf{IH})}$$

$$= - \sum_{J \subseteq [n]} (-1)^{|J \cup \{n+1\}|} \left| \bigcap_{j \in J \cup \{n+1\}} X_j \right| \qquad \text{re-indexing the sum}$$

$$= \sum_{J \subseteq [n]} (-1)^{|J \cup \{n+1\}|+1} \left| \bigcap_{j \in J \cup \{n+1\}} X_j \right| \qquad \text{distributing the } - \text{sign}$$

This covers the sizes of all the $J \subseteq [n+1]$ for which $n + 1 \in J$ *and* which contain some element of $[n]$.

The only subset of $[n+1]$ not covered by the above two sums is $\{n+1\}$, and $(-1)^{|\{n+1\}|+1} = (-1)^2 = 1$, so that

$$(-1)^{|\{n+1\}|+1} |X_{n+1}| = |X_{n+1}|$$

Together with $(\star)$, this yields the equation we wanted to prove was true.

By induction, we're done. $\square$

Proof tip

To find the size of a union of $\bigcup_{i=1}^{n} X_i$:

- Add the sizes of the individual sets X_i;

- Subtract the sizes of the double-intersections $X_i \cap X_j$;

- Add the sizes of the triple-intersections $X_i \cap X_j \cap X_k$;

- Subtract the sizes of the quadruple-intersections $X_i \cap X_j \cap X_k \cap X_\ell$;

- ...and so on ...

Keep alternating until the intersection of all the sets is covered. $\triangleleft$

Example 4.2.60

We count how many subsets of $[12]$ contain a multiple of 3. Precisely, we count the number of elements of the set

$$X_3 \cup X_6 \cup X_9 \cup X_{12}$$

where $X_k = \{S \subseteq [12] \mid k \in S\}$. We will apply the inclusion–exclusion principle:

(i) An element $S \in X_3$ is precisely a set of the form $\{3\} \cup S'$, where $S' \subseteq [12] \setminus \{3\}$. Since $[12] \setminus \{3\}$ has 11 elements, there are 2^{11} such subsets. So $|X_3| = 2^{11}$, and likewise $|X_6| = |X_9| = |X_{12}| = 2^{11}$.

(ii) An element $S \in X_3 \cap X_6$ is a set of the form $\{3, 6\} \cup S'$, where $S' \subseteq [12] \setminus \{3, 6\}$. Thus there are 2^{10} such subsets, so $|X_3 \cap X_6| = 2^{10}$. And likewise

$$|X_3 \cap X_9| = |X_3 \cap X_{12}| = |X_6 \cap X_9| = |X_6 \cap X_{12}| = |X_9 \cap X_{12}| = 2^{10}$$

(iii) Reasoning as in the last two cases, we see that

$$|X_3 \cap X_6 \cap X_9| = |X_3 \cap X_6 \cap X_{12}| = |X_3 \cap X_9 \cap X_{12}| = |X_6 \cap X_9 \cap X_{12}| = 2^9$$

(iv) ...and $|X_3 \cap X_6 \cap X_9 \cap X_{12}| = 2^8$.

Thus the number of subsets of $[12]$ which contain a multiple of 3 is

$$\underbrace{4 \times 2^{11}}_{\text{by (i)}} \quad - \quad \underbrace{6 \times 2^{10}}_{\text{by (ii)}} \quad + \quad \underbrace{4 \times 2^9}_{\text{by (iii)}} \quad - \quad \underbrace{2^8}_{\text{by (iv)}}$$

which is equal to 3840.   ◁

Exercise 4.2.61
How many natural numbers less than 1000 are multiples of 2, 3, 5 or 7?   ◁

Exercise 4.2.62
Recall the definition of the *totient* of an integer n (Definition 3.3.31). Use the inclusion–exclusion principle to show that $\varphi(100) = 40$. Use this fact to prove that the last two digits of 3^{79} are '67'.   ◁

4.3   Infinite sets

Indexed families of sets

We begin this section by generalising the indexed union, intersection and product notation that we saw in Section 4.2 (page 4.2).

Definition 4.3.1
Let I be a set. A **family of sets indexed by** I is a choice, for each $i \in I$ of a set X_i. We write $\{X_i \mid i \in I\}$ for the set of such choices.

Definition 4.3.2
Let $\{X_i \mid i \in I\}$ be a family of sets indexed by some set I. We define...

- ...the **indexed union** of $\{X_i \mid i \in I\}$ is the set $\bigcup_{i \in I} X_i$ defined by

$$\bigcup_{i \in I} X_i = \{x \mid x \in X_i \text{ for some } i \in I\}$$

- ...the **indexed intersection** of $\{X_i \mid i \in I\}$ is the set $\bigcap_{i \in I} X_i$ defined by

$$\bigcap_{i \in I} X_i = \{x \mid x \in X_i \text{ for all } i \in I\}$$

- ...the **indexed product** of $\{X_i \mid i \in I\}$ is the set $\prod_{i \in I} X_i$ defined by

$$\prod_{i \in I} X_i = \{(x_i)_{i \in I} \mid x_i \in X_i \text{ for all } i \in I\}$$

The elements $(x_i)_{i \in I}$ of $\prod_{i \in I} X_i$ are **ordered I-tuples**. Formally, an ordered I-tuple is a function $f : I \to \bigcup_{i \in I} X_i$ such that $f(i) \in X_i$ for all $i \in I$—then x_i is just shorthand for $f(i)$.

Note that when all the sets X_i are equal to some set X, the product $\prod_{i \in I} X$ is exactly the set X^I of functions $I \to X$.

Example 4.3.3
Let X be a set, and for each $n \in \mathbb{N}$, let S_n be the set of subsets of X of size n. Then

$$\bigcup_{n \in \mathbb{N}} S_n$$

is the set F of all finite subsets of X. Indeed:

- ($\subseteq$). Let $U \in \bigcup_{n \in \mathbb{N}} S_n$. Then $U \in S_n$ for some $n \in \mathbb{N}$, so that $U \subseteq X$ and U is finite (and $|U| = n$). Hence $U \in F$.

- ($\supseteq$). Let $U \in F$. Then $U \subseteq X$ is finite, so that $U \in S_{|U|}$, and hence $U \in \bigcup_{n \in \mathbb{N}} S_n$.

◁

Exercise 4.3.4
Find a family $\{U_n \mid n \in \mathbb{N}\}$ of subsets of $\mathbb{N}$ such that

- $U_m \cap U_n$ is infinite for all $m, n \in \mathbb{N}$; but

- $\bigcap_{n \in \mathbb{N}} U_n$ is empty.

◁

We can use this new indexed union and intersection notation to prove a general version of de Morgan's laws for sets.

Theorem 4.3.5 (De Morgan's laws for sets)
Let Z be a set and let $\{X_i \mid i \in I\}$ be an indexed family of sets. Then
(a) $Z \setminus \bigcup_{i \in I} X_i = \bigcap_{i \in I}(Z \setminus X_i)$;

(b) $Z \setminus \bigcap_{i \in I} X_i = \bigcup_{i \in I}(Z \setminus X_i)$.

Proof 1 of (a). In this proof, we prove (a) directly by unpacking the definitions of relative complement, indexed union and indexed intersection.

Fix z. Note that $z \in Z \setminus \bigcup_{i \in I} X_i$ if and only if

$$z \in Z \wedge \neg \left(z \in \bigcup_{i \in I} X_i \right)$$

by definition of relative complement. This holds if and only if

$$z \in Z \wedge \neg(\exists i \in I, z \in X_i)$$

by definition of indexed union. This holds if and only if

$$z \in Z \wedge \forall i \in I, z \notin X_i$$

by De Morgan's laws for quantifiers (Theorem 2.1.46). Since the proposition $z \in Z$ doesn't depend on i, this holds if and only if

$$\forall i \in I, \, (z \in Z \wedge z \notin X_i)$$

which is precisely the statement that $z \in \bigcap_{i \in I}(Z \setminus X_i)$. □

Proof 2 of (a). In this proof, we prove (a) by a double-containment argument.

- $Z \setminus \bigcup_{i \in I} X_i \subseteq \bigcap_{i \in I}(Z \setminus X_i)$.

  Let $z \in Z \setminus \bigcup_{i \in I} X_i$. We know that $z \in Z$ and $z \notin \bigcup_{i \in I} X_i$. We need to prove that $z \in \bigcap_{i \in I}(Z \setminus X_i)$; that is, we need to prove that, for all $i \in I$, we have $z \in Z \setminus X_i$; that is, $z \in Z$ and $z \notin X_i$. We have $z \in Z$ for free, so all we have to prove is that, for all $i \in I$, $z \notin X_i$.

  So let $i \in I$. If $z \in X_i$ then $z \in \bigcup_{i \in I} X_i$, contradicting the fact that $z \notin \bigcup_{i \in I} X_i$. Therefore it must be the case that $z \notin X_i$. This finishes this half of the proof.

- $Z \setminus \bigcup_{i \in I} X_i \supseteq \bigcap_{i \in I}(Z \setminus X_i)$.

  Let $z \in \bigcap_{i \in I}(Z \setminus X_i)$. We know that, for all $i \in I$, $z \in Z \setminus X_i$. Hence it's certainly true that $z \in Z$. To prove that $z \in Z \setminus \bigcup_{i \in I} X_i$, it remains to prove that $z \notin \bigcup_{i \in I} X_i$.

  Suppose $z \in \bigcup_{i \in I} X_i$. Then $z \in X_i$ for some $i \in I$. Since we already know that $z \in Z$, it follows that $z \notin Z \setminus X_i$, contradicting the fact that $z \in Z \setminus X_i$ for all $i \in I$. This finishes the second half of the proof.

We have shown containment in both directions, hence equality. □

Sizes of finite sets revisited

We have seen how to use injections, surjections and bijections to study the relative size of sets:

- If $f : X \to Y$ is injective, then $|X| \leqslant |Y|$;

- If $f : X \to Y$ is surjective, then $|X| \geqslant |Y|$;

- If $f : X \to Y$ is bijective, then $|X| = |Y|$.

Recall Definition 4.1.39, where we said a set X is *finite* if there is a bijection $[n] \to X$ for some $n \in \mathbb{N}$. The next definition takes this one step further.

> **Definition 4.3.6**
> A set X is **countably infinite** if there exists a bijection $\mathbb{N} \to X$. We say X is **countable** if it is finite or countably infinite.

Thus a set X is countably infinite if its elements can be *listed*, with one entry in the list for each natural number.

Example 4.3.7
We have already seen many examples of countably infinite sets.

- The set $\mathbb{N}$ is countably infinite, since by Exercise 4.1.15, $\mathrm{id}_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$ is a bijection.

- The function $f : \mathbb{Z} \to \mathbb{N}$ defined for $x \in \mathbb{Z}$ by

$$f(x) = \begin{cases} 2x & \text{if } x \geqslant 0 \\ -(2x+1) & \text{if } x < 0 \end{cases}$$

  is a bijection. Indeed, it has an inverse is given by

$$f^{-1}(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ -\frac{x+1}{2} & \text{if } x \text{ is odd} \end{cases}$$

  Hence the set of integers $\mathbb{Z}$ is countably infinite. The corresponding list of integers is given by

$$0, \ -1, \ 1, \ -2, \ 2, \ -3, \ 3, \ -4, \ 4, \ \ldots$$

  The fact that f^{-1} is a bijection means that each integer appears on this list exactly once.

◁

Exercise 4.3.8
Prove that the function $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $p(x, y) = 2^x(2y+1) - 1$ is a bijection. Deduce that if X and Y are countably infinite sets, then $X \times Y$ is countably infinite. ◁

Exercise 4.3.8 allows us to prove that the product of finitely many countably infinite sets are countably infinite.

Exercise 4.3.9
Let $f : X \to Y$ be a bijection. Prove that X is countably infinite if and only if Y is countably infinite. ◁

Proposition 4.3.10

Let $n \geqslant 1$ and let $X_1, \ldots, X_n$ be countably infinite sets. Then the product $\prod_{i=1}^{n} X_i$ is countably infinite.

Proof. We proceed by induction on n.

- (**BC**) When $n = 1$ the assertion is trivial: if X_1 is countably infinite then X_1 is countably infinite.

- (**IS**) Fix $n \geqslant 1$ and suppose that for any sets $X_1, \ldots, X_n$, the product $\prod_{i=1}^{n} X_i$ is countably infinite. Fix sets $X_1, \ldots, X_{n+1}$. Then $\prod_{i=1}^{n} X_i$ is countably infinite by the induction hypothesis, and X_{n+1} is countably infinite by assumption, so by Exercise 4.3.8, the set

$$\left(\prod_{i=1}^{n} X_i \right) \times X_{n+1}$$

  is countably infinite. But by Exercise 4.2.14 there is a bijection

$$\prod_{i=1}^{n+1} X_i \rightarrow \left(\prod_{i=1}^{n} X_i \right) \times X_{n+1}$$

  and so by Exercise 4.3.9 we have that $\prod_{i=1}^{n+1} X_i$ is countably infinite, as required.

By induction, we're done. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Finding a *bijection* $\mathbb{N} \rightarrow X$, or equivalently $X \rightarrow \mathbb{N}$, can be a bit of a hassle. However, in order to prove that a set X is countable, it suffices to find either a surjection $\mathbb{N} \rightarrow X$ or an injection $X \rightarrow \mathbb{N}$.

Theorem 4.3.11

Let X be an inhabited set. The following are equivalent:

(i) X is countable;

(ii) There exists a surjection $f : \mathbb{N} \rightarrow X$;

(iii) There exists an injection $f : X \rightarrow \mathbb{N}$.

Proof. We'll prove (i)⇔(ii) and (i)⇔(iii).

- (i)$\Rightarrow$(ii). Suppose X is countable. If X is countably infinite, then there exists a bijection $f : \mathbb{N} \to X$, which is a surjection. If X is finite then there exists a bijection $g : [m] \to X$, where $m = |X| \geqslant 1$. Define $f : \mathbb{N} \to X$ by

$$f(n) = \begin{cases} g(n) & \text{if } 1 \leqslant n \leqslant m \\ g(1) & \text{if } n = 0 \text{ or } n > m \end{cases}$$

  Then f is surjective: if $x \in X$ then there exists $n \in [m]$ such that $g(n) = x$, and then $f(n) = g(n) = x$.

- (ii)$\Rightarrow$(i). Suppose there exists a surjection $f : \mathbb{N} \to X$. To prove that X is countable, it suffices to prove that if X is infinite then it is countably infinite. So suppose X is infinite, and define a sequence recursively by

  ⋄ $a_0 = 0$;
  ⋄ Fix $n \in \mathbb{N}$ and suppose $a_0, \ldots, a_n$ have been defined. Define a_{n+1} to be the least natural number for which $f(a_{n+1}) \notin \{f(a_0), f(a_1), \ldots, f(a_n)\}$.

  Define $g : \mathbb{N} \to X$ by $g(n) = f(a_n)$ for all $n \in \mathbb{N}$. Then

  ⋄ g is injective, since if $m \leqslant n$ then $f(a_m) \neq f(a_n)$ by construction of the sequence $(a_n)_{n \in \mathbb{N}}$.
  ⋄ g is surjective. Indeed, given $x \in X$, by surjectivity there exists $m \in \mathbb{N}$ which is least such that $f(m) = x$, and we must have $a_n = m$ for some $n \leqslant m$ by construction of the sequence $(a_n)_{n \in \mathbb{N}}$. So $x = g(a_n)$, and hence g is surjective.

  So g is a bijection, and X is countable.

- (i)$\Rightarrow$(iii). Suppose X is countable. If X is countably infinite, then there exists a bijection $f : \mathbb{N} \to X$, so $f^{-1} : X \to \mathbb{N}$ is bijective and hence injective. If X is finite then there exists a bijection $g : [m] \to X$, where $m = |X| \geqslant 1$. Then $g^{-1} : X \to [m]$ is injective. Let $i : [m] \to \mathbb{N}$ be defined by $i(k) = k$ for all $k \in [m]$. Then $i \circ g^{-1}$ is injective; indeed, for $x, x' \in X$ we have

$$i(g^{-1}(x)) = i(g^{-1}(x')) \Rightarrow g^{-1}(x) = g^{-1}(x') \Rightarrow x = x'$$

  The first implication is by definition of i, and the second is by injectivity of g^{-1}. So there exists an injection $X \to \mathbb{N}$.

- (iii)$\Rightarrow$(i). Suppose there exists an injection $f : X \to \mathbb{N}$. To prove that X is countable, it suffices to prove that if X is infinite then it is countably infinite. Define a sequence $(a_n)_{n \in \mathbb{N}}$ recursively as follows:

  ⋄ Let a_0 be the least element of $f[X]$;

231

◇ Fix $n \in \mathbb{N}$ and suppose $a_0, \ldots, a_n$ have been defined. Let a_{n+1} be the least element of $f[X] \setminus \{a_0, \ldots, a_n\}$. This exists since f is injective, so $f[X]$ is infinite.

Define $g : \mathbb{N} \to X$ by, for each $n \in \mathbb{N}$, letting $g(n)$ be the unique value of x for which $f(x) = a_n$. Then

◇ g is injective. By construction $a_m \neq a_n$ whenever $m \neq n$. Let $x, y \in X$ be such that $f(x) = a_m$ and $f(y) = a_n$. Since f is injective, we must have $x \neq y$, and so $g(m) = x \neq y = g(n)$.

◇ g is surjective. Fix $x \in X$. Then $f(x) \in f[X]$, so there exists $m \in \mathbb{N}$ such that $f(x) = a_m$. Hence $g(m) = x$.

So g is a bijection, and X is countably infinite.

Hence the equivalences have been proved.   □

In fact, we needn't even use $\mathbb{N}$ as the domain of the surjection or the codomain of the injection; we can in fact use any countable set C.

Corollary 4.3.12
Let X be an inhabited set. The following are equivalent:

(a) X is countable;

(b) There exists a surjection $f : C \to X$ for some countable set C;

(c) There exists an injection $f : X \to C$ for some countable set C.

Exercise 4.3.13
Prove Corollary 4.3.12.   ◁

Corollary 4.3.12 is useful for proving the countability of many other sets: as we build up our repertoire of countable sets, all we need to do in order to prove a set X is countable is find a surjection from a set we already know is countable to X, or an injection from X into a set we already know is countable.

Example 4.3.14
$\mathbb{Q}$ is countable. Indeed, by Exercises 4.3.7 and 4.3.8, the set $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is countable. Moreover, there exists a surjection $q : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ defined by

$$q(a, b) = \frac{a}{b}$$

By Corollary 4.3.12, $\mathbb{Q}$ is countable.   ◁

Exercise 4.3.15

Let X be a countable set. Prove that $\binom{X}{k}$ is countable for each $k \in \mathbb{N}$. ◁

Theorem 4.3.16

A countable union of countable sets is countable. More precisely, let $\{X_n \mid n \in \mathbb{N}\}$ be a family of countable sets. Then the set X defined by

$$X = \bigcup_{n \in \mathbb{N}} X_n$$

is countable.

Proof. We may assume that the sets X_n are all inhabited, since the empty set does not contribute to the union.

For each $n \in \mathbb{N}$ there is a surjection $f_n : \mathbb{N} \to X_n$. Define $f : \mathbb{N} \times \mathbb{N} \to X$ by $f(m, n) = f_m(n)$ for all $m, n \in \mathbb{N}$. Then f is surjective: if $x \in X$ then $x \in X_m$ for some $m \in \mathbb{N}$. Since f_m is surjective, it follows that $x = f_m(n)$ for some $n \in \mathbb{N}$. But then $x = f(m, n)$. Since $\mathbb{N} \times \mathbb{N}$ is countable, it follows from Corollary 4.3.12 that X is countable. $\square$

Example 4.3.17

Let X be a countable set. The set of all finite subsets of X is countable. Indeed, the set of all finite subsets of X is equal to $\bigcup_{k \in \mathbb{N}} \binom{X}{k}$, which is a union of countably many countable sets by Exercise 4.3.15, so is countable by Theorem 4.3.16. ◁

We can also use some clever trickery to prove that certain sets are *uncountable*. The proof of the following theorem is known as **Cantor's diagonal argument**.

Theorem 4.3.18

The set $\{0, 1\}^{\mathbb{N}}$ is uncountable.

Proof. Let $f : \mathbb{N} \to \{0, 1\}^{\mathbb{N}}$ be a function. We will prove that f is not surjective by constructing a sequence which is not contained in the image of $\mathbb{N}$ under f.

Define an element $b \in \{0, 1\}^{\mathbb{N}}$, i.e. a function $b : \mathbb{N} \to \{0, 1\}$, by

$$b(n) = 1 - f(n)(n)$$

Then $b(n) \neq f(n)(n)$ for all $n \in \mathbb{N}$. If $b = f(m)$ for some m, then by definition of function equality we must have $b(m) = f(m)(m)$; but we just saw that this is necessarily false. Hence $b \notin f[\mathbb{N}]$, so f is not surjective.

Hence there does not exist a surjective function $\mathbb{N} \to \{0,1\}^{\mathbb{N}}$. By Theorem 4.3.11, the set $\{0,1\}^{\mathbb{N}}$ is uncountable. □

This result can be used to show that the set $\mathbb{R}$ of all real numbers is uncountable, though this relies on features of the real numbers that we have not developed so far in this course.

Exercise 4.3.19
Let X be a set. Prove that $\mathcal{P}(X)$ is either finite or uncountable. ◁

Chapter 5

Relations

5.1   Relations

When sets were first introduced in Section 2.2, after slewing through several definitions of set operations and set algebra, you probably wondered why you'd ever decided to embark on your journey into pure mathematics. It may have seemed at first like sets were introduced solely to shorten notation—for instance, instead of saying 'n is an integer but not a natural number', we could simply write '$n \in \mathbb{Z} \setminus \mathbb{N}$'.

But we soon saw that sets are powerful tools, which can be used to prove interesting results and solve difficult problems, largely with the help of *functions*. When we stopped studying sets in isolation, and started seeing how they interact with each other using functions in Section 2.3, their true power became apparent.

This section introduces the notion of a *relation*, which generalises that of a function.

Definition 5.1.1

Let X and Y be sets. A (**binary**) **relation** from X to Y is a logical formula $R(x,y)$ with two free variables x, y, where x has range X and y has range Y. We call X the **domain** of R and Y the **codomain** of R.

Given $x \in X$ and $y \in Y$, if $R(x,y)$ is true then we say 'x is **related** to y by R', and write $x \ R \ y$ (LaTeX code: `x\; R\; y`).[a]

---
[a]The LaTeX code `\;` inserts a small space: we use it because '$x \ R \ y$' looks better and clearer than 'xRy'.

In more human terms, a relation from X to Y is a statement about a generic element $x \in X$ and a generic element $y \in Y$, which is either true or false depending on the values of x and y.

Example 5.1.2

We have seen many examples of relations so far. For example:

- Every function $f : X \to Y$ defines a relation R_f from X to Y by letting

$$x \ R_f \ y \quad \Leftrightarrow \quad f(x) = y$$

- Given a set X, equality between elements of X ('$x = y$') is a relation from X to X.

- Divisibility ('$x \mid y$') is a relation from $\mathbb{Z}$ to $\mathbb{Z}$.

- For fixed $n \in \mathbb{Z}$, congruence modulo n ('$x \equiv y \bmod n$') is a relation from $\mathbb{Z}$ to $\mathbb{Z}$.

- Order ('$x \leqslant y$') is a relation from $\mathbb{N}$ to $\mathbb{N}$, or from $\mathbb{Z}$ to $\mathbb{Z}$, or from $\mathbb{Q}$ to $\mathbb{Q}$, and so on.

- Given sets X and Y, there is an **empty relation** $\varnothing_{X,Y}$ from X to Y, which is defined simply by declaring $\varnothing_{X,Y}(x,y)$ to be false for all $x \in X$ and $y \in Y$.

◁

Exercise 5.1.3

Define a relation R from $\mathbb{Z}$ to $\mathbb{Z}$ which is not on the list given in Example 5.1.2.   ◁

It is possible, and extremely useful, to represent relations as sets. We do this by defining the *graph* of a relation, which is the set of all pairs of elements which are related by the relation. You might recognise this as being similar to the graph of a *function* (Definition 2.3.12).

Definition 5.1.4

Let X and Y be sets, and let R be a relation from X to Y. The **graph** of R is the set $\mathrm{Gr}(R)$ (LaTeX code: `\mathrm{Gr}{R}`) of pairs $(x,y) \in X \times Y$ for which $x\,R\,y$. That is

$$\mathrm{Gr}(R) = \{(x,y) \in X \times Y \mid x\,R\,y\} \subseteq X \times Y$$

Example 5.1.5

Consider the relation of divisibility from $\mathbb{Z}$ to $\mathbb{Z}$, that is $R(x,y)$ is the statement $x \mid y$. The graph $\mathrm{Gr}(R)$ of R is the set whose elements are all pairs (m,n) where $m, n \in \mathbb{Z}$ and $m \mid n$. For example, $(2,6) \in \mathrm{Gr}(R)$ since $2 \mid 6$, but $(2,7) \notin \mathrm{Gr}(R)$ since $2 \nmid 7$.

Since $m \mid n$ if and only if $n = qm$ for some $q \in \mathbb{Z}$, we thus have

$$\mathrm{Gr}(R) = \{(m, qm) \mid m, q \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$$

◁

Exercise 5.1.6

Let X and Y be sets. What is the graph of the empty relation from X to Y?   ◁

Exercise 5.1.7

Let $f : X \to Y$ be a function, and define the relation R_f from X to Y as in Example 5.1.2. Prove that $\mathrm{Gr}(R_f) = \mathrm{Gr}(f)$—that is, the graph of the *relation* R_f is equal to the graph of the *function* f.   ◁

As with functions, the graph of a relation R from a set X to a set Y can often be represented graphically: draw a pair of axes, with the horizontal axis representing the elements of X and the vertical axis representing the elements of Y, and plot the point (x,y) if and only if $R(x,y)$ is true.

Example 5.1.8

Consider the relation S from $\mathbb{R}$ to $\mathbb{R}$ defined by $x \, S \, y \Leftrightarrow x^2 + y^2 = 1$. Then

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

Plotting $\mathrm{Gr}(S)$ on a standard pair of axes yields a circle with radius 1 centred at the point $(0, 0)$. Note that $\mathrm{Gr}(S)$ is *not* the graph of a function $s : [0, 1] \to \mathbb{R}$. Indeed, since for example both $0 \, S \, 1$ and $0 \, S \, {-1}$, the value $s(0)$ would not be uniquely defined.   ◁

Example 5.1.9

Let X be a set. The graph of the equality relation from X to X is very simple:

$$\mathrm{Gr}(=) = \{(x, y) \in X \times X \mid x = y\} = \{(x, x) \mid x \in X\} \subseteq X \times X$$

This set is often denoted Δ_X (LaTeX code: `\Delta_{X}`), and called the **diagonal subset** of $X \times X$. The reason for the word 'diagonal' is because—provided the horizontal and vertical axes have the same ordering of the elements of X—the points plotted are precisely those on the diagonal line.   ◁

Since we defined relations as particular logical formulae, and we have not defined a notion of equality between logical formulae, if we want to say that two relations are equal then first we need to define what we mean by *equal*. As with sets, this raises some subtleties: should two relations be equal when they're described by the same formula? Or should two relations be equal when they relate the same elements, even if their underlying descriptions are somewhat different? As with equality between sets (Definition 2.2.20), our notion of equality between relations will be *extensional*: for the purposes of deciding whether two relations are equal, we forget their descriptions and look only at whether or not they relate the same pairs elements.

Definition 5.1.10

Let X and Y be sets, and let R and S be relations from X to Y. We say R and S are **equal**, and write $R = S$, if

$$\forall x \in X, \forall y \in Y, (x \, R \, y \Leftrightarrow x \, S \, y)$$

That is, $R = S$ if they relate exactly the same pairs of elements.

Note that two relations R and S from a set X to a set Y are equal as relations if and only if their graphs $\mathrm{Gr}(R)$ and $\mathrm{Gr}(S)$ are equal as sets. This fact, together with the correspondence between relations from X to Y and subsets of $X \times Y$ (Theorem 5.1.11 below) is incredibly convenient, because it makes the notion of a relation more concrete.

> **Theorem 5.1.11**
> Let X and Y be sets. Any subset $G \subseteq X \times Y$ is the graph of exactly one relation R from X to Y.

Proof. Fix $G \subseteq X \times Y$. Define a relation R by

$$\forall x \in X, \, \forall y \in Y, \, x \, R \, y \Leftrightarrow (x, y) \in G$$

Then certainly $G = \mathrm{Gr}(R)$.

Moreover, if S is a relation from X to Y such that $G = \mathrm{Gr}(S)$, then, for all $x \in X$ and $y \in Y$

$$x \, S \, y \Leftrightarrow (x, y) \in \mathrm{Gr}(S) \Leftrightarrow (x, y) \in \mathrm{Gr}(R) \Leftrightarrow x \, R \, y$$

so $S = R$. Hence there is exactly one relation from X to Y whose graph is G. $\qquad\square$

Theorem 5.1.11 allows us to use the counting principles from Section 4.2 to find the number of relations from one finite set to another.

Exercise 5.1.12
Let X and Y be finite sets with $|X| = m$ and $|Y| = n$. Prove that there are 2^{mn} relations from X to Y. $\qquad\triangleleft$

Aside
It is very common to identify a relation with its graph, saying that a relation from a set X to a set Y 'is' a subset of $X \times Y$. This practice is justified by Theorem 5.1.11, which says precisely that there is a correspondence between relations from X to Y and subsets of $X \times Y$. $\qquad\triangleleft$

Relations on a set

In most of the examples of relations we've seen so far, the domain of the relation is equal to its codomain. The remainder of this section—in fact, the remainder of this *chapter*—is dedicated to such relations. So let's simplify the terminology slightly.

> **Definition 5.1.13**
> Let X be a set. A **relation on** X is a relation from X to X.

We have seen many such relations so far, such as: equality on any set, congruence modulo n on $\mathbb{Z}$, divisibility, on $\mathbb{Z}$ inclusion of subsets ($\subseteq$) on $\mathcal{P}(X)$, and comparison of size ($\leqslant$) on

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$. Remarkably, each of these relations can be characterised in one of two ways: either as an *equivalence relation* or as a *partial order*.

Equivalence relations are those that behave in some sense like equality, and partial orders are those that behave in some way like $\leqslant$.

- **Equality.** If X is any set, then equality on X satisfies:

    ⋄ Given $x \in X$, we have $x = x$;

    ⋄ Given $x, y \in X$, if $x = y$, then $y = x$;

    ⋄ Given $x, y, z \in X$, if $x = y$ and $y = z$, then $x = z$.

    Note that these are all true if we replace X by $\mathbb{Z}$ and $\cdot = \cdot$ by $\cdot \equiv \cdot \bmod n$ for some fixed $n > 0$.

- **Order.** If $X = \mathbb{N}$ (or $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$), then the order relation $\leqslant$ on X satisfies:

    ⋄ Given $x \in X$, we have $x \leqslant x$;

    ⋄ Given $x, y \in X$, if $x \leqslant y$ and $y \leqslant x$, then $x = y$;

    ⋄ Given $x, y, z \in X$, if $x \leqslant y$ and $y \leqslant z$, then $x \leqslant z$.

    Note that these are all true if we replace $(X, \leqslant)$ by $(\mathcal{P}(X), \subseteq)$ or $(\mathbb{N}, \mid)$.

For both equality and order, the first condition states that every element is related to itself, and the third condition states that in some sense we can cut out intermediate steps. These conditions are known as *reflexivity* and *transitivity*. The second condition for equality states that the direction of the relation doesn't matter; this condition is called *symmetry*. The second condition for the order relation states that the only way two objects can be related to each other in both directions is if they are equal; this condition is called *antisymmetry*.

The remainder of this section will develop the language needed to talk about equivalence relations and partial orders. We will finish the section with a discussion of equivalence relations, and then study partial orders in depth in Section 5.2.

Reflexive relations are those that relate everything to itself.

Definition 5.1.14

Let X be a set. A relation R on X is **reflexive** if $x \mathrel{R} x$ for all $x \in X$.

Example 5.1.15

Given a set X, the equality relation on X is reflexive since $x = x$ for all $x \in X$.   ◁

Example 5.1.16

The divisibility relation on $\mathbb{N}$, or on $\mathbb{Z}$, is reflexive. Given $n \in \mathbb{Z}$ we have $n = 1 \times n$, and so $n \mid n$. ◁

The following exercise demonstrates the importance of specifying the (co)domain of a relation: it shows that a logical formula may define a reflexive relation on one set, but not on another.

Exercise 5.1.17

Prove that coprimality ('$x \perp y$') is not a reflexive relation on $\mathbb{Z}$, but that it is a reflexive relation on the set $\{-1, 1\}$.

As such, it doesn't make sense to say 'coprimality is a reflexive relation' or 'coprimality is not a reflexive relation': we must specify on which set we are considering the coprimality relation. ◁

The result of the next exercise characterises reflexive relations in terms of their graph.

Exercise 5.1.18

Let X be a set and let R be a relation on X. Prove that R is reflexive if and only if $\Delta_X \subseteq \mathrm{Gr}(R)$, where Δ_X is the diagonal subset of $X \times X$ (see Example 5.1.9). Deduce that if X is finite and $|X| = n$, then there are $2^{n(n-1)}$ reflexive relations on X. ◁

Symmetric relations are those for which the *direction* of the relation doesn't matter.

Definition 5.1.19

Let X be a set. A relation R on X is **symmetric** if, for all $x, y \in X$, $x \, R \, y$ implies $y \, R \, x$.

Example 5.1.20

Some examples of symmetric relations include:

- Equality is a symmetric relation on any set X. Indeed, if $x, y \in X$ and $x = y$, then $y = x$.

- Coprimality is a symmetric relation on $\mathbb{Z}$, since if $a, b \in \mathbb{Z}$ then $a \perp b$ if and only if $b \perp a$.

- Divisibility is not a symmetric relation on $\mathbb{Z}$, since for instance $1 \mid 2$ but $2 \nmid 1$. However, divisibility *is* a symmetric relation on $\{-1, 1\}$, since $1 \mid -1$ and $-1 \mid 1$.

◁

Chapter 5. Relations

Exercise 5.1.21

Let X be a finite set with $|X| = n$. Prove that there are $2^{\binom{n}{2}} \cdot 2^n$ symmetric relations on X. ◁

A related condition a relation may possess is *antisymmetry.*

Definition 5.1.22

Let X be a set. A relation R on X is **antisymmetric** if, for all $x, y \in X$, if $x \, R \, y$ and $y \, R \, x$, then $x = y$.

A word of warning here is that 'antisymmetric' does not mean the same thing as 'not symmetric'—indeed, we we will see, equality is both symmetric and antisymmetric, and many relations are neither symmetric nor antisymmetric.[a]

Example 5.1.23

Some examples of antisymmetric relations include are as follows.

- Let X be a set. The equality relation on X is antisymmetric: it is immediate that if $x, y \in X$ and $x = y$ and $y = x$, then $x = y$.

- The relation $\leqslant$ on the set $\mathbb{N}$ (or $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$) is antisymmetric: if $m, n \in \mathbb{N}$ and $m \leqslant n$ and $n \leqslant m$, then $m = n$.

- The divisibility relation on $\mathbb{N}$ is antisymmetric. Indeed, let $m, n \in \mathbb{N}$ and suppose $m \mid n$ and $n \mid m$. Then $n = km$ for some $k \in \mathbb{Z}$ and $m = \ell n$ for some $\ell \in \mathbb{Z}$. It follows that $n = k\ell n$. If $n = 0$ then $m = n$ trivially; otherwise, we have $k\ell = 1$. Hence k is a unit; moreover, since $m, n \geqslant 0$ and $n = km$, we must have $k = 1$. Hence $m = n$.

◁

Exercise 5.1.24

Show that the divisibility relation on $\mathbb{Z}$ is not antisymmetric. ◁

Exercise 5.1.25

Let X be a set and let R be a relation on X. Prove that R is both symmetric and antisymmetric if and only if $\mathrm{Gr}(R) \subseteq \Delta_X$, where Δ_X is the diagonal subset of $X \times X$ (see Exercise 5.1.9). Deduce that the only reflexive, symmetric and antisymmetric relation on a set X is the equality relation on X. ◁

Exercise 5.1.26

Let X be a finite set with $|X| = n$. Prove that there are $3^{\binom{n}{2}} \cdot 2^n$ antisymmetric relations on X. ◁

---

[a] Even more confusingly, there is a notion of *asymmetric relation*, which also does not mean 'not symmetric'.

Transitivity is the property of $\leqslant$ that allows us to deduce, for example, that $0 \leqslant 4$, from the information that $0 \leqslant 1 \leqslant 2 \leqslant 3 \leqslant 4$.

Definition 5.1.27
Let X be a set. A relation R on X is **transitive** if, for all $x, y, z \in X$, if $x \mathrel{R} y$ and $y \mathrel{R} z$, then $x \mathrel{R} z$.

Example 5.1.28
Some examples of transitive relations include:

- Equality is a transitive relation on any set X, since it is immediate that if $x, y, z \in X$ with $x = y$ and $y = z$, then $x = z$.

- Divisibility is a transitive relation on $\mathbb{N}$, or on $\mathbb{Z}$. Indeed, if $a, b, c \in \mathbb{N}$ with $a \mid b$ and $b \mid c$, then there exist $k, \ell \in \mathbb{Z}$ such that $b = ka$ and $c = \ell b$. Then $c = (k\ell)a$, so $a \mid c$.

- Inclusion is a transitive relation on $\mathcal{P}(X)$, for any set X. Indeed, Proposition 2.2.11 implies that if $U, V, W \subseteq X$ with $U \subseteq V$ and $V \subseteq W$, then $U \subseteq W$.

$\triangleleft$

A fundamental property of transitive relations is that we can prove two elements a and b are related by finding a chain of related elements starting at a and finishing at b. This is the content of the following proposition.

Proposition 5.1.29
Let R be a relation on a set X. Then R is transitive if and only if, for any finite sequence $x_0, x_1, \ldots, x_n$ of elements of X such that $x_{i-1} \mathrel{R} x_i$ for all $i \in [n]$, we have $x_0 \mathrel{R} x_n$.

Proof. For the sake of abbreviation, let $p(n)$ be the assertion that, for any $n \geqslant 1$ and any sequence $x_0, x_1, \ldots, x_n$ of elements of X such that $x_{i-1} \mathrel{R} x_i$ for all $i \in [n]$, we have $x_0 \mathrel{R} x_n$.

We prove the two directions of the proposition separately.

- ($\Rightarrow$) Suppose R is transitive. For $n \geqslant 1$. We prove $p(n)$ is true for all $n \geqslant 1$ by induction.

    $\diamond$ (**BC**) When $n = 1$ this is immediate, since we assume that $x_0 \mathrel{R} x_1$.

244   *Chapter 5. Relations*

⋄ (**IS**) Fix $n \geqslant 1$ and suppose $p(n)$ is true. Let $x_0, \ldots, x_n, x_{n+1}$ is a sequence such that $x_{i-1} \ R \ x_i$ for all $i \in [n+1]$. We need to prove that $x_0 \ R \ x_{n+1}$.

By the induction hypothesis we know that $x_0 \ R \ x_n$. By definition of the sequence we have $x_n \ R \ x_{n+1}$. By transitivity, we have $x_0 \ R \ x_{n+1}$.

So by induction, we have proved the $\Rightarrow$ direction.

- ($\Leftarrow$) Suppose $p(n)$ is true for all $n \geqslant 1$. Then in particular $p(2)$ is true, which is precisely the assertion that R is transitive.

