PLP

An introduction to mathematical proof

Seçkin Demirbaş
University of British Columbia

Andrew Rechnitzer
University of British Columbia

Exercises for PLP

Hannah Kohut
University of British Columbia

Charlotte Trainor
University of British Columbia

August 15, 2023

Acknowledgements

A great many of the exercises in this text come from test and exam problems in first year courses at UBC Mathematics over the last couple of decades. The authors would like to acknowledge the contributions of the many people who collaborated to produce these. A very big thanks must go to Hannah Kohut and Charlotte Trainor who wrote the vast majority of the statements, hints and solutions for the exercises in the text; this book would not have been possible without their efforts. Their work was funded by UBC's Open Educational Resources Fund, and by the UBC Mathematics Department.

The authors would also like to acknowledge that the land UBC Vancouver Campus is on is the traditional, ancestral, and unceded territory of the xʷməθkʷəy̓əm (Musqueam) People. Learn more about UBC's relationship with the Musqueam Nation[3].

[3] aboriginal.ubc.ca/community-youth/musqueam-and-ubc/

Preface

The main idea of this text is to teach you how to write correct and *clear* mathematical proofs. In order to learn to prove things we will study some basic analysis. We will prove many things about the basic properties of numbers sets and functions — like

> There are more real numbers than integers.

In order to make sense of this statement we need to understand how to extend the idea of “more” from the context of finite quantities, where we are used to “more” and “less”, to the domain of infinite quantities. We’ll have to define ideas about sets and functions, manipulate and combine them with logic. Along the way we will need to think hard about how to communicate the mathematics that we are doing, so that you, and others, can follow what we are doing.

Hence, a critical part of this subject is to learn to communicate mathematics — not just do mathematics. Mathematics is not simply number crunching or using formulas — this is using mathematics. Mathematics is also about understanding and reasoning and most importantly *proving* things. Neither of these aspects is more important than the other. Up until now you have mostly done the former, and the aim of this text is to help you get better at the latter.

It is crucial that we are able to explain to others why what we know is true is actually true — this is what proofs are for. Think of the proof as a dialog between you and the reader — you have to make every (reasonable) effort to be clear, precise and accurate. Always think of the reader when you are writing. It is important to argue and write well — it is a useful skill both at university and beyond in the so-called “real world”.

The authors have spend a lot of time reading other people’s work (mostly student work, but also articles written by professional mathematicians with years of experience) and puzzling over the lines written on the page — sometimes legible, sometimes not (especially in exams). And finally after sweating for ages you realise what they were trying to say. In some circumstances one can, of course, contact the writer and ask them “What did you mean?” However, this is frequently not the case — all one has is what is written on the page.

> So that’s what he meant! Then why didn’t he say so?
>
> —Frank Harary

When you do mathematics (and other activities) there is a huge difference between reading and doing. This is especially the case with proofs. So while reading the text is a good way to learn some ideas and get a feeling for some of the stuff, it is really no substitute for *doing* the exercises. That is where you will really learn.

> I write to discover what I know
>
> —Flannery O'Connor

Behind every proof you read (and you write) lies a good bit of work. You cannot generally look at a problem and write out the proof all fine first go. You need to do some rough work to map out the structure of the proof and the details. Then *after* this you write out the proof nicely and neatly. Making sure that you present you work well forces you to think about what you are writing down. The investment in your hard work writing, pays off for the people reading your work.

> Easy reading is damned hard writing.
>
> —Nathaniel Hawthorne

Learning to write proofs takes time and effort. But the rewards are well worth it.

Seçkin Demirbaş and Andrew Rechnitzer

Contents

Chapter 1

Sets

All subjects have to start from somewhere, and we'll start our work at sets. The authors believe that you, the reader, will have all seen some basic bits of set-theory before you got to this text. We hope we can safely assume[4] that you have at least some passing familiarity with sets, intersections, unions, Venn diagrams (those famous overlapping circle pictures), and so forth. Based on this assumption, we will move quite quickly through an introduction to this topic and do our best to get you to new material. We really want to get you proving things as quickly as possible.

Set theory now appears so thoroughly throughout mathematics that it is difficult to imagine how Mathematics could have existed without it. It might be surprising to note that set theory is a much newer part of mathematics than calculus. Set theory (as its own subject) was really only invented in the 19th Century — primarily by Georg Cantor[5] Really mathematicians were using sets well before then, just without defining things quite so formally.

Since it (and logic) will form the underpinning of all the structures we will discuss in this text it is important that we start with some definitions. We should try to make them as firm and formal as we can.

1.1 Not so formal definition

In mathematics and elsewhere[6] we are used to dealing with collections of things. For example

- a family is a collection of relatives.
- hockey team is a collection of hockey players.

[4]Assumptions can be dangerous, and in general we will avoid them, or at least do our best to be honest with the reader that we are making an assumption.

[5]A mathematician we will discuss in much more detail in footnotes much like this much later in the text when we get to the topic of Cardinality in Chapter Chapter 12. We will also try to reduce the overuse of the word "much" as much as possible.

[6]Including the so-called "real life" that non-mathematicians inhabit.

- shopping list is a collection of items we need to buy.

Let us give our first definition for the course. Now this one is not so formal — but it will be enough for our purposes[7].

Definition 1.1.1 (A not so formal definition of sets). A **set** is a collection of objects. The objects are referred to as **elements** or **members** of the set. $\Diamond$

One reason to be not-so-formal here, is that while the notion of a set is relatively simple and intuitive, it turns out that making the definition completely rigorous is quite difficult. The interested reader should search-engine their way to discussions of this point.

Now — let's just take a few moments to describe some conventions. There are many of these in mathematics. These are not firm mathematical rules, but rather they are much like traditions. It makes it much easier for people reading your work to understand what you are trying to say.

- Use capital letters to denote sets, A, B, C, X, Y etc.
- Use lower case letters to denote elements of the sets a, b, c, x, y.

So when you are writing a proof or just describing what you are doing then if you stick with these conventions people reading your work (including the person marking your exams) will know — "Oh A is that set they are talking about" and "a is an element of that set.". On the other hand, if you use any old letter or symbol might be correct, but it can be unnecessarily confusing for the reader[8]. Think of it as being a bit like spelling — if you don't spell words correctly people can usually understand what you mean, but it is much easier if you spell words the same way as everyone else[9].

We will encounter more of these conventions as we go — another good one is

- The letters i, j, k, l, m, n usually denote integers.
- The letters x, y, z, w usually denote real numbers.

So — what can we do with a set? There is only thing we can ask of a set:

"Is this object in the set"

and the set will answer

"yes"

---

[7]Unfortunately the formal theory of sets gets very difficult very quickly and is well beyond the scope of this text. So rather than investing a large amount of time on the precise definition of **set**, we will make do with this one. It is better for us to just get on with learning how to give precise definitions of particular sets and how to work with them.

[8]While obfuscation can be useful in many endeavours, the authors do not know of any good reason to deliberately obfuscate your mathematics.

[9]Okay, maybe Noah Webster had some not completely unreasonable reasons for tweaking English spelling, but this author is not entirely convinced that quite so many z's are needed.

or

"no"

and nothing else. If you want to know more than just "yes" or "no", then you need to use with more complicated mathematical structures (we'll touch on some as we go along).

For example, if A is the set of even numbers we can ask "Is 4 in A" we get back the answer "yes". We write this as

$$4 \in A$$

While if we ask "Is 3 in A?" and we get back the answer "no". Mathematically we would write this as

$$3 \notin A$$

So this symbol "$\in$" is mathematical shorthand for "is an element of", while the same symbol with a stroke through it "$\notin$" is shorthand for "is not an element of". Similar "put a stroke through the symbol to indicate negation"-notation gets used a lot in different contexts and we'll see it throughout this text. While it is arguably not terribly creative, it is effective — perhaps because it isn't too creative.

This is standard notation — it is very important that you learn it and use it. Do not confuse the reader, or the person who marks your tests and exams, by using some variation of this. For instance, some of you may have previously used ε in place of $\in$ — please stop doing so. For most mathematicians, "$4\varepsilon A$" denotes the product of three things, while "$4 \in A$" is a mathematical sentence that tells us that the object "4" is a member of the set A.

1.1.1 Who is this reader you keep on mentioning?

We have referred to a "reader" several times in the text above but not really explained who we mean by "the reader". There are 3 different types of reader that we mean when we say "think about the reader": you, another person, and not-a-real-reader.

- You: Frequently, the only person who will read your mathematics is you. Your lecture notes, your homework drafts, your experimenting, etc — you typically don't show them to other people. For that sort of work ***in isolation*** it doesn't really matter too much if you don't use standard notation, take shortcuts, and a myriad of other things that people typically do to save time. However, if we only think of ourselves when we write then we can form many bad habits that we take with us when we write for other people. These shortcuts can be hard for other people to understand unless we take the time to explain them. Consequently, it is a good idea to avoid these habits even when writing for ourselves; your reader, and even your future self, will thank you.

- Another person: On many occasions another person will read your work — the most obvious being the person who marks your homework, tests and exams. Generally you will not be present while they read (and perhaps grade) your mathematics, so typically they will only be able to mark what you have written on the page; they cannot mark ***what you mean*** by what is on the page. So you need to make sure things are as clear as possible, so that what you have written conveys what you mean. If you are in the habit of using your own shorthand or definitions or notation, then you must make sure these are clearly explained.

- Not-a-real-reader: Finally, we should often think of a reader who isn't really a reader at all, but really just a mechanism we should use to decide if what we are writing is good enough. Our imaginary reader is intelligent, sensible, knows some mathematics (but not everything), and is a bit of an annoying pedant[10]. As we write we should think of this imaginary reader looking over our shoulder asking questions like "Is that the right notation?", "Is that clear enough?", "Does the logic flow in the right direction?" and offering advice like "Add another sentence to the explanation." and "Make sure you define that function."

As we continue along in this text we will keep referring to these readers and reminding you to think of them as you write. Communicating mathematics is a very important part of doing mathematics.

1.2 Describing a set

We really need to be able to describe and define lots of different sets when we are doing mathematics. It must be completely clear from the definition how to answer the question "Is this object in the set or not?"

- "Let A be the set of even integers between 1 and 13." — nice and clear.

- "Let B be the set of tall people in this class room." — not clear.

More generally if there are only a small number of elements in the set we just list them all out

- "Let $C = \{1, 2, 3\}$."

When we write out the list we put the elements inside braces $\{\cdot\}$. Do not use round, square or angle brackets — those things have other mathematical meanings — we must use braces or "curly brackets" if you like. Not that the order we write things in doesn't matter

$$C = \{1, 2, 3\} = \{2, 1, 3\} = \{3, 2, 1\}$$

[10]Is there any other sort of pedant?

because the only thing we can ask is "Is this object an element of C?" We cannot ask more complex questions like "what is the third element of C" — we require more sophisticated mathematical objects to ask such questions and we'll might get around to looking at such things later in the course.

Similarly, it doesn't matter how many times we write the same object in the list

$$C = \{1, 1, 1, 2, 3, 3, 3, 3, 1, 2, 1, 2, 1, 3\} = \{1, 2, 3\}$$

because all we ask is "Is $1 \in C$?". Not "how many times is 1 in C?" (you need a mathematical construction called a multiset to ask and answer this question).

Now — if the set is a bit bigger then we might write do something like this

- $C = \{1, 2, 3, \ldots, 40\}$ the set of all integers between 1 and 40 (inclusive).
- $A = \{1, 4, 9, 16, \ldots\}$ the set of all positive square integers

The "..." (ellipsis) is shorthand for the missing entries and tells us to follow the pattern as long as we can. You must be careful with this as you can easily confuse the reader if the pattern is not clear. That, in turn, that means that your set is not defined sufficiently precisely.

- $B = \{3, 5, 7, \ldots\}$ — is this all odd primes, or all odd numbers bigger than 1 or prime numbers that differ from a power of 2 by exactly 1?

Only use this where it is completely clear by context. A few extra words can save the reader (and yourself) a lot of confusion.

This is perhaps the most important set — many other important objects in mathematics can be built up from this.

Definition 1.2.1 Empty set. The **empty set** (or null set or void set) is the set which contains no elements. It is denoted $\varnothing$. For any object x, we always have $x \notin \varnothing$; hence $\varnothing = \{\}$. ♢

Notice that the empty set is not nothing — you should think of it as an empty bag. Be careful not to confuse it with the empty in the empty bag[11].

Example 1.2.2

- $A = \{1, 2, \varnothing\}$ — this set contains three elements; the numbers one and two and the empty set. A set can contain sets.
- $B = \{\varnothing\}$ — this set is not the empty set — it contains a single element, being the empty set. You can think of this set as being a bag that contains an empty bag.
- $C = \{\varnothing, \{\varnothing\}\}$ — this set contains two elements; the empty set and the set

[11] This potential confusion is akin to that caused by the number zero. How can something, that is "0", denote nothing? We recommend taking a little digression into this topic (with digressions into Parmenides, Leucippus, Democritus, Zeno, horror vacui, and many other topics) with your favourite search engine.

that contains the empty set (our set B above).

$\square$

Now — this is all fine when the set doesn't contain too many elements. But for infinite sets or even just big sets we can't do this and instead we have to give the defining rule. For example the set of all positive even numbers we write as

$$S = \{x \mid x \text{ is even and positive}\} = \{2, 4, 6, 8 \ldots\}$$

The second notation is also okay, but you have to be careful to make sure it is completely clear which set you are talking about. The first notation can be read as "S is the set of elements x such that x is even and positive". This is the standard way of writing a set defined by a rule. This sort of notation is sometimes called ***set-builder notation***.

$$\begin{aligned} S &= \{\text{some expression} \mid \text{some rule}\} && \text{or} \\ &= \{\text{a function} \mid \text{a domain}\} \end{aligned}$$

The set of all primes is

$$S = \{p : p \text{ is prime}\}$$

the ":" is read as "such that" or "so that", and you will also often see

$$S = \{p \text{ s.t. } p \text{ is prime}\} = \{p \mid p \text{ is prime}\}$$

This author prefers " | " since it provides a clear (even physical) demarcation. You should recognise all three notations.

While set-builder notation avoids many problems of clarity, it does not avoid all problems. A very famous example is

$$S = \{A \mid A \notin A\}$$

ie. the set of all sets that do not contain themselves. This is a problem, because if $S \in S$, then according to the defining rule, it cannot be. On the other hand, if $S \notin S$ then it must be. Hence the rule is ambiguous. This is Russell's paradox. It is closely related to the sentence

This sentence is false.

One way around these problems is to avoid talking about self-referential objects — but this is way too heavy for the moment, and we should just get back to easier sets[12].

The empty set is one important set, here are a few more. What follows is not really a formal definition of these sets, rather it is here to remind the reader of some sets that they should already know and to highlight some standard notation that people use to refer to them.

[12]The book "Gödel, Escher, Bach: An Eternal Golden Braid" by Douglas Hofstadter is a wonderful exploration of topics related to Russell's paradox and much much more.

Definition 1.2.3 Some other important sets.

- Positive integers $\mathbb{N} = \{1, 2, 3, \dots\}$ — these are usually called the **natural numbers**.
- All **integers** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- All **rational numbers** (fractions) $\mathbb{Q} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N} \right\}$
- All **real numbers** $\mathbb{R}$
- **Irrational numbers** $\mathbb{I}$ = real numbers that are not rational. Examples of this are $\sqrt{2}, \sqrt{3}, \pi, e$. Hence $\sqrt{2} \in \mathbb{R}$ and $\sqrt{2} \notin \mathbb{Q}$, so $\sqrt{2} \in \mathbb{I}$ (we'll get around to proving this later in the text).

$\diamondsuit$

Here are some points to note about the above definition.

- Unfortunately there is often confusion as to whether or not zero should be included in the set of "natural numbers". This text will not include zero as is, in the experience of the authors at least, the more common mathematical convention. If you work in formal logic, set theory or computer science, then often zero is included in the set. The number zero has an interesting history in mathematics and the reader should search-engine their way to articles on that history. Often its use in mathematics was complicated by the question "how can nothing be something?"
- We can also define the set of rational numbers as $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$. The authors prefer the one given in the definition; it feels a little "cleaner" in that we represent a third as $\frac{1}{3}$ rather than $\frac{-1}{-3}$. Of course, we can also represent $\frac{1}{3} = \frac{2}{6}$. We discuss this more in Example 9.2.7.
- We must use "blackboard bold" to denote these sets.

$$\mathbb{N} \neq N, \qquad \mathbb{R} \neq R.$$

  Notice here, these are not written in a normal bold font, but rather they are written in "blackboard bold" so that certain lines, usually the vertical ones, are doubled. This style of writing came from the need to distinguish between regular and bold face letters when writing on blackboards (as mathematicians are want to do). It eventually became standard notation both on boards and in print. Since it is now quite standard notation, please learn it and use it. Do not confuse the reader.
- Also note that $\mathbb{I}$ is not a very standard notation (though we might use it from time to time in this text) — the others are standard. This is in part because the set of irrational numbers has some pretty ugly properties — it is not closed under addition or multiplication; you can take two irrational numbers and add them to get a rational number; you can take two irrational

numbers and multiply them to get a rational number. The other sets are closed under addition and multiplication.

So now using these as standard sets we can start to build more interesting things

- Even integers

$$\begin{aligned} E &= \{n \mid n \text{ is an even integer}\} \\ &= \{n \mid n = 2k \text{ for some } k \in \mathbb{Z}\} \\ &= \{2n \mid n \in \mathbb{Z}\} \end{aligned}$$

- Square integers $S = \{n^2 \mid n \in \mathbb{Z}\}$.

One obvious question that one can ask about a set is "How many elements are there in it?" — there is quite a bit more to this question than you might think.

Definition 1.2.4 For a set S we write $|S|$ to denote the **cardinality** of S or its **cardinal number**. For finite sets, $|S|$ is just the the number of elements in S. We extend this concept to infinite sets in Chapter 12. ◊

Hence $|\varnothing| = 0$, and $|\{1, 2, \{\varnothing\}\}| = 3$. For (small) finite sets we can just list things out, but for larger sets it gets very difficult very quickly, and for infinite sets things become very weird. One thing we will study in this course is the size of sets — in particular we show that

- $|\mathbb{N}| = |\mathbb{Z}|$
- $|E| = |\mathbb{Z}|$
- $|\mathbb{Z}| = |\mathbb{Q}|$
- $|\mathbb{Z}| < |\mathbb{R}|$

These statements are really very strange and we need to build up some mathematical infrastructure to make sense of them. Notice that the first and second statement tell us that there are two infinite sets (positive integers and all integers), where one is a strict subset of the other, but they are actually the same size! The last statement is even stranger — it tells us that there are two infinite sets (integers and reals) that are definitely not the same size. This implies that there is more than one sort of infinity. Before we are done we will actually prove that there are an infinite number of different infinities!

1.3 Onward

Of course there is much more to be done with sets, however we'd really like to get into logic and proving things as quickly as possible. So we'll stop our discussion of sets for now and come back later armed with more logic and some proof ideas.

1.4 Exercises

1. Write the following sets by listing their elements.

(a) $A_1 = \{x \in \mathbb{N} \text{ s.t. } x^2 < 2\}$.

(b) $A_2 = \{x \in \mathbb{Z} \text{ s.t. } x^2 < 2\}$.

(c) $A_3 = \left\{x \in \mathbb{N} \text{ s.t. } x = 3k = \frac{216}{m} \text{ for some } k, m \in \mathbb{N}\right\}$.

(d) $A_4 = \left\{x \in \mathbb{Z} \text{ s.t. } \dfrac{x+2}{5} \in \mathbb{Z}\right\}$.

(e) $A_5 = \{a \in B \text{ s.t. } 6 \le 4a + 1 < 17\}$, where $B = \{1, 2, 3, 4, 5, 6\}$.

(f) $A_6 = \{x \in B \text{ s.t. } 50 < xd < 100 \text{ for some } d \in D\}$, where $B = \{2, 3, 5, 7, 11, 13, \ldots\}$ is the set of primes and $D = \{5, 10\}$.

(g) $A_7 = \{n \in \mathbb{Z} \text{ s.t. } n^2 - 5n - 16 \le n\}$.

2. We are going to write the following sets in set builder notation.

(a) $A = \{5, 10, 15, 20, 25, \ldots\}$.

(b) $B = \{10, 11, 12, 13, \ldots, 98, 99, 100\}$.

(c) $C = \{0, 3, 8, 15, 24, 35, ..\}$.

(d) $D = \left\{\ldots, -\frac{3}{10}, -\frac{2}{5}, -\frac{1}{2}, 0, \frac{1}{2}, \frac{2}{5}, \frac{3}{10}, \frac{4}{17}, \ldots\right\}$.

(e) $E = \{2, 4, 16, 256, 65536, 4294967296, \ldots\}$.

(f) $F = \{2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, 36, \ldots\}$.

3. In each of the following parts, a set is defined in one of three ways: (1) listing elements between braces, (2) using set builder notation, or (3) describing in words. Rewrite each set in the two forms of which it is not already given. For example, since the set in part (a) is given by method (1), write the same set using methods (2) and (3). As another example, since the set in part (c) is given by method (2), write the same set using methods (1) and (3).

(a) $A = \{0, 2, 4, 6, \ldots, 100\}$

(b) $B = \{3, 9, 27, 81, \ldots\}$

(c) $C = \{m \text{ s.t. } m \in \mathbb{Z},\ |m| \le 3\}$

(d) $D = \{4k + 1 \text{ s.t. } k \in \mathbb{Z}\}$

(e) The set E of all numbers that are the reciprocal of a natural number.

(f) The set F of all integers that are two more than a (possibly negative) multiple of 5.

4. Consider the following ill-defined set: $S = \{2, 4, \dots\}$. Show that the definition of S is ambiguous by providing two different ways that you could interpret its definition.

5. Consider the set

$$\{2n + 1 : n \in \mathbb{N}\}.$$

Explain what is wrong with each of the expressions below and why they should not be used to denote this set.

(a) $A = \{2k + 1\}$

(b) $B = \{2j + 1 : j \in N\}$.

(c) $c = \{2\ell + 1 : \ell \in \mathbb{N}\}$

(d) $D = \{2k + 1 : n \in \mathbb{N}\}$

(e) $E = \{2m + 1 : m \epsilon \mathbb{N}\}$

(f) $F = \{2N + 1 : N \in \mathbb{N}\}$

(g) $G = \{2m + 1 : m \varepsilon \mathbb{N}\}$

(h) H = {2n+1 : n in N}

6. Are the following statements true or false?

(a) $\varnothing = \{0\}$

(b) $\varnothing = \{\varnothing\}$

(c) $|\varnothing| = 0$

(d) $\{\{\varnothing\}\} = \{\varnothing\}$

(e) $\{\varnothing\} = \{\{\}\}$

7. Show that each of the numbers

$$a = 2, \qquad b = 8, \qquad \text{and} \qquad c = -12$$

do not belong to any of the following sets:

$$A = \left\{-\frac{1}{n} \text{ s.t. } n \in \mathbb{N}\right\} \qquad B = \left\{x \in \mathbb{R} \text{ s.t. } x \geq 0,\ x^2 > 100\right\}$$

$$C = \{\{2\}, \{8\}, \{-12\}\} \qquad D = \{4k \text{ s.t. } k \in \mathbb{N},\ k \text{ odd}\}$$

8. Are the following sets equal?

(a) $\mathbb{Z}$ and $\{a : a \in \mathbb{N} \text{ or } -a \in \mathbb{N}\}$

(b) $\{1, 2, 2, 3, 3, 3, 2, 2, 1\}$ and $\{1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3\}$

(c) $\{d : d \text{ is a day with 40 hours}\}$ and $\{w : w \text{ is a week with 6 days}\}$

(d) $\{p : p \text{ is prime}, p < 42\}$ and $\{1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41\}$

9. Determine which of the following sets are equal to the set $S = \left\{\frac{1}{n} \text{ s.t. } n \in \mathbb{N}\right\}$.

$$A = \left\{\frac{1}{n+1} \text{ s.t. } n \in \mathbb{N}\right\} \qquad B = \left\{\frac{1}{|n|} \text{ s.t. } n \in \mathbb{Z},\ n \neq 0\right\}$$

$$C = \left\{\frac{2}{k} \text{ s.t. } k \in \mathbb{N},\ k \text{ even}\right\} \qquad D = \left\{\frac{a}{b} \text{ s.t. } a, b \in \mathbb{N}\right\}$$

$$E = \left\{\frac{1}{n-1} \text{ s.t. } n \in \mathbb{N},\ n > 1\right\} \qquad F = \left\{\frac{1}{m} \text{ s.t. } m \in \mathbb{Z},\ m > 0\right\}$$

Chapter 2

A little logic

One of the main things we are trying to do in mathematics is prove that a statement is always true. A simple example of this is the sentence

> The square of an even number is even.

More generally we might try to show that

- a particular mathematical object has some interesting properties,
- when an object has property 1 then it always has property 2,
- an object always has property 3 or property 4 but not both at the same time, or
- you cannot find an object that has property 5.

Let's spend a little time on this simple example of squaring even numbers and explore why it is true.

- A number n is even when we can write it as $n = 2k$ where k is an integer.
- This tells us that the square of that number is $n^2 = (2k)^2 = 4k^2$.
- But now we see that n^2 can be written as two times another number: $4k^2 = 2(2k^2)$.
- And since $2k^2$ is an integer, we know that n^2 is also even.

Notice that there is quite a lot going on here — a mixture of definitions, language and logic.

Most obviously (we hope) is that we have to understand what **even** means, so we need to define it. Despite us all being quite familiar with even and odd numbers, we should define it. We should not expect that everyone has exactly the same understanding of **even** since your readers can come from extremely diverse backgrounds. This author has encountered students who were taught at school that the number 0 is neither even nor odd, and others that were taught that only positive numbers can be even or odd. To avoid potential confusion we'll use the following

> A integer is **even** when it is equal to two times another integer, and an integer is odd when it is not even.

We'll come back to this definition in the next chapter after we have done a little more logic. We'll also make it a proper formal definition with bold-text and reference numbers and so on.

Our explanation then consists of sentences asserting bits of mathematics. The sentences are arranged in a particular order and cannot be shuffled around; each one *implies* the next. To be a good explanation we should take care of our reader and use clear language and enough detail so they can follow along. To make the language flow a little more easily we connect the sentences with words and phrases like "hence", "this tells us that", "because of this we can write". These words and phrases are not just there to make the reader feel a little more comfortable, they also help us to emphasise the *logical* connections between the sentences to the reader. At the same time, we can expect our reader to do some work; they should be able to understand standard notation, do basic arithmetic and algebra, etc.

In this chapter we won't do much proving of things, but instead we will focus on basic mathematical sentences and how we combine them together using logic.

2.1 Statements and open sentences

When you pick up a piece of mathematics you find that it is made up of **declarative sentences** — sentences that declare something.

> The number $\sqrt{2}$ is not a rational number.

> The number 17 is even.

The first sentence is **true** (we will prove it later in the text) and the second is **false**. These are sentences that can be assigned a definite **truth value** — they are either true or false. We will usually denote these T and F (and so save ourselves the burden of writing the other 7 characters). A declarative sentence that can be assigned a truth value is called a **statement**.

The reader will have noticed that the definitions in the previous paragraph are not very formal or precise. Since the authors have been emphasising the importance of being careful and precise, this seems a touch hypocritical[13]. However, giving a precise formal definition of mathematical statement turns out to be quite a lot like the problem of giving a precise formal definition of sets — very difficult and lies beyond the scope of this book [14]. So please excuse the (little)

[13]Hypocrisy starts at home.

[14]The interested reader should search-engine their way to articles on the foundations of mathematics, mathematical logic, Richard's paradox, the Berry paradox, and many other interesting topics that, unfortunately, lie outside the scope of this text (since it must have a finite length).

hypocrisy and we'll just stick with this less formal and more intuitive definition of statement.

Sentences like

> I am tall

and

> This sentence is false

are not statements since we cannot decide their truth value — they are neither true or false. In the first case it is because we don't actually know who "I" is. Is it the reader or is it the author? Further, we don't have a very precise definition of "tall" Indeed the notion of what height constitutes "tall" or "short" can vary dramatically between populations [15]. The second sentence is a little more difficult. If it is true, then it tells us it must be false — how can it be both? While if it is false, then that implies it must be true — again, how can it be both? This sort of self-referential sentence is very difficult to work with, so we will avoid them.

Self-referential statements. Self-referential statements are very interesting, but we should really start with simpler and straight-forward statements before rushing into difficult and confusing ones. The interested reader should search-engine their way to the related topic of Russell's paradox. This involves the set

$$R = \{X \mid X \notin X\}.$$

This is the set of all sets that do not contain themselves. The paradox occurs when we ask if R is an element of itself? If it is, then by the definition of R it cannot be. And if it is not, then by definition it must be.

The barber-paradox is similar, but more hirsute.

Here are some simple examples of mathematical statements:

- The 100th decimal digit of π is 7.
- The square of the length of the hypotenuse of a right angle triangle is equal to the sum of the squares of the lengths of the other two sides.
- Every even integer greater than 2 can be written as the sum of two primes.

The first might be true or might be false, but it must either be true or false[16]. The second is perhaps the most famous theorem any of us know. The last statement is **Goldbach's conjecture** and it is not known whether it is true or false. However it is still a statement because it must either be true or it is false.

[15] At the time of typing this author looked up wikipedia to find that the average height of a man in the Netherlands is about 184cm, while in Vietnam it is about 162cm. Quite a sizeable difference. Sorry for the pun.

[16] Actually it is true, though you have to be careful how you count — since the number starts 3.141 . . . we have counted the initial "3" as the first decimal digit. On the other hand, if you start counting from the first "1", then the 100th digit is "9". Definitions matter.

On the other hand, a sentence like

$$x^2 - 5x + 4 = 0$$

is not a statement because its truth value depends on which number x we are discussing. In order to assign a truth value we need to know more about x. Such sentences are called **open sentences**. If we assign a value to x then the open sentence will be either true or false and so become a statement. Usually this variable will come from some predefined set — its "domain". Often this is the integers or the reals, but typically we should make sure it is clear to the reader. This sentence, $x^2 - 5x + 4 = 0$, taken over the domain of the integers is true when $x = 1, 4$ and otherwise false. We'll come back to open sentences in Chapter 6.

We now need to start playing with these statements in a more abstract way. This will allow us to talk more generally about doing operations on statements — either operations that act on a single statement or operations that act on pairs of statements. I won't care too much about the details of the statement ("It is Tuesday" or "I can write with my left-hand"), but rather just its truth value (true and false). So much as we write an integer as n or m, a real number as x or y, I will write a statement as P, Q or R. As for the open sentences, we will use the notation $P(x), Q(x), R(x)$, since their truth values depend[17] on the value of x. This is reminiscent of a function; we put in some value for x and the sentence returns to us a statement. For example, if $P(x) : x^2 - 5x + 4 = 0$, we see that $P(1)$ is true, while $P(2)$ is false.

2.2 Negation

Given a statement, P, we can form a new statement which is the *negation* of the original, which we denote $\sim P$; this little squiggle is called a tilde.

Definition 2.2.1 Let P be a statement. The **negation** of P is denoted $\sim P$. When the original statement P is true, the negation $\sim P$ is false. And when the original statement is false, the negation is true. ♢

You will also see the negation written as $!P$ or $\neg P$. Since all three are quite commonly use, you should recognise all three. To not unduly confuse your reader, you should pick one and stick with it. You should recognise all three notations, as all three are in common use; we'll use the tilde notation in this text[18].

- The negation of "It is Tuesday" is "It is not Tuesday"

[17] When the open sentence depends on more than one variable, say x, k we will write $P(x, k), Q(x, k)$ and so on.

[18] This notation for the negation of a statement goes back at least as far as an Giuseppe Peano (1897) and Bertrand Russell (1908). The use of ¬ is due to Arend Heyting (1930) — many thanks to this website. The authors could not track down the earliest use of ! to denote the negation, but we do note that it is very commonly used in programming languages.

- The negation of "I can write with my left hand" is "I cannot write with my left hand". [19]
- The negation of "The integer 4 is even" is "The integer 4 is not even" or better yet "The integer 4 is odd"[20].

For our general statement P we can summarise its truth values and the corresponding truth values of its negation in a table:

P	$\sim P$	$\sim(\sim P)$
T	F	T
F	T	F

This table is called a truth table and we'll use them quite a bit. They can be a bit dull and mechanical to use, but they make the truth values very clear and precise and can help us reduce the problem of understanding the truth value of some complicated combination of statements to a simple procedure of filling in entries of a table.

We have included a column for the double-negation of a statement, $\sim(\sim P)$. Notice that the truth values of the double-negation are the same as those of the original statement. It is related to the law of the excluded middle — a statement is true or its negation is true — there is no third (middle) option. Thus the mean of negations in mathematics is quite different from what can happen in written and spoken English[21]. Also notice that if we only have the negation to play with then we cannot really do very much at all. We need some ways of combining statements. To do this we start with the logical "conjunction" and "disjunction" — "and" and "or".

2.3 Or and And

So the two simplest ways of combining two logical statements are using "or" and "and" . The words "or" and "and" have precise mathematical meanings which sometimes differ from their use in day-to-day language. To avoid conflating these mathematical means with the colloquial meanings we can refer to "or" and "and" by the nicely latin-flavoured words "disjunction" and "conjunction";

[19] The statement "I can write with my right hand" is not the negation of "I can write with my left hand". Just because someone cannot write with the left-hand does not mean that they can write with their right. For most of human history people could not write with either hand.

[20] In this case, because 4 is an integer we know that if it is not even then it must be odd. However, this is not that case for non-integers. For example, the negation of "π is even" is "π is not even" rather than "π is odd". We'll come back to even and odd in Chapter 3.

[21] In written and spoken English a double-negation can sometimes a negation, "We don't need no education."; sometimes it is ambiguous: "I do not disagree."; and sometimes positive: "The time you have is not unlimited.". In many languages a double-negation serves as a means of emphasising the negation. "Yeah, right" is a good example of a double-positive being a (sarcastic) negative.

hopefully we won't need those for very long and we'll get used to being more precise about when we want mathematical "and" and "or" and when we are just being colloquial.

Definition 2.3.1 Let P and Q be statements.

- The **disjunction** of P and Q is the statement "P or Q" and is denoted $P \vee Q$. The disjunction is true if at least one of P and Q are true. The disjunction is only false if both P and Q are false.

- The **conjunction** of P and Q is the statement "P and Q" and is denoted $P \wedge Q$. The conjunction is true when both P and Q are true. It is false if at least one of P and Q are false.

The truth tables of the disjunction and conjunction are

P	Q	$P \vee Q$	$P \wedge Q$
T	T	T	T
T	F	T	F
F	T	T	F
F	F	F	F

$\Diamond$

Be careful to use the correct notation. The symbols $\vee$ and $\wedge$ should not be confused or interchanged with the symbols for unions and intersections, $\cup$ and $\cap$. We'll come back to unions and intersections later in the text.

Notice that this use of "or" defined above is different from how we often use "or" in spoken English. When you are on a flight and the attendant offers you a meal (assuming you are on a long flight that still offers such luxuries) you might be asked

> "Would you like chicken or beef"?

You are not being offered both; you get at most one. This is an example of "exclusive or" — one or the other, but not both. The mathematical "or" we have just described above is "inclusive or" — at least one of the two options. You should assume that when we write "or" in a mathematical context we will mean *inclusive or*. To refer to exclusive or we will typically write "either … or … but not both". If in doubt use more words to clarify things rather then save yourself a few symbols at the expense of your reader's understanding.

The use of "and" in English can also have subtle differences from the mathematical conjunction $\wedge$. For example, "and" can sometimes imply an order: "He lived and he died" is more natural than "He died and he lived". The mathematical and, by contrast, doesn't care about order: $P \wedge Q$ has the same truth table as $Q \wedge P$.

For example, take the statements "7 is prime" and "18 is odd". We can now construct a new statement

7 is prime *and* 18 is odd

Since the first statement is true and the second is false, the conjunction of the two (our new statement) is false. On the other hand

7 is prime and 18 is even

is a true statement. Similarly the statement

7 is prime or 18 is odd

is true.

"Not", "and" and "or" are three logical connectives — or logical operators. They take one or two statements and combine them to make new statements — called "compound statements". Using "not", "and" and "or" you can construct any truth table of two statements you might want (there are $2^4 = 16$ of them). If you have done some computer science you have perhaps heard of NAND (not and), NOR (not or), XOR (exclusive or) and XNOR (exclusive not or). We'll shortly see how to construct such things using the three connectives we have just defined. But first we'll introduce the logical operator that lies at the heart of most of the mathematical proofs that are coming.

2.4 The implication

In mathematics we make many statements of the form

If x is a real number then x^2 is a real number

and a large fraction of the theorems we want to prove are of this form.

Definition 2.4.1 For statements P and Q, the **implications** or **conditional** is the statement

if P then Q

and is denoted $P \implies Q$. In this context P is called the **hypothesis** and Q is called the **conclusion**. The implication is false when P is true and Q is false; otherwise it is true. The truth table is

P	Q	$P \implies Q$	$(\sim P) \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

$\lozenge$

Note 2.4.2 It is important to note that $P \implies Q$ has the same truth table as $(\sim P) \vee Q$. Additionally — the truth table is not symmetric in P and Q and hence the statements $P \implies Q$ and $Q \implies P$ have different truth tables. See the middle two rows of the table below.

P	Q	$P \implies Q$	$Q \implies P$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Further note that sometimes the hypothesis is called the **antecedent** while the conclusion is called the **consequent**[22].

Before we get to the peculiarities of the truth table, we should note that the statement "$P \implies Q$" can be read in many different ways. Some of these are (in the opinion of the authors) a little obfuscating, and we recommend to stick with "If P then Q".

- if P then Q
- P implies Q
- whenever P then also Q

The author likes the statements above because the hypothesis comes before the conclusion. One may sometimes also see the implication $P \implies Q$ written as

- P only if Q
- Q if P
- Q whenever P
- Q provided that P

The authors recommend that you avoid these (at least until you have a bit more experience with mathematical proofs) since they write the conclusion before the hypothesis. They make it very easy to confuse the flow of logic. The statement "Q if P" is particularly confusing and, in this author's opinion, should be avoided.

Many mathematicians like to use the terms "necessary" and "sufficient" when writing implications. These terms allow one to put more emphasis on either the hypothesis or conclusion — this can be quite useful depending on the context in which you are writing. Consider again our nonsense example

If he is Shakespeare then he is dead

It is *sufficient* to check that a given person is Shakespeare to decide that they must be dead. Similarly, someone is *necessarily* dead in order for them to be Shakespeare You may see the implication $P \implies Q$ written in the following ways

[22] In a more linguistic context, the hypothesis is the **protasis** and the conclusion is the **apodosis**.

- P is a sufficient condition for Q,
- P is sufficient for Q,
- Q is a necessary condition for P, or
- Q is necessary for P.

The first two of these emphasise that if you want to know that Q is true, then one need only check (ie it is *sufficient* to check) that P is true. While the last two emphasise that the truth of Q is required (it is*necessary*) for P to be true.

Now back to the truth table. At first glance it can seem a bit strange so to get the feel of it we'll use it on a couple of simple examples and then apply it to something a little larger. Consider the statements P : 13 is even and Q : 7 is odd. The statement $P \implies Q$

Different conditionals. The interested reader should look up different types of conditionals:

- the material conditional (which is the implication we discuss here)
- the indicative conditional (we really should understand that while sentences like "If 4 is a square then the sky is blue" are true, the truth of the hypothesis has nothing to do with the truth of the conclusion),
- the counterfactual conditional (the dreaded subjunctive mood is lurking here and the author dare not reveal too much of their ignorance).

Of course, one can go a long long way down the rabbit hole when you start looking into this sort of thing (see this[23] and this[24] amongst many other distractions).

> If 13 is even then 7 is odd

is true, while $Q \implies P$

> If 7 is odd then 13 is even

is false.

A more sizeable example which appears in a few textbooks in similar forms. Frequently a student will ask their instructor

> Will I pass this course?

and the author (sometimes) responds

> If you pass the exam, then you will pass the course.

[23] wikipedia.org/wiki/Down_the_Rabbit_Hole
[24] xkcd.com/214/

Under what circumstances is the author lying or telling the truth?

The author has definitely lied if you pass the exam but end up failing to course. The other 3 possible outcomes are consistent with them telling the truth. Let's explore with the caveat that this should not be considered a binding discussion about your actual passing or failing of a given course. Use P to denote "The student passes the exam", and Q to denote "The student passes the course", so we can write my statement as $P \implies Q$:

> "If the student passes the exam, then the student passes the course."

- **(T,T)** Say the student passes the exam and passes the course, then clearly $P \implies Q$ is true.
- **(T,F)** Say the student passes the exam, but fails the course. Clearly the statement is wrong and so $P \implies Q$ is false. The author lied!
- **(F,T)** Say they failed the exam, but passed the course. Well this is indeed possible — perhaps the exam was very nasty and the author was very impressed by the only-just-fail (and maybe some good homework) and so gave a passing mark overall. The statement is not false and so must be true. $P \implies Q$ is true.
- **(F,F)** Say the student fails the exam and fails the course. Well the statement is not false and so must be true. Hence $P \implies Q$ is true.

Another good example (which the author has used quite a lot when teaching) is

> If he is Shakespeare then he is dead.
>
> —No one ever actually said this (well — except just now)

- **(T,T)** Here is Shakespeare and, sure-enough, he is looking pretty dead [25]. So the implication above is not a lie.
- **(T,F)** I found Shakespeare and he is up and about looking very well! The implication above is wrong and $P \implies Q$ is false. Also we should all learn what his secret is since he is over 450 years old!
- **(F,T)** Here is Chrisopher Marlowe [26] and he is not-alive. This does not actually invalidate the implication — it is still true.

[25] If one is not careful, you can end up on a long digression into dead parrots, pet-shop sketches, and the history of British comedy around here.

(F,F) Consider a very alive modern writer — despite their accomplishments they are not Shakespeare. [27]. Again, this does not invalidate the implcation —so it is still true.

So perhaps the most important thing to re-emphasise at this point is that an implication statement is false only when it fails to deliver it's claim. That is, when we find a situation in which the hypothesis is true but the conclusion is false.

As we noted above, a very large number of mathematical statements we want to prove take the form of an implication. For example:

If n is even then n^2 is even

When we construct the proof of such a statement we need to demonstrate that it is *always true and never false*. To understand how we do so, consider again the four rows of the truth table.

P	Q	$P \implies Q$
T	T	T
T	F	F
F	T	T
F	F	T

Notice that the implication is true in three of those cases and only false in one case — namely when the hypothesis is true and the conclusion is false. So our proof needs to show that this possibility cannot happen.

Hypothesis false We can see from the truth table that the implication is always true. We don't need to know anything about the conclusion since it doesn't matter whether or not the conclusion is true or false. Because of this, a proof doesn't actually have to consider this possibility explicitly. Anyone reading the proof knows[28] the truth-table of the implication and so also knows that the implication is true when the hypothesis is false.

Hypothesis true We will have to work, since the truth-value of the implication will depend on the truth value of the conclusion. Consequently most proofs start with the assumption that the hypothesis is true and then work towards showing that the conclusion must be true.

[26]There is (was?) a theory that Marlowe faked his own death and then started writing under the name "William Shakespeare" — though this is not widely accepted. People who promulgated this theory were called Marlovians.You can search-engine your way to some interesting articles on Marlowe.

[27]I'm sure you can find a few with the help of your favourite search-engine or online purveyor of books. You might even be lucky enough to study on a campus that that has a bookstore that still sells actual books.

[28]Should know.

Note 2.4.3 Note that because we want the implication to be true always, when we have an implication involving open sentences, such as

If n is even then n^2 is even

we want this to be true for every possible choice of n in the domain (in this case, integers). Typically, we do not write

For every possible n, if n is even then n^2 is even

but instead assume that the reader will understand (by context) that we mean for every possible n.

2.5 Modus ponens and chaining implications

2.5.1 Modus ponens

Once we have proved an implication

$$P \implies Q$$

to be always true, then we would like to make use of it. We will (soon) prove that the implication

If n is even then n^2 is even

is always true. Since we know it cannot be false, we'll write down the relevant 3 rows of its truth table and suppress the 1 row corresponding to the implication being false:

P	Q	$P \implies Q$
T	T	T
F	T	T
F	F	T

Notice that if we take a number like $n = 14$, then we know it is even and so the hypothesis is true. By the above truth-table we know that the conclusion must also be true — the number $n^2 = 14^2$ is even. We don't have to do any more work; the truth table, and our proof, ensure that the conclusion is true.

More generally, if we have proved that

$$P \implies Q$$

is always true, then if we know the hypothesis P is true, then the conclusion Q must also be true.

Definition 2.5.1 Modus ponens. The deduction

- P implies Q is true, and
- P is true
- hence Q must be true.

is called **modus ponens**. ♢

This logical deduction was first formalised by Theophrastus [29].

Notice that if we have proved the implication $P \implies Q$ to be true, but the hypothesis P is false, then we ***cannot*** conclude anything about the truth value of the conclusion. When the hypothesis is false, the truth value of the conclusion doesn't matter — the implication is still true. We can verify that by considering the relevant two rows from the truth-table of the implication.

P	Q	$P \implies Q$
F	T	T
F	F	T

Similarly notice that if we have proved the implication $P \implies Q$ to be true, and we have proved the conclusion Q to be true then we cannot conclude anything about the truth value of the hypothesis P. Again, this is easily verified by considering the relevant two rows from the truth-table of the implication.

P	Q	$P \implies Q$
T	T	T
F	T	T

There is, however, one more instance in which we can make a valid conclusion. Consider again the truth-table when the implication $P \implies Q$ is true but the conclusion Q is false:

P	Q	$P \implies Q$
F	F	T

Here the only possibility is that the hypothesis must be false. This allows us to make another valid deduction.

Definition 2.5.2 Modus tollens. The deduction

- P implies Q is true, and
- Q is false
- hence P must be false.

is called **modus tollens**. ♢

So when we know (back to our silly example) that

[29] Theophrastus was a student of Plato, a contemporary of Aristotle, and wrote on everything from botany to logic. Given the fragmented historical record, it is perhaps safer to write that the first record that we have of the formal statement of modus ponens comes from Theophrastus.

> If he is Shakespeare then he is dead.

then we can conclude that any live person is not Shakespeare. We will come back to modus tollens a little later in Section 2.6 when we examine the contrapositive.

2.5.2 Affirming the consequent and denying the antecedent

Misapplication of modus ponens is a frequent source of logical errors. An extremely common one is called “affirming the consequent”.

Warning 2.5.3 A common logical error. The ***false*** deduction

- P implies Q is true, and
- Q is true,
- and hence P must be true

is called **affirming the consequent**.

The flow of logic is wrong — check the truth table. Also notice that our arrow notation for the implication, $\implies$, helps to remind us that truth should flow from the hypothesis to the conclusion and not the other way around.

To see just how wrong this can be, consider again the true implication

> If he is Shakespeare then he is dead.

If we were to affirm the consequent, then any dead man must be Shakespeare.

Affirming the consequent does occasionally get used as a rhetorical technique (especially by purveyors of nonsense):

> If they are Galileo then they are supressed. I’m being supressed, so I must be Galileo.

or (when being a bit sorry for oneself)

> If they are a great artist then they are misunderstood. I’m misunderstood so I must be a great artist.

and the social-media comment section fallacy (with thanks to this comic[30]):

> If I tell the truth then I will offend people. I am offending people, so I must be telling the truth.

So be careful of affirming the consequent — it shows up a lot and is always fallacious.

A very similar logical error is called “denying the antecedent”

Warning 2.5.4 Another common logical error. The ***false*** deduction

- P implies Q is true, and

[30] www.smbc-comics.com/comic/the-offensive-truth

- P is false,
- and hence Q must be false

is called **denying the antecedent** and is a misapplication of modus tollens.

Here are some examples:

> If I have been to Toronto then I have visited Canada. I have not been to Toronto. So I have not visited Canada.
>
> If he is Shakespeare then he is dead. Abraham Lincoln is not Shakespeare, so he must be alive.
>
> If tastes bad then it must be healthy. This tastes good, so it must be unhealthy.

2.5.3 Chaining implications together

When we construct a proof that $P \implies Q$ is true, we don't do it in one big leap. Instead we break it down into a sequence of smaller (and easier) implications that we can chain together. To see how this works, consider the following:

Result 2.5.5 *Let P, Q and R be statement. Then the following statement is always true:*

$$\Big((P \implies R) \wedge (R \implies Q)\Big) \implies (P \implies Q).$$

Since we are going to need to refer to this piece of mathematics a few times in this section, we have take the trouble to format it clearly and given it a number.