So we're done.   □

That is, Proposition 5.1.29 states that for a transitive relation R on a set X, if $x_0, x_1, \ldots, x_n \in X$, then

$$x_0 \ R \ x_1 \ R \ \cdots \ R \ x_n \quad \Rightarrow \quad x_0 \ R \ x_n$$

where '$x_0 \ R \ x_1 \ R \ \cdots \ R \ x_n$' abbreviates the assertion that $x_i \ R \ x_{i+1}$ for each $i < n$.

Exercise 5.1.30
For each of the eight subsets

$$P \subseteq \{\text{reflexive}, \text{symmetric}, \text{transitive}\}$$

find a relation satisfying (only) the properties in P.   ◁

Equivalence relations

We will now study what it is for a relation to be *equality-like*.

Definition 5.1.31
A relation R on a set X is an **equivalence relation** if R is reflexive, symmetric and transitive.

When we talk about arbitrary equivalence relations, we usually use a symbol like '$\sim$' (LaTeX code: `\sim`) or '$\equiv$' (LaTeX code: `\equiv`) or '$\approx$' (LaTeX code: `\approx`) instead of 'R'.

Example 5.1.32
We have seen two main examples of equivalence relations so far.

- Equality is an equivalence relation. The proof is immediate.

- Fix $n > 0$. Congruence modulo n is an equivalence relation on $\mathbb{Z}$; this was Theorem 3.3.6.

◁

Exercise 5.1.33

Define a relation $\sim$ on $\mathbb{Z}$ by declaring, for $m, n \in \mathbb{Z}$,

$$m \sim n \quad \Leftrightarrow \quad \varphi(m) = \varphi(n)$$

Prove that $\sim$ is an equivalence relation. ◁

Equivalence relations are useful because they allow us to ignore irrelevant information about elements of a set. As an example, to prove that, for $a \in \mathbb{Z}$, if $3 \nmid a$ then $a^2 \equiv 1 \bmod 3$, we could write $a = 3k \pm 1$ for some $k \in \mathbb{Z}$ and deduce that $a^2 = 3(3k^2 \pm 2k) + 1$. This requires us to use more information than we need: the value of k doesn't make any difference to the truth of the result, and the expression $3(3k^2 \pm 2k) + 1$ is frankly fairly ugly.

Definition 5.1.34

Let X be a set and let $\sim$ be an equivalence relation on X. The $\sim$-**equivalence class** of $x \in X$ is the set

$$[x]_\sim = \{y \in X \mid x \sim y\}$$

The **quotient** of X by $\sim$, denoted $X/\sim$, is the set of all $\sim$-equivalence classes of elements of X; that is

$$X/\sim = \{[x]_\sim \mid x \in X\}$$

Format tip

Putting braces ({ and }) around a symbol like $\sim$ tells LATEX to consider the symbol on its own, rather than in the context of its surrounding variables. Typing `X/\sim = Y` confuses LATEX slightly, since it thinks you're saying '$X/$ is related to is equal to Y', which clearly makes no sense; whereas typing `X/{\sim} = Y` signifies to LATEX that the $\sim$ symbol isn't relating anything. Compare:

$$X/\sim= Y \qquad \text{vs.} \qquad X/\sim = Y$$

◁

Example 5.1.35

Let $\sim$ be the relation of congruence modulo 5 on the set of integers. Then

$$[0]_\sim = \{a \in \mathbb{Z} \mid a \sim 0\}$$

Now, $a \sim 0$ if and only if $5 \mid a$, so we can also write

$$[0]_\sim = \{\dots, -10, -5, 0, 5, 10, \dots\} = \{5k \mid k \in \mathbb{Z}\}$$

So in fact $[0]_\sim = [5k]_\sim$ for any $k \in \mathbb{Z}$. And likewise

$$[r]_\sim = [r + 5k]_\sim$$

for all $r, k \in \mathbb{Z}$ ◁

Definition 5.1.36

Consider the relation of congruence modulo n on the set $\mathbb{Z}$ of integers. We call the equivalence class of $a \in \mathbb{Z}$ the **congruence class** of a modulo n, denoted $[a]_n$, and we write $\mathbb{Z}/n\mathbb{Z}$ to denote the quotient of $\mathbb{Z}$ by the relation of congruence modulo n.

Example 5.1.37

The set $\mathbb{Z}/5\mathbb{Z}$ has five elements:

$$\mathbb{Z}/5\mathbb{Z} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$$

Example 5.1.35 demonstrates that for all $n \in \mathbb{Z}$ and all $0 \leqslant r < 5$, we have $[n]_5 = [r]_5$ if and only if n leaves a remainder of r when divided by 5. For example, $[7]_5 = [2]_5$.   ◁

Exercise 5.1.38

Let n be a modulus. Prove that $\mathbb{Z}/n\mathbb{Z}$ is finite and $|\mathbb{Z}/n\mathbb{Z}| = n$.   ◁

Exercise 5.1.38 doesn't tell us much more than we already know: namely, that there are only finitely many possible remainders modulo n. But it makes our lives significantly easier for doing modular arithmetic, because now there are only finitely many objects to work with.

One last word on equivalence relations is that they are essentially the same thing as partitions (see Definition 4.2.36).

Exercise 5.1.39

If $\sim$ be an equivalence relation on X, then $X/\sim$ is a partition X. Deduce that, for $x, y \in X$, we have $x \sim y$ if and only if $[x]_\sim = [y]_\sim$.   ◁

In fact, the converse of 5.1.39 is also true, as we prove next.

Proposition 5.1.40

Let X be a set and let $\mathcal{U}$ be a partition of X. Then $\mathcal{U} = X/\sim$ for exactly one equivalence relation $\sim$ on X.

Proof. Define a relation $\sim$ by

$$x \sim y \quad \Leftrightarrow \quad \exists U \in \mathcal{U}, \ x \in U \text{ and } y \in U$$

for all $x, y \in X$. That is, $x \sim y$ if and only if x and y are elements of the same set of the partition. We check that $\sim$ is an equivalence relation.

- **Reflexivity.** Let $x \in X$. Then $x \in U$ for some $U \in \mathcal{U}$ since $\bigcup_{U \in \mathcal{U}} U = X$. Hence $x \sim x$.

- **Symmetry.** Let $x, y \in X$ and suppose $x \sim y$. Then there is some $U \in \mathcal{U}$ with $x \in U$ and $y \in U$. But then it is immediate that $y \sim x$.

- **Transitivity.** Let $x, y, z \in X$ and suppose that $x \sim y$ and $y \sim z$. Then there exist $U, V \in \mathcal{U}$ with $x, y \in U$ and $y, z \in V$. Thus $y \in U \cap V$. Since $\mathcal{U}$ is a partition of X, its elements are pairwise disjoint; thus if $U \neq V$ then $U \cap V = \varnothing$. Hence $U = V$. Thus $x \in U$ and $z \in U$, so $x \sim z$.

The definition of $\sim$ makes it immediate that $X/\sim = \mathcal{U}$.

To prove that $\sim$ is the only such relation, suppose $\approx$ is another equivalence relation on X for which $X/\approx = \mathcal{U}$. Then, given $x, y \in X$, we have:

$$
\begin{aligned}
x \sim y &\Leftrightarrow [x]_\sim = [y]_\sim & &\text{by Exercise 5.1.39} \\
&\Leftrightarrow \exists U \in \mathcal{U}, \ x \in U \wedge y \in U & &\text{by definition of } \sim \\
&\Leftrightarrow \exists z \in X, \ x \in [z]_\approx \wedge y \in [z]_\approx & &\text{since } \mathcal{U} = X/\approx \\
&\Leftrightarrow \exists z \in X, \ x \approx z \wedge y \approx z & &\text{by definition of } [z]_\approx \\
&\Leftrightarrow x \approx y & &\text{by symmetry and transitivity}
\end{aligned}
$$

So $\sim \, = \, \approx$. $\qquad\square$

5.2   Orders and lattices

We saw in Section 5.1 how equivalence relations behave like '=', in the sense that they are reflexive, symmetric and transitive.

This section explores a new kind of relation which behaves like '$\leqslant$'. This kind of relation proves to be extremely useful for making sense of mathematical structures, and has powerful applications throughout mathematics, computer science and even linguistics.

Definition 5.2.1

A relation R on a set X is a **partial order** if R is reflexive, antisymmetric and transitive. That is, if:

* (Reflexivity) $x \, R \, x$ for all $x \in X$;

* (Antisymmetry) For all $x, y \in X$, if $x \, R \, y$ and $y \, R \, x$, then $x = y$;

* (Transitivity) For all $x, y, z \in X$, if $x \, R \, y$ and $y \, R \, z$, then $x \, R \, z$.

A set X together with a partial order R on X is called a **partially ordered set**, or **poset** for short, and is denoted (X, R).

When we talk about partial orders, we usually use a suggestive symbol like '$\preceq$' (LATEX code: `\preceq`) or '$\sqsubseteq$' (LATEX code: `\sqsubseteq`).

Example 5.2.2

We have seen many examples of posets so far:

* Any of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$, with the usual order relation $\leqslant$.

* Given a set X, its power set $\mathcal{P}(X)$ is partially ordered by $\subseteq$. Indeed:

    ⋄ **Reflexivity.** If $U \in \mathcal{P}(X)$ then $U \subseteq U$.

    ⋄ **Antisymmetry.** If $U, V \in \mathcal{P}(X)$ with $U \subseteq V$ and $V \subseteq U$, then $U = V$ by definition of set equality.

    ⋄ **Transitivity.** If $U, V, W \in \mathcal{P}(X)$ with $U \subseteq V$ and $V \subseteq W$, then $U \subseteq W$ by Proposition 2.2.11.

* The set $\mathbb{N}$ of natural numbers is partially ordered by divisibility (see Examples 5.1.16, 5.1.23 and 5.1.28). However, by Exercise 5.1.24, the set $\mathbb{Z}$ of integers is not partially ordered by divisibility, since divisibility is not antisymmetric on $\mathbb{Z}$.

- Any set X is partially ordered by its equality relation. This is called the **discrete order** on X.

$\triangleleft$

Much like the difference between the relations $\leqslant$ and $<$ on $\mathbb{N}$, or between $\subseteq$ and $\subsetneq$ on $\mathbb{P}(X)$, every partial order can be *strictified*, in a precise sense outlined in the following definition and proposition.

Definition 5.2.3
A relation R on a set X is a **strict partial order** if it is irreflexive, asymmetric and transitive. That is, if:
- (Irreflexivity) $\neg(x \: R \: x)$ for all $x \in X$;

- (Asymmetry) For all $x, y \in X$, if $x \: R \: y$, then $\neg(y \: R \: x)$;

- (Transitivity) For all $x, y, z \in X$, if $x \: R \: y$ and $y \: R \: z$, then $x \: R \: z$.

Proposition 5.2.4
Let X be a set. Partial orders $\preccurlyeq$ on X are in natural correspondence with strict partial orders $\prec$ on X, according to the rule:

$$x \preccurlyeq y \;\Leftrightarrow\; (x \prec y \vee x = y) \quad \text{and} \quad x \prec y \;\Leftrightarrow\; (x \preccurlyeq y \wedge x \neq y)$$

Proof. Let P be the set of all partial orders on X and let S be the set of all strict partial orders on X. Define functions

$$f : P \to S \quad \text{and} \quad g : S \to P$$

as in the statement of the proposition, namely:

- Given a partial order $\preccurlyeq$, let $f(\preccurlyeq)$ be the relation $\prec$ defined for $x, y \in X$ by letting $x \prec y$ be true if and only if $x \preccurlyeq y$ and $x \neq y$;

- Given a strict partial order $\prec$, let $g(\prec)$ be the relation $\preccurlyeq$ defined for $x, y \in X$ by letting $x \preccurlyeq y$ be true if and only if $x \prec y$ or $x = y$.

We'll prove that f and g are mutually inverse functions. Indeed:

- f is well-defined. To see this, fix $\preccurlyeq$ and $\prec \; = f(\preccurlyeq)$ and note that:

⋄ $\prec$ is irreflexive, since for $x \in X$ if $x \prec x$ then $x \neq x$, which is a contradiction.

⋄ $\prec$ is asymmetric. To see this, let $x, y \in X$ and suppose $x \prec y$. Then $x \preccurlyeq y$ and $x \neq y$. If also $y \prec x$, then we'd have $y \preccurlyeq x$, so that $x = y$ by antisymmetry of $\preccurlyeq$. But $x \neq y$, so this is a contradiction.

⋄ $\prec$ is transitive. To see this, let $x, y, z \in X$ and suppose $x \prec y$ and $y \prec z$. Then $x \preccurlyeq y$ and $y \preccurlyeq z$, so that $x \preccurlyeq z$. Moreover, if $x = z$ then we'd also have $z \preccurlyeq x$ by reflexivity of $\preccurlyeq$, so $z \preccurlyeq y$ by transitivity of $\preccurlyeq$, and hence $y = z$ by antisymmetry of $\preccurlyeq$. But this contradicts $y \prec z$.

So $\prec$ is a strict partial order on X.

- g is well-defined. To see this, fix $\prec$ and $\preccurlyeq = g(\prec)$ and note that:

  ⋄ $\preccurlyeq$ is reflexive. This is built into the definition of $\preccurlyeq$.

  ⋄ $\preccurlyeq$ is symmetric. To see this, fix $x, y \in X$ and suppose $x \preccurlyeq y$ and $y \preccurlyeq x$. Now if $x \neq y$ then $x \prec y$ and $y \prec x$, but this contradicts asymmetry of $\prec$. Hence $x = y$.

  ⋄ $\preccurlyeq$ is transitive. To see this, fix $x, y, z \in X$ and suppose $x \preccurlyeq y$ and $y \preccurlyeq z$. Then one of the following four cases must be true:

   * $x = y = z$. In this case, $x = z$, so $x \preccurlyeq z$.
   * $x = y \prec z$. In this case, $x \prec z$, so $x \preccurlyeq z$.
   * $x \prec y = z$. In this case, $x \prec z$, so $x \preccurlyeq z$.
   * $x \prec y \prec z$. In this case, $x \prec z$ by transitivity of $\prec$, so $x \preccurlyeq z$.

   In any case, we have that $x \preccurlyeq z$.

So $\preccurlyeq$ is a partial order on X.

- $g \circ f = \mathrm{id}_P$. To see this, let $\prec = f(\preccurlyeq)$ and $\sqsubseteq = g(\prec)$. For $x, y \in X$, we have $x \sqsubseteq y$ if and only if $x \prec y$ or $x = y$, which in turn occurs if and only if $x = y$ or both $x \preccurlyeq y$ and $x \neq y$. This is equivalent to $x \preccurlyeq y$, since if $x = y$ then $x \preccurlyeq y$ by reflexivity. Hence $\sqsubseteq$ and $\preccurlyeq$ are equal relations, so $g \circ f = \mathrm{id}_P$.

- $f \circ g = \mathrm{id}_S$. To see this, let $\preccurlyeq = g(\prec)$ and $\sqsubset = f(\preccurlyeq)$. For $x, y \in X$, we have $x \sqsubset y$ if and only if $x \preccurlyeq y$ and $x \neq y$, which in turn occurs if and only if $x \neq y$ and either $x \prec y$ or $x = y$. Since $x \neq y$ precludes $x = y$, this is equivalent to $x \prec y$. Hence $\prec$ and $\sqsubset$ are equal relations, so $f \circ g = \mathrm{id}_S$.

So f and g are mutually inverse functions, and we have established the required bijection.

□

In light of Proposition 5.2.4, we will freely translate between partial orders and strict partial orders wherever necessary. When we do so, we will use $\prec$ (LaTeX code: `\prec`) to denote the 'strict' version, and $\preccurlyeq$ to denote the 'weak' version. (Likewise for $\sqsubset$ (LaTeX code: `\sqsubet`).)

Definition 5.2.5

Let $(X, \preccurlyeq)$ be a poset. A $\preccurlyeq$-**least element** of X (or a **least element of X with respect to** $\preccurlyeq$) is an element $\bot \in X$ (LaTeX code: `\bot`) such that $\bot \preccurlyeq x$ for all $x \in X$. A $\preccurlyeq$-**greatest element** of X (or a **greatest element of X with respect to** $\preccurlyeq$) is an element $\top \in X$ (LaTeX code: `\top`) such that $x \preccurlyeq \top$ for all $x \in X$.

Example 5.2.6

Some examples of least and greatest elements that we have already seen are:

- In $(\mathbb{N}, \leqslant)$, 0 is a least element; there is no greatest element.

- Let $n \in \mathbb{N}$ with $n > 0$. Then 1 is a least element of $([n], \leqslant)$, and n is a greatest element.

- $(\mathbb{Z}, \leqslant)$ has no greatest or least elements.

$\triangleleft$

Proposition 5.2.7 says that least and greatest elements of posets are unique, if they exist. This allows us to talk about 'the' least or 'the' greatest element of a poset.

Proposition 5.2.7

Let $(X, \preccurlyeq)$ be a poset. If X has a least element, then it is unique; and if X has a greatest element, then it is unique.

Proof. Suppose X has a least element ℓ. We prove that if ℓ' is another least element, then $\ell' = \ell$.

So take another least element ℓ'. Since ℓ is a least element, we have $\ell \preccurlyeq \ell'$. Since ℓ' is a least element, we have $\ell' \preccurlyeq \ell$. By antisymmetry of $\preccurlyeq$, it follows that $\ell = \ell'$.

Hence least elements are unique. The proof for greatest elements is similar, and is left as an exercise. $\qquad\square$

Exercise 5.2.8

Let X be a set. The poset $(\mathcal{P}(X), \subseteq)$ has a least element and a greatest element; find both. $\triangleleft$

Exercise 5.2.9

Prove that the least element of $\mathbb{N}$ with respect to divisibility is 1, and the greatest element is 0.   ◁

Definition 5.2.10

Let $(X, \preccurlyeq)$ be a poset and let $A \subseteq X$. A $\preccurlyeq$-**supremum** of A is an element $s \in X$ such that

- $a \preccurlyeq s$ for each $a \in A$; and

- If $s' \in X$ with $a \preccurlyeq s'$ for all $a \in A$, then $s \preccurlyeq s'$.

A $\preccurlyeq$-**infimum** of A is an element $i \in X$ such that

- $i \preccurlyeq a$ for each $a \in A$; and

- If $i' \in X$ with $i' \preccurlyeq a$ for all $a \in A$, then $i' \preccurlyeq i$.

Example 5.2.11

The well-ordering principle states that if $U \subseteq \mathbb{N}$ is inhabited then U has a $\leqslant$-infimum, and moreover the infimum of U is an element of U.   ◁

Exercise 5.2.12

Let X be a set, and let $U, V \in \mathcal{P}(X)$. Prove that the $\subseteq$-supremum of $\{U, V\}$ is $U \cup V$, and the $\subseteq$-infimum of $\{U, V\}$ is $U \cap V$.   ◁

Exercise 5.2.13

Let $a, b \in \mathbb{N}$. Show that $\gcd(a, b)$ is an infimum of $\{a, b\}$ and that $\operatorname{lcm}(a, b)$ is a supremum of $\{a, b\}$ with respect to divisbility.   ◁

Example 5.2.14

Define $U = [0, 1) = \{x \in \mathbb{R} \mid 0 \leqslant x < 1\}$. We prove that U has both an infimum and a supremum in the poset $(\mathbb{R}, \leqslant)$.

- **Infimum.** 0 is an infimum for U. Indeed:

  (i) Let $x \in U$. Then $0 \leqslant x$ by definition of U.

  (ii) Let $y \in \mathbb{R}$ and suppose that $y \leqslant x$ for all $x \in U$. Then $y \leqslant 0$, since $0 \in U$.

  so 0 is as required.

- **Supremum.** 1 is a supremum for U. Indeed:

  (i) Let $x \in U$. Then $x < 1$ by definition of U, so certainly $x \leqslant 1$.

(ii) Let $y \in \mathbb{R}$ and suppose that $x \leqslant y$ for all $x \in U$. We prove that $1 \leqslant y$ by contradiction. So suppose it is not the case that $1 \leqslant y$. Then $y < 1$. Since $x \leqslant y$ for all $x \in U$, we have $0 \leqslant y$. But then

$$0 \leqslant y = \frac{y+y}{2} < \frac{y+1}{2} < \frac{1+1}{2} = 1$$

But then $\frac{y+1}{2} \in U$ and $y < \frac{y+1}{2}$. This contradicts the assumption that $x \leqslant y$ for all $x \in U$. So it must in fact have been the case that $1 \leqslant y$.

so 1 is as required.

◁

The following proposition proves that suprema and infima are unique, provided they exist.

Proposition 5.2.15

Let $(X, \preccurlyeq)$ is a poset, and let $A \subseteq X$.

(i) If $s, s' \in X$ are suprema of A, then $s = s'$;

(ii) If $i, i' \in X$ are infima of A, then $i = i'$.

Proof. Suppose s, s' are suprema of A. Then:

- $a \preccurlyeq s'$ for all $a \in A$, so $s' \preccurlyeq s$ since s is a supremum of A;

- $a \preccurlyeq s$ for all $a \in A$, so $s \preccurlyeq s'$ since s' is a supremum of A.

Since $\preccurlyeq$ is antisymmetric, it follows that $s = s'$. This proves (i).

The proof of (ii) is almost identical and is left as an exercise to the reader. $\square$

Notation 5.2.16

Let $(X, \preccurlyeq)$ be a poset and let $U \subseteq X$. Denote the $\preccurlyeq$-infimum of U, if it exists, by $\bigwedge U$ (LATEX code: `\bigwedge`); and denote the $\preccurlyeq$-supremum of U, if it exists, by $\bigvee U$ (LATEX code: `\bigvee`). Moreover, for $x, y \in X$, write

$$\bigwedge \{x, y\} = x \wedge y \text{ (LATEX code: \texttt{\textbackslash wedge})}, \qquad \bigvee \{x, y\} = x \vee y \text{ (LATEX code: \texttt{\textbackslash vee})}$$

Example 5.2.17

Some examples of Notation 5.2.16 are as follows.

- Let X be a set. In $(\mathcal{P}(X), \subseteq)$ we have $U \wedge V = U \cap V$ and $U \vee V = U \cup V$ for all $U, V \in \mathcal{P}(X)$.

- We have seen that, in $(\mathbb{N}, |)$, we have $a \wedge b = \gcd(a, b)$ and $a \vee b = \operatorname{lcm}(a, b)$ for all $a, b \in \mathbb{N}$.

- In $(\mathbb{R}, \leqslant)$, we have $a \wedge b = \min\{a, b\}$ and $a \vee b = \max\{a, b\}$.

$\triangleleft$

Definition 5.2.18
A **lattice** is a poset $(X, \preccurlyeq)$ such that every pair of elements of X has a $\preccurlyeq$-supremum and a $\preccurlyeq$-infimum.

Example 5.2.19
We have seen that $(\mathcal{P}(X), \subseteq)$, $(\mathbb{R}, \leqslant)$ and $(\mathbb{N}, |)$ are lattices. $\triangleleft$

Proposition 5.2.20 (Associativity laws for lattices)
Let $(X, \preccurlyeq)$ be a lattice, and let $x, y, z \in X$. Then

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \qquad \text{and} \qquad x \vee (y \vee z) = (x \vee y) \vee z$$

Proof. We prove $x \wedge (y \wedge z) = (x \wedge y) \wedge z$; the other equation is dual and is left as an exercise. We prove that the sets $\{x, y \wedge z\}$ and $\{x \wedge y, z\}$ have the same sets of lower bounds, and hence the same infima. So let

$$L_1 = \{i \in X \mid i \preccurlyeq x \text{ and } i \preccurlyeq y \wedge z\} \quad \text{and} \quad L_2 = \{i \in X \mid i \preccurlyeq x \wedge y \text{ and } i \preccurlyeq z\}$$

We prove $L_1 = L = L_2$, where

$$L = \{i \in X \mid i \preccurlyeq x, \; i \preccurlyeq y \text{ and } i \preccurlyeq z\}$$

First we prove $L_1 = L$. Indeed:

- $L_1 \subseteq L$. To see this, suppose $i \in L_1$. Then $i \preccurlyeq x$ by definition of L_1. Since $i \preccurlyeq y \wedge z$, and $y \wedge z \preccurlyeq y$ and $y \wedge z \preccurlyeq z$, we have $i \preccurlyeq y$ and $i \preccurlyeq z$ by transitivity of $\preccurlyeq$.

- $L \subseteq L_1$. To see this, suppose $i \in L$. Then $i \preccurlyeq x$ by definition of L. Moreover, $i \preccurlyeq y$ and $i \preccurlyeq z$ by definition of L, so that $i \preccurlyeq y \wedge z$ by definition of $\wedge$. Hence $i \in L$.

The proof that $L_2 = L$ is similar. Hence $L_1 = L_2$. But $x \wedge (y \wedge z)$ is, by definition of $\wedge$, the $\preccurlyeq$-greatest element of L_1, which exists since $(X, \preccurlyeq)$ is a lattice. Likewise, $(x \wedge y) \wedge z$ is the $\preccurlyeq$-greatest element of L_2.

Since $L_1 = L_2$, it follows that $x \wedge (y \wedge z) = (x \wedge y) \wedge z$, as required. $\square$

Exercise 5.2.21 (Commutativity laws for lattices)

Let $(X, \preccurlyeq)$ be a lattice. Prove that, for all $x, y \in X$, we have

$$x \wedge y = y \wedge x \quad \text{and} \quad x \vee y = y \vee x$$

◁

Exercise 5.2.22 (Absorption laws for lattices)

Let $(X, \preccurlyeq)$ be a lattice. Prove that, for all $x, y \in X$, we have

$$x \vee (x \wedge y) = x \qquad \text{and} \qquad x \wedge (x \vee y) = x$$

◁

Example 5.2.23

It follows from what we've proved that if $a, b, c \in \mathbb{Z}$ then

$$\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$$

For example, take $a = 882$, $b = 588$ and $c = 252$. Then

- $\gcd(b, c) = 84$, so $\gcd(a, \gcd(b, c)) = \gcd(882, 84) = 42$;

- $\gcd(a, b) = 294$, so $\gcd(\gcd(a, b), c) = \gcd(294, 252) = 42$.

These are indeed equal. ◁

Distributive lattices and Boolean algebras

One particularly important class of lattice is that of a *distributive lattice*, in which suprema and infima interact in a particularly convenient way. This makes algebraic manipulations of expressions involving suprema and infima particularly simple.

Definition 5.2.24

A lattice $(X, \preccurlyeq)$ is **distributive** if

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \text{and} \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

for all $x, y, z \in X$.

Example 5.2.25

For any set X, the power set lattice $(\mathcal{P}(X), \subseteq)$ is distributive. That is to say that for all $U, V, W \subseteq X$ we have

$$U \cap (V \cup W) = (U \cap V) \cup (U \cap W) \quad \text{and} \quad U \cup (V \cap W) = (U \cup V) \cap (U \cup W)$$

This was the content of Example 2.2.34 and Exercise 2.2.35.   ◁

Exercise 5.2.26
Prove that $(\mathbb{N}, |)$ is a distributive lattice.   ◁

Definition 5.2.27
Let $(X, \preccurlyeq)$ be a lattice with a greatest element $\top$ and a least element $\bot$, and let $x \in X$. A **complement** for x is an element y such that

$$x \wedge y = \bot \quad \text{and} \quad x \vee y = \top$$

Example 5.2.28
Let X be a set. We show that every element $U \in \mathcal{P}(X)$ has a complement.   ◁

Exercise 5.2.29
Let $(X, \preccurlyeq)$ be a distributive lattice with a greatest element and a least element, and let $x \in X$. Prove that, if a complement for x exists, then it is unique; that is, prove that if $y, y' \in X$ are complements for X, then $y = y'$.   ◁

Exercise 5.2.29 justifies the following notation.

Notation 5.2.30
Let $(X, \preccurlyeq)$ be a distributive lattice with greatest and least elements. If $x \in X$ has a complement, denote it by $\neg x$.

Definition 5.2.31
A lattice $(X, \preccurlyeq)$ is **complemented** if every element $x \in X$ has a complement. A **Boolean algebra** is a complemented distributive lattice with a greatest element and a least element.

The many preceding examples and exercises concerning $(\mathcal{P}(X), \subseteq)$ piece together to provide a proof of the following theorem.

Theorem 5.2.32
Let X be a set. Then $(\mathbb{P}(X), \subseteq)$ is a Boolean algebra.

Another extremely important example of a Boolean algebra is known as the *Lindenbaum–Tarski algebra*, which we define in Definition 5.2.35. In order to define it, we need to prove that the definition will make sense. First of all, we fix some notation.

Definition 5.2.33

Let P be a set, thought of as a set of propositional variables. Write $L(P)$ to denote the set of propositional formulae with propositional variables in P—that is, the elements of $L(P)$ are strings built from the elements of P, using the operations of conjunction ($\wedge$), disjunction ($\vee$) and negation ($\neg$).

Lemma 5.2.34

Logical equivalence $\equiv$ is an equivalence relation on $L(P)$.

Proof. This is immediate from definition of equivalence relation, since for $s, t \in L(P)$, $s \equiv t$ is defined to mean that s and t have the same truth values for all assignments of truth values to their propositional variables. $\square$

In what follows, the set P of propositional variables is fixed; we may moreover take it to be countably infinite, since all strings in $L(P)$ are finite.

Definition 5.2.35

The **Lindenbaum–Tarski algebra** (**for propositional logic**) over P is the pair $(A, \vdash)$, where $A = L(P)/\equiv$ and $\vdash$ is the relation on A defined by $[s]_\equiv \vdash [t]_\equiv$ if and only if $s \Rightarrow t$ is a tautology.

In what follows, we will simply write $[-]$ for $[-]_\equiv$.

Theorem 5.2.36

The Lindenbaum–Tarski algebra is a Boolean algebra.

Sketch proof. There is lots to prove here! Indeed, we must prove:

- $\vdash$ is a well-defined relation on A; that is, if $s \equiv s'$ and $t \equiv t'$ then we must have $[s] \vdash [t]$ if and only if $[s'] \vdash [t']$.

- $\vdash$ is a partial order on A; that is, it is reflexive, antisymmetric and transitive.

- The poset $(A, \vdash)$ is a lattice; that is, it has suprema and infima.

- The lattice $(A, \vdash)$ is distributive, has a greatest element and a least element, and is complemented.

We will omit most of the details, which are left as an exercise; instead, we outline what the components involved are.

The fact that $\vdash$ is a partial order can be proved as follows.

- Reflexivity of $\vdash$ follows from the fact that $s \Rightarrow s$ is a tautology for all propositional formulae s.

- Symmetry of $\vdash$ follows from the fact that, for all propositional formulae s, t, if $s \Leftrightarrow t$ is a tautology then s and t are logically equivalent.

- Transitivity of $\vdash$ follows immediately from transitivity of $\Rightarrow$.

The fact that $(A, \vdash)$ is a lattice can be proved by verifying that:

- Given $[s], [t] \in A$, the infimum $[s] \wedge [t]$ is given by conjunction, namely $[s] \wedge [t] = [s \wedge t]$.

- Given $[s], [t] \in A$, the supremum $[s] \vee [t]$ is given by disjunction, namely $[s] \vee [t] = [s \vee t]$.

Finally, distributivity of suprema and infima in $(A, \vdash)$ follows from the corresponding properties of conjunction and disjunction; $(A, \vdash)$ has greatest element $[p \Rightarrow p]$ and least element $[\neg(p \Rightarrow p)]$, where p is some fixed propositional variable; and the complement of $[s] \in A$ is given by $[\neg s]$. $\qquad \square$

We finish this section on orders and lattices with a general version of de Morgan's laws for Boolean algebras, which by Theorems 5.2.32 and 5.2.36 implies the versions we proved for logical formulae (Theorem 2.1.14) and for sets (Theorem 2.2.40).

Theorem 5.2.37 (De Morgan's laws)
Let $(X, \preccurlyeq)$ be a Boolean algebra, and let $x, y \in X$. Then

$$\neg(x \wedge y) = (\neg x) \vee (\neg y) \quad \text{and} \quad \neg(x \vee y) = (\neg x) \wedge (\neg y)$$

Proof. We prove $\neg(x \wedge y) = (\neg x) \vee (\neg y)$ $\qquad \square$

5.3 Well-foundedness and structural induction

<div style="text-align: center">

Warning!

This section is not yet finished—do not rely on its correctness or completeness.

</div>

Section 1.3 introduced induction as a technique for proving statements which are true of all natural numbers. We saw induction in three flavours: weak induction, strong induction and the well-ordering principle.

- The **principle of weak induction** exploited the *inductively defined* structure of $\mathbb{N}$. Every natural number can be obtained from 0 by repeatedly applying the successor ('plus one') operation, so if a statement $p(n)$ is true of 0, and its truth is preserved by the successor operation (i.e. if $p(n) \Rightarrow p(n+1)$ is true for all $n \in \mathbb{N}$), then it must be true of all natural numbers

- The **well-ordering principle** exploited the *well-founded* nature of the order relation $<$ on $\mathbb{N}$. It says that every inhabited subset of $\mathbb{N}$, so that any proposition $p(n)$ which is *not* true of all natural numbers n must have a least counterexample—this led to the technique of proof by infinite descent.

In this section, we will generalise these techniques to other sets with an *inductively defined* or a *well-founded* structure.

- An *inductively defined set* will, intuitively, be a set X built from some set of *basic elements* (like zero) using a set of *constructors* (like the successor operation). We will be able to perform induction on these sets to prove that a statement $p(x)$ is true for all $x \in X$ by proving that it is true for the basic elements, and then proving that its truth is preserved by the constructors. This proof technique generalises weak induction and is called *structural induction*.

- A set X with a *well-founded relation* R will allow us to generalise proof by infinite descent: if there is a counterexample to a logical formula $p(x)$, then there must be one which is 'minimal' with respect to R. This leads to a proof technique called *well-founded induction*, which has similarities with strong induction.

Structural induction is conceptually easier to comprehend than well-founded induction, so we will introduce it first. However, we will not be able to prove that it is a valid proof technique until after we have introduced well-founded induction.

<div style="text-align: center">259</div>

Inductively defined sets

In Section 1.3, we formalised the idea that the set of natural numbers should be what is obtained by starting with zero and repeating the successor ('plus one') operation. In a sense, zero was a *basic element*—we posited its existence from the outset—and the successor operation *constructed* the remaining elements.

Although hidden beneath the surface, this method of defining a set was implicitly used in Section 2.1 when defining propositional formulae. Here, our *basic elements* were propositional variables $p, q, r, s, \ldots$, and the remaining propositional formulae could be *constructed* by repeatedly applying the logical connectives $\wedge$, $\vee$, $\neg$ and $\Rightarrow$.

Definition 5.3.1

An **inductively defined set** is a set X equipped with a subset $B \subseteq X$ of **basic elements** and a set C of **constructors**, with the following properties:

(i) Each constructor $f \in C$ is a function $f : X^n \to X$ for some $n \in \mathbb{N}$. The natural number n is called the **arity** of f.

(ii) For all constructors $f, g \in C$ if m, n are the arities of f, g, respectively, and $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n \in X$ are such that

$$f(x_1, x_2, \ldots, x_m) = g(y_1, y_2, \ldots, y_n)$$

then $m = n$, $f = g$ and $x_i = y_i$ for all $i \in [m]$.

(iii) For all constructors $f \in C$, the image of f is a subset of $X \setminus B$. That is, no basic element is of the form $f(x_1, x_2, \ldots, x_n)$ for any constructor f and elements $x_1, x_2, \ldots, x_n \in X$.

(iv) For all $x \in X \setminus B$, then $x = f(x_1, x_2, \ldots, x_n)$ for some constructor $f \in C$ of arity n.

Example 5.3.2

The set $\mathbb{N}$ of natural number is inductively defined by taking $B = \{0\}$ and $C = \{s\}$, where $s : \mathbb{N} \to \mathbb{N}$ is defined by $s(n) = n + 1$ for all $n \in \mathbb{N}$. Indeed:

(i) $s : \mathbb{N} \to \mathbb{N}$ is a constructor of arity 1.

(ii) Let $f, g \in C$. Then $f = g = s$; and if $x, y \in \mathbb{N}$ with $s(x) = s(y)$, then $x + 1 = y + 1$, so $x = y$.

(iii) $s[\mathbb{N}] \subseteq \mathbb{N} \setminus \{0\}$ since $0 \neq x + 1$ for any $x \in \mathbb{N}$.

(iv) For all $x \in \mathbb{N} \setminus \{0\}$ we have $x = x' + 1$ for some $x' \in \mathbb{N}$—namely, $x' = x - 1$—and so $x = s(x')$.

$\lhd$

Exercise 5.3.3
Prove that the set $E = \{1, 2, 4, 8, 16 \ldots\}$ of powers of 2 is inductively defined by taking $B = \{1\}$ and $C = \{d\}$, where $d : E \to E$ is defined by $d(n) = 2n$ for all $n \in \mathbb{N}$. $\lhd$

Exercise 5.3.4
Prove that $\mathbb{N}$ is inductively defined by taking $B = 0$ and $C = \{f\}$, where $f : \mathbb{N} \to \mathbb{N}$ is defined by

$$
f(n) = \begin{cases} 1 & \text{if } n = 0 \\ 2(n-1) & \text{if } n = 2^k + 1 \text{ for some } k \in \mathbb{N} \\ n - 1 & \text{otherwise} \end{cases}
$$

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

To do: Example: propositional formulae

Theorem 5.3.5 (Principle of structural induction)
Let X be an inductively defined set, and let $p(x)$ be a logical formula concerning elements of X. Suppose that

- $p(b)$ is true for all basic elements $b \in X$; and

- For all constructors f of arity n and all $x_1, x_2, \ldots, x_n \in X$, if $p(x_1), p(x_2), \ldots, p(x_n)$ are all true, then $p(f(x_1, x_2, \ldots, x_n))$ is true.

Then $p(x)$ is true for all $x \in X$.

We will prove Theorem 5.3.5 on page 269.

Example 5.3.6
To do: Structural induction on $\mathbb{N}$ is weak induction. $\lhd$

To do: Disjunctive normal form

To do: Generalise to quotients of inductive structures $\rightsquigarrow$ induction on $\mathbb{Z}$ using 0 and $+, -$ and on $\mathbb{Z}^{>0}$ using 1 and $p \times (-)$.

We saw in Proposition 5.3.13 that the relation R on the set $\mathbb{Z}^{>0}$ of positive integers defined

for $m, n \in \mathbb{Z}^{>0}$ by

$$m \; R \; n \quad \Leftrightarrow \quad n = pm \text{ for some prime } p > 0$$

is well-founded. We can use well-founded induction to prove a general formula for the totient of an integer n.

Theorem 5.3.7 (Formula for Euler's totient function)

Let $n \in \mathbb{Z}$ be nonzero, and let $\varphi : \mathbb{Z} \to \mathbb{N}$ be Euler's totient function (see Definition 3.3.31). Then

$$\varphi(n) = |n| \cdot \prod_{p \mid n \text{ prime}} \left(1 - \frac{1}{p} \right)$$

where the product is indexed over the distinct positive prime factors p of n.

Proof. If $n < 0$ then $\varphi(n) = \varphi(-n)$, $|n| = -n$ and $p \mid n$ if and only if $p \mid -n$, so the theorem holds for negative integers if and only if it holds for positive integers.

We prove the formula for $n > 0$ by well-founded induction on $\mathbb{Z}^{>0}$ with respect to the relation R defined in Proposition 5.3.13.

- **(BC)** $\varphi(1) = 1$ and, since no prime p divides 1, we have $\prod_{p \mid 1 \text{ prime}} \left(1 - \frac{1}{p} \right) = 1$. Hence

$$1 \cdot \prod_{p \mid 1 \text{ prime}} \left(1 - \frac{1}{p} \right) = 1 \cdot 1 = 1$$

  as erquired.

- **(IS)** Fix $n \geq 1$ and suppose that

$$\varphi(n) = n \cdot \prod_{p \mid n \text{ prime}} \left(1 - \frac{1}{p} \right)$$

  Let $q > 0$ be prime. We prove that

$$\varphi(qn) = qn \cdot \prod_{p \mid qn \text{ prime}} \left(1 - \frac{1}{p} \right)$$

⋄ Suppose $q \mid n$. Then by we have

$$\varphi(qn) = q\varphi(n) \qquad\qquad \text{by Exercise 4.2.56}$$

$$= qn \cdot \prod_{p \mid n \, prime} \left(1 - \frac{1}{p}\right) \qquad\qquad \text{by induction hypothesis}$$

$$= qn \cdot \prod_{p \mid qn \, prime} \left(1 - \frac{1}{p}\right)$$

The last equation holds because the fact that $q \mid n$ implies that, for all positive primes p, we have $p \mid n$ if and only if $p \mid qn$.

⋄ Suppose $q \nmid n$. Then $q \perp n$, so we have

$$\varphi(qn) = \varphi(q)\varphi(n) \qquad\qquad \text{by Theorem 4.2.55}$$

$$= \varphi(q) \cdot n \cdot \prod_{p \mid n \text{ prime}} \left(1 - \frac{1}{p}\right) \qquad\qquad \text{by induction hypothesis}$$

$$= (q - 1) \cdot n \cdot \prod_{p \mid n \text{ prime}} \left(1 - \frac{1}{q}\right) \qquad\qquad \text{by Example 3.3.32}$$

$$= q \left(1 - \frac{1}{p}\right) n \cdot \prod_{p \mid n \text{ prime}} \left(1 - \frac{1}{p}\right) \qquad\qquad \text{rearranging}$$

$$= qn \cdot \left(\prod_{p \mid n \text{ prime}} \left(1 - \frac{1}{p}\right) \right) \cdot \left(1 - \frac{1}{q}\right) \qquad \text{rearranging}$$

$$= qn \cdot \prod_{p \mid qn} \left(1 - \frac{1}{p}\right) \qquad\qquad \text{reindexing the product}$$

In both cases, we have shown that the formula holds.

By induction, we're done. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Well-founded relations

First, we introduce the notion of a *well-founded relation*.

Definition 5.3.8

Let X be a set. A relation R on X is **well-founded** if every inhabited subset of X has an R-**minimal** element, in the following sense: for each inhabited $U \subseteq X$, there exists $m \in U$ such that $\neg(x \, R \, m)$ for all $x \in U$. A relation that is not well-founded is called **ill-founded**.

Example 5.3.9

The relation $<$ on $\mathbb{N}$ is well-founded—this is just a fancy way of stating the well-ordering principle (Theorem 1.3.37). Indeed, let $U \subseteq \mathbb{N}$ be an inhabited subset. By the well-ordering principle, there exists an element $m \in U$ such that $m \leqslant x$ for all $x \in U$. But this says precisely that $\neg(x < m)$ for all $x \in U$. ◁

Example 5.3.10

However, the relation $<$ on $\mathbb{Z}$ is not well-founded—indeed, $\mathbb{Z}$ is an inhabited subset of $\mathbb{Z}$ with no $<$-least element. ◁

Exercise 5.3.11

Let $<^1$ be the relation on $\mathbb{N}$ defined for $m, n \in \mathbb{N}$ by

$$m <^1 n \quad \Leftrightarrow \quad n = m + 1$$

Prove that $<^1$ is a well-founded relation on $\mathbb{N}$. ◁

Proposition 5.3.12

Let X be a set and let R be a relation on X. R is well-founded if and only if there is no infinite R-descending chains; that is, there does not exist a sequence $(x_n)_{n \in \mathbb{N}}$ of elements of X such that $x_{n+1} \, R \, x_n$ for all $n \in \mathbb{N}$.

Proof. We prove the contrapositives of the two directions; that is, R is ill-founded if and only if R has an infinite descending R-chain.

- ($\Rightarrow$) Suppose that R is ill-founded, and let $U \subseteq X$ be an inhabited subset with no R-minimal element. Define a sequence $(x_n)_{n \in \mathbb{N}}$ of elements of X—in fact, of U—recursively as follows:

    ◇ Let $x_0 \in U$ be arbitrarily chosen.

    ◇ Fix $n \in \mathbb{N}$ and suppose $x_0, x_1, \ldots, x_n \in U$ have been defined. Since U has no R-minimal element, it contains an element which is related to x_n by R; define x_{n+1} to be such an element.

    Then $(x_n)_{n \in \mathbb{N}}$ is an infinite R-descending chain

- ($\Leftarrow$) Suppose there is an infinite R-descending chain $(x_n)_{n \in \mathbb{N}}$. Define $U = \{x_n \mid n \in \mathbb{N}\}$ to be the set of elements in this sequence. Then U has no R-minimal element. Indeed, given $m \in U$, we must have $m = x_n$ for some $n \in \mathbb{N}$; but then $x_{n+1} \in U$ and $x_{n+1} \, R \, m$. Hence R is ill-founded.

$\square$

Proposition 5.3.13

Let $\mathbb{Z}^{>0}$ be the set of positive integers and define a relation R on $\mathbb{Z}^{>0}$ by

$$m \ R \ n \quad \Leftrightarrow \quad n = pm \text{ for some prime } p > 0$$

for all $m, n > 0$. Then R is a well-founded relation on $\mathbb{Z}^{>0}$.

Proof. Suppose that $(x_n)_{n \in \mathbb{N}}$ is an infinite R-descending chain in $\mathbb{Z}^{>0}$. Since $x_{n+1} \ R \ x_n$ for all $n \in \mathbb{N}$, we have $x_n = px_{n+1}$ for some positive prime p for all $n \in \mathbb{N}$. Since all positive primes are greater than or equal to 2, this implies that $x_n \geqslant 2x_{n+1}$ for all $n \in \mathbb{N}$.

We prove by strong induction on $n \in \mathbb{N}$ that $x_0 > 2^n x_{n+1}$ for all $n \in \mathbb{N}$.

- (**BC**) We proved above that $x_0 \geqslant 2x_1$. Hence $x_0 > x_1 = 2^0 x_1$, as required.

- (**IS**) Fix $n \in \mathbb{N}$ and suppose $x_0 > 2^n x_{n+1}$. We want to show $x_0 > 2^{n+1} x_{n+2}$. Well $x_{n+1} > 2x_{n+2}$, as proved above, and hence

$$x_0 \overset{\text{IH}}{>} 2^n x_{n+1} > 2^n \cdot 2x_{n+2} = 2^{n+1} x_{n+2}$$

  as required.

By induction, we've shown that $x_0 > 2^n x_{n+1}$ for all $n \in \mathbb{N}$. But $x_{n+1} > 0$ for all $n \in \mathbb{N}$, so $x_0 > 2^n$ for all $n \in \mathbb{N}$. This implies that x_0 is greater than every integer, which is a contradiction.

So such a sequence $(x_n)_{n \in \mathbb{N}}$ cannot exist, and by Proposition 5.3.12, the relation R is well-founded. $\square$

Exercise 5.3.14

Let X be a set and let R be a well-founded relation on X. Given $x, y \in X$, prove that not both $x \ R \ y$ and $y \ R \ x$ are true. $\triangleleft$

Theorem 5.3.15 (Principle of well-founded induction)

Let X be a set, let R be a well-founded relation on X, and let $p(x)$ be a logical formula concerning elements of X. Suppose that for each $x \in X$, the following is true:

If $p(y)$ is true for all R-predecessors y of x, then $p(x)$ is true.

That is, suppose for each $x \in X$ that

$$[\forall y \in X, (y \ R \ x \Rightarrow p(y))] \Rightarrow p(x)$$

Then $p(x)$ is true for all $x \in X$.

Proof. Suppose that, for each $x \in X$, if $p(y)$ is true for all R-predecessors y of x, then $p(x)$ is true. Let

$$U = \{x \in X \mid \neg p(x)\}$$

Towards a contradiction, suppose that $p(x)$ is false for some $x \in X$. Then U is inhabited. Since R is well-founded, U has an R-minimal element $m \in U$. Now

(i) $p(m)$ is false, since $m \in U$.

(ii) $p(x)$ is true for all $x \in X$ with $x \mathrel{R} m$. To see this, note that if $p(x)$ is false and $x \mathrel{R} m$, then $x \in U$, so that $m \mathrel{R} x$ by R-minimality of m in U. Since also $x \mathrel{R} m$, this contradicts Exercise 5.3.14.

Since $p(x)$ is true for all $x \in X$ with $x \mathrel{R} m$, by assumption we also have that $p(m)$ is true. But this contradicts our assumption that $m \in U$.

So it must in fact be the case that $U = \varnothing$, so that $p(x)$ is true for all $x \in X$. $\qquad\qquad\square$

Exercise 5.3.16

Prove that the principle of $<$-induction on $\mathbb{N}$ is precisely strong induction. Specifically, prove that the following two statements are equivalent:

(i) $p(0)$ is true and, for all $n \in \mathbb{N}$, if $p(k)$ is true for all $k \leqslant n$, then $p(n+1)$ is true;

(ii) For all $n \in \mathbb{N}$, if $p(k)$ is true for all $k < n$, then $p(n)$ is true.

Strong induction says that we can deduce that $p(n)$ is true for all $n \in \mathbb{N}$ from the knowledge that (i) is true for all $n \in \mathbb{N}$; and $<$-induction tells us that $p(n)$ is true for all $n \in \mathbb{N}$ from the knowledge that (ii) is true for all $n \in \mathbb{N}$. You should prove that (i) and (ii) are equivalent. $\qquad\qquad\triangleleft$

Example 5.3.17

Let $<^1$ be the relation on $\mathbb{N}$ defined in Exercise 5.3.11. We prove that the principle of $<^1$-induction on $\mathbb{N}$ is precisely strong induction. Specifically, prove that the following two statements are equivalent:

(i) $p(0)$ is true and, for all $n \in \mathbb{N}$, if $p(n)$ is true then $p(n+1)$ is true;

(ii) For all $n \in \mathbb{N}$, if $p(k)$ is true for all $k \in \mathbb{N}$ with $k + 1 = n$, then $p(n)$ is true.

Weak induction says that we can deduce that $p(n)$ is true for all $n \in \mathbb{N}$ from the knowledge that (i) is true for all $n \in \mathbb{N}$; and $<^1$-induction tells us that $p(n)$ is true for all $n \in \mathbb{N}$ from the knowledge that (ii) is true for all $n \in \mathbb{N}$. We prove that (i) and (ii) are equivalent.

- (i) $\Rightarrow$ (ii). Suppose that $p(0)$ and, for all $n \in \mathbb{N}$, if $p(n)$ is true then $p(n+1)$ is true. We will prove that

$$[\forall m \in \mathbb{N}, \, (n = m+1 \Rightarrow p(m))] \Rightarrow p(n)$$

  is true for all $n \in \mathbb{N}$.

  So fix $n \in \mathbb{N}$, and assume $\forall m \in \mathbb{N}, \, (n = m+1 \Rightarrow p(m))$. We prove $p(n)$ is true.

  ◇ If $n = 0$ then we're done, since $p(0)$ is true by assumption.

  ◇ If $n > 0$ then $n = m+1$ for some $m \in \mathbb{N}$. By our assumption, we have $\forall m \in \mathbb{N}, \, (n = m+1 \Rightarrow p(m))$, and so in particular, $p(m)$ is true. By the weak induction step, we have $p(m) \Rightarrow p(m+1)$ is true. But then $p(m+1)$ is true. Since $n = m+1$, we have that $p(n)$ is true.

  In any case, we've proved that $p(n)$ is true, as required.

- (ii) $\Rightarrow$ (i). For $n \in \mathbb{N}$, denote the following statement by $H(n)$

$$[\forall m \in \mathbb{N}, \, (n = m+1 \Rightarrow p(m))] \Rightarrow p(n)$$

  Assume $H(n)$ is true for all $n \in \mathbb{N}$. We prove that $p(0)$ is true and, for all $n \in \mathbb{N}$, if $p(n)$ is true then $p(n+1)$ is true.

  ◇ $p(0)$ is true. Indeed, for any $m \in \mathbb{N}$ we have that $0 = m+1$ is false, so the statement $0 = m+1 \Rightarrow p(m)$ is true. Hence $\forall m \in \mathbb{N}, \, (0 = m+1 \Rightarrow p(m))$ is true. Since $H(0)$ is true, it follows that $p(0)$ is true.

  ◇ Fix $n \in \mathbb{N}$ and suppose $p(n)$ is true. By $H(n+1)$, we have that if $p(n+1)$ is true for all $m \in \mathbb{N}$ with $m+1 = n+1$, then $p(n+1)$ is true. But the only $m \in \mathbb{N}$ such that $m+1 = n+1$ is n itself, and $p(n)$ is true by assumption; so by $H(n+1)$, we have $p(n+1)$, as required.

Hence the two induction principles are equivalent. ◁

Example 5.3.18

◁

Structural induction from well-founded induction

We will now derive the principle of structural induction in terms of the principle of well-founded induction. To do this, we need to associate to each inductively defined set X a corresponding well-founded relation R_X, such that well-founded induction on R_X corresponds with structural induction on X.

Definition 5.3.19

Let X be an inductively defined set. Define a relation R_X on X as follows: for all $x, y \in X$, $x \ R_X \ y$ if and only if

$$y = f(x_1, x_2, \ldots, x_n)$$

for some constructor f of arity n and elements $x_1, x_2, \ldots, x_n$, such that $x_i = x$ for some $i \in [n]$.

Example 5.3.20

Let $\mathbb{N}$ be the set of natural numbers, taken to be inductively defined in the usual way. Since the only constructor is the successor operation, we must have for $m, n \in \mathbb{N}$ that

$$m \ R_{\mathbb{N}} \ n \quad \Leftrightarrow \quad n = m + 1$$

This is precisely the relation $<^1$ from Exercise 5.3.11. We already established that structural induction on $\mathbb{N}$ is precisely weak induction (Example 5.3.6), and that well-founded induction on $<^1$ is also precisely weak induction (Example 5.3.17).   ◁

Example 5.3.21

Let P be a set of propositional variables and let $L(P)$ be the set of propositional formulae built from variables in P and the logical operators $\wedge$, $\vee$, $\Rightarrow$ and $\neg$.

Then $R = R_{L(P)}$ is the relation defined for $s, t \in L(P)$ by letting $s \ R \ t$ if and only if

$$t \in \{s \wedge u, \ u \wedge s, \ s \vee u, \ u \vee s, \ s \Rightarrow u, \ u \Rightarrow s, \ \neg s\}$$

for some $u \in L(P)$.   ◁

The plan for the rest of this section is to demonstrate that structural induction follows from well-founded induction. To do this, we prove that the relation R_X associated with an inductively defined set X is well-founded, and then we prove that structural induction on X is equivalent to well-founded induction on R_X.

To simplify our proofs, we introduce the notion of *rank*. The rank of an element x of an inductively defined set X is a natural number which says how many constructors need to be applied in order to obtain x.

Definition 5.3.22

Let X be an inductively defined set. The function rank : $X \to \mathbb{N}$ is defined recursively as follows:

- If b is a basic element of X, then $\text{rank}(b) = 0$.

- Let f be a constructor of arity n and let $x_1, x_2, \ldots, x_n \in X$. Then

$$\text{rank}(f(x_1, x_2, \ldots, x_n)) = \max\{\text{rank}(x_1), \text{rank}(x_2), \ldots, \text{rank}(x_n)\} + 1$$

Note that rank : $X \to \mathbb{N}$ is a well-defined function, since by the conditions listed in Definition 5.3.1, every element of X is either basic or has a unique representation in the form $f(x_1, x_2, \ldots, x_n)$ for some constructor f and elements $x_1, x_2, \ldots, x_n \in X$.

Example 5.3.23
The rank function on the inductively defined set of natural numbers is fairly boring. Indeed, it tells us that

- rank$(0) = 0$; and

- rank$(n + 1) = $ rank$(n) + 1$ for all $n \in \mathbb{N}$.

It can easily be seen that rank$(n) = n$ for all $n \in \mathbb{N}$. This makes sense, since n can be obtained from 0 by iterating the successor operation n times. ◁

Lemma 5.3.24
Let X be an inductively defined set. The relation R_X defined in Definition 5.3.19 is well-founded.

Proof. □

Proof of Theorem 5.3.5. **To do:** Write proof □

To do: Examples and exercises

Chapter 6

Real analysis

6.1   Inequalities and bounds

We first encountered the real numbers in Section 1.1, when the real numbers were introduced using a vague (but intuitive) notion of an *infinite number line* (Definition 1.1.24):

$$
\begin{array}{ccccccccccc}
-5 & -4 & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5
\end{array}
$$
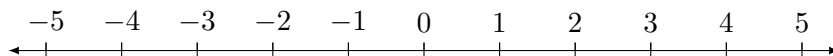
This section will scrutinise the set of real numbers in its capacity as a *complete ordered field*. Decomposing what this means:

- A *field* is a set with a notion of 'zero' and 'one', in which it makes sense to talk about addition, subtraction, multiplication, and division by everything except zero. Examples are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{Z}/p\mathbb{Z}$ when p is a prime number (but not when p is composite). However, $\mathbb{Z}$ is not a field, since we can't freely divide by nonzero elements—for example, $1 \in \mathbb{Z}$ and $2 \in \mathbb{Z}$, but no integer n satisfies $2n = 1$.

- An *ordered field* is a field which is equipped with a well-behaved notion of order. Both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields, but $\mathbb{Z}/p\mathbb{Z}$ is not. We'll see why soon.

- A *complete ordered field* is an ordered field in which every set with an upper bound has a *least* upper bound. As we will see, $\mathbb{Q}$ is not a complete ordered field, but $\mathbb{R}$ is.

We will first establish a small set of rules (axioms) that a set (with appropriate structure) should follow in order to be considered a complete ordered field. The rest of the section will be concerned with proving some theorems that will be extremely useful in real analysis. Most of these theorems are *inequalities*, that is statements that exploit the order structure of the reals. Later in the section, we will consider *suprema* and *infima*, which exploit the completeness of the reals.

⊛ Axiomatising the real numbers

First on our agenda is establishing a set of rules that characterise the reals.

First and foremost, we should be able to perform arithmetic with real numbers—real numbers can be added, subtracted, multiplied and divided (except by zero). This is to say that the real numbers are a *field*—Axioms 6.1.1 make this precise.

Axioms 6.1.1 (Field axioms)
Let X be a set equipped with elements 0 ('zero') and 1 ('unit'), and binary operations $+$

('addition') and · ('multiplication'). The structure $(X, 0, 1, +, \cdot)$ is a **field** if it satisfies the following axioms:

- **Zero and unit**

   (F1) $0 \neq 1$.

- **Axioms for addition**

   (F2) (Associativity) $x + (y + z) = (x + y) + z$ for all $x, y, z \in X$.

   (F3) (Identity) $x + 0 = x$ for all $x \in X$.

   (F4) (Inverse) For all $x \in X$, there exists $y \in X$ such that $x + y = 0$.

   (F5) (Commutativity) $x + y = y + x$ for all $x, y \in X$.

- **Axioms for multiplication**

   (F6) (Associativity) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in X$.

   (F7) (Identity) $x \cdot 1 = x$ for all $x \in X$.

   (F8) (Inverse) For all $x \in X$ with $x \neq 0$, there exists $y \in X$ such that $x \cdot y = 1$.

   (F9) (Commutativity) $x \cdot y = y \cdot x$ for all $x, y \in X$.

- **Distributivity**

   (F10) $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ for all $x, y, z \in X$.

Example 6.1.2

The rationals $\mathbb{Q}$ and the reals $\mathbb{R}$ both form fields with their usual notions of zero, unit, addition and multiplication. However, the integers $\mathbb{Z}$ do not, since for example 2 has no multiplicative inverse. ◁

Example 6.1.3

Let $p > 0$ be prime. The set $\mathbb{Z}/p\mathbb{Z}$ (see Definition 5.1.36) is a field, with zero element $[0]_p$ and unit element $[1]_p$, and with addition and multiplication defined by

$$[a]_p + [b]_p = [a + b]_p \quad \text{and} \quad [a]_p \cdot [b]_p = [ab]_p$$

for all $a, b \in \mathbb{Z}$. Well-definedness of these operations is immediate from Theorem 3.3.6 and the modular arithmetic theorem (Theorem 3.3.9).

The only axiom which is not easy to verify is the multiplicative inverse axiom (F8). Indeed, if $[a]_p \in \mathbb{Z}/p\mathbb{Z}$ then $[a]_p \neq [0]_p$ if and only if $p \nmid a$. But if $p \nmid a$ then $a \perp p$, so a has a multiplicative inverse u modulo p. This implies that $[a]_p \cdot [u]_p = [au]_p = [1]_p$. So (F8) holds. ◁

Exercise 6.1.4

Let $n > 0$ be composite. Prove that $\mathbb{Z}/n\mathbb{Z}$ is not a field, where zero, unit, addition and multiplication are defined as in Example 6.1.3. ◁

Axioms 6.1.1 tell us that every element of a field has an additive inverse, and every *nonzero* element of a field has a multiplicative inverse. It would be convenient if inverses were *unique* whenever they exist. Proposition 6.1.5 proves that this is the case.

Proposition 6.1.5 (Uniqueness of inverses)

Let $(X, 0, 1, +, \cdot)$ be a field and let $x \in X$. Then

(a) Suppose $y, z \in X$ are such that $x + y = 0$ and $x + z = 0$. Then $y = z$.

(b) Suppose $x \neq 0$ and $y, z \in X$ are such that $x \cdot y = 1$ and $x \cdot z = 1$. Then $y = z$.

Proof of (a). By calculation, we have

$$
\begin{aligned}
y &= y + 0 && \text{by (F3)} \\
&= y + (x + z) && \text{by definition of } z \\
&= (y + x) + z && \text{by associativity (F2)} \\
&= (x + y) + z && \text{by commutativity (F5)} \\
&= 0 + z && \text{by definition of } y \\
&= z + 0 && \text{by commutativity (F5)} \\
&= z && \text{by (F3)}
\end{aligned}
$$

so indeed $y = z$.

The proof of (b) is essentially the same and is left as an exercise. $\square$

Since inverses are unique, it makes sense to have notation to refer to them.

Notation 6.1.6

Let $(X, 0, 1, +, \cdot)$ be a field and let $x \in X$. Write $-x$ for the (unique) additive inverse of x and, if $x \neq 0$ write x^{-1} for the (unique) multiplicative inverse of x.

Example 6.1.7

In the fields $\mathbb{Q}$ and $\mathbb{R}$, the additive inverse $-x$ of an element x is simply its negative, and the multiplicative inverse x^{-1} of some $x \neq 0$ is simply its reciprocal $\frac{1}{x}$. ◁

Example 6.1.8

Let $p > 0$ be prime and let $[a]_p \in \mathbb{Z}/p\mathbb{Z}$. Then $-[a]_p = [-a]_p$ and, if $p \nmid a$, then $[a]_p^{-1} = [u]_p$, where u is any integer satisfying $au \equiv 1 \bmod p$. ◁

Example 6.1.9
Let $(X, 0, 1, +, \cdot)$ be a field. We prove that if $x \in X$ then $x \cdot 0 = 0$. Well, $0 = 0 + 0$ by (F3). Hence $x \cdot 0 = x \cdot (0 + 0)$. By distributivity (F10), we have $x \cdot (0 + 0) = (x \cdot 0) + (x \cdot 0)$. Hence

$$x \cdot 0 = (x \cdot 0) + (x \cdot 0)$$

Let $y = -(x \cdot 0)$. Then

$$
\begin{aligned}
0 &= x \cdot 0 + y && \text{by (F4)} \\
&= ((x \cdot 0) + (x \cdot 0)) + y && \text{as above} \\
&= (x \cdot 0) + ((x \cdot 0) + y) && \text{by associativity (F2)} \\
&= (x \cdot 0) + 0 && \text{by (F4)} \\
&= x \cdot 0 && \text{by (F3)}
\end{aligned}
$$

so indeed we have $x \cdot 0 = 0$. ◁

Exercise 6.1.10
Let $(X, 0, 1, +, \cdot)$ be a field. Prove that $(-1)^{-1} = -1$. ◁

What makes the real numbers useful is not simply our ability to add, subtract, multiply and divide them; we can also compare their size—indeed, this is what gives rise to the informal notion of a *number line*. Axioms 6.1.11 make precise exactly what it means for the elements of a field to be assembled into a 'number line'.

Axioms 6.1.11 (Ordered field axioms)
Let X be a set, $0, 1 \in X$ be elements, $+, \cdot$ be binary operations, and $\leqslant$ be a relation on X. The structure $(X, 0, 1, +, \cdot, \leqslant)$ is an **ordered field** if it satisfies the field axioms (F1)–(F10) (see Axioms 6.1.1) and, additionally, it satisfies the following axioms:

- **Linear order axioms**

  (PO1) (Reflexivity) $x \leqslant x$ for all $x \in X$.

  (PO2) (Antisymmetry) For all $x, y \in X$, if $x \leqslant y$ and $y \leqslant x$, then $x = y$.

  (PO3) (Transitivity) For all $x, y, z \in X$, if $x \leqslant y$ and $y \leqslant z$, then $x \leqslant z$.

  (PO4) (Linearity) For all $x, y \in X$, either $x \leqslant y$ or $y \leqslant x$.

- **Interaction of order with arithmetic**

  (OF1) For all $x, y, z \in \mathbb{R}$, if $x \leqslant y$, then $x + z \leqslant y + z$.

  (OF2) For all $x, y \in \mathbb{R}$, if $0 \leqslant x$ and $0 \leqslant y$, then $0 \leqslant xy$.

Example 6.1.12

The field $\mathbb{Q}$ of rational numbers and and the field $\mathbb{R}$ of real numbers, with their usual notions of ordering, can easily be seen to form ordered fields.   ◁

Example 6.1.13

We prove that, in any ordered field, we have $0 \leqslant 1$. Note first that either $0 \leqslant 1$ or $1 \leqslant 0$ by linearity (PO4). If $0 \leqslant 1$ then we're done, so suppose $1 \leqslant 0$. Then $0 \leqslant -1$; indeed:

$$
\begin{aligned}
0 &= 1 + (-1) && \text{by (F4)} \\
&\leqslant 0 + (-1) && \text{by (OF1), since } 1 \leqslant 0 \\
&= (-1) + 0 && \text{by commutativity (F5)} \\
&= -1 && \text{by (F3)}
\end{aligned}
$$

By (OF2), it follows that $0 \leqslant (-1)(-1)$. But $(-1)(-1) = 1$ by Exercise 6.1.10, and hence $0 \leqslant 1$. Since $1 \leqslant 0$ and $0 \leqslant 1$, we have $0 = 1$ by antisymmetry (PO2). But this contradicts axiom (F1). Hence $0 \leqslant 1$. In fact, $0 < 1$ since $0 \neq 1$.   ◁

We have seen that $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields (Examples 6.1.7 and 6.1.12), and that $\mathbb{Z}/p\mathbb{Z}$ is a field for $p > 0$ prime (Example 6.1.3). The following proposition is an interesting result proving that there is no notion of 'ordering' under which the field $\mathbb{Z}/p\mathbb{Z}$ can be made into an ordered field!

Proposition 6.1.14

Let $p > 0$ be prime. There is no relation $\leqslant$ on $\mathbb{Z}/p\mathbb{Z}$ which satisfies the ordered field axioms.

Proof. We just showed that $[0] \leqslant [1]$. It follows that, for all $a \in \mathbb{Z}$, we have $[a] \leqslant [a] + [1]$; indeed:

$$
\begin{aligned}
[a] &= [a] + [0] && \text{by (F3)} \\
&\leqslant [a] + [1] && \text{by (OF1), since } [0] \leqslant [1] \\
&= [a + 1] && \text{by definition of } + \text{ on } \mathbb{Z}/p\mathbb{Z}
\end{aligned}
$$

It is a straightforward induction to prove that $[a] \leqslant [a + n]$ for all $n \in \mathbb{N}$. But then we have

$$[1] \leqslant [1 + (p - 1)] = [p] = [0]$$

so $[0] \leqslant [1]$ and $[1] \leqslant [0]$. This implies $[0] = [1]$ by antisymmetry (PO2), contradicting axiom (F1).   □

Exercise 6.1.15

Let $(X, 0, 1, +, \cdot)$ be a field. Prove that if X is finite, then there is no relation $\leqslant$ on X such that $(X, 0, 1, +, \cdot, \leqslant)$ is an ordered field.   ◁

Theorem 6.1.16 below summarises some properties of ordered fields which will be useful in our proofs. Note, however, that this is certainly *not* an exhaustive list of elementary properties of ordered fields that we will use in our subsequent proofs—to explicitly state and prove all of these would not make for a scintillating read.

Theorem 6.1.16

Let $(X, 0, 1, +, \cdot, \leqslant)$ be an ordered field. Then

(a) For all $x, y \in X$, $x \leqslant y$ if and only if $0 \leqslant y - x$;

(b) For all $x \in X$, $-x \leqslant 0 \leqslant x$ or $x \leqslant 0 \leqslant -x$;

(c) For all $x, x', y, y' \in X$, if $x \leqslant x'$ and $y \leqslant y'$, then $x + y \leqslant x' + y'$;

(d) For all $x, y, z \in X$, if $0 \leqslant x$ and $y \leqslant z$, then $xy \leqslant xz$;

(e) For all nonzero $x \in X$, if $0 \leqslant x$, then $0 \leqslant x^{-1}$.

(f) For all nonzero $x, y \in X$, if $x \leqslant y$, then $y^{-1} \leqslant x^{-1}$.

Proof of (a), (b) and (e).

(a) ($\Rightarrow$) Suppose $x \leqslant y$. Then by additivity (OF1), $x + (-x) \leqslant y + (-x)$, that is $0 \leqslant y - x$.
($\Leftarrow$) Suppose $0 \leqslant y - x$. By additivity (OF1), $0 + x \leqslant (y - x) + x$; that is, $x \leqslant y$.

(b) We know by linearity (PO4) that either $0 \leqslant x$ or $x \leqslant 0$. If $0 \leqslant x$, then by (OF1) we have $0 + (-x) \leqslant x + (-x)$, that is $-x \leqslant 0$. Likewise, if $x \leqslant 0$ then $0 \leqslant -x$.

(e) Suppose $0 \leqslant x$. By linearity (PO4), either $0 \leqslant x^{-1}$ or $x^{-1} \leqslant 0$. If $x^{-1} \leqslant 0$, then by (d) we have $x^{-1} \cdot x \leqslant 0 \cdot x$, that is $1 \leqslant 0$. This contradicts Example 6.1.13, so we must have $0 \leqslant x^{-1}$.

The proofs of the remaining properties are left as an exercise. $\qquad\qquad\square$

We wanted to characterise the reals completely, but so far we have failed to do so—indeed, Exercise 6.1.12 showed that both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields, so the ordered field axioms do not suffice to distinguish $\mathbb{Q}$ from $\mathbb{R}$. The final piece in the puzzle is *completeness*. This single additional axiom distinguishes $\mathbb{Q}$ from $\mathbb{R}$, and in fact completely characterises $\mathbb{R}$ (see Theorem 6.1.18).

Axioms 6.1.17 (Complete ordered field axioms)

Let X be a set, $0, 1 \in X$ be elements, $+, \cdot$ be binary operations, and $\leqslant$ be a relation on X. The structure $(X, 0, 1, +, \cdot, \leqslant)$ is a **complete ordered field** if it is an ordered field—that

is, it satisfies axioms (F1)–(F10), (PO1)–(PO4) and (OF1)–(OF2) (see Axioms 6.1.1 and 6.1.11)—and, in addition, it satisfies the following **completeness axiom**:

(C1) Let $A \subseteq X$. If A has an upper bound, then it has a least upper bound. Specifically, if there exists $u \in X$ such that $a \leqslant u$ for all $a \in A$, then there exists $s \in X$ such that

> ⋄ $a \leqslant s$ for all $a \in A$; and
> ⋄ If $s' \in X$ is such that $a \leqslant s'$ for all $a \in A$, then $s \leqslant s'$.

We call such a value $s \in X$ a **supremum** for A.

Theorem 6.1.18

The real numbers $(\mathbb{R}, 0, 1, +, \cdot, \leqslant)$ form a compete ordered field. Moreover, any two complete ordered fields are essentially the same.[a]   □

---

[a]The notion of 'sameness' here is *isomorphism* (specifically, isomorphism of ordered fields), a concept which is beyond the scope of these notes.

The proof of Theorem 6.1.18 is intricate and far beyond the scope of these notes, so is omitted. What it tells us is that it doesn't matter exactly how we define the reals, since any complete ordered field will do. We can therefore proceed with confidence that, no matter what notion of 'real numbers' we settle on, everything we prove will be true of that notion. This is for the best, since we haven't actually defined the set $\mathbb{R}$ of real numbers at all!

The two most common approaches to constructing a set of real numbers are:

- **Dedekind reals.** In this approach, real numbers are identified with particular subsets of $\mathbb{Q}$—informally speaking, $r \in \mathbb{R}$ is identified with the set of rational numbers less than r.

- **Cauchy reals.** In this approach, real numbers are identified with equivalence classes of sequences of rational numbers—informally speaking, $r \in \mathbb{R}$ is identified with the set of sequences of rational numbers which converge to r (in the sense of Definition 6.2.7).

Discussion of Dedekind and Cauchy reals is relegated to the appendices of these notes—see Section B.2.

We will focus on the reals in their capacity as a complete ordered field towards the end of this section, when we study suprema and infima. However, the completeness axiom (C1) will not be needed in any of our proofs until that point.

Magnitude and scalar product

In this part of the section, we home in on sets of the form $\mathbb{R}^n$, for $n \in \mathbb{N}$. Elements of $\mathbb{R}^n$ are sequences of the form $(x_1, x_2, \ldots, x_n)$, where each $x_i \in \mathbb{R}$. With our interpretation of the reals $\mathbb{R}$ as a *line*, we can interpret a sequence $(x_1, x_2, \ldots, x_n)$ as a point in *n-dimensional space*:

- 0-dimensional space is a single point. The set $\mathbb{R}^0$ has one element, namely the empty sequence (), so this makes sense.

- 1-dimensional space is a line. This matches our intuition that $\mathbb{R} = \mathbb{R}^1$ forms a line.

- 2-dimensional space is a *plane*. The elements of $\mathbb{R}^2$ are pairs (x, y), where x and y are both real numbers. We can interpret the pair (x, y) as *coordinates* for a point which is situated x units to the right of $(0,0)$ and y units above $(0,0)$ (where negative values of x or y reverse this direction)—see Figure 6.1.

$(-3, 2)$ $(-2, 2)$ $(-1, 2)$ $(0, 2)$ $(1, 2)$ $(2, 2)$ $(3, 2)$

$(-3, 1)$ $(-2, 1)$ $(-1, 1)$ $(0, 1)$ $(1, 1)$ $(2, 1)$ $(3, 1)$

$(-3, 0)$ $(-2, 0)$ $(-1, 0)$ $(0, 0)$ $(1, 0)$ $(2, 0)$ $(3, 0)$

$(-3, -1)$ $(-2, -1)$ $(-1, -1)$ $(0, -1)$ $(1, -1)$ $(2, -1)$ $(3, -1)$
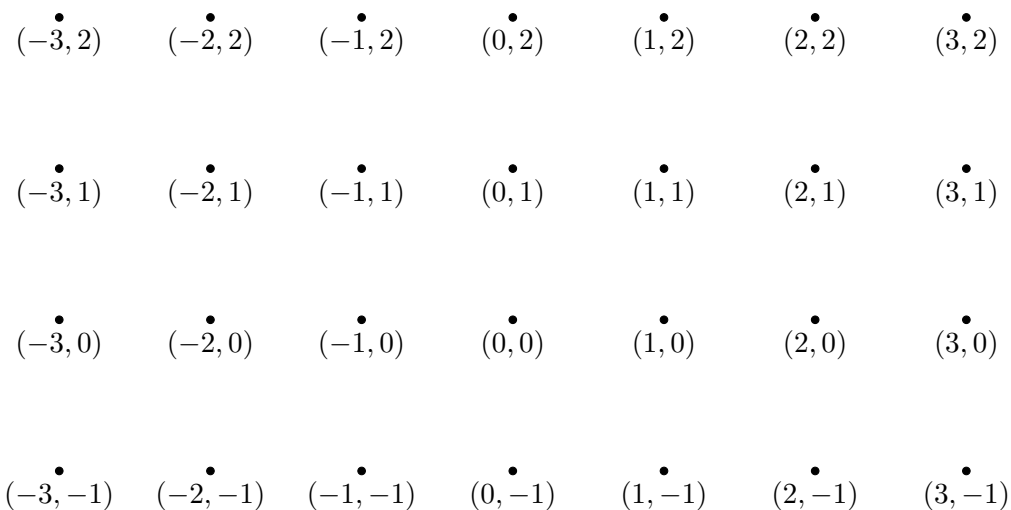
Figure 6.1: Some points in $\mathbb{R}^2$

With this intuition in mind, we set up the following notation.

Notation 6.1.19

Let $n \in \mathbb{N}$. Elements of $\mathbb{R}^n$ will be denoted $\vec{x}, \vec{y}, \vec{z}, \ldots$ (LaTeX code: `\vec`) and called (*n*-**dimensional**) **vectors**. Given a vector $\vec{x} \in \mathbb{R}^n$, we write x_i for the ith **component** of $\vec{x}$, so that

$$\vec{x} = (x_1, x_2, \ldots, x_n)$$

The element $(0, 0, \ldots, 0) \in \mathbb{R}^n$ is called the **origin** or **zero vector** of $\mathbb{R}^n$, and is denoted by $\vec{0}$.

Moreover, if $\vec{x}, \vec{y} \in \mathbb{R}^n$ and $a \in \mathbb{R}$ we write

$$\vec{x} + \vec{y} = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \quad \text{and} \quad a\vec{x} = (ax_1, ax_2, \ldots, ax_n)$$

Example 6.1.20

For all $\vec{x} \in \mathbb{R}^n$, we have

$$\vec{x} + \vec{0} = \vec{x} \quad \text{and} \quad 1\vec{x} = \vec{x}$$

◁

Definition 6.1.21

Let $\vec{x} \in \mathbb{R}^n$. The **magnitude** of $\vec{x}$ is the real number $\|\vec{x}\|$ (LaTeX code: `\lVert \vec x \rVert`) defined by

$$\|\vec{x}\| = \sqrt{\sum_{i=1}^{n} x_i^2} = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}$$

Given vectors $\vec{x}, \vec{y} \in \mathbb{R}^n$, the **distance** from $\vec{x}$ to $\vec{y}$ is defined to be $\|\vec{y} - \vec{x}\|$. Thus the magnitude of a vector can be thought of as the distance from that vector to the origin.