This result is an example of a tautology, a statement that is always true. We will come back to tautologies later in the text. To show that it is always true we could either build the truth-table, or we can do some reasoning. Both of these methods are *proofs*, but we won't be quite so formal until the next chapter. The truth-table is not hard to construct but a bit tedious; since each of P, Q, R can either be true or false, there are $2^3 = 8$ rows to consider:

P	Q	R	$P \implies R$	$R \implies Q$	$P \implies Q$	The statement Result 2.5.5
T	T	T	T	T	T	T
T	T	F	F	T	T	T
T	F	T	T	F	F	T
T	F	F	F	T	F	T
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	T	F	T	T
F	F	F	T	T	T	T

The above is a perfectly reasonable way to show that the statement is always true. However, one can do the same just by a little reasoning; it also has the benefit of improving our understanding of the statement. We'll present the argument in dot-point form:

- The statement is an implication with hypothesis $((P \implies R) \wedge (R \implies Q))$ and conclusion $(P \implies Q)$. An implication is false when the hypothesis is true but the conclusion is false, and otherwise the implication is true.
- Since the conclusion, $(P \implies Q)$, is itself an implication, it can only be false when its hypothesis is true and its conclusion is false. So we must have P is true, but Q is false.
- In order for the hypothesis to be true, both implications, $(P \implies R)$ and $(R \implies Q)$, must be true (since a conjunction of two statements is only true when both statements are true).
    - Since P is true, and we require $(P \implies R)$ to be true, we must have R is true.
    - Since Q is false and we require $(R \implies Q)$ to be true, we must have R is false.

  But since R is a statement it cannot be true and false at the same time.
- So there is no way for us to make the statement false. Since it is never false, it must always be true.

So back to the statement $(P \implies Q)$. We'd like to show it is always true, but we cannot do it in one big leap. Instead, assume that we can make two smaller steps and prove that the two implications $(P \implies R)$ and $(R \implies Q)$ are always true. The conjunction of two implications, $(P \implies R) \wedge (R \implies Q)$, is also true and is exactly the hypothesis in Result Result 2.5.5. Since the implication in Result Result 2.5.5 is always true and its hypothesis is true — modus ponens — its conclusion must be true.

So while we could try to prove $(P \implies Q)$ is true in one big leap, it is sufficient to instead prove it is true in two smaller steps $(P \implies R)$ and $(R \implies Q)$. More generally when we prove $(P \implies Q)$, we will instead prove a sequence of implications:

$$\begin{aligned} P &\implies P_1 && \text{and} \\ P_1 &\implies P_2 && \text{and} \\ P_2 &\implies P_3 && \text{and}\dots \\ &\vdots \\ P_n &\implies Q \end{aligned}$$

where each of these intermediate implications is easier to prove.

Once we have done that, consider what happens if P is true or P is false:

P is true If P is true, the first implication tells us P_1 is true (modus ponens). Then since P_1 is true, the next implication tells us P_2 is true (again modus ponens). Since P_2 is true, P_3 is true, P_4 is true, and so on until we can conclude Q is true. Since P is true and Q is true, the implication $P \implies Q$ is true.

P is false On the other hand, if P is false then we know, just by looking at the implication truth-table, that the implication $P \implies Q$ is true.

Notice that when P is false, the fact that $(P \implies Q)$ is true is immediate and simply relies on the truth-table of the implication; we don't have to do any work or any reasoning. On the other hand, when P is true, we do need to work to show that $(P \implies Q)$ is true. For this reason almost all of our proofs will start with the *assumption* that P is true. We generally leave the case "P is false" unstated, assuming that our reader knows their truth-tables.

2.6 The converse, contrapositive and biconditional

We really want to get to our first proofs, but we need to do a tiny bit more logic, and define a few terms, before we get there. Consider the following thtree statements derived from implication $P \implies Q$.

Definition 2.6.1 Contrapositive, converse and inverse. Let P and Q be statements, then:

- the statement $(\sim Q) \implies (\sim P)$ is the **contrapositive**,
- the statement $Q \implies P$ is the **converse**, and
- the statement $(\sim P) \implies (\sim Q)$ is the **inverse**

of the implication $P \implies Q$. ♢

The contrapositive and converse appear quite frequently in mathematical writing, but the inverse is rare (in this author's experience at least). The truth-tables of the implication, contrapositive, converse and inverse are:

P	Q	$P \implies Q$	$\sim Q \implies \sim P$	$Q \implies P$	$\sim P \implies \sim Q$
T	T	T	T	T	T
T	F	F	F	T	T
F	T	T	T	F	F
F	F	T	T	T	T

The above tables show that the original implication and the contrapositive have the exactly same truth tables, and that the converse and inverse have the same tables. However we also see that the original implication does not have the same table as the converse or inverse. The inverse is not very commonly used, however the contrapositive and converse will be very useful for us as we continue.

Remark 2.6.2 Contraposition, conversion and inversion.. Note that the act of forming the contrapositive of $P \implies Q$ is **contraposition**. While forming the converse is (sometimes) called **conversion**, and forming the inverse is called **inversion**. Notice that the inversion is conversion of the contraposition of the implication.

Doing it twice. The inverse is also the contraposition of the conversion of the implication. The contraposition is also the inversion of the conversion. One could make a nice little table of the compositions of contraposition, conversion and inversion. Perhaps that is a good exercise.

While the converse is useful for forming mathematical statements, it can also be the source of bad logic (this is a good moment to go back and look at the warnings Warning 2.5.3 and Warning 2.5.4). The statement

> If he is Shakespeare then he is dead.

and its converse

> If he is dead then he is Shakespeare.

definitely do not mean the same thing[31]. However, the converse is often a source of interesting mathematics; once we have proved an implication, we should consider whether or not the converse is true. For example, we have already seen that

> If n is even then n^2 is even

is true. It's converse is

> If n^2 is even then n is even

is also true and will turn out to be quite useful later in the text.

The contrapositive can be extremely helpful — it might be hard to prove the original implication, but much easier to prove the contrapositive. Consider the statement

> If n^2 is odd then n is odd

This, it turns out, is awkward to prove as it is stated. Its contrapositive, however, is

> If n is not odd then n^2 is not odd.

or equivalently (assuming we are only talking about integers[32])

[31] Not every dead person is Shakespeare — ask any Elvis fan.

[32] Such assumptions happen quite frequently and the reader is often left to infer things from context. Writers do this, not just to be lazy, but so that the text flows and that one is not stating every single assumption in every single statement. That can make reading tedious, toilsome and tiring. Who doesn't like an alliteration.

If n is even then n^2 is even

which, even though we haven't written up the proof formally, we know is true. Since the truth-table of the contrapositive is identical to the original implcation, we now know that

If n^2 is odd then n is odd

must also be true.

Sometimes both an implication and its converse are true. That is

$$(P \implies Q) \wedge (Q \implies P)$$

This really means that whenever P is true, so is Q, and whenever Q is true so is P. It tells us that there is some sort of equivalence between what is expressed by P and Q. We can rewrite the above statement using the symbol $\iff$. It is our last connective and is called the "biconditional".

Definition 2.6.3 The biconditional. Let P and Q be statements. The **biconditional**, $P \iff Q$, read as "P if and only if Q", is true when P and Q have the same truth value and false when P and Q take different truth values. ◊

The biconditional $P \iff Q$ is also sometimes written as

- P iff Q,
- P is equivalent to Q, or
- P is a necessary and sufficient condition for Q.

Note that "iff" is still read as "if and only if" (and not as "iffffffffff" with a long "f"-noise).

Remark 2.6.4 We noted in the definition above, that $P \iff Q$ is true when P, Q have the same truth-values and false when P, Q have different truth-values. This in turn means that $P \iff Q$ has the same truth table as the statement $(P \implies Q) \wedge (Q \implies P)$.

P	Q	$P \iff Q$	$P \implies Q$	$Q \implies P$	$(P \implies Q) \wedge (Q \implies P)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

One of the first biconditional statements that we'll prove is

n^2 is odd if and only if n is odd.

but we have to walk before we run, so armed with all this logic this lets get on to our first proofs. After that we'll come back to logic.

2.7 Exercises

1. Determine whether or not each of the following is a statement or an open sentence. If it is a statement, determine if it is true or false.

(a) If 13 is prime, then 6 is also prime.

(b) If 6 is prime, then 13 is also prime.

(c) $f(3) = 2$

(d) 13 is prime and 6 is prime.

(e) 13 is prime or 6 is prime.

(f) The circle's radius is equal to 1.

2. Indicate whether the following are true or false.

(a) If today is Saturday, then it is a weekend.

(b) If it is a weekend, then today is Saturday.

(c) If the moon is made of cheese, then every cat in this room is purple.

3. Indicate whether the following are true or false. Explain your answers.

(a) If x is even, then $x \in \{2n : n \in \mathbb{N}\}$.

(b) If x is prime, then $x = 2k + 1$ for some $k \in \mathbb{Z}$.

(c) If $x \in \{3k : k \in \mathbb{Z}\}$ then $x \in \{6k : k \in \mathbb{Z}\}$.

(d) If $x \in \{6k : k \in \mathbb{Z}\}$ then $x \in \{3k : k \in \mathbb{Z}\}$.

4. Indicate whether the following are true or false.

(a) 3 is prime and 3 is even.

(b) 3 is prime or 3 is even.

(c) For $x \in \mathbb{R}$, $x^2 > x$ when $x > 1$, and 18 is composite.

(d) For $x \in \mathbb{R}$, $x^2 > x$ when $x > 1$, or 18 is composite.

5. Write the following sentences in symbolic logic notation. Make sure to note which statements/open sentences are denoted with which letter.

Example: The sentence, "The car is red and blue but not green" can be written as $(P \wedge Q) \wedge (\sim R))$, where P: "The car is red", Q: "The car is blue", and R: "The car is green". Also, the truth value of this sentence depends on the car, so it is an open sentence, not a statement.

(a) 8 is even and 5 is prime.

(b) If n is a multiple of 4 and 6, then it is a multiple of 24.

(c) If n is a not a multiple of 10, then it is a multiple of 2 but is not a multiple of 5.

(d) $3 \leq x \leq 6$.

(e) A real number x is less than -2 or greater than 2 if its square is greater than 4.

(f) If a function f is differentiable everywhere then whenever $x \in \mathbb{R}$ is a local maximum of f we have $f'(x) = 0$.

6. Write the following symbolic statements as English sentences.

(a) $(x \in \mathbb{R}) \implies (x^2 \in \mathbb{R}) \wedge (x^2 \geq 0)$.

(b) $4 \in \{2\ell : \ell \in \mathbb{N}\}$

(c) $(x \in \mathbb{N}) \implies \sim (x^2 = 0)$.

(d) $(x \in \mathbb{Z}) \implies \big(x \in \{2\ell : \ell \in \mathbb{Z}\}\big) \vee \big(x \in \{2k+1 : k \in \mathbb{Z}\}\big)$

7. Let P and Q be statements. Write out the truth tables for

(a) $(\sim P) \implies Q$

(b) $(P \wedge Q) \vee \big((\sim P) \implies Q\big)$

(c) $P \wedge (\sim P)$

(d) $P \vee (\sim P)$

(e) $(P \implies Q) \iff (Q \implies P)$

8. Let P and Q be statements. Show that the truth table for $\sim (P \implies Q)$ is the same as the truth table for $P \wedge \sim Q$.

9. In each of the following situations, determine whether or not it was raining on the given day, or explain why you cannot determine whether or not it was raining. For each situation we give you two pieces of information that are true; one is an implication and one is a statement.

(a) If it rains, then I bring an umbrella to work. I brought an umbrella to work on Monday.

(b) If it rains, then I bring an umbrella to work. I did not bring an umbrella to work on Tuesday.

(c) Whenever I am late for work, it rains. I was late to work on Wednesday.

(d) Whenever I am late for work, it rains. I was not late to work on Thursday.

10. There is an old saying: ”Red sky at night, sailor's delight. Red sky at morning, sailors take warning.” The phrase tells us that if the sky is red at night, tomorrow's weather will be good for sailing. However, if the sky is red in the morning, there will be a storm that day, and sailors should be prepared.

Assume that the following statement is true:

If the sky is red and it is morning, then sailors should take warning.

Now assume also that ...

(a) the sky is red. What can we conclude?

(b) the sky is red and it is morning. What can we conclude?

(c) sailors should take warning. What can we conclude?

(d) it is not true that (the sky is red and it is morning). That is, the sky is not red or it is not morning. What can we conclude?

(e) sailors should not take warning. What can we conclude?

11. Write the contrapositive of the following statements.

(a) If n is a multiple of 4 and 6, then it is a multiple of 24.

(b) If n is not a multiple of 10, then it is a multiple of 2 but is not a multiple of 5.

(c) A real number x is less than -2 or greater than 2 if its square is greater than 4.

(d) $(x \in \mathbb{R}) \implies (x^2 \in \mathbb{R}) \wedge (x^2 \geq 0)$.

(e) $(x \in \mathbb{N}) \implies \sim (x^2 = 0)$.

(f) $x \in \{3k : k \in \mathbb{Z}\} \implies x \in \{6k : k \in \mathbb{Z}\}$

12. Let $m \in \mathbb{N}$. Then two true statements are:

If m is odd, then m^2 is odd.
If m is even, then m^2 is divisible by 4.

Construct the contrapositive of each implication to give a total of four different implications. Which combinations can you chain together (so that the conclusion of the first is the hypothesis of the second), and what new implications do these combinations form?

13. In Chapter 11, we will prove that the following implication is true for $p = 2$:

If p is prime, then $\sqrt{p}$ is irrational.

In fact, this implication is true for any prime number p.

Write out the contrapositive, converse, and inverse of this implication. Can you determine whether any of these are true or false statements from the fact that the original implication is true?

14. Let P, Q, and R be statements. Suppose that

- "$P \implies (Q \wedge R)$"is false, and
- "$\big((\sim Q) \wedge R\big) \implies (\sim P)$" is true.

Which of P, Q, and R can you determine are true or false?

15. Let P, Q, R, and S be statements. Suppose that

- S is true,
- "$\big(R \vee (\sim P)\big) \implies \big(Q \wedge (\sim S)\big)$" is true, and
- "$P \iff \big(Q \vee (\sim S)\big)$" is true.

Determine the truth values of P, Q, and R.

16. Let P, Q, R, and S be statements. Suppose that

- "$((P \vee Q) \implies R) \iff (Q \wedge S)$" is true,
- "$(P \vee Q) \implies R$" is false, and
- S is true.

Determine the truth values of P, Q, and R.

Chapter 3

Direct proofs

Before we get to actually proving things we should spend a little time looking at how we name and prioritise mathematical statements. Not all things we want to prove are created equal and as a consequence they get different names.

Axioms Axioms are these are statements we accept as true without proof. Clearly they are very important since all our work hangs on them.

Facts We can also state some things as facts — these might be provable from axioms, but for the purposes of our text we don't want to go to the trouble (effort?) of proving them.

In this text we will use the following as an axiom.

Axiom 3.0.1 *Let n and m be integers. Then the following numbers are also integers*

$$-n, \qquad n+m, \qquad n-m \qquad \text{and} \qquad nm.$$

The authors are going to assume that you are familiar with the above properties and we do not need to delve deeper into them. The following is a statement that can be proved from the standard axioms of real numbers — we are not going to prove that, but we will use it. So we'll state it as a fact.

Fact 3.0.2 *Let x be a real number. Then $x^2 \geq 0$.*

Axioms of real numbers. The real numbers have an interesting history and you might be surprised to know that the first rigorous definition was only written down in 1871 by Georg Cantor — about 2 centuries after calculus was discovered by Newton and Leibniz! We'll discuss Cantor quite a bit later in the text. Your favourite search-engine can direct you to the axioms of the real numbers.

Another useful fact is Euclidean Divison, also called the division algorithm by some texts. It will come in very handy when we discuss even and odd numbers (for example).

Fact 3.0.3 Euclidean division. *Given integers a, b with $b > 0$, we can always find unique integers q, r so that*

$$a = bq + r$$

with $0 \leq r < b$.

So axioms and facts are slightly odd in that we don't have to prove them, but lets move onto statements that we do prove to be true.

Theorems A Theorem is a true statement that is important and interesting — Pythagorous' theorem for example. Or Euclid's theorem stating that there are an infinite number of prime numbers. Also, it is sometimes the case that implicit in the use of the word "Theorem" is that this is a result that we will use later to build other interesting results.

Corollary A Corollary is a true statement that is a consequence of a previous theorem. Of course, this makes almost everything a corollary of something else, but we tend to only use the term when the corollary is a useful (and fairly immediate?) consequence of a theorem.

Lemma A Lemma is a true statement that by itself might not be so interesting, but will help us build a more important result (such as a theorem). It is a helping result or a stepping stone to a bigger result[33]. You will occasionally see lemma pluralised as "lemmata".

Result and Proposition Otherwise we might just call a true statement a "Result" (especially if it is just an exercise or an example) or perhaps, if a little more important, a "Proposition".

3.1 Trivialities and vacuousness

As we said previously, most of the statements we want to prove are of the form $P \implies Q$. Before we get into proofs of more substance, we'll look at **trivial proofs** and **vacuous proofs**. These are two special cases that don't show up very often but you should know what they are. Recall that when we wrote out the truth table for $P \implies Q$ there were two observations we made:

- If P is false, then $P \implies Q$ is always true, independent of the truth value of Q.
- If Q is true, then $P \implies Q$ is always true, independent of the truth value of P.

[33] Indeed, the German word for Lemma is "Hilfssatz" — a helping result

The first of these is **vacuously true** — and the second is **trivially true**. They are both direct consequences of the truth table of the implication; no work is required. The results are of little use and so mathematicians use the dismissive terms **trivial** and **vacuous**. Consider:

Result 3.1.1 *Let $x \in \mathbb{R}$. If 8 is prime then $x^3 = 17$.*

So $P(x)$: 8 is prime, and $Q(x)$: $x^3 = 17$. A quick check shows that the hypothesis is false, so the result is vacuous. Of course we need to explain this to the reader in our proof otherwise its not a proof. It is safe to assume (in the context of writing a proof) that the reader knows their truth-tables. We don't have to explain everything in every proof.

Proof. Since $8 = 2 \times 4$ it is not prime, the hypothesis is false and thus the implications is always true. ■

Now providing the reader knows what a prime number is, and that they recall the truth-table of the implication, then we have clearly demonstrated that the hypothesis is false and so the implication must be true. Thus the reader is now convinced, and all is good.

Prime number? Now the authors are being a little bit sloppy here — we have assumed that the reader knows the definition of **prime**. While this is quite a basic notion of number, this author has been surprised by the very non-standard definitions of **prime number** that some students have been taught at school. Consequently we'll define prime numbers carefully in the next section.

This is an example of a vacuous proof — it is true because the hypothesis is always false. Notice that we cannot use modus ponens with such an implication because the hypothesis will never be true; the implication is true but in a rather useless way.

Despite this being a vacuous proof, we can learn something useful from how it is formatted. It is customary to tell the reader "the proof starts here" and "the proof finishes there", so that they know that all the necessary logic and mathematics is contained within that chunk of text. Typically we'll start a proof by writing "Proof:" (maybe underlined) and then finish it with a little square "□". The little square denotes "End of proof" or "QED" = "quod erat demonstrandum" = "which was to be demonstrated". It is perhaps a little pompous to write "QED" for such a little proof, so it is far more typical to see the little square. Some texts will use a little diamond "♦" or "♢", or a little filled in square "■". Some online-texts will simply enclose the whole proof in a box. In the HTML version of this text we'll enclose the proof in a box and also end it with a little square, while the PDF version of the text will simply have a little square.

Let's look at another example.

Result 3.1.2 *Let $n \in \mathbb{Z}$. If $n^2 < 0$ then $n^3 > 8$.*

Before writing anything down we should really read the hypothesis and conclusion very carefully. Notice that the hypothesis is saying something false. We know that the square of a number cannot be negative (we stated this as Fact 3.0.2), so the hypothesis is false.

Proof. The square of any real number is not negative; since the hypothesis is false, the statement is true. ■

The authors made an assumption about our reader in that proof — we've assumed that the reader knows Fact 3.0.2 well and so doesn't need to be reminded of it in the proof. We could choose to make this more explicit depending on our audience and the context. If you are in doubt as to what your readers know, you should put in more details.

A slightly more explicit proof. By Fact 3.0.2 we know that the square of any real number is not negative. Since the hypothesis is false, the statement is true. ■

There are related (and similarly quite useless) results which come from the conclusion being true independent of the hypothesis. For example:

Result 3.1.3 *Let* $x \in \mathbb{R}$*. If* $x < 3$ *then* 17 *is prime.*

Proof. Since 17 is a prime number the conclusion is always true. Hence the statement is true. ■

Primes and sieves. Here it would be sufficient to show that 17 is not divisible by 2,3 and 5. More generally to show that a number n is prime it suffices to show that it is not divisible by any prime smaller than $\sqrt{n}$ — this is (essentially) the sieve of Eratosthenese. Eratosthenese was also the first person to calculate the circumference of the Earth, invented the leap-day, was the chief librarian at the Library of Alexandria, and invented the study of geography! There are now much more efficient ways for large numbers and a quick bit of search-engineing will direct you to some of them. Anyway, a quick bit of arithmetic gives us $17 = 8 \times 2 + 1 = 5 \times 3 + 2 = 3 \times 5 + 2$, so by Euclidean division (remember Fact 3.0.3), 17 is not divisible by 2, 3 or 5 and hence must be prime.

This is an example of a trivial proof. We could put in more details to prove that 17 really is prime but we are going to assume that our reader knows their times-tables and the first few primes. Notice that since the conclusion is always true, we cannot use modus tollens with this result. Again, the result is true but in a useless way.

Here is another one.

Result 3.1.4 *Let* $x \in \mathbb{R}$*. If* $x < 0$ *then* $x^2 + 1 > 0$*.*

So now this looks a little harder but we can again look at this statement and see what is going on. The square of any number is always bigger or equal to zero (again Fact 3.0.2 is lurking here), so if we add 1 to it then it is definitely bigger than 0. We just need to translate this into mathematical language: Take any real number. Its square is bigger or equal to zero, so when we add 1, it is strictly bigger than 0.

Proof. Let $x \in \mathbb{R}$. Then $x^2 \geq 0$. Hence $x^2 + 1 \geq 1 > 0$. Since the conclusion is always true, the statement is always true. ■

Enough with the vacuous trivialities, it is high time we looked at some real results.

3.2 Direct proofs

A lot of the examples we will see shortly will involve even and odd numbers. Let us define these formally so we have a clear and solid base for our proofs.

Definition 3.2.1 An integer n is **even** if $n = 2k$ for some $k \in \mathbb{Z}$. ♢

So since $14 = 2 \times 7$ and $7 \in \mathbb{Z}$, we know that 14 is even. Similarly $-22 = 2 \times (-11)$ and $(-11) \in \mathbb{Z}$, so -22 is even.

0 is even. This author has encountered students who were taught that 0 is neither even nor odd — this is false. Since $0 = 2 \times 0$ and $0 \in \mathbb{Z}$, it follows that 0 is most definitely even.

When we first encounter "even" we learn that a number that is not even is "odd". At that time we have not yet encountered fractions or reals, so implicitly we thought all numbers were integers. But we know about rationals and reals (and maybe even complex numbers), so we should define odd numbers a little more carefully.

Definition 3.2.2 An integer n is **odd** if $n = 2\ell + 1$ for some $\ell \in \mathbb{Z}$. ♢

Since $13 = 2 \times 6 + 1$ and $6 \in \mathbb{Z}$ we know that 13 is odd. Similarly, -21 is odd because $-21 = 2 \times (-11) + 1$ and $-11 \in \mathbb{Z}$.

We should make a few observations about definitions before we move on to prove something.

The word "If" Notice that in both definitions we use the word "if" when we really mean "if and only if". If a number n is even then it can be written as $n = 2k$ for some integer k. AND if we can write $n = 2\ell$ for some integer ℓ, then we say that n is even. This becomes quite cumbersome, so it is convention that we write "if" in this context in definitions instead of writing "if and only if". We can safely assume that our reader knows this convention.

Find it easily Also we should make sure our definition is clear on the page. We declare it with "Definition:"! It is poor writing to hide important definitions inside the middle of an otherwise undistinguished paragraph (though this does happen from time to time). Some writers will put the key word being defined in inverted commas, or italics, or bold or underline, to further highlight it. If the definition is of an important object or property, then the reader should be able to find it and read it very easily.

Number it We have numbered[34] the definition so that we can refer to it easily (if necessary).

[34]Assigning numbers to results, lemmas, theorems and so on is standard practice in mathe-

"For some" is coming We have also used the phrase "for some" in both definitions. We haven't yet covered quantifiers in any sort of detail, but we will do so in Chapter 6 after a little more logic and some more proofs.

Definition 3.2.3 We say that two integers have the **same parity** if they are both even or they are both odd. Otherwise we say that the numbers have **opposite parities**. $\diamondsuit$

For a little more practice with definitions, lets extend the idea of "evenness" (being divisible by two):

Definition 3.2.4 Let n and k be integers. We say that k **divides** n if we can find an integer ℓ so that $n = \ell k$. In this case we write $k \mid n$ and say that k is a **divisor** of n and that n is a **multiple** of k. $\diamondsuit$

There is nothing in this definition that you haven't seen before (we hope), but it is worth looking at its structure since it is very typical.

- We start by defining the objects and symbols in our definition (this will necessarily build on previous definitions).
- We then define our main property **divides**.
- We follow up with some additional properties related to the main one.
- We have also used "if" in the definition in the way that we highlighted previously — we really mean "if and only if".

Finally, lets do one more definition related to divisibility — primes.

Definition 3.2.5 Let n be a natural number strictly greater than one. We say that n is **prime** if it cannot be written as the product of two smaller natural numbers. Equivalently n is prime when the only natural numbers that divide it are are 1 and itself.

If a natural number strictly greater than 1 is not prime then we say that it is **composite**. Finally, the number 1 is neither prime nor composite. $\diamondsuit$

Primality of 1. The primality of the number 1 has not always been as clear as it is today. Indeed, many mathematicians in the 19th century considered 1 to be prime and there are lists of prime-numbers published as late as the 1950's that have 1 as the first prime. Today, however, mathematicians treat 1 as a **unit** — a special case that is neither prime nor composite. One very good reason for doing so is that a great many results about prime numbers becomes substantially

matical writing. Unfortunately the topic of numbering equations is much less settled. This author has gotten into some strongly worded "discussions" with their coauthors on exactly this topic. Some authors like to number all equations, some like to only number the equations that get referenced inside the same document, and some like to number only the important equations. See these papers for an good discussion of numbering, Samaritans, Fisher, Occam and Fisher-Occam. It is also a good illustration of how mathematicians like a good argument over tiny details.

simpler and cleaner to state if 1 is not prime.

The interested reader can search engine their way to some interesting articles on this topic including this one[35].

Remark 3.2.6 The importance of being strict or equal. Notice in the above definition the emphasis we have placed on *strictly greater than one*. We really want the reader to realise that we mean "$>$" and not "$\geq$". In general, when writing inequalities in words (rather than symbols) it is a good idea to be very explicit so as to avoid possible confusion:

- $a < b$: "a *strictly* less than b"
- $a \leq b$: "a less than *or equal to* b"

If we were to write "a less than b" we may leave the reader confused as to whether or not a is allowed to be equal to b.

Let us go back to one of our first examples, and now that we have the right definitions and have done the required logic, we can prove it.

Result 3.2.7 *If n is even then n^2 is even.*

Lets think through our truth table again:

- If the hypothesis is false, the implication is true — no work required.
- If the hypothesis is true, then the implication will be true or false depending on the truth value of the conclusion — work required!

Just as we will many many times in the future, *we start by assuming the hypothesis is true.*

> Assume n is an even number.

What are we trying to get to?

> n^2 is an even number.

Know your definitions. It is very important to know definitions precisely. We cannot prove involving an object or property unless we can rigorously and carefully define it. The authors will likely nag you again and again about this.

If you have trouble memorising definitions, then we recommend you search-engine your way to some memorisation tips and tricks. You could also nag the authors back about producing nice auxillary materials that, say, could be easily reviewed on flash-cards or a phone.

At this point we know where we will start and where we need to end up, so a good next step is to flesh out what both the hypothesis and conclusion mean.

- If n is an even number then we can write it as $n = 2k$, where k is an integer.
- If n^2 is an even number then we can write it as $n^2 = 2\ell$, where ℓ is an integer.

[35] `cs.uwaterloo.ca/journals/JIS/VOL15/Caldwell2/cald6.html`

Remark 3.2.8 Not all even numbers are equal. Notice here that our result involves two even numbers, n and n^2. When I have invoked the definition of even, I have been careful to write $n = 2k$ and $n^2 = 2\ell$ using *different symbols*. This is important because it helps us to avoid making any *additional* assumptions about those numbers. Maybe we'll end up showing they are the same, and maybe we won't.

If we were to *accidentally* use the same symbols (and the authors know you won't do this after this warning), then we would have

- n is even, so $n = 2k$
- n^2 is even, so $n^2 = 2k$
- But then $n^2 = n$ which means $n^2 - n = 0$
- Factoring this gives $n(n-1) = 0$ and so $n = 0, 1$

So by reusing the symbol "k", we have inadvertently assumed that $n = 0, 1$, which is definitely not the result as stated.

Now since we know that $n = 2k$, we also know that $n^2 = (2k)(2k) = 4k^2$. From this we know $n^2 = 4k^2 = 2(2k^2)$. Since k is an integer, k^2 is an integer and $2k^2$ is an intger. So we've shown that n^2 can be written as twice and integer. In other words, we shown that it is even — exactly what we needed to do.

But we're not done. We have (in our work above) worked out ***how*** to prove our result, but we still need to write it up nicely. In this way proving a result really breaks into two parts

Scratch work Scratch work or proof-strategy or exploration or … — this is typically the difficult part, trying to work out what is going on, what does the hypothesis mean, what does the conclusion mean, how do we get from one to the other. What is the idea or path of the proof.

Write-up Once we have all the ideas and parts we still need to write things up nicely. This is typically easier than the scratch work, but it is non-trivial. We'll still need to work to make sure our presentation is clear, precise and easy to follow.

Let's write more nicely (and quite explicitly) with dot-points.

Proof.

- Assume n is even.
- So we can write $n = 2k$, where $k \in \mathbb{Z}$.
- But now, $n^2 = 4k^2$.
- This in turn implies that $n^2 = 2(2k^2)$.
- Since $2k^2$ is an integer, it follows that n^2 is even.

■

Notice that we don't prove that $2k^2 \in \mathbb{Z}$, nor do we have to explain basic facts about multiplication (as stated in Axiom 3.0.1); it is sufficiently obvious[36] that we can assume the reader will follow. Recall that back at the start of this chapter we warned you that we would make such assumptions about our (hypothetical) reader when writing our proofs.

Also notice the structure of the proof.

- P is true — where P is "n is even".
- $P \implies P_1$ is true — where P_1 is "$n = 2k$ for some $k \in \mathbb{Z}$".

  This follows from the definition of even.
- $P_1 \implies P_2$ is true — where P_2 is "$n^2 = 4k^2$".

  This is a basic fact about multiplication. To be more specific, "if $a = b$ then $ac = bc$".
- $P_2 \implies P_3$ is true — where P_3 is "n^2 is twice an integer".

  We are really using the fact that $4 = 2 \times 2$ and that multiplication is associative; we can expect the reader to understand this[37].
- $P_3 \implies Q$ is true.

  This is just the definition of even again.

So we have really shown

$$(P \implies P_1) \wedge (P_1 \implies P_2) \wedge (P_2 \implies P_3) \wedge (P_3 \implies Q)$$

And since we assume P is true, P_1 is true (modus ponens is our friend). Since P_1 is true, P_2 is true. And so forth until we conclude that Q is true. Hence we have shown that when P is true, we must have that Q is true.

This sort of proof in which we start by assuming the hypothesis is true and then work towards the conclusion is called a **direct proof**.

Now of course, when we actually prove something we don't go into this level of lurid detail. But for a first proof its not a bad idea to really see what is going. Let's write the proof more compactly, and a little more naturally:

Proof. Assume n is even. Hence we can write $n = 2k$ where $k \in \mathbb{Z}$. Then $n^2 = 4k^2 = 2(2k^2)$. Since $2k^2 \in \mathbb{Z}$ it follows that n^2 is even. ■

You can see there are some standard phrases that get used again and again

- Hence...
- It follows that...

[36] Well known to those that know it well, as this author's PhD supervisor says.

[37] Or they can quickly recall (or search-engine towards recalling) that the associativity of multiplication is just the fact that $a \times (b \times c) = (a \times b) \times c$.

- So...
- This implies that...
- We can now write...

These serve to make the proof more legible and flow a little more naturally.

Result 3.2.9 *Let n be an integer. If n is odd then $2n + 7$ is also odd.*

We don't leap into the proof; we start with scratch work.

- Assume the hypothesis is true (if it is false, there is nothing to be done).
- The hypothesis means that $n = 2k + 1$ for some integer k.
- The conclusion means that $2n + 7 = 2\ell + 1$ for some $\ell \in \mathbb{Z}$.
- But if $n = 2k + 1$, then $2n + 7 = 2(2k + 1) + 7 = 4k + 9 = 2(2k + 4) + 1$.
- Since $2k + 4 \in \mathbb{Z}$, $2n + 7$ is odd.

So we've got the idea, lets write it up.

Proof. Assume that n is an odd integer and so $n = 2k + 1$ for some $k \in \mathbb{Z}$. So

$$2n + 7 = 2(2k + 1) + 7 = 4k + 9 = 2(2k + 4) + 1.$$

Since k is an integer, $2k + 4$ is also an integer and so $2n + 7$ is odd. ∎

Another one — this one for you

Result 3.2.10 *If n is odd then n^2 is odd.*

Do your scratch work before you write up the proof — even if you see the way to prove it. Writing the scratch work really helps to formulate your ideas and makes writing out the proof much easier.

Proof. Assume that n is an odd integer and so $n = 2k + 1$ for some $k \in \mathbb{Z}$. So

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

Since k is an integer, $2k^2 + 2k$ is also an integer and so n^2 is odd. ∎

3.3 Proofs of inequalities

Not all mathematics involves integers, nor do all proofs involve equalities. So we should do a few examples of inequalities involving real numbers. This isn't just for variety, but does illustrate an important point about how our scratch work can often be quite different in logical structure from the final proof.

Result 3.3.1 *Let $x, y \in \mathbb{R}$. Then $x^2 + y^2 \geq 2xy$.*

As always we start with some scratch work. We don't know too many facts about inequalities — well, we do, but we haven't stated too many of them as facts or axioms in this text. We do know that $x^2 \geq 0$ no matter which real number we take for x — this was stated as Fact 3.0.2. So it would suffice to rearrange our inequality to make it look like the square of something.

$$x^2 + y^2 - 2xy \geq 0$$

But this is precisely $(x-y)^2 \geq 0$, which follows from the fact that we are squaring something.

So we see a way to prove things. But we should be very careful of the logical order here — how does the truth flow from one statement to another. Look at the structure of what we have done above.

- We started from the conclusion $x^2 + y^2 \geq 2xy$
- We finished at the fact that the square of any real number is non-negative.

This order is ***not correct***. We know that we must finish at the conclusion, not start at it. But we can reorder our work to give it the correct logical flow:

- Start from the fact that the square of a real number is non-negative.
- $(x - y)$ is a real, so its square is non-negative.
- Expand this expression and rearrange it
- Arrive at the conclusion.

This is quite common when we prove inequalities; the logical flow in scratch work is often the reverse of what is required for the proof. We typically start at the inequality we want to prove and then work our way to something we know — a fact, an axiom, a previous result or theorem. To then present the proof we must start at the axiom, fact or theorem, and then work our way to the result. We can now write things up nicely:

Proof. Let x, y be real numbers. Hence $(x - y)^2 \geq 0$. Expanding this gives $x^2 - 2xy + y^2 \geq 0$. This can then be rewritten as $x^2 + y^2 \geq 2xy$ and so gives the required result. ■

That was very illustrative (which is, of course, why we include this topic). Our scratch work can look very different from the final write up of the proof. We should do a couple more, but first a useful fact about inequalities, multiplication and division.

Fact 3.3.2 *Let $a, b, c \in \mathbb{R}$ with $a \geq b$.*

- *If $c > 0$ then $ac \geq bc$ and $a/c \geq b/c$.*
- *If $c < 0$ then $ac \leq bc$ and $a/c \leq b/c$.*

In proofs we will often need to combine inequalities together to make new inequalities. Very frequently we will make use of the fact that if $a > b$ and $b > c$ then we know that $a > c$. This is the **transitivity** of “$>$” (see Section 9.2). For example, if we know $a > b > 0$ and $c > d > 0$, then by multiplying the first inequality by c we get $ac > bc$. Similarly, multiplying the second inequality by b we get $bc > bd$. These two inequalities together imply that $ac > bd$.

Result 3.3.3 *Let $x \in \mathbb{R}$. If $x \geq 4$ then $x^2 - 3x + 7 \geq 11$.*

This one isn't too bad and we should break things into pieces.

- We know that $x \geq 4 > 0$, so then multiplying this by x gives us $x^2 \geq 4x$, and similarly, multiplying it by 4 gives us $4x > 16$. Hence we know that $x^2 \geq 16$.
- Similarly, since we know $x \geq 4$ we know that $3x \geq 12$. Ah —now there is a problem — we are about to try to take the difference of inequalities. Bad.
- Instead, go back and write $x^2 - 3x = x(x-3)$. Then since $x \geq 4$, $(x-3) \geq 1$. Hence $x^2 - 3x = x(x-3) \geq x$. So, because $x \geq 4$ we know that $x^2 - 3x \geq 4$.
- Adding 7 to both sides then gives us $x^2 - 3x + 7 \geq 4 + 7 = 11$.

We should now carefully check the flow of logic. We do indeed start with the hypothesis $x \geq 4$ and arrive at the conclusion. The order is good! Time to write it up.

Proof. Let $x \geq 4$ be a real number. Then we know that $x - 3 \geq 1$, and so $x(x-3) \geq 4$. Thus $x(x-3) + 7 = x^2 - 3x + 7 \geq 11$ as required. ■

In this case the logical flow in our scratch work matched the flow required for the proof. This is different from the previous example. There is not a hard rule that holds for all results. We need to be able to look at our scratch work, see the logical flow and determine how to translate that into a correct proof.

At the end of Chapter 5 we'll prove the triangle inequality. We can't do this just yet as it requires requires the development of a bit little more logical machinery.

3.4 A quick visit to disproofs

Lets look a little way ahead and think about how we might prove an implication to be false. Consider

If $n \in \mathbb{N}$ then $2^n + 1$ is prime.

How is our theorem true — the conclusion must be true every time the hypothesis is true. Hiding in this is that it must be true every single time the hypothesis is true.

So how could our theorem be false? We need the hypothesis to be true while the conclusion is false. But to be more precise — it only has to fail ***once***. So lets explore a few values of n:

- $n = 1$ then $2^n + 1 = 2 + 1 = 3$ which is prime.

- $n = 2$ then $2^n + 1 = 4 + 1 = 5$ which is prime.
- $n = 3$ then $2^n + 1 = 8 + 1 = 9 = 3 \times 3$ which is not prime.

So since there is a value of n that makes the hypothesis true, but the conclusion false, the implication is false. We are hiding here the idea of **quantifiers**

For all n, $P(n)$

There exists n, $P(n)$

We'll come back to these in Chapter 6, but after we've done a little more logic.

3.5 Exercises

1. If n is even then $n^2 + 3n + 5$ is odd.

2. Prove that the product of two odd numbers is odd.

3. We have already seen a proof that the product of two odd numbers is also odd. We'll now look at the remaining cases for the parity of a product or sum of two integers.

For each of the following cases, determine if the resulting number is even or odd, and prove your statement:

(a) the sum of two odd numbers;

(b) the sum of two even numbers;

(c) the sum of an even and an odd number;

(d) the product of two even numbers;

(e) the product of an even and an odd number.

4. Consider the faulty proof below for the following statement:

Show that if $x + y$ is odd, then either x or y is odd, but not both.

Faulty proof. Assume that either x or y is odd, but not both. Assume that x is odd and y is even (otherwise, switch x and y in the following argument). By the definitions of odd and even numbers, we know that $x = 2n + 1$ and $y = 2m$ for some $n, m \in \mathbb{Z}$. Then

$$x + y = (2n + 1) + (2m) = 2(n + m) + 1.$$

Since $n, m \in \mathbb{Z}$ and the sum of integers is also an integer, we see that $n + m \in \mathbb{Z}$, so that $x + y$ fits the definition of an odd number. ∎

Identify any issues with the proof as written above.

5. Consider the faulty proof below for the following statement:

The sum of two odd integers is even.

Faulty proof. Given $a = 2k + 1$ and $b = 2\ell + 1$,

$$a + b = (2k + 1) + (2\ell + 1) = 2(k + \ell + 1).$$

Since $k + \ell + 1 \in \mathbb{Z}$, $a + b$ is even. ■

Identify any issues with the proof as written above, and then give a proper proof of the statement.

6. Let $n, a, b, x, y \in \mathbb{Z}$. If $n \mid a$ and $n \mid b$, then $n \mid (ax + by)$.

7. Let $n, a \in \mathbb{Z}$. Prove that if $n \mid a$ and $n \mid (a + 1)$, then $n = -1$ or $n = 1$.

8. Let $a \in \mathbb{Z}$. If $3 \mid a$ and $2 \mid a$, then $6 \mid a$.

9. Let $n \in \mathbb{Z}$. If $3 \mid (n - 4)$, then $3 \mid (n^2 - 1)$.

10. Consider the faulty proof below for the following statement:

Let a, b, and c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Faulty proof. Assume a, b, and c are integers such that $a \mid b$ and $b \mid c$. Since a divides b, we have that $b = ka$ for some $k \in \mathbb{Z}$. Moreover, since b divides c, we have that $c = kb$ for some $k \in \mathbb{Z}$. But then

$$c = k(ka) = k^2 a,$$

Since k is an integer, $k^2 \in \mathbb{Z}$, and it follows that a divides c. ■

Identify any issues with the proof as written above, and then give a correct proof of the statement.

11. Consider the faulty proof that $2 = 1$.
Faulty proof. Assume that $x = y$. Then multiplying both sides by x gives

$$\begin{aligned} x^2 &= xy \\ \Rightarrow x^2 - y^2 &= xy - y^2 \\ \Rightarrow (x + y)(x - y) &= y(x - y) \\ \Rightarrow x + y &= y \\ \Rightarrow 2y &= y \end{aligned}$$

Letting $x = y = 1$, we have shown that $2 = 1$. ■

Identify any issues with the proof as written above.

12. The *floor* function, denoted by $\lfloor x \rfloor$, is defined to be the function that takes a real number x and returns the greatest integer less than or equal to x. This is also sometimes called the *greatest integer function.* For example,

$$\lfloor 3.5 \rfloor = 3, \qquad \lfloor -2.5 \rfloor = -3, \qquad \text{and} \qquad \lfloor 7 \rfloor = 7.$$

Using this definition, prove that

$$\lfloor x \rfloor = x \implies x \in \mathbb{Z},$$

and that

$$x \in \mathbb{Z} \implies \lfloor x \rfloor = x.$$

13. *Definition*: We call a number n an *integer root* if $n^k = m$ for some $k \in \mathbb{N}$ and $m \in \mathbb{Z}$.

For example, $\sqrt{7}$ is an integer root because $\left(\sqrt{7}\right)^2 = 7$. However, $\frac{5}{3}$ is not an integer root (but proving that is a little beyond this point in the text).

Use the above definition to show that if a and b are integer roots, then so is ab.

14. Consider the faulty proof below for the following statement:

Let x be a positive real number. If $x < 1$, then $1 < \dfrac{3x+2}{5x}$.

Faulty proof. Let x be positive. Then by multiplying the inequality

$$1 < \frac{3x+2}{5x}$$

by $5x$, which is positive, we obtain

$$5x < 3x + 2.$$

Collecting like terms, we have $2x < 2$, and finally dividing by 2, we have $x < 1$. ■

Identify any issues with the proof as written above, and then give a correct proof of the statement.

15. Consider the faulty proof below for the following statement:

Let x be a negative real number. Show that $-1 < \dfrac{5}{3x-5}$.

Faulty proof. Let x be negative. Then by multiplying the inequality

$$-1 < \frac{5}{3x-5}$$

by $3x - 5$ we obtain

$$-3x + 5 < 5.$$

and therefore $-3x < 0$. Dividing by -3 we end up with $x < 0$, which is true. ■

Identify any issues with the proof as written above, and then give a correct proof of the statement.

16. Let x, y be positive real numbers. Without using Calculus, prove that

$$(x > y) \implies (\sqrt{x} > \sqrt{y})$$

17. Consider the faulty proof below for the following statement:

Let $a, b \in \mathbb{R}$. If $0 < a < b$, then

$$\sqrt{ab} < \frac{a+b}{2}$$

Faulty proof.

$$\begin{aligned}
\sqrt{ab} &< \frac{a+b}{2} \\
ab &< \frac{(a+b)^2}{4} \\
4ab &< a^2 + 2ab + b^2 \\
0 &< a^2 - 2ab + b^2 \\
0 &< (a-b)^2
\end{aligned}$$

■

Identify any issues with the proof as written above and give a correct proof.

18. Let $x, y \in \mathbb{R}$ such that $x, y \geq 0$. Show that $\sqrt{x+y} \leq \sqrt{x} + \sqrt{y}$.

You may use the following without proof:

$$\text{If } 0 \leq a \leq b, \text{ then } \sqrt{a} \leq \sqrt{b}.$$

Chapter 4

More logic

Before we continue proving things, we need to learn more about how to manipulate logical expressions. We need to be able to rewrite statements as *equivalent* statements — create a new statement with the same truth table as the original. We have already seen an example of this in the contrapositive. In order to do that, we also need to understand how negation interacts with the disjunction, conjunction and implication. Our starting point for all of this is to think about statements which are always true.

4.1 Tautologies and contradictions

If we play around with compound statements and explore what can and cannot happen, we will quickly run into some statements which seem (potentially) rather silly:

$$P \vee (\sim P)$$

This statement is always true — no matter whether P is true or false. Such a statement is called a **tautology**. Why might this be useful? Well — you've seen that when we prove things, we need to use things that are true and the above is always true.

Here is another (more obviously useful) one

$$\sim (P \wedge Q) \iff ((\sim P) \vee (\sim Q))$$

This statement is always true no matter what the truth values of P and Q, so it is a tautology. To see this we could either write up the truth-table, or argue

- The left-hand clause is false only when P and Q are both true. Otherwise it is false.
- The right-hand clause is false only when $\sim P$ and $\sim Q$ are both false. That is, it is only true when both P and Q are false. Otherwise it is true.

- Hence both clauses take the same truth values and so the biconditional is always true.

We'll come back to this expression very shortly.

Just as there are statements that are always true, there are statements such as

$$P \wedge (\sim P)$$

that are always false.This is a **contradiction**. Another example is

$$(P \wedge Q) \wedge ((\sim P) \vee (\sim Q))$$

Lets write these definitions in a proper formal way so that we can refer back to it easily later if we need to do so.

Definition 4.1.1 Tautologies and contradictions. A **tautology** is a statement that is always true, while a **contradiction** is a statement that is always false. ♢

We will use tautologies in the very near future, but contraditions will have to wait until later in the course — there is a proof technique called "proof by contradiction" which relies on us arriving at a contradiction.

4.2 Logical equivalence

Not all tautologies are terribly useful, but we will use one family of tautologies again and again as we write proofs: **logical equivalences**. We have seen that the two statements

$$(P \wedge Q) \qquad \text{and} \qquad (Q \wedge P)$$

have the same truth tables; it only takes a moment to write down the table to convince yourself.

We could write this "have the same truth tables"-fact as follows:

$$(P \wedge Q) \iff (Q \wedge P) \text{ is a tautology}$$

Take a moment to parse this. The biconditional at the heart of the statement must be true, and a quick review of the biconditional tells us that both sides must be true at the same time and false at the same time — exactly what we want to express. This way of writing things is still cumbersome, and mathematicians will always seek out nicer notation if it is available.

Definition 4.2.1 We say that two statements R and S are **logically equivalent** when the statement $R \iff S$ is a tautology. In this case we write $R \equiv S$. ♢

Remark 4.2.2 Equivalent and equal? Note that some texts use "=" to denote logical equivalence, while this author much prefers "≡". One can get into long debates as to whether or not "=" is equivalent to "≡" despite not being equal. And unfortunately there is no clean and well established convention in the mathematical community. You should, as a reader, recognise both (from context).

Another logical equivalence we've already seen (back in Section 2.4) is

$$(P \implies Q) \equiv ((\sim P) \vee Q)$$

where we have written this down with plenty of brackets to avoid potential ambiguities.

Logical equivalence becomes very useful when we are trying to prove things. If we start with a difficult statement R, and transform it into an easier and logically equivalent statement S, then a proof of S automatically gives us a proof of R.

Here is a list of useful logical equivalences which will be very handy for proving things as we continue in the text. These constitute our first important result and since we will use it frequently we should call it a theorem.

Theorem 4.2.3 Logical equivalences. *Let P, Q and R be statements. Then*

- *Implication:* $(P \implies Q) \equiv ((\sim P) \vee Q)$
- *Contrapositive:* $(P \implies Q) \equiv ((\sim Q) \implies (\sim P))$
- *Biconditional:* $(P \iff Q) \equiv ((P \implies Q) \wedge (Q \implies P))$
- *Double negation:* $\sim (\sim (P)) \equiv P$
- *Commutative laws*
  - $P \vee Q \equiv Q \vee P$
  - $P \wedge Q \equiv Q \wedge P$
- *Associative laws*
  - $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$
  - $P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$
- *Distributive laws*
  - $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$.
  - $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.
- *DeMorgan's laws*
  - $\sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q)$
  - $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q)$

Proof. These can all be proved in a straightforward, but slightly tedious, manner by computing and comparing truth tables. ■

DeMorgan and camels. De Morgan's laws are named after the 19th century mathematician, Augustus De Morgan, though they were known at least as far back as Aristotle.

This author notes that he has come across many variations of the name, "de Morgan", "De Morgan" and "DeMorgan", but has yet to find anyone writing it with the medial capitalisation so beloved by tech-companies: "deMorgan". Medial capitalisation is very common in computer langauges to make multi-word variable names legible without spaces; in that context it is frequently called camelCase.

By chaining the logical equivalences in Theorem 3 together we can make new ones. For example, we can show the equivalence of the contrapositive as follows:

Example 4.2.4 Show that the contrapositive is logically equivalent to the original implication.

$$\begin{aligned}
(P \implies Q) &\equiv ((\sim P) \vee Q) && \text{implication as or}\\
&\equiv Q \vee (\sim P) && \text{commutation of or}\\
&\equiv \sim (\sim Q) \vee (\sim P) && \text{double negation}\\
&\equiv (\sim Q) \implies (\sim P) && \text{or as implication}
\end{aligned}$$

Arguably this would be easier to do using a truth table, but the above is much more informative. □

Here is a nice, and useful, example.

Example 4.2.5 Prove that $\sim (P \implies Q) \equiv P \wedge (\sim Q)$.

$$\begin{aligned}
\sim (P \implies Q) &\equiv \sim ((\sim P) \vee Q) && \text{rewrite implication as or}\\
&\equiv (\sim (\sim P)) \wedge (\sim Q) && \text{DeMorgan}\\
&\equiv P \wedge (\sim Q) && \text{double negation}
\end{aligned}$$

□

Another nice, and useful example. In fact it is so nice and useful, we probably should have made it an exercise:

Example 4.2.6 Show $\sim (P \iff Q) \equiv (P \wedge \sim Q) \vee (Q \wedge \sim P)$.

$$\begin{aligned}
\sim (P \iff Q) &\equiv \sim ((P \implies Q) \wedge (Q \implies P)) && \text{rewrite biconditional}\\
&\equiv (\sim (P \implies Q) \vee \sim (Q \implies P)) && \text{DeMorgan}\\
&\equiv (P \wedge (\sim Q)) \vee (Q \wedge (\sim P)) && \text{previous example}
\end{aligned}$$

□

So we now have another useful theorem

Theorem 4.2.7 Negating implications and biconditionals. *For statements P and Q we have*

- $\sim (P \implies Q) \equiv P \wedge (\sim Q)$
- $\sim (P \iff Q) \equiv (P \wedge (\sim Q)) \vee (Q \wedge (\sim P))$

This one will be very useful later on, so we'll call it a lemma. It isn't quite complete, you'll have to finish it off as an exercise later.

Lemma 4.2.8 *Let P, Q and R be statements. Then*

$$((P \vee R) \implies Q) \equiv ((P \implies Q) \wedge (R \implies Q))$$

Proof. We leave the proof as an exercise. ■

Some practice negating things.

Example 4.2.9 What is the negation of

$$(x^2 \geq 4) \wedge (x < 1)$$

Remeber to be careful when we negating inequalities. The negation of $a < b$ is $a \geq b$, and the negation of $a \leq b$ is $a > b$.

Solution.

$$\begin{aligned} \sim ((x^2 \geq 4) \wedge (x < 1)) &\equiv (\sim (x^2 \geq 4) \vee \sim (x < 1)) \\ &\equiv (x^2 < 4) \vee (x \geq 1) \end{aligned}$$

□

Example 4.2.10 Negate the statement

$$(x^2 \geq 1) \implies (x \geq 1).$$

Solution. Remeber to be careful with those inequalities.

$$\begin{aligned} \sim ((x^2 \geq 1) \implies (x \geq 1)) &\equiv (x^2 \geq 1) \wedge \sim (x \geq 1) \\ &\equiv (x^2 \geq 1) \wedge (x < 1) \end{aligned}$$

□

Example 4.2.11 Negate "The integer x is odd if and only if x^2 is odd."

Solution. This is actually a true statement (one we'll prove soon), but we can negate it anyway. We'll make use of the fact that if an integer is not odd, then it must be even (and vice-versa).

$$\begin{aligned} \sim ((x \text{ is odd}) \iff (x^2 \text{ is odd})) &\equiv \Big((x \text{ is odd}) \wedge \sim (x^2 \text{ is odd})\Big) \vee \Big((x^2 \text{ is odd}) \wedge \sim (x \text{ is odd})\Big) \\ &\equiv \Big((x \text{ is odd}) \wedge (x^2 \text{ is not odd})\Big) \vee \Big((x^2 \text{ is odd}) \wedge (x \text{ is not odd})\Big) \\ &\equiv \Big((x \text{ is odd}) \wedge (x^2 \text{ is even})\Big) \vee \Big((x^2 \text{ is odd}) \wedge (x \text{ is even})\Big) \end{aligned}$$

Oof! That is not so pretty. □

We are ready for some more proofs, but first — there are some exercises for you.

4.3 Exercises

1. Use truth tables to determine whether or not the following pairs of statements are logically equivalent.

(a) "$(\sim P) \vee Q$" and "$P \Rightarrow Q$".

(b) "$P \Leftrightarrow Q$" and "$(\sim P) \Leftrightarrow (\sim Q)$".

(c) "$P \Rightarrow (Q \vee R)$" and "$P \Rightarrow ((\sim Q) \Rightarrow R)$".

(d) "$(P \vee Q) \Rightarrow R$" and "$(P \Rightarrow R) \wedge (Q \Rightarrow R)$".

(e) "$P \Rightarrow (Q \vee R)$" and "$(Q \wedge R) \Rightarrow P$".

2. Use the logical equivalences given in Theorem 4.2.3 and Theorem 4.2.7 to negate the following sentences.

(a) 8 is even and 5 is prime.

(b) If n is a multiple of 4 and 6, then it is a multiple of 24.

(c) If n is not a multiple of 10, then it is a multiple of 2 but is not a multiple of 5.

(d) $3 \leq x \leq 6$.

(e) A real number x is less than -2 or greater than 2 if its square is greater than 4.

(f) If a function f is differentiable everywhere then whenever $x \in \mathbb{R}$ is a local maximum of f we have $f'(x) = 0$.

3. Show that the following pairs of statements are logically equivalent using Theorem 4.2.3.

(a) $P \iff Q$ and $(\sim P) \iff (\sim Q)$

(b) $P \implies (Q \vee R)$ and $P \implies ((\sim Q) \implies R)$

(c) $(P \vee Q) \implies R$ and $(P \implies R) \wedge (Q \implies R)$

Chapter 5

More proofs

Now that we've done a little more logic we should get back to proving things. Consider the following examples which (superficially) look quite similar to those we did back in Chapter 3:

Example 5.0.1 Let n be an integer. If $3n+7$ is even then n is odd.

Scratchwork.

- As always — assume the hypothesis is true.

$$3n+7=2k$$

- Then we try to use this to say something about the conclusion.

$$n=\frac{2k-7}{3}$$

- And now we are stuck, because it isn't clear that n is an integer and we need to show that

$$\frac{2k-7}{3}=2\ell+1$$

  for some integer ℓ. This doesn't look so obvious. Though it is surprising how many students will try to claim that one can deduce the parity from here.

Urgh. □

Example 5.0.2 If $n \in \mathbb{Z}$ then n^2+5n-7 is odd.

Scratchwork. Again, we start as we did previously; assume the hypothesis is true and work towards the conclusion.

- Assume the hypothesis is true — so n is an integer.

- Then $n^2 + 5n - 7 = 2\ell + 1$ means that we need

$$\begin{aligned} n^2 + 5n - 6 &= 2\ell && \text{and so} \\ n^2 + 5n &= 2(\ell + 3) \end{aligned}$$

- So…? Help — I'm stuck.

This would be a lot easier if we knew more about the parity of n. □

In both cases we can make our lives much easier by manipulating the original statement into another form by use of logical equivalences. More precisely

$$\begin{aligned} (P \implies Q) &\equiv (\sim Q \implies \sim P) \\ (P \vee R) \implies Q &\equiv (P \implies Q) \wedge (R \implies Q) \end{aligned}$$

In both cases, proving the statement on the left-hand side of the equivalence is completely logically equivalent to proving the statement on the right-hand side of the equivalence. So if the statement on the right-hand-side is easier, then we should just do that instead. Lets apply these equivalences to the above examples:

Example 5.0.1 starts with the statement

> Let n be an integer. If $3n + 7$ is even then n is odd.

The contrapositive of this is then

> Let n be an integer. If n is not odd then $3n + 7$ is not even.

However since we know that n is an integer, we can clean this up still more

> Let n be an integer. If n is even then $3n + 7$ is odd.

And now we are at a statement that looks exactly like results we proved in Chapter 3. This process of proving the contrapositive of the original statement is called **contrapositive proof** (not such an inventive term, but quite descriptive).

Manipulating Example 5.0.2 requires a little more thought. One of the impediments that we had was that we didn't know about the parity of n. However since n is an integer, we know it must be even or odd. Indeed,

> (n is an integer) $\equiv$ ((n is even) or (n is odd))

Hence we can rewrite Example 5.0.2 as

> If n is even or n is odd, then $n^2 + 3n - 9$ is odd.

We can then use the one of the above logical equivalences to rewrite this as

> (If n is even then $n^2 + 3n - 9$ is odd) and (If n is odd then $n^2 + 3n - 9$ is odd)

Again, we have arrived at statements that look just like those we proved in Chapter 3. This is an example of a **proof by cases**.

5.1 Contrapositive

As we have just seen, when we are presented with an implication to prove we should take a moment to think about the contrapositive of that implication — it might be easier! However, it do that we need to be able to *contrapose* a statement quickly. But that, in turn, requires us to negate statements fluently. Practice is crucial.

Once you have this fluency it only takes a moment to write down the contrapositive when you start your scratch work. Then you can assess what looks easier: the original or the contrapositive. If the contrapositive looks easier to prove, then we should proceed down that path. On the other hand, when it looks harder stick with the original.

It's time to return to Example 5.0.1 and try out a **contrapositive proof**.

Example 5.1.1 Example 5.0.1 redux. Let n be an integer. Prove that if $3n+7$ is even, then n is odd.

Scratchwork. First up, lets write out some scratch work / explorations.

- We got stuck when we tried a direct proof, so write down the contrapositive:

$$(n \text{ is even}) \implies (3n+7 \text{ is odd})$$

  This looks easier.

- Assume n is even.

$$\begin{aligned} n &= 2k \\ 3n+7 &= 6k+7 = 2(3k+3)+1 \end{aligned}$$

- Since $3k+3 \in \mathbb{Z}$ we are done.

Now that we've worked out how to make the proof work, we can write it up nicely. Since we are not using a direct proof we should alert the reader that we are going to prove the contrapositive. Otherwise it can look a little strange — I'm not going to assume the hypothesis is true, instead I'm going to assume the conclusion is false. Think about the reader!

Solution.

Proof. We prove the contrapositive. Assume that n is even and hence $n=2k$ for some integer k. This means that we can write

$$3n+7 = 6k+7 = 2(3k+3)+1.$$

Since $3k+3 \in \mathbb{Z}$, it follows that $3n+7$ is odd as required. ■

□

Remark 5.1.2 Warn your reader. As noted in the example above, when you prove the contrapositive of the result you should warn the reader of what you are going to do. You don't need to write much

- "We prove the contrapositive…",
- "Consider the contrapositive…",
- or even (if, say you are writing a test and running out of time)"Do contrapositive…"

A few words from you can save the reader a lot of confusion "Why are they assuming the conclusion is false?", "What is going on here?", etc.

Of course, there can be more than one way to prove things. Here is another proof of the same result, this one using a direct proof. Is uses a cute little trick that is worth remembering.

Example 5.1.3 Example 5.0.1 redux redux. Let n be an integer. If $3n+7$ is even, then n is odd.

Solution.

Proof. Assume that $3n+7$ is even. Hence $3n+7=2\ell$, where ℓ is some integer. Now we can write

$$\begin{aligned} n &= (3n+7)-(2n+7) \\ &= 2\ell - 2n - 7 \\ &= 2(\ell - n - 4) + 1 \end{aligned}$$

Since $\ell - n + 4 \in \mathbb{Z}$ it follows that n is odd. ■

□

Another similar example…

Example 5.1.4 Let $n \in \mathbb{Z}$. If n^2+4n+5 is odd, then n is even.

Scratchwork. The first thing we should do as part of our scratch work is to write down the contrapositive:

$$(n \text{ is not even}) \implies (n^2+4n+5 \text{ is not odd})$$

We've been a little sloppy here — we didn't write down the "Let $n \in \mathbb{Z}$", but it is scratch work not the actually proof. It is okay to be a *little bit* sloppy. The integerness of n means that we can simplify this further to

$$(n\text{is odd}) \implies (n^2+4n+5 \text{ is even})$$

This is now straight-forward for us.

Solution.

Proof. Let $n \in \mathbb{Z}$ and assume n is odd. Then $n=2k+1$ for some integer k. Hence

$$n^2+4n+5 = (2k+1)^2 + 4(2k+1) + 5$$

$$= 4k^2 + 4k + 1 + 8k + 4 + 5$$
$$= 4k^2 + 12k + 10 = 2(2k^2 + 6k + 5)$$

Since $2k^2 + 6k + 5$ is an integer, we know that $n^2 + 4n + 5$ is even as required. ■

The above proof can be improved. First up, we forgot to warn the reader "we are going to prove the contrapositive". Second, the reader doesn't need to see those boring algebraic manipulations; we can reasonably assume that the reader can do some basic algebra. So with those things in mind, here is a better proof.

Proof. We will prove the contrapositive, so let $n \in \mathbb{Z}$ and assume n is odd. Then $n = 2k + 1$ for some integer k. Hence

$$n^2 + 4n + 5 = 4k^2 + 12k + 10 = 2(2k^2 + 6k + 5)$$

and since $2k^2 + 6k + 5$ is an integer, we know that $n^2 + 4n + 5$ is even. ■

□

Let us now prove a simple (but useful) biconditional result. We'll call it a result rather than an example, because we'll need to refer back it later. We could even call it a lemma — in fact, let's do that.

Lemma 5.1.5 *Let $n \in \mathbb{Z}$, then n^2 is odd if and only if n is odd.*

It pays to do some exercises. If you haven't done it already, now is a good time to do this exercise 4.3.3.a. It tells us that the above is logically equivalent to "n^2 is even if and only if n is even", which is another useful (equivalent) result.

We've not proved a biconditional before, so where do we start. Our starting point is to rewrite the biconditional as implications because we know what we have to do to prove those. Recall from Theorem 4.2.3 that

$$P \iff Q \equiv (P \implies Q) \wedge (Q \implies P)$$

But how do we prove the conjunction of two implications?

Go back to first principles — we want to show that the statement cannot be false. This means that we must show that *both* implications are true. Hence we have to show that *both*

- If n^2 is odd then n is odd.
- If n is odd then n^2 is odd.

are true and then it follows that the conjunction is true, and so our original biconditional statement is true. Hence our proof consists of two parts (ie sub-proofs).

Of course, we have to tell the reader what we are doing. Statements like "We prove each implication in turn" or "We first prove one direction and then the other" are good ways to warn the reader what structure to expect. Then you can make this structure very easy to read by using dot-points or other formatting tricks.

Proof. We must show both that if n is odd then n^2 is odd, and if n^2 is odd then n is odd.

- Assume n is odd and so $x = 2k+1$ for some $k \in \mathbb{Z}$. Then $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Since $2k^2 + 2k$ is an integer, it follows that x^2 is odd.

- To prove that if x^2 is odd then x is odd we will show the contrapositive. Assume x is even and so $x = 2k$. Then $x^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, it follows that x^2 is even.

■

So this is pretty much just what we did for the other proofs, we just had to do it twice. First we proved $\implies$ and then we proved $\Leftarrow$. And we told the reader what we were doing; we didn't leave them to guess.

Parity proofs can get a little dull, so lets prove something a little different. Again, we'll call it a lemma because it might be useful later on.

Lemma 5.1.6 *Let a, b be non-zero integers. If $a \neq \pm b$ then $a \nmid b$ or $b \nmid a$.*

Because this result is about divisibility now is a good time to review Definition 3.2.4. Unfortunately that definition tells us what it means for an integer to *be* divisible by another, but not what is means when one integer is *not* divisible. However, we can turn that around using the contrapositive. The result then becomes

If $a \mid b$ and $b \mid a$ then $a = \pm b$.

This looks a lot easier. When we assume the hypothesis to be true we can use the definition of divisibility quite directly. This is a good sign that the contrapositive was the right thing to do.
Proof.

- Assume $a \mid b$ and $b \mid a$.

- Hence there are integers k, ℓ so that $b = ka$ and $a = \ell b$.

- Thus we can write $b = ka = k\ell b$.

- Since $b \neq 0$ we can divide both sides by b to get

$$k\ell = 1$$

- Now since $k, \ell \in \mathbb{Z}$ it follows that the only solutions to this are $k, l \in \{1, -1\}$.

- This gives $b = \pm a$ as required.

■

Of course we can also write this out in proper sentences and not point form. Actually, because we wrote things nicely above, we really just need to remove the dots:

Proof. Assume $a \mid b$ and $b \mid a$. Hence there are integers k, ℓ so that $b = ka$ and $a = \ell b$. Thus we can write $b = ka = k\ell b$. Since $b \neq 0$ we can divide both sides by b to get $k\ell = 1$. Now since $k, \ell \in \mathbb{Z}$ it follows that the only solutions to this are $k, l \in \{1, -1\}$. This gives $b = \pm a$ as required. ∎

5.2 Proofs with cases

Recall Lemma 4.2.8.

$$((P \vee Q) \implies R) \equiv ((P \implies R) \wedge (Q \implies R))$$

This tells us how to structure a proof when the hypothesis is a disjunction. That is, when the hypothesis can be broken into two (or more) cases.

Take another look at Example 5.0.2. At first glance, the hypothesis is just a single statement "n is an integer", and it is not immediately obvious that it can be broken into separate cases. However there is a clue in the conclusion, "$n^2 + 5n - 7$ is odd"; it tells us to think about parity. Any integer is either even or it is odd, so we can break the hypothesis into two cases

- n is even, or
- n is odd.

Because of this, the original statement can be massaged into the form of Lemma 4.2.8.

$$((n \text{ is even}) \vee (n \text{ is odd})) \implies n^2 + 5n - 7 \text{ is odd}$$

Lemma 4.2.8 then tells us that this is logically equivalent to

$$(n \text{ is even} \implies n^2 + 5n - 7 \text{ is odd}) \wedge (n \text{ is odd} \implies n^2 + 5n - 7 \text{ is odd}).$$

To show that this *conjunction* is true, we just need to show that both parts are true. That is, our proof will split into two **cases**.

1. Prove that (n is even $\implies n^2 + 5n - 7$ is odd).
2. Prove that (n is odd $\implies n^2 + 5n - 7$ is odd).

This is an example of **proof by cases**.

Of course, we don't just leap into things and write "Proof 1" and "Proof 2"; we need to explain to the reader what is happening. We need to explain that the hypothesis breaks into separate cases, and then we should make it clear where each case starts and where it ends. And, it won't hurt to summarise at the end of the proof that since we have proved all the cases, the result is true. Be nice to your reader — an extra sentence or two can make their life much easier.

Self interest? Sometimes the "reader" is a just a device to help us to think about how we are writing, but sometimes the "reader" is the person who marks your homework, tests and exams. Being nice to the reader can be good for the writer too.

Proof. Let $n \in \mathbb{Z}$. Since n can be either even or odd, we consider both cases separately.

- Case 1: Assume n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$ and $n^2 - 3n + 9 = 4k^2 - 6k + 9 = 2(2k^2 - 3k + 4) + 1$. Since $2k^2 - 3k + 4$ is an integer, $n^2 - 3n + 9$ is odd.

- Case 2: Now assume n is odd, then $n = 2k + 1$ for some $k \in \mathbb{Z}$ and $n^2-3n+9 = (4k^2+4k+1)-(6k+3)+9 = 4k^2-2k+7 = 2(2k^2-k+3)+1$. Since $2k^2 - k + 3$ is an integer, $n^2 - 3n + 9$ is odd.

Since both cases are true, the result follows. ∎

The above shows the very standard structure of **proof by cases** or **proof by case analysis**. Of course, not all such proofs consist of just two cases. More generally the structure will be as follows.

Proof.

- The hypothesis breaks into N cases.
- Here is my proof of case 1.
- Here is my proof of case 2.
- ⋮
- Here is my proof of case N.
- Since I've proved all N cases the proof is done.

∎

One of the hardest parts of case-analysis is to be sure that you have found all the cases. And since each case is really its own proof, it is possible that a single case breaks into several sub-cases, each of which requires its own proof. Case analysis is also sometimes called **Proof by exhaustion**! As an extreme example, the original proof of "The four colour theorem" by Appel & Haken in 1976 required the checking of about 1900 different cases. Thankfully that was done by a computer; though that was very controversial at the time.

4 colours by computer. The 4 colour Theorem tells you that any map (eg, a map of countries of the world) can be coloured using no more than 4 colours, so that no two neighbouring regions have the same colour. The interested reader can search-engine their way to many articles on the topic. The original proof by Appel & Haken was one of the first computer-aided proofs. The idea of getting a computer is not without objections — if a proof involves so many logical steps that it cannot be verified by a human, then is it really a proof? Again, the interested reader should search-engine their way to articles on philosophical questions that emerge from computer-aided proof.

Note that it is significantly easier to prove that you need no more than 5 colours, and we might even do it at the end of this text (assuming the author gets around to it). No computers are required! The proof actually started as a flawed attempt to prove the 4 colour Theorem by Kempe in 1879 which was rescued a decade later by Heawood as the 5 colour Theorem.

Remark 5.2.1 Keep cases just in case "without loss of generality" causes mistakes. You will have noticed that the two cases in the proof above are *very* similar. This is not unusual. It is very often the case that the cases in proof by cases are very similar to each other[38]. Many writers will omit one or more of these similar cases and instead write "The proof of the second case is similar to the proof of the first, so we omit it". You might also see "Without loss of generality (we will only do the first case)", which busy hard-working mathematicians will contract to "WLOG".

"WLOG" is a notoriously dangerous mathematical phrase[39] in mathematics. It sits with phrases such as

- Clearly
- Obviously
- It is easy to show that
- A quick calculation shows

Every mathematician has been caught out by one of these. What we thought would be an easy turned out to be much harder due to that little detail we didn't consider.

Premature optimisation is the root of all evil

Dictum attribution. This quote is usually attributed to Donald Knuth and is perhaps one of the best rules-of-thumb in programming. Knuth, however referred to it (at least once) as Hoare's dictum, after Tony Hoare. Hoare, however, attributed it to Edsger Dijkstra. Attribution quandaries aside, this makes an important point — make it right, not fast.

Of course, once it is right, then making it a bit faster is a good idea, but not at the expense of introducing errors. The interested reader should search-engine their way to the full quote and discussions thereof.

One should be very careful using WLOG (and its siblings). We should be very sure that the cases really are very similar. Indeed, it is much safer (as a general rule for the inexperienced prover) to actually do all those cases in your scratch work. *Then* determine whether or not they really are similar enough that skipping them is not going to cause any problems. And on then skip them when writting up the proof.

Here are another couple of results to play with

Lemma 5.2.2 *If two integers a and b have opposite parities then their sum is odd.*

Proof. Let a and b be integers and assume they have opposite parities. Now either a is even or a odd; we prove each case in turn.

[38] Enough cases for a luggage related pun if only we could pack one in here. Sorry.

[39] We keep a list. Well — we should keep a list.

- Assume a is even. Since a and b have opposite parities, we know that b is odd. Hence we can write $a = 2k, b = 2\ell + 1$ for some $k, \ell \in \mathbb{Z}$. This means that $a+b = 2k+2\ell+1 = 2(k+\ell)+1$. Since $k+\ell \in \mathbb{Z}$ we know that $a+b$ is odd.

- Now assume a is odd. Since a and b have opposite parities, we know that b is even. Hence we can write $a = 2k+1, b = 2\ell$ for some $k, \ell \in \mathbb{Z}$. This means that $a+b = 2k+2\ell+1 = 2(k+\ell)+1$, and since $k+\ell \in \mathbb{Z}$ we know that $a+b$ is odd.

In both cases, $a+b$ is odd as required. ■

and

Lemma 5.2.3 *Let $a, b \in \mathbb{Z}$. The number ab is even if and only if a is even or b is even.*

Proof. Let a, b be integers. We prove each implication in turn.

- To prove the forward implication we prove the contrapositive. Hence assume that both a, b are odd. So we can write $a = 2k+1$ and $b = 2\ell+1$ where $k, \ell \in \mathbb{Z}$. Now $ab = (2k+1)(2\ell+1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell)$. Since $2k\ell + k + \ell \in \mathbb{Z}$ we know that ab is odd as required.

- The reverse implication breaks into two cases.

  - Assume a is even. Then we can write $a = 2k$ where $k \in \mathbb{Z}$. So $ab = 2kb = 2(kb)$. Since $kb \in \mathbb{Z}$ it follows that ab is even.
  - Now assume that b is even. Then we can write $b = 2\ell$ where $\ell \in \mathbb{Z}$. So $ab = 2a\ell = 2(a\ell)$. Since $a\ell \in \mathbb{Z}$ it follows that ab is even.

  In either case ab is even as required.

■

Remark 5.2.4 Symmetry and WLOG. These last two results display a great deal of symmetry. That is, one can swap a and b without changing the result. That symmetry indicates that it may be possible to shorten the proof, by appealing to that symmetry to justify why a case can be skipped. However, correctly identifying such symmetries and their consequences takes practice. Consequently we still recommend that you avoid WLOG-ing when working through this book, and only WLOG once you have spent many more hours proving things.

Result 5.2.5 *Let $n \in \mathbb{Z}$, then $3 \mid n$ if and only if $3 \mid n^2$.*

In order to prove this we'll make use of **Euclidean division**. We stated this at the beginning of Chapter 3 as Fact 3.0.3. Please revise it before continuing.

Fact 3.0.3 tells us that every integer n can (by dividing by two) be written *uniquely* as either

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

for some integer k. That is, every integer is either even or odd. The same result tells that every integer n can (by dividing by three) be written *uniquely* as

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

for some integer k. It is this consequence of Euclidean division that will help us prove our result. Time for some scratch work.

It is a biconditional statement so we need to prove both the forward implication and the reverse implication.

- ($\Longrightarrow$): Assume $3 \mid n$, so $n = 3k$ where k is some integer. Hence $n^2 = 9k^2$ which is a multiple of 3. Not so bad.
- ($\Leftarrow$): If we try assuming that $3 \mid n^2$ we aren't going to get very far, so instead we look at the contrapositive.

  $$3 \nmid n \implies 3 \nmid n^2$$

  Here is where we can use Euclidean division.

  Any integer n can be written uniquely as one of $n = 3k, n = 3k + 1$ or $n = 3k + 2$ where $k \in \mathbb{Z}$. Now, we assume that $3 \nmid n$, so we cannot have $n = 3k$. Hence we have 2 cases to explore, namely $n = 3k + 1, n = 3k + 2$.

  - If $n = 3k + 1$ then $n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$, and so is not divisible by 3
  - If $n = 3k+2$ then $n^2 = (3k+2)^2 = 9k^2+12k+4 = 3(3k^2+4k+1)+1$, and so is not divisible by 3

  Since both cases work out, we are ready to write things up nicely.

Proof of Result 5.2.5. We prove each implication in turn.

- We start with the forward implication. Assume that $3 \mid n$, so $m = 3k$ where $k \in \mathbb{Z}$. Hence $n^2 = 3(3k^2)$, and since $3k^2 \in \mathbb{Z}$ we know that $3 \mid n^2$.
- To prove the reverse implication we prove the contrapositive. Assume that n is an integer, and that $3 \nmid n$. Hence (by Euclidean division), we know that either $n = 3k + 1$ or $n = 3k + 2$ where k is some integer.

  - Assume that $n = 3k + 1$, then $n^2 = 3(3k^2 + 2k) + 1$, and so is not divisible by 3.
  - Similarly, if we assume that $n = 3k + 2$, then $n^2 = 3(3k^2 + 4k + 1) + 1$, and so is not divisible by 3.

  In either case we conclude that $3 \nmid n^2$ as required.

■

Remark 5.2.6 The importance of uniqueness. Notice that in the above scratch work and proof we have used the *uniqueness* of Euclidean divison to show that n^2 is not divisible by 3. Once we have shown (in a case) that $n^2 = 3\ell + 1$ for some integer ℓ, Fact 3.0.3 tells us that there is no other way to write $n^2 = 3q$ with $q \in \mathbb{Z}$. Similarly, in the case where we show that $n^2 = 3\ell + 2$, the uniqueness of Euclidean division means that there is no way for us to write n^2 as 3 times an integer.

We have now had some practice with direct and contrapositive proofs, as well as proof by cases. It will soon be time to go back and do some more logic; we really need to look at quantifiers. But before that, we should do one two more examples of proof by cases — congruence modulo n, and the triangle inequality.

5.3 Congruence modulo n

Many results about divisibility of integers involve a fair bit of tedious work involving proof by cases; Result 5.2.5 is a good example of this. In that case we are interested in divisibility by 3 and so we use Euclidean division to separate the integers into 3 cases depending on their remainder. Much of that work can be simplified by introducing congruence.

Definition 5.3.1 Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. We say that a is **congruent to** b **modulo** n when $n \mid (a - b)$. The "n" is refered to as the **modulus** and we write the congruence as $a \equiv b \pmod{n}$.

When $n \nmid (a - b)$ we say that a is not congruent to b modulo n, and write $a \not\equiv b \pmod{n}$. ♢

Some simple examples:

- 19 is congruent to 5 modulo 7, since $19 - 5 = 14 = 2(7)$,
- 11 is congruent to 27 modulo 4, since $11 - 27 = -16 = 4(-4)$, and
- 13 is not congruent to 7 modulo 5 since $13 - 7 = 6$ and $5 \nmid 6$.

Also notice that congruence nicely extends parity; we can re-express parity as just congruence modulo 2.

Result 5.3.2 *Let a, b be integers. Then $a \equiv b \pmod{2}$ if and only if a and b have the same parity.*

Proof. We prove both implications in turn. So start by assuming that $a \equiv b \pmod{2}$. Then we know that $2 \mid (a - b)$ and thus $a - b = 2k$ for some $k \in \mathbb{Z}$. Now either a is even or odd.

- When a is even, we know that $a = 2\ell$ for some integer ℓ, and thus $b = 2k + 2\ell$ and so is also even.
- Similarly when a is odd, we know that $a = 2m + 1$ for some integer m, and thus $b = 2k + 2m + 1$ and so is also odd.

Thus being congruent modulo 2 implies that they have the same parity.

Now assume that a, b have the same parity. Then either they are both even or they are both odd.

- When a, b are both even, we can write $a = 2k, b = 2\ell$ and so $a - b = 2(k - \ell)$.
- When a, b are both odd, we can write $a = 2k + 1, b = 2\ell + 1$ and so $a - b = 2(k - \ell)$.

In both cases the difference $a - b$ is divisible by 2 and so $a \equiv b \pmod 2$ as required. ■

Perhaps the main reason that congruence modulo m is so important is that congruence interacts very nicely with basic arithmetic operations. This gives rise to what is known as **modular arithmetic**.

Theorem 5.3.3 Modular arithmetic. *Let $n \in \mathbb{N}$, and let $a, b, c, d \in \mathbb{Z}$ so that*

$$a \equiv c \pmod n \qquad \textit{and} \qquad b \equiv d \pmod n$$

Then

$$a + b \equiv c + d \pmod n, \qquad a - b \equiv c - d \pmod n \qquad \textit{and} \qquad ab \equiv cd \pmod n.$$

Proof. Let $n \in \mathbb{N}$, and let $a, b, c, d \in \mathbb{Z}$ so that $a \equiv c \pmod n$ and $b \equiv d \pmod n$. Hence $a = c + nk, b = d + n\ell$ where k, ℓ are integers.

- We can write $(a + b) = (c + d) + n(k + \ell)$, so $(a + b) - (c + d) = n(k + \ell)$. Hence $(a + b) \equiv (c + d) \pmod n$.
- Similarly, we can write $(a-b) = (c-d)+n(k-\ell)$, so $(a-b)-(c-d) = n(k-\ell)$. Hence $(a - b) \equiv (c - d) \pmod n$.
- Now $ab = (c + nk)(d + n\ell) = cd + n(dk + c\ell) + n^2kl$. So $ab - cd = n(dk + c\ell + nkl)$, and hence $ab \equiv cd \pmod n$.

■

We can now use this result to simplify some of our proof-by-cases proofs. Let's start by reproving Result 5.2.5. And we start that by restating the result in terms of congruences:

Another proof of Result 5.2.5. We start by restating the result in terms of congruences:

$$n \equiv 0 \pmod 3 \iff n^2 \equiv 0 \pmod 3,$$

and now we prove each implication in turn

- Assume that $n \equiv 0 \pmod 3$, then by Theorem 5.3.3 we know that $n^2 \equiv 0 \pmod 3$ as required.
- We prove the contrapositive of the reverse implication, so assume that $n \not\equiv 0 \pmod 3$. Thus either $n \equiv 1 \pmod 3$ or $n \equiv 2 \pmod 3$.
  - When $n \equiv 1 \pmod 3$, Theorem 5.3.3 tells us that $n^2 \equiv 1 \pmod 3$.
  - Similarly, when $n \equiv 2 \pmod 3$, we know that $n^2 \equiv 4 \pmod 3$. And since $4 \equiv 1 \pmod 3$, this means that $n^2 \equiv 1 \pmod 3$.

So in both cases, $n^2 \not\equiv 0 \pmod 3$ as required.

■

Notice we are doing something a little sneaky in the proof. We deduced that since $n^2 \equiv 4 \pmod 3$ and $4 \equiv 1 \pmod 3$, we know that $n^2 \equiv 1 \pmod 3$. This is because congruence is **transitive** — a notion we will return to in Chapter 9. But since it is quite useful, let's prove it now.

Result 5.3.4 *Let $n \in \mathbb{N}$, and let $a, b, c \in \mathbb{Z}$ so that $a \equiv b \pmod n$ and $b \equiv c \pmod n$. Then $a \equiv c \pmod n$.*

Proof. Let a, b, c and n be as stated. Then we know that for some $k, \ell \in \mathbb{Z}$

$$a - b = nk \qquad \text{and} \qquad b - c = n\ell.$$

Then $(a - b) + (b - c) = a - c = n(k + \ell)$ and so $a \equiv c \pmod n$. ■

Here is another example; congruence makes this easier to prove.

Result 5.3.5 *Let $a, b \in \mathbb{Z}$. If $3 \nmid a$ and $3 \nmid b$ then $3 \mid (a^2 - b^2)$.*

Proof. Let $3 \nmid a$ and $3 \nmid b$. Then, by Euclidean division, we know that $a \equiv 1 \pmod 3$ or $a \equiv 2 \pmod 3$.

- When $a \equiv 1 \pmod 3$, $a^2 \equiv 1 \pmod 3$.
- And, when $a \equiv 2 \pmod 3$, $a^2 \equiv 4 \pmod 3$. Since $4 \equiv 1 \pmod 3$, we also have that $a^2 \equiv 1 \pmod 3$.

So in either case $a^2 \equiv 1 \pmod 3$. This also implies that $b^2 \equiv 1 \pmod 3$. Thus $a^2 - b^2 \equiv 0 \pmod 3$. So finally we can conclude that $3 \mid (a^2 - b^2)$ as required. ■

We will return to congruences and modular arithmetic in Section 9.4, but now we turn to a very famous inequality.

5.4 Absolute values and the triangle inequality

The triangle inequality is a very simple inequality that turns out to be extremely useful. It relates the absolute value of the sum of numbers to the absolute values of those numbers. So before we state it, we should formalise the absolute value function.

Definition 5.4.1 Let $x \in \mathbb{R}$, then the absolute value of x is denoted $|x|$ and is given by

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

◊

How we compute[40] the absolute value of a number depends on whether that

[40]When we first encounter the absolute value, it is often tempting to think of it a function that "removes the minus sign". Such thinking leads to errors. In particular, if x is a negative

number is negative or not — it is an example of a piecewise function.

$$|8| = 8$$
$$|-5| = -(-5) = 5$$

Since the absolute value is defined in two branches like this, it naturally leads to proofs that require cases. The proof of the triangle inequality is a good example of this. Before we state (and prove) the triangle inequality, let's prove a few useful lemmas that describe some useful properties of the absolute value.

Lemma 5.4.2 *Let $x \in \mathbb{R}$, then $|x| \geq 0$.*

We will split the proof into two cases. The first dealing with $x \geq 0$ and the second with $x < 0$. Doing this allows us to rewrite the absolute value $|x|$ as either x or $-x$, and so simplify our analysis.

Proof. Let $x \in \mathbb{R}$ so that either $x \geq 0$ or $x < 0$.

- When $x \geq 0$, we know that $|x| = x$, and so $|x| \geq 0$.
- Now assume that $x < 0$. Then $|x| = -x$. Now since x is negative, it follows that $-x$ is positive, and so $|x| = -x > 0$.

In both cases we have shown that $|x| \geq 0$. ■

To prove the next result it is actually convenient to use a more symmetric definition of the absolute value function that splits into three cases:

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

We do this to take advantage of the fact[41] that $-0 = 0$.

Lemma 5.4.3 *Let $x \in \mathbb{R}$ then $|x| = |-x|$.*

Proof. Let $x \in \mathbb{R}$, then either $x = 0, x > 0, x < 0$.

- When $x = 0$, then $-x = x = 0$ and $|x| = |-x| = 0$.
- Now, let $x > 0$. This means that $|x| = x$. Further $-x < 0$ and so $|-x| = -(-x) = x = |x|$.
- Finally, let $x < 0$, so that $|x| = -x$. Additionally, $-x > 0$ and so $|-x| = (-x) = |x|$.

In all three cases the result holds. ■

We can reuse the basic ideas of this proof to obtain the following

---

number then $|x| = -x$, and the presence of that minus sign can be very confusing.

[41] In computing and in some applications it can be quite useful to have a "signed zero". The interested reader should search-engine their way to more information on this topic and the related topic of the extended real number system. You have actually already seen some of the ideas when you studied limits to zero and to $\pm\infty$ in Calculus 1.

Lemma 5.4.4 *Let $x \in \mathbb{R}$, then $-|x| \leq x \leq |x|$.*

Proof. Let $x \in \mathbb{R}$ so that either $x \geq 0$ or $x < 0$.

- When $x \geq 0$, we know that $|x| = x$. Now since $x \geq 0$, it follows that $-|x| \leq 0 \leq x = |x|$.
- Now assume that $x < 0$. Then $|x| = -x$, so that $-|x| = x$. Now since $x < 0$ it follows that $-|x| = x < 0 \leq |x|$.

In both cases we have shown that $-|x| \leq x \leq |x|$ as required. ■

We can extend the above lemma a little to get a very useful result. It tells us how to transform bounds on quantity into bounds on its absolute value and vice-versa.

Lemma 5.4.5 *Let $x, y \in \mathbb{R}$, then*

$$|x| \leq y \iff -y \leq x \leq y$$

Proof. We prove each implication in turn.

- Assume that $|x| \leq y$. Now either $x \geq 0$ or $x < 0$.
  - When $x \geq 0$, we know that $|x| = x$. Hence $y \geq |x| = x \geq 0 \geq -y$.
  - On the other hand if $x < 0$, we know that $y \geq |x| = -x > 0$. So, multiplying through by -1 we have $-y \leq x < 0 \leq y$.

  In both cases we have shown that $-y \leq x \leq y$ as required.
- Now assume that $-y \leq x \leq y$. Again, either $x \geq 0$ or $x < 0$.
  - When $x \geq 0$, we know that $x = |x|$. So, by assumption $y \geq x = |x|$.
  - Now, when $x \leq 0$, $|x| = -x$. Transform our assumption $y \geq x \geq -y$, by multiplying everything by -1, giving $-y \leq -x = |x| \leq y$.

  In both cases we have shown that $|x| \leq y$ as required.

■

Okay, now we can prove our main result; it tells us that the absolute value of the sum of two numbers is smaller[42] than the sum of the absolute values. It is a very simple but turns out to be extremely useful[43].

---

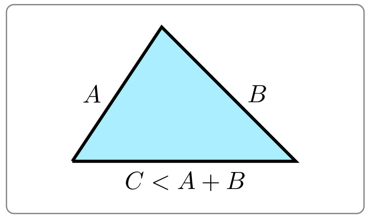
[42]This gives a nice counter example to the misquotation of Aristotle about sums and parts that has been worn out from (over/mis)use.

[43]Mathematicians like results like this one. When we define a new mathematical operation or function, we want to see how it interacts with the ones we already know. When you did Calculus you saw results like this — we have just defined limits, how do limits interact with addition, multiplication and division? There are many other examples including the product rule and the quotient rule and integration by parts. We will see more examples when we get to functions in Chapter 10.

Theorem 5.4.6 The triangle inequality. *Let $x, y \in \mathbb{R}$, then*

$$|x + y| \le |x| + |y|.$$

The inequality gets its name from a more geometric interpretation[44]. It tells us that the length of the third side of the triangle, C, is bounded by the sum of the lengths of the other two sides, A, B.



Now, rather than leap into a neat proof of this, we should take some time to explore the problem and the various cases that might arise. Since the values of $|x|, |y|$ and $|x + y|$ all depend on whether each quantity is positive or negative[45].

- Notice that if both $x, y \ge 0$, then it is easy to prove since

$$|x| + |y| = x + y$$

- Similarly, if both $x, y < 0$, then we know that $x + y < 0$ and so we have

$$|x| + |y| = (-x) + (-y) = -(x + y) = |x + y|$$

- A little more care is required when (say) $x \ge 0$ but $y < 0$. In this case we have

$$|x| + |y| = x + (-y) = x - y$$

  and it is not immediately obvious how to relate this to $(x + y)$. One way to proceed is to break this case into subcases depending on whether $(x+y) \ge 0$ or $(x + y) < 0$. Urgh.

Let us instead take a step back and start again, but this time from assumptions about $(a + b)$. Either $a + b \ge 0$ or $a + b < 0$.

- In the first case

$$|a + b| = a + b$$

  and we know, from our lemma above, that $a \le |a|$ and $b \le |b|$, so

$$|a + b| = a + b \le |a| + |b|.$$

[44]Indeed it was likely first proved by the ancient Greeks, and appears in Book 1 of Euclid's Elements as Proposition 20. The interested reader should search-engine their way to a discussion of Euclid's elements — likely one of the most influential books ever written.

[45]The pedantic reader will notice that we could have said "whether each quantity is non-negative or negative", since we have defined the absolute value function to lump $x = 0$ together with $x > 0$. We could have split absolute value function in 3 pieces $x > 0, x = 0, x < 0$ as we did in one of the proofs earlier in the section. While this is nicely symmetric, it does make our proofs longer, since we have to consider 3 cases for each quantity.

- Now, the second case gives

$$|a+b| = -(a+b) = -a-b$$

Our lemma above tells us that $-a \leq |a|$ (and similarly that $-b \leq |b|$), so

$$|a+b| = (-a) + (-b) \leq |a| + |b|$$

Oof! Now we can write it up.

Proof. Let $a, b \in \mathbb{R}$. Either $(a+b) \geq 0$ or $(a+b) < 0$.

- When $(a+b) \geq 0$, we know that $|a+b| = a+b$. By Lemma 5.4.4, we know that $a \leq |a|$ and $b \leq |b|$. Thus $|a+b| = a+b \leq |a| + |b|$.
- When $(a+b) < 0$, we have $|a+b| = -a-b = (-a)+(-b)$. Again, by Lemma 5.4.4 $-a \leq |-a| = |a|$ and $-b \leq |-b| \leq |b|$, and so $|a+b| = -(a+b) = (-a)+(-b) \leq |a|+|b|$.

In both cases we have that $|a+b| \leq |a| + |b|$ as required. ■

This is not the only way to prove this result. We can be a little more sneaky via the inequality in Lemma 5.4.5.

Another proof. Let $x, y \in \mathbb{R}$. Then from Lemma 5.4.4we know that $x \leq |x|$, and that $-x \leq |-x| = |x|$, and hence $x \geq -|x|$. Putting those together we have

$$-|x| \leq x \leq |x|$$

Similarly, we know that $-|y| \leq y \leq |y|$. Adding these inequalities together gives

$$-|x| - |y| \leq (x+y) \leq |x| + |y|$$

and so, by Lemma 5.4.5 above

$$|x+y| \leq |x| + |y|$$

as required. ■

A useful corollary of the triangle inequality is a bound on the absolute value of the difference of two numbers. This is often called the reverse triangle inequality.

Corollary 5.4.7 Reverse triangle inequality. *Let $x, y \in \mathbb{R}$ then*

$$|x-y| \geq \Big| |x| - |y| \Big|$$

Proof. From the triangle inequality $|x| + |y| \geq |x+y|$ we can arrive at the following two inequalities, by setting $x = a, y = b-a$ and $x = b, y = a-b$

$$|a| + |b-a| \geq |b|$$
$$|b| + |a-b| \geq |a|$$

Rearranging these gives

$$|b-a| \geq |b| - |a|$$

and $|b| - |a| \geq -|a - b|$, which can be rewritten as

$$-(|b| - |a|) \leq |b - a|$$

Putting these together gives

$$-(|b| - |a|) \leq |b - a| \leq |b| - |a|$$

from which the result follows. ■

5.5 Exercises

1. Let $n \in \mathbb{Z}$. Prove that if $n^2 + 4n + 5$ is odd, then n is even.

2. Let $n \in \mathbb{Z}$. Show that if $5 \nmid n^2$, then $5 \nmid n$.

3. Let $n \in \mathbb{Z}$. Prove that if $5 \nmid n$ or $2 \nmid n$, then $10 \nmid n$.

4. Let $n, m \in \mathbb{N}$. Prove that if $n \neq 1$ and $n \neq 2$, then $n \nmid m$ or $n \nmid (m + 2)$.

5. Let $n, m \in \mathbb{Z}$. Prove that if $n^2 + m^2$ is even, then n, m have the same parity.

6. Let $x \in \mathbb{R}$. Show that if $x^3 + 5x \geq x^2 + 1$, then $x > 0$.

7. We say that the pair of numbers a, b are consecutive in the set S when $a < b$ and there is no number $c \in S$ so that $a < c < b$. That is, the number b is the next number in the set after a. For example:

- 5 and 6 are consecutive integers.
- 10 and 12 are consecutive even numbers.
- 25 and 30 are consecutive multiples of 5.

Prove the following statement:
Let $a, b \in \mathbb{Z}$. If $a + b$ is not odd, then a and b are not consecutive.

8. Prove that if n is an even integer then $n = 4k$ or $n = 4k + 2$ for some integer k.

9. Let $n \in \mathbb{Z}$. Show that $2 \mid (n^4 - 7)$ if and only if $4 \mid (n^2 + 3)$.

10. Let $a \in \mathbb{Z}$. Prove that $3 \mid 5a$ if and only if $3 \mid a$.

11. Let $n \in \mathbb{Z}$. Show that $(n^2 - 1)(n^2 + 2n)$ is divisible by 4.

12. Prove the following statement:
If $x + y$ is odd, then either x or y is odd, but not both.

13. Let $n \in \mathbb{Z}$. Prove that if $3 \mid (n^2 + 4n + 1)$, then $n \equiv 1 \pmod 3$.

14. Let $m \in \mathbb{Z}$. Prove that if $5 \nmid m$, then $m^2 \equiv 1 \pmod 5$ or $m^2 \equiv -1 \pmod 5$.

15. Let $q \in \mathbb{Z}$. If $3 \nmid q$, then $q^2 \equiv 1 \pmod 3$.

16. Prove that if $n \in \mathbb{Z}$, then the sum $n^3 + (n + 1)^3 + (n + 2)^3$ is divisible by 9.

17. Prove that $\forall a \in \mathbb{Z}$, $a^5 \equiv a \pmod 5$.

18. Without using the triangle inequality, prove that if $x \in \mathbb{R}$, then $|x+4| + |x-3| \geq 7$.

19. Let $x \in \mathbb{R}$. Show that if $|x-1| < 1$, then $|x^2 - 1| < 3$. You may use the following result without proof:

$$|ab| = |a| \cdot |b| \text{ for any } a, b \in \mathbb{R}.$$

20. Let $x \in \mathbb{R}$. Show that if $|x-2| < 1$, then $|2x^2 - 3x - 2| < 7$. You may use the following result without proof:

$$|ab| = |a| \cdot |b| \text{ for any } a, b \in \mathbb{R}.$$

21. Prove the reverse triangle inequality. That is, given $x, y \in \mathbb{R}$, prove

$$|x-y| \geq \big||x| - |y|\big|.$$

22. We say that a function f is *decreasing* on its domain D if for all $x, y \in D$, whenever $x \leq y$, we have $f(x) \geq f(y)$. Explain why the following statement is false:

Let $f : \mathbb{R} - \{0\} \to \mathbb{R}$ be defined by $f(x) = 1/x$. Then f is decreasing.