Example 6.1.22

In $\mathbb{R}^2$, Definition 6.1.21 says that

$$\|(x, y)\| = \sqrt{x^2 + y^2}$$

This matches the intuition obtained from the Pythagorean theorem on the sides of right-hand triangles. For example, consider the triangle with vertices $(0, 0)$, $(4, 0)$ and $(4, 3)$:
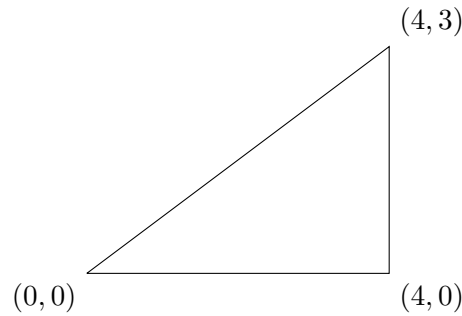
The hypotenuse of the triangle has magnitude

$$\|(4, 3)\| = \sqrt{4^2 + 3^2} = \sqrt{25} = 5$$

◁

Exercise 6.1.23

Let $\vec{x}, \vec{y} \in \mathbb{R}^n$. Prove that $\|\vec{x} - \vec{y}\| = \|\vec{y} - \vec{x}\|$. That is, the distance from $\vec{x}$ to $\vec{y}$ is equal to the distance from $\vec{y}$ to $\vec{x}$. ◁

Exercise 6.1.24

Prove that if $x \in \mathbb{R}$ then the magnitude $\|(x)\|$ is equal to the absolute value $|x|$. ◁

Exercise 6.1.25

Let $\vec{x} \in \mathbb{R}^n$. Prove that $\|\vec{x}\| = 0$ if and only if $\vec{x} = \vec{0}$. ◁

The triangle inequality and the Cauchy–Schwarz inequality

The first, and simplest, inequality that we investigate is the (one-dimensional version of the) *triangle inequality* (Theorem 6.1.27). It is so named because of a generalisation to higher dimensions (Theorem 6.1.37), which can be interpreted geometrically as saying that the sum of two side lengths of a triangle is greater than or equal to the third side length.

The triangle inequality is used very frequently in mathematical proofs—you will encounter it repeatedly in Sections 6.2 and 6.3—yet its proof is surprisingly simple.

Before we can prove the triangle inequality, we need the following fact about square roots of real numbers.

Lemma 6.1.26

Let $x, y \in \mathbb{R}$. If $0 \leqslant x \leqslant y$, then $\sqrt{x} \leqslant \sqrt{y}$.

Proof. Suppose $0 \leqslant x \leqslant y$. Note that, by definition of the square root symbol, we have $\sqrt{x} \geqslant 0$ and $\sqrt{y} \geqslant 0$.

Suppose $\sqrt{x} > \sqrt{y}$. By two applications of Theorem 6.1.16(d), we have

$$y = \sqrt{y} \cdot \sqrt{y} < \sqrt{x} \cdot \sqrt{y} < \sqrt{x} \cdot \sqrt{x} = x$$

so that $y < x$. But this contradicts the assumption that $x \leqslant y$. Hence $\sqrt{x} \leqslant \sqrt{y}$, as required. □

Theorem 6.1.27 (Triangle inequality in one dimension)

Let $x, y \in \mathbb{R}$. Then $|x + y| \leqslant |x| + |y|$. Moreover, $|x + y| = |x| + |y|$ if and only if x and y have the same sign.

Proof. Note first that $xy \leqslant |xy|$; indeed, xy and $|xy|$ are equal if xy is non-negative, and

otherwise we have $xy < 0 < |xy|$. Also $x^2 = |x|^2$ and $y^2 = |y|^2$. Hence

$$(x + y)^2 = x^2 + 2xy + y^2 \leqslant |x|^2 + 2|xy| + |y|^2 = (|x| + |y|)^2$$

Taking (nonnegative) square roots yields

$$|x + y| \leqslant ||x| + |y||$$

by Lemma 6.1.26. But $|x| + |y| \geqslant 0$, so $||x| + |y|| = |x| + |y|$. This completes the first part of the proof.

Equality holds in the above if and only if $xy = |xy|$, which occurs if and only if $xy \geqslant 0$. But this is true if and only if x and y are both non-negative or both non-positive—that is, they have the same sign.   □

Example 6.1.28

Let $x, y \in \mathbb{R}$. We prove that

$$\frac{|x + y|}{1 + |x + y|} \leqslant \frac{|x|}{1 + |x|} + \frac{|y|}{1 + |y|}$$

First note that, if $0 \leqslant s \leqslant t$, then

$$\frac{s}{1 + s} \leqslant \frac{t}{1 + t}$$

To see this, note that

$$
\begin{aligned}
s \leqslant t \Rightarrow 1 + s \leqslant 1 + t & \qquad\qquad \text{rearranging} \\
\Rightarrow \frac{1}{1 + t} \leqslant \frac{1}{1 + s} & \qquad\qquad \text{since } 1 + s, 1 + t \geqslant 0 \\
\Rightarrow 1 - \frac{1}{1 + s} \leqslant 1 - \frac{1}{1 + t} & \qquad\qquad \text{rearranging} \\
\Rightarrow \frac{s}{1 + s} \leqslant \frac{t}{1 + t} & \qquad\qquad \text{rearranging}
\end{aligned}
$$

Now letting $s = |x + y|$ and $t = |x| + |y|$, we have $s \leqslant t$ by the triangle inequality, and hence

$$\frac{|x + y|}{1 + |x + y|} \leqslant \frac{|x|}{1 + |x| + |y|} + \frac{|y|}{1 + |x| + |y|} \leqslant \frac{|x|}{1 + |x|} + \frac{|y|}{1 + |y|}$$

as required.   ◁

Exercise 6.1.29

Let $n \in \mathbb{N}$ and let $x_i \in \mathbb{R}$ for each $i \in [n]$. Prove that

$$\left| \sum_{i=1}^{n} x_i \right| \leqslant \sum_{i=1}^{n} |x_i|$$

with equality if and only if the numbers x_i are either all positive or all negative.   ◁

Exercise 6.1.30

Let $x, y \in \mathbb{R}$. Prove that

$$\big|\,|x| - |y|\,\big| \leqslant |x - y|$$

◁

We will generalise the triangle inequality to arbitrary dimensions in Theorem 6.1.37. Our proof will go via the *Cauchy–Schwarz inequality* (Theorem 6.1.34). To motivate the Cauchy–Schwarz inequality, we introduce another geometric notion called the *scalar product* of two vectors.

Definition 6.1.31

Let $\vec{x}, \vec{y} \in \mathbb{R}^n$. The **scalar product** (or **dot product**) of $\vec{x}$ with $\vec{y}$ is the real number $\vec{x} \cdot \vec{y}$ (LaTeX code: `\cdot`) defined by

$$\vec{x} \cdot \vec{y} = \sum_{i=1}^{n} x_i y_i = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$$

Example 6.1.32

Let $\vec{x} \in \mathbb{R}^n$. Then $\vec{x} \cdot \vec{x} = \|\vec{x}\|^2$. Indeed

$$\vec{x} \cdot \vec{x} = \sum_{i=1}^{n} x_i^2 = \|\vec{x}\|^2$$

◁

Exercise 6.1.33

Let $\vec{x}, \vec{y}, \vec{z}, \vec{w} \in \mathbb{R}^n$ and let $a, b, c, d \in \mathbb{R}$. Prove that

$$(a\vec{x} + b\vec{y}) \cdot (c\vec{z} + d\vec{w}) = ac(\vec{x} \cdot \vec{z}) + ad(\vec{x} \cdot \vec{w}) + bc(\vec{y} \cdot \vec{z}) + bd(\vec{y} \cdot \vec{w})$$

◁

Intuitively, the scalar product of two vectors $\vec{x}$ and $\vec{y}$ measures the extent to which $\vec{x}$ and $\vec{y}$ fail to be *orthogonal*. In fact, if θ is the acute angle formed between the lines ℓ_1 and ℓ_2, where ℓ_1 passes through $\vec{0}$ and $\vec{x}$ and ℓ_2 passes through $\vec{0}$ and $\vec{y}$, then a formula for the scalar product of $\vec{x}$ and $\vec{y}$ is given by

$$\vec{x} \cdot \vec{y} = \|\vec{x}\|\|\vec{y}\| \cos\theta$$
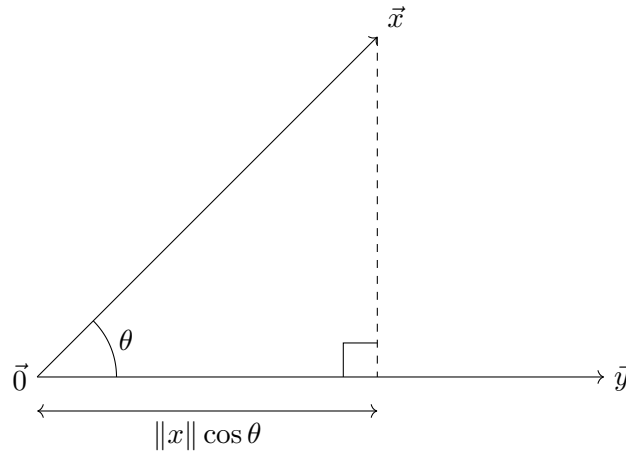
Evidently, $\vec{x}$ and $\vec{y}$ are orthogonal if and only if $\cos\theta = 0$, in which case $\vec{x} \cdot \vec{y} = 0$ as well. We cannot prove this yet, though, as we have not yet defined trigonometric functions or explored their properties, but hopefully this provides some useful intuition.

The Cauchy–Schwarz inequality provides a useful comparison of the size of a scalar product of two vectors with the magnitudes of the vectors.

Theorem 6.1.34 (Cauchy–Schwarz inequality)
Let $n \in \mathbb{N}$ and let $x_i, y_i \in \mathbb{R}$ for each $i \in [n]$. Then

$$|\vec{x} \cdot \vec{y}| \leqslant \|\vec{x}\|\|\vec{y}\|$$

with equality if and only if $a\vec{x} = b\vec{y}$ for some $a, b \in \mathbb{R}$ which are not both zero.

Proof. If $\vec{y} = \vec{0}$, then this is trivial: both sides of the equation are equal to zero! So assume that $\vec{y} \neq \vec{0}$. In particular, by Exercise 6.1.25, we have $\|\vec{y}\| > 0$.

Define $k = \dfrac{\vec{x} \cdot \vec{y}}{\|\vec{y}\|^2}$. Then

$$\begin{aligned}
0 \leqslant \|\vec{x} - k\vec{y}\|^2 \qquad &\text{since squares are nonnegative} \\
= (\vec{x} - k\vec{y}) \cdot (\vec{x} - k\vec{y}) \qquad &\text{by Example 6.1.32} \\
= (\vec{x} \cdot \vec{x}) - 2k(\vec{x} \cdot \vec{y}) + k^2(\vec{y} \cdot \vec{y}) \qquad &\text{by Exercise 6.1.33} \\
= \|\vec{x}\|^2 - \frac{(\vec{x} \cdot \vec{y})^2}{\|y\|^2} \qquad &\text{by definition of } k
\end{aligned}$$

Multiplying through by $\|\vec{y}\|^2$, which is non-negative and therefore doesn't change the sign of the inequality, yields

$$0 \leqslant \|\vec{x}\|^2 \|\vec{y}\|^2 - (\vec{x} \cdot \vec{y})^2$$

which is equivalent to what was to be proved.

Evidently, equality holds if and only if $\|\vec{x} - k\vec{y}\| = 0$, which by Exercise 6.1.25 occurs if and only if $\vec{x} - k\vec{y} = 0$. Now:

- If $\vec{x} - k\vec{y} = 0$, then we have

$$
\begin{aligned}
& \vec{x} - k\vec{y} = 0 \\
& \Leftrightarrow \vec{x} - \frac{\vec{x} \cdot \vec{y}}{\|\vec{y}\|^2}\vec{y} = 0 && \text{by definition of } k \\
& \Leftrightarrow \|\vec{y}\|^2 \vec{x} = (\vec{x} \cdot \vec{y})\vec{y} && \text{rearranging}
\end{aligned}
$$

  If $\vec{y} \neq \vec{0}$ then let $a = \|\vec{y}\|^2$ and $b = \vec{x} \cdot \vec{y}$; otherwise, let $a = 0$ and $b = 1$. In both cases, we have $a\vec{x} = b\vec{y}$ and a, b are not both zero.

  If $a\vec{x} = b\vec{y}$ for some $a, b \in \mathbb{R}$ not both zero, then either:

  ◇ $a = 0$ and $b \neq 0$, in which case $\vec{y} = 0$ and we have equality in the Cauchy–Schwarz inequality; or

  ◇ $a \neq 0$, in which case $\vec{y} = \frac{b}{a}\vec{x}$. Write $c = \frac{b}{a}$. Then

$$
\begin{aligned}
|\vec{x} \cdot \vec{y}| &= |\vec{x} \cdot (c\vec{x})| \\
&= |c(\vec{x} \cdot \vec{x})| && \text{by Exercise 6.1.33} \\
&= |c|\|\vec{x}\|^2 && \text{by Example 6.1.32} \\
&= \|\vec{x}\|\|c\vec{x}\| && \text{rearranging} \\
&= \|\vec{x}\|\|\vec{y}\|
\end{aligned}
$$

  In either case, we have equality in the Cauchy–Schwarz inequality.

So equality holds if and only if $a\vec{x} = b\vec{y}$ for some $a, b \in \mathbb{R}$ not both zero. □

Example 6.1.35
Let $a, b, c \in \mathbb{R}$. We'll prove that

$$ab + bc + ca \leqslant a^2 + b^2 + c^2$$

and examine when equality holds.

Letting $\vec{x} = (a, b, c)$ and $\vec{y} = (b, c, a)$ yields

$$\vec{x} \cdot \vec{y} = ab + bc + ca$$

and

$$\|\vec{x}\| = \sqrt{a^2 + b^2 + c^2} = \sqrt{b^2 + c^2 + a^2} = \|\vec{y}\|$$

Hence $\|\vec{x}\|\|\vec{y}\| = a^2 + b^2 + c^2$. By the Cauchy–Schwarz inequality, it follows that

$$\vec{x} \cdot \vec{y} = ab + bc + ca \leqslant a^2 + b^2 + c^2 = \|\vec{x}\|\|\vec{y}\|$$

as required. Equality holds if and only if $k(a, b, c) = \ell(b, c, a)$ for some $k, \ell \in \mathbb{R}$ not both zero. We may assume $k \neq 0$—otherwise, swap the vectors $\vec{x}$ and $\vec{y}$ in what follows. Then, letting $t = \frac{\ell}{k}$, we have

$$
\begin{aligned}
&k(a, b, c) = \ell(b, c, a) \\
&\Leftrightarrow (a, b, c) = (tb, tc, ta) &&\text{by definition of } t \\
&\Leftrightarrow (a, b, c) = (t^2 c, t^2 a, t^2 b) &&\text{substituting } a = tb \text{ etc.} \\
&\Leftrightarrow (a, b, c) = (t^3 a, t^3 b, t^3 c) &&\text{substituting } a = tb \text{ etc. again} \\
&\Leftrightarrow \vec{x} = t^3 \vec{x}
\end{aligned}
$$

This occurs if and only if either $(a, b, c) = (0, 0, 0)$, or $t = 1$, in which case

$$(a, b, c) = (tb, tc, ta) = (b, c, a)$$

So equality holds if and only if $a = b = c$.   ◁

Exercise 6.1.36
Let $r \in \mathbb{N}$ and let $a_1, a_2, \ldots, a_r \in \mathbb{R}$ be such that $a_1^2 + a_2^2 + \cdots + a_n^2 = 6$. Prove that

$$(a_1 + 2a_2 + \cdots + na_n)^2 \leqslant n(n+1)(2n+1)$$

and determine when equality holds.   ◁

We now use the Cauchy–Schwarz inequality to generalise the one-dimensional version of the triangle inequality (Theorem 6.1.27) to arbitrary (finite) dimensions.

Theorem 6.1.37 (Triangle inequality)
Let $\vec{x}, \vec{y} \in \mathbb{R}^2$. Then
$$\|\vec{x} + \vec{y}\| \leqslant \|\vec{x}\| + \|\vec{y}\|$$
with equality if and only if $a\vec{x} = b\vec{y}$ for some real numbers $a, b \geqslant 0$.

Proof. We proceed by calculation:

$$
\begin{aligned}
\|\vec{x} + \vec{y}\|^2 &= (\vec{x} + \vec{y}) \cdot (\vec{x} + \vec{y}) && \text{by Example 6.1.32} \\
&= (\vec{x} \cdot \vec{x}) + 2(\vec{x} \cdot \vec{y}) + (\vec{y} \cdot \vec{y}) && \text{by Exercise 6.1.33} \\
&\leqslant (\vec{x} \cdot \vec{x}) + 2|\vec{x} \cdot \vec{y}| + (\vec{y} \cdot \vec{y}) && \text{since } a \leqslant |a| \text{ for all } a \in \mathbb{R} \\
&\leqslant \|\vec{x}\|^2 + 2\|x\|\|y\| + \|\vec{y}\|^2 && \text{by Exercise 6.1.32 and Cauchy–Schwarz} \\
&= (\|\vec{x}\| + \|\vec{y}\|)^2 && \text{rearranging}
\end{aligned}
$$

Taking (nonnegative) square roots of both sides yields

$$
\|\vec{x} + \vec{y}\| \leqslant \|\vec{x}\| + \|\vec{y}\|
$$

by Lemma 6.1.26, as required.

Equality holds if and only if the two '$\leqslant$' symbols in the above derivation are in fact '$=$' symbols.

- The first inequality is equality if and only if $\vec{x} \cdot \vec{y} = |\vec{x} \cdot \vec{y}|$, which holds if and only if $\vec{x} \cdot \vec{y} \geqslant 0$.

- The second inequality is equality if and only if equality holds in the Cauchy–Schwarz inequality. In turn, this occurs if and only if $a\vec{x} = b\vec{y}$ for some $a, b \in \mathbb{R}$. We may, moreover, assume that $a \geqslant 0$—if not, replace a and b by their negatives.

If $a = 0$ then we can take $b = 0$. If $a > 0$, then by Example 6.1.32 and Exercise 6.1.33, we have

$$
\vec{x} \cdot \left(\frac{b}{a}\vec{x} \right) = \frac{b}{a}\|\vec{x}\|^2
$$

which is non-negative if and only if $b \geqslant 0$, since we are assuming that $a \geqslant 0$.

Thus, equality holds in the triangle inequality if and only if $a\vec{x} = b\vec{y}$ for some $a, b \geqslant 0$. $\quad\square$

This general version of the triangle inequality has a geometric interpretation in terms of—you guessed it—triangles. Any three points $\vec{a}, \vec{b}, \vec{c} \in \mathbb{R}^n$ form a (potentially flat) triangle:
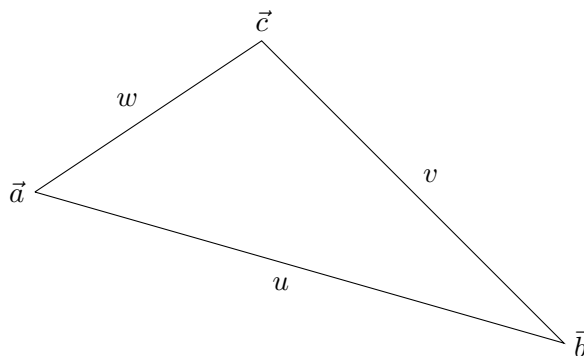
The side lengths u, v, w are given by the following equations:

$$u = \|\vec{b} - \vec{a}\|, \quad v = \|\vec{c} - \vec{b}\|, \quad w = \|\vec{a} - \vec{c}\|$$

The triangle inequality says tells us that $u \leqslant v + w$. Indeed:

$$
\begin{aligned}
u &= \|\vec{b} - \vec{a}\| && \text{by definition of } u \\
&= \|(\vec{b} - \vec{c}) + (\vec{c} - \vec{a})\| && \text{rearranging} \\
&\leqslant \|\vec{b} - \vec{c}\| + \|\vec{c} - \vec{a}\| && \text{by the triangle inequality} \\
&= \|\vec{c} - \vec{b}\| + \|\vec{a} - \vec{c}\| && \text{by Exercise 6.1.23} \\
&= v + w && \text{by definition of } v \text{ and } w
\end{aligned}
$$

That is, the triangle inequality says that the sum of two side lengths of a triangle is greater than or equal to the third side length. Moreover, it tells us $u = v + w$ precisely when $k(\vec{a} - \vec{c}) = \ell(\vec{c} - \vec{b})$ for some $k, \ell \geqslant 0$. If $k = 0$ then

$$\vec{c} \quad = \quad \vec{b} \quad = \quad 0\vec{a} + (1 - 0)\vec{b}$$

if $k > 0$, then $k + \ell > 0$, so we have

$$\vec{c} \quad = \quad \frac{k}{k + \ell}\vec{a} + \frac{\ell}{k + \ell}\vec{b} \quad = \quad \frac{k}{k + \ell}\vec{a} + \left(1 - \frac{k}{k + \ell}\right)\vec{b}$$

Examining this a bit more closely yields that $u = v + w$ if and only if

$$\vec{c} = t\vec{a} + (1 - t)\vec{b}$$

for some $0 \leqslant t \leqslant 1$, which is to say precisely that $\vec{c}$ lies on the line segment between $\vec{a}$ and $\vec{b}$. In other words, equality holds in the triangle inequality only if the three vertices of the triangle are *collinear*, which is to say that the triangle whose vertices are the points $\vec{a}$, $\vec{b}$ and $\vec{c}$, is flat.

Inequalities of means

Our goal now is to explore different kinds of average—specifically, *means*—of finite sets of non-negative real numbers. We will compare the relative sizes of these means with respect to one-another, with emphasis on three particular kinds of mean: the *arithmetic mean* (Definition 6.1.38), the *geometric mean* (Definition 6.1.40) and the *harmonic mean* (Definition 6.1.48). These means in fact assemble into a continuum of means, called *generalised means* (Definition 6.1.56), all of which can be compared with one another.

Definition 6.1.38
Let $n \geqslant 1$. The (**arithmetic**) **mean** of real numbers $x_1, \ldots, x_n$ is

$$\frac{1}{n} \sum_{i=1}^{n} x_i = \frac{x_1 + x_2 + \cdots + x_n}{n}$$

Example 6.1.39
The arithmetic mean of the numbers   ◁

Definition 6.1.40
Let $n \geqslant 1$. The **geometric mean** of non-negative real numbers $x_1, \ldots, x_n$ is

$$\sqrt[n]{\prod_{i=1}^{n} x_i} = \sqrt[n]{x_1 \cdot x_2 \cdot \cdots \cdot x_n}$$

The following theorem is commonly known as the **AM–GM inequality**.

Theorem 6.1.41 (Inequality of arithmetic and geometric means)
Let $n \in \mathbb{N}$ and $x_1, x_2, \ldots, x_n \geqslant 0$. Then

$$\underbrace{\sqrt[n]{x_1 \cdots x_n}}_{\text{geometric mean}} \leqslant \underbrace{\frac{x_1 + \cdots + x_n}{n}}_{\text{arithmetic mean}}$$

with equality if and only if $x_1 = \cdots = x_n$.

Proof when $n = 2$. We need to show that, if $x, y \in \mathbb{R}$ with $x, y \geqslant 0$, then

$$\sqrt{xy} \leqslant \frac{x + y}{2}$$

with equality if and only if $x = y$.

First note that the square roots of x and y exist since they are non-negative. Now

$$
\begin{aligned}
0 \leqslant (\sqrt{x} - \sqrt{y})^2 & \qquad \text{since squares are nonnegative} \\
= (\sqrt{x})^2 - 2\sqrt{x}\sqrt{y} + (\sqrt{y})^2 & \qquad \text{expanding} \\
= x - 2\sqrt{xy} + y & \qquad \text{rearranging}
\end{aligned}
$$

Rearranging the inequality $0 \leqslant x - 2\sqrt{xy} + y$ yields the desired result.

If $\sqrt{xy} = \frac{x+y}{2}$, then we can rearrange the equation as follows:

$$
\begin{aligned}
\sqrt{xy} = \frac{x + y}{2} \Rightarrow 2\sqrt{xy} = x + y & \qquad \text{multiplying by 2} \\
\Rightarrow 4xy = x^2 + 2xy + y^2 & \qquad \text{squaring both sides} \\
\Rightarrow x^2 - 2xy + y^2 = 0 & \qquad \text{rearranging} \\
\Rightarrow (x - y)^2 = 0 & \qquad \text{factorising} \\
\Rightarrow x - y = 0 & \qquad \text{since } a^2 = 0 \Rightarrow a = 0 \text{ for } a \in \mathbb{R} \\
\Rightarrow x = y & \qquad \text{rearranging}
\end{aligned}
$$

So we have proved both parts of the theorem. □

Example 6.1.42
We use the AM–GM inequality to prove that the area of a rectangle with fixed perimeter is maximised when the rectangle is a square.

Indeed, fix a perimeter $p > 0$, and let $x, y > 0$ be side lengths of a rectangle with perimeter p—that is, x and y satisfy the equation $2x + 2y = p$. The area a of the rectangle satisfies $a = xy$. By the AM–GM inequality, we have

$$
a = xy \leqslant \left(\frac{x + y}{2} \right)^2 = \frac{p^2}{16}
$$

Equality holds if and only if $x = y$, in other words, if and only if the rectangle is a square. ◁

Exercise 6.1.43
Let $a, b > 0$ be real numbers. Prove that $\dfrac{a^2 + b^2}{2} \geqslant ab$. ◁

Example 6.1.44
Let $x > 0$. We find the minimum possible value of $x + \frac{9}{x}$. By the AM–GM inequality, we have

$$
x + \frac{9}{x} \geqslant 2\sqrt{x \cdot \frac{9}{x}} = 2\sqrt{9} = 6
$$

with equality if and only if $x = \frac{9}{x}$, which occurs if and only if $x = 3$. Hence the minimum value of $x + \frac{9}{x}$ when $x > 0$ is 6. ◁

Exercise 6.1.45

Let $x > 0$ and let $n \in \mathbb{N}$. Find the minimum possible value of $\displaystyle\sum_{k=-n}^{n} x^k$. ◁

Exercises 6.1.46 and 6.1.47 complete the proof of the AM–GM inequality (Theorem 6.1.41). Before proceeding with the exercises, let's fix some notation: for each $n \in \mathbb{N}$, let $p_{\text{AM–GM}}(n)$ be the assertion that the AM–GM inequality holds for collections of n numbers; that is, $p_{\text{AM–GM}}(n)$ is the assertion:

> For all $x_1, x_2, \ldots, x_n \geqslant 0$, we have
> $$\frac{1}{n}\sum_{i=1}^{n} x_i \leqslant \sqrt[n]{\prod_{i=1}^{n} x_i}$$
> with equality if and only if $x_1 = x_2 = \cdots = x_n$.

Note that we already proved $p_{\text{AM–GM}}(2)$.

Exercise 6.1.46

Let $r \in \mathbb{N}$ and let $x_1, x_2, \ldots, x_{2r} \in \mathbb{R}$. Write

$$a = \frac{1}{r}\sum_{i=1}^{r} x_i \quad \text{and} \quad g = \sqrt[r]{\prod_{i=1}^{r} x_i}$$

for the arithmetic and geometric means, respectively, of the numbers $x_1, \ldots, x_r$; write

$$a' = \frac{1}{r}\sum_{i=r+1}^{2r} x_i \quad \text{and} \quad g' = \sqrt[r]{\prod_{i=r+1}^{2r} x_i}$$

for the arithmetic and geometric means, respectively, of the numbers $x_{r+1}, \ldots, x_{2r}$; and write

$$A = \frac{1}{2r}\sum_{i=1}^{2r} x_i \quad \text{and} \quad G = \sqrt[2r]{\prod_{i=1}^{2r} x_i}$$

for the arithmetic and geometric means, respectively, of all the numbers $x_1, \ldots, x_{2r}$.

Prove that

$$A = \frac{a + a'}{2} \quad \text{and} \quad G = \sqrt{gg'}$$

Deduce that, for each $r \in \mathbb{N}$, if $p_{\text{AM–GM}}(r)$ is true then $p_{\text{AM–GM}}(2r)$ is true. Deduce further than $p_{\text{AM–GM}}(2^m)$ is true for all $m \in \mathbb{N}$. ◁

Exercise 6.1.47

Let $r \geqslant 2$ and let $x_1, \ldots, x_{r-1} \in \mathbb{N}$. Define

$$x_r = \frac{1}{r-1} \sum_{i=1}^{r-1} x_i$$

Prove that

$$\frac{1}{r} \sum_{i=1}^{r} x_i = x_r$$

Assuming $p_{\text{AM–GM}}(r)$, deduce that

$$x_r^r \leqslant \prod_{i=1}^{r} x_i = \left(\prod_{i=1}^{r-1} x_i \right) \cdot x_r$$

with equality if and only if $x_1 = x_2 = \cdots = x_r$. Deduce that $p_{\text{AM–GM}}(r)$ implies $p_{\text{AM–GM}}(r-1)$. Use Exercise 6.1.46 to deduce further that $p_{\text{AM–GM}}(n)$ is true for all $n \geqslant 1$. ◁

We now introduce another kind of mean, called the *harmonic mean*.

Definition 6.1.48

Let $n \in \mathbb{N}$. The **harmonic mean** of nonzero real numbers $x_1, x_2, \ldots, x_n$ is

$$\left(\frac{1}{n} \sum_{i=1}^{n} x_i^{-1} \right)^{-1} = \frac{n}{\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}}$$

The harmonic mean of two nonzero real numbers x and y has a simpler expression:

$$\left(\frac{x^{-1} + y^{-1}}{2} \right)^{-1} = \frac{2xy}{x+y}$$

The harmonic mean arises naturally when considering

Example 6.1.49

The cities of York and Leeds are located $d > 0$ miles apart. Two cars drive from York to Leeds, then immediately turn around and drive back. The two cars depart from York at the same time and arrive back in York at the same time.

- The first car drives from York to Leeds at a constant speed of u miles per hour, and drives back to York at a constant speed of v miles per hour.

- The second car drives from York to Leeds and back again at the same constant speed of w miles per hour.

According to the following formula from physics:

$$\text{speed} \times \text{time} = \text{distance}$$

the time spent driving by the first car is $\frac{d}{u} + \frac{d}{v}$, and the time spent driving by the second car is $\frac{2d}{w}$.

Since the cars spend the same amount of time driving, it follows that

$$\frac{2d}{w} = \frac{d}{u} + \frac{d}{v} \qquad \Rightarrow \qquad w = \frac{2uv}{u+v}$$

That is, the second car's speed is the harmonic mean of the two speeds driven by the first car. ◁

As might be expected, we now prove a theorem relating the harmonic means with the other means we have established so far—this theorem is known as the **GM–HM inequality**.

Theorem 6.1.50 (Inequality of geometric and harmonic means)
Let $n \in \mathbb{N}$ and $x_1, x_2, \ldots, x_n > 0$. Then

$$\underbrace{\frac{n}{\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}}}_{\text{harmonic mean}} \leqslant \underbrace{\sqrt[n]{x_1 x_2 \cdots x_n}}_{\text{geometric mean}}$$

with equality if and only if $x_1 = \cdots = x_n$.

Proof when $n = 2$. We need to prove that if $x, y > 0$, then

$$\frac{2}{\frac{1}{x} + \frac{1}{y}} \leqslant \sqrt{xy}$$

This is almost immediate from the AM–GM inequality (Theorem 6.1.41). Indeed, since all numbers in sight are positive, we can take reciprocals to see that this inequality is equivalent to the assertion that

$$\frac{1}{\sqrt{xy}} \leqslant \frac{x^{-1} + y^{-1}}{2}$$

But $\frac{1}{\sqrt{xy}} = \sqrt{x^{-1}y^{-1}}$, so this is immediate from the AM–GM inequality.   □

Exercise 6.1.51
Prove the GM–HM inequality for general values of $n \in \mathbb{N}$.   ◁

Another example of a mean that has applications in probability theory and statistics is that of the *quadratic mean*.

Definition 6.1.52
Let $n \in \mathbb{N}$. The **quadratic mean** (or **root-mean-square**) of real numbers $x_1, x_2, \ldots, x_n$ is

$$\left(\frac{1}{n} \sum_{i=1}^{n} x_i^2 \right)^{\frac{1}{2}} = \sqrt{\frac{x_1^2 + x_2^2 + \cdots + x_n^2}{n}}$$

The following theorem is, predictably, known as the **QM–AM inequality** (or **RMS–AM inequality**); it is a nice application of the Cauchy–Schwarz inequality.

Theorem 6.1.53 (Inequality of quadratic and arithmetic means)
Let $n > 0$ and $x_1, x_2, \ldots, x_n \geqslant 0$. Then

$$\underbrace{\frac{x_1 + \cdots + x_n}{n}}_{\text{arithmetic mean}} \leqslant \underbrace{\sqrt{\frac{x_1^2 + x_2^2 + \cdots + x_n^2}{n}}}_{\text{quadratic mean}}$$

with equality if and only if $x_1 = \cdots = x_n$.

Proof. Define

$$\vec{x} = (x_1, x_2, \ldots, x_n) \quad \text{and} \quad \vec{y} = (1, 1, \ldots, 1)$$

Then

$$
\begin{aligned}
x_1 + x_2 + \cdots + x_n &= \vec{x} \cdot \vec{y} && \text{by definition of scalar product} \\
&\leqslant \|\vec{x}\| \|\vec{y}\| && \text{by Cauchy–Schwarz} \\
&= \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2} \cdot \sqrt{n} && \text{evaluating the magnitudes}
\end{aligned}
$$

Dividing through by n yields

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \leqslant \sqrt{\frac{x_1^2 + x_2^2 + \cdots + x_n^2}{n}}$$

as required. Equality holds if and only if equality holds in the Cauchy–Schwarz inequality, which occurs if and only if

$$(ax_1, ax_2, \ldots, ax_n) = (b, b, \ldots, b)$$

for some $a, b \in \mathbb{R}$ not both zero. If $a = 0$ then $b = 0$, so we must have $a \neq 0$. Hence equality holds if and only if $x_i = \frac{b}{a}$ for all $i \in [n]$—in particular, if and only if $x_1 = x_2 = \cdots = x_n$. $\quad\square$

To summarise, what we have proved so far is

$$\begin{array}{cccccccc}
\text{harmonic} & \overset{(6.1.50)}{\leqslant} & \text{geometric} & \overset{(6.1.41)}{\leqslant} & \text{arithmetic} & \overset{(6.1.53)}{\leqslant} & \text{quadratic} \\
\text{mean} & & \text{mean} & & \text{mean} & & \text{mean}
\end{array}$$

with equality in each case if and only if the real numbers whose means we are taking are all equal.

The following exercise allows us to bookend our chain of inequalities with the minimum and maximum of the collections of numbers.

Exercise 6.1.54

Let $n > 0$ and let $x_1, x_2, \ldots, x_n$ be positive real numbers. Prove that

$$\min\{x_1, x_2, \ldots, x_n\} \leqslant \left(\frac{1}{n} \sum_{i=1}^{n} x_i^{-1} \right)^{-1} \quad \text{and} \quad \max\{x_1, x_2, \ldots, x_n\} \geqslant \left(\frac{1}{n} \sum_{i=1}^{n} x_i^2 \right)^{\frac{1}{2}}$$

with equality in each case if and only if $x_1 = x_2 = \cdots = x_n$. $\quad\triangleleft$

✳ Generalised means

We conclude this section by mentioning a generalisation of the results we have proved about means. We are not yet ready to prove the results that we mention; they are only here for the sake of interest.

Definition 6.1.55

The **extended real number line** is the (ordered) set $[-\infty, \infty]$, defined by

$$[-\infty, \infty] = \mathbb{R} \cup \{-\infty, \infty\}$$

where $\mathbb{R}$ is the set of real numbers with its usual ordering, and $-\infty, \infty$ are new elements ordered in such a way that $-\infty < x < \infty$ for all $x \in \mathbb{R}$.

Note that the extended real line does *not* form a field—the arithmetic operations are not defined on $-\infty$ or ∞, and we will at no point treat $-\infty$ and ∞ as real numbers; they are merely elements which extend the reals to add a least element and a greatest element.

Definition 6.1.56

Let $p \in [-\infty, \infty]$, let $n \in \mathbb{N}$, and let $x_1, x_2, \ldots, x_n$ be positive real numbers. The **generalised mean with exponent** p (or simply p-**mean**) $x_1, x_2, \ldots, x_n$ is the real number $M_p(x_1, x_2, \ldots, x_n)$ defined by

$$M_p(x_1, x_2, \ldots, x_n) = \left(\frac{1}{n} \sum_{i=1}^{n} x_i^p \right)^{\frac{1}{p}}$$

if $p \notin \{-\infty, 0, \infty\}$, and by

$$M_p(x_1, x_2, \ldots, x_n) = \lim_{q \to p} M_q(x_1, x_2, \ldots, x_n)$$

if $p \in \{-\infty, 0, \infty\}$, where the notation $\lim_{q \to p}$ refers to the **limit**, to be defined in Section 8.5.

We can see immediately that the harmonic, arithmetic and quadratic means of a finite set of positive real numbers are the p-means for a suitable value of p: the harmonic mean is the (-1)-mean, the arithmetic mean is the 1-mean, and the quadratic mean is the 2-mean. Furthermore, Proposition 6.1.57 exhibits the *minimum* as the $(-\infty)$-mean, the *geometric mean* as the 0-mean, and the *maximum* as the ∞-mean.

Proposition 6.1.57

Let $n > 0$ and let $x_1, x_2, \ldots, x_n \geqslant 0$. Then

- $M_{-\infty}(x_1, x_2, \ldots, x_n) = \min\{x_1, x_2, \ldots, x_n\}$;

- $M_0(x_1, x_2, \ldots, x_n) = \sqrt[n]{x_1 x_2 \cdots x_n}$; and

- $M_\infty(x_1, x_2, \ldots, x_n) = \min\{x_1, x_2, \ldots, x_n\}$. $\qquad\qquad\square$

All of the inequalities of means we have seen so far will be subsumed by Theorem 6.1.58, which compares the p-mean and q-mean of a set of numbers for all values of $p, q \in [-\infty, \infty]$.

Theorem 6.1.58

Let $n > 0$, let $x_1, x_2, \ldots, x_n \geqslant 0$ and let $p, q \in [-\infty, \infty]$ with $p < q$. Then

$$M_p(x_1, x_2, \ldots, x_n) \leqslant M_q(x_1, x_2, \ldots, x_n)$$

with equality if and only if $x_1 = x_2 = \cdots = x_n$. □

Theorem 6.1.58 implies each of the following:

- **HM–min inequality** (Exercise 6.1.54): take $p = -\infty$ and $q = -1$;

- **GM–HM inequality** (Theorem 6.1.50): take $p = -1$ and $q = 0$;

- **AM–GM inequality** (Theorem 6.1.41): take $p = 0$ and $q = 1$;

- **QM–AM inequality** (Theorem 6.1.53): take $p = 1$ and $q = 2$;

- **max–QM inequality** (Exercise 6.1.54): take $p = 2$ and $q = \infty$.

6.2   Sequences and convergence

<div align="center">

Warning!

This section is not yet finished—do not rely on its correctness or completeness.

</div>

As we saw at the beginning of Section 6.1, the property of the real numbers that really sets them apart from the rational numbers is *completeness* (see Axioms 6.1.17), which says that every set of real numbers with an upper bound has a supremum. This seemingly innocuous statement turns out to form the basis of all of real analysis, since it allows us to reason about mathematical objects involving real numbers by studying their local behaviour (**To do:** Write chapter intro describing local behaviour and refer back to it).

Sequences of real numbers

To do: Motivate sequences

Definition 6.2.1

A **sequence of real numbers** is a function $x : \mathbb{N} \to \mathbb{R}$. Given a sequence x, we write x_n instead of $x(n)$ and write $(x_n)_{n \geqslant 0}$, or even just (x_n), instead of $x : \mathbb{N} \to \mathbb{R}$. The values x_n are called the **terms** of the sequence, and the variable n is called the **index** of the term x_n.