Rewrite the statement to make it true by changing the domain of the function f. Then prove your statement.

Chapter 6

Quantifiers

The authors of this text have aimed to get you started proving things as quickly as possible. This meant that we had to skip over several important topics and return to them later. That is why the text has bounced between logic and proof and logic and proof, and now we return one last time to logic.

The first result we really proved in this text (way back at Result 3.2.7) was

$$(n \text{ is even}) \implies (n^2 \text{ is even}).$$

We approached the proof by thinking about how the implication could possibly be false. That, in turn, led us to assume the hypothesis to be true, and to show that the conclusion could not possibly be false. In so doing, we have hidden something from you, the reader. Sorry, but the authors felt this was a necessary but well-intentioned untruth[46] to achieve their aim of getting you to start proving things as quickly as possible.

Consider the truth-values of hypothesis and conclusion of the above implication carefully. "n is even" and "n^2 is even" are *not* a statement, they are both **open sentences**[47] whose truth values depend on the variable n. We have hidden from you, our reader, is the implicit scope on the variable n. We implied that we want this result to be true *every possible integer* n. To make this implicit explicit:

$$\text{For every integer } n, (n \text{ is even}) \implies (n^2 \text{ is even}).$$

The effect of that extra bit of text is to provide *scope* to the variable n, and so turns the open sentence into a statement with a well-defined truth value. And once we have a statement we can try to prove it.

6.1 Quantified statements

Let us now go back to sentences like

$$x^2 - 5x + 4 = 0.$$

[46] A teenie-tiny one.

[47] The reader who has momentarily forgotten the difference between **statement** and **open sentence** should quickly jump back to Chapter 2

We were unable to assign a truth value to this statement because we had no information about x. It is clear that this sentence is true for some values of x and false for others:

- If $x = 0$ the sentence makes sense but is false.
- If $x = 1$ the sentence makes sense and is true.
- If x is the colour blue, then it doesn't even make sense.

We can write the open sentence above as

$$P(x) : x^2 - 5x + 4 = 0$$

Now we can express things in a more compact (and a little more abstract) way: $P(0)$ is false, while $P(4)$ is true.

Just as Result 3.2.7 was a statement about integers, we might choose to study the open sentence over, say, the set $S = \{0, 1, 2, 3, 4\}$. In this case we would analyse the truth-values of $P(x)$ over the **domain**[48] S. Checking carefully we find that

$P(1), P(4)$ are true and $P(0), P(2), P(3)$ are false.

Such lists are going to become very cumbersome over big domains, let alone infinite[49] domains. However, we could summarise that list by saying that the statement is true sometimes, but not true always. To be a little more precise:

- $P(x)$ is true for some $x \in S$, and
- $P(x)$ is not true for all $x \in S$.

Notice that the extra bits of text "for some $x \in S$" and "for all $x \in S$" place restrictions which values of x we take, and so turn the open sentences into statements. With that extra text we can now assign truth values.

To be even more careful, we can write the above as

- There exists $x \in S$ so that $x^2 - 5x + 4 = 0$, and
- For all $x \in S$, $x^2 + 5x - 4 = 0$

where the first is now a true statement, and the second is a false statement. The extra bits "For all" and "There exists" are called **quantifiers**.

Definition 6.1.1 We typically work with two quantifiers in mathematics — the **universal quantifier** and the **existential quantifier**.

- The **universal quantifier** is denoted $\forall$ and is read as "for all" or "for

[48]Again, this terminology is reminiscent of functions.

[49]Actually we cannot even construct such lists over some types of infinite domains — see Chapter 12.

every". The statement

$$\forall x \in A, P(x)$$

is true provided $P(x)$ is true for every single value of $x \in A$ and otherwise the statement is false.

- The **existential quantifier** is denoted $\exists$ and is read as "there exists". The statement

$$\exists x \in A \text{ so that } P(x)$$

is true provided there is at least one value of $x \in A$ so that $P(x)$ is true, and otherwise the statement is false.

◊

Other quantifiers? Sometimes in mathematics we also use the **unique existential quantifier** to indicate that there exists one and only one object of interest. It is sometimes denoted $\exists!$. For example, "the equation $n^3 = -1$ has exactly one solution over the integers". We won't use this particular type of quantifier very often in this course.

Note that one can express the unique existential quantifier in terms of the usual existential quantifier. The interested reader should play around to work out how to do this, or just search-engine their way to it.

The unique existential quantifier is not alone; one can construct an infinite family of quantifiers of the form, "there are exactly 2…", "there are exactly 3…", etc. Further one can also consider quantifiers such as "for all but one", or "for all but a finite number"

Back to our two statements above. We can now write them as

- "$\exists x \in S$ such that $x^2 - 5x + 4 = 0$" or "$\exists x \in S$ s.t. $x^2 - 5x + 4 = 0$".
- "For every $x \in S, x^2 - 5x + 4 = 0$" or "$\forall x \in S, x^2 - 5x + 4 = 0$"

Remark 6.1.2 Punctuation please. Be careful to punctuate these statements nicely — make sure that it is clear to the reader where the quantifier stops and the open sentence begins. In the case of for-all statements we usually just place a comma:

$$\underbrace{\forall x \in S}_{\text{quantifier}} \quad \underbrace{,}_{\text{punctuation}} \quad \underbrace{P(x)}_{\text{open sentence}}$$

For there-exists statements we write in "so that" or "such that", since that is how the statements are typically read. Your busy hard-working mathematician will contract the "so that" to "s.t.":

$$\underbrace{\exists x \in S}_{\text{quantifier}} \quad \underbrace{\text{s.t.}}_{\text{punctuation}} \quad \underbrace{P(x)}_{\text{open sentence}}$$

It is also generally considered bad style to use $\exists$ and $\forall$ in sentences in place of "there exists" and "for all". Mind you, that doesn't stop people doing it, but in general, it is okay to do in a mathematical statement or equation, but you should avoid writing them in the middle of paragraphs (except in scratch work).

Quantifiers are often a point of confusion for students. This can be exacerbated by the number of different ways they can be expressed in written or spoken languauge. For example, the statement "$\exists x \in A$ s.t. $P(x)$" can be read as

- There exists x in A so that $P(x)$ is true.
- There is x in A so that $P(x)$ is true.
- There is at least one x in A so that $P(x)$ is true.
- $P(x)$ is true for at least one value of x from A
- We can find an x in A so that $P(x)$ is true.
- We can always find an x in A that makes $P(x)$ is true.
- At least one x in A exists so that $P(x)$ is true.
- ...

The above is just what the author thought of in a couple of minutes.

Similarly, the statement "$\forall x \in A, P(x)$" can be read in many ways:

- For all x in A, $P(x)$ is true.
- For every x in A, $P(x)$ is true.
- No matter which x we choose from A, $P(x)$ is true.
- Every single x in A makes $P(x)$ true.
- $P(x)$ is true for every x in A.
- Every choice of x from A makes $P(x)$ true.
- All the x in A makes $P(x)$ true.
- ...

Oof!

We need to add one more to the list of ways to read $\forall x \in A, P(x)$:

- If x is in A then $P(x)$ is true.

This is critically important, because it shows us a link between the universal quantifier and the implication. It shows us that:

$$(\forall x \in A, P(x)) \equiv (x \in A \implies P(x))$$

Thankfully it is not too hard to see why — think about their truth values.

- $\forall x \in A, P(x)$ is true provided $P(x)$ is true for every single x from A. It is false if we can find at least one value of x from A so that $P(x)$ is false.

- On the other hand, the implication $x \in A \implies P(x)$, is false when the hypothesis is true, but the conclusion is false. That is, we can find a value of $x \in A$ so that $P(x)$ is false. Otherwise the implication is true.

More generally when we have a statement like

> If n is even then n^2 is true.

there is an implicit assumption that we actually mean

> For all n, if n is even then n^2 is even.

So it is typically understood that when we write

$$P(x) \implies Q(x)$$

the reader should really read this as

$$\forall x, P(x) \implies Q(x)$$

Of course, we don't really mean for every single possible value of the variable x taken from the set of all possible things in this and every other universe. We actually mean

$$\forall x \in A, P(x) \implies Q(x)$$

where the set A is often inferred by context. So when we are talking about even and odd numbers (as above), we really mean

> For all integers n, if n is even then n^2 is true.

Typically the context is clear, and so it is is just cumbersome[50] to write "$\forall x \in A, \ldots$" before our statements. When it is *us* doing the writing, *we* can look after our reader and try to make sure the context is clear. To this end, a good general rule is:

> If you are worried that the reader might not understand the context or that your statements might be open to misinterpretation, then put in more words and more details.

or, to be a little more to the point:

> If in doubt, put in more details.

Time for a simple example (we'll do more complicated ones in the next section).

Example 6.1.3 Let $P(n)$ be the open sentence "$(7n - 6)/3$ is an integer." over

[50] And tedious for the hard-working time-pressed mathematician.

the domain $\mathbb{Z}$. Explain whether the following statements are true

$$\exists n \in \mathbb{Z} \text{ s.t. } P(n)$$
$$\forall n \in \mathbb{Z}, P(n)$$

Solution. Let us think about each in turn.

- In order for this to be true we need to find at least one integer n that makes $P(n)$ to be true. For example, setting $n = 0$ gives

  $$P(0) : -2 \text{ is an integer}$$

  which is true.

  Since we have found at least one value of n to make the open sentence true, the statement is true.

- In order for the second statement to be true, no matter which integer n we choose, the statement $P(n)$ is true. However, if we pick $n = 1$ then

  $$P(1) : \frac{1}{3} \text{ is an integer}$$

  which is clearly false.

  Since we cannot pick whatever integer n we want, and still have $P(n)$ true, it follows that the statement is false. To be more precise, it is false because there is some n so that $P(n)$ is false. In symbols this is:

  $$\exists n \in \mathbb{Z} \text{ s.t. } \sim P(n).$$

□

Notice that in the case of the second statement in the above exercise, we have shown the statement to be false, by demonstrating that its **negation** is true. This brings us to negating quantifiers.

6.2 Negation of quantifiers

This last example brings us to the negation of quantifiers. This isn't difficult, but we should still be careful. Consider the statement

$$\forall n \in \mathbb{N}, n^2 + 1 \text{ is prime.}$$

In order for this to be true, we require that no matter which natural number n, the number $n^2 + 1$ is prime.

$$n = 1 \qquad 1^2 + 1 = 2 \text{ which is prime.}$$
$$n = 2 \qquad 2^2 + 1 = 5 \text{ which is prime.}$$

$$n = 3 \qquad 3^2 + 1 = 10 = 2 \times 5 \text{ is not prime.}$$

Since it fails when $n = 3$, the statement is false.

Think carefully about what we have actually done here. We showed that this statement is false, by demonstrating that we could find $n \in \mathbb{N}$ so that $n^2 + 1$ is not prime. That is, we proved that the statement

$$\exists n \in \mathbb{N} \text{ s.t. } n^2 + 1 \text{ is not prime}$$

is true. What we are really doing here is proving that our original statement is false, by demonstrating that the negation of that statement is true.

Now consider the statement

$$\exists n \in \mathbb{N} \text{ s.t. } n^2 < n$$

You can convince yourself that this is false just by plugging in a few numbers or by drawing some graphs. However *convincing* is not the same as *proving*. In order for this to be false, we need to show that no matter which $n \in \mathbb{N}$ we choose, $n^2 \geq n$. That is, we have to show that

$$\forall n \in \mathbb{N}, n^2 \geq n.$$

We'll do that shortly. But again, we are showing that the original is false by proving the negation to be true.

Notice that our first statement was

$$\forall n \in \mathbb{N}, P(n)$$

and we showed that it was false by proving that

$$\exists n \in \mathbb{N} \text{ s.t. } \sim P(n)$$

is true. And similarly, our second statement was

$$\exists n \in \mathbb{N} \text{ s.t. } Q(n)$$

and to prove it false, we have to show that

$$\forall n \in \mathbb{N}, \sim Q(n)$$

is true.

More generally, when we negate a "for all" we get "there exists" and when we negate "there exists" we have "for all". This is a very important result and we'll summarise it by a theorem.

Theorem 6.2.1 *Let $P(x)$ be an open sentence over the domain A, then*

$$\begin{aligned} \sim (\forall x \in A, P(x)) &\equiv \exists x \in A \text{ s.t. } \sim (P(x)) \\ \sim (\exists x \in A \text{ s.t. } P(x)) &\equiv \forall x \in A, \sim (P(x)) \end{aligned}$$

Note that the negated statement still has the same ***domain****.*

Warning 6.2.2 The domain remains. An extremely common error to make is to assert that

$$\begin{aligned} \sim (\forall x \in A, P(x)) &\equiv \underbrace{\forall x \notin A}_{\text{bad!}} \text{ s.t. } P(x) && \text{do not do this} \\ &\equiv \underbrace{\exists x \notin A}_{\text{also bad!}} \text{ s.t. } P(x) && \text{nor this} \end{aligned}$$

These statements are not equivalent. Nor are

$$\sim (\exists x \in A, P(x)) \equiv \underbrace{\exists x \notin A}_{\text{bad!}} \text{ s.t. } P(x) \qquad \text{don't do this either}$$

The domain of the quantifier remains unchanged when the statement is negated.

For example, consider the statement

$$\forall n \in \mathbb{N} \text{ s.t. } n \geq 0.$$

This is definitely true; every natural number is non-negative. Because of this, the negation of the above must be false. However, if we were to *incorrectly* compute the negation as

$$\exists n \notin \mathbb{N}, n < 0$$

then we have a problem. Since the number $n = -1$ is not a natural number, and is less than 0, the above is also true. So remember

> The domain of a quantified statement does not change when it is negated.

Let us do a couple of simple examples and we'll get to more difficult ones in the next section.

Example 6.2.3 Determine whether or not the following statements are true or false and then prove your answer.

a $\exists n \in \mathbb{Z}$ s.t. $\frac{n+7}{3} \in \mathbb{Z}$.

b $\exists n \in \mathbb{Z}$ s.t. $\frac{n^2+1}{4} \in \mathbb{Z}$.

Solution. We tackle each in turn.

a This is true. It suffices to find one example of an integer n so that $\frac{n+7}{3}$ is an integer. Our proof just has do that — notice that it does not have to say how we found the example, just demonstrate that it works.

  Proof. The statement is true. Let $n = 2$. Then $\frac{n+7}{3} = \frac{9}{3} = 3 \in \mathbb{Z}$ as required. ■

b This is a little harder. Notice that the statement is really saying that n^2+1 is divisible by 4. Try a few values of n:

$$n = 1 : \frac{1^2+1}{4} = \frac{2}{4} = \frac{1}{2} \qquad n = 2 : \frac{2^2+1}{4} = \frac{5}{4}$$
$$n = 3 : \frac{3^2+1}{4} = \frac{10}{4} = \frac{5}{2} \qquad n = 4 : \frac{4^2+1}{4} = \frac{17}{4}$$

Not looking promising. Notice it fails both when n is even and n is odd. We can use that to form our proof. Now, we don't directly prove the statement is false, instead we prove the negation is true. So we can start our proof by saying just that.

Proof. The statement is false; we demonstrate this by proving the negation to be true. The negation is

$$\forall n \in \mathbb{Z}, \frac{n^2+1}{4} \notin \mathbb{Z}$$

Assume $n \in \mathbb{Z}$, then n is either even or odd.

- When n is even, we can write $n = 2k$ for some integer k. Then $n^2 + 1 = 4k^2 + 1 = 4(k^2) + 1$. Hence $n^2 + 1$ is not divisible by 4.
- On the other hand, when n is odd, we can write $n = 2k + 1$ for some integer k. Then $n^2 + 1 = 4k^2 + 4k + 2 = 4(k^2 + k) + 2$. Hence $n^2 + 1$ is not divisible by 4.

In either case $\frac{n^2+1}{4}$ is not an integer. Since the negation is true, the original statement is false. ■

□

Example 6.2.4 Determine whether or not the following statements are true or false and then prove your answer.

a $\forall n \in \mathbb{Z}, \frac{n^2+n}{2} \in \mathbb{Z}$.

b $\forall n \in \mathbb{Z}, n^2 - 8n + 1 < 0$.

Solution. We tackle each in turn.

a This one is quite similar to the second statement in the previous example. It is actually true, and we can leverage the parity of n to get the result we need.

Proof. The statement is true. Let $n \in \mathbb{N}$, then n is even or odd.

- When n is even, $n = 2k$ for some $k \in \mathbb{Z}$. Hence $n^2 + n = 4k^2 + 2k = 2(2k^2 + k)$ and so is even.

- When n is odd, $n = 2k + 1$ for some $k \in \mathbb{Z}$. Hence $n^2 + n = 4k^2 + 6k + 2 = 2(2k^2 + 3k + 1)$ and so is even.

Since in both cases $n^2 + n$ is even, it is divisible by 2. The result follows. ■

Alternatively, we might try to prove the result by noticing that $n^2 + n = n(n + 1)$ is the product of successive integers. Hence one if $n, n + 1$ must be even, and the product of any integer and an even number is even, so the result must be even. That would work, excepting that we have not actually proved that "product of any integer and an even number is even". Its not a hard result, but we should prove it before using it.

b If we just try plugging in a few small integers, the result holds. However, we know that n^2 gets bigger much faster than n does, so the result should be false when n is big. Consequently we can show it is false by just plugging in a sufficiently large value of n.

Proof. The result is false. We prove that the negation is true. The negation is

$$\exists n \in \mathbb{Z}, n^2 - 8n + 1 \geq 0.$$

Let $n = 10$ then $n^2 - 8n + 1 = 100 - 80 + 1 = 21 \geq 0$ as required. Since the negation is true, the original statement is false. ■

□

6.3 Nested quantifiers

Example 6.3.1 Rewrite the following using quantifiers, and then write out their negations.

- There is a real number y such that $1/y = y + 1$.
- For every integer z there is a natural number w such that $z^2 < w$.

Solution. Translating the statements into symbols gives

- $\exists y \in \mathbb{R}$ s.t. $1/y = y + 1$
- $\forall z \in \mathbb{Z}, \exists w \in \mathbb{N}$ s.t. $z^2 < w$

The negations are then:

$$\begin{aligned} \sim (\exists y \in \mathbb{R} \text{ s.t. } 1/y = y + 1) &\equiv \forall y \in \mathbb{R} \text{ s.t. } \sim (1/y = y + 1) \\ &\equiv \forall y \in \mathbb{R} \text{ s.t. } 1/y \neq y + 1. \end{aligned}$$

and

$$\sim (\forall z \in \mathbb{Z}, \exists w \in \mathbb{N} \text{ s.t. } z^2 < w) \equiv \exists z \in \mathbb{Z} \text{ s.t. } \sim (\exists w \in \mathbb{N} \text{ s.t. } z^2 < w)$$

$$\equiv \exists z \in \mathbb{Z} \text{ s.t. } \forall w \in \mathbb{N}, \sim (z^2 < w)$$
$$\equiv \exists z \in \mathbb{Z} \text{ s.t. } \forall w \in \mathbb{N}, z^2 \geq w.$$

Notice how we can slide the negation from left to right, and along the way $\forall$ becomes $\exists$ and $\exists$ becomes $\forall$. And, of course, the domains are unchanged by negation. □

The first statement is, in plain(er) english

> You can pick some real number y to make $1/y = y + 1$.

In writing it in this way, the authors have tried to take a mathematical statement into an exercise for the reader. "You — dear reader — can find (go on!) some real number y that has the property that $1/y$ is equal to $1 + y$". Similarly, we can write the statement $\forall z \in \mathbb{R}, z^2 \geq 0$ as

> No matter which real number z you pick, z^2 is non-negative.

Again, we have made this into an exercise for the reader. "You — dear reader — can pick any value of z you want, it will always turn out that $z^2 \geq 0$." So far, nothing too controversial, but lets move on to the second example above since it contains nested quantifiers. But a warning first.

Warning 6.3.2 Quantifiers do not commute. Nested quantifiers do not commute. The statement

$$\forall x, \exists y \text{ s.t. } P(x, y)$$

is not logically equivalent to

$$\exists y \text{ s.t. } \forall x, P(x, y).$$

The second example above contains nested quantifiers. Let us work through it slowly and carefully by writing it as a task for the reader.

> No matter which $z \in \mathbb{Z}$ you pick, there is a choice of $w \in \mathbb{N}$ so that $z^2 < w$.

This statement is true. To see why, we should think of it as a 2-player game. Player 1 picks any z they want, and Player 2 has to choose a value of w so that $z^2 < w$. Player 1 goes first and Player 2 goes second.

- Player 1 picks some integer z.
- Player 2 knows the value of z and can make their choice accordingly. With a little thought, Player 2 realises that choosing $w = z^2 + 1$ will work nicely (though they should be careful to make sure their choice is from the correct domain).

This is then the basis for proving the statement is true.

Proof. Let $z \in \mathbb{Z}$. Then choose $w = z^2 + 1$. Since $z \in \mathbb{Z}$ we know that w is a positive integer and so $w \in \mathbb{N}$. Then $z^2 < z^2 + 1 = w$. Hence the statement is true. ■

What if we reverse the order of the quantifiers?

$$\exists w \in \mathbb{N} \text{ s.t. } \forall z \in \mathbb{Z}, z^2 < w.$$

Again, we translate this into an exercise for the reader

> You can choose some $w \in \mathbb{N}$, so that no matter what integer z is then chosen, $z^2 < w$.

This is false. Player 1 now has to pick w first, and Player 2 picks z second. Player 1 knows nothing about what Player 2 is going to do. So Player 1 might think "I'll pick a really big number, say $w = 100$", but then Player 2 knows this value of w and can just pick a large value of z.

The best way (arguably) to prove the statement false, is to show that its negation is true. So a **disproof** of the statement is just a proof of the negation of the statement. So write down the negation:

$$\forall w \in \mathbb{N}, \exists z \in \mathbb{Z} \text{ s.t. } z^2 \geq w.$$

and again write it as a task for the reader:

> No matter which $w \in \mathbb{N}$ you pick, there will always be some choice of $z \in \mathbb{Z}$ so that $z^2 \geq w$.

Again, Player 1 goes first and Player 2 goes second. Player 1 knows nothing about what Player 2 will do, but Player 2 knows what Player 1 did.

- Player 1 picks some $w \in \mathbb{N}$.
- Player 2 knows the value of w, and then (after some thought) picks $z = w+1$

It is now sufficient to check that Player 2 has chosen z from the correct domain, and that $z^2 = (w^2 + 2w + 1) \geq w$ (which it is since $w \geq 1$).

Proof. The original statement is false, so we prove the negation to be true. The negation is

$$\forall w \in \mathbb{N}, \exists z \in \mathbb{Z} \text{ s.t. } z^2 \geq w.$$

Let $w \in \mathbb{N}$ and then choose $z = w+1$. Since $w \in \mathbb{N}$, we know that $z \in \mathbb{Z}$. Further since $w \geq 1$ we know that

$$z^2 = (w+1)^2 = w^2 + 2w + 1 = (w^2 + w + 1) + w \geq w$$

as required. Since the negation is true, the original is false. ■

Remark 6.3.3 Context and dropping domain. Mathematicians sometimes are a little sloppy with the way they write quantifiers, especially when the domain of those quantifiers is known by context. For example, if we are doing calculus, then most of our variables will be real numbers, while if we are working on a number theory problem, then our variables are likely to be integers. If the context is clear the domains will often be dropped.

So one might see the statement

$$\begin{aligned} \forall x \in \mathbb{R}, \text{ if } x < -2 \text{ then } x^2 > 4 &\qquad \text{written as} \\ \forall x, \text{ if } x < -2 \text{ then } x^2 > 4 &\qquad \text{or even as} \\ \text{if } x < -2 \text{ then } x^2 > 4 & \end{aligned}$$

In this last statement we have dropped the quantifier completely. The universal quantifier is implicit — the statement has to be true for all x in the domain. So, when you see an implication

$$P(x) \implies Q(x)$$

it is really

$$\forall x, \ P(x) \implies Q(x).$$

Your hard-working time-pressed mathematician has just dropped a couple of symbols to save time. This is a little sloppy, but really quite standard.

When students encounter nested quantifiers for the first time they typically find them quite difficult. They are quite difficult but they do become easier with practice. Accordingly, the following example is one of this author's favourites. It, and its kin, have appeared on nearly every exam the author has given for this topic. The author's students are likely to have chosen a different type of question as their favourite. We will provide lots of similar exercises for you — dear reader — to practice, so that any dislike of nested quantifiers can be dispelled.

Example 6.3.4 Consider the following four statements:

(a) $\exists x \in \mathbb{R}$ s.t. $\exists y \in \mathbb{R}$ s.t. $xy = x + y$

(b) $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}, xy = x + y$

(c) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $xy = x + y$

(d) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, xy = x + y$.

Determine the truth value of the following four statements and prove your answers.

We will work through the statements in order, thinking about them as two-player games as we did above. We will also drop "$\in \mathbb{R}$" from the quantifiers; the reader should understand, by context, that all our variables are selected from $\mathbb{R}$.

Finally — remember to be careful of the order of the quantifiers.

Scratchwork.

(a) This is true.

- Player 1 only has to choose one number. They choose $x = 0$.
- Player 2 only has to choose one number and they know Player 1's choice. So they also choose $y = 0$

Then $xy = 0 = 0 + 0 = x + y$.

(b) Again think about the 2 players:

- Player 1 gets to choose only one number x
- Player 2 then has to be able to choose any real number y so that the equation holds.

This feels unlikely to work because we can "solve" the equation for y to get $y = \frac{x}{x-1}$. That is, for any given x-value there is going be exactly one y-value. So it feels like it will likely be false.

To see that it *is* false, write down the negation:

$$\forall x, \exists y \text{ s.t. } xy \neq x + y.$$

- Player 1 can choose any real number x they want.
- Player 2 then has to be able to choose a real number y so that $xy \neq x + y$. A good choice is $y = 1$ (though there are infinitely many other good choices)

Now no matter what x-value, $xy = x$ and $x + y = x + 1$, and $x \neq x + 1$. We just have to write it up.

(c) This one is a bit tricky. Again, think about our two players.

- Player 1 chooses whatever x-value they feel like.
- Player 2 knows that value of x and based on that has to make a very careful choice of y. But that just requires Player 2 to solve $x + y = xy$. Easy!

$$\begin{aligned} x + y &= xy \\ y - xy &= -x \\ y &= \frac{-x}{1-x} = \frac{x}{x-1} \end{aligned}$$

All good? Not quite — things go wrong when $x = 1$.
When $x = 1$, our equation is $y + 1 = y$. There is no real number y that makes that true.

So everything seemed fine until we considered $x = 1$. So perhaps it is false?

You know the drill now; write down the negation and think about our two players:

$$\exists x \text{ s.t. } \forall y, xy \neq x + y.$$

- Player 1 makes a single careful choice of $x = 1$
- Then no matter what y-value Player 2 chooses, $xy = y$ and $x+y = y+1$, so $xy \neq x + y$.

So it is false. We just need to write out the proof.

(d) This one is also false, and it is easy to see why from the negation:

$$\exists x \text{ s.t. } \exists y \text{ s.t. } xy \neq x + y.$$

It suffices for Player 1 to pick $x = 1$, and Player 2 to then pick $y = 1$. Then $xy = 1$ and $x + y = 2$.

Solution.

Proof. The statement is true. Pick $x = y = 0$ then $xy = 0$ and $x + y = 0$. ■

We give two proofs of (b), depending on how we choose y.

Proof. We prove this to be false by showing the negation is true. The negation is

$$\forall x, \exists y \text{ s.t. } xy \neq x + y.$$

Pick any $x \in \mathbb{R}$, and then set $y = 1$. Since $xy = x$ and $x + y = x + 1$, we have that $xy \neq x + y$ as required. Since the negation is true, the original statement is false. ■

Proof. The statement is false. Let x be any real number. Then either $x = 0$ or $x \neq 0$.

- When $x = 0$ set $y = 1$. Then $xy = 0$ and $x + y = 1$.
- When $x \neq 0$ set $y = 0$. Then $xy = 0$ and $x + y = x$.

In both cases $xy \neq x + y$ as required. ■

Proof. The statement is false. We prove the negation

$$\exists x \text{ s.t. } \forall y, xy \neq x + y.$$

is true. Pick $x = 1$, then no matter what y is chosen, $xy = y$ and $x + y = y + 1$, and Consequently $y \neq y + 1$. Since the negation is true, the original statement is false. ■

Proof. The statement is false. We prove the negation:

$$\exists x \text{ s.t. } \exists y \text{ s.t. } xy \neq x + y.$$

Pick $x = 1$ and $y = 1$, then $xy = 1$ and $x + y = 2$. Since the negation is true, the original is false. ■

□

I hope the reader can see why the above example makes for a good exam question. It is a good mathematical and logical workout. With that in mind, we (and the author really means you) should do another one. But before we leap into another fun example, a quick warning about negating implications:

Warning 6.3.5 Common implication errors. Remember that

$$\sim (P \implies Q) \quad \equiv \quad (P \wedge \sim Q).$$

The negation of $P \implies Q$ is ***definitely not***

$$\underbrace{(P \implies \sim Q)}_{\text{bad!}} \qquad \text{don't do this!}$$

This is a surprisingly common error. Please memorise Theorem 4.2.7.

It's also important to remember that:

- if the hypothesis of an implication is false, the implication is true, and
- if the conclusion of an implication is true, the implication is true.

On with the fun!

Example 6.3.6 Determine the truth value of the following four statements and prove your answers.

- $\exists x \in \mathbb{R}$ s.t. $\exists y \in \mathbb{R}$ s.t. $(y \neq 0) \implies xy = 1$
- $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}, (y \neq 0) \implies xy = 1$
- $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $(y \neq 0) \implies xy = 1$
- $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, (y \neq 0) \implies xy = 1$

Remember that we must pick the value of x before we pick the value of y in every single case. You might find it helpful to write out the negations before deciding how to approach these.

Scratchwork.

(a) As suggested, we'll write out the negation:

$$\forall x, \forall y, (y \neq 0) \wedge (xy \neq 1)$$

where we have dropped the "$\in \mathbb{R}$", assuming the reader will understand by context.

Now, in order to make an implication true, we just have to make the hypothesis false and that is quite easy in this case. Pick any x you want and then choose $y = 0$. That's enough to make a proof (it also gives us a hint for one of the other statements).

(b) Consider the original statement and what our two players have to do.

- Player 1 has to choose some x
- Now, no matter what Player 2 picks, the implication must be true.

Let us assume Player 1 has chosen some x we don't know what it is yet, but let us assume they have chosen it. What can player 2 do to make the implication true. There are three ways to make it true: (hypothesis, conclusion) = (T,T), (F,T), (F,F). When Player 2 picks $y = 0$, the hypothesis is false making the implication true. However, when they pick something else, the conclusion is only true when $y = 1/x$. But this means for every other choice of y, the conclusion will be false. It really looks like this statement is false.

Time to think about the negation:

$$\forall x, \exists y \text{ s.t. } (y \neq 0) \wedge (xy \neq 1)$$

What do our players do?

- Player 1 can pick whatever x they like, so they do.
- Player 2 knows the value of x and so can choose y to make the conjunction true. In particular, if Player 1 picked $x = 0$, then Player 2 can choose $y = 1$. On the other hand, if Player 1 picked any other value of x, then Player 2 can choose $y = -x$.

In both cases, $y \neq 0$ and $xy = 0$ or $xy = -x^2 \neq 1$. Now just write it up!

(c) Think about our two players.

- Player 1 can pick any x they want.
- Player 2 just needs to make the implication true by careful choice of y. By choosing $y = 0$ they can make the hypothesis false.

Since Player 2 can always make the hypothesis false, the implication is true.

(d) Last one. Oof.

Again, let us think about our two players.

- Player 1 picks whatever x they want
- Player 2 picks whatever y they want.

So, no matter what x was chosen, when Player 2 chooses $y = 0$, the implication is true. But what about all the other choices? This feels unlikely.

Look at the negation:

$$\exists x \text{ s.t. }, \exists y \text{ s.t. } (y \neq 0) \wedge xy \neq 1$$

Ah - this is much easier. Player 1 can choose $x = 0$ and Player 2 can choose $y = 1$. Then $y \neq 0$ and $xy = 0 \neq 1$. There are, many other choices that would also work.

Solution.

Proof. The statement is true. Take $x = 0, y = 0$. Since the hypothesis is false, the implication is true. ■

Proof. The statement is true. Take $x = y = 2$, then the hypothesis and conclusion are both true, so the implication is true. ■

Proof. The statement is false, so we prove the negation:

$$\forall x, \exists y \text{ s.t. } (y \neq 0) \wedge (xy \neq 1)$$

Let x be any real number. Then either $x = 0$ or $x \neq 0$.

- If $x = 0$ then pick $y = 1$. Then $xy = 0$
- On the other hand, if $x \neq 0$ then pick $y = -x$, so that $xy = -x^2$

In both cases, $y \neq 0$ and $xy \neq 1$. Since the negation is true, the original statement is false. ■

Proof. We prove the negation. Let x be any real number. Either $x = 1$ or $x \neq 1$. If $x = 1$ then pick $y = 2$, so that $xy = 2$. On the other hand, if $x \neq 1$, then pick $y = 1$ so that $xy = x \neq 1$. In both cases we have that $y \neq 0$ and $xy \neq 1$ as required. Since the negation is true, the original is false. ■

Proof. The statement is true. Let x be any real number and then choose $y = 0$. Since the hypothesis is false, the implication is true. ■

Proof. Let x be any real number. Either $x = 0$ or $x \neq 0$. If $x = 0$ then pick $y = 0$ making the hypothesis false. On the other hand, if $x \neq 0$ then set $y = \frac{1}{x} \neq 0$. In that case both the hypothesis and conclusion are true. In either case the implication is true. ■

Proof. We prove the negation:

$$\exists x \text{ s.t. }, \exists y \text{ s.t. } (y \neq 0) \wedge xy \neq 1.$$

Pick $x = 0, y = 1$. Then $xy = 0 \neq 1$ and $y \neq 0$. Hence the negation is true and the original statement is false. ■

□

6.4 Quantifiers and rigorous limits

Quantifiers appear all over mathematics, and it is essential that you become comfortable reading, understanding and applying them. One particularly important application of quantifiers is to make the notions of limits rigorous. You have[51]

[51]At least we think you should have. The authors are making an assumption about your mathematical education here, and we appologise if you have, in fact, not encountered limits before now.

encountered the idea of a **limit** when you studied differential calculus; the idea that the value of a function gets "closer and closer" to a particular value as we take the argument of that function "closer and closer" to (say) zero. Quantifiers allow us to make "closer and closer" rigorous[52]. We will start with the idea of the limit of a sequence, and then move on to limits of functions. So we begin with the definition of a sequence.

6.4.1 Convergence of sequences

Definition 6.4.1 A **sequence** is an ordered list of real numbers. It is typically denoted

$$(x_n)_{n\in\mathbb{N}} = (x_1, x_2, x_3, \dots)$$

The numbers $x_1, x_2, \cdots$ are the **terms** of the sequence. You will also sometimes see alternate notation such as

$$(x_n)_n, \qquad (x_n)_{n\geq 1} \qquad \text{or} \qquad (x_n)$$

In some texts you will also see a sequence denoted with braces, $\{x_n\}$; we will not use that notation to avoid confusion with set notation. ♢

An alternate way to think of a sequence is as a function that takes natural numbers and maps them to real numbers. So, for example, the sequence $\left(\frac{1}{n}\right)_n$ is just the function $f : \mathbb{N} \to \mathbb{R}$ defined by $f(n) = 1/n$. We will come back to functions in Chapter 10. We also note that one can generalise this definition to sequences of other types of numbers or objects, but we will focus on sequences of real numbers.

We will typically define a particular sequence either by giving the first few terms,

$$(x_n) = (2, 3, 5, 7, 11, \dots)$$

or by giving a formula for the n^{th} term in the sequence:

$$(x_n) = \left(\frac{1}{n}\right)$$

ie, the sequence $(1, 1/2, 1/3, 1/4, \dots)$. Just as was the case with defining sets, we must make sure that we give the reader enough information to understand our definition. In this way, giving a formula for the n^{th} term is typically preferred[53].

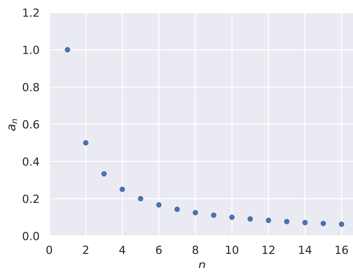
[52]We recommend looking up the history of **infinitesimals** and **fluxions** which predate the rigorous definition of limits we give here. The calculus of Newton and Leibniz used infinitesimals to understand limits and derivatives. These ideas were attacked by Berkeley in his 1734 book "The Analyst" in which he refers to infinitesimals as "the ghosts of departed quantities". The rigorous definition of limits, and so a rigorous foundation for calculus, was given almost 150 years later by Cauchy, Bolzano and Weierstrass. There is much of interest here for a motivated reader with a good search engine. We also recommend a little digression into **surreal numbers**, **hyperreal numbers** and **nonstandard analysis** — things can get pretty weird.

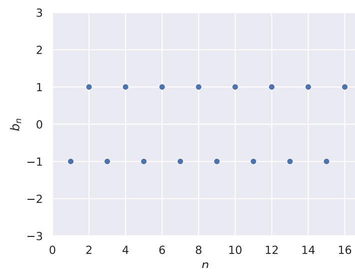
[53]The reader should assume that the sequence $(2, 3, 5, 7, 11, \dots)$ is just the prime numbers, but

Typically one can compute the first few terms of a sequence by hand, and then the next many terms by computer. However, we are very often interested in the behaviour of the terms of the sequence as n becomes very large. So, for example, consider the sequences

$$(a_n) = \left(\frac{1}{n}\right)_n = \left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right)$$
$$(b_n) = ((-1)^n)_n = (1, -1, 1, -1, \dots)$$

Here are plots of the first few terms to see how they behave.





Notice that in the first sequence, as n gets larger and larger, the term a_n gets closer and closer to 0. In this case we will say that "a_n **converges** to 0". In the second case, the sequence simply bounces back and forth between $+1$ and -1 and does not appear to "settle" to any particular value. In this case we will say that "b_n diverges". Let's see how we can turn this intuitive (but imprecise) understanding of convergence and turn it into a rigorous, precise definition.

To start towards that definition, let us rephrase convergence as a sort of two player game as we did for some of the nested quantifier examples earlier in this chapter, and focus on the example of $(a_n) = \left(\frac{1}{n}\right)$. In this game, Player 1 has to choose a small positive number, and then Player 2 has to work out how big does n have to be so that we can guarantee that the distance between a_n and 0 is smaller than Player 1's number. So, for example,

- Player 1 says "Make the distance between a_n and 0 smaller than 0.01."
- Player 2 does some thinking and replies "Choose any $n > 100$ and then it will work."

We can verify this by computing the distance[54] between two numbers using the

a little digging in the Online Encyclopedia of Integer Sequences shows a few other possibilities (some reasonable and some weird) including "partitions" (the number of ways of writing a given integer as a sum of smaller positive integers), "additive primes" (the sum of the digits is also prime), "absolute primes" (every permutation of the digits is also a prime) and lengths of "Farey sequences" (the reader should search-engine this one). Of course, if we are doing a good job as an author then we will have provided the reader with enough context to determine the sequence correctly.

[54]The absolute value is an example of a **metric** or **distance function**. You already know other examples of metrics — for example, the distance between points (x, y) and (z, w) on the Cartesian plane is given by $d = \sqrt{(x-z)^2 + (y-w)^2}$; this is called the Euclidean metric. Another way to compute distances on the Cartesian plane is the taxicab metric $d = |x - z| + |y - w|$. A search-engine will guide you to more on this topic.

absolute value, and then noting that

$$n > 100 \qquad \Longrightarrow \qquad \frac{1}{n} < \frac{1}{100} = 0.01 \qquad \Longrightarrow \qquad \left|\frac{1}{n} - 0\right| < 0.01.$$

This is just one instance, and Player 1 could have chosen 0.01 or 2^{-30}. Indeed, Player 1 can choose ***any arbitrarily small*** positive number ε, and then Player 2 can always work out how big to make n so that the distance between a_n and 0 is guaranteed to be smaller than ε.

- Player 1 says "I have chosen $\varepsilon > 0$, please make the distance between a_n and 0 smaller than ε."
- Player 2 does some thinking and replies "Choose any $n > \frac{1}{\varepsilon}$ and then it will work."

Again, we can verify this:

$$n > \frac{1}{\varepsilon} \qquad \Longrightarrow \qquad \frac{1}{n} < \varepsilon \qquad \Longrightarrow \qquad \left|\frac{1}{n} - 0\right| < \varepsilon$$

That is, Player 2 can set some point in the sequence $N = \frac{1}{\varepsilon}$, so that for every value of $n > N$, we can guarantee that $|a_n - 0| < \varepsilon$. We can rephrase this outcome as

> No matter which $\varepsilon > 0$ that Player 1 chooses, Player 2 can always find some N so that if $n > N$ then $|a_n - 0| < \varepsilon$.

If we now try to play the same game with the second sequence $(b_n) = ((-1)^n)$, then we will quickly see that it does not work. Let us attempt to show that the sequence converges to 1 using the same game

- Player 1 says "Make the distance between b_n and 1 smaller than 0.01."
- Player 2 does some thinking and replies "Well, if n is even then this will be true, but it will fail for every single odd value of n. I cannot give you a guarantee."

Player 2 cannot win. When n is even, $b_n = 1$ and so $|b_n - 1| = 0 < 0.01$, but when n is odd, $b_n = -1$ and so $|b_n - 1| = 2 > 0.01$. So there is no way to make n sufficiently big, ie all n bigger than some N, so that $|b_n - 1| < 0.01$. We can rephrase this outcome as

> There is a choice of ε so that no matter which N Player 2 chooses, there will always be some $n > N$ so that $|b_n - 1| > \varepsilon$.

This example will help us understand how to turn the intuitive idea of convergence into the rigorous definition.

6.4.1.1 Quantifying towards a definition

To start towards our definition, we need to first describe all the objects involved, and then we explain that convergence means that the objects satisfy certain conditions. In this case, we will start with something like

> Let $(x_n)_n$ be a sequence of real numbers, that is, $x_n \in \mathbb{R}$, for all $n \in \mathbb{N}$. Then we say that (x_n) converges to a real number L when …

and now we need to explain those conditions. Let us start with our intuitive idea

> Let $(x_n)_n$ be a sequence of real numbers, that is, $x_n \in \mathbb{R}$, for all $n \in \mathbb{N}$. Then we say that (x_n) converges to a real number L when x_n gets ***closer and closer*** to L as n becomes ***larger and larger***.

While this is quite descriptive, it is not actually all that precise. Let us rewrite it as follows:

> Let $(x_n)_n$ be a sequence of real numbers, that is, $x_n \in \mathbb{R}$, for all $n \in \mathbb{N}$. Then we say that (x_n) converges to a real number L when x_n moves ***arbitrarily close*** to L as n becomes ***larger and larger***.

Now this means that in order for x_n to converge to L, it must be possible to bring the number x_n as close to L as we want by making n really big. This is exactly like the two player game we described above: Player 1 can make any choice of ε and then Player 2 has to work out how large to make n. Let us write our definition again:

> Let $(x_n)_n$ be a sequence of real numbers, that is, $x_n \in \mathbb{R}$, for all $n \in \mathbb{N}$. Then we say that (x_n) converges to a real number L when ***no matter what positive*** ε ***we choose***, then ***for all*** n ***sufficiently large***, we have $|x_n - L| < \varepsilon$.

Now, in our game, Player 2 established just how big n needs so that we can guarantee the sequence terms are close enough to L. We denoted that threshold by N, and it will almost always depend on ε. Of course, since Player 1 chooses ε first, Player 2 can pick N with full knowledge of what Player 1 did. Time for another attempt at the definition:

> Let $(x_n)_n$ be a sequence of real numbers, that is, $x_n \in \mathbb{R}$, for all $n \in \mathbb{N}$. Then we say that (x_n) converges to a real number L when ***for all*** $\varepsilon > 0$, ***there is*** $N \in \mathbb{N}$, so that ***for all natural numbers*** $n > N$ we have $|x_n - L| < \varepsilon$.

This is now pretty good. All that remains is to tweak the phrasing a little, clean it up and make it into a formal definition[55].

[55] This is, more or less, the definition given by Bolzano in 1816.

Definition 6.4.2 Let (x_n) be a sequence of real numbers. We say that (x_n) has a **limit** $L \in \mathbb{R}$ when

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} \text{ s.t. } \forall n \in \mathbb{N}, (n > N) \implies (|x_n - L| < \varepsilon).$$

In this case we say that the sequence **converges** to L and write

$$x_n \to L \qquad \text{or} \qquad \lim_{n\to\infty} x_n = L.$$

If the sequence doesn't converge to any number L, we say that the sequence **diverges**. ♢

6.4.1.2 Some examples

Time to put our newly rigorised[56] understanding of limits to work.

[56]The authors were quite sure that "rigorised" is not a real word and were surprised to find it in the dictionary.

Example 6.4.3 Let $c \in \mathbb{R}$. Show that the constant sequence $(x_n)_{n\in\mathbb{N}} = (c)_{n\in\mathbb{N}}$ converges to c.

Scratchwork. We know, at least intuitively, that the constant sequence must converge to that constant value its elements take. It makes sense. But, how can we prove it rigorously using the definition of sequence convergence.

Again, think of the two player game[57]. We need to show that no matter which $\varepsilon > 0$ that Player 1 chooses, Player 2 can always find a threshold $N \in \mathbb{N}$ (which, in general will depend on ε), so that whenever $n > N$ we have $|x_n - c| < \varepsilon$.

Now assume that Player 1 picked an $\varepsilon > 0$ and try to understand what Player 2 needs to show. They want to show that with the right choice of $N \in \mathbb{N}$, we can keep $|x_n - c| < \varepsilon$. But since x_n constant $x_n = c$, we can simplify the inequality that needs to be satisfied:

$$|x_n - c| < \varepsilon \qquad \text{becomes} \qquad |c - c| = 0 < \varepsilon.$$

But since we know $\varepsilon > 0$, this will be true independent of n. This, in turn, means that Player 2 is free to choose any $N \in \mathbb{N}$. Now Player 2 could be mysterious and pick any random value (eg $N = 98127$) but let's force Player 2 to be a bit nicer to the audience (ie to the reader) and get them to pick a sensible value like $N = 1$. Then for all $n > N = 1$, we have $|x_n - c| = |c - c| = 0 < \varepsilon$ as required.

All that remains is to write this nice and tidy in a proof.

Solution.

Proof. Let $\varepsilon > 0$ be given and pick $N = 1$. Then, for all $n > N$, we have

$$|x_n - c| = |c - c| = 0 < \varepsilon.$$

Therefore we conclude that (x_n) converges to c as required. ■

□

Notice that the proof in our example does not have to explain ***how*** we came up with the choice of N, it merely has to show that it works. Our definition of convergence requires that "there exists N", not that "there exists N with a nice explanation of how it was found". This can sometimes make a nicely written proof seem much more clever than it really is. The reader can be left thinking "How on earth did they know how to choose that?". But you should remember that the author of the proof probably did a lot of careful scratch work to work out how to make the proof nice and neat; that scratch work is not required for the proof to be valid. Of course, if the author knows their audience well, and knows they might need some help, then the author will hopefully leave some explanation in the text nearby.

Example 6.4.4 Show that the sequence $(a_n)_{n\in\mathbb{N}} = (\frac{1}{n})_{n\in\mathbb{N}}$ converges to 0.

Scratchwork. This is precisely the example we did above to introduce the idea of convergence. We have even discussed how to think of proving the convergence

[57] We'll dispense with this analogy soon.

as a two player game. So, let us dispense with the game analogy.

We are going to start by choosing some arbitrary $\varepsilon > 0$, and then we need to find a threshold N so that for every $n > N$, we know that $|a_n - 0| < \varepsilon$. Now, our argument from the previous example won't work here, since $|a_n - 0| = \frac{1}{n}$ is no longer constant and varies with n. Let us try rewriting things a little to help us think.

We've chosen some arbitrary $\varepsilon > 0$, and we need to show that $|a_n - 0| = \frac{1}{n} < \varepsilon$ when n is big enough, ie for $n > N$. But the inequality

$$\frac{1}{n} < \varepsilon \qquad \iff \qquad n > \frac{1}{\varepsilon}$$

since both n, ε are positive. So this means that given our ε, we need to work out how to make sure that $n > \frac{1}{\varepsilon}$, because then we know that $\frac{1}{n} < \varepsilon$.

Well, if we set $N = \frac{1}{\varepsilon}$, then when we require $n > N$, then we have that $n > N > \varepsilon$ and so $\frac{1}{n} < \frac{1}{N} < \frac{1}{\varepsilon}$ implying that $\frac{1}{n} < \frac{1}{\varepsilon}$. The only hitch is that our definition requires that N be a natural number. But that is easy to fix, instead of setting $N = \frac{1}{\varepsilon}$, we can just take N to be the next integer bigger than $\frac{1}{\varepsilon}$. That is, we set N to be the **ceiling** of $\frac{1}{\varepsilon}$ which we write as $N = \left\lceil \frac{1}{\varepsilon} \right\rceil$.

Here, we should mention that even though any $N > \frac{1}{\varepsilon}$ would work for our arguments above and that we have infinitely many possible choices for N it is important to either picking a specific N as we did in this scratch work, or prove the existence of such an N without giving it explicitly — using results like the Archimedean property[58] or similar. Simply saying that such number *should* exist is not an adequate justification. With that caveat out of the way, let's tidy this up and write the proof.

Solution.

Proof. Let $\varepsilon > 0$. Then pick $N = \left\lceil \frac{1}{\varepsilon} \right\rceil$, so that $N \geq \frac{1}{\varepsilon}$. Then for all $n > N$, we have that

$$|a_n - 0| = \frac{1}{n} < \frac{1}{N} = \varepsilon$$

Therefore we see that (a_n) converges to 0. ■

□

Example 6.4.5 Show that the sequence $(x_n) = \left(\dfrac{2n+4}{n+1}\right)$ converges to 2.

Scratchwork. Again, let's start with the scratch work.

Our zeroth[59] step is to pick some arbitrary $\varepsilon > 0$. Now, as we saw in the previous example, we need to understand how to choose n so that we can guarantee

$$|x_n - L| = \left|\frac{2n+4}{n+1} - 2\right| < \varepsilon$$

[58]This says, roughly, that given any two positive real numbers, x, y, we can always find an integer n, so that $nx > y$. This appears in a more geometric guise in Book V of Euclid's Elements, and Archimedes attributes it to Eudoxus.

To help us understand this, we should clean up the inequality and simplify the expression inside the absolute value. Simplifying shows us that we actually want

$$\left|\frac{2n+4}{n+1} - 2\right| = \left|\frac{2n+4-(2n+2)}{n+1}\right| = \left|\frac{2}{n+1}\right| < \varepsilon.$$

At this point we should reiterate — we have not proved this yet, this is just what we *want* to be true. We still need to work out how we choose n to make sure this is true.

We can even go a little further. Since we know n is a natural number, we know that $\frac{2}{n+1} > 0$ and so we can write

$$\left|\frac{2}{n+1}\right| = \frac{2}{n+1} < \varepsilon.$$

This is a little easier to manipulate, and we can quickly isolate n:

$$\frac{2}{n+1} < \varepsilon \qquad \iff \qquad n+1 > \frac{2}{\varepsilon} \qquad \iff \qquad n > \frac{2}{\varepsilon} - 1$$

So, this means that if we have $n > \frac{2}{\varepsilon} - 1$, then we know (moving back along our chain of reasoning) that $|x_n - 2| < \varepsilon$. So it makes sense for us to choose $N = \left\lceil \frac{2}{\varepsilon} \right\rceil - 1$. Again, we make use of the ceiling function to ensure that N is an integer.

Oops! But be careful — what happens if $\varepsilon = 1000$? Then we choose $N = 0$ which is not a natural number. Thankfully this is easily fixed, let us just take N to be a little bit larger. Indeed, we can set $N = \left\lceil \frac{2}{\varepsilon} \right\rceil$ and everything works out nicely. More generally, in these types of proofs, once you have worked out an N, one is free to make it *larger* (you should ask yourself why). One could also argue that the choice $N = \left\lceil \frac{2}{\varepsilon} \right\rceil$ is a little neater[60] and does not change the proof very much.

Solution.

Proof. Let $\varepsilon > 0$, set $N = \lceil (2/\varepsilon) \rceil$ and let $n > N$. By our choice of n, we know that

$$n > N > \frac{2}{\varepsilon}$$

From this we know that $n + 1 > n > \frac{2}{\varepsilon}$ and so

$$\frac{2}{n+1} < \varepsilon$$

Hence

$$|x_n - 2| = \left|\frac{2n+4}{n+1} - 2\right| = \left|\frac{2}{n+1}\right| = \frac{2}{n+1} < \varepsilon,$$

as required. ■

□

[59]This is barely a step at all really. But we do need ε.

Of course we also know that not every sequence converges — we have already seen an example of this above. Let us redo that example using our rigorous definition of convergence.

Example 6.4.6 Show that the sequence $(b_n) = ((-1)^n)$ does not converge to 1.

Scratchwork. Even though we wish to show that the sequence (b_n) does not converge to 1, our starting point will still be the definition of convergence. Recall that the sequence (b_n) converges to 1 when

$$\forall \varepsilon > 0, \exists N \in \mathbb{N} \text{ s.t. } \forall n \in \mathbb{N}(n > N) \implies (|b_n - 1| < \varepsilon).$$

We want to show that this is false, and we do so by showing that the negation is true. The negation is

$$\exists \varepsilon > 0 \text{ s.t. } \forall N \in \mathbb{N}, \exists n \in \mathbb{N} \text{ s.t. } (n > N) \wedge (|(-1)^n - 1| \geq \varepsilon).$$

So, if we can show that this is true, then the original statement is false, and so the sequence (b_n) does not converge to 1.

Now, let's try to understand this statement. It says that we need to show that there is an $\varepsilon > 0$ such that no matter what $N \in \mathbb{N}$ we choose, there is always at least one $n > N$ such that $|(-1)^n - 1|$ is greater than ε. Now, notice that we don't have to show this for all ε (indeed we can't), we just need to find one ε that makes things work.

As we saw above, sequence (b_n) alternates between -1 and 1.

- For n even, $b_n = (-1)^n = 1$ and so $|b_n - 1| = 0 < \varepsilon$. So this is true for all $\varepsilon > 0$ and all even n.
- On the other hand, for n odd, we have $b_n = (-1)^n = -1$, and so $|b_n - 1| = |-1-1| = 2$. So, as long as we choose $0 < \varepsilon < 2$, this case will fail for all odd $n \in \mathbb{N}$.

So to make the proof work, we can choose, say, $\varepsilon = 1$ and then show that things go wrong for odd n. Time for the proof.

Solution.

Proof. We show that the sequence $(b_n) = ((-1)^n)$ doesn't converge to 1. To this we show that

$$\exists \varepsilon > 0 \text{ s.t. } \forall N \in \mathbb{N}, \exists n \in \mathbb{N} \text{ s.t. } (n > N) \wedge (|(-1)^n - 1| \geq \varepsilon).$$

Let $\varepsilon = 1$ and let N be any natural number. Now set $n = 2N + 1$, so that $b_n = (-1)^n = -1$. Then

$$|b_n - 1| = |-1-1| = 2 > \varepsilon.$$

Therefore we conclude that the sequence does not converge to 1. ■

[60] Mathematicians generally find "neatness" to be desirable in a proof. Of course, one should not make things so neat that the logic is obscured.

Notice that we set $n = 2N + 1$ in our proof and everything worked out nicely. We can actually choose any odd number larger than N. In fact, we could change the wording of the proof to say "Let n be any odd number larger than N" and it would be correct. But, since we can can make a simple explicit choice, we should do so. $\square$

In general, when we talk about the divergence of a sequence, we don't say that the sequence does not converge to a given specific number L. Rather, we typically want to prove[61] that it does not converge to ***any*** number L. This is a much stronger statement. Written as a quantified statement, it is

$$\forall L \in \mathbb{R}, \exists \varepsilon > 0 \text{ s.t. } \forall N \in \mathbb{N}, \exists n \in \mathbb{N} \text{ s.t. } (n > N) \wedge (|x_n - L| \geq \varepsilon),$$

and says that for any number L, the sequence doesn't converge to that number.

Let's do an example where we show that a sequence actually diverges. That is, it does not converge to any number $L \in \mathbb{R}$.

Example 6.4.7 Show that the sequence $(x_n) = (n)$ diverges.

Scratchwork. First, let's write down what we want to show:

$$\forall L \in \mathbb{R}, \exists \varepsilon > 0 \text{ s.t. } \forall N \in \mathbb{N}, \exists n \in \mathbb{N} \text{ s.t. } (n > N) \wedge (|n - L| \geq \varepsilon).$$

Since we need to make this work for every possible L, we let L be an arbitrary real number. Now, what we want is to satisfy $|n - L| \geq \varepsilon$ for some ε and some n. It can be a little intimidating to try to this for an arbitrary L, so perhaps it is better to think about a few different L-values.

- When $L = 0$, the we can simplify $|n - L| = |n| = n$. Now since, $n \in \mathbb{N}$, we know that $n \geq 1$. So if we pick $\varepsilon = 1$, then we will have $|n - L| \geq \varepsilon$ for all $n \in \mathbb{N}$. Now, it is easy to also enforce the requirement that $n > N$, no matter what N is chosen, just pick $n = N + 1$.

- Similarly, if we set $L = -1$, then we have $|n - L| = |n - (-1)| = n + 1$. So again, we can pick $\varepsilon = 1$ and then $|n - L| \geq \varepsilon$ for all $n \in \mathbb{N}$. This reasoning will actually work for any $L \leq 0$. Again, to also enforce the requirement that $n > N$, we can just pick $n = N + 1$.

- What about when, say, $L = 17$, we will have $|n - L| = |n - 17|$. Now, provided $n > 17$, this will be bigger than zero. In particular, if we set $n \geq 18$, then we will have $|n - 17| > 1$. ***However***, this is not quite right. We not only need that $|n - 17| \geq \varepsilon$ but we also need that $n > N$, no matter what choice of $N \in \mathbb{N}$. Thankfully this is easily fixed, just choose $n = \max\{17, N\} + 1$. Alternatively, since we know $N \geq 1$, we can choose $n = N + 17$.

- More generally, if $L > 0$, then we can choose $n \geq \lceil L \rceil + 1$, and then $|n - L| \geq 1$. Just as in the previous point, we need to satisfy $n > N$, so

[61] There are exceptions to this. For example, one easy way to show that a *series* diverges is to show that summands do not converge to zero.

pick $n = \max\{\lceil L \rceil, N\} + 1$. Notice that a similar choice works when $L \leq 0$, just take $n = \max\{\lceil |L| \rceil, N\} + 1$.

We are now ready to write the proof.

Solution.

Proof. Let L be an arbitrary real number and set $\varepsilon = 1$. Then for any $N \in \mathbb{N}$, set $n = \max\{N, \lceil |L| \rceil\} + 1$. Then this gives

$$n > N \qquad \text{and} \qquad |n - L| > 1 = \varepsilon$$

Therefore the sequence $(x_n) = (n)$ diverges. ■

Notice how short the proof is compared to the scratch work. This is not unusual. A nice neat proof can hide a lot of work. □

6.4.2 The limit of a function

Note that in this section of the text we restrict ourselves to real-valued functions. That is, functions that take a real number as input and return a real number as output, just like those you worked with in Calculus courses. We do look at more general functions in Chapter 10, but not their limits.

We define the limits of functions in very much the same way as the limits of sequences. The definition is more general, as now we can talk of the limit of a function as its argument approaches more general points, while for a sequence, we only talked of its behaviour as $n \to \infty$. Let's give the definition and then we'll explain it.

Definition 6.4.8 Let $a, L \in \mathbb{R}$ and let f be a real-valued function. We say that the **limit** of f as x approaches a is L when

$$\forall \varepsilon > 0, \exists \delta > 0 \text{ s.t. } (0 < |x - a| < \delta) \implies (|f(x) - L| < \varepsilon).$$

In this case we write

$$\lim_{x \to a} f(x) = L \qquad \text{or sometimes} \qquad f(x) \xrightarrow[x \to a]{} L$$

and say that f **converges** to L as x approaches a. We also sometimes say the limit of f as x goes to a is L, which we denote by

$$f(x) \to L \text{ as } x \to a.$$

If f does not converge to any finite limit L as x approaches a, then we say that f **diverges** as x approaches a. ♢

This definition may look[62] more complicated than the equivalent definition for the convergence of a sequence, Definition 6.4.2. But if we do some reverse

[62] In fairness, it is a little more complicated. But it is not *that* much more complicated.

engineering (much as we did for sequence convergence above, but in reverse) then we can read the definition as

- **For all** positive ε, **there is some** positive δ so that **if** the distance between x and a is less than delta (but not zero), **then** the distance between $f(x)$ and L is less than ε.

We can rephrase these quantifiers as little:

- **No matter which** positive ε, **we can always find some** positive δ so that **if** the distance between x and a is less than delta (but not zero), **then** the distance between $f(x)$ and L is less than ε.

This is telling us that if we need to make the distance between the function and its limit very small, we can always find some δ so that we just need to make the distance $|x - a| < \delta$. That is

- We can make the distance between $f(x)$ and L **as small as we want**, by making the distance between x and a **arbitrarily small** (but not zero).

So we reach

- We can make $f(x)$ **closer and closer** to L by taking x **closer and closer** to a (but not actually equal).

This is probably, more or less, the working definition of a limit of a function you used in your first Calculus course. This gives reasonable intuition, but the power of quantifiers is to make everything precise and eliminate misunderstandings.

Remark 6.4.9 Why exclude $x = a$. Notice that the definition of convergence of a function says that given any ε we can find δ so that when

$$0 < |x - a| < \delta$$

we know that the distance between the function and its limit is smaller than ε. This hypothesis tells us that the distance between x and a has to be small, but not zero — that is we do not require the function be close to its limit exactly at $x = a$. This is because the definition of **limit** has been crafted to tell us how the function behaves as it *approaches* $x = a$. We do not care about what happens exactly at $x = a$, and indeed we do not even require that the function be defined there. In fact, many important applications of limits — such as derivatives — would not work if we extended this hypothesis to include $x = a$.

Notice also, that our definition of limits of sequences had a similar quirk. We defined the limit in terms of the behaviour of the sequence terms as n became very very large. We did not care about the "infiniteth" term in the sequence — if such a thing were defined.

Let's put this definiton to work by considering the limit of a simple function.

Example 6.4.10 Show that for any $a \in \mathbb{R}$, $\lim_{x \to a} x = a$.

Scratchwork. In this example we want to show that the function $f(x) = x$ converges to the limit a as x goes to a. Even though this feels more like a tautology than an example, it is a good exercise in applying the limit definition.

To prove that $\lim_{x\to a} x = a$ the definition tells us that we need to show that

$$\forall \varepsilon > 0, \exists \delta \text{ s.t. } 0 \text{ s.t. } (0 < |x-a| < \delta) \implies (|f(x) - L| < \varepsilon).$$

Now, this simplifies immediately since we have $f(x) = x$ and $L = a$:

$$\forall \varepsilon > 0, \exists \delta \text{ s.t. } 0 \text{ s.t. } (0 < |x-a| < \delta) \implies (|x - a| < \varepsilon).$$

So, given an arbitrary $\varepsilon > 0$, we need a $\delta > 0$ such that

$$0 < |x-a| < \delta \implies |x-a| < \varepsilon.$$

That is, whatever positive δ we pick, whenever $0 < |x-a| < \delta$, it implies that $|x-a| < \varepsilon$. A good[63] choice for δ is simply $\delta = \varepsilon$.

Now, let's write this in a proof.

Solution.

Proof. Suppose ε is any positive real number. Then pick $\delta = \varepsilon$. Then whenever $|x-a| < \delta$, then we know that $|f(x) - a| = |x-a| < \delta = \varepsilon$ as required. ■

□

That one is arguably a little too simple. Here is a slightly more complicated one.

Example 6.4.11 Let $a \in \mathbb{R}$. Prove that

$$\lim_{x\to a} 3x + 5 = 3a + 5.$$

Scratchwork. Again, our starting point is to look at the definition. We need to prove that

$$\forall \varepsilon > 0, \exists \delta > 0 \text{ s.t. } (0 < |x-a| < \delta) \implies (|(3x+5) - (3a+5)| < \varepsilon).$$

Before we go much further, we should clean this up a little. We can simplify that last inequality. That is $|(3x+5) - (3a+5)| = |3x - 3a| = 3|x-a|$, so

$$\forall \varepsilon > 0, \exists \delta > 0 \text{ s.t. } (0 < |x-a| < \delta) \implies (3|x-a| < \varepsilon).$$

Now this is looking pretty similar to the previous example. Given any ε, we need to pick δ, so that when $0 < |x-a| < \delta$, we guarantee that $3|x-a| < \varepsilon$. If we rearrange this last inequality, we want

$$|x-a| < \frac{\varepsilon}{3}.$$

[63] There are an infinite number of possible correct choices of δ. Indeed, $\delta = \varepsilon/n$ for any $n \in \mathbb{N}$ works. But the choice of $\delta = \varepsilon$ is good because it works, while being neat and simple.

And thus we pick $\delta = \frac{\varepsilon}{3}$.

Alternatively, if we assume that we have $0 < |x - a| < \delta$, then multiplying everything by 3 gives:

$$0 < 3|x - a| < 3\delta$$

and thus we need $3\delta \leq \varepsilon$. So again, we reach the neat choice of $\delta = \frac{\varepsilon}{3}$. Time for the proof.

Solution.

Proof. Let ε be any positive real number. Then pick $\delta = \frac{\varepsilon}{3}$. Then as long as $|x - a| < \delta$, we have that

$$|(3x + 5) - (3a + 5)| = |3x - 3a| = 3|x - a| < 3\delta = \varepsilon.$$

And thus $(3x + 5)$ converges to $3a + 5$ as x approaches a. ■

As you can see, the proof of the statement is very short, clean, and doesn't omit any necessary information. And, as was the case with our proofs above, we don't explain to the reader how we come up with the choice of $\delta = \varepsilon/3$, we just have to prove that it works. □

Let's ratchet up the difficultly a little.

Example 6.4.12 Show that $\lim_{x \to 2} \left(\frac{1}{x}\right) = \frac{1}{2}$.

Scratchwork. Just like in our previous example(s) we start with the definition of convergence and adapt it to the problem at hand. We need to show that

$$\forall \varepsilon > 0, \exists \delta > 0 \text{ s.t. } (0 < |x - 2| < \delta) \implies \left(\left|\frac{1}{x} - \frac{1}{2}\right| < \varepsilon\right).$$

Again, we can clean up and simplify the final inequality, since

$$\left|\frac{1}{x} - \frac{1}{2}\right| = \left|\frac{2 - x}{2x}\right| = \frac{|x - 2|}{2|x|}.$$

Thus we need to show that

$$\forall \varepsilon > 0, \exists \delta > 0 \text{ s.t. } (0 < |x - 2| < \delta) \implies \left(\frac{|2 - x|}{2|x|} < \varepsilon\right).$$

Now that we know what we need to show, let $\varepsilon > 0$ be arbitrary. Then, we want a $\delta > 0$ such that if we assume $0 < |x - 2| < \delta$, we can guarantee that $\frac{|x-2|}{2|x|} < \varepsilon$. Well, if we know that $|x - 2| < \delta$, then we can write

$$\frac{|x - 2|}{2|x|} < \frac{\delta}{2|x|} < \varepsilon$$

and so we need

$$\delta < 2|x|\varepsilon.$$

This is not quite enough — our choice of δ should not depend on x. We need some bound on x.

Recall our intuitive idea of the limit, as x gets very close to 2, the function $\frac{1}{x}$ gets very close to $\frac{1}{2}$. We don't really care what happens when x is a long way from 2, and only on what happens when x is very close to 2. Thus we should be able to focus on the region around $x = 2$, say, $1 < x < 3$, or equivalently, $|x - 2| < 1$.

How[64] does this help us? Well, if we know that $1 < x < 3$, then we know[65] that $|x| > 1$, and so

$$\frac{|x-2|}{2|x|} < \frac{\delta}{2|x|} < \frac{\delta}{2} \leq \varepsilon$$

And thus we need to ensure that

$$\delta \leq 2\varepsilon.$$

At this point it seems that we can choose any $\delta \leq 2\varepsilon$, but this is not quite right. Say, we chose a large value of ε, like $\varepsilon = 3$, and so we could pick $\delta = 2\varepsilon = 6$. With that choice of ε and δ, the implication at the heart of the definition of convergence becomes

$$(|x-2| < 6) \implies \left(\left|\frac{1}{x} - \frac{1}{2}\right| < 3\right).$$

Unfortunately this is false. We could take, say $x = \frac{1}{10} = 0.1$, and then the hypothesis is true, since $|x - 2| = 1.9 < 6$, but the conclusion is false since $\left|\frac{1}{x} - \frac{1}{2}\right| = |10 - 0.5| = 9.5 > 3$.

What went wrong? Remember to make our bound on $|x|$ we required that $|x - 2| < 1$. This is the same as requiring that $\delta \leq 1$. So we have actually imposed two requirements on δ. We need both $\delta \leq 1$ *and* $\delta \leq 2\varepsilon$. To enforce both of these we can pick

$$\delta = \min\{1, 2\varepsilon\}.$$

Now we can finally write up the proof.

Solution.

Proof. Let $\varepsilon > 0$ and set $\delta = \min\{1, 2\varepsilon\}$. Now assume that $0 < |x - 2| < \delta$. Since $\delta \leq 1$, we know that $|x - 2| < 1$ and so $1 < |x| < 3$ and thus $2|x| > 2$.

Then

$$\left|\frac{1}{x} - \frac{1}{2}\right| = \frac{|x-2|}{2|x|} < \frac{|x-2|}{2} < \frac{\delta}{2}.$$

Since $\delta < 2\varepsilon$, we know that

$$\left|\frac{1}{x} - \frac{1}{2}\right| < \varepsilon$$

and so $\frac{1}{x} \to \frac{1}{2}$ as $x \to 2$. ■

□

[64]Should one ask rhetorical questions in a textbook?

6.5 (Optional) Properties of limits

6.5.1 (Optional) Some properties of limits of sequences

When we work with sequences, it is not convenient to prove sequence convergence for each and every sequence individually. We can make use of some more general properties of limits of sequences to simplify our work. You will have already seen some "limit laws" when you studied calculus. We will prove some similar results in this section.

Theorem 6.5.1 Basic properties of limits of sequences. *Let (x_n) and (y_n) be sequences so that*

$$\lim_{n\to\infty} x_n = a \qquad \text{and} \qquad \lim_{n\to\infty} y_n = b$$

Additionally let $c, d \in \mathbb{R}$. Then

(a) *The limit of a sequence is unique*

(b) *Linearity of limits:* $\lim_{n\to\infty}(c \cdot x_n + d \cdot y_n) = c \cdot a + d \cdot b$.

(c) *Product of limits:* $\lim_{n\to\infty}(x_n \cdot y_n) = a \cdot b$.

(d) *Reciprocal of limit:* $\lim_{n\to\infty} \frac{1}{y_n} = \frac{1}{b}$ *as long as* $b \neq 0$

(e) *Ratio of limits:* $\lim_{n\to\infty} \frac{x_n}{y_n} = \frac{a}{b}$ *as long as* $b \neq 0$

Notice that for the sequences $(1/b_n)$ and (a_n/b_n) to be defined for all n we need $b_n \neq 0$, but we have not stated that in the theorem. This is because the condition that the limit $b_n \to b \neq 0$ implies that when n is *large enough*[66] we know that $b_n \neq 0$ — this is a consequence of Lemma 6.5.5 below. This is enough to tell us that when n is large everything is defined, and, typically, we don't worry about what happens when n is small.

6.5.1.1 Uniqueness of limits

To prove the first property — uniqueness of limits — we need to do some scratch work to build up our intuition. A very standard approach to proving uniqueness is to assume that we have two objects satisfying the property and then show that those two things must actually be the same.

So, let (x_n) be a convergent sequence and that

$$\lim_{n\to\infty} x_n = K \qquad \text{and also} \qquad \lim_{n\to\infty} x_n = L$$

[65] Be careful with the inequalities here.

[66] To be more precise, we can find some N_0 so that when $n > N_0$ we know that $|b_n| > 0$.

ie, there are two limits. Of course, we don't want these limits to *actually* be different, even though we've labelled them by different variables. We want to show that they are the same, that is $K = L$. In other words,

$$\text{(the limit is unique)} \equiv \Big((\lim_{n\to\infty} x_n = K) \wedge (\lim_{n\to\infty} x_n = L) \implies (K = L) \Big).$$

Assume the hypothesis is true. So

$$\lim_{n\to\infty} x_n = K \qquad \text{and also} \qquad \lim_{n\to\infty} x_n = L$$

and then we try to show that $K = L$. Intuitively this makes sense. Since $\lim_{n\to\infty} x_n = K$, we know that we can make x_n arbitrarily close to K by making n large enough. Similarly, we can make x_n arbitrarily close to L. The only way this can happen is if K and L are also arbitrarily close to each other. And the only way that can happen is if they are actually the same.

This is an important point that we will have to prove. Namely, we are claiming that if two numbers are arbitrarily close to each other, then they must be equal. Rewriting this with quantifiers gives

$$(\forall \varepsilon > 0, |K - L| < \varepsilon) \implies (K = L).$$

At first glance this might look a little hard to prove, but think about its contrapositive:

$$(K \neq L) \implies (\exists \varepsilon > 0 \text{ s.t. } |K - L| \geq \varepsilon).$$

So if two numbers are different, then we can find some positive number ε so that the distance between those two numbers is bigger. That doesn't sound so bad. It is a useful result, so we'll make it into a lemma.

Lemma 6.5.2 *Let $K, L \in \mathbb{R}$. If for every $\varepsilon > 0$ we have that $|K - L| < \varepsilon$, then we must have that $K = L$.*

Proof. We prove the contrapositive. Let $K, L \in \mathbb{R}$ so that $K \neq L$. Then set $\varepsilon = \frac{|K-L|}{2}$. Since $K \neq L$ we know that $\varepsilon > 0$. Then we have that $|K - L| = 2\varepsilon > \varepsilon$ and so the result holds. ■

Okay, to recap, we have assumed that $x_n \to K$ and $x_n \to L$. This means that

- for all $\varepsilon_K > 0$, there is some $N_K \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ if $n > N_K$ then $|x_n - K| < \varepsilon_K$, and
- for all $\varepsilon_L > 0$, there is some $N_L \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ if $n > N_L$ then $|x_n - L| < \varepsilon_L$.

Notice that we have carefully used different symbols for the ε and N to describe the convergence of $x_n \to K$ and $x_n \to L$. We do this so that we are not accidentally assuming anything extra[67] about how x_n converges to K or L. Now, this tells us that when n is big enough — ie $n > \max\{N_K, N_L\}$, that

$$|x_n - K| < \varepsilon_K \qquad \text{and} \qquad |x_n - L| < \varepsilon_L.$$

[67] We saw something like this back in Remark 3.2.8 — we recommend that the reader quickly review that remark.

But how do we use this, and the lemma above, to tell us about the size of $|K-L|$?

There is a really nice trick using the Theorem 5.4.6 and a little algebra. First, we add zero in a sneaky way that allows us to rewrite $K-L$ in terms of $(K-x_n)$ and $(L-x_n)$:

$$|K-L| = |K-L+0| = |K-L+\underbrace{(x_n-x_n)}_{=0}| = |(K-x_n)+(x_n-L)|$$

Now apply the triangle inequality:

$$|K-L| = |(K-x_n)+(x_n-L)| \leq |K-x_n| + |x_n-L| = |x_n-K| + |x_n-L|$$

This gives us a way to bound the distance between K and L in terms of the distances between x_n and K and between x_n and L. But our assumption about the convergence of x_n gives us exactly that information. That is

$$|K-L| \leq |x_n-K| + |x_n-L| < \varepsilon_K + \varepsilon_L$$

Now, given any ε, we can[68] choose $\varepsilon_K = \varepsilon_L = \frac{\varepsilon}{2}$. Then

- since $x_n \to K$, we know that there is some N_K so that when $n > N_K$, we have that $|x_n - K| < \frac{\varepsilon}{2}$.
- Similarly, since $x_n \to L$, we know that there is some N_L so that when $n > N_L$, we have that $|x_n - L| < \frac{\varepsilon}{2}$.

Then our reasoning above tells us that $|K-L| < \varepsilon$ providing $n > \max\{N_K, N_L\}$. And finally we can use Lemma 6.5.2 to complete the result.

Oof!

Proof of uniqueness of limits. Let (x_n) be a convergent sequence. We will prove that its limit is unique. To do so we prove that if $x_n \to K$ and $x_n \to L$ then we must have that $K = L$.

So assume that $x_n \to K$ and $x_n \to L$, and let $\varepsilon > 0$.

- Since $x_n \to K$, there is some $N_K \in \mathbb{N}$ so that for all $n > N_K$ we have that $|x_n - K| < \frac{\varepsilon}{2}$.
- And, since $x_n \to L$, there is some $N_L \in \mathbb{N}$ so that for all $n > N_L$ we have that $|x_n - L| < \frac{\varepsilon}{2}$.

So if we pick $N = \max\{N_K, N_L\}$ then for all $n > N$ the triangle inequality implies that

$$|K-L| = |(K-x_n)+(x_n-L)| \leq |x_n-K| + |x_n-L| \leq \varepsilon$$

Note that K, L are constants so the inequality $|K-L| < \varepsilon$ must hold independently of the value of n. And since it holds for any $\varepsilon > 0$ Lemma 6.5.2 implies that $K = L$ as required. ■

[68] There are lots of potential choices here. For example, we can also pick $\varepsilon_K = \alpha\varepsilon, \varepsilon_L = \beta\varepsilon$ with $\alpha, \beta > 0$ and $\alpha + \beta \leq 1$, so that $\varepsilon_K + \varepsilon_L \leq \varepsilon$.

6.5.1.2 Linearity of limits

No time to rest! Let's get working on the linearity of limits. We prove this by breaking the result down into two simpler lemmas.

Lemma 6.5.3 *Let $a, c \in \mathbb{R}$ and let (x_n) be a sequence that converges to a. The sequence $(c \cdot x_n)$ converges to $c \cdot a$.*

Lemma 6.5.4 *Let $a, b \in \mathbb{R}$ and let (x_n) and (y_n) be sequences so that $x_n \to a$ and $y_n \to b$. The sequence $(z_n) = (x_n + y_n)$ converges to $a + b$.*

Once we prove both of these, the linearity of limits follows quite directly:

$$\begin{aligned}\lim_{n\to\infty}(c \cdot x_n + d \cdot y_n) &= \lim_{n\to\infty}(c \cdot x_n) + \lim_{n\to\infty}(d \cdot y_n)\\ &= c \cdot \lim_{n\to\infty}(x_n) + d \cdot \lim_{n\to\infty}(y_n).\end{aligned}$$

The first of these lemmas is a little easier than the second, so we'll start there. And, as usual, we start with scratch work. Notice that when $c = 0$ the result simplifies down to the statement that the constant sequence $x_n = 0$ converges to 0. This is just Example 6.4.3 and we can recycle that proof. So since we know how to prove the case $c = 0$, we can now work on $c \neq 0$.

Notice that the statement is really a conditional. If $x_n \to a$ then $c \cdot x_n \to c \cdot a$. We'll assume that $x_n \to a$ and then work towards showing that $c \cdot x_n \to c \cdot a$. To do this we have to prove that for all $\varepsilon > 0$, there is some $N \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ if $n > N$ then $|cx_n - ca| < \varepsilon$. Let's manipulate this inequality a little:

$$|cx_n - ca| = |c||x_n - a|$$

and so it suffices for us to show that $|x_n - a| < \frac{\varepsilon}{|c|}$.

Well, now we can put our assumption that $x_n \to a$ to use. That assumption tells us that for *any* $\varepsilon_x > 0$, there is $N_x \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ when $n > N_x$ then $|x_n - a| < \varepsilon_x$. We are being careful to label those constants with the subscript x to help remind us that those constants describe the convergence of $x_n \to a$.

Since this works for *any* ε_x, we are free to set $\varepsilon_x = \frac{\varepsilon}{|c|}$. Then we know there is N_x so that if $n > N_x$ then $|x_n - a| < \frac{\varepsilon}{|c|}$ and thus $|c||x_n - a| < \varepsilon$, just as we need. All that remains is to write it up as a neat proof.

Proof of Lemma 6.5.3. Let $\varepsilon > 0$ and assume that $x_n \to a$. We split the proof into two cases, $c = 0$ and $c \neq 0$.

When $c = 0$, then we have that $c \cdot x_n = 0$, and hence we trivially have

$$|c \cdot x_n - c \cdot a| = |0 - 0| < \varepsilon$$

Thus $0x_n \to 0$.

So now assume that $c \neq 0$. Since $x_n \to a$, we know that there exists $N_x \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ when $n > N_x$, we have $|x_n - a| < \frac{\varepsilon}{|c|}$. Let $N = N_x$ and then provided $n > N$,

$$|c \cdot x_n - c \cdot a| = |c||x_n - a| < \varepsilon.$$

And thus $c \cdot x_n \to c \cdot a$ as required. ■

We can actually clean this proof up and write it as a single case. We had to separate our the case $c = 0$ so that we did not divide ε by 0. However, we should remember that we do have some flexibility. Here is an alternate, slightly cleaner proof.

Second proof of Lemma 6.5.3. Let $\varepsilon > 0$ and assume that $x_n \to a$. We know that there exists $N_x \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ when $n > N_x$, we have $|x_n - a| < \frac{\varepsilon}{|c|+1}$. Let $N = N_x$ and then provided $n > N$,

$$|c \cdot x_n - c \cdot a| = |c||x_n - a| < \frac{|c|\varepsilon}{|c|+1} < \varepsilon.$$

And thus $c \cdot x_n \to c \cdot a$ as required. ■

Let us now turn to Lemma 6.5.4. Notice that, again, it is really a conditional: "if those sequences converge to a and b, then their sum converges to $a + b$." So our proof will start by assuming the hypothesis is true and then working our way to the conclusion. We start by assuming that $x_n \to a$ and $y_n \to b$ and, as is always the case, it is a good idea to write down the meaning of the things that we have assumed and also to write down the meaning of what we want to show.

Our assumptions that $x_n \to a$ and $y_n \to b$ mean[69][70]:

- for any $\varepsilon_x > 0$ there is some $N_x \in \mathbb{N}$ so that for all $n \in \mathbb{N}$, if $n > N$ then $|x_n - a| < \varepsilon_x$, and
- for any $\varepsilon_y > 0$ there is some $N_y \in \mathbb{N}$ so that for all $n \in \mathbb{N}$, if $n > N$ then $|y_n - b| < \varepsilon_y$.

And we wish to show that

- for any $\varepsilon > 0$ there is some $N \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ if $n > N$ then
$$|(x_n + y_n) - (a + b)| < \varepsilon.$$

The triangle inequality, Theorem 5.4.6, helps us here. It tells us how to bound the quantity $|(x_n + y_n) - (a + b)|$ by $|x_n - a|$ and $|y_n - b|$:

$$|(x_n + y_n) - (a + b)| = |(x_n - a) + (y_n - b)| \leq |x_n - a| + |y_n - b|$$

And then since we have assumed that $(x_n), (y_n)$ converge to a, b, we know that by making n very big, we can make both $|x_n - a|$ and $|y_n - b|$ very small. This then implies that we can make $|(x_n + y_n) - (a + b)|$ very small. In particular, if we can make both $|x_n - a|$ and $|y_n - b|$ smaller than $\frac{\varepsilon}{2}$, then the triangle inequality tells us that $|(x_n + y_n) - (a + b)|$ is smaller than ε. This is precisely what we need to prove the result.

---

[69] Know your definitons!

[70] Again, we are careful to use different ε and different N for each convergence statement in order to avoid making accidental extra assumptions.

Time to use our assumptions $x_n \to a$ and $y_n \to b$. Since[71] the definition of convergence works for *any* choice of ε, we can pick $\varepsilon_x = \varepsilon_y = \frac{\varepsilon}{2}$. Then

- there is N_x so that when $n > N_x$, $|x_n - a| < \varepsilon_x = \frac{\varepsilon}{2}$, and
- there is N_y so that when $n > N_y$, $|x_n - b| < \varepsilon_y = \frac{\varepsilon}{2}$.

This means that for any $n > \max\{N_x, N_y\}$ we have $|x_n - a| + |x_n - b| < \varepsilon$, which, in turn, guarantees that $|(x_n + y_n) - (a + b)| < \varepsilon$. Now we just have to tidy it up and write it in a nice proof.

Proof of Lemma 6.5.4. Assume that $x_n \to a$ and $y_n \to b$. We will show that $z_n = x_n + y_n \to a + b$.

Let $\varepsilon > 0$. Then since $x_n \to a$, we know that there exists $N_x \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ if $n > N_x$ then $|x_n - a| < \frac{\varepsilon}{2}$. Similarly, since $y_n \to b$, we know that there exists $N_y \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ if $n > N_y$ then $|y_n - b| < \frac{\varepsilon}{2}$.

Now pick $N = \max\{N_x, N_y\}$. Then for all $n \in \mathbb{N}$ with $n > N$, we have

$$\begin{aligned} |z_n - (a + b)| &= |x_n - a + y_n - b| \\ &\leq |x_n - a| + |y_n - b| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

and thus $z_n \to (a + b)$ as required. ■

Now that we have proved these two lemmas we can complete our proof of the linearity of limits:

Proof of the linearity of limits. Let $a, b, c, d \in \mathbb{R}$ and let (x_n) and (y_n) be sequences so that

$$\lim_{n\to\infty} x_n = a \qquad \text{and} \qquad \lim_{n\to\infty} y_n = b.$$

Then by Lemma 6.5.3:

$$\lim_{n\to\infty} c \cdot x_n = c \cdot a \qquad \text{and} \qquad \lim_{n\to\infty} d \cdot y_n = d \cdot b.$$

and then by Lemma 6.5.4:

$$\lim_{n\to\infty} (c \cdot x_n + d \cdot b_n) = \lim_{n\to\infty} c \cdot x_n + \lim_{n\to\infty} d \cdot b_n = c \cdot a + c \cdot b$$

as required.

Notice that by working in this order, we have been careful to first establish the convergence of the sequences (cx_n) and (dy_n), via Lemma 6.5.3, before establishing the convergence of their sum. This is necessary because Lemma 6.5.4 only works for the sum of convergent sequences. ■

[71] We used a very similar idea in our proof of uniqueness of limits.

6.5.1.3 Product of limits

Again, the statement is really an impliction: “if $x_n \to a$ and $y_n \to b$ then $x_n \cdot y_n \to a \cdot b$”. So we assume that $x_n \to a$ and $y_n \to b$. This means, roughly speaking, that when n is really big, we know that $|x_n - a|$ and $|y_n - b|$ are small. And from that we need to show that $|x_n \cdot y_n - a \cdot b|$ is also small.

So we have to somehow express

$$|x_n \cdot y_n - a \cdot b| \qquad \text{in terms of} \qquad |x_n - a| \text{ and } |y_n - b|$$

and we can do it by carefully adding and subtracting terms.

$$\begin{aligned}(x_n \cdot y_n - a \cdot b) &= (x_n \cdot y_n - a \cdot b) + \underbrace{(x_n \cdot b - x_n \cdot b)}_{=0} \\ &= x_n(y_n - b) + b(x_n - a)\end{aligned}$$

So then, a little application of the triangle inequality gives

$$\begin{aligned}|x_n \cdot y_n - a \cdot b| &= |x_n(y_n - b) + b(x_n - a)| \\ &\leq |x_n(y_n - b)| + |b(x_n - a)| \\ &= |x_n| \cdot |y_n - b| + |b| \cdot |x_n - a|\end{aligned}$$

Similar to the argument we used to prove Lemma 6.5.4, we see that if we can keep $|x_n| \cdot |y_n - b| < \varepsilon/2$ and $|b| \cdot |x_n - a| < \varepsilon/2$, then we are done. But, how can we do that? Well, we can recycle the ideas from the proof of Lemma 6.5.3 to keep $|b| \cdot |x_n - a| < \varepsilon/2$, i.e. $|x_n - a| < \frac{\varepsilon}{2|b|+1}$, since $|b|$ is a constant. But that argument doesn't work for the other term, $|x_n| \cdot |y_n - b|$ since x_n need not be a constant.

However, we do know when n is very large that x_n must be close a, its limit. So we should be able to bound $\frac{|a|}{2} \leq |x_n| \leq \frac{3|a|}{2}$ for some sufficiently large n. This, in turn, would allow us to bound

$$\frac{|a|}{2}|y_n - b| \leq |x_n| \cdot |y_n - b| \leq \frac{3|a|}{2}|y_n - b|$$

And now, we use our control[72] over $|y_n - b|$, to make sure that $\frac{3|a|}{2}|y_n - b| < \varepsilon/2$.

Let us make this intermediate result bounding $|x_n|$, into a lemma. It takes a little careful juggling of inequalities and the reverse triangle inequality, Corollary 5.4.7, helps us. Then we can use the lemma to finish our proof.

Lemma 6.5.5 *Let $a \in \mathbb{R}$ and let (x_n) be a sequence that converges to a. Then there is some $N \in \mathbb{N}$ so that for all $n \in \mathbb{N}$, when $n > N$, we have*

$$\frac{|a|}{2} \leq |x_n| \leq \frac{3|a|}{2}.$$

[72] That is, since $y_n \to b$ we know that we can make $|y_n - b|$ as small as we need, just by making n sufficiently large. In this way, our knowledge that y_n converges, gives us some control over the size of that term, $|y_n - b|$.

Proof. Let a and (x_n) be as given, and let $\varepsilon = \frac{|a|}{2}$. Then since $x_n \to a$, we know that there is $N \in \mathbb{N}$ so that for all integer $n > N$,

$$|x_n - a| < \frac{|a|}{2}.$$

The reverse triangle inequality, Corollary 5.4.7 then tells us that

$$|x_n - a| \geq ||x_n| - |a||$$

and hence we know that

$$||x_n| - |a|| < \frac{|a|}{2}$$

This is equivalent (see Lemma 5.4.5) to the statement

$$-\frac{|a|}{2} < |x_n| - |a| < \frac{|a|}{2}$$

from which the result quickly follows by adding $|a|$ to both sides. ■

Proof of the product of limits. Let (x_n) and (y_n) be sequences so that $x_n \to a$ and $y_n \to b$. Let $\varepsilon > 0$. Then, since those sequences converge we know that

- there is some N_x so that for all $n > N_x$ we have $|x_n - a| < \frac{\varepsilon}{2|b|+1}$, and
- there is some N_y so that for all $n > N_y$ we have $|y_n - b| < \frac{\varepsilon}{3|a|+1}$.

Notice that we have chosen denominators $2|b| + 1$ and $3|a| + 1$ to avoid the possibility of dividing by zero when a or b is zero. We also know

- by Lemma 6.5.5 there is some N_a so that for all $n > N_a$, we have $|x_n| < \frac{3|a|}{2}$.

Now assume that $n > \max\{N_x, N_y, N_a\}$, then

$$\begin{aligned}
|x_n y_n - ab| &= |x_n(y_n - b) + b(x_n - a)| \\
&\leq |x_n||y_n - b| + |b||x_n - a| \\
&\leq \frac{3|a|}{2}|y_n - b| + |b||x_n - a| && \text{by bound on } |x_n| \\
&< \frac{3|a|}{2} \cdot \frac{\varepsilon}{3|a|+1} + |b| \cdot \frac{\varepsilon}{2|b|+1} && \text{convergence of } x_n, y_n \\
&< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.
\end{aligned}$$

and thus $x_n \cdot y_n \to a \cdot b$ as required. ■

6.5.1.4 Ratio of limits

We are on the home stretch now. We can prove the last property — the ratio of limits e — by combining the third and forth properties — the product of limits c and the reciprocal of a limit d. So we now just[73] need to prove the reciprocal of limits.

Again, Item d is a conditional statement, so to prove it, we assume the hypothesis, $(y_n) \to b$ and $b \neq 0$, and then show that $\left(\frac{1}{y_n}\right) \to \frac{1}{b}$.

- So the assumption tells us that $b \neq 0$ and for all $\varepsilon_y > 0$, there is some $N_y \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ when $n > N_y$ then $|y_n - b| < \varepsilon_y$.
- While to prove the conclusion we need to show that for all $\varepsilon > 0$ there is some $N \in \mathbb{N}$ so that for all $n \in \mathbb{N}$ when $n > N$ then $\left|\frac{1}{y_n} - \frac{1}{b}\right| < \varepsilon$.

Obviously[74] we need to somehow relate this final inequality, $\left|\frac{1}{y_n} - \frac{1}{b}\right| < \varepsilon$, to the inequality we get from the convergence of $y_n \to b$, namely $|y_n - b| < \varepsilon_y$. So, time to do some rewriting:

$$\begin{aligned} \left|\frac{1}{y_n} - \frac{1}{b}\right| &= \left|\frac{(b - y_n)}{b \cdot y_n}\right| \\ &= \frac{|b - y_n|}{|b \cdot y_n|} = \frac{1}{|b|} \cdot \frac{1}{|y_n|} \cdot |y_n - b| \end{aligned}$$

And hence we need to choose N so that we can guarantee that

$$\left|\frac{1}{y_n} - \frac{1}{b}\right| = \frac{1}{|b|} \cdot \frac{1}{|y_n|} \cdot |y_n - b| < \varepsilon,$$

or equivalently:

$$|y_n - b| < |b| \cdot |y_n| \cdot \varepsilon.$$

Now since we have control[75] over the size of $|y_n - b|$, we can make it really small. But, just as was the case when we proved the product of limits c, we first have to bound $|y_n|$. Thankfully we did all that hard work already when we proved Lemma 6.5.5. That lemma tells us that there is some N_b so that when $n > N_b$ we know that

$$\frac{|b|}{2} < |y_n| < \frac{3|b|}{2}$$

Thus when $n > N_b$, we know that $\frac{|b|^2}{2} \cdot \varepsilon < |b| \cdot |y_n| \cdot \varepsilon$ So, if we can guarantee that

$$|y_n - b| < \frac{|b|^2}{2} \cdot \varepsilon$$

[73] When someone says that you "just" need to do something, you are right to be skeptical. "Just" can be a very dangerous word.

[74] Another dangerous word. Sorry. Better to say something like "Similarly to our earlier proofs in this section". The point of this footnote is to draw the reader's attention to the fact that words like "obviously", "clearly", or "just", are very subjective and should generally be avoided. But, we hope that it is clear to the reader that instructions like this are obviously to be disregarded from time to time. All things in moderation.

[75] That is, since $y_n \to b$, we know that we can make $|y_n - b|$ as small as we want by making n sufficiently large.

then we have

$$|y_n - b| < \frac{|b|^2}{2} \cdot \varepsilon < |b| \cdot |y_n| \cdot \varepsilon$$

and so $\left|\frac{1}{y_n} - \frac{1}{b}\right| < \varepsilon$ as required. Therefore we set $\varepsilon_y = \frac{|b|^2}{2} \cdot \varepsilon$.

The proof is ready to go. We just have to tidy things up and be careful of our various N's and ε's.

Proof of the reciprocal of a limit. Let $b \in \mathbb{R}$ with $b \neq 0$ and let (y_n) be a sequence that converges to b.

Now let $\varepsilon > 0$. Since $y_n \to b$, Lemma 6.5.5 implies that there is $N_b \in \mathbb{N}$ so that for all integer $n > N_b$

$$\frac{|b|}{2} < |y_n|.$$

Additionally, since $y_n \to b$, we can find $N_y \in \mathbb{N}$ so that for all integer $n > N_y$,

$$|y_n - b| < \frac{|b|^2}{2} \cdot \varepsilon.$$

Thus, if we pick $N = \max\{N_b, N_y\}$, then for all integer $n > N$, we have

$$\begin{aligned}\left|\frac{1}{y_n} - \frac{1}{b}\right| &= \frac{|y_n - b|}{|b| \cdot |y_n|} \\ &< |y_n - b| \cdot \frac{2}{|b|^2} \\ &< \frac{|b|^2}{2} \cdot \varepsilon \cdot \frac{2}{|b|^2} = \varepsilon\end{aligned}$$

And therefore the result follows. ■

Now that we have proved both the product of limits property and the reciprocal of limits property, we get the ratio of limits property quite directly.