Example 6.2.2

Some very basic but very boring examples of sequences are *constant sequences*. For example, the constant sequence with value 0 is

$$(0, 0, 0, 0, 0, 0, \dots)$$

More generally, for fixed $a \in \mathbb{R}$, the constant sequence with value a is defined by $x_n = a$ for all $n \in \mathbb{N}$. ◁

Example 6.2.3

Sequences can be defined just like functions. For example, there is a sequence defined by $x_n = 2^n$ for all $n \in \mathbb{N}$. Writing out the first few terms, this sequence is

$$(1, 2, 4, 8, 16, \dots)$$

◁

Sometimes it will be convenient to start the indexing of our sequence from numbers other than 0, particularly when an expression involving a variable n isn't defined when $n = 0$. We'll denote such sequences by $(x_n)_{n \geqslant 1}$ or $(x_n)_{n \geqslant 2}$, and so on.

Example 6.2.4

Let $(z_n)_{n \geqslant 2}$ be the sequence defined by $z_n = \frac{(n+1)(n+2)}{(n-1)n}$ for all $n \geqslant 2$:

$$\left(6, \frac{10}{3}, \frac{5}{2}, \frac{21}{10}, \cdots \right)$$

The indexing of this sequence begins at 2, rather than 0, since when $n = 0$ or $n = 1$, the expression $\frac{(n+1)(n+2)}{(n-1)n}$ is undefined. We could *reindex* the sequence: by letting $z'_n = z_{n+2}$ for all $n \geqslant 0$, we obtain a new sequence $(z'_n)_{n \geqslant 0}$ defined by $z'_n = \frac{(n+3)(n+4)}{(n+1)(n+2)}$ whose indexing starts from 0. Fortunately for us, such matters won't cause any problems—it's just important to make sure that whenever we define a sequence, we make sure the terms make sense for all of the indices. ◁

Of particular interest to us will be sequences whose terms get closer and closer to a fixed real number.

Example 6.2.5

Consider the sequence $(y_n)_{n \geqslant 1}$ defined by $y_n = \frac{1}{n}$ for all $n \geqslant 1$:

$$\left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \cdots \right)$$

It is fairly clear that the terms y_n become closer and closer to 0 as n grows; the following diagram is a plot of y_n against n for a few values of n. ◁

Example 6.2.6

Define a sequence $(r_n)_{n \geqslant 0}$ by $r_n = \frac{2n}{n+1}$ for all $n \in \mathbb{N}$. Some of the values of this sequence are illustrated in the following table:

n	r_n	decimal expansion
0	0	0
1	1	1
2	$\frac{4}{3}$	$1.333\ldots$
3	$\frac{3}{2}$	1.5
$\vdots$	$\vdots$	$\vdots$
10	$\frac{20}{11}$	$1.818\ldots$
$\vdots$	$\vdots$	$\vdots$
100	$\frac{200}{101}$	$1.980\ldots$
$\vdots$	$\vdots$	$\vdots$
1000	$\frac{2000}{1001}$	$1.998\ldots$
$\vdots$	$\vdots$	$\vdots$

As n increases, the values of r_n become closer and closer to 2. ◁

The precise sense in which the terms of the sequences in Examples 6.2.5 and 6.2.6 'get closer' to 0 and 2, respectively, is called *convergence*, which we will define momentarily in Definition 6.2.7.

First, let's try to work out what the definition *should be* for a sequence (x_n) to converge to a real number a.

A naïve answer might be to say that the sequence is 'eventually equal to a'—that is, after some point in the sequence, all terms are equal to a. Unfortunately, this isn't quite good enough: if it were, then the values $r_n = \frac{2n}{n+1}$ from Example 6.2.6 would be equal to 2 for sufficiently large n. However, if for some $n \in \mathbb{N}$ we have $\frac{2n}{n+1} = 2$, then it follows that $2n = 2(n+1)$; rearranging this gives $1 = 0$, which is a contradiction.

However, this answer isn't too far from giving us what we need. Instead of saying that the terms x_n are eventually *equal* to a, we might want to say that they become *infinitely close* to a, whatever that means.

We can't really make sense of an 'infinitely small positive distance' (e.g. Exercise 1.2.13), so we might instead make sense of 'infinitely close' by saying that the terms x_n eventually become as close to a as we could possibly want them to be. Spelling this out, this means that for any positive distance ε (LaTeX code: `\varepsilon`) (read: 'epsilon')[a] no matter how small, the terms x_n are eventually within distance ε of a. In summary:

---

[a] The lower case Greek letter *epsilon* (ε) is traditionally used in analysis to denote a positive quantity whose value can be made arbitrarily small. We will encounter this letter frequently in this section and the next when discussing convergence.

> **Definition 6.2.7**
>
> Let (x_n) be a sequence and let $a \in \mathbb{R}$. We say that (x_n) **converges** to a, and write $(x_n) \to a$ (LaTeX code: `\to`), if the following condition holds:
>
> $$\forall \varepsilon > 0, \ \exists N \in \mathbb{N}, \ \forall n \geqslant N, \ |x_n - a| < \varepsilon$$
>
> The value a is called a **limit** of (x_n). Moreover, we say that a sequence (x_n) **converges** if it has a limit, and diverges otherwise.

Before we move onto some examples, let's quickly digest the definition of the expression $(x_n) \to a$. The following table presents a suggestion of how you might read the expression '$\forall \varepsilon > 0, \ \exists N \in \mathbb{N}, \ \forall n \geqslant N, \ |x_n - a| < \varepsilon$' in English.

Symbols	English
$\forall \varepsilon > 0 \ldots$	For any positive distance ε (no matter how small)...
$\ldots \exists N \in \mathbb{N} \ldots$	...there is a stage in the sequence...
$\ldots \forall n \geqslant N \ldots$	...after which all terms in the sequence...
$\ldots |x_n - a| < \varepsilon.$	...are within distance ε of a.

Thus, a sequence (x_n) converges to a if '*for any positive distance ε (no matter how small), there is a stage in the sequence after which all terms in the sequence are within ε of a*'. After reading this a few times, you should hopefully be content that this definition captures what is meant by saying that the terms in the sequence are eventually as close to a as we could possibly want them to be.

We are now ready to see some examples of convergent (and divergent) sequences. When reading the following proofs, keep in mind the logical structure—that is, the alternating quantifiers $\forall \varepsilon \ldots \exists N \ldots \forall n \ldots$—in the definition of $(x_n) \to a$.

Example 6.2.8

The sequence (y_n) defined by $y_n = \frac{1}{n}$ for all $n \geqslant 1$ converges to 0. To see this, by Definition 6.2.7, we need to prove

$$\forall \varepsilon > 0, \ \exists N \in \mathbb{N}, \ \forall n \geqslant N, \ \left| \frac{1}{n} - 0 \right| < \varepsilon$$

So fix $\varepsilon > 0$. Our goal is to find $N \in \mathbb{N}$ such that $\left| \frac{1}{n} \right| < \varepsilon$ for all $n \geqslant N$.

Let N be any natural number which is greater than $\frac{1}{\varepsilon}$. Then for all $n \geqslant N$, we have

$$
\begin{aligned}
\left|\frac{1}{n}\right| &= \frac{1}{n} && \text{since } \frac{1}{n} > 0 \text{ for all } n \geqslant 1 \\
&\leqslant \frac{1}{N} && \text{since } n \geqslant N \\
&< \frac{1}{1/\varepsilon} && \text{since } N > \frac{1}{\varepsilon} \\
&= \varepsilon
\end{aligned}
$$

Hence $|y_n| < \varepsilon$ for all $n \geqslant N$. Thus we have proved that $(y_n) \to 0$. ◁

Remark 6.2.9
The value of N you need to find in the proof of convergence will usually depend on the parameter ε. (For instance, in Example 6.2.8, we defined N to be some natural number greater than $\frac{1}{\varepsilon}$.) This is to be expected—remember that ε is the distance away from the limit that the terms are allowed to vary after the Nth term. If you make this distance smaller, you'll probably have to go further into the sequence before your terms are all close enough to a. In particular, the value of N will usually grow as the value of ε gets smaller. This was the case in Example 6.2.8: note that $\frac{1}{\varepsilon}$ increases as ε decreases. ◁

Example 6.2.10
Let (r_n) be the sequence from Example 6.2.6 defined by $r_n = \frac{2n}{n+1}$ for all $n \in \mathbb{N}$. We'll prove that $(r_n) \to 2$. So fix $\varepsilon > 0$. We need to find $N \in \mathbb{N}$ such that

$$
\left|\frac{2n}{n+1} - 2\right| < \varepsilon \text{ for all } n \geqslant N
$$

To find such a value of n, we'll first do some algebra. Note first that for all $n \in \mathbb{N}$ we have

$$
\left|\frac{2n}{n+1} - 2\right| = \left|\frac{2n - 2(n+1)}{n+1}\right| = \left|\frac{-2}{n+1}\right| = \frac{2}{n+1}
$$

Rearranging the inequality $\frac{2}{n+1} < \varepsilon$ gives $\frac{n+1}{2} > \frac{1}{\varepsilon}$, and hence $n > \frac{2}{\varepsilon} - 1$.

To be clear, what we've shown so far is that a *necessary* condition for $|r_n - 2| < \varepsilon$ to hold is that $n > \frac{2}{\varepsilon} - 1$. This informs us what the desired value of N might look like—we will then verify that the desired inequality holds.

So define $N = \frac{2}{\varepsilon} - 1$. For all $n \geqslant N$, we have

$$
\begin{aligned}
\left| \frac{2n}{n+1} - 2 \right| = \frac{2}{n+1} && \text{by the above work} \\
\leqslant \frac{2}{N+1} && \text{since } n \geqslant N \\
< \frac{2}{\left(\frac{2}{\varepsilon} - 1 \right) + 1} && \text{since } N > \frac{2}{\varepsilon} - 1 \\
= \frac{2}{2/\varepsilon} && \text{rearranging} \\
= \varepsilon && \text{rearranging}
\end{aligned}
$$

Thus, as claimed, we have $|r_n - 2| < \varepsilon$ for all $n \geqslant N$. It follows that $(r_n) \to 2$, as required. ◁

Exercise 6.2.11
Let (x_n) be the constant sequence with value $a \in \mathbb{R}$. Prove that $(x_n) \to a$. ◁

Exercise 6.2.12
Prove that the sequence (z_n) defined by $z_n = \frac{n+1}{n+2}$ converges to 1. ◁

The following proposition is a technical tool, which proves that convergence of sequences is unaffected by changing finitely many terms at the beginning of a sequence.

Proposition 6.2.13
Let (x_n) be a sequence and suppose that $(x_n) \to a$. Let (y_n) be another sequence and suppose that there is some $k \in \mathbb{N}$ such that $x_n = y_n$ for all $n \geqslant k$. Prove that $(y_n) \to a$.

Proof. Fix $\varepsilon > 0$. We need to find $N \in \mathbb{N}$ such that $|y_n - a| < \varepsilon$ for all $n \geqslant N$.

Since $(x_n) \to a$, there is some $M \in \mathbb{N}$ such that $|x_n - a| < \varepsilon$ for all $n \geqslant M$. Let N be the greater of M and k. Then for all $n \geqslant N$, we have $y_n = x_n$, since $n \geqslant k$, and hence $|y_n - a| = |x_n - a| < \varepsilon$, since $n \geqslant M$.

Hence $(y_n) \to a$, as required. □

Before we go too much further, let's see some examples of sequences which *diverge*. Recall (Definition 6.2.7) that a sequence (x_n) converges if $(x_n) \to a$ for some $a \in \mathbb{R}$. Spelling this out symbolically, to say '(x_n) converges' is to say the following:

$$
\exists a \in \mathbb{R}, \ \forall \varepsilon > 0, \ \exists N \in \mathbb{N}, \ \forall n \geqslant N, \ |x_n - a| < \varepsilon
$$

We can negate this using the tools of Section 2.1: to say that a sequence (x_n) diverges is to say the following:

$$\forall a \in \mathbb{R}, \; \exists \varepsilon > 0, \; \forall N \in \mathbb{N}, \; \exists n \geqslant N, \; |x_n - a| \geqslant \varepsilon$$

In more intuitive terms: for all possible candidates for a limit $a \in \mathbb{R}$, there is a positive distance ε such that, no matter how far down the sequence you go (say x_N), you can find a term x_n beyond that point which is at distance $\geqslant \varepsilon$ away from a.

Example 6.2.14

Let (x_n) be the sequence defined by $x_n = (-1)^n$ for all $n \in \mathbb{N}$:

$$(1, -1, 1, -1, 1, -1, \ldots)$$

We'll prove that (x_n) diverges. Fix $a \in \mathbb{R}$. Intuitively, if a is non-negative, then it must be at distance $\geqslant 1$ away from -1, and if a is negative, then it must be at distance $\geqslant 1$ away from 1. We'll now make this precise.

So let $\varepsilon = 1$, and fix $N \in \mathbb{N}$. We need to find $n \geqslant N$ such that $|(-1)^n - a| \geqslant 1$. We'll split into cases based on whether a is non-negative or negative.

- Suppose $a \geqslant 0$. Then $-1 - a \leqslant -1 < 0$, so that we have

$$|-1 - a| = a - (-1) = a + 1 \geqslant 1$$

  So let $n = 2N + 1$. Then $n \geqslant N$ and n is odd, so that

$$|x_n - a| = |(-1)^n - a| = |-1 - a| \geqslant 1$$

- Suppose $a < 0$. Then $1 - a > 1 > 0$, so that we have

$$|1 - a| = 1 - a > 1$$

  So let $n = 2N$. Then $n \geqslant N$ and n is even, so that

$$|x_n - a| = |(-1)^n - a| = |1 - a| \geqslant 1$$

In both cases, we've found $n \geqslant N$ such that $|x_n - a| \geqslant 1$. It follows that (x_n) diverges. ◁

Example 6.2.14 is an example of a *periodic* sequence—that is, it's a sequence that repeats itself. It is difficult for such sequences to converge since, intuitively speaking, they jump up and down a lot. (In fact, the only way that a period sequence *can* converge is if it is a constant sequence!)

Exercise 6.2.15

Let (y_n) be the sequence defined by $y_n = n$ for all $n \in \mathbb{N}$:

$$(0, 1, 2, 3, \dots)$$

Prove that (y_n) diverges. ◁

Finding limits of sequences can be tricky. The following theorem (Theorem 6.2.16) makes it slightly easier by saying that if a sequence is built up using arithmetic operations—addition, subtraction, multiplication and division—from sequences whose limits you know, then you can simply apply those arithmetic operations to the limits.

Theorem 6.2.16

Let (x_n) and (y_n) be sequences of real numbers, let $a, b \in \mathbb{R}$, and suppose that $(x_n) \to a$ and $(y_n) \to b$. Then

(a) $(x_n + y_n) \to a + b$;

(b) $(x_n - y_n) \to a - b$;

(c) $(x_n y_n) \to ab$; and

(d) $\left(\frac{x_n}{y_n}\right) \to \frac{a}{b}$, so long as $y_n \neq 0$ for all $n \in \mathbb{N}$ and $b \neq 0$.

Proof. **To do:** Write proof ☐

Theorem 6.2.16 *appears* obvious, but as you can see in the proof, it is more complicated than perhaps expected. It was worth the hard work, though, because we can now compute more complicated limits formed in terms of arithmetic operations by taking the limits of the individual components. The following example uses Theorem 6.2.16 to prove that $\left(\frac{2n}{n+1}\right) \to 2$ in a much simpler way than we saw in Example 6.2.10.

Example 6.2.17

We provide another proof that the sequence (r_n) of Example 6.2.6, defined by $r_n = \frac{2n}{n+1}$ for all $n \in \mathbb{N}$, converges to 2.

For all $n \geqslant 1$, dividing by the top and bottom gives

$$r_n = \frac{2}{1 + \frac{1}{n}}$$

The constant sequences (2) and (1) converge to 2 and 1, respectively; and by Example 6.2.8, we know that $\left(\frac{1}{n}\right) \to 0$. It follows that

$$(r_n) \to \frac{2}{1+0} = 2$$

as required.   ◁

Exercise 6.2.18
To do: Write exercise   ◁

To do: Motivate

> **Theorem 6.2.19** (Uniqueness of limits)
> Let (x_n) be a sequence and let $a, b \in \mathbb{R}$. If $(x_n) \to a$ and $(x_n) \to b$, then $a = b$.

Proof. We'll prove that $|a - b| = 0$, which will imply that $a = b$. To do this, we'll prove that $|a - b|$ is not positive: we already know it's non-negative, so this will imply that it is equal to zero. To prove that $|a - b|$ is not positive, we'll prove that it is less than every positive number.

So fix $\varepsilon > 0$. Then also $\frac{\varepsilon}{2} > 0$. The definition of convergence (Definition 6.2.7) tells us that:

- There exists $N_1 \in \mathbb{N}$ such that $|x_n - a| < \frac{\varepsilon}{2}$ for all $n \geqslant N_1$; and

- There exists $N_2 \in \mathbb{N}$ such that $|x_n - b| < \frac{\varepsilon}{2}$ for all $n \geqslant N_2$.

Let n be the greatest of N_1 and N_2. Then $n \geqslant N_1$ and $n \geqslant N_2$, and hence

$$|x_n - a| < \frac{\varepsilon}{2} \quad \text{and} \quad |x_n - b| < \frac{\varepsilon}{2}$$

By the triangle inequality (Theorem 6.1.27), it follows that

$$
\begin{aligned}
|a - b| &= |(a - x_n) + (x_n - b)| &&\text{by cancelling the } x_n \text{ terms} \\
&\leqslant |a - x_n| + |x_n - b| &&\text{by the triangle inequality} \\
&= |x_n - a| + |x_n - b| &&\text{by Exercise 6.1.23} \\
&< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon &&\text{since } n \geqslant N_1 \text{ and } n \geqslant N_2
\end{aligned}
$$

Since $|a - b| < \varepsilon$ for all $\varepsilon > 0$, it follows that $|a - b|$ is a non-negative real number that is less than every positive real number, so that it is equal to zero.

Since $|a - b| = 0$, we have $a - b = 0$, and so $a = b$.   □

Theorem 6.2.19 tells us that if a sequence converges, then its limit is uniquely determined. This allows us to talk about *the* limit of a convergent sequence, and in particular justifies the following notation.

Notation 6.2.20
Let (x_n) be a convergent sequence. Write $\lim_{n\to\infty} x_n$ for its (unique) limit.

To do: Warn about the symbol ∞.

Example 6.2.21
Examples 6.2.8 and 6.2.10 tell us that

$$\lim_{n\to\infty} \frac{1}{n} = 0 \quad \text{and} \quad \lim_{n\to\infty} \frac{2n}{n+1} \to 2$$

◁

To do: Introduce squeeze theorem

Theorem 6.2.22 (Squeeze theorem)
Let (x_n), (y_n) and (z_n) be sequences of real numbers such that:

(i) $(x_n) \to a$ and $(z_n) \to a$; and

(ii) $x_n \leqslant y_n \leqslant z_n$ for all $n \in \mathbb{N}$.

Then $(y_n) \to a$.

Proof. Fix $\varepsilon > 0$. We need to find $N \in \mathbb{N}$ such that $|y_n - a| < \varepsilon$ for all $n \geqslant N$.

Since $(x_n) \to a$ and $(z_n) \to a$, there exist $N_1, N_2 \in \mathbb{N}$ such that

- $|x_n - a| < \varepsilon$ for all $n \geqslant N_1$;
- $|z_n - a| < \varepsilon$ for all $n \geqslant N_2$.

Letting N be the greatest of N_1 and N_2 then tells us that both $|x_n - a|$ and $|z_n - a|$ are less than ε whenever $n \geqslant N$.

We will prove that $|y_n - a| < \varepsilon$ for all $n \geqslant N$. To see this let $n \geqslant N$. Either $y_n \geqslant a$ or $y_n \leqslant a$.

- If $y_n \geqslant a$, then we have $a \leqslant y_n \leqslant z_n$. It follows that

$$|y_n - a| = y_n - a \leqslant z_n - a = |z_n - a| < \varepsilon$$

- If $y_n \leqslant a$, then we have $x_n \leqslant y_n \leqslant a$. It follows that

$$|y_n - a| = a - y_n \leqslant a - x_n = |x_n - a| < \varepsilon$$

Since in both cases we have proved $|y_n - a| < \varepsilon$, we may conclude that $(y_n) \to a$.   □

Example 6.2.23
To do: ◁

Example 6.2.24
To do: ◁

Exercise 6.2.25
To do: ◁

Exercise 6.2.26
To do: ◁

Existence of limits

It is often useful to know that a sequence converges, but not necessary to go to the arduous lengths of computing its limit. However, as it currently stands, we don't really have any tools for proving that a sequence converges other than finding a limit for it! This section explores the properties of $\mathbb{R}$ that allow us to know when a sequence does or does not converge.

First, recall from Section 6.1 that $\mathbb{R}$ is a *complete ordered field* (see Axioms 6.1.17). In fact, it's the only one—this was the content of Theorem 6.1.18. To repeat, this means is that every subset $A \subseteq \mathbb{R}$ that has a (real) upper bound has a least (real) upper bound, called a *supremum*. This property is called *completeness*.

Exercise 6.2.27
Let $A \subseteq \mathbb{R}$. Write down the definitions of what it means for a real number u to be an **upper bound** of A, and what it means for a real number s to be a **supremum** of A.   ◁

We can use the completeness axiom to prove results about existence of limits of sequences.

Perhaps the most fundamental result is the *monotone convergence theorem* (Theorem 6.2.32), since it underlies the proofs of all the other results that we will prove. What it says is that if the terms in a sequence always increase, or always decrease, and the set of terms in the sequence is bounded, then the sequence converges to a limit.

The sequence (r_n) from Example 6.2.6, defined by $r_n = \frac{2n}{n+1}$ for all $n \in \mathbb{N}$, is an example

of such a sequence. We proved that it converged by computing its limit in Example 6.2.10 and again in Example 6.2.17. We will soon (Example 6.2.34) use the monotone convergence theorem to give *yet another proof* that it converges, but this time without going to the trouble of first finding its limit.

Before we can state the monotone convergence theorem, we must first define what we mean by a *monotonic sequence.*

Definition 6.2.28

A sequence of real numbers (x_n) is...

- ...**increasing** if $m \leqslant n$ implies $x_m \leqslant x_n$ for all $m, n \in \mathbb{N}$;

- ...**decreasing** if $m \leqslant n$ implies $x_m \geqslant x_n$ for all $m, n \in \mathbb{N}$.

If a sequence is either increasing or decreasing, we say it is **monotonic**.

Example 6.2.29

The sequence (x_n) defined by $x_n = n^2$ for all $n \in \mathbb{N}$ is increasing, since for all $m, n \in \mathbb{N}$, if $m \leqslant n$, then $m^2 \leqslant n^2$. To see this, note that if $m \leqslant n$, then $n - m \geqslant 0$ and $n + m \geqslant 0$, so that

$$n^2 - m^2 = (n - m)(n + m) \geqslant 0 \cdot 0 = 0$$

and hence $n^2 \geqslant m^2$, as required. ◁

Example 6.2.30

The sequence (r_n) from Example 6.2.6, defined by $r_n = \frac{2n}{n+1}$ for all $n \in \mathbb{N}$, is increasing. To see this, suppose $m \leqslant n$. Then $n = m + k$ for some $k \geqslant 0$. Now

$$
\begin{aligned}
& 0 \leqslant k && \text{by assumption} \\
\Leftrightarrow\ & m^2 + km + m \leqslant m^2 + km + m + k && \text{adding } m^2 + km + m \text{ to both sides} \\
\Leftrightarrow\ & m(m + k + 1) \leqslant (m + 1)(m + k) && \text{factorising} \\
\Leftrightarrow\ & m(n + 1) \leqslant (m + 1)n && \text{since } n = m + k \\
\Leftrightarrow\ & \frac{m}{m + 1} \leqslant \frac{n}{n + 1} && \text{dividing both sides by } (m + 1)(n + 1) \\
\Leftrightarrow\ & r_m \leqslant r_n && \text{by definition of } (r_n)
\end{aligned}
$$

Note that the step where we divided through by $(m+1)(n+1)$ is justified since this quantity is positive.

It is perhaps useful to add that to *come up with* this proof, it is more likely that you would start with the assumption $r_m \leqslant r_n$ and derive that $k \geqslant 0$—noting that all steps are reversible then allows us to write it in the 'correct' order. ◁

Exercise 6.2.31
To do: ◁

Theorem 6.2.32 (Monotone convergence theorem)
Let (x_n) be a sequence of real numbers.

(a) If (x_n) is increasing and has an upper bound,[a] then it converges;

(b) If (x_n) is decreasing and has a lower bound, then it converges.

---

[a]Officially, what it means to say a *sequence* (x_n) has an upper (or lower) bound is to say that the *set* $\{x_n : n \in \mathbb{N}\}$ has an upper (or lower) bound.

Proof of (a). We prove (a) here—part (b) is Exercise 6.2.33.

So suppose (x_n) is increasing and has an upper bound. Then:

(i) $x_m \leqslant x_n$ for all $m \leqslant n$; and

(ii) There is some real number u such that $u \geqslant x_n$ for all $n \in \mathbb{N}$.

Condition (ii) tells us that the set $\{x_n \mid n \in \mathbb{N}\} \subseteq \mathbb{R}$ has an upper bound. By the completeness axiom, it has a supremum a. We prove that $(x_n) \to a$.

So let $\varepsilon > 0$. We need to find $N \in \mathbb{N}$ such that $|x_n - a| < \varepsilon$ for all $n \geqslant N$.

Since a is a supremum of $\{x_n \mid n \in \mathbb{N}\}$, there is some $N \in \mathbb{N}$ such that $x_N > a - \varepsilon$.

Since (x_n) is increasing, by (i) we have $x_N \leqslant x_n$ for all $n \geqslant N$. Moreover, since a is an upper bound for the sequence, we actually have $x_N \leqslant x_n \leqslant a$ for all $n \geqslant N$.

Putting this together, for all $n \geqslant N$, we have

$$\begin{aligned}
|x_n - a| = a - x_n & \qquad \text{since } x_n - a \leqslant 0 \\
\leqslant a - x_N & \qquad \text{since } x_N \leqslant x_n \text{ for all } n \geqslant N \\
< \varepsilon & \qquad \text{since } x_N > a - \varepsilon
\end{aligned}$$

It follows that $(x_n) \to a$, as required.   □

Exercise 6.2.33
Prove part (b) of the monotone convergence theorem (Theorem 6.2.32). That is, prove
that if a sequence (x_n) is decreasing and has a lower bound, then it converges.   ◁

Example 6.2.34
To do: ◁

Example 6.2.35
To do: ◁

Exercise 6.2.36
To do: ◁

Exercise 6.2.37
To do: ◁

To do: subsequences, Cauchy sequences, Bolzano–Weierstrass theorem

6.3   Series and sums

<div align="center">

Warning!

This section is not yet finished—do not rely on its correctness or completeness.

</div>

To do: Lots of stuff

Proposition 6.3.1

Let $x \in \mathbb{R}$ with $-1 < x < 1$. Then $\displaystyle\sum_{n \in \mathbb{N}} x^n = \frac{1}{1-x}$.

Proof. Given $N \in \mathbb{N}$, the Nth partial sum S_N of the series is given by by

$$S_N = \sum_{n=0}^{N} x^n = 1 + x + x^2 + \cdots + x^N$$

Note that

$$x S_N = \sum_{n=0}^{n} x^{n+1} = x + x^2 + \cdots + x^{N+1} = S_{N+1} - 1$$

and hence

$$(1-x)S_N = S_N - xS_N = S_N - (S_{N+1} - 1) = 1 - (S_{N+1} - S_N) = 1 - x^{N+1}$$

and hence dividing by $1 - x$, which is permissible since $x \neq 1$, yields

$$S_N = \frac{1 - x^{N+1}}{1-x}$$

To do: Finish proof $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ $\square$

Proposition 6.3.2

Let $x \in \mathbb{R}$ with $-1 < x < 1$. Then $\displaystyle\sum_{n \in \mathbb{N}} n x^{n-1} = \frac{1}{(1-x)^2}$

Chapter 7

Discrete probability theory

7.1   Discrete probability spaces

Probability theory is a field of mathematics which attempts to model randomness and uncertainty in the 'real world'. The mathematical machinery it develops allows us to understand how this randomness behaves and to extract information which is useful for making predictions.

Discrete probability theory, in particular, concerns situations in which the possible outcomes form a *countable* set. This simplifies matters considerably: if there are only countably many outcomes, then the probability that any event occurs is determined entirely by the probabilities that the individual outcomes comprised by the event occur.

For example, the number N of words spoken by a child over the course of a year takes values in $\mathbb{N}$, so is discrete. To each $n \in \mathbb{N}$, we may assign a probability that $N = n$, which can take positive values in a meaningful way, and from these probabilities we can compute the probabilities of more general events occurring (e.g. the probability that the child says under a million words). However, the height H grown by the child over the same period takes values in $[0, \infty)$, which is uncountable; for each $h \in [0, \infty)$, the probability that $H = h$ is zero, so these probabilities give us no information. We must study the behaviour of H through some other means.

In this chapter, we will concern ourselves only with the discrete setting.

It is important to understand from the outset that, although we use language like *outcome*, *event*, *probability* and *random*, and although we use real-world examples, everything we do concerns mathematical objects: sets, elements of sets, and functions. If we say, for example, "the probability that a roll of a fair six-sided die shows 3 or 4 is $\frac{1}{3}$," we are actually interpreting the situation mathematically—the *outcomes* of the die rolls are interpreted as the elements of the set $[6]$; the *event* that the die shows 3 or 4 is interpreted as the subset $\{3, 4\} \subseteq [6]$; and the *probability* that this event occurs is the value of a particular function $\mathbb{P} : \mathcal{P}([6]) \to [0, 1]$ on input $\{3, 4\}$. The mathematical interpretation is called a **model** of the real-world situation.

Definition 7.1.1

A **discrete probability space** is a pair $(\Omega, \mathbb{P})$ (LaTeX code: `(\Omega, \mathbb{P})`), consisting of a countable set Ω and a function $\mathbb{P} : \mathcal{P}(\Omega) \to [0, 1]$, such that

(i) $\mathbb{P}(\Omega) = 1$; and

(ii) (**Countable additivity**) If $\{A_i \mid i \in I\}$ is any family of pairwise disjoint subsets of Ω, indexed by a countable set I, then

$$\mathbb{P}\left(\bigcup_{i \in I} A_i\right) = \sum_{i \in I} \mathbb{P}(A_i)$$

The set Ω is called the **sample space**; the elements $\omega \in \Omega$ are called **outcomes**;[a] the subsets $A \subseteq \Omega$ are called **events**; and the function $\mathbb{P}$ is called the **probability measure**. Given an event A, the value $\mathbb{P}(A)$ is called the **probability of** A.

---

[a] The symbols Ω, ω (LaTeX code: `\Omega, \omega`) are the upper- and lower-case forms, respectively, of the Greek letter *omega*.

There is a general notion of a probability space, which does not require the sample space Ω to be countable. This definition is significantly more technical, so we restrict our attention in this section to *discrete* probability spaces. Thus, whenever we say 'probability space' in this chapter, the probability space can be assumed to be discrete. However, when our proofs do not specifically use countability of Ω, they typically are true of arbitrary probability spaces. As such, we will specify discreteness in the statement of results only when countability of the sample space is required.

Example 7.1.2

We model the roll of a fair six-sided die.

The possible **outcomes** of the roll are 1, 2, 3, 4, 5 and 6, so we can take $\Omega = [6]$ to be the sample space.

The **events** correspond with subsets of $[6]$. For example:

- $\{4\}$ is the event that the die roll shows 4. This event occurs with probability $\frac{1}{6}$.

- $\{1, 3, 5\}$ is the event that the die roll is odd. This event occurs with probability $\frac{1}{2}$

- $\{1, 4, 6\}$ is the event that the die roll is not prime. This event occurs with probability $\frac{1}{2}$.

- $\{3, 4, 5, 6\}$ is the event that the die roll shows a number greater than 2. This event occurs with probability $\frac{2}{3}$.

- $\{1, 2, 3, 4, 5, 6\}$ is the event that anything happens. This event occurs with probability 1.

- $\varnothing$ is the event that nothing happens. This event occurs with probability 0.

More generally, since each outcome occurs with equal probability $\frac{1}{6}$, we can define

$$\mathbb{P}(A) = \frac{|A|}{6} \text{ for all events } A$$

We will verify that $\mathbb{P}$ defines a probability measure on $[6]$ in Example 7.1.6.   ◁

Example 7.1.3
Let $(\Omega, \mathbb{P})$ be a probability space. We prove that $\mathbb{P}(\varnothing) = 0$.

Note that Ω and $\varnothing$ are disjoint, so by countable additivity, we have

$$1 = \mathbb{P}(\Omega) = \mathbb{P}(\Omega \cup \varnothing) = \mathbb{P}(\Omega) + \mathbb{P}(\varnothing) = 1 + \mathbb{P}(\varnothing)$$

Subtracting 1 throughout yields $\mathbb{P}(\varnothing) = 0$, as required.   ◁

Exercise 7.1.4
Let $(\Omega, \mathbb{P})$ be a probability space. Prove that

$$\mathbb{P}(\Omega \setminus A) = 1 - \mathbb{P}(A)$$

for all events A.   ◁

Countable additivity of probability measures—that is, condition (ii) in Definition 7.1.1—implies that probabilities of events are determined by probabilities of individual outcomes. This is made precise in Proposition 7.1.5.

Proposition 7.1.5
Let Ω be a countable set and let $\mathbb{P} : \mathcal{P}(\Omega) \to [0, 1]$ be a function such that $\mathbb{P}(\Omega) = 1$. The following are equivalent:

(i) $\mathbb{P}$ is a probability measure on Ω;

(ii) $\sum_{\omega \in A} \mathbb{P}(\{\omega\}) = \mathbb{P}(A)$ for all $A \subseteq \Omega$.

Proof. Since $\mathbb{P}(\Omega) = 1$, it suffices to prove that condition (ii) of Proposition 7.1.5 is equivalent to countable additivity of $\mathbb{P}$.

- (i)⇒(ii). Suppose $\mathbb{P}$ is a probability measure on Ω. Let $A \subseteq \Omega$.

  Note that since $A \subseteq \Omega$ and Ω is countably infinite, it follows that $\{\{\omega\} \mid \omega \in A\}$ is a countable family of pairwise disjoint sets. By countable additivity, we have

  $$\mathbb{P}(A) = \mathbb{P}\left(\bigcup_{\omega \in A}\{\omega\}\right) = \sum_{\omega \in A}\mathbb{P}(\{\omega\})$$

  as required. Hence condition (ii) of the proposition is satisfied.

- (ii)⇒(i). Suppose that $\sum_{\omega \in A}\mathbb{P}(\{\omega\}) = \mathbb{P}(A)$ for all $A \subseteq \Omega$. We prove that $\mathbb{P}$ is a probability measure on Ω.

  So let $\{A_i \mid i \in I\}$ be a family of pairwise disjoint events, indexed by a countable set I. Define $A = \bigcup_{i \in I} A_i$. Since the sets A_i partition A, summing over elements of A is the same as summing over each of the sets A_i individually, and then adding those results together; specifically, for each A-tuple $(p_\omega)_{\omega \in A}$, we have

  $$\sum_{\omega \in A} p_\omega = \sum_{i \in I}\sum_{\omega \in A_i} p_\omega$$

  Hence

  $$
  \begin{aligned}
  \mathbb{P}(A) &= \sum_{\omega \in A}\mathbb{P}(\{\omega\}) && \text{by condition (ii) of the proposition} \\
  &= \sum_{i \in I}\sum_{\omega \in A_i}\mathbb{P}(\{\omega\}) && \text{by the above observation} \\
  &= \sum_{i \in I}\mathbb{P}(A_i) && \text{by condition (ii) of the proposition}
  \end{aligned}
  $$

  So $\mathbb{P}$ satisfies the countable additivity condition. Thus $\mathbb{P}$ is a probability measure on Ω.

Hence the two conditions are equivalent. □

Example 7.1.6
We prove that the function $\mathbb{P}$ from Exercise 7.1.2 truly does define a probability measure. Indeed, let $\Omega = [6]$ and let $\mathbb{P} : \mathcal{P}(\Omega) \to [0, 1]$ be defined by

$$\mathbb{P}(A) = \frac{|A|}{6} \text{ for all events } A$$

Then $\mathbb{P}(\Omega) = \frac{6}{6} = 1$, so condition (i) in Definition 7.1.1 is satisfied. Moreover, for each $A \subseteq [6]$ we have

$$\sum_{\omega \in A}\mathbb{P}(\{\omega\}) = \sum_{\omega \in A}\frac{1}{6} = \frac{|A|}{6} = \mathbb{P}(A)$$

so, by Proposition 7.1.5, $\mathbb{P}$ defines a probability measure on $[6]$. ◁

Proposition 7.1.5 makes defining probability measures much easier, since it implies that probability measures are determined entirely by their values on individual outcomes. This means that, in order to define a probability measure, we only need to specify its values on individual outcomes and check that the sum of these probabilities is equal to 1. This is significantly easier than defining $\mathbb{P}(A)$ on *all* events $A \subseteq \Omega$ and checking the two conditions of Definition 7.1.1.

This is made precise in Proposition 7.1.7 below.

Proposition 7.1.7

Let Ω be a countable set and, for each $\omega \in \Omega$, let $p_\omega \in [0, 1]$. If $\sum_{\omega \in \Omega} p_\omega = 1$, then there is a unique probability measure $\mathbb{P}$ on Ω such that $\mathbb{P}(\{\omega\}) = p_\omega$ for each $\omega \in \Omega$.

Proof. We prove existence and uniqueness of $\mathbb{P}$ separately.

- **Existence.** Define $\mathbb{P} : \mathcal{P}(\Omega) \to [0, 1]$ be defined by

$$\mathbb{P}(A) = \sum_{\omega \in A} p_\omega$$

  for all events $A \subseteq \Omega$. Then condition (ii) of Proposition 7.1.5 is automatically satisfied, and indeed $\mathbb{P}(\{\omega\}) = p_\omega$ for each $\omega \in \Omega$. Moreover

$$\mathbb{P}(\Omega) = \sum_{\omega \in \Omega} \mathbb{P}(\{\omega\}) = \sum_{\omega \in \Omega} p_\omega = 1$$

  and so condition (i) of Definition 7.1.1 is satisfied. Hence $\mathbb{P}$ defines a probability measure on Ω.

- **Uniqueness.** Suppose that $\mathbb{P}' : \mathcal{P}(\Omega) \to [0, 1]$ is another probability measure such that $\mathbb{P}'(\{\omega\}) = p_\omega$ for all $\omega \in \Omega$. For each event $A \subseteq \Omega$, condition (ii) of Proposition 7.1.5 implies that

$$\mathbb{P}'(A) = \sum_{\omega \in A} \mathbb{P}'(\{\omega\}) = \sum_{\omega \in A} p_\omega = \mathbb{P}(A)$$

  hence $\mathbb{P}' = \mathbb{P}$.

So $\mathbb{P}$ is uniquely determined by the values p_ω. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

The assignments of $p_\omega \in [0, 1]$ to each $\omega \in \Omega$ in fact defines something that we will later defined to be a *probability mass function* (Definition 7.2.6).

With Proposition 7.1.7 proved, we will henceforth specify probability measures $\mathbb{P}$ on sample spaces Ω by specifying only the values of $\mathbb{P}(\{\omega\})$ for $\omega \in \Omega$.

Example 7.1.8

Let $p \in [0, 1]$. A coin, which shows heads with probability p, is repeatedly flipped until heads shows.

The outcomes of such a sequence of coin flips all take the form

$$(\underbrace{\text{tails}, \text{tails}, \cdots, \text{tails}}_{n \text{ 'tails'}}, \text{heads})$$

for some $n \in \mathbb{N}$. Identifying such a sequence with the number n of flips before heads shows, we can take $\Omega = \mathbb{N}$ to be the sample space.

For each $n \in \mathbb{N}$, we can define

$$\mathbb{P}(\{n\}) = (1 - p)^n p$$

This will define a probability measure on $\mathbb{N}$, provided these probabilities all sum to 1; and indeed by Proposition 6.3.1, we have

$$\sum_{n \in \mathbb{N}} \mathbb{P}(\{n\}) = \sum_{n \in \mathbb{N}} (1 - p)^n p = p \cdot \frac{1}{1 - (1 - p)} = p \cdot \frac{1}{p} = 1$$

By Proposition 7.1.7, it follows that $(\Omega, \mathbb{P})$ is a probability space. ◁

Exercise 7.1.9

A fair six-sided die is rolled twice. Define a probability space $(\Omega, \mathbb{P})$ that models this situation. ◁

Exercise 7.1.10

Let $(\Omega, \mathbb{P})$ be a probability space and let A, B be events with $A \subseteq B$. Prove that $\mathbb{P}(A) \leqslant \mathbb{P}(B)$. ◁

Set operations on events

In the real world, we might want to talk about the probability that two events both happen, or the probability that an event doesn't happen, or the probability that at least one of some collection of events happens. This is interpreted mathematically in terms of set operations.

Example 7.1.11

Let $(\Omega, \mathbb{P})$ be the probability space modelling two rolls of a fair six-sided die—that is, the sample space $\Omega = [6] \times [6]$ with probability measure $\mathbb{P}$ defined by $\mathbb{P}(\{(a, b)\}) = \frac{1}{36}$ for each $(a, b) \in \Omega$.

Let A be the event that the sum of the die rolls is even, that is

$$A = \begin{Bmatrix} (1,1), & (1,3), & (1,5), & (2,2), & (2,4), & (2,6), \\ (3,1), & (3,3), & (3,5), & (4,2), & (4,4), & (4,6), \\ (5,1), & (5,3), & (5,5), & (6,2), & (6,4), & (6,6) \end{Bmatrix}$$

and let B be the event that the sum of the die rolls is greater than or equal to 9, that is

$$B = \{(3,6), (4,5), (4,6), (5,4), (5,5), (5,6), (6,3), (6,4), (6,5), (6,6)\}$$

Then

- Consider the event that the sum of the die rolls is even **or** greater than or equal to 9. An outcome ω gives rise to this event precisely when either $\omega \in A$ or $\omega \in B$; so the event in question is $A \cup B$;

- Consider the event that the sum of the die rolls is even **and** greater than or equal to 9. An outcome ω gives rise to this event precisely when both $\omega \in A$ and $\omega \in B$; so the event in question is $A \cap B$;

- Consider the event that the sum of the die rolls is **not** even. An outcome ω gives rise to this event precisely when $\omega \notin A$; so the event in question is is $([6] \times [6]) \setminus A$.

Thus we can interpret 'or' as union, 'and' as intersection, and 'not' as relative complement in the sample space. ◁

The intuition provided by Example 7.1.11 is formalised in Exercise 7.1.13. Before we do this, we adopt a convention that simplifies notation when discussing events in probability spaces.

Notation 7.1.12

Let $(\Omega, \mathbb{P})$ be a probability space. When a subset $A \subseteq \Omega$ is interpreted as an event, we will write A^c for $\Omega \setminus A$ (instead of $\mathcal{U} \setminus A$ where $\mathcal{U}$ is the universe of discourse).

That is, when we talk about the complement *of an event*, we really mean their relative complement inside the sample space.

Exercise 7.1.13

Let $(\Omega, \mathbb{P})$ be a probability space, and let $p(\omega), q(\omega)$ be logical formulae with free variable ω ranging over Ω. Let

$$A = \{\omega \in \Omega \mid p(\omega)\} \quad \text{and} \quad B = \{\omega \in \Omega \mid q(\omega)\}$$

Prove that

- $\{\omega \in \Omega \mid p(\omega) \wedge q(\omega)\} = A \cap B$;

- $\{\omega \in \Omega \mid p(\omega) \vee q(\omega)\} = A \cup B$;

- $\{\omega \in \Omega \mid \neg p(\omega)\} = A^c$.

For reference, in Example 7.1.11, we had $\Omega = [6] \times [6]$ and we defined $p(a, b)$ to be '$a + b$ is even' and $q(a, b)$ to be '$a + b \geqslant 7$'. ◁

With this in mind, it will be useful to know how set operations on events interact with probabilities. A useful tool in this investigation is that of an *indicator function*.

Definition 7.1.14
Let Ω be a set and let $A \subseteq \Omega$. The **indicator function** of A in Ω is the function $i_A : \Omega \to \{0, 1\}$ defined by
$$i_A(\omega) = \begin{cases} 1 & \text{if } \omega \in A \\ 0 & \text{if } \omega \notin A \end{cases}$$

Proposition 7.1.15
Let Ω be a set and let $A, B \subseteq \Omega$. Then for all $\omega \in \Omega$ we have

(i) $i_{A \cap B}(\omega) = i_A(\omega) i_B(\omega)$;

(ii) $i_{A \cup B}(\omega) = i_A(\omega) + i_B(\omega) - i_{A \cap B}(\omega)$; and

(iii) $i_{A^c}(\omega) = 1 - i_A(\omega)$.

Proof. Proof of (i) Let $\omega \in \Omega$. If $\omega \in A \cap B$ then $\omega \in A$ and $\omega \in B$, so that $i_{A \cap B}(\omega) = i_A(\omega) = i_B(\omega) = 1$. Hence
$$i_A(\omega) i_B(\omega) = 1 = i_{A \cap B}(\omega)$$

If $\omega \notin A \cap B$ then either $\omega \notin A$ or $\omega \notin B$. Hence $i_{A \cap B}(\omega) = 0$, and either $i_A(\omega) = 0$ or $i_B(\omega) = 0$. Thus
$$i_A(\omega) i_B(\omega) = 0 = i_{A \cap B}(\omega)$$

In both cases, we have $i_{A \cap B}(\omega) = i_A(\omega) i_B(\omega)$, as required. □

Exercise 7.1.16
Prove parts (ii) and (iii) of Proposition 7.1.15. ◁

Exercise 7.1.17

Let $(\Omega, \mathbb{P})$ be a discrete probability space, and for each $\omega \in \Omega$ let $p_\omega = \mathbb{P}(\{\omega\})$. Prove that, for each event A, we have

$$\mathbb{P}(A) = \sum_{\omega \in \Omega} p_\omega i_A(\omega)$$

◁

Theorem 7.1.18

Let $(\Omega, \mathbb{P})$ be a probability space and let $A, B \subseteq \Omega$. Then

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$$

Proof. For each $\omega \in \Omega$, let $p_\omega = \mathbb{P}(\{\omega\})$. Then

$$
\begin{aligned}
\mathbb{P}(A \cup B) &= \sum_{\omega \in \Omega} p_\omega i_{A \cup B}(\omega) && \text{by Exercise 7.1.17} \\
&= \sum_{\omega \in \Omega} p_\omega (i_A(\omega) + i_B(\omega) - i_{A \cap B}(\omega)) && \text{by Proposition 7.1.15(ii)} \\
&= \sum_{\omega \in \Omega} p_\omega i_A(\omega) + \sum_{\omega \in \Omega} p_\omega i_B(\omega) + \sum_{\omega \in \Omega} p_\omega i_{A \cap B}(\omega) && \text{rearranging} \\
&= \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B) && \text{by Exercise 7.1.17}
\end{aligned}
$$

as required. ☐

Although there are nice expressions for unions and complements of events, it is not always the case that intersection of events corresponds with multiplication of probabilities.

Example 7.1.19

Let $\Omega = [3]$ and define a probability measure $\mathbb{P}$ on Ω by letting

$$\mathbb{P}(\{1\}) = \frac{1}{4}, \qquad \mathbb{P}(\{2\}) = \frac{1}{2} \qquad \text{and} \qquad \mathbb{P}(\{3\}) = \frac{1}{4}$$

Then we have

$$\mathbb{P}(\{1,2\} \cap \{2,3\}) = \mathbb{P}(\{2\}) = \frac{1}{2} \neq \frac{9}{16} = \frac{3}{4} \cdot \frac{3}{4} = \mathbb{P}(\{1,2\}) \cdot \mathbb{P}(\{2,3\})$$

◁

This demonstrates that it is not always the case that $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$ for events A, B in a given probability space. Pairs of events A, B for which this equation *is* true are said to be *independent*.

Definition 7.1.20

Let $(\Omega, \mathbb{P})$ be a probability space and let A, B be events. We say A and B are **independent** if $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$; otherwise, we say they are **dependent**. More generally, events $A_1, A_2, \ldots, A_n$ are **mutually independent** if

$$\mathbb{P}(A_1 \cap A_2 \cap \cdots \cap A_n) = \mathbb{P}(A_1)\mathbb{P}(A_2) \cdots \mathbb{P}(A_n)$$

Example 7.1.21

A fair six-sided die is rolled twice. Let A be the event that the first roll shows 4, and let B be the event that the second roll is even. Then

$$A = \{(4, 1), (4, 2), (4, 3), (4, 4), (4, 5), (4, 6)\}$$

so $\mathbb{P}(A) = \frac{6}{36} = \frac{1}{6}$; and

$$B = \{(a, 2), (a, 4), (a, 6) \mid a \in [6]\}$$

so $\mathbb{P}(B) = \frac{18}{36} = \frac{1}{2}$. Moreover $A \cap B = \{(4, 2), (4, 4), (4, 6)\}$, so it follows that

$$\mathbb{P}(A \cap B) = \frac{3}{36} = \frac{1}{12} = \frac{1}{6} \cdot \frac{1}{2} = \mathbb{P}(A)\mathbb{P}(B)$$

so the events A and B are independent.

Let C be the event that the sum of the two dice rolls is equal to 5. Then

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

so $\mathbb{P}(C) = \frac{4}{36} = \frac{1}{9}$. Moreover $A \cap C = \{(4, 1)\}$, so it follows that

$$\mathbb{P}(A \cap C) = \frac{1}{36} \neq \frac{1}{54} = \frac{1}{6} \cdot \frac{1}{9} = \mathbb{P}(A)\mathbb{P}(C)$$

so the events A and C are dependent. ◁

Exercise 7.1.22

Let $(\Omega, \mathbb{P})$ be a probability space. Under what conditions is an event A independent from itself? ◁

Conditional probability

Suppose we model a real-world situation, such as the roll of a die or the flip of a coin, using a probability $(\Omega, \mathbb{P})$. When we receive new information, the situation might change, and we might want to model this new situation by updating our probabilities to reflect the fact that we know that B has occurred. This is done by defining a new probability measure $\widetilde{\mathbb{P}}$ on Ω. What follows is an example of this.

Example 7.1.23

Two cards are drawn at random, in order, without replacement, from a 52-card deck. We can model this situation by letting the sample space Ω be the set of ordered pairs of distinct cards, and letting $\mathbb{P}$ assign an equal probability (of $\frac{1}{|\Omega|}$) to each outcome. Note that $|\Omega| = 52 \cdot 51$, and so

$$\mathbb{P}(\{\omega\}) = \frac{1}{52 \cdot 51}$$

for each outcome ω.

We will compute two probabilities:

- The probability that the second card drawn is a heart.

- The probability that the second card drawn is a heart *given that* the first card drawn is a diamond.

Let $A \subseteq \Omega$ be the event that the second card drawn is a heart, and let $B \subseteq \Omega$ be the event that the first card drawn is a diamond.

To compute $\mathbb{P}(A)$, note first that $A = A' \cup A''$, where

- A' is the event that both cards are hearts, so that $|A'| = 13 \cdot 12$; and

- A'' is the event that only the second card is a heart, so that $|A''| = 39 \cdot 13$.

Since $A' \cap A'' = \varnothing$, it follows from countable additivity that

$$\mathbb{P}(A) = \mathbb{P}(A') + \mathbb{P}(A'') = \frac{13 \cdot 12 + 39 \cdot 13}{52 \cdot 51} = \frac{13 \cdot (12 + 39)}{52 \cdot 51} = \frac{1}{4}$$

Now suppose we know that first card drawn is a diamond—that is, event B has occurred—and we wish to update our probability that A occurs. We do this by defining a new probability measure

$$\widetilde{\mathbb{P}} : \mathcal{P}(\Omega) \to [0, 1]$$

such that:

(a) The outcomes that do not give rise to the event B are assigned probability zero; that is, $\widetilde{\mathbb{P}}(\{\omega\}) = 0$ for all $\omega \notin B$; and

(b) The outcomes that give rise to the event B are assigned probabilities proportional to their old probability; that is, there is some $k \in \mathbb{R}$ such that $\widetilde{\mathbb{P}}(\omega) = k\mathbb{P}(\omega)$ for all $\omega \in B$.

In order for $\widetilde{\mathbb{P}}$ to be a probability measure on Ω, we need condition (i) of Definition 7.1.1 to occur.

$$
\begin{aligned}
\widetilde{\mathbb{P}}(\Omega) &= \sum_{\omega \in \Omega} \widetilde{\mathbb{P}}(\{\omega\}) && \text{by condition (ii) of Proposition 7.1.5} \\
&= \sum_{\omega \in B} \widetilde{\mathbb{P}}(\{\omega\}) && \text{since } \widetilde{\mathbb{P}}(\{\omega\}) = 0 \text{ for } \omega \notin B \\
&= \sum_{\omega \in B} k\mathbb{P}(\{\omega\}) && \text{since } \widetilde{\mathbb{P}}(\{\omega\}) = k\mathbb{P}(\{\omega\} \text{ for } \omega \in B \\
&= k\mathbb{P}(B) && \text{by condition (ii) of Proposition 7.1.5}
\end{aligned}
$$

Since we need $\widetilde{\mathbb{P}}(\Omega) = 1$, we must therefore take $k = \frac{1}{\mathbb{P}(B)}$. (In particular, we need $\mathbb{P}(B) > 0$ for this notion to be well-defined.)

Recall that, before we knew that the first card was a diamond, the probability that the second card is a heart was $\frac{1}{4}$. We now calculate how this probability changes with the updated information that the first card was a diamond.

The event that the second card is a heart in the new probability space is precisely $A \cap B$, since it is the subset of B consisting of all the outcomes ω giving rise to the event A. As such, the new probability that the second card is a heart is given by

$$
\widetilde{\mathbb{P}}(A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}
$$

Now:

- $A \cap B$ is the event that the first card is a diamond and the second is a heart. To specify such an event, we need only specify the ranks of the two cards, so $|A \cap B| = 13 \cdot 13$ and hence $\mathbb{P}(A \cap B) = \frac{13 \cdot 13}{52 \cdot 51}$.

- B is the event that the first card is a diamond. A similar procedure as with A yields $\mathbb{P}(B) = \frac{1}{4}$.

Hence

$$
\widetilde{\mathbb{P}}(A) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} = \frac{13 \cdot 13 \cdot 4}{52 \cdot 51} = \frac{13}{51}
$$

Thus the knowledge that the first card drawn is a diamond very slightly increases the probability that the second card is a heart from $\frac{1}{4} = \frac{13}{52}$ to $\frac{13}{51}$. $\lhd$

Example 7.1.23 suggests the following schema: upon discovering that an event B occurs, the probability that event A occurs should change from $\mathbb{P}(A)$ to $\frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$. This motivates the following definition of *conditional probability*.

Definition 7.1.24

Let $(\Omega, \mathbb{P})$ be a probability space and let A, B be events such that $\mathbb{P}(B) > 0$. The **conditional probability of A given B** is the number $\mathbb{P}(A \mid B)$ (LaTeX code: `\mathbb{P}(A \mid B)`) defined by

$$\mathbb{P}(A \mid B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$$

Example 7.1.25

A fair six-sided die is rolled twice. We compute the probability that the first roll showed a 2 given that the sum of the die rolls is less than 5.

We can model this situation by taking the sample space to be $[6] \times [6]$, with each outcome having an equal probability of $\frac{1}{36}$.

Let A be the event that the first die roll shows a 2, that is

$$A = \{(2,1), (2,2), (2,3), (2,4), (2,5), (2,6)\}$$

and let B be the event that the sum of the die rolls is less than 5, that is

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

We need to compute $\mathbb{P}(A \mid B)$. Well,

$$A \cap B = \{(2,1), (2,2)\}$$

so $\mathbb{P}(A \cap B) = \frac{2}{36}$; and $\mathbb{P}(B) = \frac{6}{36}$. Hence

$$\mathbb{P}(A \mid B) = \frac{\frac{2}{36}}{\frac{6}{36}} = \frac{2}{6} = \frac{1}{3}$$

◁

Exercise 7.1.26

A fair six-sided die is rolled three times. What is the probability that the sum of the die rolls is less than or equal to 12, given that each die roll shows a power of 2? ◁

Exercise 7.1.27

Let $(\Omega, \mathbb{P})$ be a probability space and let A, B be events with $\mathbb{P}(B) > 0$. Prove that

$$\mathbb{P}(A \mid B) = \mathbb{P}(A \cap B \mid B)$$

◁

Exercise 7.1.28

Let $(\Omega, \mathbb{P})$ be a probability space and let A, B be events such that $\mathbb{P}(B) > 0$. Prove that $\mathbb{P}(A \mid B) = \mathbb{P}(A)$ if and only if A and B are independent. ◁

We will soon see some useful real-world applications of probability theory using *Bayes's theorem* (Theorem 7.1.33). Before we do so, some technical results will be useful in our proofs.

Proposition 7.1.29

Let $(\Omega, \mathbb{P})$ be a probability space and let A, B be events with $0 < \mathbb{P}(B) < 1$. Then

$$\mathbb{P}(A) = \mathbb{P}(A \mid B)\mathbb{P}(B) + \mathbb{P}(A \mid B^c)\mathbb{P}(B^c)$$

Proof. Note first that we can write

$$A = A \cap \Omega = A \cap (B \cup B^c) = (A \cap B) \cup (A \cap B^c)$$

and moreover the events $A \cap B$ and $A \cap B^c$ are mutually exclusive. Hence

$$\mathbb{P}(A) = \mathbb{P}(A \cap B) + \mathbb{P}(A \cap B^c)$$

by countable additivity. The definition of conditional probability (Definition 7.1.24) then gives

$$\mathbb{P}(A) = \mathbb{P}(A \mid B)\mathbb{P}(B) + \mathbb{P}(A \mid B^c)\mathbb{P}(B^c)$$

as required. $\qquad\square$

Example 7.1.30

An animal rescue centre houses a hundred animals, sixty of which are dogs and forty of which are cats. Ten of the dogs and ten of the cats hate humans. We compute the probability that a randomly selected animal hates humans.

Let A be the event that a randomly selected animal hates humans, and let B be the event that the animal is a dog. Note that B^c is precisely the event that the animal is a cat. The information we are given says that:

- $\mathbb{P}(B) = \frac{60}{100}$, since 60 of the 100 animals are dogs;

- $\mathbb{P}(B^c) = \frac{40}{100}$, since 40 of the 100 animals are cats;

- $\mathbb{P}(A \mid B) = \frac{10}{60}$, since 10 of the 60 dogs hate humans;

- $\mathbb{P}(A \mid B^c) = \frac{10}{40}$, since 10 of the 40 cats hate humans.

By Proposition 7.1.29, it follows that the probability that a randomly selected animal hates humans is

$$\mathbb{P}(A) = \mathbb{P}(A \mid B)\mathbb{P}(B) + \mathbb{P}(A \mid B^c)\mathbb{P}(B^c) = \frac{60}{100} \cdot \frac{10}{60} + \frac{40}{100} \cdot \frac{10}{40} = \frac{20}{100} = \frac{1}{5}$$

$\triangleleft$

The following exercise generalises Proposition 7.1.29 to arbitrary partitions of a sample space into events with positive probabilities.

Example 7.1.31

The animal rescue centre from Example 7.1.30 acquires twenty additional rabbits, of whom sixteen hate humans. We compute the probability that a randomly selected animal hates humans, given the new arrivals.

A randomly selected animal must be either a dog, a cat or a rabbit, and each of these occurs with positive probability. Thus, letting D be the event that the selected animal is a dog, C be the event that the animal is a cat, and R be the event that the animal is a rabbit, we see that the sets D, C, R form a partition of the sample space.

Letting A be the event that the selected animal hates humans. Then

$$\mathbb{P}(A) = \mathbb{P}(A \mid D)\mathbb{P}(D) + \mathbb{P}(A \mid C)\mathbb{P}(C) + \mathbb{P}(A \mid R)\mathbb{P}(R) = \frac{10}{60} \cdot \frac{60}{120} + \frac{10}{40} \cdot \frac{40}{120} + \frac{16}{20} \cdot \frac{20}{120} = \frac{3}{10}$$

<div align="right">◁</div>

Proposition 7.1.32 below is a technical result which proves that conditional probability truly does yield a new probability measure on a given sample space.

Proposition 7.1.32

Let $(\Omega, \mathbb{P})$ be a discrete probability space and let B be an event such that $\mathbb{P}(B) > 0$. The function $\widetilde{\mathbb{P}} : \mathcal{P}(\Omega) \to [0, 1]$ defined by

$$\widetilde{\mathbb{P}}(A) = \mathbb{P}(A \mid B) \text{ for all } A \subseteq \Omega$$

defines a probability measure on Ω.

Proof. First note that

$$\widetilde{\mathbb{P}}(\Omega) = \mathbb{P}(\Omega \mid B) = \frac{\mathbb{P}(\Omega \cap B)}{\mathbb{P}(B)} = \frac{\mathbb{P}(B)}{\mathbb{P}(B)} = 1$$

so condition (i) of Definition 7.1.1 is satisfied.

Moreover, for each $A \subseteq \Omega$ we have

$$
\begin{aligned}
\widetilde{\mathbb{P}}(A) &= \mathbb{P}(A \mid B) && \text{by definition of } \widetilde{\mathbb{P}} \\
&= \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} && \text{by Definition 7.1.24} \\
&= \frac{1}{\mathbb{P}(B)} \sum_{\omega \in A \cap B} \mathbb{P}(\{\omega\}) && \text{byProposition 7.1.5} \\
&= \sum_{\omega \in A \cap B} \mathbb{P}(\{\omega\} \mid B) && \text{by Definition 7.1.24} \\
&= \sum_{\omega \in A} \mathbb{P}(\{\omega\} \mid B) && \text{since } \mathbb{P}(\{\omega\} \mid B) = 0 \text{ for } \omega \in A \setminus B \\
&= \sum_{\omega \in A} \widetilde{\mathbb{P}}(\{\omega\}) && \text{by definition of } \widetilde{\mathbb{P}}
\end{aligned}
$$

so condition (ii) of Proposition 7.1.5 is satisfied. Hence $\widetilde{\mathbb{P}}$ defines a probability measure on Ω. $\square$

Proposition 7.1.32 implies that we can use all the results we've proved about probability measures to conditional probability given a fixed event B. For example, Theorem 7.1.18 implies that

$$\mathbb{P}(A \cup A' \mid B) = \mathbb{P}(A \mid B) + \mathbb{P}(A' \mid B) - \mathbb{P}(A \cap A' \mid B)$$

for all events A, A', B in a probability space $(\Omega, \mathbb{P})$ such that $\mathbb{P}(B) > 0$.

The next theorem we prove has a very short proof, but is extremely important in applied probability theory.

Theorem 7.1.33 (Bayes's theorem)

Let $(\Omega, \mathbb{P})$ be a probability space and let A, B be events with positive probabilities. Then

$$\mathbb{P}(B \mid A) = \frac{\mathbb{P}(A \mid B)\mathbb{P}(B)}{\mathbb{P}(A)}$$

Proof. Definition 7.1.24 gives

$$\mathbb{P}(A \mid B)\mathbb{P}(B) = \mathbb{P}(A \cap B) = \mathbb{P}(B \cap A) = \mathbb{P}(B \mid A)\mathbb{P}(A)$$

Dividing through by $\mathbb{P}(A)$ yields the desired equation. $\square$

As stated, Bayes's theorem is not necessarily particularly enlightening, but its usefulness increases sharply when combined with Proposition 7.1.29.

Corollary 7.1.34

Let $(\Omega, \mathbb{P})$ be a probability space and let A, B be events such that $\mathbb{P}(A) > 0$ and $0 < \mathbb{P}(B) < 1$. Then

$$\mathbb{P}(B \mid A) = \frac{\mathbb{P}(A \mid B)\mathbb{P}(B)}{\mathbb{P}(A \mid B)\mathbb{P}(B) + \mathbb{P}(A \mid B^c)\mathbb{P}(B^c)}$$

Proof. Bayes's theorem tells us that

$$\mathbb{P}(B \mid A) = \frac{\mathbb{P}(A \mid B)\mathbb{P}(B)}{\mathbb{P}(A)}$$

By Proposition 7.1.29 we have

$$\mathbb{P}(A) = \mathbb{P}(A \mid B)\mathbb{P}(B) + \mathbb{P}(A \mid B^c)\mathbb{P}(B^c)$$

Substituting for $\mathbb{P}(A)$ therefore yields

$$\mathbb{P}(B \mid A) = \frac{\mathbb{P}(A \mid B)\mathbb{P}(B)}{\mathbb{P}(A \mid B)\mathbb{P}(B) + \mathbb{P}(A \mid B^c)\mathbb{P}(B^c)}$$

as required. $\square$

The following example is particularly counterintuitive.

Example 7.1.35

A town has 10000 people, 30 of whom are infected with Disease X. Medical scientists develop a test for Disease X, which is accurate 99% of the time. A person takes the test, which comes back positive. We compute the probability that the person truly is infected with Disease X.

Let A be the event that the person tests positive for Disease X, and let B be the event that the person is infected with Disease X. We need to compute $\mathbb{P}(B \mid A)$.

By Corollary 7.1.34, we have

$$\mathbb{P}(B \mid A) = \frac{\mathbb{P}(A \mid B)}{\mathbb{P}(A \mid B)\mathbb{P}(B) + \mathbb{P}(A \mid B^c)\mathbb{P}(B^c)}$$

It remains to compute the individual probabilities on the right-hand side of this equation. Well,

- $\mathbb{P}(A \mid B)$ is the probability that the person tests positive for Disease X, given that they are infected. This is equal to $\frac{99}{100}$, since the test is accurate with probability 99%.

- $\mathbb{P}(A \mid B^c)$ is the probability that the person tests positive for Disease X, given that they are *not* infected. This is equal to $\frac{1}{100}$, since the test is *inaccurate* with probability 1%.

- $\mathbb{P}(B) = \frac{30}{10000}$, since 30 of the 10000 inhabitants are infected with Disease X.

- $\mathbb{P}(B^c) = \frac{9970}{10000}$, since 9970 of the 10000 inhabitants are *not* infected with Disease X.

Piecing this together gives

$$\mathbb{P}(B \mid A) = \frac{\frac{99}{100} \cdot \frac{30}{10000}}{\frac{99}{100} \cdot \frac{30}{10000} + \frac{1}{100} \cdot \frac{9970}{10000}} = \frac{297}{1294} \approx 0.23$$

Remarkably, the probability that the person is infected with Disease X given that the test is positive is only 23%, even though the test is accurate 99% of the time! ◁

The following result generalises Corollary 7.1.34 to arbitrary partitions of the sample space into sets with positive probabilities.

Corollary 7.1.36

Let $(\Omega, \mathbb{P})$ be a probability space, let A be an event with $\mathbb{P}(A) > 0$, and let $\{B_i \mid i \in I\}$ be a family of mutually exclusive events indexed by a countable set I such that

$$\mathbb{P}(B_i) > 0 \text{ for all } i \in I \qquad \text{and} \qquad \bigcup_{i \in I} \mathbb{P}(B_i) = \Omega$$

Then

$$\mathbb{P}(B_i \mid A) = \frac{\mathbb{P}(A \mid B_i)\mathbb{P}(B_i)}{\sum_{i \in I} \mathbb{P}(A \mid B_i)\mathbb{P}(B_i)}$$

for each $i \in I$.

Proof. Bayes's theorem tells us that

$$\mathbb{P}(B \mid A) = \frac{\mathbb{P}(A \mid B)\mathbb{P}(B)}{\mathbb{P}(A)}$$

By countable additivity, we have

$$\mathbb{P}(A) = \sum_{i \in I} \mathbb{P}(A \mid B_i)\mathbb{P}(B_i)$$

Substituting for $\mathbb{P}(A)$ therefore yields

$$\mathbb{P}(B_i \mid A) = \frac{\mathbb{P}(A \mid B_i)\mathbb{P}(B_i)}{\sum_{i \in I} \mathbb{P}(A \mid B_i)\mathbb{P}(B_i)}$$

as required. □

Example 7.1.37

A car company, *Cars N'At*, makes three models of cars, which it imaginatively named *Model A*, *Model B* and *Model C*. It made 3000 Model As, 6500 Model Bs, and 500 Model Cs. In a given day, a Model A breaks down with probability $\frac{1}{100}$, a Model B breaks down with probability $\frac{1}{200}$, and the notoriously unreliable Model C breaks down with probability $\frac{1}{20}$. An angry driver calls Cars N'At to complain that their car has broken down. We compute the probability that the driver was driving a Model C car.

Let A be the event that the car is a Model A, let B be the event that the car is a Model B, and let C be the event that the car is a Model C. Then

$$\mathbb{P}(A) = \frac{3000}{10000}, \quad \mathbb{P}(B) = \frac{6500}{10000}, \quad \mathbb{P}(C) = \frac{500}{10000}$$

Let D be the event that the car broke down. Then

$$\mathbb{P}(D \mid A) = \frac{1}{100}, \quad \mathbb{P}(D \mid B) = \frac{1}{200}, \quad \mathbb{P}(D \mid C) = \frac{1}{20}$$

We need to compute $\mathbb{P}(C \mid D)$. Since the events A, B, C partition the sample space and have positive probabilities, we can use Corollary 7.1.36, which tells us that

$$\mathbb{P}(C \mid D) = \frac{\mathbb{P}(D \mid C)\mathbb{P}(C)}{\mathbb{P}(D \mid A)\mathbb{P}(A) + \mathbb{P}(D \mid B)\mathbb{P}(B) + \mathbb{P}(D \mid C)\mathbb{P}(C)}$$

Substituting the probabilities that we computed above, it follows that

$$\mathbb{P}(C \mid D) = \frac{\frac{1}{20} \cdot \frac{500}{10000}}{\frac{1}{100} \cdot \frac{3000}{10000} + \frac{1}{200} \cdot \frac{6500}{10000} + \frac{1}{20} \cdot \frac{500}{10000}} = \frac{2}{7} \approx 0.29$$

◁

Exercise 7.1.38

In Example 7.1.37, find the probabilities that the car was a Model A and that the car was a Model B. ◁

7.2 Discrete random variables

Events in a probability space are sometimes unenlightening when looked at in isolation. For example, suppose we roll a fair six-sided die twice. The outcomes are elements of the set $[6] \times [6]$, each occurring with equal probability $\frac{1}{36}$. The event that the die rolls sum to 7 is precisely the subset

$$\{(1,6), (2,5), (3,4), (4,3), (5,2), (6,1)\} \subseteq [6] \times [6]$$

and so we can say that the probability that the two rolls sum to 7 is

$$\mathbb{P}(\{(1,6), (2,5), (3,4), (4,3), (5,2), (6,1)\}) = \frac{1}{6}$$

However, it is not at all clear from the expression $\{(1,6), (2,5), (3,4), (4,3), (5,2), (6,1)\}$ that, when we wrote it down, what we had in mind was the event that the sum of the die rolls is 7. Moreover, the expression of the event in this way does not make it clear how to generalise to other possible sums of die rolls.

Note that the sum of the die rolls defines a function $S : [6] \times [6] \to [12]$, defined by

$$S(a, b) = a + b \text{ for all } (a, b) \in [6] \times [6]$$

The function S allows us to express our event in a more enlightening way: indeed,

$$\{(1,6), (2,5), (3,4), (4,3), (5,2), (6,1)\} = \{(a, b) \in [6] \times [6] \mid a + b = 7\} = S^{-1}[\{7\}]$$

(Recall the definition of *preimage* in Definition 2.3.35.) Thus the probability that the sum of the two die rolls is 7 is equal to $\mathbb{P}(S^{-1}[\{7\}])$.

If we think of S not as a function $[6] \times [6] \to [12]$, but as a $[12]$-valued *random variable*, which varies according to a random outcome in $[6] \times [6]$, then we can informally say

$$\mathbb{P}\{S = 7\} = \frac{1}{6} \quad \text{which formally means} \quad \mathbb{P}(S^{-1}[\{7\}]) = \frac{1}{6}$$

This affords us much more generality. Indeed, we could ask what the probability is that the die rolls sum to a value greater than or equal to 7. In this case, note that the die rolls (a, b) sum to a number greater than or equal to 7 if and only if $a + b \in \{7, 8, 9, 10, 11, 12\}$, which occurs if and only if $(a, b) \in S^{-1}[\{7, 8, 9, 10, 11, 12\}]$. Thus, we might informally say

$$\mathbb{P}\{S \geqslant 7\} = \frac{7}{12} \quad \text{which formally means} \quad \mathbb{P}(S^{-1}[\{7, 8, 9, 10, 11, 12\}]) = \frac{7}{12}$$

We might also ask what the probability is that the sum of the die rolls is prime. In this case, we might informally say

$$\mathbb{P}\{S \text{ is prime}\} = \frac{5}{12} \quad \text{which formally means} \quad \mathbb{P}(S^{-1}[\{2, 3, 5, 7, 11\}]) = \frac{5}{12}$$

and so on. In each of these cases, we're defining events—which are subsets of the sample space—in terms of conditions on the values of a random variable (which is, formally, a function).

We make the above intuition formal in Definition 7.2.1.

Definition 7.2.1

Let $(\Omega, \mathbb{P})$ be a probability space and let E be a set. An E-**valued random variable on** $(\Omega, \mathbb{P})$ is a function $X : \Omega \to E$ such that the image

$$X[\Omega] = \{X(\omega) \mid \omega \in \Omega\}$$

is countable. The set E is called the **state space** of X. A random variable with countable state space is called a **discrete random variable**.

Before we proceed with examples, some notation for events regarding values of random variables will be particularly useful.

Notation 7.2.2

Let $(\Omega, \mathbb{P})$ be a probability space, let E be a set and let X be an E-valued random variable on $(\Omega, \mathbb{P})$. For each $e \in E$, write

$$\{X = e\} = \{\omega \in \Omega \mid X(\omega) = e\} = X^{-1}[\{e\}]$$

to denote the event that X takes the value e. More generally, for each logical formula $p(x)$ with free variable x ranging over E, we write

$$\{p(X)\} = \{\omega \in \Omega \mid p(X(\omega))\} = X^{-1}[\{e \in E \mid p(e)\}]$$

for the event that the value of X satisfies $p(x)$.

We will usually write $\mathbb{P}\{X = e\}$ instead of $\mathbb{P}(\{X = e\})$ for the probability that a random variable X takes a value e, and so on.

Example 7.2.3

We can model a sequence of three coin flips using the probability space $(\Omega, \mathbb{P})$, where $\Omega = \{\mathrm{H}, \mathrm{T}\}^3$ and $\mathbb{P}(\{\omega\}) = \frac{1}{8}$ for all $\omega \in \Omega$.

Let N be the real-valued random variable representing number of heads that show. This is formalised as a function

$$N : \Omega \to \mathbb{R} \quad \text{where} \quad N(i_1, i_2, i_3) = \text{the number of heads amongst } i_1, i_2, i_3$$

for example, $N(\mathrm{H}, \mathrm{T}, \mathrm{H}) = 2$. Now

- The probability that exactly two heads show is

$$\begin{aligned}
\mathbb{P}\{N = 2\} &= \mathbb{P}(N^{-1}[\{2\}]) && \text{by Notation 7.2.2} \\
&= \mathbb{P}(\{(\mathrm{H},\mathrm{H},\mathrm{T}), (\mathrm{H},\mathrm{T},\mathrm{H}), (\mathrm{T},\mathrm{H},\mathrm{H})\}) && \text{evaluating event } N^{-1}[\{2\}] \\
&= \frac{3}{2^3} = \frac{3}{8}
\end{aligned}$$

- The probability that at least two heads show is

$$\begin{aligned}
\mathbb{P}\{N \geqslant 2\} &= \mathbb{P}(\{\omega \in \Omega \mid N(\omega) \geqslant 2\}) && \text{by Notation 7.2.2} \\
&= \mathbb{P}\left(\left\{\begin{matrix}(\mathrm{H},\mathrm{H},\mathrm{T}), & (\mathrm{H},\mathrm{T},\mathrm{H}), \\ (\mathrm{T},\mathrm{H},\mathrm{H}), & (\mathrm{H},\mathrm{H},\mathrm{H})\end{matrix}\right\}\right) && \text{evaluating event} \\
&= \frac{4}{2^3} = \frac{1}{2}
\end{aligned}$$

◁

Exercise 7.2.4
With probability space $(\Omega, \mathbb{P})$ and random variable N defined as in Example 7.2.3, compute $\mathbb{P}\{N \text{ is odd}\}$ and $\mathbb{P}\{N = 4\}$. ◁

Exercise 7.2.5
Let $(\Omega, \mathbb{P})$ be a probability space, let E be a set, let X be an E-valued random variable and let $U \subseteq E$. Prove that the event $\{X \in U\}$ is equal to the preimage $X^{-1}[U]$. Deduce that

$$\mathbb{P}\{X \in U\} = \sum_{e \in U} f_X(e)$$

◁

Each random variable comes with an associated *probability mass function*, which allows us to 'forget' the underlying probability space for the purposes of studying only the random variable.

Definition 7.2.6
Let $(\Omega, \mathbb{P})$ be a probability space, let $X : \Omega \to E$ be an E-valued random variable. The **probability mass function** of X is the function $f_X : S \to [0, 1]$ defined by

$$f_X(e) = \mathbb{P}\{X = e\} \text{ for all } e \in S$$

Example 7.2.7
The probability mass function of the random variable N from Exercise 7.2.3 is the function $f_N : \mathbb{R} \to [0, 1]$ defined by

$$f_N(e) = \mathbb{P}\{N = e\} = \frac{1}{8}\binom{3}{e}$$

for all $e \in \{0, 1, 2, 3\}$, and $f_N(e) = 0$ otherwise. Indeed, there are $2^3 = 8$ possible outcomes, each equally likely, and $\binom{3}{e}$ of those outcomes show exactly e heads for $e \in \{0, 1, 2, 3\}$.   ◁

In the previous exercise, we could have just specified the value of f_N on $\{0, 1, 2, 3\}$, with the understanding that N does not take values outside of this set and hence that $\mathbb{P}\{N = e\} = 0$ for all $e \notin \{0, 1, 2, 3\}$. This issue arises frequently when dealing with real-valued discrete random variables, and it will be useful to ignore most (or all) of those real numbers which are not values of the random variable.

As such, for $E \subseteq \mathbb{R}$, we will from now on blur the distinction between the following concepts:

  (i) E-valued random variables;

  (ii) real-valued random variables X such that $\mathbb{P}\{X = x\} = 0$ for all $x \notin E$.