Proof of the ratio of limits. Let x_n and y_n be sequences so that $x_n \to a$ and $y_n \to b \neq 0$. Then by the reciprocal of limits d we know that $\frac{1}{y_n} \to \frac{1}{b}$. And so, by the product of limits c, we know that

$$\lim_{n\to\infty} \frac{x_n}{y_n} = \lim_{n\to\infty} x_n \cdot \frac{1}{y_n} = \frac{a}{b}$$

as required. ■

6.5.2 (Optional) Some properties of limits of functions

The basic properties of limits of functions are very similar to those satisfied by the limits of sequences and should be familiar to the reader who has taken a Calculus course.

Theorem 6.5.6 Basic properties of limits of functions. *Let $a, K, L \in \mathbb{R}$*

and let f and g be real valued functions so that

$$\lim_{x\to a} f(x) = K \qquad \textit{and} \qquad \lim_{x\to a} g(x) = L.$$

Additionally let $c, d \in \mathbb{R}$. *Then*

(a) *The limit of a function at a given point is unique.*

(b) *Linearity of limits:* $\lim_{x\to a}(c \cdot f(x) + d \cdot g(x)) = cK + dL$.

(c) *Product of limits:* $\lim_{x\to a} f(x) \cdot g(x) = K \cdot L$.

(d) *Reciprocal of limit:* $\lim_{x\to a} \frac{1}{g(x)} = \frac{1}{L}$ *as long as* $L \neq 0$.

(e) *Ratio of limits:* $\lim_{x\to a} \frac{f(x)}{g(x)} = \frac{K}{L}$ *as long as* $L \neq 0$.

Notice that the properties of limits of sequences are very similar to the properties of limits of sequences. The proofs are actually very similar as well. The main difference is that instead of picking some threshold $N \in \mathbb{N}$ we need to pick δ. Further, where we picked N to be at least as large as the other N's used to ensure that all inequalities are satisfied (eg the proof of Item c in Theorem 6.5.1), we will need to pick δ to be smaller than all the other δ's used. Because of these similarities we are going to give the proofs without scratch-work; we recommend the reader refer back to Subsection 6.5.1 for the ideas underlying behind the proofs.

Also notice that for the reciprocal $1/g(x)$ and ratio $f(x)/g(x)$ to be defined we require that $g(x) \neq 0$ but we have not stated this in the theorem. This is very similar to the situation for Theorem 6.5.1 above. The condition that $L \neq 0$ tells that when x is *close enough*[76] to a that $g(x) \neq 0$ — this is a consequence of Lemma 6.5.9 below. Since we are typically only interested in what happens when x is close to a, the condition that $L \neq 0$ ensures that $1/g(x)$ and ratio $f(x)/g(x)$ are defined.

6.5.2.1 Uniqueness of limits

Proof of the uniqueness of limits. To show that the limit of a function is unique, we prove that if

$$\lim_{x\to a} f(x) = K \qquad \text{and also} \qquad \lim_{x\to a} f(x) = L$$

then $K = L$.

So now assume that $\lim_{x\to a} f(x) = K$ and $\lim_{x\to a} f(x) = L$, and moreover let $\varepsilon > 0$.

- Since $\lim_{x\to a} f(x) = K$, we see that $\exists \delta_K > 0$ so that when $0 < |x - a| < \delta_K$

[76] That is, we can find some $c > 0$ so that when $|x - a| < c$, we know $|g(x)| > 0$.

we have $|f(x) - K| < \frac{\varepsilon}{2}$.

- Similarly, since $\lim_{x\to a} f(x) = L$, we see that $\exists \delta_L > 0$ so that when $0 < |x - a| < \delta_L$ we have $|f(x) - K| < \frac{\varepsilon}{2}$.

Thus, if we pick $\delta = \min\{\delta_K, \delta_L\}$ then when $0 < |x - a| < \delta$ we know that

$$|K - L| = |(K - f(x)) + (f(x) - L)| \leq |f(x) - K| + |f(x) - L| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

This, by Lemma 6.5.2, implies that $K = L$, and therefore the limit of a function at a point is unique. ■

6.5.2.2 Linearity of limits

We prove the linearity of limits via two simpler lemmas.

Lemma 6.5.7 *Let $a, K, c \in \mathbb{R}$ and let f be a real value function so that*

$$\lim_{x\to a} f(x) = K.$$

Then

$$\lim_{x\to a} c \cdot f(x) = c \cdot K.$$

Proof. Let a, c, K, f be as in the statement of the lemma. Now let $\varepsilon > 0$, so that by the convergence of f we know that there is some δ_K so that when $0 < |x - a| < \delta_K$ we have that

$$|f(x) - K| < \frac{\varepsilon}{|c| + 1}.$$

Notice that this choice avoids any problems that might arise in the case that $c = 0$.

Now let $\delta = \delta_K$, so that when $0 < |x - a| < \delta = \delta_K$ we know that

$$|c \cdot f(x) - c \cdot K| < |c| \cdot |f(x) - K| < \frac{|c|}{|c| + 1}\varepsilon < \varepsilon$$

and thus $cf(x) \to cK$ as $x \to a$ as required. ■

Lemma 6.5.8 *Let $a, K, L \in \mathbb{R}$ and let f and g be real valued functions so that*

$$\lim_{x\to a} f(x) = K \qquad \text{and} \qquad \lim_{x\to a} g(x) = L.$$

Then

$$\lim_{x\to a} f(x) + g(x) = K + L.$$

Proof. Let a, K, L, f, g be as in the statement of the lemma, and let $\varepsilon > 0$. Then

- since $f(x) \to K$ we know that there is some δ_K so that when $0 < |x-a| < \delta_K$ we have that $|f(x) - K| < \frac{\varepsilon}{2}$,

- and similarly, since $g(x) \to L$ we know that there is some δ_L so that when $0 < |x-a| < \delta_L$ we have that $|g(x) - L| < \frac{\varepsilon}{2}$.

Pick $\delta = \min\{\delta_K, \delta_L\}$, so that for all x with $0 < |x-a| < \delta$ we know that

$$\begin{aligned} |(f(x)+g(x)) - (K+L)| &= |(f(x)-K) + (g(x)-L)| \\ &\leq |f(x)-K| + |g(x)-L| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

Thus $(f(x)+g(x)) \to (K+L)$ as $x \to a$ as required. ■

Equipped with these two lemmas, the proof of the linearity of limits of functions is quite straightforward.

Proof of the linearity of limits. Let f and g be functions so that

$$\lim_{x\to a} f(x) = K \qquad \text{and} \qquad \lim_{x\to a} g(x) = L.$$

Moreover, let $c, d \in \mathbb{R}$. Then using Lemma 6.5.7 we know that

$$\lim_{x\to a} c \cdot f(x) = c \cdot K \qquad \text{and} \qquad \lim_{x\to a} d \cdot g(x) = d \cdot L.$$

And then Lemma 6.5.8 we get

$$\lim_{x\to a} (c \cdot f(x) + d \cdot g(x)) = c \cdot K + d \cdot L$$

as desired. ■

6.5.2.3 Product of limits

As was the case for sequences, our proof of the product of limits (and also the reciprocal of limits) relies the "trick" of rewriting

$$\begin{aligned} |f(x) \cdot g(x) - K \cdot L| &= |f(x) \cdot g(x) - f(x) \cdot L + f(x) \cdot L - K \cdot L| \\ &= |f(x)(g(x)-L) + L(f(x)-K)| \\ &\leq |f(x)| \cdot |g(x)-L| + |L| \cdot |f(x)-K|. \end{aligned}$$

So we again require some control over the size of the function close to $x = a$. Consequently we need lemma analogous to Lemma 6.5.5 that gives us a rigorous bound on $f(x)$ when x is close to a.

Lemma 6.5.9 *Let $a, K \in \mathbb{R}$ and let $f(x)$ be a function that converges to K as x approaches a. Then, there is some $\delta > 0$ so that when $0 < |x-a| < \delta$, we have*

$$\frac{|K|}{2} \leq |f(x)| \leq \frac{3|K|}{2}.$$

Now that we have this lemma we can proceed with the proof.

Proof of the product of limits. Let a, K, L, f, g be as in the statement of the lemma, and let $\varepsilon > 0$. Then we assemble the following three facts:

- Since $f(x) \to K$ as $x \to a$, there is some $\delta_K > 0$ so that when $0 < |x - a| < \delta_K$ we know that $|f(x) - K| < \frac{\varepsilon}{2|L|+1}$.
- Similarly, since $g(x) \to L$ as $x \to a$, there is some $\delta_L > 0$ so that when $0 < |x - a| < \delta_L$ we know that $|g(x) - L| < \frac{\varepsilon}{3|K|+1}$.
- Finally, since $f(x) \to L$ as $x \to a$, Lemma 6.5.9 tells us that there is some δ_f so that when $0 < |x - a| < \delta_f$ we know that $|f(x)| < \frac{3|K|}{2}$.

Notice that we have chosen denominators of $2|L| + 1$ and $3|K| + 1$ to avoid any problems that could arise if we had $L = 0$ or $K = 0$.

Now let $\delta = \min\{\delta_K, \delta_L, \delta_f\}$. Then when $0 < |x - a| < \delta$ we know that

$$|f(x)-K| < \frac{\varepsilon}{2|L|+1} \qquad \text{and} \qquad |g(x)-L| < \frac{\varepsilon}{3|K|+1} \qquad \text{and} \qquad |f(x)| < \frac{3|K|}{2}.$$

Then:

$$\begin{aligned}
|f(x) \cdot g(x) - K \cdot L| &= |f(x)(g(x) - L) + L(f(x) - K)| \\
&\leq |f(x)| \cdot |g(x) - L| + |L| \cdot |f(x) - K| \\
&\leq \frac{3|K|}{2} \cdot \frac{\varepsilon}{3|K|+1} + |L| \cdot \frac{\varepsilon}{2|L|+1} \\
&\frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.
\end{aligned}$$

Hence the result follows. ∎

6.5.2.4 Ratio of limits

As was the case for limits of sequences, we prove the limit of ratios of functions by first proving the limit of the reciprocal of a function and then using the above result on the limit of products to complete the result.

Proof of the reciprocal of limits. Let a, L and g be as stated, and let $\varepsilon > 0$ be arbitrary. Then

- since $\lim_{x\to a} g(x) = L$, there is some δ_L so that when $0 < |x - a| < \delta_L$, we know that
$$|g(x) - L| < \varepsilon\frac{|L|^2}{2},$$
- and similarly, since $\lim_{x\to a} g(x) = L$, Lemma 6.5.9 implies that there is some δ_g so that when $0 < |x - a| < \delta_g$, we know that $\frac{|L|}{2} < |g(x)|$.

Now pick $\delta = \min\{\delta_L, \delta_g\}$. Then whenever $0 < |x - a| < \delta$ we get

$$\left|\frac{1}{g(x)} - \frac{1}{L}\right| = \left|\frac{(L - g(x))}{L \cdot g(x)}\right|$$

$$= \frac{1}{|L|} \cdot \frac{1}{|g|} \cdot |g(x) - L|$$
$$< \frac{2}{|L|^2} \cdot \varepsilon \cdot \frac{|L|^2}{2} = \varepsilon.$$

Therefore the result follows. ■

Putting this result together with the result for the product of limits gives us the ratio of limits.

Proof of the ratio of limits. Let f and g be functions so that $\lim_{x\to a} f(x) = K$ and $\lim_{x\to a} g(x) = L \neq 0$. Then from Item d we see that

$$\lim_{x\to a} \frac{1}{g(x)} = \frac{1}{L}$$

and then by Item c we get

$$\lim_{x\to a} \left(\frac{f(x)}{g(x)}\right) = \lim_{x\to a} f(x) \cdot \lim_{x\to a} \left(\frac{1}{g(x)}\right)$$
$$= K \cdot \frac{1}{L} = \frac{K}{L}$$

Therefore the result follows. ■

6.6 Exercises

1. Prove that for all $n \in \mathbb{Z}$, $3 \mid (n^3 - n)$.

2. Prove that for all $n, k \in \mathbb{Z}$, if $k \mid (2n+1)$ and $k \mid (4n^2+1)$, then $k \in \{-1, 1\}$.

3. For all $n \in \mathbb{Z}$, prove that if there exists $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = n$, then $n \not\equiv 3 \pmod 4$.

4. Prove or disprove the following statement:

$$\forall a, b \in \mathbb{Z}, \text{ if } 3 \mid (a^2 + b^2), \text{ then } 3 \mid a \text{ and } 3 \mid b.$$

5. Let $n, a, b \in \mathbb{Z}$. We know that if $n \mid a$ or $n \mid b$, then $n \mid ab$. Is the converse true as well?

6. Let $f : \mathbb{R} \to \mathbb{R}$ be a function. We say that f is

- even if $f(-x) = f(x)$ for all $x \in \mathbb{R}$;
- odd if $f(-x) = -f(x)$ for all $x \in \mathbb{R}$.

Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$. If $f + g$ is odd, are f and g also odd?

7. Determine whether the following four statements are true or false. Explain your answers.

(a) $\exists x \in \mathbb{Z}$ s.t. $\exists y \in \mathbb{Z}$ s.t. $x + y = 3$.

(b) $\exists x \in \mathbb{Z}$ s.t. $\forall y \in \mathbb{Z}, x + y = 3$.

(c) $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ s.t. $x + y = 3$.

(d) $\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x + y = 3$.

8. Determine whether the following four statements are true or false. Explain your answers.

(a) $\exists x \in \mathbb{R}$ s.t. $\exists y \in \mathbb{R}$ s.t. $x^2 < y$.

(b) $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}, x^2 < y$.

(c) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $x^2 < y$.

(d) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, x^2 < y$.

9. Let $P \subset \mathbb{N}$ be the set of prime numbers $P = \{2, 3, 5, 7, 11, \ldots\}$. Determine whether the following statements are true or false. Prove your answers ("true" or "false" is not sufficient).

(a) $\forall x \in P$, $\forall y \in P$, $x + y \in P$.

(b) $\forall x \in P$, $\exists y \in P$ such that $x + y \in P$.

(c) $\exists x \in P$ such that $\forall y \in P$, $x + y \in P$.

(d) $\exists x \in P$ such that $\exists y \in P$, $x + y \in P$.

10. Given the sets,

$$A = \{n \in \mathbb{Z} \text{ s.t. } 3 \mid n\}, B = \{n \in \mathbb{Z} \text{ s.t. } 4 \nmid n\}, \text{ and } C = \{n \in \mathbb{Z} \text{ s.t. } 6 \nmid n\}$$

determine whether the following statements are true or false, and justify your answer.

(a) $\forall a \in A$, $\exists b \in B$ such that $a + b \in C$.

(b) $\exists a \in A$ such that $\forall b \in B$, $a + b \in C$.

(c) $\forall a \in A$, $\forall b \in B$, $a + b \in C$.

(d) $\exists a \in A$ and $\exists b \in B$ such that $a + b \in C$.

11. Determine whether the following statements are true or false. Explain your answers.

(a) $\exists x \in \mathbb{R}$ s.t. $\exists y \in \mathbb{R}$ s.t. $(xy > 0) \implies (x + y > 0)$.

(b) $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}, (xy > 0) \implies (x + y > 0)$.

(c) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $(xy > 0) \implies (x + y > 0)$.

(d) $\forall x \in \mathbb{R}, \forall y \in \mathbb{R}, (xy > 0) \implies (x + y > 0)$.

(e) $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}, (xy \geq 0) \implies (x + y \geq 0)$.

(f) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $(xy \geq 0) \implies (x + y \geq 0)$.

12. Determine whether the following four statements are true or false. Explain your answers.

(a) $\forall y \in \mathbb{R}, \forall z \in \mathbb{R}, \exists x \in \mathbb{R}$ s.t. $x + y = z$.

(b) $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}, \forall z \in \mathbb{R}, x + y = z$.

(c) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $\exists z \in \mathbb{R}$ s.t. if $z > y$ then $z > x + y$.

(d) $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $\forall z \in \mathbb{R}$, if $z > y$ then $z > x + y$.

13. Let $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be functions. For just this question,

- we call f *type A*, if $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $y \geq x$ and $|f(y)| \geq 1$, and
- we say that g is *type B* if $\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}$, if $y \geq x$, then $|g(y)| \geq 1$.

Prove or find a counterexample for the following statements.

(a) If a function is type A, then it is type B.

(b) If a function is type B, then it is type A.

14. Write down the negation of each of the following statements. Then determine whether each statement is true or false. Justify your answers.

(a) $\exists x \in \mathbb{Z}$ such that $(x > 84)$ and $x \equiv 75 \pmod{84}$.

(b) $\exists x, y \in \mathbb{Z}$ such that if $1 \geq x^2 \geq y^2$, then $x \geq y$.

(c) $\forall z \in \mathbb{N}$, $\exists x, y \in \mathbb{Z}$ such that $z = x^2 + y^2$.

(d) $\exists a \in \mathbb{R}$ such that $a > 0$ and $\forall x \in \mathbb{R}$, if $x \geq a$, then $2^{-x} < \dfrac{1}{100}$.

(e) $\forall n \in \mathbb{R}$, n is even if and only if n^2 is even.

15. Prove or disprove the following statements.

(a) $\forall a \in \mathbb{N}$, $\forall b \in \mathbb{N}$ if $b < a$, then $b - b^2 < a$.

(b) $\forall p \in \mathbb{N}$, $\forall q \in \mathbb{N}$, if $\sqrt{\dfrac{p}{q}} \in \mathbb{N}$, then $\sqrt{p} \in \mathbb{N}$ and $\sqrt{q} \in \mathbb{N}$.

(c) $\forall a, b \in \mathbb{R}$, $\exists c, d \in \mathbb{R}$, such that if $ab \geq cd$, then $a \geq c$ and $b \geq d$.

(d) $\forall a, b \in \mathbb{N}$, if $\exists x, y \in \mathbb{Z}$ and $\exists k \in \mathbb{N}$ such that $ax + by = k$, then $(k \mid a)$ and $(k \mid b)$.

16. Show that $\lim_{x \to 4} (-3x + 5) = -7$.

17. Show that $\lim_{x \to 1} x^2 = 1$.

18. Show that $\lim_{n \to \infty} 1/n^2 = 0$.

19. Let $f : \mathbb{R} - \{0\} \to \mathbb{R}$ be defined by

$$f(x) = 6x \sin\left(\frac{1}{x}\right).$$

Show that $\lim_{x \to 0} f(x) = 0$.

20. Prove that the sequence $(x_n)_{n \in \mathbb{N}} = \left((-1)^n + \frac{1}{n}\right)_{n \in \mathbb{N}}$ does not converge to 0.

21. Prove that

$$\lim_{n \to \infty} \left(1 - \frac{2}{n^2} - \frac{3}{n^3}\right) = 1.$$

You may use the following fact: Let x, y be positive real numbers. Then

$$\sqrt{x} < \sqrt{y} \iff x < y.$$

22. Let $(s_n)_{n \in \mathbb{N}}$ be a sequence. We say that $\lim_{n \to \infty} s_n = +\infty$ if the following holds:

$$\forall M > 0, \exists N \in \mathbb{N} \text{ such that } \forall n \in \mathbb{N}, n \geq N \implies s_n \geq M.$$

(a) In words, explain what the definition above means.

(b) Negate the statement above in order to describe what $\lim_{n \to \infty} s_n \neq +\infty$ means.

(c) Show that $\lim_{n \to \infty} \sqrt{n} = +\infty$

(d) Show that $\lim_{n \to \infty} (-1)^n \sqrt{n} \neq +\infty$

(e) Show that $\lim_{n \to \infty} (n^2 - 100n) = +\infty$

23. Let $\{a_n\}_{n \in \mathbb{N}}$ be a sequence. We say that a sequence $\{a_n\}_{n \in \mathbb{N}}$ is *bounded* if there is some $M \in \mathbb{R}$ such that $|a_n| \leq M$ for all $n \in \mathbb{N}$.

(a) Show that if $\lim_{n \to \infty} a_n = L$ for some $L \in \mathbb{R}$, then $\{a_n\}_{n \in \mathbb{N}}$ is bounded.

(b) Show that the converse of the statement in (a) is false.

24. Before completing this question, you should look over Exercise 6.6.23.

A sequence $(a_n)_{n \in \mathbb{N}}$ is *bounded* if there is some $M \geq 0$ such that $|a_n| \leq M$ for all $n \in \mathbb{N}$. If no such M exists, then we say $(a_n)_{n \in \mathbb{N}}$ is *unbounded*.

We say that $(a_n)_{n \in \mathbb{N}}$ is *increasing* if $a_{n+1} \geq a_n$ for all $n \in \mathbb{N}$.

(a) Show that there is an unbounded sequence $(a_n)_{n\in\mathbb{N}}$ with $\lim_{n\to\infty} a_n \neq +\infty$.

(b) Show that there is an increasing sequence $(a_n)_{n\in\mathbb{N}}$ with $\lim_{n\to\infty} a_n \neq +\infty$.

(c) Show that if $(a_n)_{n\in\mathbb{N}}$ is unbounded and increasing, then $\lim_{n\to\infty} a_n = +\infty$.

Parts (a) and (b) tell us that when proving the statement in part (c), we need to use both conditions given.

25. Typically, we define the distance between two real numbers via the absolute value function: $d(x,y) = |x-y|$. This means that we can see the distance as a function on real numbers that takes two numbers and gives us a non-negative number as the distance. This helps us generalize the definition of a "distance". However a function needs to satisfy more than being non-negative to be called a "distance".

Indeed, we define a *distance* (or *metric*) on $\mathbb{R}$, as a function $d : \mathbb{R}\times\mathbb{R} \to [0,\infty)$, that satisfies the properties,

- $\forall x, y \in \mathbb{R}$, $d(x,y) = 0$ if and only if $x = y$.
- $\forall x, y \in \mathbb{R}$, $d(x,y) = d(y,x)$.
- $\forall x, y, z \in \mathbb{R}$, $d(x,y) \leq d(x,z) + d(z,y)$ (this property is also known as, as you guessed it, the "triangle inequality").

Now, we can define the function $D : \mathbb{R}\times\mathbb{R} \to [0,\infty)$, as,

$$D(x,y) = \begin{cases} 1 & \text{if } x \neq y \\ 0 & \text{if } x = y \end{cases}$$

(a) We see that D satisfies the first two properties. Show that D satisfies the triangle inequality to conclude that D is a distance.

(b) Given a distance function, d, we can define sequence convergence as follows,

A sequence $(x_n)_{n\in\mathbb{N}}$ converges to a number L if and only if $\forall \varepsilon > 0$, $\exists N \in \mathbb{N}$ such that $\forall n > N$, $d(x_n, L) < \varepsilon$.

Using this definition and the distance function, D, as above, show that a sequence $(x_n)_{n\in\mathbb{N}}$ converges to L implies that the set $\{n \in \mathbb{N} : x_n \neq L\}$ is finite.

Chapter 7

Induction

In this text we started by doing a little bit of sets and a little logic. The aim of these brief introductions was to get you — our reader — started proving things as quickly as possible. We continued with a some basic logical equivalence to show us how to prove cases, biconditionals and contrapositives, and how to work with quantified statements. We have put these methods to work on some basic results on parity and divisibility; while those result were not terribly deep, their simplicity made them good places to learn our proof basics. We will soon apply all[77] of proof skills to more general mathematical problems, but we will first introduce a more specialised, but still extremely useful proof method. **Mathematical induction** is a method for proving statements of the form

$$\forall n \in \mathbb{N}, P(n).$$

The archetypal induction-proof example is the result

$$\text{For all } n \in \mathbb{N}, 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

or, to write it in a slightly more compact way

$$\forall n \in \mathbb{N}, \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Gauss learns to sum. Carl Friedrich Gauss (1777 – 1855) had a huge impact on many areas of mathematics; the interested reader should search-engine their way to more information. When he was in primary school his teacher (no doubt wanting to occupy their students for a while) set the problem of adding up $1 + 2 + \cdots + 99 + 100$. Gauss worked this out extremely quickly by realising that you can add numbers in pairs

$$1 + 100 = 101$$

[77]We still need to learn about **proof by contradiction**, but this author likes to leave that topic until the reader has had a chance to practice other proof methods.

$$2 + 99 = 101$$
$$3 + 98 = 101$$
$$\vdots$$

There are $n/2$ pairs, each adding to $n + 1$. This trick gives the above result and can be generalised, but best we still learn induction — it has uses way beyond sums.

Warning 7.0.1 The law of the instrument. Like any tool, induction is not guaranteed to work everywhere. However, like any tool, it is useful to have and part of learning to use the tool is to understand when it might help and when it might not. There is a tendency when one learns a nice new mathematical method that one tries to apply it to every problem that one comes across. This is often summarised as the **law of the instrument** — being the tendency to always use the same tool, even when it isn't the best tool for the job [78]. Anyway, with that caveat, the authors should get on with it and start talking about induction.

7.1 Induction

Induction, once you get past some of the technicalities, is a very intuitive idea. This author likes to think of induction like climbing an infinite ladder and an induction argument is really just a proof that we can climb that ladder. The proof is in 3 parts:

- If you can step onto the ladder, and
- from the current step you can reach the next step, then
- you can climb the ladder as high as you want.

As more concrete mathematical example, say we wish to prove

$$\text{For all } n \in \mathbb{N}, n^2 + 5n - 7 \text{ is odd.}$$

The dedicated reader may recall a very similar example in Chapter 5 and realise that we can do this using proof by cases, however, it is a good example for proof by "ladder idea".

- Step onto the ladder. When $n = 1$ the polynomial is $1 + 5 - 7 = -1$ which is odd. So the assertion is true for the very smallest value of n.
- Climb from one rung to the next. We wish to show that if the assertion is true for the current value of $n = k$, then it is also true for $n = k + 1$. That

[78] There are also variations of this rule that make reference to hammers — when you have a fancy new hammer, everything is a nail.

is, if we are on the current step, we can move up to the next step. So, to be more precise, we want to show that

$$(k^2 + 5k - 7 \text{ is odd}) \implies ((k+1)^2 + 5(k+1) - 7 \text{ is odd})$$

So this is just a little direct proof hiding inside our argument.

Proof: Assume $k^2 + 5k - 7 = 2\ell + 1$. Then

$$\begin{aligned}(k+1)^2 + 5(k+1) - 7 &= k^2 + 2k + 1 + 5k + 5 - 7 \\ &= \underbrace{k^2 + 5k - 7}_{=2\ell+1} + (2k+6) \\ &= 2(\ell + k + 3) + 1.\end{aligned}$$

Hence $(k+1)^2 + 5(k+1) - 7$ is odd as required.

- Conclusion. So how do we put these facts together? The first fact guarantees that our result is true for $n = 1$. Then the second fact tells us that since it is true for $n = 1$, it is also true for $n = 2$. But then since it is true for $n = 2$, it true for $n = 3$ (by the same fact). Applying that fact again and again gives us $n = 4, n = 5, n = 6, \cdots$.

Strictly speaking we have to be a bit more careful with that final "…", but we'll see how to do that below.

This proof method, **mathematical induction**, is formalised in the next theorem.

Theorem 7.1.1 The principle of mathematical induction. *For every $n \in \mathbb{N}$ let $P(n)$ be a statement. If*

- *$P(1)$ is a true statement, and*
- *the implication $P(k) \implies P(k+1)$ is true for all $k \in \mathbb{N}$*

then $P(n)$ is true for all $n \in \mathbb{N}$.

We can't quite give a complete proof of this theorem, though we can give almost everything that is needed. Call this a "proof sketch" — the core ideas are there, but we'll skip over a technicality and also write it a little informally.

Proof-sketch. Start by assuming the hypotheses of the theorem are true. That is, we assume that

- $P(1)$ is true, and
- the implication $P(k) \implies P(k+1)$ is true for all natural numbers k.

Then the core idea of the proof is construct two sets

- The "good" set:

  $$G = \{n \in \mathbb{N} \mid P(n) \text{ is true}\}$$

  This is the set of all n-values for which our statement is true. By assumption, we know that $1 \in G$, and $G \neq \varnothing$.

- The "bad" set:

$$B = \{n \in \mathbb{N} \mid P(n) \text{ is false}\}.$$

This is the set of all n-values for which our statement is false.

As is often the case, the "good" isn't as interesting as the "bad", and we'll focus on the set B. It is either empty or non-empty.

If B is empty, then we are done, because then $P(n)$ must be true for every single $n \in \mathbb{N}$ as required.

- As B is not empty, we can look for the smallest element in B. And since B is a non-empty set of natural numbers we can always find its smallest smallest element. However we do note that this is not possible for all sets — we'll come back to this point shortly.
- Let ℓ be this smallest number in B.
- From the hypothesis in the theorem, we know that $\ell > 1$ (since $P(1)$ is true).
- By the way we constructed B and ℓ, we know that $P(n)$ is true for all $1 \leq n < \ell$.
- Now we have a problem:
  - we know that $P(\ell - 1)$ is true, but
  - we also know that the implication $P(\ell - 1) \implies P(\ell)$ is true (since that is one of the hypotheses).
  - But if $P(\ell - 1)$ is true, and $P(\ell)$ is false, then that implication is false.
- This is a **contradiction** — our assumption is contradicted by $P(\ell)$ being false.
- The only way to resolve this situation is to conclude that no such ℓ exists — that is, B is empty.

Hence we must have $P(n)$ is true for all natural numbers n ■

There are two sneaky things going on in this proof. Firstly, we are doing a **proof by contradiction** by stealth; don't worry too much about this yet as we'll return to those proofs later in the text. Second, and more important in the short term, is that the proof relies on a delicate point

> since B is just a non-empty set of natural numbers, we can always find the smallest number in that set.

We are using here something called the **well ordering principle**. This guarantees us that we can always find the smallest element in a set of natural numbers. This is very definitely false for other sets of numbers — if we build a set of integers, or rational numbers, or real numbers, then it might not have a minimum.

Example 7.1.2 Sets without minima. Consider the following sets

$$\{2k \mid k \in \mathbb{Z}\} \qquad \left\{\frac{1}{n} \mid n \in \mathbb{N}\right\} \qquad (0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

None of these sets have minimum elements; you can always find another element that is smaller.

Solution. Note that this argument requires proof by contradiction and if the reader is confused by the details of this argument, we suggest that they wait until we have covered that topic and then return to this discussion. In fact, making this an example in that section is a good idea and the authors might do exactly that.

Consider the set $\{2k \mid k \in \mathbb{Z}\}$.

- Either this set has a minimum or it does not.
- If it does have a minimum, call that minimum ℓ.
- However, the number $\ell - 2$ is also in the set, and $\ell - 2 < \ell$.
- So ℓ cannot be the minimum.

So the set cannot have a minimum.

Similarly, if $(0, 1)$ has a minimum then call it q. But then since $0 < q < 1$, we know that $0 < q/2 < q$. So $q/2$ is in the set and smaller than q, so q cannot be a minimum. Hence no such minimum exists. The same argument works for the set $\{1/n \mid n \in \mathbb{N}\}$. □

Now that we are armed with a formal statement of **mathematical induction**, we should make use of it. The typical first example is the simple summation we saw in the introduction to this chapter. However (arguably) this can give the wrong idea of what induction is. To (hopefully) avoid this potential trap, let us do an example about divisibility.

Result 7.1.3 *For every natural number n, $3|(4^n - 1)$.*

So our statement is $P(n)$ is "$3|(4^n - 1)$". To prove this true for all naturals n using induction, we need to show

- The statement $P(1)$ is true, and
- The implications $P(k) \implies P(k + 1)$ is true for all $k \in \mathbb{N}$.

In most cases (but definitely not all), showing that $P(1)$ is true is easy, and proving the inductive step requires work.

- Setting $n = 1$ in our statement gives

  $$3|(4^1 - 1)$$

  which is true (since $4 - 1 = 3$).

- Now the harder part — the inductive step: We have to prove that

  $$(3|(4^k - 1)) \implies (3|(4^{k+1} - 1))$$

  for all $k \in \mathbb{N}$. That is, the inductive step requires us to prove an implication. As we have done many times before (and will do many times in the future), we assume the hypothesis is true and work our way to the conclusion. So we start by assuming that $3|(4^k - 1)$, which means that

  $$4^k - 1 = 3\ell \qquad \text{for some } \ell \in \mathbb{Z}$$

  and we want to arrive at

  $$4^{k+1} - 1 = 3m \qquad \text{so that} \qquad 3|(4^{k+1} - 1)$$

  We need to think about how we can construct $4^{k+1} - 1$ from $4^k - 1$. Multiplying by 4 is a good way to go:

  $$\begin{aligned} 4^k - 1 &= 3\ell \\ 4^k &= 3\ell + 1 \\ 4^{k+1} &= 12\ell + 4 \\ 4^{k+1} - 1 &= 12\ell + 3 = 3(4\ell + 1) \end{aligned}$$

  And since $4\ell + 1 \in \mathbb{Z}$ we have reached the conclusion we want.

Now that we know how to prove the base case (that was easy) and we know how to prove the inductive step (not too bad), we can put things together into a proof. Remember to tell the reader what we are doing.

Proof. We proceed by induction.

- Base case — When $n = 1$ the result is true since $3|(4 - 1)$.
- Inductive hypothesis — Assume $P(k)$ is true. Then $4^k - 1 = 3\ell$ for some $\ell \in \mathbb{Z}$. Then

  $$\begin{aligned} 4^{k+1} - 1 &= 4(4^k) - 1 \\ &= 4(4^k - 1) + 4 - 1 \\ &= 4 \cdot 3\ell + 3 = 3(4\ell + 1) \end{aligned}$$

  Thus if $P(k)$ then $P(k + 1)$.

By the principle of mathematical induction the statement is true for all naturals n. ■

Remark 7.1.4 Make structure obvious to the reader. Notice that we are making the structure of the proof very clear. We start by telling reader that we are using induction. We have then labelled the two conditions "base case" and "inductive hypothesis" or "inductive step", so that it is very clear how the proof is being constructed. We then have a little summarising sentence at the end saying "by induction it is true!" It means that a reader who is familiar with induction can readily check off each part of the induction proof against what they know about induction as they read the proof. We make it easy for them to read and verify the proof. (This is an especially good idea when someone has to mark your work, not just read it!)

We can rewrite our above simple parity example with this same structure. It is good practice.

Example 7.1.5 For all $n \in \mathbb{N}, n^2 + 5n - 7$ is odd.

Solution.

Proof. We use induction to prove the result.

- Base case. When $n = 1$, the polynomial gives $1 + 5 - 7 = -1$. Hence the base case is true.
- Inductive step. Assume that $k^2 + 5k - 7$ is odd, and so $k^2 + 5k - 7 = 2\ell + 1$. Then

  $$(k+1)^2 + 5(k+1) - 7 = 2k + 6 + (k^2 + 5k - 7) = 2(k+3) + 2\ell + 1$$

  and hence is also odd.

By mathematical induction the result holds for all $n \in \mathbb{N}$. ■

□

Extend to all $n \in \mathbb{Z}$. If we wish to prove this same result by induction but for all integers n, we could split the problem into 3. The first we just did, we could then prove it holds for $n = 0$ —easy! And then for negative integers we could rewrite the result as

$$\forall n \in \mathbb{N}, (-n)^2 + 5(-n) - 7 \text{ is odd.}$$

To avoid doing the very standard summation examples for a touch longer, we'll do an inequality. This particular example is another classic induction problem[79].

Result 7.1.6 *Let $n \in \mathbb{N}$ and let $x \in \mathbb{R}$ with $x > -1$. Then*

$$(1 + x)^n \geq 1 + nx.$$

If we choose to use induction (and we will), then it is a good idea to clarify what the actual statement is. Rewriting things carefully, we can write

$$P(n) : \text{if } (x > -1) \text{ then } (1 + x)^n \geq (1 + nx).$$

- First up, we verify the base case; setting $n = 1$ gives

  $$(x > -1) \implies (1 + x)^1 \geq 1 + x$$

[79]Like many of the authors "jokes" it is an antique and should be handled with care.

Since $(1+x)^1 = 1+x$, the conclusion is always true, so the implication is true, and the base case is true.

- Now the induction step. We assume that $P(k)$ is true. That is

$$(x > -1) \implies (1+x)^k \geq 1 + kx$$

is a true statement, and we then need to prove that

$$(x > -1) \implies (1+x)^{k+1} \geq 1 + (k+1)x.$$

To prove this second implication, we do as we have done so many times, and will do many times in the future, we assume the hypothesis is true. So we assume $(x > -1)$. From the first implication (and our assumption that $x > -1$) we know that $(1+x)^k \geq 1 + kx$. We now need to prove that $(1+x)^{k+1}$ is bigger than $1 + (k+1)x$.

A good place to start is to take the inequality we know and try to make it look like the inequality we want.

$$\begin{aligned} (1+x)^k &\geq 1 + kx && \text{multiply by } (1+x) \\ (1+x)^{k+1} &\geq (1+kx)(1+x) \\ &= 1 + (k+1)x + kx^2 \end{aligned}$$

Nearly there, we just need to get rid of this kx^2 term. We know $x^2 \geq 0$, so $kx^2 \geq 0$ and hence

$$(1+x)^{k+1} \geq 1 + (k+1)x + kx^2 \geq 1 + (k+1)x$$

as required.

But there is a problem: where have we used the assumption $x > -1$?

When you are doing mathematics and answering problems, you should keep your eyes open for this sort of thing. If you haven't used one of the hypotheses in your proof then there is very likely to be an error somewhere!

Now — our work above is not actually wrong, but that is more by luck than by design[80]. Where we multiplied by $1+x$ we didn't examine whether quantity is positive or negative. When we multiply an inequality by something positive (say $+2$), then inequality keeps the same sign:

$$2 \leq 3 \qquad\qquad \implies 4 \leq 6.$$

but when we multiply by something negative (say -2), the sign flips:

$$2 \leq 3 \qquad\qquad \implies (-4) \geq (-6)$$

[80]Of course the author actually designed the example to illustrate this luck. So perhaps it is designed luck?

Thankfully since $x > -1$, we know that $1 + x > 0$ and so we are not multiplying by a negative number. We don't have to go back and fix our scratch work, but we should make sure that we highlight this point when we write up the proof. We help our reader understand important subtle details by pointing them out.

Proof. We use induction.

- Based case: when $n = 1$, the statement is true since $(1 + x)^1 = 1 + 1 \cdot x$.

- Induction step. We assume that $x > -1$ and that $(1 + x)^k \geq 1 + kx$. Since $x > -1$, we know that $1 + x > 0$ and so multiplying through by $1 + x$ doesn't change the sign of the inequality:

$$\begin{aligned} (1+x)^k(1+x) &\geq (1+kx)(1+x) && \text{factor left and expand right} \\ (1+x)^{k+1} &\geq 1+(k+1)x+kx^2 && \text{since } x^2 \geq 0 \\ &\geq 1+(k+1)x \end{aligned}$$

  as required.

So by induction the inequality is true for all $n \in \mathbb{N}$. ■

Now we are ready to do the very standard summation example. But first a warning[81]:

Warning 7.1.7 Induction is not summation. Induction requires us to prove both that

- the base case, $P(1)$, is true, and

- the inductive hypothesis, $P(k) \implies P(k + 1)$, is true for all $k \in \mathbb{N}$.

Mathematical induction is not simply adding the next term to both sides of the equation.

With that out of the way:

Result 7.1.8 *For every natural number n, $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$*

- The base case is very easy (as it often is). When $n = 1$ we have:

$$\sum_{k=1}^{n} k = \frac{1 \cdot 2}{2} \qquad \text{which is}$$

$$1 = 1 \checkmark.$$

- As is typical, the inductive step needs a bit more work. We need to prove that

$$\left(1 + 2 + \cdots + k = \frac{k(k+1)}{2}\right) \implies \left(1 + 2 + \cdots + k + k + 1 = \frac{(k+1)(k+2)}{2}\right)$$

[81] A nag?

> Like most proofs of implications, we start by assuming the hypothesis is true and try to work our way to the conclusion. In this case, it is pretty clear that we can get from the first statement to the second just by adding $(k+1)$ to both sides. Note that "adding $k+1$ to both sides" is ***not*** the induction step. The induction step requires us to prove that $P(k) \implies P(k+1)$, and we prove that ***in this particular example*** by adding $k+1$ to both sides. This is a very common error (and more than a little frustrating to mark[82]).

We are now ready to write things up nicely.
Proof. We proceed by induction.

- Base case — When $n = 1$ the statement is true since $1 = \frac{1 \cdot 2}{2}$.
- Inductive hypothesis — Assume the statement is true for $n = k$, that is

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

  Adding $k+1$ to both sides gives

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

  Hence if the statement is true for $n = k$ then it must be true for $n = k+1$.

By the principle of mathematical induction it is true for all natural numbers n.
■

It is a good idea to see a few false induction proofs. Each of these examples contains a flaw.

Example 7.1.9 Polynomial primes. For all $n \in \mathbb{N}, n^2 - n + 41$ is prime.

We call the following argument a "misproof" since it looks like a proof, but is incorrect. In the solution below we explain why it is wrong.

[82] Be nice to your marker?

Misproof. We check the first values of n:

- $n = 1$: $1 - 1 + 41 = 41$ which is prime.
- $n = 2$: $4 - 2 + 41 = 43$ which is prime.
- $n = 3$: $9 - 3 + 41 = 47$ which is prime.
- $n = 4$: $16 - 4 + 41 = 53$ which is prime.
- $n = 5$: $25 - 5 + 41 = 61$ which is prime.

Since it is true for the first few values of n, it is true for all n. ■

Solution. This is a very wrong proof. ***Examples are not proof.***

Surprisingly this polynomial does give you prime numbers for $n = 1, \cdots, 40$. This was first noticed by Euler[83]. However when $n = 41$ it is clearly not prime, since it gives $41^2 - 41 + 41 = 41^2$. □

Example 7.1.10 Everything you know about 2 is wrong? For all $n \in \mathbb{N}$, $n + 1 < n$.

We give the flawed proof and then explain what is wrong with it in the solutions below.

Misproof. We prove this by induction. So assume that the statement is true for $n = k$. That is

$$k + 1 < k.$$

Then we can write, by adding 1 to both sides of the above inequality

$$(k + 2) < (k + 1)$$

And thus the statement is true for $n = k + 1$. By mathematical induction, the statement is true for all $n \in \mathbb{N}$. ■

Solution. This proof of the *inductive step* is perfectly correct. We have correctly shown that

$$(k + 1 < k) \implies (k + 2 < k + 1)$$

However this is a vacuous statement since the hypothesis is never true. This is the flaw in our proof — we did not check the base-case. When $n = 1$ the statement is false.

Since the base case fails, we cannot use mathematical induction. Both the base case and the inductive step must be true for an induction proof to work. □

Example 7.1.11 Pólya's colourless horses. This is George Pólya's proof that "All horses have the same colour".

Again, we'll first give the flawed proof, and then show you where it goes wrong.

---

[83]The interested reader should search-engine their way to "Euler's lucky numbers". There is actually some quite deep number theory lurking in side that polynomial.

Misproof. We proceed by induction.

- Base case: When there is only 1 horse, it has the same colour as itself. So the statement is true when there is exactly 1 horse.

- Inductive step: We assume the statement is true when there are $n = k$ horses. Now consider a set of $n = k + 1$ horses. Exclude one of those horses from the set to obtain a set of k horses. By assumption all those horses have the same colour. Put that excluded horse back into the set and remove another. Now the set again has k horses and so they all have the same colour. This means that all the $k + 1$ horses (including the two we temporarily removed) must have the same colour.

By induction the statement is true for all $n \in \mathbb{N}$. ■

Solution. So what is wrong here? There is a subtle error in the inductive step. Remember that the inductive step has to be true for all $k \in \mathbb{N}$, however it contains the tacit assumption that k is not too small. To see why, step through the argument carefully when $k = 1$.

Assume that the statement is true when $n = k = 1$. Then consider a set of $n = k + 1 = 2$ horses: call them Alice and Bob[84]. Now we remove one horse (Alice), and then every horse remaining in the set (which is just Bob) has the same colour. Now we put Alice back and take Bob out. So Alice has the same colour as every horse in the set — which is just Alice. At no point do we ever compare the colour of Alice or Bob with a third horse[85]. Consequently we cannot infer any relationship between the colours of equine Alice or Bob. □

7.2 More general inductions

7.2.1 A little more general

There was nothing special about starting at $n = 1$ in our proof-sketch of the principle of mathematical induction. All that was required was that we could find the smallest integer in a set of natural numbers. We can quite readily generalise the proof to other sets of integers — as long as we can find the smallest integer in that set. So for example, instead of considering $P(n)$ for all natural numbers n, we could consider $P(n)$ for all integer $n \geq -3$, or all integers $n \geq 7$ and so forth.

This idea leads to a slightly more general form of mathematical induction. The only differences are that the base case need not be at $n = 1$, and that the inductive step must now be true for all integer k starting from the value in the base case. This is sometimes called **extended mathematical induction**.

Theorem 7.2.1 Principle of mathematical induction. *For a fixed integer ℓ, let $S = \{n \in \mathbb{Z} \mid n \geq \ell\}$. For each integer $n \in S$, let $P(n)$ be a statement. If*

[84] Very traditional names for horses with side-interests in cryptography.
[85] A stalking horse? A dark horse?

- *$P(\ell)$ is true, and*
- *if the implication $P(k) \implies P(k+1)$ is true for all $k \in S$*

then $P(n)$ is true for all $n \in S$.

We should put this theorem to work:

Result 7.2.2 *For every integer $n \geq 5$, $2^n \geq n^2$.*

The proof of this result is nearly the same as our previous induction proofs; it consists of a basis case and an inductive step. The difference is that the basis step starts at $n = 5$.

- When $n = 5$ the inequality is $2^5 = 32 \geq 5^2 = 25$, which is true.
- For the inductive step we need to prove that

$$\left(2^k > k^2\right) \implies \left(2^{k+1} > (k+1)^2\right)$$

So we assume the first inequality, $2^k > k^2$, and have to work our way to the second, $2^{k+1} > (k+1)^2$. Multiplying the original inequality by 2 might be a good place to start.

$$2 \cdot 2^k = 2^{k+1} > 2k^2$$

So we need to show that $2k^2 \geq (k+1)^2$ or $k^2 \geq 2k+1$. Well since $k \geq 5$ we have $k^2 \geq 5k = 2k + 3k$ and since $k > 1$, $3k > 1$ and we are done.

Now we can write it up nicely.
Proof. We proceed by induction.

- Basis step — when $n = 5$ we have $2^5 = 32 > 5^2 = 25$. Hence the statement is true for $n = 5$.
- Inductive hypothesis — assume $2^k > k^2$. Then $2^{k+1} = 2 \cdot 2^k > 2k^2$. Since $k \geq 5$ we have $k^2 \geq 5k$, and hence

$$2^{k+1} > 2k^2 = k^2 + k^2 = k^2 + 5k = k^2 + 2k + 3k.$$

Now since $k \geq 5$, we know that $3k > 1$, and so

$$2^{k+1} > k^2 + 2k + 1 = (k+1)^2$$

Thus if $P(k)$ is true then $P(k+1)$ is true.

By the principle of mathematical induction the statement is true for all $n \geq 5$. ■

It's not a discussion of induction without some summation example.

Result 7.2.3 *Let $a \in \mathbb{Z}$, then*

$$a + (a+1) + \cdots + n = \sum_{j=a}^{n} j = \frac{(n+a)(n+1-a)}{2}$$

Proof. We prove this by induction. When $n = a$ we have $\frac{(a+a)(a+1-a)}{2} = a$ as required, so the base case holds.

Now assume that the result holds for $n = k$. Hence

$$\begin{aligned} a + (a+1) + \cdots + k &= \frac{(k+a)(k+1-a)}{2} \qquad \text{and so} \\ a + (a+1) + \cdots + k + (k+1) &= \frac{(k+a)(k+1-a)}{2} + (k+1) \\ &= \frac{1}{2}\left(k^2 + 3k + 2 + a - a^2\right) \\ &= \frac{1}{2}\left(k+1+a)(k+2-a)\right) \end{aligned}$$

as required. Since both the base case and induction step hold, the result follows by induction. ■

Here is another inequality result

Result 7.2.4 *For any integer $n \geq 4$, $n! > 2^n$.*
Proof. We prove the result by induction. When $n = 4$ we have

$$4! = 24 > 16 = 2^4$$

so the base case is true.

Let us now assume that $k! > 2^k$. Then

$$\begin{aligned} k! &> 2^k \\ (k+1)k! &> (k+1)2^k \\ (k+1)! &> (2 + (k-1))2^k \\ &= 2^{k+1} + (k-1)2^k > 2^{k+1} \end{aligned}$$

where we have used the fact that $(k+1) > 0$ and $(k-1) \geq 0$.

Since both the base case and induction hypothesis are true, the result follows by the principle of mathematical induction. ■

These inequality induction problems tend to be the most tricky of these 3 standard induction questions. Induction has its uses way beyond summation, divisibility and inequalities. Here are some more diverse examples.

Result 7.2.5 *For any integer $n \geq 3$, one can always find n distinct natural numbers $\{a_1, a_2, \cdots, a_n\}$ so that*

$$1 = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

As an example:

$$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}.$$

Proof. We prove this result by induction. When $n = 3$, the result holds (as was stated above) with the set $\{2, 3, 6\}$.

Now assume the result holds for $n = k$. Hence there is a set $\{a_1, a_2, \cdots, a_k\}$ so that

$$1 = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_k}$$

Notice two things. First, none of the a_i can be one, because otherwise the sum would be too large. Second, by dividing by two we get

$$\frac{1}{2} = \frac{1}{2a_1} + \frac{1}{2a_2} + \cdots + \frac{1}{2a_k}$$

So we can make a new set of $k+1$ numbers $\{2, 2a_1, 2a_2, \ldots, 2a_k\}$ so that the sum of their reciprocals is

$$\frac{1}{2} + \underbrace{\frac{1}{2a_1} + \frac{1}{2a_2} + \cdots + \frac{1}{2a_k}}_{=\frac{1}{2}} = 1$$

as required.

Since the base case is true, and the induction hypothesis is true, the result follows by mathematical induction.

Note that instead of dividing everything by two, one could also "split" the largest number in the set via

$$\frac{1}{x} = \frac{1}{1+x} + \frac{1}{x(x+1)},$$

since

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

■

Egyptian fractions. The result above is an example of writing a rational number as an **Egyptian fraction**. More generally, an Egyptian fraction is a sum of reciprocals of integers. For example

$$\frac{17}{12} = \frac{1}{1} + \frac{1}{3} + \frac{1}{12}.$$

The interested reader should work out how to write any given rational number in this way.

The next two examples are calculus-flavoured and so we assume some understanding[86] of results on derivatives and integrals. Those ideas are not covered in

[86] That is, some standard results from typical Calculus-1 and -2 courses on differential and

this text (except as a way of constructing some nice examples and exercises).

Result 7.2.6 *Let* $n \in \mathbb{N}, f(x) = x\log(x)$ *and use* $f^{(n)}(x)$ *to denote the* n^{th} *derivative of* $f(x)$*. Then for any* $n \geq 2$

$$f^{(n)}(x) = (-1)^n \frac{(n-2)!}{x^{n-1}}$$

Note that we are using $\log x$ *to denote the* ***natural logarithm****.*

Proof. We prove the result by induction. Let f be as defined in the statement of the result.

First note that

$$\begin{aligned} f(x) &= x\log x \\ f'(x) &= 1 + \log x \\ f''(x) &= \frac{1}{x} \end{aligned}$$

and hence the result holds for $n = 2$.

Assume the result holds for $n = k$, then

$$\begin{aligned} \frac{\mathrm{d}}{\mathrm{d}x} f^{(k)}(x) &= \frac{\mathrm{d}}{\mathrm{d}x}(-1)^k \frac{(k-2)!}{x^{k-1}} \\ &= (-1)^k (k-2)! \cdot (-1)(k-1)x^{-k} \\ &= (-1)^{k+1} \frac{(k-1)!}{x^k} \end{aligned}$$

as required. Since the base case and inductive step hold, the result follows by induction. ■

Result 7.2.7 *For every integer* $n \geq 0$,

$$n! = \int_0^\infty x^n e^{-x} \mathrm{d}x$$

To prove this result we'll make use of the following fact (which you probably covered in a calculus course).

Fact 7.2.8 *For any* $n \in \mathbb{Z}$,

$$\lim_{x\to\infty} \frac{x^n}{e^x} = 0.$$

Proof of Result 7.2.7. We prove this by induction.

- When $n = 0$ we have

$$\begin{aligned} \int_0^\infty e^{-x}\mathrm{d}x &= \left[-e^{-x}\right]_0^\infty \\ &= 1 - \lim_{b\to\infty} e^{-b} \end{aligned}$$

integral calculus.

$$= 1 - 0 = 1 = 0!$$

where we have used Fact 7.2.8 to evaluate the limit. Hence the base case is true.

- Assume that the result holds for $n = k$. Then we evaluate the integral for $n = k + 1$ using integration by parts.

$$\begin{aligned}\int_0^\infty x^{k+1}e^{-x}\mathrm{d}x &= \left[-e^{-x}x^{k+1}\right]_0^\infty + \int_0^\infty (k+1)x^k e^{-x}\mathrm{d}x \\ &= (k+1)\int_0^\infty x^k e^{-x}\mathrm{d}x + 0 - \lim_{b\to 0} e^{-x}x^{k+1} \\ &= (k+1)\int_0^\infty x^k e^{-x}\mathrm{d}x \\ &= (k+1)k! = (k+1)!\end{aligned}$$

as required. Again we have used Fact 7.2.8 to evaluate the limits.

By the principle of mathematical induction, the result holds for all $n \geq 0$. ■

7.2.2 More general and yet equivalent

We can generalise induction yet further with a *stronger* hypothesis in the induction step. In particular, we can set up induction so that we use all of the earlier statements $P(\ell), \cdots, P(k)$ to prove the next $P(k+1)$. This stronger hypothesis gives the result its name, rather than the actual result being stronger. We have called this a corollary because one can prove it from regular induction (and we will). In fact, it is equivalent to regular induction, which we can show by proving regular induction from strong induction.

Corollary 7.2.9 Strong induction. *For a fixed integer ℓ, let $S = \{n \in \mathbb{Z} \mid n \geq \ell\}$. For each integer $n \in S$, let $P(n)$ be a statement. If*

- *$P(\ell)$ is true, and*
- *if the implication $P(\ell) \wedge P(\ell+1) \wedge \cdots \wedge P(k) \implies P(k+1)$ is true for all $k \in S$*

then $P(n)$ is true for all $n \in S$.

Proof. As always, we start by assuming the hypotheses are true and work our way to the conclusion. So assume that $P(\ell)$ is true, and that $P(\ell) \wedge P(\ell+1) \wedge \cdots \wedge P(k) \implies P(k+1)$ is true for all $k \in S$.

To use regular induction we use a little trick. Let $Q(n)$ be the statement

$$P(\ell), P(\ell+1), \cdots, P(n) \text{ are all true}$$

Then since $P(1)$ is true, we know that $Q(1)$ is true. Further, since we know that

$$P(\ell) \wedge P(\ell+1) \wedge \cdots \wedge P(k) \implies P(k+1)$$

then if $Q(k)$ is true, then $Q(k+1)$ is true. Hence $Q(k) \implies Q(k+1)$ is true. By (regular) mathematical induction, we know that $Q(n)$ is true for all $n \in S$, and so $P(n)$ is true for all $n \in S$ as required. ∎

We can actually go further and prove that strong induction implies regular induction. This proves that the two types of induction are actually equivalent to each other. Anything you can prove with one, you can prove with the other; though that does not say the proofs would be equally appealing.

Corollary 7.2.10 Strong implies weak. *Strong induction is equivalent to regular induction.*

Proof. We are actually proving here that Strong Induction (Corollary 7.2.9) if and only if Mathematical Induction (Theorem 7.2.1). We have already proved that regular induction implies strong induction in the proof of Corollary 7.2.9, so it is sufficient for us to prove that strong induction implies regular induction.

Assume the hypothesis of regular induction. That is $P(\ell)$ is true and $P(k) \implies P(k+1)$ for any $k \in S$. Again a small trick can be used:

$$P(\ell) \wedge P(\ell+1) \wedge \cdots \wedge P(k) \implies P(k)$$

The only way the above can be false is if the hypothesis is true but the conclusion is false. That cannot happen because $P(k)$ appears in the conjunction of the hypothesis (and so must be true) and as the conclusion. Put this above together with the assumption $P(k) \implies P(k+1)$:

$$P(\ell) \wedge P(\ell+1) \wedge \cdots \wedge P(k) \implies P(k) \implies P(k+1)$$

and we have satisfied the hypotheses of strong induction. Hence $P(n)$ is true for all $n \in S$. ∎

Result 7.2.11 *Any integer $n \geq 12$ can be written as a sum of 3's and 7's. That is we can find non-negative integer a, b so that $n = 3a + 7b$.*

Proof. We prove this by strong induction.

- When $n = 12$, we can set $a = 4, b = 0$. Then since $12 = 3 \times 4$ the result holds.

- The inductive step is simpler if we also show that the result holds for $n = 13, 14$. In particular since $13 = 2 \times 3 + 7$ and $14 = 2 \times 7$, the result is true for $n = 12, 13, 14$.

- Now assume that the result holds for all $n = 12, 13, 14 \ldots, k$, with $k \geq 14$, and so we can write $k-2 = 3a+7b$. Then it follows that $k+1 = 3+(k-2) = 3(a+1) + 7b$ and so has the required form. That is, since the result holds for all $n = 12, \ldots, k$, we know that it holds for $n = k+1$.

So by strong induction, the result holds for all integer $n \geq 12$. ∎

Result 7.2.12 *Let $z \in \mathbb{R}$ be any real number so that $z + z^{-1} \in \mathbb{Z}$. Then for any integer n, $z^n + z^{-n} \in \mathbb{Z}$*

Proof. To simplify the discussion, let q_n denote $z^n + z^{-n}$. By assumption we have that $q_1 \in \mathbb{Z}$. Further note that $q_{-n} = q_n$ so it is sufficient to prove that $q_n \in \mathbb{Z}$ for all integer $n \geq 0$; we do so by induction.

When $n = 0$, we have

$$z^0 + z^{-0} = q_0 = 2 \in \mathbb{Z}$$

so the result holds.

Now assume that the result holds for $0 \leq n \leq k$. So we know that q_1, q_{k-1}, q_k are integers. Hence

$$\begin{aligned} q_k q_1 &= (z^k + z^{-k})(z + z^{-1}) \\ &= z^{k+1} + z^{k-1} + z^{1-k} + z^{-k-1} \\ &= \underbrace{z^{k-1} + z^{1-k}}_{=q_{k-1}} + \underbrace{z^{k+1} + z^{-1-k}}_{=q_{k+1}} \end{aligned}$$

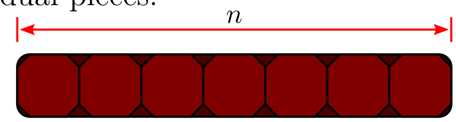
So we have

$$q_{k+1} = q_k q_1 - q_{k-1}$$

Since $q_1, q_{k-1}, q_k \in \mathbb{Z}$ we know that $q_{k+1} \in \mathbb{Z}$ as required. The result then follows by mathematical induction. ■

A chocolate bar example.

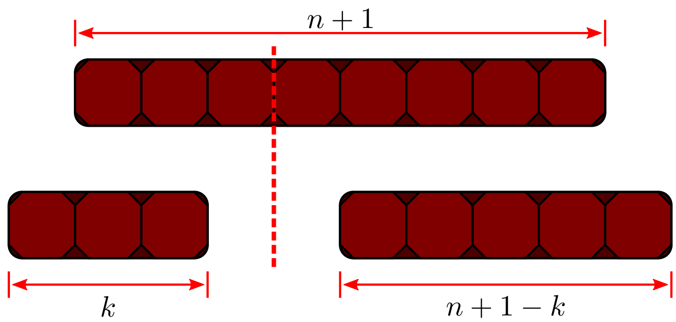
Example 7.2.13 Breaking a bar of chocolate. Say we have a bar of chocolate as shown below — a line of n blocks. Prove that it takes $n - 1$ breaks to split it into n individual pieces.



We prove this by strong induction.

- First, when $n = 1$, there is nothing to do; it takes 0 breaks to split it into 1 block. The result holds.

- Now assume that the result holds for bars of $1, 2, \ldots, n$ blocks, and then consider a bar of $n + 1$ blocks. Say we split it into two pieces, one of size k, and one of size $n + 1 - k$ (with $k = 1, 2, \ldots, n$). This takes 1 break, and we are left with the problem of splitting up the bar of k blocks and the bar of $n + 1 - k$ blocks (as shown below).



> However, by assumption, we know that splitting a bar of k blocks takes $k-1$ breaks, and splitting a bar of $n+1-k$ blocks takes $n-k$ breaks. So, in total we'll need $1+k-1+n-k=n$ breaks. Notice that this is independent of our choice k. Hence the result holds for a bar of $n+1$ blocks.

By strong induction the result holds for all n.

A slightly higher dimensional analogue of this problem involves cutting a pizza using n straight slices. The interested reader should search-engine their way to the "lazy caterer sequence", or (equivalently) the central polygonal numbers. Going up one more dimension one arrives at the "cake numbers" which define the number of chunks of cake you can make when slicing a cube with n-planes. □

Here is a more gamey example.

Example 7.2.14 A game of taking away. Let n be a natural number. Two players place n balls in a box. The players take turns removing either one, two or three balls from the box. The player that removes the last ball loses.

So for example, if there are 13 balls in the box, the game could play out as

- Player 1 removes 3 balls, leaving 10
- Player 2 then removes 2 balls, leaving 8
- Player 1 removes another 3 balls, leaving 5
- Player 2 removes 2 balls, leaving 3
- Player 1 removes 2 balls leaving 1
- Player 2 now must remove the last ball and so loses the game.

We can prove that if $n \equiv 1 \pmod 4$, then Player 2 can always win (if they are careful). We prove this by strong induction.

When the game starts with $n = 1 = 4 \times 0 + 1$ balls, Player 1 must remove the only ball from box and so loses.

Now assume that Player 2 can always win when $n = 4\ell+1$ for $n = 1, 5, \ldots, 4\ell+1$. Now consider what happens when the box starts with $n = 4\ell + 5$ balls. Since Player 2 knows how to win if they leave Player 1 with $4\ell + 1$ balls, they will respond to Player 1's move by trying to get to $4\ell + 1$ balls.

- If Player 1 removes 1 ball, then this gives $4\ell + 4$, and so Player 2 takes 3 balls
- If Player 1 removes 2 balls, then this gives $4\ell + 3$, and so Player 2 takes 2 balls
- If Player 1 removes 3 balls, then this gives $4\ell + 2$, and so Player 2 takes 1 ball

So, no matter what Player 1 does, Player 2 can choose their move so as to leave Player 1 with $4\ell + 1$ balls. From that point, by assumption, Player 2 has a winning strategy.

So by strong induction, Player 2 has a winning strategy whenever $n = 4\ell + 1$. □

Here are a couple of examples involving the Fibonacci numbers. Even those these are well known we'll take a moment to define them formally.

Definition 7.2.15 The **Fibonacci numbers** are defined recursively[87] by

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+1} = F_n + F_{n-1}.$$

The first few Fibonacci numbers are $0, 1, 1, 2, 3, 5, 8, 13, \ldots$ ♢

The Fibonacci numbers have many interesting properties and patterns. They also show up all over mathematics and one can find (via the reader's favourite search engine) many examples of Fibonacci numbers in the "real world". We'll start off with an easy result that doesn't require strong induction and then work up towards some harder ones.

Result 7.2.16 *The Fibonacci numbers satisfy*

$$\sum_{\ell=1}^{n} F_\ell = F_{n+2} - 1.$$

Proof. We prove this by induction. When $n = 1$ the statement becomes

$$F_1 = F_3 - 1$$

and since $F_1 = 1, F_3 = 2$ it is true.

Now assume that the result holds for $n = k$. That is

$$F_1 + F_2 + \cdots + F_k = F_{k+2} - 1$$

Then we have

$$\begin{aligned} F_1 + F_2 + \cdots + F_k + F_{k+1} &= F_{k+1} + F_{k+2} - 1 \\ &= F_{k+3} - 1 \end{aligned}$$

as required. Since both the base case and inductive step are true, the result follows by induction. ■

[87] i.e. we give the first few Fibonacci numbers, and then we define later Fibonacci numbers in terms of earlier Fibonacci numbers.

Result 7.2.17 *The Fibonacci numbers satisfy*

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

This is known as Cassini's identity.
Proof. We prove this by induction. When $n = 1$:

$$F_2F_0 - F_1^2 = 0 - 1 = -1$$

as required.

Now assume that it holds for $n = k$, so that

$$F_{k+1}F_{k-1} - F_k^2 = (-1)^k$$

Now consider

$$\begin{aligned} F_{k+2}F_k - F_{k+1}^2 &= (F_{k+1} + F_k)F_k - (F_k + F_{k-1})F_{k+1} \\ &= \underbrace{F_{k+1}F_k} + F_k^2 - \underbrace{F_kF_{k+1}} - F_{k-1}F_{k+1} \\ &= F_k^2 - F_{k-1}F_{k+1} \\ &= -(F_{k+1}F_{k-1} - F_k^2) \\ &= (-1)^{k+1} \end{aligned}$$

as required. Since both the base case and inductive step hold, the result follows by induction. ■

Result 7.2.18 *Let $q \in \mathbb{N}$. Then $5 \mid F_{5n}$ for all $n \in \mathbb{N}$.*
Proof. Fix $q \in \mathbb{N}$. We prove the result by induction. When $n = 1$ the result holds since $F_5 = 5$.

Now assume that $5 \mid F_{5k}$. Now

$$\begin{aligned} F_{5k+5} &= F_{5k+4} + F_{5k+3} \\ &= (F_{5k+3} + F_{5k+2}) + F_{5k+3} = 2F_{5k+3} + F_{5k+2} \\ &= 2(F_{5k+2} + 2F_{5k+1}) + F_{k+2} = 3F_{5k+2} + 2F_{5k+1} \\ &= 3(F_{5k+1} + F_{5k}) + 2F_{5k+1} = 5F_{5k+1} + 3F_{5k} \end{aligned}$$

Now since $5 \mid F_{5k}$ it follows that $5 \mid F_{5k+5}$. The result follows by induction. ■

Result 7.2.19 *The Fibonacci numbers satisfy*

$$\begin{aligned} F_{2n-1} &= F_n^2 + F_{n-1}^2 \qquad \textit{and} \\ F_{2n} &= F_{n+1}^2 - F_{n-1}^2. \end{aligned}$$

Proof. Induction is not the easiest way to prove these, but we will press on. The results hold when $n = 1$ since

$$\begin{aligned} F_1 &= 1 = 1^2 + 0^2 = F_1^2 + F_0^2 \\ F_2 &= 1 = 1^2 - 0^2 = F_2^2 - F_0^2 \end{aligned}$$

Now assume the result holds for all $k \leq n$. Now from the recurrence that defines the Fibonacci numbers:

$$\begin{aligned} F_{2k+1} &= F_{2k} + F_{2k-1} \\ &= (F_{k+1}^2 - F_{k-1}^2) + (F_k^2 + F_{k-1}^2) && \text{by assumption} \\ &= F_{k+1}^2 + F_k^2 \end{aligned}$$

as required. We do similarly for the other equation (though more gymnastics are required).

$$\begin{aligned} F_{2k+2} &= F_{2k+1} + F_{2k} \\ &= (F_{k+1}^2 + F_k^2) + (F_{k+1}^2 - F_{k-1}^2) \end{aligned}$$

Try to make the first bracket look like $F_{k+2}^2 = (F_{k+1} + F_k)^2$

$$= (F_{k+1}^2 \underbrace{+2F_{k+1}F_k}_{+} + F_k^2) + (F_{k+1}^2 - F_{k-1}^2) \underbrace{-2F_kF_{k+1}}_{-}$$

Now manipulate the second bracket using difference of squares and then $F_{k+1} - F_{k-1} = F_k$

$$\begin{aligned} &= (F_{k+1} + F_k)^2 + (F_{k+1} - F_{k-1})(F_{k+1} + F_{k-1}) - 2F_kF_{k+1} \\ &= F_{k+2}^2 + F_k(F_{k+1} + F_{k-1} - 2F_{k+1}) \\ &= F_{k+2}^2 - F_k(F_{k+1} - F_{k-1}) \\ &= F_{k+2}^2 - F_k^2 \end{aligned}$$

as required.

Since the base case is true and the inductive step is true, the result follows by induction. ■

Next is an important example that proves every integer bigger than 2 can be written as a product of prime numbers. This statement is part of the Fundamental Theorem of Arithmetic, which also says that the product is *unique*. Proving uniqueness takes more work — see Section 9.6. This result focuses on proving the *existence* of at least one factorisation into primes.

This is also a really good example of a result that we all know, but we haven't proved. When we do sit down to try to prove such results it can be easy to get confused or disoriented because the result seems so obvious; we've known and worked with the result for years! Some such results may indeed be trivial while some need more work. It is always a good idea to go back to the basic definitions and methods to help work your way to a proof.

Example 7.2.20 There exists a prime factorisation. Let $n \in \mathbb{N}$, $n \geq 2$. Then n is a product of prime numbers.

Scratchwork. Notice that the statement includes the case where n is prime, whence n is the product of a single prime — itself! Then, any integer greater than

2 is prime or not prime. If it is not prime, what can we say about its divisors?

Let's try to prove the statement using induction on n. The base case should be $n = 2$. In this case, the statement is true, since 2 is prime, and therefore a product of prime numbers (in this case, the product of a single prime number, 2). Now suppose the result holds for $n = k$, so that $n = k$ is a product of prime numbers. We need to show that $k + 1$ is a product of prime numbers. We can try to prove this by considering two cases: $k + 1$ is prime, or $k + 1$ is not prime, one of which must be true.

- $k + 1$ is prime: then the result holds for $n = k + 1$, so we're done.

- $k + 1$ is not prime: here we can't conclude anything immediately. Instead we'll try to use the inductive hypothesis to show that the result holds. By definition, $k + 1$ not being prime means that there are $a, b \in \mathbb{N}$, $1 < a, b < k + 1$, such that $k + 1 = ab$.

  Now, if we knew a and b could be written as a product of prime numbers, then we'd also have that $k+1$ is a product of prime numbers. But we don't know this, since for the inductive hypothesis, we only assumed that $n = k$ could be written as a product of prime numbers. Indeed, it is not clear how we can get from $n = k$ to $n = k + 1$ in our inductive step since k and $k + 1$ don't share common factors other than ± 1 (see Exercise 3.5.7). This suggests that we use strong induction instead of regular induction.

Let's try again using strong induction. The base case is the same as before. This time, for the inductive hypothesis, instead of just assuming that $n = k$ is a product of prime numbers, we assume that for any $2 \leq n \leq k$, n is a product of prime numbers. We need to show that $k + 1$ is a product of prime numbers. Again we can split this into two cases.

- $k + 1$ is prime: then the result holds for $n = k + 1$, so we're done.

- $k + 1$ is not prime: By definition, $k + 1$ not being prime means that there are $a, b \in \mathbb{N}$, $1 < a, b < k + 1$, such that $k + 1 = ab$. By the inductive hypothesis, both a and b can be written as a product of prime numbers; that is $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$ for prime numbers $p_1, \ldots, p_r, q_1, \ldots, q_s$. (Note that these prime numbers are not necessarily distinct, and if a or b were itself prime, then $r = 1$ or $s = 1$, respectively.) Then

  $$k + 1 = ab = p_1 \cdots p_r q_1 \cdots q_s$$

  and so $k + 1$ may be written as a product of prime numbers.

In either case, we've concluded that $k + 1$ is a product of prime numbers, and so the inductive step is complete. Let's write up our argument.

Solution.

Proof. Let $n \in \mathbb{N}$, $n \geq 2$. We proceed by strong induction on n. For the base case, suppose $n = 2$. Then n is prime, and the result holds.

Now suppose that the result holds for all $2 \le n \le k$; that is, if $n \le k$, then n is a product of prime numbers. Either $k+1$ is prime, or not prime. If $k+1$ is prime, then the result holds. So suppose that $k+1$ is not prime. Then, by definition, $k+1 = ab$ for some $a, b \in \mathbb{N}$, $1 < a, b < k+1$. By the inductive hypothesis, both a and b can be written as a product of prime numbers; that is $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$ for prime numbers $p_1, \ldots, p_r, q_1, \ldots, q_s$. Then

$$k + 1 = ab = p_1 \cdots p_r q_1 \cdots q_s$$

and so $k+1$ may be written as a product of prime numbers. Thus the result holds for $k+1$. Thus by strong induction, any $n \in \mathbb{N}$, $n \ge 2$ is a product of prime numbers. ■

□

Finally, a nice trigonometric example[88]. We'll assume that you remember (or can quickly revise) the formulas

$$\cos(a + b) = \cos a \cos b - \sin a \sin b$$
$$\cos(a - b) = \cos a \cos b + \sin a \sin b$$

Result 7.2.21 *Let $\theta \in \mathbb{R}$ be fixed. Let $p_0 = 1$ and $p_1 = \cos\theta$ and define $p_n = 2p_1 p_{n-1} - p_{n-2}$. Prove that $p_n = \cos(n\theta)$ for all integer $n \ge 0$.*

Proof. We prove the result by induction. When $n = 0$ we have $p_0 = \cos 0 = 1$, so the base case is true. We now turn to the inductive step.

Assume that the result hold for $n = 0, 1, \cdots, k$. In particular,

$$p_1 = \cos\theta \qquad\qquad p_k = \cos k\theta$$

Now it suffices to show that $p_{k+1} = 2p_1 p_k - p_{k-1} = \cos((k+1)\theta)$. Substitute in the values of p_1, p_k, p_{k-1}:

$$p_{k+1} = 2\cos\theta\cos(k\theta) - \cos((k-1)\theta)$$

Recall (from the formulas above) that

$$\cos((k+1)\theta) = \cos\theta\cos k\theta - \sin\theta\sin k\theta \qquad \text{and}$$
$$\cos((k-1)\theta) = \cos\theta\cos k\theta + \sin\theta\sin k\theta$$

so that

$$\cos((k+1)\theta) + \cos((k-1)\theta) = 2\cos\theta\cos k\theta$$

Substituting this into the expression for p_{k+1} above then gives

$$p_{k+1} = \cos((k+1)\theta)$$

as required. ■

[88]We hope the reader didn't think they could avoid trigonometry just because this isn't a calculus text. Take this as a sine of how important the topic is (and its related puns).

7.3 Exercises

1. Prove, using induction, that $\forall n \in \mathbb{N}$, $3 \mid (n^3 - n)$.

2. Let $n \in \mathbb{N}$ so that $n \geq 2$. Use mathematical induction to prove that

$$n! \leq n^n$$

Recall that $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$.

3. Let $n \in \mathbb{N}$. Prove that $\forall n \geq 7$, $n! > 3^n$.

4. Let $n \in \mathbb{N}$. Prove by induction on n, that $\exists x, y, z \in \mathbb{Z}$ such that $x \geq 2$, $y \geq 2$, and $z \geq 2$ and satisfy $x^2 + y^2 = z^{2n+1}$.

5. Let $m \in \mathbb{N}$, with m even. Show that 8 divides $3^m - 1$.

6. The *distributive law* says that for any real numbers a, b, c, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Use induction to show that for any $n \geq 2$ and any real numbers $a, b_1, b_2 \ldots, b_n$

$$a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n.$$

7. Let $n \in \mathbb{N}$. Using induction, prove that $2^n \geq 2n$.

8. Let $n \in \mathbb{N} \cup \{0\}$. Show that 5 divides $2^{2n+1} + 3^{2n+1}$.

9. Let $n \in \mathbb{N}$, $n \geq 2$. Suppose that $x_1, x_2, \ldots, x_n \in \mathbb{Q}$. Show by induction that $x_1 + x_2 + \cdots + x_n \in \mathbb{Q}$.

10. Prove that, $\forall n \in \mathbb{N}$, $\displaystyle\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2$.

11. Prove that $\sum_{j=1}^{n} j^3 > \frac{1}{4} n^4$ for all $n \in \mathbb{N}$.

12. Let r be a real number so that $r \neq 1$. Use induction to show that

$$\sum_{i=0}^{n} r^i = \frac{1 - r^{n+1}}{1 - r}$$

for $n \in \{0, 1, 2, \ldots\}$.

Note: you may have seen a proof of this that does not use induction. Make sure your proof here uses induction.

13. Let $k \in \mathbb{N}$. Compute the k^{th} derivative of the following functions. Use induction to prove that your answer is correct.

(a) $f(x) = x^n$ for $n \in \mathbb{N}$ with $0 \leq k \leq n$.

(b) $g(x) = x^{-n}$ for $n \in \mathbb{N}$.

(c) $h(x) = \frac{1}{\sqrt{9-2x}}$.

You may use the chain and power rules in your solutions.

14. Let $n \in \mathbb{N}$. Prove that

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

15. Let $n \in \mathbb{N}$. Show that

$$\sum_{k=1}^{n} \frac{1}{2^k} < 1$$

16. Determine why the proposed proof of the following statement is incorrect:

Every non-empty subset A of the natural numbers has a maximum element. That is, there is some $a \in A$ such that $b \leq a$ for all $b \in A$.

Faulty proof. Let $A \subseteq \mathbb{N}$ be non-empty. We proceed with induction on $|A|$.

If $|A| = 1$, then the single element of A is its maximum.

Now suppose that $|A| = n + 1$ for some $n \geq 1$, and that any subset of $\mathbb{N}$ of size n has a maximum element. Choose some $a \in A$, and let $B = A \setminus \{a\}$. Then $B \subseteq \mathbb{N}$, and $|B| = n$. By the inductive hypothesis, B has a maximum element, say b. Therefore $c \leq b$ for all $c \in A \setminus \{a\}$. If $a \leq b$ as well, then b is the maximum element of A. If $b \leq a$, then $c \leq b \leq a$ for all $c \in A \setminus \{a\}$. Therefore a is the maximum element of A.

Taking $n \to \infty$, we see that any non-empty $A \subset \mathbb{N}$ has a maximum. ■

17. Let $n \in \mathbb{Z}$, $n \geq 0$.

(a) Use induction and l'Hôpital's rule to show that

$$\lim_{x \to \infty} x^n e^{-x} = 0.$$

(b) Show that

$$n! = \int_0^\infty x^n e^{-x} \mathrm{d}x.$$

For this question

- recall that $0! = 1$, and
- you may use basic facts about limits and integration from your Calculus-1 course.

18. Let $a_1, a_2, \ldots$ be real numbers. Prove, using induction, that for all $n \in \mathbb{N}$,

$$\left| \sum_{k=1}^{n} a_k \right| \leq \sum_{k=1}^{n} |a_k|.$$

You may assume the triangle inequality, $|x + y| \leq |x| + |y|$ for all real numbers x and y.

19. All numbers of the form $1007, 10017, 100117, 1001117, 10011117, \ldots$ are divisible by 53.

20. Let F_k be the k^{th} Fibonacci number, and let $q \in \mathbb{N}$. Show that $F_q \mid F_{qn}$ for all $n \in \mathbb{N}$. This generalises Result 7.2.18.

21. Let $n, r \in \mathbb{Z}$ so that $0 \leq r \leq n$. We define the binomial coefficient

$$\binom{n}{r} = \frac{n!}{(n-r)!r!}.$$

(a) Prove that the binomial coefficients satisfy Pascal's identity:

$$\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1} \qquad \text{for } 0 < r \leq n$$

(b) and so prove, using induction, the Binomal Theorem:

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

for any $a, b \in \mathbb{R}$ and any $n \in \mathbb{N}$.

22. Let $s \in \mathbb{R}$, $s > 0$. Suppose $f : \mathbb{R} \to \mathbb{R}$ is a continuous function such that

(a) for any $n \in \mathbb{N}$, the n^{th} derivative $f^{(n)}$ exists and is continuous,

(b) the limit $\lim_{x \to \infty} e^{-sx} f(x) = 0$, and

(c) for any $n \in \mathbb{N}$, $\lim_{x \to \infty} e^{-sx} f^{(n)}(x) = 0$

From f we can define a new *transformed* function

$$\mathcal{L}\{f\}(s) = \int_0^\infty f(x) e^{-sx} \, \mathrm{d}x.$$

Prove that for any $k \in \mathbb{N}$, that

$$\mathcal{L}\left\{f^{(k)}\right\}(s) = s^k \mathcal{L}\{f\}(x) - \sum_{i=0}^{k-1} s^{k-1-i} f^{(i)}(0)$$

This result tells us that the transform of any derivative is simply related to the transform of the original function. That is, the differential equation in f turns into an algebraic equation in $\mathcal{L}(f)$ This sort of result can come in very handy when studying differential equations.

23. Let $\alpha \in \mathbb{R}$ such that $\alpha + \frac{1}{\alpha} \in \mathbb{Z}$. Prove that $\alpha^n + \frac{1}{\alpha^n} \in \mathbb{Z}$ for any $n \in \mathbb{N} \cup \{0\}$.

24. Show that every natural number, n, can be written as

$$n = 3^m a,$$

where $m \in \mathbb{Z}$ such that $m \geq 0$, $a \in \mathbb{N}$ and $3 \nmid a$.

25. You go on vacation to a foreign country. The local currency only has 3 and 5 dollar bills, and locals will only give items a price $p \in \mathbb{N}$ such that $p \geq 8$. Assume that you have access to an unlimited supply of 3 and 5 dollar bills. Can you buy any souvenir you want? Give a proof or a counterexample.

26. Let $a_0, a_1, a_2, \dots$ be a sequence recursively defined as $a_0 = 2$, $a_1 = 1$, and

$$a_n = a_{n-1} + 6a_{n-2} \quad \text{for } n \geq 2.$$

Prove by induction that

$$a_n = (-2)^n + 3^n \quad \text{for all } n \geq 0.$$

27. Show that every $n \in \mathbb{N}$ can be written in binary. That is, for all $n \in \mathbb{N}$, there exists an $m \in \mathbb{Z}$ with $m \geq 0$ and constants $c_0, c_1, c_2, \dots, c_m \in \{0, 1\}$ such that

$$a = c_m \cdot 2^m + c_{m-1} \cdot 2^{m-1} + \cdots + c_1 \cdot 2 + c_0.$$

For example,

$$537 = 512 + 16 + 8 + 1 = 2^9 + 2^4 + 2^3 + 2^0,$$

so $m = 9$ and $(c_0, c_1, c_2, \dots, c_9) = (1, 0, 0, 1, 1, 0, 0, 0, 0, 1)$.

28. For $n \in \mathbb{N}$, consider the recurrence

$$T(1) = 1 \qquad \text{and for } n \geq 2 \qquad T(n) = 2T\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + n$$

The first few values of $T(n)$ are

$$1, 4, 5, 12, 13, 16, 17, 32, 33, \dots$$

Use strong induction to prove that for $n \geq 1$, $T(n)$ satisfies the bound

$$T(n) \leq n \log_2 n + n.$$

Note that the logarithm has base 2, and that the floor function, $\lfloor x \rfloor$, gives the largest integer smaller or equal to x.

Recurrences such as this one appear very frequently in the analysis of "divide and conquer" algorithms. That class of algorithms (roughly speaking) work by repeatedly splitting a larger problem into smaller pieces until they can be solved trivially. The interested reader should search-engine their way to more information.

29. Use strong induction to prove the following:

Suppose you begin with a pile of n stones ($n \geq 2$) and split this pile into n separate piles of one stone each by successively splitting a pile of stones into two smaller piles. Each time you split a pile you multiply the number of stones in each of the two smaller piles you form, so that if these piles have p and q stones in them, respectively, you compute pq. Show that no matter how you split the piles (eventually into n piles of one stone each), the sum of the products computed at each step equals $\dfrac{n(n-1)}{2}$.

For example — say with start with 5 stones and split them as follows:

$$(5) \to \underbrace{(3)(2)}_{=6} \to \underbrace{(2)(1)}_{=2}\underbrace{(1)(1)}_{=1} \to \underbrace{(1)(1)}_{=1}(1)(1)(1).$$

Then, we get, $6 + 2 + 1 + 1 = 10 = \frac{5\times 4}{2}$ ✓.

Chapter 8

Return to sets

As we mentioned early, we have changed the order of topics a little in this text so that we can get to proving things as quickly as possible and get you more comfortable with basic proof methods. This meant that we skipped several basic aspects of sets that we should now cover. Thankfully we can now do a bit more with these basic bits of set theory — indeed we can prove some things!

8.1 Subsets

When we defined sets way back at the beginning of the course, we saw that the only thing we can ask a set is

> Is this object in the set?

and the set can only respond to us with either

> Yes.

or

> No.

We can make this simple structure much more interesting by enriching it using some of the logic we have learned. Consider the sets

$$A = \{1, 2, 3\} \qquad\qquad B = \{0, 1, 2, 3, 4\}.$$

We see that every single element of A is contained in the set B. So rather than asking one-by-one whether or not individual elements of A are contained in B, we can instead ask if all the elements of A are contained in B. Equivalently, we can ask "Is A contained in B". This is the idea of A being a subset of B.

Definition 8.1.1 Let A and B be sets.

- We say that A is a **subset** of B if every element of A is also an element of B. We denote this $A \subseteq B$.

- If A is not a subset of B, then we denote this as $A \not\subseteq B$.
- Further, if A is a subset of B but there is at least one element of B that is not in A then we say that A is a **proper subset** of B. We denote this by $A \subset B$.
- If $A \subseteq B$ then B is a **superset** of A which we can write as $B \supseteq A$. Similarly, if $A \subset B$ then B is a **proper superset** of A which write as $B \supset A$

Finally,

- Two sets A and B are equal if A is a subset of B and B is a subset of A. That is

$$(A = B) \equiv ((A \subseteq B) \wedge (B \subseteq A))$$

$\Diamond$

Some things to note

- The empty set is a subset of every set. That is, for any set A, we always have that $\varnothing \subseteq A$.
- That $A \subseteq B$ is equivalent to saying that if we take any element of A then it is also an element of B. That is

$$(A \subseteq B) \equiv (\forall a \in A, a \in B) \equiv (a \in A \implies a \in B).$$

- If $A \not\subseteq B$, then there is at least one element of A that is not in B. That is

$$(A \not\subseteq B) \equiv (\exists a \in A \text{ s.t. } a \notin B)$$

- Since two sets are equal when they are subsets of each other, we prove set equality using a two part proof. The first part proving that $A \subseteq B$ and then the second part showing that $B \subseteq A$.

Example 8.1.2 Let $S = \{1, 2\}$. What are all the subsets of S?

- The subsets are $\varnothing, \{1\}, \{2\}, \{1, 2\}$.

$\square$

Result 8.1.3 *Let* $A = \{n \in \mathbb{Z} \mid 6|n\}$ *and* $B = \{n \in \mathbb{Z} \mid 2|n\}$. *Then* $A \subseteq B$.

First lets write a few elements of these sets

$$A = \{\dots, -18, -12, -6, 0, 6, 12, 18, \dots\} \quad B = \{\dots, -6, -4, -2, 0, 2, 4, 6, \dots\}$$

The result we are trying to prove is that $A \subseteq B$. This is equivalent to showing that if $a \in A$ then $a \in B$ (which is essentially saying that if an integer is divisible by 6 then it is divisible by 2). Hence to prove the result we are going to assume that $a \in A$ and then work our way to proving that $a \in B$.

- First up we make sure that the reader knows we are going to take A, B to be the sets in the statement of the result.
- Assume $a \in A$.
- Then this means that a is an integer that is divisible by 6. That is $a = 6\ell$ for some $\ell \in \mathbb{Z}$.
- We need to show that $a \in B$. This is equivalent to showing that we can write $a = 2k$ where k is some integer.
- But we know that $a = 6\ell = 2(3\ell)$ and since $3\ell \in \mathbb{Z}$ we are done.

Of course, we aren't really done until we write thing up nicely.
Proof. Let A, B be the sets defined in the result. Assume that $a \in A$. Hence we can write $a = 6\ell$ where $\ell \in \mathbb{Z}$. But now since $6\ell = 2(3\ell)$ and 3ℓ is an integer, we know that $a \in B$. Thus $A \subseteq B$. ■

The following result expresses that being a subset is a transitive relation. We'll see much more about transitivity in the near future.

Result 8.1.4 *Let A, B, C be sets. Then if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.*

We should start by breaking things down carefully because there are a few nested implications hidden inside this result.

- The hypothesis is $A \subseteq B$ and $B \subseteq C$. We can, in turn, write this as
$$(a \in A \implies a \in B) \wedge (b \in B \implies b \in C)$$
- The conclusion says $A \subseteq C$. This can similarly be written as
$$a \in A \implies a \in C.$$
- Since we are trying to prove an implication, we start by assuming the hypothesis is true. So we assume that
$$(a \in A \implies a \in B) \wedge (b \in B \implies b \in C)$$
Notice this we do *not* assume that $a \in A$ and $b \in B$, rather we are assuming that the above implications are both true[89].
- Now we want to prove that the conclusion is true, namely that
$$a \in A \implies a \in C.$$
This we can do by assuming that the hypothesis is true and showing the conclusion.[90] That is, assume that $a \in A$ and then work towards showing that $a \in C$.

[89] And, as you have now memorised, an implication is only false when its hypothesis is true and its conclusion false.

[90] Equivalently, we know that either $a \in A$ or $a \notin A$. When $a \in A$ we have precisely this case. On the other hand, if $a \notin A$ then the implication $(a \in A) \implies (a \in C)$ is true since the hypothesis is false. So it is only when $a \in A$ that there is work to do.

- Since now we have assumed that $a \in A$ and $a \in A \implies a \in B$, we know that $a \in B$. And then, in turn, our assumption that $a \in B \implies a \in C$, we know that $a \in C$. Precisely what we need!

Oof! The above analysis becomes much easier with practice.
Proof. Assume that $A \subseteq B$ and $B \subseteq C$. We wish to show that now $A \subseteq C$, so let $a \in A$. Since we know that $A \subseteq B$, we know that $a \in B$. And since we know that $B \subseteq C$, we know that $a \in C$. Hence we have shown that $A \subseteq C$. ■

So even though our scratch work took some twists and turns, our proof is quite succinct.

Once you start thinking about subsets of a set A, it is quite natural to ask[91] "What are all the subsets of a given set?" The resulting *set of sets* is called the **power set**. This set will be very important when we look at the cardinality of sets, particularly the cardinality of infinite sets. But first, we should really give it a precise definition.

Definition 8.1.5 Let A be a set. The **power set** of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A. ♢

Note that the elements of $\mathcal{P}(A)$ are themselves sets, and

$$X \in \mathcal{P}(A) \iff X \subseteq A.$$

When we get to the chapter on cardinality we'll prove that if A is a finite set with $|A| = n$ then $|\mathcal{P}(A)| = 2^n$. We will also prove an important result about the power set of an infinite set.

Example 8.1.6 What are $\mathcal{P}(\{1,2,3\}), \mathcal{P}(\varnothing)$ and $\mathcal{P}(\mathcal{P}(\varnothing))$?

$$\begin{aligned} \mathcal{P}(\{1,2,3\}) &= \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\} \\ \mathcal{P}(\varnothing) &= \{\varnothing\} \\ \mathcal{P}(\mathcal{P}(\varnothing)) &= \mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\} \end{aligned}$$

□

Result 8.1.7 *Let A, B be sets. Then $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.*

Since this is a biconditional we need to prove both directions. Lets start with the forward implication and then turn to the converse.

- We want to show that $A \subseteq B \implies \mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- So we assume that $A \subseteq B$ and we want to prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- This is equivalent to showing that $X \in \mathcal{P}(A) \implies X \in \mathcal{P}(B)$ — note that X is now itself a set (which is why[92] we've used a capital X rather than a lower case x).

---

[91] Well, the author thinks it is a natural question and hopes you think it is one too.
[92] The power of good notational conventions!

- So just as was the case in the previous proof, we assume that the hypothesis, $X \in \mathcal{P}(A)$ is true. This means that $X \subseteq A$.
- But our previous[93] result — Result 8.1.4 — tells us that if $X \subseteq A$ and $A \subseteq B$ then $X \subseteq B$.
- This, in turn, implies that $X \in \mathcal{P}(B)$, and so $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Okay, now lets look at the converse.

- We want to show that $\mathcal{P}(A) \subseteq \mathcal{P}(B) \implies A \subseteq B$.
- So we assume that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- But now $A \in \mathcal{P}(A)$, and so $A \in \mathcal{P}(B)$.
- Hence A must be a subset of B — by definition of the power set.

As always, once the scratch work is done, its time to write up.
Proof. We prove each implication in turn.

- Assume that $A \subseteq B$, and let $X \in \mathcal{P}(A)$. Hence $X \subseteq A$. By our result above, this, in turn, implies that $X \subseteq B$. By the definition of the power set, this tells us that $X \in \mathcal{P}(B)$. Thus we have shown that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- Now turn to the converse and assume that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Since $A \in \mathcal{P}(A)$, this implies that $A \in \mathcal{P}(B)$. But, by the definition of the power set, this tells us that $A \subseteq B$, and we are done.

Since we have proved both implications we have proved the result. ■

We can think of forming the power set as an operation on a set. Since it is the only operation we have discussed so far, we could keep applying it to see what sorts of things we get. That is, what is the power set of a power set of a power set of a… This is not an entirely silly idea, and we will look at this when we get to the chapter on cardinality, but exploring other set operations is a better use of our time at present.

8.2 Set operations

The first two set operations we'll discuss are union and intersection. Rather than having more discursive blurb, the authors should get on with it and just define them.

Definition 8.2.1 Let A and B be sets. The **union** of A and B, denoted $A \cup B$,

[93]We could refer to this by number as well — that is probably a good idea if the result isn't so close by within the document. However, it is just up there so referring to it as "previous result" is fine.

is the set of all elements in A or B.

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

$\diamondsuit$

A couple of things to note here. First — the symbol "$\cup$" is not the letter "u". Second — we are using the word "or" in the definition in its inclusive mathematical sense. Indeed we could rewrite the above definition as

$$(x \in A \cup B) \iff (x \in A) \vee (x \in B)$$

We'll draw some pictures to help illustrate things shortly. But first, another definition.

Definition 8.2.2 Let A and B be sets. The **intersection** of A and B, denoted $A \cap B$, to be the set of elements that belong to both A and B.

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

If the intersection $A \cap B = \varnothing$, then we say that A and B are disjoint. $\diamondsuit$

Again, the symbol "$\cap$" is not an upside-down letter "u", and we are using the word "and" in this definition in its precise mathematical meaning. Just as we rewrote the definition of union, we can rewrite the definition of intersection as

$$(x \in A \cap B) \iff (x \in A) \wedge (x \in B)$$

Indeed there are many parallels between how the operators union and intersection act on sets and how the logical operators "or" and "and" act on mathematical statements. These parallel are reinforced by the similarity in notations.

Warning 8.2.3 The right notation in the right place.. Please be careful to not confuse set and logical operations. When A and B are sets, we cannot take their conjunction or disjunction: "$A \vee B$" "$A \wedge B$" do not make sense. Similarly, if P and Q are statements we cannot take their union or intersection: "$P \cup Q$" and "$P \cap Q$" do not make sense.

Example 8.2.4 Let $A = \{1, 2, 3, 4\}$, $B = \{p : p \text{ is prime}\}$, $C = \{5, 7, 9\}$ and $D = \{\text{even positive integers}\}$. Then

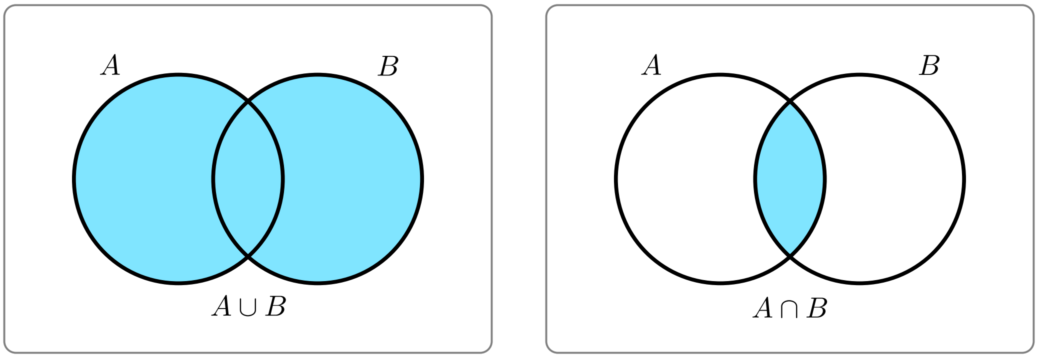
$$\begin{aligned} A \cap B &= \{2, 3\} \\ B \cap D &= \{2\} \\ A \cup C &= \{1, 2, 3, 4, 5, 7, 9\} \\ A \cap C &= \varnothing \end{aligned}$$

$\square$

We can visualise the operations of union and intersection using a Venn diagram[94]. These diagrams might seem like an obvious and simple idea, however

[94] John Venn was a 19th century English logician and mathematician. He introduced "Eulerian

it is much more recent than the cartesian plane. Venn diagrams are 19th century mathematics, while the cartesian plane is 17th century mathematics[95].