Example 7.2.8
The probability mass function of the random variable N from Example 7.2.3 can be taken to be the function $f_X : \{0, 1, 2, 3\} \to [0, 1]$ defined by

$$f_X(k) = \frac{1}{8}\binom{3}{k} \text{ for all } k \in \{0, 1, 2, 3\}$$

◁

Lemma 7.2.9
Let $(\Omega, \mathbb{P})$ be a probability space, let E be a set and let X be an E-valued random variable. The sets $\{X = e\}$ for $e \in E$ are mutually exclusive, and their union is Ω.

Proof. If $e, e' \in E$, then for all $\omega \in \Omega$ we have

$$\omega \in \{X = e\} \cap \{X = e'\} \Leftrightarrow \omega \in X^{-1}[\{e\}] \cap X^{-1}[\{e'\}] \quad \text{by Notation 7.2.2}$$
$$\Leftrightarrow X(\omega) = e \text{ and } X(\omega) = e' \quad \text{by definition of preimage}$$
$$\Rightarrow e = e'$$

so if $e \neq e'$ then $\{X = e\} \cap \{X = e'\} = \varnothing$. So the events are mutually exclusive.

Moreover, if $\omega \in \Omega$, then $\omega \in \{X = X(\omega)\}$. Hence

$$\Omega = \bigcup_{e \in E} \{X = e\}$$

as required.   □

> **Theorem 7.2.10**
> Let $(\Omega, \mathbb{P})$ be a probability space, let E be a countable set, and let X be an E-valued random variable. Then
> $$\sum_{e \in E} f_X(e) = 1$$

Proof. Since $f_X(e) = \mathbb{P}\{X = e\}$ for all $e \in E$, we need to check that

$$\sum_{e \in E} \mathbb{P}\{X = e\} = 1$$

By Lemma 7.2.9, we have

$$\sum_{e \in E} \mathbb{P}\{X = e\} = \mathbb{P}\left(\bigcup_{e \in E} \{X = e\}\right) = \mathbb{P}(\Omega) = 1$$

as required. □

The following corollary follows immediately.

Corollary 7.2.11
Let $(\Omega, \mathbb{P})$ be a probability space, let E be a countable set, and let X be an E-valued random variable. The function $X_* \mathbb{P} : \mathcal{P}(E) \to [0, 1]$ defined by

$$(X_* \mathbb{P})(A) = \sum_{e \in A} f_X(e) = \mathbb{P}\{X \in A\}$$

for all $A \subseteq E$ defines a probability measure on E. The space $(E, X_* \mathbb{P})$ is called the **pushforward probability measure** of X. □

Corollary 7.2.11 implies that any statement about probability measures can be applied to the pushforward measure. For example,

$$\mathbb{P}\{X \in A \cup B\} = \mathbb{P}\{X \in A\} + \mathbb{P}\{X \in B\} - \mathbb{P}\{X \in A \cap B\}$$

for all subsets $A, B \subseteq E$.

As with events, there is a notion of independence for random variables.

> **Definition 7.2.12**
> Let $(\Omega, \mathbb{P})$ be a discrete probability space and let $X, Y : \Omega \to E$ be discrete random variables on $(\Omega, \mathbb{P})$. We say X and Y are **independent** if, for all $e, e' \in E$, the events $\{X = e\}$ and $\{Y = e'\}$ are independent. More generally, random variables $X_1, X_2, \ldots, X_n$ are **mutually independent** if, for all $e_1, e_2, \ldots, e_n \in E$, the events $\{X_i = e_i\}$ are mutually independent.

Example 7.2.13

A fair six-sided die is rolled twice. Let X be the value shown on the first roll and Y be the value shown on the second roll.

We can model this situation by letting $\Omega = [6] \times [6]$ with $\mathbb{P}(\{(a,b)\}) = \frac{1}{36}$ for all $(a,b) \in \Omega$. The random variables X, Y can thus be taken to be functions $\Omega \to [6]$ defined by

$$X(a,b) = a \text{ and } Y(a,b) = b \text{ for all } (a,b) \in \Omega$$

So let $e, e' \in [6]$. Note first that

$$
\begin{aligned}
\{X = e\} \cap \{Y = e'\} &= \{(a,b) \in \Omega \mid a = e\} \cap \{(a,b) \in \Omega \mid b = e'\} \quad \text{by Notation 7.2.2} \\
&= \{(a,b) \in \Omega \mid a = e \text{ and } b = e'\} \\
&= \{(e,e')\}
\end{aligned}
$$

Hence

$$\mathbb{P}(\{X = e\} \cap \{Y = e'\}) = \mathbb{P}(\{(e,e')\}) = \frac{1}{36} = \frac{1}{6} \cdot \frac{1}{6} = \mathbb{P}\{X = e\}\mathbb{P}\{Y = e'\}$$

The events $\{X = e\}$ and $\{Y = e'\}$ are independent, and so X and Y are independent. ◁

Exercise 7.2.14

A coin which shows heads with probability $p \in [0,1]$, and tails otherwise, is flipped five times. For each $i \in [5]$, let

$$
X_i = \begin{cases}
0 & \text{if the } i^{\text{th}} \text{ flip shows tails} \\
1 & \text{if the } i^{\text{th}} \text{ flip shows heads}
\end{cases}
$$

Prove that the random variables X_1, X_2, X_3, X_4, X_5 are mutually independent. ◁

One final technicality that we mention before continuing concerns performing arithmetic with random variables which assume real values.

Notation 7.2.15

Let $(\Omega, \mathbb{P})$ be a probability space, and let X, Y be real-valued random variables on $(\Omega, \mathbb{P})$. Then we can define a new real-valued random variable $X + Y$ by

$$(X + Y)(\omega) = X(\omega) + Y(\omega) \text{ for all } \omega \in \Omega$$

Likewise for multipication, scalar multiplication and constants: for each $\omega \in \Omega$, define

$$(XY)(\omega) = X(\omega)Y(\omega), \quad (aX)(\omega) = a \cdot X(\omega), \quad a(\omega) = a$$

where $a \in \mathbb{R}$. Note that the random variables $X + Y, XY, aX, a$ are all supported on a countable set.

Example 7.2.16

A coin which shows heads with probability $p \in [0,1]$, and tails otherwise, is flipped n times. For each $i \in [n]$, let

$$X_i = \begin{cases} 0 & \text{if the } i^{\text{th}} \text{ flip shows tails} \\ 1 & \text{if the } i^{\text{th}} \text{ flip shows heads} \end{cases}$$

Then each X_i is a $\{0,1\}$-valued random variable.

Define $X = X_1 + X_2 + \cdots + X_n$. Then X is a $\{0,1,\ldots,n\}$-valued random variable representing the number of heads that show in total after the coin is flipped n times. ◁

Probability distributions

Most of the random variables we are interested in are characterised by one of a few *probability distributions*. We won't define the term 'probability distribution' precisely—indeed, its use in the mathematical literature is often ambiguous and informal—instead, we will take it to mean any description of the random behaviour of a probability space or random variable.

The *uniform distribution* models the real-world situation in which any of a fixed number of outcomes occurs with equal probability.

Definition 7.2.17 (Uniform distribution)

Let $(\Omega, \mathbb{P})$ be a probability space, let E be a finite set, and let $X : \Omega \to E$ be a random variable. We say X follows the **uniform distribution on** E, or X is **uniformly distributed on** E, if f_X is constant—that is, if

$$f_X(e) = \frac{1}{|E|} \text{ for all } e \in E$$

If X is uniformly distributed on E, we write $X \sim \text{Unif}(E)$ (LaTeX code: `\sim`).

Example 7.2.18

Let $(\Omega, \mathbb{P})$ be the probability space modelling the roll of a fair six-sided die, and let X be the $[6]$-valued random variable representing the number shown. Then for each $k \in [6]$ we have

$$f_X(k) = \mathbb{P}\{X = k\} = \mathbb{P}(\{k\}) = \frac{1}{6}$$

so X is uniformly distributed on $[6]$. ◁

Exercise 7.2.19

Let $(\Omega, \mathbb{P})$ be the probability space modelling the roll of a fair six-sided die, and let X be

the $\{0, 1\}$-valued random variable which is equal to 0 if the die shows an even number and 1 if the die shows an odd number. Prove that $X \sim \mathrm{Unif}(\{0, 1\})$.   ◁

Before we continue, we prove that the notion of 'uniform distribution' does not make sense for countably infinite sets.

Theorem 7.2.20

Let $(\Omega, \mathbb{P})$ be a probability space and let E be a countably infinite set. There is no notion of a uniformly E-valued random variable X—that is, there is no $p \in [0, 1]$ such that $f_X(e) = p$ for all $e \in E$.

Proof. We may assume $E = \mathbb{N}$; otherwise, re-index the sums accordingly.

Let $p \in [0, 1]$. Note that

$$\sum_{n \in \mathbb{N}} f_X(n) = \sum_{n \in \mathbb{N}} p = \lim_{N \to \infty} \sum_{n=0}^{N} p = \lim_{N \to \infty} (N + 1)p$$

If $p = 0$ then

$$\lim_{N \to \infty} (N + 1)p = \lim_{N \to \infty} 0 = 0$$

If $p > 0$ then, for all $K > 0$, letting $N = \frac{K}{p}$ yields $(N + 1)p = K + p > K$, and hence

$$\lim_{N \to \infty} (N + 1)p = \infty$$

Thus $\sum_{n \in \mathbb{N}} p \neq 1$ for all $p \in [0, 1]$.

In both cases, we have contradicted Theorem 7.2.10. As such, there can be no random variable $X : \Omega \to \mathbb{N}$ such that f_X is constant.   □

The *Bernoulli distribution* models real-world situations in which one of two outcomes occurs, but not necessarily with the same probability.

Definition 7.2.21 (Bernoulli distribution)

Let $(\Omega, \mathbb{P})$ be a probability space. A $\{0, 1\}$-valued random variable X follows the **Bernoulli distribution with parameter** p if its probability mass function $f_X : \{0, 1\} \to [0, 1]$ satisfies

$$f_X(0) = 1 - p \quad \text{and} \quad f_X(1) = p$$

If X follows the Bernoulli distribution with parameter p, we write $X \sim \mathrm{B}(1, p)$.

The reason behind the notation $\mathrm{B}(1,p)$ will become clear soon—the Bernoulli distribution is a specific instance of a more general distribution, which we will see in Definition 7.2.24.

Example 7.2.22
A coin shows 'heads' with probability p and 'tails' with probability $1 - p$. Let X be the random variable which takes the value 0 if the coin shows tails and 1 if the coin shows heads. Then $X \sim \mathrm{B}(1,p)$. ◁

Exercise 7.2.23
Let X be a $\{0,1\}$-valued random variable. Prove that $X \sim \mathrm{U}(\{0,1\})$ if and only if $X \sim \mathrm{B}(1,\frac{1}{2})$. ◁

Suppose that, instead of flipping a coin just once, as in Example 7.2.22, you flip it n times. The total number of heads that show must be an element of $\{0,1,\ldots,n\}$, and each such element occurs with some positive probability. The resulting probability distribution is called the *binomial distribution*.

Definition 7.2.24 (Binomial distribution)
Let $(\Omega, \mathbb{P})$ be a probability space. A $\{0,1,\ldots,n\}$-valued random variable X follows the **binomial distribution with parameters** n,p if its probability mass function $f_X : \{0,1,\ldots,n\} \to [0,1]$ satisfies

$$f_X(k) = \binom{n}{k} p^k (1-p)^{n-k}$$

for all $k \in \{0,1,\ldots,n\}$. If X follows the binomial distribution with parameters n,p, we write $X \sim \mathrm{B}(n,p)$.

Example 7.2.25
A coin which shows heads with probability $p \in [0,1]$, and tails otherwise, is flipped n times. We will prove that the number of heads that show is binomially distributed.

We can model this situation with probability space $(\Omega, \mathbb{P})$ defined by taking $\Omega = \{\mathrm{H}, \mathrm{T}\}^n$, and letting $\mathbb{P}(\{\omega\}) = p^h(1-p)^t$ for all $\omega \in \Omega$, where h is the number of heads that show and t is the number of tails that show in outcome ω. For example, if $n = 5$ then

$$\mathbb{P}(\{\mathrm{HTHHT}\}) = p^3(1-p)^2 \quad \text{and} \quad \mathbb{P}(\{\mathrm{TTTTT}\}) = (1-p)^5$$

Note in particular that $h + t = n$.

Let X be the random variable which counts the number of heads that show. Formally, we can define $X : \{\mathrm{H}, \mathrm{T}\}^n \to \{0,1,\ldots,n\}$ by letting $X(\omega)$ be the number of heads that show in outcome ω. For example if $n = 5$ then

$$X(\mathrm{HTHHT}) = 3 \quad \text{and} \quad X(\mathrm{TTTTT}) = 0$$

The event $\{X = k\}$ is the set of n-tuples of 'H's and 'T's which contain exactly k 'H'. Hence $|\{X = k\}| = \binom{n}{k}$, since such an n-tuple can be specified by choosing the k positions of the 'H's, and putting 'T's in the remaining positions. Since each outcome in this event occurs with equal probability $p^k(1-p)^{n-k}$, it follows that

$$f_X(k) = \binom{n}{k} p^k(1-p)^{n-k}$$

for all $k \in \{0, 1, \ldots, n\}$. Hence $X \sim \mathrm{B}(n, p)$. ◁

The following theorem proves that the sum of Bernoulli random variables follows the binomial distribution.

Theorem 7.2.26

Let $(\Omega, \mathbb{P})$ be a probability space, let $p \in [0, 1]$ and let $X_1, X_2, \ldots, X_n : \Omega \to \{0, 1\}$ be independent random variables such that $X_i \sim \mathrm{B}(1, p)$. Then

$$X_1 + X_2 + \cdots + X_n \sim \mathrm{B}(n, p)$$

Proof. Let $X = X_1 + X_2 + \cdots + X_n$. For each outcome ω and each $k \in \{0, 1, \ldots, n\}$, we have $X(\omega) = k$ if and only if exactly k of the values $X_1(\omega), X_2(\omega), \ldots, X_n(\omega)$ are equal to 1.

For each specification S of *which* of the random variables X_i is equal to 1, let $A_S \subseteq \Omega$ be the event that this occurs. Formally, this is to say that, for each $S \subseteq [n]$, we define

$$A_S = \{\omega \in \Omega \mid X_i(\omega) = 0 \text{ for all } i \notin S \text{ and } X_i(\omega) = 1 \text{ for all } i \in S\}$$

Then $\mathbb{P}(A_S) = p^k(1-p)^{n-k}$, since the random variables $X_1, X_2, \ldots, X_n$ are mutually independent.

As argued above sets $\{A_S \mid U \subseteq [n], |S| = k\}$ form a partition of $\{X = k\}$, and hence

$$f_X(k) = \sum_{S \in \binom{[n]}{k}} \mathbb{P}(A_S) = \sum_{S \in \binom{[n]}{k}} p^k(1-p)^{n-k} = \binom{n}{k} p^k(1-p)^{n-k}$$

which is to say that $X \sim \mathrm{B}(n, p)$. □

We will make heavy use of Theorem 7.2.26 in Section 7.3, when we will study the *expectation* of binomially distributed random variables. First, let's will look at a couple of scenarios in which a binomially distributed random variable is expressed as a sum of independent Bernoulli random variables.

Example 7.2.27

In Example 7.2.25, we could have defined $\{0,1\}$-valued random variables $X_1, X_2, \ldots, X_n$ by letting

$$X_i(\omega) = \begin{cases} 0 & \text{if the } i^{\text{th}} \text{ coin flip shows tails} \\ 1 & \text{if the } i^{\text{th}} \text{ coin flip shows heads} \end{cases}$$

Then the number of heads shown in total is the random variable $X = X_1 + X_2 + \cdots + X_n$. Note that each random variable X_i follows the Bernoulli distribution with parameter p, and they are independent, so that $X \sim \mathrm{B}(n, p)$ by Theorem 7.2.26. ◁

In Example 7.2.25, we flipped a coin a fixed number of times and counted how many heads showed. Now suppose that we flip a coin repeatedly until heads show, and then stop. The number of times the coin was flipped before heads shows could, theoretically, be any natural number. This situation is modelled by the *geometric distribution*.

Definition 7.2.28 (Geometric distribution on $\mathbb{N}$)

Let $(\Omega, \mathbb{P})$ be a probability space. An $\mathbb{N}$-valued random variable X follows the **geometric distribution with parameter** p if its probability mass function $f_X : \mathbb{N} \to [0, 1]$ satisfies

$$f_X(k) = (1-p)^k p \text{ for all } k \in \mathbb{N}$$

If X follows the geometric distribution with parameter p, we write $X \sim \mathrm{Geom}(p)$.

Example 7.2.29

A coin which shows heads with probability $p \in [0, 1]$, and tails otherwise, is flipped repeatedly until heads shows. ◁

Exercise 7.2.30

Let $p \in [0, 1]$ and let $X \sim \mathrm{Geom}(p)$. Prove that

$$\mathbb{P}\{X \text{ is even}\} = \frac{1}{1 - p}$$

What is the probability that X is odd? ◁

Occasionally, it will be useful to consider geometrically distributed random variables which are valued in the set

$$\mathbb{N}^+ = \{1, 2, 3, \ldots\}$$

of all *positive* natural numbers. The probability mass function of such a random variable is slightly different.

Definition 7.2.31 (Geometric distribution on $\mathbb{N}^+$)

Let $(\Omega, \mathbb{P})$ be a probability space. An $\mathbb{N}^+$-valued random variable X follows the **geometric distribution with parameter** p if its probability mass function $f_X : \mathbb{N} \to [0, 1]$ satisfies

$$f_X(k) = (1 - p)^{k-1} p \text{ for all } k \in \mathbb{N}^+$$

If X follows the geometric distribution with parameter p, we write $X \sim \text{Geom}(p)$.

It is to be understood from context whether a given geometric random variable is $\mathbb{N}$-valued or $\mathbb{N}^+$-valued.

Example 7.2.32

An urn contains $n \geqslant 1$ distinct coupons. Each time you draw a coupon that you have not drawn before, you get a stamp. When you get all n stamps, you win. Let X be the number of coupons drawn up to, and including, a winning draw.

For each $k \in [n]$, let X_k be the random variable representing the number of draws required to draw the kth new coupon, after $k - 1$ coupons have been collected. Then the total number of times a coupon must be drawn is $X = X_1 + X_2 + \cdots + X_n$.

After $k - 1$ coupons have been collected, there are $n - k + 1$ uncollected coupons remaining in the urn, and hence on any given draw, an uncollected coupon is drawn with probability $\frac{n-k+1}{n}$, and a coupon that has already been collected is drawn with probability $\frac{k-1}{n}$. Hence for each $r \in \mathbb{N}^+$ we have

$$\mathbb{P}[X_k = r] = \left(\frac{k - 1}{n}\right)^{r-1} \left(\frac{n - k + 1}{n}\right)$$

That is to say, X_k is geometrically distributed on $\mathbb{N}^+$ with parameter $\frac{n-k+1}{n}$.

We will use this in Example 7.3.15 to compute the number of times a person should expect to have to draw coupons from the urn until they win.   ◁

7.3   Expectation

We motivate the definition of *expectation* (Definition 7.3.2) with the following example.

Example 7.3.1

For each $n \geqslant 1$, let X_n be the average value shown when a fair six-sided die is rolled n times.

When n is small, the value of X_n is somewhat unpredictable. For example, X_1 is uniformly distributed, since it takes each of the values $1, 2, 3, 4, 5, 6$ with equal probability. This is summarised in the following table:

e	1	2	3	4	5	6
$\mathbb{P}\{X_1 = e\}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$

The distribution of X_2 is shown in the following table:

e	1	1.5	2	2.5	3	3.5	4	4.5	5	5.5	6
$\mathbb{P}\{X_2 = e\}$	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

As can be seen, the probabilities increase towards the middle of the table; the extreme values occur with low probability. This effect is exaggerated as n increases. Indeed,

$$\mathbb{P}\{X_n = 1\} = \mathbb{P}\{X_n = 6\} = \frac{1}{6^n}$$

which is extremely small when n is large; however, it can be shown that for all $\varepsilon > 0$, we have

$$\mathbb{P}\{3.5 - \varepsilon < X_n < 3.5 + \varepsilon\} \to 1$$

Thus when we roll a die repeatedly, we can expect its value to approach 3.5 with arbitrary precision. This is an instance of a theorem called the *law of large numbers*, which we will not prove here. ◁

The value 3.5 in Example 7.3.1 is special because it is the average of the numbers $1, 2, 3, 4, 5, 6$. More generally, assignments of different probabilities to different values of a random variable X yields a *weighted average* of the possible values. This weighted average, known as the *expectation* of the random variable, behaves in the same way as the number 3.5 did in Example 7.3.1.

Definition 7.3.2

Let $(\Omega, \mathbb{P})$ be a probability space, let $E \subseteq \mathbb{R}$ be countable, and let X be an E-valued random variable on $(\Omega, \mathbb{P})$. The **expectation** (or **expected value**) of X, if it exists, is the real number $\mathbb{E}[X]$ (LaTeX code: `\mathbb{E}`) defined by

$$\mathbb{E}[X] = \sum_{e \in E} e f_X(e)$$

Example 7.3.3

Let X be a random variable representing the value shown when a fair six-sided die is rolled. Then $X \sim \mathrm{U}([6])$, so that $f_X(k) = \frac{1}{6}$ for all $k \in [6]$, and hence

$$\mathbb{E}[X] = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = \frac{21}{6} = 3.5$$

so the expected value of the die roll is 3.5. ◁

Example 7.3.4

Let $p \in [0,1]$ and let $X \sim \mathrm{B}(1,p)$. Then

$$\mathbb{E}[X] = 0 \cdot (1-p) + 1 \cdot p = p$$

So the expected value of a Bernoulli random variable is equal to the parameter. ◁

Exercise 7.3.5

Let $(\Omega, \mathbb{P})$ be a probability space and let $c \in \mathbb{R}$. Thinking of c as a *constant* real-valued random variable,[a] prove that $\mathbb{E}[c] = c$. ◁

The following lemma provides an alternative method for computing the expectation of a random variable. It will be useful for proving that expectation is *linear* in Theorem 7.3.11.

Lemma 7.3.6

Let $(\Omega, \mathbb{P})$ be a probability space, let E be a countable set and let X be an E-valued random variable on $(\Omega, \mathbb{P})$. Then

$$\mathbb{E}[X] = \sum_{\omega \in \Omega} X(\omega) \mathbb{P}(\{\omega\})$$

Proof. Recall from Lemma 7.2.9 that

$$\Omega = \bigcup_{e \in E} \{X = e\}$$

---

[a] Formally, we should define $X : \Omega \to \mathbb{R}$ by letting $X(\omega) = c$ for all $\omega \in \Omega$; then compute $\mathbb{E}[X]$.

and the events $\{X = e\}$ are mutually exclusive. Hence

$$
\begin{aligned}
\sum_{\omega \in \Omega} X(\omega)\mathbb{P}(\{\omega\}) &= \sum_{e \in E} \sum_{\omega \in \{X = e\}} X(\omega)\mathbb{P}(\{\omega\}) && \text{by Lemma 7.2.9} \\
&= \sum_{e \in E} e\mathbb{P}\{X = e\} && \text{by (ii) in Proposition 7.1.5} \\
&= \sum_{e \in E} e f_X(e) && \text{by Definition 7.2.6}
\end{aligned}
$$

as required. □

Proposition 7.3.7

Let $n \in \mathbb{N}$ and $p \in [0, 1]$, and suppose that X is a random variable such that $X \sim \mathrm{B}(n, p)$. Then $\mathbb{E}[X] = np$.

Proof. Since $X \sim \mathrm{B}(n, p)$, we have $f_X(k) = \binom{n}{k}p^k(1 - p)^{n-k}$ for all $0 \leqslant k \leqslant n$. Hence

$$
\begin{aligned}
\mathbb{E}[X] &= \sum_{k=0}^{n} k \cdot \binom{n}{k}p^k(1 - p)^{n-k} && \text{by definition of expectation} \\
&= \sum_{k=1}^{n} k \cdot \binom{n}{k}p^k(1 - p)^{n-k} && \text{since the } k = 0 \text{ term is zero} \\
&= \sum_{k=1}^{n} n\binom{n - 1}{k - 1}p^k(1 - p)^{n-k} && \text{by Proposition 4.2.45} \\
&= \sum_{\ell=0}^{n-1} n\binom{n - 1}{\ell}p^{\ell+1}(1 - p)^{(n-1)-\ell} && \text{writing } \ell = k + 1 \\
&= np \cdot \sum_{\ell=0}^{n-1} \binom{n - 1}{\ell}p^\ell(1 - p)^{(n-1)-\ell} && \text{pulling out constant factors} \\
&= np(p + (1 - p))^{n-1} && \text{by the binomial theorem} \\
&= np && \text{since } p + (1 - p) = 1
\end{aligned}
$$

as required. □

Example 7.3.8

A coin which shows heads with probability $\frac{1}{3}$, and tails otherwise, is tossed 12 times. Letting X be the random variable represent the number of heads that show, we see that $X \sim \mathrm{B}(12, \frac{1}{3})$, and hence the expected number of heads that show is equal to

$$
\mathbb{E}[X] = 12 \cdot \frac{1}{3} = 4
$$

◁

Exercise 7.3.9

Use Proposition 6.3.2 to prove that the expectation of a $\mathbb{N}$-valued random variable which is geometrically distributed with parameter $p \in [0, 1]$ is equal to $\frac{1-p}{p}$. Use this to compute the expected number of times a coin must be flipped before the first time heads shows, given that heads shows with probability $\frac{2}{7}$. ◁

Exercise 7.3.10

Prove that the expectation of a $\mathbb{N}^+$-valued random variable which is geometrically distributed with parameter $p \in [0, 1]$ is equal to $\frac{1}{p}$. ◁

Theorem 7.3.11 (Linearity of expectation)

Let $(\Omega, \mathbb{P})$ be a probability space, let $E \subseteq \mathbb{R}$ be countable, let X and Y be E-valued random variables on $(\Omega, \mathbb{P})$, and let $a, b \in \mathbb{R}$. Then

$$\mathbb{E}[aX + bY] = a\mathbb{E}[X] + b\mathbb{E}[Y]$$

Proof. This follows directly from the fact that summation is linear. Indeed,

$$
\begin{aligned}
\mathbb{E}[aX + bY] &= \sum_{\omega \in \Omega} (aX + bY)(\omega)\mathbb{P}(\{\omega\}) && \text{by Lemma 7.3.6} \\
&= \sum_{\omega \in \Omega} \Big(aX(\omega)\mathbb{P}(\{\omega\}) + bY(\omega)\mathbb{P}(\{\omega\}) \Big) && \text{expanding} \\
&= a\sum_{\omega \in \Omega} X(\omega)\mathbb{P}(\{\omega\}) + b\sum_{\omega \in \Omega} Y(\omega)\mathbb{P}(\{\omega\}) && \text{by linearity of summation} \\
&= a\mathbb{E}[X] + b\mathbb{E}[Y] && \text{by Lemma 7.3.6}
\end{aligned}
$$

as required.   □

Example 7.3.12

Let X be a random variable representing the sum of the numbers shown when a fair six-sided die is rolled twice. We can write $X = Y + Z$, where Y is the value of the first die roll and Z is the value of the second die roll. By Example 7.3.3, we have $\mathbb{E}[Y] = \mathbb{E}[Z] = 3.5$. Linearity of expectation then yields

$$\mathbb{E}[X] = \mathbb{E}[Y] + \mathbb{E}[Z] = 3.5 + 3.5 = 7$$

so the expected value of the sum of the two die rolls is 7. ◁

Example 7.3.13

A coin, when flipped, shows heads with probability $p \in [0, 1]$. The coin is flipped. If it

shows heads, I gain \$10; if it shows tails, I lose \$20. We compute the least value of p that ensures that I do not expect to lose money.

Let X be the random variable which is equal to 0 if tails shows, and 1 if heads shows. then $X \sim \mathrm{B}(1, p)$, so that $\mathbb{E}[X] = p$ by Example 7.3.4. Let Y be the amount of money I gain. Then

$$Y = 10X - 20(1 - X) = 30X - 20$$

Hence my expected winnings are

$$\mathbb{E}[Y] = 30\mathbb{E}[X] - 20 = 30p - 20$$

In order for this number to be non-negative, we require $p \geqslant \frac{2}{3}$. $\triangleleft$

Theorem 7.3.11 generalises by induction to linear combinations of countably many random variables; this is proved in the following exercise

Exercise 7.3.14
Let $(\Omega, \mathbb{P})$ be a probability space, let $E \subseteq \mathbb{R}$ be countable, let $\{X_i \mid i \in I\}$ be a family of E-valued random variables on $(\Omega, \mathbb{P})$, indexed by some countable set I, and let $\{a_n \mid n \in \mathbb{N}\}$ be an I-indexed family of real numbers. Prove that

$$\mathbb{E}\left[\sum_{i \in I} a_i X_i\right] = \sum_{i \in I} a_i \mathbb{E}[X_i]$$

$\triangleleft$

Example 7.3.15
Recall Exercise 7.2.32: an urn contains $n \geqslant 1$ distinct coupons. Each time you draw a coupon that you have not drawn before, you get a stamp. When you get all n stamps, you win. We find the expected number of times you need to draw a coupon from the urn in order to win.

For each $k \in [n]$, let X_k be the random variable representing the number of draws required to draw the kth new coupon, after $k - 1$ coupons have been collected. Then the total number of times a coupon must be drawn is $X = X_1 + X_2 + \cdots + X_n$.

We already saw that $X_k \sim \mathrm{Geom}\left(\frac{n-k+1}{n}\right)$ for each $k \in [n]$. By Exercise 7.3.10, we have $\mathbb{E}[X_k] = \frac{n}{n-k+1}$ for all $k \in [n]$. By linearity of expectation, it follows that

$$\mathbb{E}[X] = \sum_{k=1}^{n} \mathbb{E}[X_k] = \sum_{k=1}^{n} \frac{n}{n - k + 1} = n \sum_{i=1}^{n} \frac{1}{i}$$

$\triangleleft$

Chapter 8

Additional topics

8.1   Ring theory

In Chapter 3 we examined the integers by pushing their *arithmetic structure* to their limits. Everything we did—including the definition and study of divisibility—was done in terms of addition, subtraction and multiplication.

Given a set R, provided we can make sense of addition, subtraction and multiplication, we can make all the same basic definitions—like divisibility, greatest common divisors, and so on—and ask ourselves to what extent the results that held true of integers hold for R.

This motivates the definition of a *ring*.

Definition 8.1.1

A (**commutative**) **ring** (**with unity**) is a set R equipped with:

- An **addition** function $a : R \times R \to R$; we write $a(r, s) = r + s$ for $r, s \in R$;

- A **negation** function $n : R \to R$; we write $n(r) = -r$ for $r \in R$;

- A **multiplication** function $m : R \times R \to R$; we write $m(r, s) = r \cdot s$ for $r, s \in R$;

- An **additive identity** element $0_R \in R$;

- A **multiplicative identity** element $1_R \in R$

such that the following conditions hold:

- Properties of addition

  ◇ (Associativity) If $r, s, t \in R$ then $(r + s) + t = r + (s + t)$;

  ◇ (Identity) If $r \in R$ then $r + 0_R = 0_R + r = r$;

  ◇ (Inverse) If $r \in R$ then $r + (-r) = (-r) + r = 0_R$;

  ◇ (Commutativity) If $r, s \in R$ then $r + s = s + r$.

- Properties of multiplication

  ◇ (Associativity) If $r, s, t \in R$ then $(r \cdot s) \cdot t = r \cdot (s \cdot t)$;

  ◇ (Identity) If $r \in R$ then $r \cdot 1_R = 1_R \cdot r = r$;

  ◇ (Commutativity) If $r, s \in R$ then $r \cdot s = s \cdot r$.

- Relationship between addition and multiplication

  ◇ (Distributivity) If $r, s, t \in R$ then $r \cdot (s + t) = (r \cdot s) + r \cdot t$.

Example 8.1.2
The number sets $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are all rings with their usual notions of addition and multiplication and so on. The ring $\mathbb{Z}$ of integers was our focus in Chapter 3. ◁

Example 8.1.3
Let X be a set. Then the power set $\mathcal{P}(X)$ is a ring, with:

- $U + V = U \triangle V$; that is, addition is given by the symmetric difference.

- $-U = U$;

- $U \cdot V = U \cap V$; that is, multiplication is given by intersection;

- $0_{\mathcal{P}(X)} = \varnothing$;

- $1_{\mathcal{P}(X)} = X$.

◁

Exercise 8.1.4
Verify that $\mathcal{P}(X)$, as described in Example 8.1.3, is a ring. ◁

Example 8.1.5
There are many other rings. Some commonly occuring ones are:

- Given a ring R, there is a ring $R[x]$ of **polynomials over** R. That is, expressions of the form
$$r_0 + r_1 x + \cdots + r_n x^n$$
where $n \in \mathbb{N}$ and $r_0, \ldots, r_n \in R$.

- If $n \in \mathbb{Z}$ is not a perfect square, we can define
$$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$$
with addition and multiplication defined as you'd expect; in particular
$$(a + b\sqrt{n})(c + d\sqrt{n}) = (ac + bdn) + (ad + bc)\sqrt{n}$$
This is defined even when $n < 0$. For example in $\mathbb{Z}[\sqrt{-5}]$ we have
$$(1 - \sqrt{-5})(1 + \sqrt{-5}) = (1 + 5) + (1 - 1)\sqrt{-5} = 6$$

- Given $n > 0$, the set $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$ can be given the structure of a ring by declaring $a + b$ to be the remainder of $a + b$ when divided by n, and likewise for $a \cdot b$.

$\triangleleft$

Many of the definitions that we provided for integers can then be carried over to arbitrary rings; we'll spend most of the rest of this section comparing them.

Units and zero divisors

Definition 8.1.6

Let R be a ring.

- Let $r, s \in R$. We say r **divides** s, and write $r \mid s$ if there exists $q \in R$ such that $s = qr$.

- $u \in R$ is a **unit** if $u \mid 1_R$.

Example 8.1.7

Some examples of divisors and units in rings are as follows:

- We showed above that $1 + \sqrt{5} \mid 6$ in $\mathbb{Z}[\sqrt{-5}]$.

- The number $1 + \sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$: indeed, $1 + \sqrt{2} \mid 1$ since

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = (-1 + 2) + (-1 + 1)\sqrt{2} = 1$$

- In $\mathbb{Q}$ and $\mathbb{R}$, every non-zero element is a unit. Indeed, if $x \in \mathbb{Q}$ and $x \neq 0$ then $\frac{1}{x} \in \mathbb{Q}$, so $x \cdot \frac{1}{x} = 1$, so $x \mid 1$. Likewise with $\mathbb{R}$.

- We know that if $a \perp n$ then a has a multiplicative inverse modulo n; this is precisely the assertion that $a \perp n$ if and only if a is a unit in $\mathbb{Z}_n$. (Contrast this to the situation of $\mathbb{Z}$, where the only units are -1 and 1.)

$\triangleleft$

One definition that we *didn't* give for the integers, because it would have been silly, is that of a *zero divisor*.

Definition 8.1.8

Let R be a ring. A **zero divisor** in R is an element $r \in R$ such that $r \mid 0_R$. We say R is an **integral domain** if the only zero divisor in R is 0_R itself.

So for example $\mathbb{Z}$ is an integral domain, since if $r \in \mathbb{Z}$ and $r \mid 0$, then $r = 0$.

Proposition 8.1.9

Let $n > 1$. Then $\mathbb{Z}_n$ is an integral domain if and only if n is prime.

Proof. Suppose n is composite, say $n = ab$ where $0 < a < n$ and $0 < b < n$. Then $ab = 0$ in $\mathbb{Z}_n$, so $a \mid 0$, even though $a \neq 0$. Hence $\mathbb{Z}_n$ is not an integral domain.

Conversely, suppose n is prime. Then $a \perp n$ for all $a \in \mathbb{Z}_n$ with $a \neq 0$, so a has a multiplicative inverse $b \in \mathbb{Z}_n$ modulo n. That is, $ab = 1$ in $\mathbb{Z}_n$. Suppose, furthermore, that a is a zero divisor. Then $ac = 0$ for some $c \in \mathbb{Z}_n$ with $c \neq 0$. Hence

$$c = 1 \cdot c = (ab)c = (ac)b = 0b = 0$$

contradicting the fact that $c \neq 0$. So a must not be a zero divisor. So $\mathbb{Z}_n$ is an integral domain. $\square$

Primes and irreducibles

The definitions of primes and irreducibles in $\mathbb{Z}$ carry over to arbitrary integral domains.

Definition 8.1.10

Let R be an integral domain and let $p \in R$. Then

- p is **prime** if p is a non-zero non-unit and, for all $r, s \in R$, if $p \mid rs$ then $p \mid r$ or $p \mid s$;

- p is **irreducible** if p is a non-zero non-unit and, for all $r, s \in R$, if $p = rs$ then either r is a unit or s is a unit.

Primes and irreducibles coincide in the ring $\mathbb{Z}$, as we proved in Theorem 3.2.11, but this is not necessarily the case in an arbitrary ring.

Example 8.1.11

In $\mathbb{Z}[\sqrt{-5}]$, the element 2 is irreducible. Moreover, since $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$, we have

$$2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

However, $2 \nmid 1 + \sqrt{-5}$ and $2 \nmid 1 - \sqrt{-5}$. Indeed, if $2 \mid 1 + \sqrt{-5}$, then there will exist $a, b \in \mathbb{Z}$ such that

$$1 + \sqrt{-5} = 2(a + b\sqrt{-5}) = 2a + 2b\sqrt{-5}$$

But this implies that $1 = 2a$, and hence $2 \mid 1$ in $\mathbb{Z}$, which is nonsense. Likewise for $1 - \sqrt{-5}$.

Hence 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$. However 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, though the proof of this is omitted here because it's a little involved. ◁

We can classify some rings in which primes and irreducibles *do* coincide, however.

Principal ideal domains

Definition 8.1.12
Let R be a ring. An **ideal** in R is a subset $I \subseteq R$ such that

- If $x, y \in I$ then $x - y \in I$; and

- If $x \in I$ and $r \in R$ then $rx \in I$.

Example 8.1.13
We have seen **To do:** reference; PS4 Q3 that if $I \subseteq \mathbb{Z}$ is an ideal then

$$I = d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\}$$

for some $d \in \mathbb{Z}$. ◁

The proof of Exercise 8.1.13 relies fundamentally on the division theorem. However, we cannot state the division theorem for an arbitrary ring because it used the order relation $\leqslant$ on $\mathbb{Z}$, which might not exist in an arbitrary ring.

Example 8.1.14
There is an ideal in $\mathbb{Z}[x]$ defined by

$$(2, x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\} = \{2a + xq(x) \mid a \in \mathbb{Z}, \ q(x) \in \mathbb{Z}[x]\}$$

◁

Ideals in a ring R give rise to a nice kind of an equivalence relation, called a **congruence relation**. Define $\equiv_I$ by $r \equiv_I s$ if and only if $r - s \in I$. The quotient $R/\equiv_I$ is denoted by R/I, and the equivalence class $[r]_{\equiv_I}$ is denoted by $r + I$.

Example 8.1.15
In $\mathbb{Z}$, if $I = n\mathbb{Z}$ then, given $a, b \in \mathbb{Z}$, we have

$$a \equiv_{n\mathbb{Z}} b \quad \Leftrightarrow \quad a - b \in n\mathbb{Z} \quad \Leftrightarrow \quad n \mid a - b \quad \Leftrightarrow \quad a \equiv b \bmod n$$

Hence $a + n\mathbb{Z} = [a]_n$ and $\mathbb{Z}/n\mathbb{Z}$ is what we previously called $\mathbb{Z}/n\mathbb{Z}$. ◁

Moreover, in any ring R with ideal I, the relation $\equiv_I$ is compatible with the operations of R; in other words, if $r + s = r' + s'$ in R then

$$(r + s) + I = (r' + s') + I$$

and likewise for multiplication. Hence we have a form of modular arithmetic that we can perform in any ring.

Example 8.1.16

Consider the ring $\mathbb{R}[x]$ of polynomials with real coefficients. Define

$$I = \langle x^2 + 1 \rangle = \{(x^2 + 1)f(x) \mid f(x) \in \mathbb{R}[x]\}$$

Then I is an ideal in $\mathbb{R}[x]$, and the quotient ring $R[x]/\langle x^2 + 1 \rangle$ is 'the same' as the set of complex numbers; that is, the real numbers extended by allowing $\sqrt{-1}$ to exist. ◁

Principal ideal domains

Definition 8.1.17

An ideal I is **principal** if there exists $d \in R$ such that

$$I = \{rd \mid r \in R\}$$

In this case we write $I = (d)$. A ring R is called a **principal ideal domain** if every ideal in R is principal.

A consequence of 8.1.13 is:

Proposition 8.1.18

$\mathbb{Z}$ is a principal ideal domain.

Nonetheless, there are other examples of principal ideal domains, such as $\mathbb{Q}[x]$ and $\mathbb{Z}[\sqrt{-1}]$.

Theorem 8.1.19

Let R be a ring. If R is a principal ideal domain, then every irreducible element $p \in R$ is prime.

Proof. Let $p \in R$ and suppose p is irreducible.

First note that if $I \subseteq R$ is an ideal and $p \in I$, then either $I = (p)$ or $I = R$. Certainly $(p) \subseteq I$ since p, and hence all multiples of p are elements of I. Since R is a principal ideal

domain, $I = (x)$ for some $x \in R$. Since $p \in I$ we must have $p = rx$ for some $r \in I$. Since p is irreducible, either x is a unit or r is a unit. If x is a unit then $I = R$. If r is a unit then $qr = 1$ for some $q \in R$, so $x = qrx = qp \in (p)$, so $I \subseteq (p)$, and hence $I = (p)$. So either $I = (p)$ or $I = R$.

Now fix $r, s \in R$ and suppose that $p \mid rs$. We need to prove that $p \mid r$ or $p \mid s$. **To do: Finish proof** $\square$

8.2   Ordinal and cardinal numbers

8.3   Boolean algebra

8.4 Complex numbers

8.5   Limits and asymptotes

Appendix A

Hints for selected exercises

Hint for Exercise 1.2.9
Suppose $n = d_r \cdot 10^r + \cdots + d_1 \cdot 10 + d_0$ and let $s = d_r + \cdots + d_1 + d_0$. Start by proving that $3 \mid n - s$.

Hint for Exercise 1.2.21
Use the law of excluded middle with the proposition '$\sqrt{2}^{\sqrt{2}}$ is rational'.

Hint for Exercise 1.2.34
Look carefully at the definition of divisibility (Definition 1.1.12).

Hint for Exercise 1.3.13
Let $q(n)$ be the statement $p(n + b)$ and prove $q(n)$ for all $n \geqslant 0$ by induction on n.

Hint for Exercise 1.3.42
Prove first that if $a \in \mathbb{Z}$ and a^2 is divisible by 3, then a is divisible by 3.

Hint for Exercise 2.3.28
Look closely at Definition 2.3.23.

Hint for Exercise 3.1.11
Remember that negative integers can be greatest common divisors too.

Hint for Exercise 3.1.13
Start by proving that d and d' must divide each other.

Hint for Exercise 3.1.24
Exercise 3.1.21 would be a good starting point.

Hint for Exercise 3.1.39
This is essentially the same as Exercise 3.1.13.

Hint for Exercise 3.1.41
Define $m = \dfrac{ab}{\gcd(a,b)}$ and prove that m satisfies the definition of being a least common multiple of a and b (Definition 3.1.38). Then apply Exercise 3.1.39.

Hint for Exercise 3.2.5
Use the factorial formula for binomial coefficients (Theorem 1.3.31).

Hint for Exercise 3.2.9
Assume $p = mn$ for some $m, n \in \mathbb{Z}$. Prove that m or n is a unit.

Hint for Exercise 3.2.22
What are the prime factors of $n! - 1$?

Hint for Exercise 3.3.23
Consider the list $a^0, a^1, a^2, \dots$. Since there are only finitely many remainders modulo n, we must have $a^i \equiv a^j \bmod n$ for some $0 \leqslant i < j$.

Hint for Exercise 3.3.30
First find the remainder of 244886 when divided by 12.

Hint for Exercise 3.3.33
Consider what it means for an element of $[p^k]$ *not* to be coprime to p^k.

Hint for Exercise 3.3.38
You need to use the fact that p is prime at some point in your proof.

Hint for Exercise 3.3.39
Pair as many elements of $[p - 1]$ as you can into multiplicative inverse pairs modulo p.

Hint for Exercise 3.3.49
This generalisation will be tricky! You may need to generalise the definitions and results about greatest common divisors and least common multiples that we have seen so far, including Bézout's lemma. You might want to try proving this first in the case that $n_i \perp n_j$ for all $i \neq j$.

Hint for Exercise 3.3.50
Observe that if $a, k \in \mathbb{Z}$ and $k \mid a$, then $k \mid a + k$.

Hint for Exercise 4.1.10
Recall Definition 2.3.29.

Hint for Exercise 4.1.12

If Z were a subset of Y, then we could easily define an injection $i : Z \to Y$ by $i(z) = z$ for all $z \in Z$. Are there any subsets of Y that are associated with a function with codomain Y?

Hint for Exercise 4.1.16

Write the elements of both sets on an $m \times n$ grid, and then find a function that sends an element on one grid to the corresponding element of the other. Quotients and remainders might be useful! (See Section 3.1.)

Hint for Exercise 4.1.22

When defining a left inverse $g : Y \to X$ for f, consider for each $y \in Y$ whether or not y is in the image of f. If it is, what value must $g(y)$ take? If it isn't, does it matter what value $g(y)$ takes?

Hint for Exercise 4.1.25

Think about how you prove that a function f is surjective and, given $y \in Y$, identify where in the proof you define an element of X that you could take to be the value $g(y)$ of a right inverse $g : Y \to X$.

Hint for Exercise 4.1.28

For part (c), don't try to write a formula for the inverse of h; instead, use the fundamental theorem of arithmetic.

Hint for Exercise 4.1.33

Use Exercise 4.1.29.

Hint for Exercise 4.2.29

Any function $f : X \to Y$ with finite domain can be specified by listing its values. For each $x \in X$, how many choices do you have for the value $f(x)$?

Hint for Exercise 4.2.34

An injection $[3] \to [4]$ must have exactly three values.

Hint for Exercise 4.2.47

How many ways can you select $k + 1$ animals from a set containing n cats and one dog?

Hint for Exercise 4.2.50

Find two procedures for counting the number of pairs (U, u), such that $U \subseteq [n]$ is a k-element subset and $u \in U$. Equivalently, count the number of ways of forming a committee of size k from a population of size n, and then appointing one member of the committee to be the chair.

Hint for Exercise 4.2.54

Find an expression for $(a + b + c)!$ in terms of $a!$, $b!$, $c!$ and $\binom{a+b+c}{a,b,c}$, following the pattern of Theorem 4.2.49.

Hint for Exercise 4.2.56

Find a bijection $[p] \times C_n \to C_{pn}$, where C_n is defined as in Theorem 4.2.55.

Hint for Exercise 4.3.4

You need to find a family of subsets of $\mathbb{N}$ such that (i) any two of the subsets have infinitely many elements in common, but (ii) given any natural number, you can find one of the subsets that it is *not* an element of.

Hint for Exercise 4.3.8

Use prime factorisation.

Hint for Exercise 4.3.15

Suppose $X = \mathbb{N}$. By Proposition 4.3.10, the set $\mathbb{N}^k$ is countable. By Theorem 4.3.11(c), it suffices to find an injection $\binom{\mathbb{N}}{k} \to \mathbb{N}^k$.

Hint for Exercise 4.3.19

We have already proved this when X is finite. When X is countably infinite, find a bijection $\{0,1\}^X \to \mathcal{P}(X)$ and apply Theorem 4.3.18. When X is uncountably infinite, find an injection $X \to \mathcal{P}(X)$ and find a way to apply Corollary 4.3.12.

Hint for Exercise 5.2.26

Use the characterisation of gcd and lcm in terms of prime factorisation.

Hint for Exercise 5.2.29

Use distributivity, together with the fact that $\bot \vee y' = y'$ and $\top \wedge y' = y'$.

Hints for exercises in Chapter 5 and thereafter are coming soon.

Appendix B

Foundations

B.1   Logical theories and models

First-order logic

Throughout, a countably infinite set Var of **variables** is fixed.

Definition B.1.1

A **signature for first-order logic** is a quadruple $\Sigma = (\mathcal{C}, \mathcal{F}, \mathcal{R}, \mathrm{ar})$, where $\mathcal{C}$, $\mathcal{F}$ and $\mathcal{R}$ are pairwise disjoint sets and $\mathrm{ar} : \mathcal{F} \cup \mathcal{R} \to \mathbb{N}$ is a function. **To do:** Provide more intuition. The elements of $\mathcal{C}$ are called **constant symbols**, the elements of $\mathcal{F}$ are called **function symbols** and the elements of $\mathcal{R}$ are called **relation symbols**. Given a function symbol or relation symbol $s \in \mathcal{F} \cup \mathcal{R}$, the value $\mathrm{ar}(s)$ is the **arity** of s.

To do: Examples

Definition B.1.2

Let Σ be a signature for first-order logic. The set $\mathrm{Term}(\Sigma)$ of all Σ-**terms**, and the function $\mathrm{FV} : \mathrm{Term}(\Sigma) \to \mathcal{P}(\mathrm{Var})$ assigning to each term its set of **free variables**, are defined inductively as follows.

- If x is a variable, then x is a term and $\mathrm{FV}(x) = \{x\}$;

- If c is a constant symbol, then c is a term and $\mathrm{FV}(c) = \varnothing$;

- If f is a function symbol of arity k and $t_1, \ldots, t_k$ are terms, then $f(t_1, \ldots, t_k)$ is a term and $\mathrm{FV}(f(t_1, \ldots, t_k)) = \mathrm{FV}(t_1) \cup \cdots \cup \mathrm{FV}(t_k)$.

A term with no free variables is called a **closed term**.

To do: Examples

Definition B.1.3

Let Σ be a signature for first-order logic. The set $\mathrm{Form}(\Sigma)$ of all **logical formulae** over Σ (or Σ-**formulae**), and the function $\mathrm{FV} : \mathrm{Form}(\Sigma) \to \mathcal{P}(\mathrm{Var})$ assigning to each formula its set of **free variables**, are defined inductively as follows.

- $\bot$ is a formula and $\mathrm{FV}(\bot) = \varnothing$;

- If r is a relation symbol of arity k and $t_1, \ldots, t_k$ are terms, then $r(t_1, \ldots, t_k)$ is a formula and $\mathrm{FV}(r(t_1, \ldots, t_k)) = \mathrm{FV}(t_1) \cup \cdots \cup \mathrm{FV}(t_k)$;

- If p is a formula, then $\neg p$ is a formula and $\mathrm{FV}(\neg p) = \mathrm{FV}(p)$.

- If p and q are formulae, then $(p \wedge q)$, $(p \vee q)$ and $(p \Rightarrow q)$ are formulae and

$$\mathrm{FV}(p \wedge q) = \mathrm{FV}(p \vee q) = \mathrm{FV}(p \Rightarrow q) = \mathrm{FV}(p) \cup \mathrm{FV}(q)$$

- If p is a formula and $x \in \mathrm{FV}(p)$, then $\forall x,\, p$ and $\exists x,\, p$ are formulae and

$$\mathrm{FV}(\forall x,\, p) = \mathrm{FV}(\exists x,\, p) = \mathrm{FV}(p) \setminus \{x\}$$

A logical formula with no free variables is called a **sentence**.

To do: Examples

Definition B.1.4

Let Σ be a signature for first-order logic. A **theory** over Σ is a set of Σ-sentences.

To do: Examples

Structures and models

Definition B.1.5

Let Σ be a signature for first-order logic. A Σ-**structure** $\mathfrak{A}$ (LaTeX code: `\mathfrak`) consists of a set A together with:

- For each constant symbol c, an element $c^{\mathfrak{A}} \in A$;

- For each function symbol f of arity k, a function $f^{\mathfrak{A}} : A^k \to A$; and

- For each relation symbol r of arity k, a subset $r^{\mathfrak{A}} \subseteq A^k$.

To do: Examples

Definition B.1.6

Let Σ be a structure for first-order logic and let $\mathfrak{A}$ be a Σ-structure. For each closed Σ-term t, the **interpretation** $t^{\mathfrak{A}}$ of t in $\mathfrak{A}$ is defined inductively by

- If $t = c$ is a constant symbol, then $t^{\mathfrak{A}} = c^{\mathfrak{A}}$.

- If $t = f(t_1, \ldots, t_k)$, where f is a function symbol of arity k and $t_1, \ldots, t_k$ are closed terms, then $t^{\mathfrak{A}} = f^{\mathfrak{A}}(t_1^{\mathfrak{A}}, \ldots, t_k^{\mathfrak{A}})$.

Definition B.1.7

Let Σ be a structure for first-order logic. The relation $\vDash$ from the set of all Σ-structures to the set of all sentences over Σ is defined, for all Σ-structures $\mathfrak{A}$, inductively on sentences as follows:

- $\mathfrak{A} \nvDash \bot$;

- For all relation symbols r of arity k and all terms $t_1, \ldots, t_k$

$$\mathfrak{A} \vDash r(t_1, \ldots, t_k) \text{ if and only if } (t_1^{\mathfrak{A}}, \ldots, t_k^{\mathfrak{A}}) \in r^{\mathfrak{A}}$$

- For all sentences p, q

$$\mathfrak{A} \vDash p \wedge q \text{ if and only if } \mathfrak{A} \vDash p \text{ and } \mathfrak{A} \vDash q$$

- For all sentences p, q

$$\mathfrak{A} \vDash p \vee q \text{ if and only if } \mathfrak{A} \vDash p \text{ or } \mathfrak{A} \vDash q$$

- For all sentences p

$$\mathfrak{A} \vDash p \Rightarrow q \text{ if and only if } \mathfrak{A} \vDash p \text{ implies } \mathfrak{A} \vDash q$$

- For all sentences p

$$\mathfrak{A} \vDash \neg p \text{ if and only if } \mathfrak{A} \nvDash p$$

- For all formulae $p(x)$ with one free variable

$$\mathfrak{A} \vDash \forall x,\, p(x) \text{ if and only if } \mathfrak{A} \vdash p(a) \text{ for all } a \in A$$

- For all formulae $p(x)$ with one free variable

$$\mathfrak{A} \vDash \exists x,\, p(x) \text{ if and only if } \mathfrak{A} \vdash p(a) \text{ for some } a \in A$$

To do: Examples

Definition B.1.8

Let Σ be a signature for first-order logic and let T be a first-order theory over Σ. A **model** of T is a Σ-structure $\mathfrak{A}$ such that $\mathfrak{A} \vDash p$ for all $p \in T$.

B.2   Set theoretic foundations

Zermelo–Fraenkel set theory

To do: Motivation

Axioms B.2.1 (Zermelo–Fraenkel axioms)

The following axioms, taken over the signature with a single relation symbol $\in$ of arity 2, are **Zermelo–Fraenkel axioms** for set theory.

- (**Extensionality**) If two sets have the same elements, then they are equal.

$$\forall X,\ \forall Y,\ [(\forall x,\ (x \in X \Leftrightarrow x \in Y)) \Rightarrow X = Y]$$

  The axiom of extensionality states that equality of sets can be proved by double-containment.

- (**Foundation**) Every set has an element which is $\in$-minimal, in the sense of Definition 5.3.8.

$$\forall X,\ \exists x,\ [x \in X \wedge \forall u \in X,\ u \notin x]$$

  The axiom of foundation states that $\in$ is a well-founded relation.

- (**Empty set**) There is a set with no elements.

$$\exists X,\ \forall x,\ x \notin X$$

  The empty set axiom asserts the existence of $\varnothing$.

- (**Separation**) For any logical formula $p(x)$ with one free variable, and any set X, there is a set consisting of the elements of X satisfying $p(x)$.

$$\forall X,\ \exists U,\ \forall x,\ [x \in U \Leftrightarrow (x \in X \wedge p(x))]$$

  The axiom of separation asserts the existence of sets of the form $\{x \in X \mid p(x)\}$.

- (**Pairing**) For any two sets x and y, there is a set containing only x and y.

$$\forall x,\ \forall y,\ \exists X,\ \forall u,\ [u \in X \Leftrightarrow (u = x \vee u = y)]$$

  The axiom of pairing asserts the existence of sets of the form $\{x, y\}$.

- (**Union**) The union of any family of sets exists and is a set.

$$\forall F,\ \exists U,\ \forall x,\ [x \in U \Leftrightarrow \exists X,\ (x \in X \wedge X \in F)]$$

  The axiom of union asserts that if $F = \{X_i \mid i \in I\}$ is a family of sets then the set $U = \bigcup_{i \in I} X_i$ exists.

- (**Replacement**) The image of any set under any function is a set. That is, for each logical formula $p(x, y)$ with two free variables x, y, we have

$$\forall X, \ [(\forall x \in X, \ \exists! y, \ p(x, y)) \Rightarrow \exists Y, \ \forall y, \ y \in Y \Leftrightarrow \exists x \in X, \ p(x, y)]$$

- (**Power set**) The set of all subsets of a set is a set.

$$\forall X, \ \exists P, \ \forall U, \ [U \in P \Leftrightarrow \forall u, \ (u \in U \Rightarrow u \in X)]$$

  The axiom of power set asserts the existence of $\mathcal{P}(X)$ for all sets X.

- (**Infinity**) There is an inhabited set containing successors[a] of all of its elements.

$$\exists X, \ [(\exists u, \ u \in X) \wedge \forall x, \ (x \in X \Rightarrow x \cup \{x\} \in X)]$$

  Together with the axioms of empty set and replacement, the axiom of infinity implies the existence of the set $\{\varnothing, \varnothing^+, \varnothing^{++}, \varnothing^{+++}, \dots\}$. We will make use of this in Definition B.2.3. Note also that we used the axiom of union in order to state the axiom of infinity.

The logical theory consisting of the Zermelo–Fraenkel axioms is called **Zermelo–Fraenkel set theory**, or simply 'ZF'.

To do: V, apparent circularity.

Axiom B.2.2 (Axiom of choice)
Every family of inhabited sets admits a choice function. That is, for every set I and every family $\{X_i \mid i \in I\}$ of inhabited sets indexed by I, there is a function $f : I \to \bigcup_{i \in I} X_i$ such that $f(i) \in X_i$ for each $i \in I$. Formally,

$$\forall F, \ [\varnothing \notin F \Rightarrow \exists f : F \to U, \ \forall X \in F, \ X \in f(X)]$$

where $U = \bigcup F = \bigcup_{X \in F} X$ is the union of all the sets in the family F.

The logical theory consisting of the ZF axioms (Axioms B.2.1) together with the axiom of choice (Axiom B.2.2) is known as **Zermelo–Frankel set theory with choice**, or simply 'ZFC'.

Constructions of common mathematical objects

To do: Set operations

---

[a]Here, the *successor* of a set x is defined to be $x \cup \{x\}$.

To do: Ordered n-tuples

To do: Functions

To do: Relations

Constructions of the number sets

As we saw in Section 1.3, the Peano axioms 1.3.1 are very powerful, in that from a very basic set of rules we can write down everything we know about the natural numbers; and, moreover, any set $\mathbb{N}$ with an element 0 and a successor operation $(-)^+$ could be treated as a set of natural numbers. But how do we know that such a set, element and operation actually exist? In this section, we construct the *von Neumann natural numbers*—this is an encoding of natural numbers as *sets*, and with the successor operation defined as in Definition B.2.3.

Definition B.2.3

Given a set X, the **successor set** of X is the set X^+ defined by

$$X^+ = X \cup \{X\}$$

A **von Neumann natural number** is any set obtainable from $\varnothing$ by repeatedly taking successor sets. Write $0_{\mathrm{vN}} = \varnothing$ and $(n+1)_{\mathrm{vN}} = (n_{\mathrm{vN}})^+$; that is

$$0_{\mathrm{vN}} = \varnothing, \quad 1_{\mathrm{vN}} = \varnothing^+, \quad 2_{\mathrm{vN}} = \varnothing^{++}, \quad 3_{\mathrm{vN}} = \varnothing^{+++}, \quad 4_{\mathrm{vN}} = \varnothing^{++++}, \quad \ldots$$

Example B.2.4

The first three von Neumann natural numbers are:

- $0_{\mathrm{vN}} = \varnothing$;

- $1_{\mathrm{vN}} = \varnothing^+ = \varnothing \cup \{\varnothing\} = \{\varnothing\}$;

- $2_{\mathrm{vN}} = \varnothing^{++} = \{\varnothing\}^+ = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}$.

$\triangleleft$

Exercise B.2.5

Write out the elements of 3_{vN} $(= \varnothing^{+++})$ and of 4_{vN}. $\triangleleft$

Exercise B.2.6

Recall the definition of von Neumann natural numbers from Definition B.2.3. Prove that $|n_{\mathrm{vN}}| = n$ for all $n \in \mathbb{N}$. $\triangleleft$

Theorem B.2.7
Axioms 1.3.1 are satisfied by letting $\mathbb{N}$ be the set of von Neumann natural numbers, letting the zero element be the empty set, and the successor operation $(-)^+$ be as defined in Definition B.2.3.

Proof. **To do:** □

Example B.2.8
We verify Axiom 1.3.1(c); that is, $n_{\mathrm{vN}}^+ \neq 0_{\mathrm{vN}}$ for all von Neumann natural numbers n_{vN}. This is easy to check—indeed, $n_{\mathrm{vN}} \in n_{\mathrm{vN}}^+$ since $n_{\mathrm{vN}}^+ = n_{\mathrm{vN}} \cup \{n_{\mathrm{vN}}\}$ and $n_{\mathrm{vN}} \in \{n_{\mathrm{vN}}\}$; but $n_{\mathrm{vN}} \notin 0_{\mathrm{vN}}$ since $0_{\mathrm{vN}} = \varnothing$ and $\varnothing$ has no elements. ◁

Since we know by Theorem B.2.7 that the von Neumann natural numbers satisfy the Peano axioms (Axioms 1.3.1), we may declare 'the natural numbers' to be the von Neumann natural numbers, and have done with it. As such, you can—if you want—think of all natural numbers in these notes as being their corresponding von Neumann natural number. From now on, we will only use a subscript 'vN' when it is imperative that a natural number be treated as a von Neumann natural number.

To do: Arithmetic operations, order

To do: Define relation for the integers, prove it's well-defined, provide intuition.

Definition B.2.9
The **set of integers** is the set $\mathbb{Z}$ defined by

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$$

where $\sim$ is the relation on $\mathbb{N} \times \mathbb{N}$ defined by

$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c$$

for all $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$.

To do: Arithmetic operations, order

To do: Define relation for the rationals, prove it's well-defined, provide intuition.

Definition B.2.10

The **set of rational numbers** is the set $\mathbb{Q}$ defined by

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))/\sim$$

where $\sim$ is the relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ defined by

$$(a, b) \sim (c, d) \text{ if and only if } ad = bc$$

for all $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

To do: Arithmetic operations, order

To do: Motivate Dedekind cuts

Definition B.2.11 (Dedekind's construction of the real numbers)

The **set of** (**Dedekind**) **real numbers** is the set $\mathbb{R}$ defined by

$$\mathbb{R} = \{D \subseteq \mathbb{Q} \mid D \text{ is bounded above and downwards-closed}\}$$

To do: Arithmetic operations, order

To do: Motivate Cauchy reals

Definition B.2.12 (Cauchy's construction of the real numbers)

The **set of** (**Cauchy**) **real numbers** is the set $\mathbb{R}$ defined by

$$\mathbb{R} = \{(x_n) \in \mathbb{Q}^{\mathbb{N}} \mid (x_n) \text{ is Cauchy}\}/\sim$$

where $\sim$ is the relation defined by

$$(x_n) \sim (y_n) \text{ if and only if } (x_n - y_n) \to 0$$

for all Cauchy sequences $(x_n), (y_n)$ of rational numbers.

To do: Arithmetic operations, order

To do: Motivate definition of complex numbers

Definition B.2.13

The **set of complex numbers** is the set $\mathbb{C} = \mathbb{R} \times \mathbb{R}$.

To do: Arithmetic operations

B.3 Other foundational matters

Appendix C

Typesetting mathematics in LaTeX

Being able to type up your mathematical writing is a beneficial skill to have; unfortunately, most Office-style WYSIWYG ('what you see is what you get') text editors are not designed for this task—they just can't cope with all the notation.

LaTeX[a] is a markup language that allows you to input both text and mathematical notation, the latter in the form of code, which is then beautifully typeset. What follows is a brisk intro to LaTeX, that should suffice for the purposes of this course.

Finding the software

There are several good LaTeX editors that you can install on your computer—I recommend Texmaker (`http://www.xm1math.net/texmaker/`) if you're new to it, because it's cross-platform and fairly intuitive.

There are also online editors that you can use if you want to avoid installing new software; I highly recommend ShareLaTeX (`http://www.sharelatex.com`), which is free to use and stores your `.tex` files on the cloud.

There is some faffing around to be done with document headers and so on. So that you can avoid this, I've uploaded template `.tex` files to Blackboard that you can use in your homework write-ups.

---

[a]The word LaTeX is pronounced like 'lay-tek' or 'lah-tek'; some people pronounce the 'k' like the German 'ch' sound, meant to resemble the Greek letter chi (χ). It doesn't really matter, but if you pronounce it like 'lay-teks' then people will think you're talking about something somewhat different.

Text mode and math mode

Before we get into the nitty-gritty, I should mention the difference between 'text mode' and 'math mode'.

- **Text mode** is the default mode: the stuff you type will appear as text, and this is the mode you should use when writing anything that isn't mathematical notation.

- You should use **math mode** when you're typing anything which is mathematical notation, including variables, numbers, fractions, square roots, powers, sums, products, binomial coefficients, and so on.

To enter math mode, enclose whatever mathematical notation you are writing with dollar signs (`$`). For example, if I type `$E=mc^2$` then LaTeX shows $E = mc^2$. Sometimes it is convenient to put longer expressions on their own line, in which case you can enclose it with double-dollar signs (`$$`); for example, if I type `$$a^2+b^2+c^2=ab+bc+ca$$` then LaTeX displays

$$a^2 + b^2 + c^2 = ab + bc + ca$$

on a line all of its own.

If you need to type text inside math mode (enclosed by `$` signs), you can do that using `\text{...}`, for example the code

```
$$\sum_{i=1}^n i = \frac{n(n+1)}{2} \text{ for all } n \in \mathbb{N}$$
```

gives

$$\sum_{i=1}^n i = \frac{n(n+1)}{2} \text{ for all } n \in \mathbb{N}$$

Note the spaces before and after 'for all'; had I left those out of the code, they would not appear because LaTeX ignores spacing in math mode. You can force a space by putting a backslash before a space, for example `$a b$` gives ab but `$a\ b$` gives $a\ b$.

All mathematical notation should be in math mode, including single variables. Notice the difference between the following two lines:

<div align="center">If a and b are both even then so is a+b.</div>

<div align="center">If a and b are both even then so is $a + b$.</div>

While the first is written entirely in text mode, the second is written using math mode for the variables and $+$ sign.

Mathematical symbols

The following table lists—I hope—all of the mathematical symbols you will need in this course. If you come across other symbols, please let me know.

Logic		
conjunction, disjunction	$\wedge, \vee$	`\wedge, \vee`
negation	$\neg$	`\neg`
implication, biconditional	$\Rightarrow, \Leftrightarrow$	`\Rightarrow, \Leftrightarrow`
exclusive disjunction	$\oplus$	`\oplus`
true, false (in truth table)	$\checkmark, \times$	`\checkmark, \times`
quantifiers (universal, existential)	$\forall, \exists$	`\forall, \exists`
Set theory		
element, subset	$\in, \subseteq$	`\in, \subseteq`
not equal, proper subset	$\ne, \subsetneqq$	`\ne, \subsetneqq`
intersection, (indexed)	$\cap, \bigcap_{i=1}^{n}$	`\cap, \bigcap_{i=1}^{n}`
union, (indexed)	$\cup, \bigcup_{i=1}^{n}$	`\cup, \bigcup_{i=1}^{n}`
relative complement, complement	$X \setminus Y, X^c$	`\setminus, X^c`
product, (indexed)	$\times, \prod_{i=1}^{n}$	`\times, \prod_{i=1}^{n}`
implied lists	$\{1, \dots, n\}$	`\{ 1, \dots, n \}`
indexed sets	$\{x_i \mid i \in I\}$	`\{ x_i \mid i \in I \}`
set-builder notation	$\{x \mid p(x)\}$	`\{ x \mid p(x) \}`
empty, universal set	$\varnothing, \mathcal{U}$	`\varnothing, \mathcal{U}`
number sets	$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$	`\mathbb{N}, \mathbb{Z}`, etc.
Numbers and combinatorics		
multiplication	$m \times n, m \cdot n$	`\times, \cdot`
fractions, exponents	$\frac{m}{n}, m^n$	`\frac{m}{n}, m^{n}`
order relations	$\leqslant, \geqslant$	`\le, \ge`
divisibility, (non-)	$m \mid n, m \nmid n$	`\mid, \nmid`
binomial coefficient	$\binom{n}{k}$	`\binom{n}{k}`
indexed sum, product	$\sum_{i=1}^{n} a_i, \prod_{i=1}^{n} a_i$	`\sum_{i=1}^{n} a_i, \prod`
modular arithmetic	$a \equiv b \bmod n$	`a \equiv b \bmod{n}`
Functions and relations		
functions	$f : X \to Y$	`f : X \to Y`
composition	$g \circ f$	`\circ`
isomorphism	$\cong$	`\cong`
equivalence relations	$\sim, \approx$	`\sim, \approx`
Structured sets		
order relation	$\preccurlyeq, \prec$	`\preceq, \prec`
group operations	$\cdot, \star, \circ$	`\cdot, \star, \circ`

Organisation and formatting

When typing up solutions to problem, organisation can be the difference between a masterpiece and an unreadable heap of notation. Here are some tips to help you organise your work:

Sections and paragraphs

You can split your work up into sections, subsections, subsubsections, and even subsubsubsections. To do this, use `\section{Section title}` or `\section*{Section title}`; the former includes a section number, and the latter omits it. To start a new paragraph, simply make two new lines in the code.

Bulleted and enumerated lists

Sometimes it is useful to use bullet points or give an enumerated list. For example, in these notes, I separate the base case from the induction step in proofs by induction by using bullet points.

For a bulleted list you can use the `itemize` environment:

```
\begin{itemize}
\item Something here\dots
\item You can do lists within lists:
  \begin{itemize}
  \item Like this.
  \item Isn't it crazy!
  \end{itemize}
\item Well, not that crazy.
\end{itemize}
```

- Something here...

- You can do lists within lists:

    ⋄ Like this.

    ⋄ Isn't it crazy!

- Well, not that crazy.

For an enumerated list, you can use the `enumerate` environment. You can play around with different methods of enumeration, which you specify in square brackets `[...]`; personally I like `(1)`, `(i)` and `(a)` the best:

```
\begin{enumerate}[(a)]
\item Here's the first thing;
\item Here's the second thing;
\item And here's the third thing.
\end{enumerate}
```

(a) Here's the first thing;

(b) Here's the second thing;

(c) And here's the third thing.

Definitions, results and proofs

If you use the provided templates, you can make definitions, and state and prove results, using the following environments:

`definition`, `example`, `proposition`, `theorem`, `lemma`, `corollary`, `proof`

They are given a number **m.n**, where m is the section number and n is the position within the section.

Here's an example of a theorem appearing in the third section of a document, in which five definitions, results or examples come before it:

```
\begin{theorem}
If $n \in \mathbb{N}$ then $n \ge 0$.
\end{theorem}

\begin{proof}
This is really obvious.
\end{proof}
```

Theorem 3.6. If $n \in \mathbb{N}$ then $n \geqslant 0$.

Proof. This is really obvious.   □

Note that the box (□) designating the end of the proof is inserted automatically when you close the `proof` environment.

Labels

As you change the contents of a document, the numbering of the definitions, examples and results might change. To refer to a specific result, instead of typing the number and having to change it each time the number changes, you can use the `\label` and `\ref` commands.

An example of this in action is as follows:

383

```
\begin{definition}
\label{defDivides}
Say $a$ \textbf{divides} $b$ if there
exists $k \in \mathbb{Z}$ such that
$ka=b$.
\end{definition}

We will use Definition
\ref{defDivides} for absolutely
nothing.
```

Definition 2.11. Say a **divides** b if there exists $k \in \mathbb{Z}$ such that $ka = b$.

We will use Definition 2.11 for absolutely nothing.

Formatting

In text mode. To put the icing on the cake, you might want to make some words **bold** or *italicised*. This is simple: for bold text type `\textbf{text here}` and for italic text type `\textit{text here}`. In Texmaker and ShareLaTeX you can press `Ctrl+B` and `Ctrl+I` to avoid having to type all this out. Other useful fonts include `monospace` (`\texttt{text here}`), sans-serif (`\textsf{text here}`) and underlined (`\underline{text here}`).

In math mode. There are also various fonts or font styles that you can use inside math mode, including:

- Roman (i.e. not italic): AaBbCc, `\mathrm{AaBbCc}`;

- Bold: **AaBbCc**, `\mathbf{AaBbCc}`;

- Sans-serif: AaBbCc, `\mathsf{AaBbCc}`;

- Blackboard bold: $\mathbb{ABCDE}$, `\mathbb{ABCDE}` — only capital letters;

- Fraktur: $\mathfrak{AaBbCc}$, `\mathfrak{AaBbCc}`;

- Calligraphic: $\mathcal{ABCDE}$, `\mathcal{ABCDE}` — only capital letters;

Tables

Tables can be created using the `tabular` environment. You can specify how columns are aligned and separated as an argument to the command `\begin{tabular}`: write `l`, `c` or `r` to specify that a column should be aligned left, centre or right, respectively. If you want columns to be separated by a single or double line, enter a single or double bar (`|` or `||`), respectively.

Columns are then separated by ampersands (`&`) and you can move to a new row by entering a double-backslash (`\\`). To insert a horizontal line between two rows, simply enter `\hline`.

Here's an example:

```
\begin{tabular}{c||ccc}
$\times$ & 1 & 2 & 3 \\ \hline \hline
1 & 1 & 2 & 3 \\
2 & 2 & 4 & 6 \\
3 & 3 & 6 & 9 \\
\end{tabular}
```

$\times$	1	2	3
1	1	2	3
2	2	4	6
3	3	6	9

Aligned equations

Occasionally a proof may require you to demonstrate that two terms are equal by proving a sequence of intermediate equations. This can be done using the `align*` environment, which behaves much like the `tabular` environment.

New lines are introduced by inserting a double-backslash (`\\`), and the two columns are separated by an ampersand (`&`). The left column is aligned right, and the right column is aligned left. Here's an example:

```
\begin{align*}
(n+1)!  - n!  & = (n+1)n!  - n!  \\
& = n \cdot n!  + n!  - n!  \\
& = n \cdot n!
\end{align*}
```

$$
\begin{aligned}
(n+1)! - n! &= (n+1)n! - n! \\
&= n \cdot n! + n! - n! \\
&= n \cdot n!
\end{aligned}
$$

Note that the `align*` environment automatically enters into math mode, so to enter text you should use the `\text` command.

Entering more ampersands will create more columns, whose alignment alternates (right, left, right, left, and so on). For example, to add annotations to each line, you can enter a double-ampersand (`&&`). For example, the following code. . .

```
\begin{align*}
(n+1)! - n! & = (n+1)n! - n! && \text{by recursive def of factorials}
\\
 & = n \cdot n! + n! - n! && \text{by distributivity} \\
```

```
 & = n \cdot n! && \text{by cancellation}
\end{align*}
```

. . . yields the following output:

$$(n + 1)! - n! = (n + 1)n! - n! \qquad \text{by recursive def of factorials}$$
$$= n \cdot n! + n! - n! \qquad \text{by distributivity}$$
$$= n \cdot n! \qquad \text{by cancellation}$$

Note again that, because the `align*` environment automatically enters math mode, any annotations must be made within the `\text` command.

Graphics

To insert graphics into your documents, you need to make sure that the code `\usepackage{graphicx}` is somewhere in the document header, i.e. above the line that says `\begin{document}`.

Images can then be inserted using the `\includegraphics` command. The format is

`\includegraphics[parameters]{filename}`

where, in the above, `parameters` denotes information telling LATEX how large you want the image to be, and `filename` is the name of the image file, which. . .

- . . . excludes the extension, for example '`donkey`' instead of '`donkey.png`';

- . . . includes the path relative to the main .tex file, for example if *donkey.png* is stored in a directory called *images*, you would enter '`images/donkey`' instead of '`donkey`'.

The simplest way to control the size of the image is to enter `[width=k\textwidth]`, where `k` is a scaling factor between 0 and 1.

For example, the following code:

```
\begin{center}
\includegraphics[width=0.3\textwidth]{donkey}
\end{center}
```

yields the following output:

More advanced techniques

I should take a moment to emphasise that what really matters is your ability to communicate mathematical arguments clearly and correctly. The LaTeX tools discussed so far in this section are more than sufficient for our purposes.

However, if you are interested in pushing your LaTeX skills further or there is a feature you're unsure about how to implement, then I recommend browsing or searching one of the following websites:

- `http://tex.stackexchange.com` — Q&A website about LaTeX

- `https://en.wikibooks.org/wiki/LaTeX` — online LaTeX manual

Practice page

Use the provided LaTeX template `template.tex` to re-create the following page:

Squarefree integers
Carl Friedrich Gauss, Wednesday 14th September 1831

Introduction

When you've written this page, you will be unstoppable, at least as far as typesetting mathematics is concerned. You will need to implement:

- Text mode stuff: sections, paragraphs, text formatting, labels and references, lists;
- Math mode stuff: definitions and results, aligned equations, etc.

So let's get on with it!

1   Squarefree integers

1.1   Definition and an elementary result

Definition 1.1. An integer a is **squarefree** if it is divisible by no perfect square other than 1. That is, if n^2 divides a then $n^2 = 1$.

Proposition 1.2. A non-zero non-unit a is squarefree if and only if

$$a = p_1 \times p_2 \times \cdots \times p_n$$

for distinct primes $p_1, p_2, \ldots, p_n$.

Proof. We leave the proof as an exercise to the reader.   □

1.2   Some examples

Example 1.3. Some concrete examples include:

(i) 5610 is squarefree by Proposition 1.2, since

$$\begin{aligned}
5610 &= 10 \times 561 \\
&= (2 \times 5) \times (11 \times 17)
\end{aligned}$$

(ii) 12 is not squarefree since $4 \mid 12$ and $4 = 2^2$.

1

Index

Index of notation