Remark 8.2.5 Long equations, sides, and short-hands. Some of the results we want to prove (like the one coming shortly) involve showing that a long expression on one side of an equality is actually the same as the long expression on the other side. To ease both the writer and the reader of the resulting calculations, we refer to the expressions on either side[96] as "the left-hand side" and "the right-hand side". In typical mathematician style, even this is too long and they are almost always contracted further to "LHS" and "RHS". This shorthand allows us to avoid writing (and reading) chunks of text (with the associated potential errors), but, perhaps more importantly, allows us to indicate that one side of an equation remains fixed unchanged while we work on the other.

Here is a good example adapted from one in "The book of proof" by Richard Hammack[97].

Example 8.2.6 Let

$$A = \{n \in \mathbb{Z} \ : \ 15|n\} \qquad B = \{n \in \mathbb{Z} \ : \ 3|n\} \qquad C = \{n \in \mathbb{Z} \ : \ 5|n\}$$

Prove that $A = B \cap C$.

Scratchwork. So — scratch work first. To prove the equality we need to show that the LHS is a subset of the RHS and vice versa. So we start by proving that $A \subseteq B \cap C$.

- Let $a \in A$, so a is an integer divisible by 15.
- Hence we can write $a = 15k$.
- We now need to show that $a \in B$ and $a \in C$, so that $a \in B \cap C$.

circles" (which later became to be known as Venn diagrams) in a paper "On the Diagrammatic and Mechanical Representation of Propositions and Reasoning". He also built a machine to bowl cricket balls.

[95] Or, if you look into the history a little more, 14th century.

[96] This is, because mathematics is most commonly written sinistrodextrally (left-to-right). Though of course, we could use similar shorthand if we wrote dextrosinistrally or even boustrophedonically! It seems unlikely that anyone would write mathematics vertically. And yes, this footnote is here mostly just to use the word "boustrophedonically".

[97] `www.people.vcu.edu/~rhammack/BookOfProof/`

- Well, since $a = 15k$ we know that $a = 3(5k)$, and because $5k \in \mathbb{Z}$, a is divisible by 3. Hence $a \in B$.
- Similarly, since $a = 15k$ we know that $a = 5(3k)$, and because $3k \in \mathbb{Z}$, a is divisible by 5. Hence $a \in C$.
- Since $a \in B$ and $a \in C$, we know that $a \in B \cap C$.

Thus $A \subseteq B \cap C$.

Now we must argue that $B \cap C \subseteq A$.

- Let $x \in B \cap C$. Notice that we're calling it x rather than b or c since that is a more neutral letter, while b or c suggest that the element might belong to B or C but not both.
- Since $x \in B \cap C$ we know that $x \in B$ and that $x \in C$.
- Because $x \in B$, $x = 3k$ for some integer k.
- Similarly, because $x \in C$, we know that $x = 5\ell$ for some integer ℓ. Notice that we did not write $x = 5k$ since we have already used k to express that x is divisible by 3.
- This implies that $x = 3k = 5\ell$, and we are close to being done.
- Since $5\ell = 3k$ we know that 5ℓ is divisible by 3. We'd like to show that ℓ is a multiple by 3 (which would make sense because 3 and 5 are prime numbers[98]). Perhaps the easiest way to do this is to investigate what happens if ℓ is a multiple of 3 or not. There are 3 possibilities, $\ell = 3j, 3j+1, 3j+2$, for some integer j (we are using Euclidean division here).
    - If $\ell = 3j$ then $5\ell = 15j$ which is precisely what we want.
    - If $\ell = 3j + 1$ then $5\ell = 15j + 5 = 3(5j + 1) + 2$, and so 5ℓ is not divisible by 3. But this contradicts the fact that $x \in B$.
    - Similarly $\ell = 3j + 2$ then $5\ell = 15j + 10 = 3(5j + 3) + 1$, and so 5ℓ is not divisible by 3. Again this contradicts the fact that $x \in B$.

  Hence the only possibility is that ℓ is a multiple of 3. Thus we can write $x = 5\ell = 5 \cdot 3 \cdot j$ for some integer j.
- Hence x is divisible by 15 and $x \in A$.

Thus $B \cap C \subseteq A$.

Oof! Everything is there, we just have to write it up nicely.

Solution.

Proof. Let A, B, C be defined as above. We prove the equality by first proving that the LHS is a subset of the RHS and then vice-versa.

- Let $a \in A$. Then $a = 15m$ for some $m \in \mathbb{Z}$. This means that $a = 3(5m)$ and $a = 5(3m)$. Since both $3m, 5m \in \mathbb{Z}$, it follows that $a \in B$ and $a \in C$. Thus $a \in B \cap C$ as required.
- Now let $x \in B \cap C$. Then $x = 3k$ and $x = 5\ell$ for some integers k, ℓ, so we must have that $3k = 5\ell$. Since $\ell \in \mathbb{Z}$ we know it can be written as $\ell = 3j, 3j + 1$ or $3j + 2$ (by Euclidean division).
  - If $\ell = 3j$ for some integer j, then $x = 5\ell = 15j$ and so is a multiple of 15.
  - If $\ell = 3j + 1$ then $x = 15j + 5 = 3(5j + 1) + 2$, while if $\ell = 3j + 2$ then $x = 15j + 10 = 3(5j + 3) + 1$. In either of these cases, we contradict our assumption that x is a multiple of 3.

  Hence we must have that $\ell = 3j$. Hence $x = 5\ell = 5 \cdot 3j = 15(j)$ for some integer j, and so x is divisible by 15. Hence $x \in A$ as required.

So we have shown that $A = B \cap C$. ■

Here is an alternative way to show that $B \cap C \subseteq A$. It relies on the fact that $5 = 6 - 1$.

Proof. Assume that $x \in B \cap C$, and so $x \in B$ and $x \in C$. Then we know that there are $k, \ell \in \mathbb{Z}$ so $x = 3k$ and $x = 5\ell$. Thus we know that $3k = 5\ell$. From this

$$3k = 6\ell - \ell \qquad \text{and thus}$$
$$\ell = 6\ell - 3k = 3(2\ell - k)$$

That is, ℓ must be divisible by 3. But now $x = 5\ell = 15(2\ell - k)$ and so is divisible by 15. Thus $x \in A$ as required. ■

□

Given two sets A, B we sometimes might need to construct a new set which contains all the elements of A that are not in B. This is the set-difference.

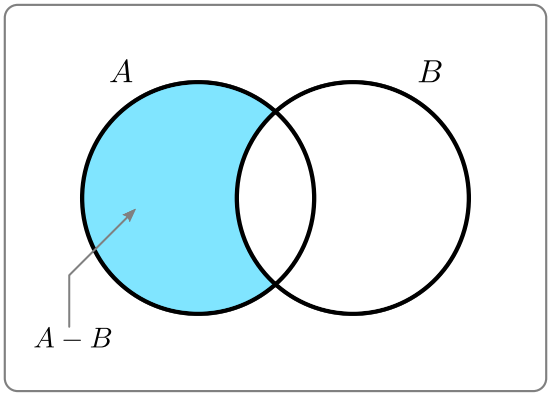
Definition 8.2.7 Let A and B be sets. Then the **difference**, $A - B$ (which is also written $A \setminus B$) is the elements in A that are not in B

$$A - B = \{x \in A \mid x \notin B\}$$

This new set is sometimes called the "**relative complement** of B in A". ♢

Another picture:

[98] This proof can be made a bit more direct if we make use of the fact that every integer has a unique prime factorisation, but we haven't proved that yet.



Example 8.2.8 If we reuse the sets we just defined in the example Example 8.2.4 then,

$$A - D = \{1, 3\}$$
$$C - A = \{5, 7, 9\}$$

□

To define our next set operation we first need the **univeral set** U. This is the set from which we are taking objects to make our sets — it (essentially) tells us what domain we are working in. For many of our results U will be the set of natural numbers, for some other results U might be the set of reals. It depends on context. But given the universal set we can define our last operation.

Definition 8.2.9 Given a **universal set** U and a set $A \subset U$, we define the **complement** of A, denoted $\bar{A}$ to be the set of elements not in A.

$$\bar{A} = \{x \in U | x \notin A\}$$

or equivalently:

$$x \in \bar{A} \iff x \notin A$$

◊

Note

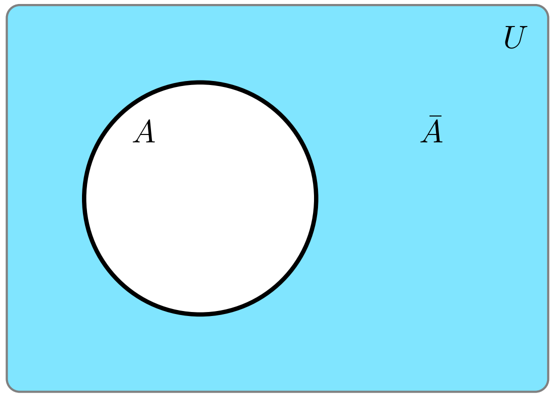
- While it is a nice thing to say, "compl-I-ment" is not the same as "compl-E-ment".
- The complement acts on sets in much the same way that negation acts on logical statements. The complement of the complement is the original set:

$$\bar{\bar{A}} = A.$$

- We can express $A - B$ using the complement as

$$A - B = A \cap \bar{B}$$

Another descriptive picture:



Example 8.2.10 Let $U = \{1, 2, \ldots, 20\}$, $A = \{2, 3, 5, 7, 11, 13, 17, 19\}$ and $B = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20\}$. Determine the following sets

$$\bar{B} \qquad A - B \qquad A \cap \bar{B} \qquad \bar{\bar{B}}$$

Solution. We can just chug through the definitions carefully to get

$$\begin{aligned} \bar{B} &= \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19\} \\ A - B &= \{3, 5, 7, 11, 13, 17, 19\} \\ A \cap \bar{B} &= \{3, 5, 7, 11, 13, 17, 19\} = A - B \\ \bar{\bar{B}} &= B \end{aligned}$$

□

8.3 Cartesian products of sets

Now when we were defining sets we used lists $A = \{1, 2, 3\}$ and the order in which we put things in the list didn't matter. On some occasions we really need to put things into some order; we need a way to write an ordered pair of elements in which one of the pair is the *first* and the other is the *second*. Coordinates of points, (x, y), in the plane are a very good example of this: the first number is the x-coordinate (horizontal position) and the second is the y-coordinate (vertical position), and we should not mix them up[99]. The point $(1, 13)$ on the plane is not the same as the point $(13, 1)$. We are used to this notation, "(x, y)", but we should define it before we go any further.

[99]Mind you, people rarely call the parts of an x, y-coordinate by their correct names. The x (ie the first of the pair) is called the **abscissa** and its use goes back at least as far as Fibonacci. The y (the second of the pair) is the **ordinate**. These terms are not so common in modern English and people typically just call them x-coordinate and y-coordinate (which is a little jarring to the ear of the pedant).

Definition 8.3.1 An **ordered pair** of elements is an ordered list of two elements. We write this as (a, b) with round brackets rather than braces. Ordered pairs have the properties that

- $(a, b) \neq (b, a)$ unless $a = b$, and
- $(a, b) = (c, d)$ only when $(a = c)$ and $(b = d)$.

◊

Given two sets A, B, the set of all possible ordered pairs is the **Cartesian product** of those sets. To be more precise:

Definition 8.3.2 Cartesian product. Let A, B be sets. The **Cartesian product**,or just **product**, of A and B is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$. We write this as $A \times B$.

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

Note that $A \times B \neq B \times A$, unless $A = B$. ◊

Example 8.3.3 If we set $A = \{a, b, c\}$ and $B = \{1, 2\}$ then

$$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

□

So we are used to playing with cartesian products in the context of functions — $\mathbb{R} \times \mathbb{R}$ is the whole **cartesian plane**[100] and functions we are used to are just subsets of this. For example, the parabola $y = x^2$ is the set

$$\left\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\right\}$$

which is a subset of $\mathbb{R} \times \mathbb{R}$.

8.4 Some set-flavoured results

There are quite a few standard results that describe how the set operations defined above interact with each other. We'll state some of the more important ones as a theorem (or two (or three)). But first, let us summarise what we have learned above.

Remark 8.4.1 A set of results about sets seen earlier. Let A, B be sets. Then

- $(A \subseteq B) \equiv (\forall x \in A, x \in B) \equiv (x \in A \implies x \in B)$.

[100]While this is named for the French mathematician and philosopher Rene Descartes (1596 – 1650), it was also invented by Pierre de Fermat (1601 – 1665), and even earlier by Nicole Oresme (1325 – 1382). Fermat is famous for writing his "Last Theorem" in the margin of a book, and Oresme was the first to prove that the infinite series $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$ does not converge.

- $(A = B) \equiv ((A \subseteq B) \wedge (B \subseteq A)) \equiv ((x \in A) \iff (x \in B))$
- $(x \in A \cap B) \equiv ((x \in A) \wedge (x \in B))$
- $(x \in A \cup B) \equiv ((x \in A) \vee (x \in B))$
- $(x \in \bar{A}) \equiv (x \notin A) \equiv\sim (x \in A)$
- $(x \in A - B) \equiv ((x \in A) \wedge (x \notin B)) \equiv ((x \in A) \wedge \sim (x \in B))$

Using these we can prove the following theorems

Theorem 8.4.2 DeMorgan's laws. *Let A, B be sets contained in a universal set U. Then*

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$
$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

Theorem 8.4.3 Distributive laws. *Let A, B, C be sets then*

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

and

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

The above are not so hard to understand. You can see that the distributive laws for sets look very much like the distributive laws for additional and multiplication. Laws for set differences are less obvious and we certainly wouldn't expect you to remember them. However they do make very good exercises! And, as you'll see in the examples below, a quick sketch of Venn diagrams can help a lot. ***But*** a Venn diagram is not a proof [101].

Theorem 8.4.4 Set differences. *Let A, B, C be sets contained in a universal set U. Then*

$$A - B = A \cap \bar{B}$$
$$A - (B \cap C) = (A - B) \cup (A - C)$$
$$A - (B \cup C) = (A - B) \cap (A - C)$$
$$A - (B - C) = (A \cap C) \cup (A - B)$$

When we prove the above theorems we'll make use of some simple little results that follow quite directly from the definitions of our set operations. Rather than explaining those results again and again in each proof (where the reader has to

[101] The Venn diagram is good scratch work for a proof, but really what one is doing is showing that for a particular choice of sets (ie the ones drawn) everything works out. To be a proof it has to work for every choice.

check the reasoning each time), we'll put them in a separate little result of their own. Since it is a helpful result we'll call it a lemma.

Lemma 8.4.5 *Let A, B be sets.*

- *If $x \in A$ then $x \in A \cup B$.*
- *If $x \in A \cap B$ then $x \in A$.*
- *If $x \notin A \cup B$ then $x \notin A$ and $x \notin B$.*
- *If $x \notin A \cap B$ then $x \notin A$ or $x \notin B$.*

The contrapositives of these statements also turn out to be useful in certain circumstances, so we state them explicitly.

- *If $x \notin A \cup B$ then $x \notin A$*
- *If $x \notin A$ then $x \notin A \cap B$*
- *If $x \in A$ or $x \in B$ then $x \in A \cup B$.*
- *If $x \in A$ and $x \in B$ then $x \in A \cap B$.*

These are straight forward to prove using the logic we know and the definitions of union and intersection.

Proof. We prove each in order.

- Assume $x \in A$. Then $x \in A$ or $x \in B$. Hence $x \in A \cup B$.
- Assume $x \in A \cap B$. Hence $x \in A$ and $x \in B$. Thus we have that $x \in A$ as required.
- The contrapositive of the statement is the definition of intersection, so the statement is true.
- The contrapositive of the statement is the definition of union, so the statement is true.

■

Remark 8.4.6 Careful choice of B. Take a careful look at the first of the statements in the lemma above. Observe that the hypothesis does not mention the set B that is in the conclusion. This is a useful observation. It means that we can apply the result by choosing B to be some set we are interested in. That is:

If $x \in A$ then x is in the union of A and *any set we choose.*

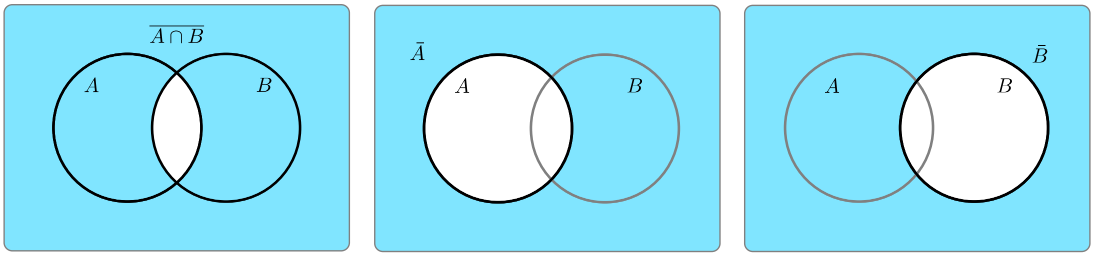
and similarly the second (its contrapositive) says

If $x \notin A$ then x is not in the intersection of A and *any set we choose.*

Okay, primed with these results let's prove one of DeMorgan's laws

Example 8.4.7 Let A, B be sets included in a universal set U, then $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

Scratchwork. First we should draw a Venn diagram describing the sets $\overline{A \cap B}, \bar{A}$ and $\bar{B}$:



Again, note that though Venn diagrams are useful tools for to understand and explore problems like these, they are not proofs. You should think of them as tools to help your scratch work.

Its an equality so we have to prove that the LHS is a subset of the RHS and vice-versa. Let's do those in order.

- Assume $x \in \overline{A \cap B}$.
- By definition of set complement this means that $x \notin (A \cap B)$.
- Now our helpful lemma comes to our aid. It tells that this implies that $x \notin A$ or $x \notin B$.
  - If $x \notin A$ then $x \in \bar{A}$. As per our helpful lemma, if x is an element of a particular set, then it is an element of the union of that set and any other set we choose. Hence, if $x \in \bar{A}$ then $x \in \bar{A} \cup \bar{B}$.
  - Similarly, if $x \notin B$ then $x \in \bar{B}$, and so $x \in \bar{B} \cup \bar{A}$.
- In either case $x \in \bar{A} \cup \bar{B}$ as required.

And the other inclusion:

- Assume $x \in \bar{A} \cup \bar{B}$. Hence $x \in \bar{A}$ or $x \in \bar{B}$.
  - If $x \in \bar{A}$ then $x \notin A$. As above, our helpful lemma comes to our aid. If we know that x is not an element of a particular set, then it is not in the intersection of that set and any other set we choose. Hence, if $x \notin A$ then $x \notin A \cap B$.
  - If $x \in \bar{B}$ then $x \notin B$, and by a similar argument, $x \notin A \cap B$.
- In either case $x \notin A \cap B$, so $x \in \overline{A \cap B}$ as required.

Now we can write this as a proper proof.

Solution.

Proof. We first prove that $\overline{A \cap B} \subset \bar{A} \cup \bar{B}$ and then the reverse inclusion.

- Let $x \in \overline{A \cap B}$, and hence $x \notin (A \cap B)$. This implies that $x \notin A$ or $x \notin B$. If $x \notin A$ then $x \in \bar{A}$, and so $x \in \bar{A} \cup \bar{B}$. Similarly, if $x \notin B$ then $x \in \bar{B}$, and so $x \in \bar{B} \cup \bar{A}$. In either case, $x \in \bar{A} \cup \bar{B}$ as required.
- Now assume that $x \in \bar{A} \cup \bar{B}$, so $x \in \bar{A}$ or $x \in \bar{B}$. If $x \in \bar{A}$ then $x \notin A$, and so $x \notin A \cap B$. Similarly if $x \in \bar{B}$ then $x \notin B$, and so $x \notin B \cap A$. In either case $x \notin A \cap B$, and so $x \in \overline{A \cap B}$.

Since we have shown both inclusions, $\overline{A \cap B} = \bar{A} \cup \bar{B}$ ■

□

What about a distributive law or two?

Example 8.4.8 Let A, B, C be non-empty sets, then $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Notice that this result still holds when the sets are allowed to be empty, but the proof of the result is a little messier and involves more cases.

Scratchwork. Unfortunately it isn't so easy to draw a useful picture here[102], but thankfully this isn't too hard to prove. It is a set-equality, so we need to prove the LHS is a subset of the RHS and vice-versa.

- Let $p \in A \times (B \cup C)$. Notice that since A, B, C are non-empty, we know that p exists. Since the LHS is the cartesian product of two sets, this element p is really an ordered pair of elements. It is probably a bit easier to follow what is going to happen if we make this clear from the start. With this in mind, let us restart things.
- Let $(x, y) \in A \times (B \cup C)$.
- This means that $x \in A$ and $y \in B \cup C$.
- Hence $y \in B$ or $y \in C$.
  - Let $y \in B$, then since $x \in A$, we know that $(x, y) \in A \times B$. Thus $(x, y) \in (A \times B) \cup (\text{any set we choose})$, and so $(x, y) \in (A \times B) \cup (A \times C)$.
  - Similarly, let $y \in C$. Since $y \in C$ and $x \in A$, we know that $(x, y) \in A \times C$, and so $(x, y) \in (A \times B) \cup (A \times C)$.
- So $(x, y) \in RHS$.

And the other way around…

- Let $(x, y) \in (A \times B) \cup (A \times C)$, so $(x, y) \in (A \times B)$ or $(x, y) \in (A \times C)$. Again, since A, B, C are non-empty we know that such an (x, y) exists.
  - If $(x, y) \in (A \times B)$ then $x \in A$ and $y \in B$. Hence $y \in B \cup (\text{any set we choose})$, and so $y \in B \cup C$.
  - Similarly, if $(x, y) \in A \times C$ then $x \in A$ and $y \in C$. Hence $y \in C \cup B$.

- In either case $x \in A$ and $y \in B \cup C$, so $(x, y) \in LHS$.

Now we clean it up and make it a proof.

Solution.

Proof. We prove each inclusion in turn. Assume that $(x, y) \in A \times (B \cup C)$, so that $x \in A$ and $y \in B \cup C$. Since the sets are non-empty, such a (x, y) exists. Since $y \in B \cup C$, we know that $y \in B$ or $y \in C$.

- If $y \in B$, then since $x \in A$, we know that $(x, y) \in A \times B$.
- Similarly, if $y \in C$ we know that $(x, y) \in A \times C$.

In both cases we have that $(x, y) \in (A \times B) \cup (A \times C)$, and so $LHS \subseteq RHS$.

Now assume that $(x, y) \in RHS$, so $(x, y) \in A \times B$ or $(x, y) \in A \times C$. Again, since the sets are non-empty, such an (x, y) exists.

- If $(x, y) \in A \times B$, then $x \in A$ and $y \in B$. Hence $y \in B \cup C$.
- Similarly, if $(x, y) \in A \times C$, then $x \in A$ and $y \in C$. Thus $y \in C \cup B$.

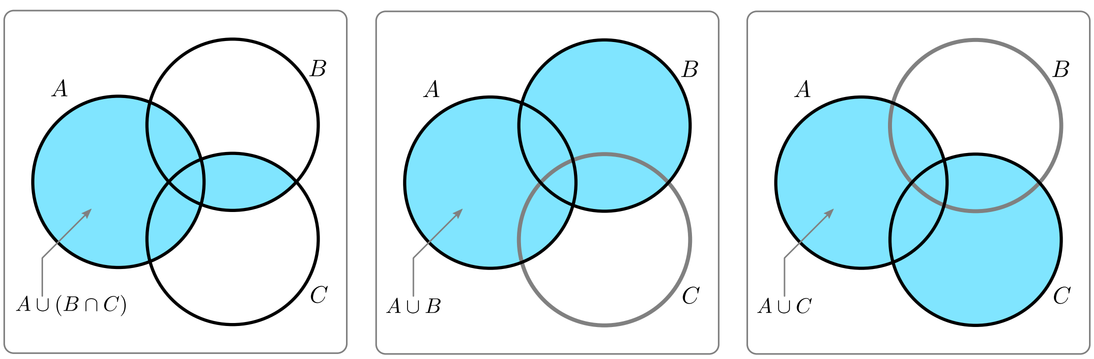
In either case we know that $x \in A$ and $y \in B \cup C$, so $(x, y) \in A \times (B \cup C)$ as required. ■

□

A more challenging distributive law.

Example 8.4.9 Let A, B, C be sets, then $A \cup (B \cap C) = (A \cup C) \cap (A \cup B)$.

Scratchwork. Again, a picture helps.



Lets prove the inclusions one at a time. First LHS is a subset of the RHS.

- Let $x \in A \cup (B \cap C)$, so that $x \in A$ or $x \in (B \cap C)$.
  - Assume $x \in A$.
  - Hence $x \in A \cup B$ and $x \in A \cup C$ (again because we know that if $x \in A$ then it is in the union of A and any set we choose).

[102] Well … I guess we could draw A, B, C as one-dimensional sets lying on different axes, and then the product would be some rectangular region in the plane? Something like that might work. A good exercise for the eager reader.

  - Thus $x \in (A \cup B) \cap (A \cup C)$.

- On the other hand, assume that $x \in B \cap C$
  - Hence $x \in B$ and $x \in C$.
  - Since $x \in B$, we know that $x \in B \cup A$.
  - Similarly, since $x \in C$, we know that $x \in C \cup A$
  - Because both $x \in A \cup B$ and $x \in A \cup C$, we have that $x \in (A \cup B) \cap (A \cup C)$.

- In both cases, $x \in (A \cup B) \cap (A \cup C)$.

Now we prove that the RHS is a subset of the LHS.

- Let $x \in (A \cup B) \cap (A \cup C)$, so that $x \in A \cup B$ and $x \in A \cup C$.

- At this point it is a good idea to explore the 4 possibilities that this suggests.
  - $(x \in A) \wedge (x \in A)$ — this is easy because we have that $x \in A \cup$ (any set we choose)
  - $(x \in A) \wedge (x \in C)$ — this is also easy because we have that $x \in A \cup$ (any set we choose)
  - $(x \in B) \wedge (x \in A)$ — similarly we have that $x \in A \cup$(any set we choose)
  - $(x \in B) \wedge (x \in C)$ — not too hard because $x \in B \cap C$

  So these four possibilities really break down into two cases. Either $x \in A$ or $x \notin A$.
  - If $x \in A$, then we know that $x \in A \cup$anything and so $x \in A \cup (B \cap C)$.
  - Otherwise, if $x \notin A$ then we must have that $x \in B$ and $x \in C$, so $x \in B \cap C$. Then since $x \in B \cap C$, we also have that $x \in (B \cap C) \cup A$.

- In either case we have that $x \in A \cup (B \cap C)$.

Solution.

Proof. We prove each inclusion in turn. Start by assuming that $x \in A \cup (B \cap C)$. Then $x \in A$ or $x \in B \cap C$. We consider each case in turn.

- Assume $x \in A$. Then $x \in A \cup B$ and $x \in A \cup C$ and so $x \in RHS$.

- Assume now that $x \in B \cap C$. Then $x \in B$ and $x \in C$, so $x \in B \cup A$ and $x \in C \cup A$. Thus $x \in RHS$.

In either case we have $x \in RHS$.

Now assume that $x \in (A \cup B) \cap (A \cup C)$, and so $x \in A \cup B$ and $x \in A \cup C$.

- If $x \in A$ then $x \in A \cup (B \cap C)$.

- If $x \notin A$ then since $x \in A \cup B$, we must have $x \in B$. Similarly since $x \in A \cup C$ we have $x \in C$. Since $x \in B$ and $x \in C$, $x \in B \cap C$. Thus $x \in A \cup (B \cap C)$.

Thus if $x \in LHS$ then $x \in RHS$. And so $LHS \subseteq RHS$. ■

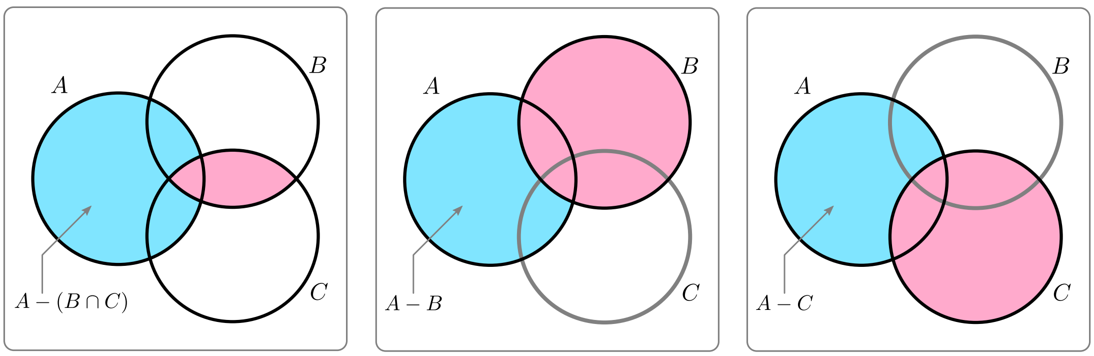
□

We'll prove that $A - (B \cap C) = (A - B) \cup (A - C)$ using the distributive and DeMorgans laws.

Example 8.4.10 Let A, B, C be sets included in a universal set U. Show that

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

Scratchwork. A picture can help us understand this



Let us start with the LHS and we'll use DeMorgan's laws and distributive laws to arrive at the RHS.

$$\begin{aligned} A - (B \cap C) &= A \cap \overline{(B \cap C)} && \text{set-difference as intersection} \\ &= A \cap (\bar{B} \cup \bar{C}) && \text{DeMorgan} \\ &= (A \cap \bar{B}) \cup (A \cap \bar{C}) && \text{distributive} \\ &= (A - B) \cup (A - C) && \text{intersection as set-difference} \end{aligned}$$

That is much much easier than proving it from first principles — that is proving it as we proved the couple of examples above. Of course, this argument things requires that we have already done the hard work of proving those other results.

Now the above calculation is all but a proof, we just need a few words. Also, we probably don't need to annotate our calculation as we have done above — though it wouldn't hurt. If we don't then we should, at a minimum, tell the reader what set laws we have used.

Solution.

Proof. Let A, B, C be sets, then

$$\begin{aligned} A - (B \cap C) &= A \cap \overline{(B \cap C)} \\ &= A \cap (\bar{B} \cup \bar{C}) \\ &= (A \cap \bar{B}) \cup (A \cap \bar{C}) \end{aligned}$$

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

where we have used DeMorgans' laws, the distributive law and the fact that $A - B = A \cap \bar{B}$. ■

□

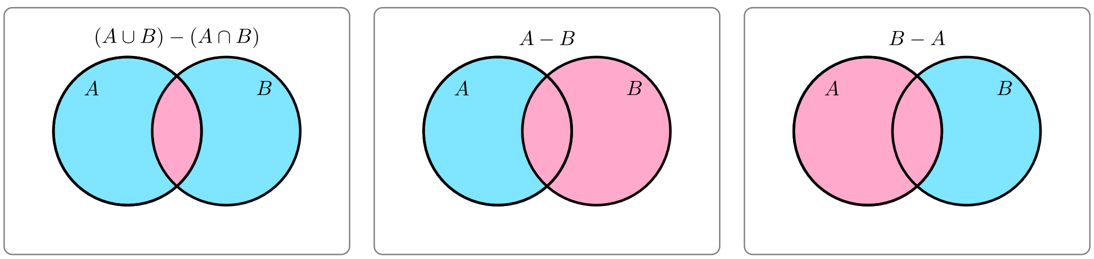
A couple more examples.

Example 8.4.11 Let A, B be sets included in a universal set U. Show that

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

This quantity is called the symmetric difference of A and B and is sometimes denoted $A \Delta B$.

Scratchwork. So we can start by trying to rewrite set differences as intersections and see what happens. Actually, we should start by drawing a picture of what is happening.



Now lets try

$$\begin{aligned}
(A \cup B) - (A \cap B) &= (A \cup B) \cap \overline{(A \cap B)} && \text{DeMorgan it} \\
&= (A \cup B) \cap (\bar{A} \cup \bar{B}) && \text{Distribute} \\
&= \big(A \cap (\bar{A} \cup \bar{B})\big) \cup \big(B \cap (\bar{A} \cup \bar{B})\big) && \text{expand more} \\
&= (A \cap \bar{A}) \cup (A \cap \bar{B}) \cup (B \cap \bar{A}) \cup (B \cap \bar{B}) && \text{now clean up} \\
&= \varnothing \cup (A \cap \bar{B}) \cup (B \cap \bar{A}) \cup \varnothing && \text{rewrite} \\
&= (A - B) \cup (B - A)
\end{aligned}$$

Oof! Here we have used that $C \cap \bar{C} = \varnothing$ and $C \cup \varnothing = C$ for any set C.

What if we try starting with the right and work to the left?

$$\begin{aligned}
(A - B) \cup (B - A) &= (A \cap \bar{B}) \cup (B \cap \bar{A}) && \text{expand} \\
&= \big((A \cap \bar{B}) \cup B\big) \cap \big((A \cap \bar{B}) \cup \bar{A}\big) && \text{expand more} \\
&= \big((A \cup B) \cap (B \cap \bar{B})\big) \cap \big((A \cup \bar{A}) \cap (\bar{B} \cup \bar{A})\big) && \text{clean up} \\
&= \big((A \cup B) \cap U\big) \cap \big(U \cap (\bar{B} \cup \bar{A})\big) && \text{clean more} \\
&= (A \cup B) \cap (\bar{B} \cup \bar{A}) && \text{deMorgan it} \\
&= (A \cup B) \cap \overline{(A \cap B)} \\
&= (A \cup B) - (A \cap B)
\end{aligned}$$

Not much difference really. Here we have used that $C \cup \bar{C} = U$ and $C \cap U = C$.

Solution.

Proof. Let A, B be sets. Then

$$\begin{aligned}
(A \cup B) - (A \cap B) &= (A \cup B) \cap \overline{(A \cap B)} && \text{DeMorgans law}\\
&= (A \cup B) \cap (\bar{A} \cup \bar{B}) && \text{distributive law}\\
&= \big(A \cap (\bar{A} \cup \bar{B})\big) \cup \big(B \cap (\bar{A} \cup \bar{B})\big) && \text{distributive law again}\\
&= (A \cap \bar{A}) \cup (A \cap \bar{B}) \cup (B \cap \bar{A}) \cup (B \cap \bar{B})\\
&= \varnothing \cup (A \cap \bar{B}) \cup (B \cap \bar{A}) \cup \varnothing\\
&= (A - B) \cup (B - A) && \text{as required.}
\end{aligned}$$

Notice that in the last couple of steps we have used the following two facts

$$C \cap \bar{C} = \varnothing \qquad \text{and} \qquad C \cup \varnothing = C$$

for any set C. ■

We can also prove this result from first principles — by showing each side is a subset of the other. We don't present any scratch work here, rather we just leap into the proof. You can see that it is not really any cleaner than the proof we have presented above, but it is always worth seeing things from a different perspective.

Proof. We start by proving the left-hand side is a subset of the right-hand side and then the reverse inclusion. We also make use of the following two facts

$$(x \notin A \cap B) \implies (x \notin A) \vee (x \notin B) \quad \text{and} \quad (x \notin A) \implies (x \notin A \cap B)$$

which are simply the contrapositives of the following statements

$$(x \in A) \wedge (x \in B) \implies (x \in A \cap B) \quad \text{and} \quad (x \in A \cap B) \implies (x \in A)$$

- Assume $x \in LHS$, so $x \in (A \cup B)$ and $x \notin (A \cap B)$. This second fact implies that $x \notin A$ or $x \notin B$.
    - If $x \notin A$ then since $x \in A \cup B$, it follows that we must have $x \in B$. Since $x \in B$ and $x \notin A$, we have that $x \in B - A$.
    - Similarly, if $x \notin B$ then since $x \in A \cup B$, we must have $x \in A$. Hence $x \in A - B$.

  In either case $x \in (A - B) \cup (B - A)$, so $LHS \subseteq RHS$.
- Now assume that $x \in RHS$, so $x \in A - B$ or $x \in B - A$.
    - If $x \in A - B$, then $x \in A$ but $x \notin B$. Since $x \in A$, $x \in A \cup B$. And since $x \notin B$, we know that $x \notin B \cap A$. Hence $x \in (A \cup B) - (A \cap B)$.
    - Similarly, if $x \in B - A$, then $x \in B$ but $x \notin A$. Since $x \in B$, $x \in B \cup A$. And since $x \notin A$, we know that $x \notin A \cap B$. Hence $x \in (A \cup B) - (A \cap B)$.

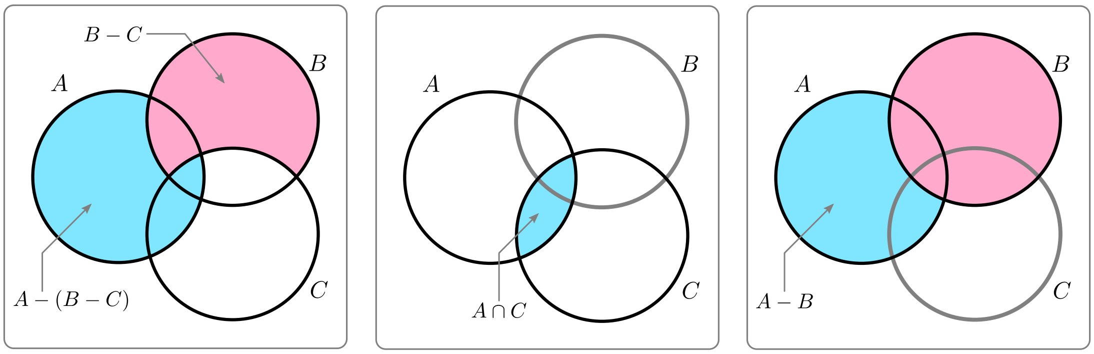
  Thus we know that $RHS \subseteq LHS$. Consequently $LHS = RHS$ as required.

■

□

Example 8.4.12 Let A, B, C be sets included in a universal set U. Prove that $A - (B - C) = (A \cap C) \cup (A - B)$.

Scratchwork. Again, we start with a picture of what is going on:



And now we should play around with some of what we already know

$$\begin{aligned}
A - (B - C) &= A \cap \overline{(B - C)} && \text{set difference as intersection}\\
&= A \cap \overline{B \cap \bar{C}} && \text{set difference as intersection}\\
&= A \cap (\bar{B} \cup \bar{\bar{C}}) && \text{DeMorgan}\\
&= A \cap (\bar{B} \cup C) && \text{double complement}\\
&= (A \cap \bar{B}) \cup (A \cap C) && \text{distributive law}\\
&= (A \cap C) \cup (A - B) && \text{intersection as set difference}
\end{aligned}$$

oof!

Solution.

Proof. Let A, B, C be sets as given in the statement of the result. Then

$$\begin{aligned}
A - (B - C) &= A \cap \overline{(B - C)}\\
&= A \cap \overline{B \cap \bar{C}}\\
&= A \cap (\bar{B} \cup C)\\
&= (A \cap \bar{B}) \cup (A \cap C)\\
&= (A \cap C) \cup (A - B)
\end{aligned}$$

where we have used the fact that $A - B = A \cap \bar{B}$, DeMorgans laws and distributive laws. ■

□

8.5 Indexed sets

Our usual set notation works well when we have a small number of sets; if our work involves three sets, we can just denote them A, B and C. However, this quickly becomes inconvenient when we have even a moderate number of sets; what should we use to denote the 17^{th} set? One solution it to use indices to distinguish between sets:

$$A_1, A_2, A_3, \ldots$$

More generally, our indices do not need to be natural numbers, but instead come from any set. So, for example, we could define a family of sets indexed by elements of another set S

$$\{A_\alpha \text{ s.t. } \alpha \in S\}$$

In this context[103] we call S the **indexing set**, and the sets A_α the **indexed sets**. Typically, the indexing set is a subset of the natural numbers.

Now, recall that we defined the intersection of sets A and B to be the set of all elements that are in both sets. Similarly the union of A and B is the set of all elements that are in at least one of the sets. It is not hard to extend this to the intersection and union of three sets:

$$A \cap B \cap C = \{x \text{ s.t. } x \text{ is every one of } A, B, C\}$$

and

$$A \cup B \cup C = \{x \text{ s.t. } x \text{ is in at least one of } A, B, C\}$$

Writing the intersection and union this way, shows how we can extend them to intersections and unions of large numbers of sets. Indeed we define,

Definition 8.5.1 Let $N \in \mathbb{N}$ and let $A_1, A_2, \ldots, A_N$ be a collection of sets. We define the intersection of $A_1, A_2, \ldots, A_N$ as

$$\bigcap_{k=1}^{N} A_k = \{x \text{ s.t. } x \in A_j \text{ for all } j \in \{1, 2, \ldots, N\}\}.$$

We similarly define their union to be

$$\bigcup_{k=1}^{N} A_k = \{x \text{ s.t. } x \in A_j \text{ for some } j \in \{1, 2, \ldots, N\}\}.$$

$\Diamond$

This notation is very useful when we have to work with lots of sets[104]. We can generalise it further. For example, these unions and intersections need not start at index 1. Nor do they need to be unions and intersections over finite collections of sets.

Definition 8.5.2 Let $m, M \in \mathbb{N}$ with $m \leq M$, and let A_k be a set for all $k = m, m+1, \ldots, M$. Then

$$\bigcap_{k=m}^{M} A_k = \{x \text{ s.t. } \forall j \in \{m, m+1, \ldots, M\}, x \in A_j\}$$

[103]We hope the reader will forgive the authors for not making a formal definition here.

[104]As you can see, this notation is very similar to the Σ, Π notation we use to denote sums and products.

$$\bigcup_{k=m}^{M} A_k = \{x \text{ s.t. } \exists j \in \{m, m+1, \ldots, M\} \text{ s.t. } x \in A_j\}$$

Further, let $B_m, B_{m+1}, B_{m+2}, \ldots$ be sets, then

$$\bigcap_{k=m}^{\infty} B_k = \{x \text{ s.t. } \forall j \in \mathbb{N} \text{ with } j \geq m, x \in B_j\}$$

$$\bigcup_{k=m}^{\infty} B_k = \{x \text{ s.t. } \exists j \in \mathbb{N} \text{ with } j \geq m \text{ s.t. } x \in B_j\}$$

$\Diamond$

These definitions tell us that if $x \in \bigcap_{n=m}^{\infty} A_n$, then $x \in A_k$ for every single $k \geq m$. On the other hand, if we know that $x \notin \bigcap_{n=m}^{\infty} A_n$, then there must be at least one index $k \geq m$ so that $x \notin A_k$. Similarly, if $x \in \bigcup_{n=m}^{\infty} A_n$, then there is at least one index $k \geq m$ so that $x \in A_k$. And if $x \notin \bigcup_{n=m}^{\infty} A_n$, then $x \notin A_k$ for every single $k \geq m$.

Example 8.5.3 Consider the indexed sets, $A_n = \left(-\frac{1}{n}, \frac{1}{n}\right)$ for $n \in \mathbb{N}$. So that, for example,

$$A_2 = \left(-\frac{1}{2}, \frac{1}{2}\right) \qquad \text{and} \qquad A_{27} = \left(-\frac{1}{27}, \frac{1}{27}\right).$$

Then

$$0 \in \bigcap_{n=1}^{\infty} A_n$$

but

$$\frac{1}{e} \notin \bigcap_{n=1}^{\infty} A_n.$$

The first of these is true since $0 \in A_n = \left(-\frac{1}{n}, \frac{1}{n}\right)$ for all $n \in \mathbb{N}$. The second follows[105] since $e < 3$ and so $\frac{1}{e} > \frac{1}{3}$ and so $\frac{1}{e} \notin A_3$; since it is not in one of the sets, it cannot be in the intersection of those sets.

Actually we have something a little stronger here. We have $\frac{1}{e} \notin \left(-\frac{1}{n}, \frac{1}{n}\right)$ for any $n \geq 3$. But since we want to show that $\frac{1}{e}$ is not in the intersection, it is enough to show that it is not in at least one of the intersecting sets. $\square$

In general, we don't have to take our indices from the natural numbers. We can index sets with rational numbers, real number, matrices, colours — just about any set. For example, for any real number $x \in (0, 10)$ we can define

$$A_x = [-x, x^2] = \left\{t \in \mathbb{R} \text{ s.t. } -x \leq t \leq x^2\right\}.$$

[105] We are assuming that we know $e = 2.71828\ldots$. It is not too hard to show that $2 < e < 3$, but it does take some calculus.

So that $A_5 = [5, 25]$ and $A_\pi = [-\pi, \pi^2]$. So the A_x form a family of sets indexed by real numbers. Sometimes we might need to take the union and intersection of all the sets in such a family, and so we generalise the notation even more.

Definition 8.5.4 Let $\mathcal{S}$ be a set, and let A_s be a set for all $s \in \mathcal{S}$. Then we can define the intersection and union over all of these sets:

$$\bigcap_{s\in\mathcal{S}} A_s = \{x \text{ s.t. } \forall s \in \mathcal{S}, x \in A_s\},$$

and

$$\bigcup_{s\in\mathcal{S}} A_s = \{x \text{ s.t. } \exists s \in \mathcal{S} \text{ s.t. } x \in A_s\},$$

$\Diamond$

Remark 8.5.5 When we do have sets indexed by the natural numbers, say $A_m, A_{m+1}, A_{m+2}, \ldots$ etc, it can be convenient to write their intersection and union as

$$A_m \cap A_{m+1} \cap A_{m+2} \cap \cdots \qquad \text{and} \qquad A_m \cup A_{m+1} \cup A_{m+2} \cup \cdots$$

It is arguably better to avoid this notation in favour of the more precise notation above. We should make sure that things are clear for our reader.

A more subtle, but very important point, is that when sets are indexed by real numbers it can, in fact, be impossible to write the union or intersection of those sets in this way. This is because the real numbers are not **countable**. There is simply no way to write out the real numbers in an ordered list in this way. The interested reader should jump ahead to Chapter 12 for more on the uncountability of the reals.

Example 8.5.6 Determine whether or not the following statements are true or false.

(a) $\displaystyle\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, \frac{1}{n}\right) = \emptyset$

(b) $\displaystyle 3 \in \bigcup_{n=3}^{\infty} \left(2 + \frac{1}{n}, 3 - \frac{1}{n}\right]$

(c) Given the indexed sets $A_x = [-x, x^2]$, for $x \in \mathbb{R}, x > 0$, we have

$$0 \in \bigcap_{x\in(0,1)} A_x.$$

(d) Given the indexed sets $A_y = \big(-e^y, 1 - \frac{1}{y}\big]$, for $y \in \mathbb{R}$, we have

$$1 \in \bigcup_{y\in(1,\infty)} A_y.$$

(e) $[-1, 0) \subseteq \bigcup_{n=2}^{\infty} \left[-1, -\frac{1}{n}\right]$

(f) $\bigcap_{n=5}^{\infty} \left[0, 1 + \frac{1}{n}\right) \subseteq [0, 1)$

Solution.

(a) This statement is false since for all $n \in \mathbb{N}$, we have $0 \in \left(-\frac{1}{n}, \frac{1}{n}\right)$. Therefore $\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, \frac{1}{n}\right) \neq \emptyset$.

Notice that we see that our indexed sets are getting smaller and smaller as n grows larger and larger. We also see that

$$\bigcap_{n=1}^{k} \left(-\frac{1}{n}, \frac{1}{n}\right) = \left(-\frac{1}{k}, \frac{1}{k}\right).$$

One might take this to suggest that we can understand $\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, \frac{1}{n}\right)$, by just looking at what happens to A_k as k goes to infinity. This is a dangerous line of reasoning. Since $-\frac{1}{k}$ and $\frac{1}{k}$ both go to 0 as k goes to infinity, we are tempted to say that $\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, \frac{1}{n}\right) = (0, 0) = \emptyset$. But we have already shown the intersection is not empty since it contains 0. It is important to use the definitions carefully to determine what the intersections or unions contain.

(b) We see that this statement is false since in order for 3 to be in $\bigcup_{n=3}^{\infty} \left(2 + \frac{1}{n}, 3 - \frac{1}{n}\right]$, it must be in at least one of the sets $\left(2 + \frac{1}{n}, 3 - \frac{1}{n}\right]$ for $n \in \{3, 4, 5, \ldots\}$.

But, we see that for all $n \in \{3, 4, 5, \ldots\}$, $3 - \frac{1}{n} < 3$, which implies that $3 \notin \left(2 + \frac{1}{n}, 3 - \frac{1}{n}\right]$ for any $n \in \{3, 4, 5, \ldots\}$. Therefore $3 \notin \bigcup_{n=3}^{\infty} \left(2 + \frac{1}{n}, 3 - \frac{1}{n}\right]$.

(c) We see that for all $x \in (0, 1)$, we have $-x < 0$ and $x^2 > 0$. Thus, this statement is true since we have $0 \in [-x, x^2]$, for all $x \in (0, 1)$.

(d) This statement is false since for all $y \in (1, \infty)$, we see $1 - \frac{1}{n} < 1$, and hence $1 \notin \big(-e^y, 1 - \frac{1}{y}\big]$ for any $y \in (1, \infty)$.

(e) This statement is true. To show it let $x \in [-1, 0)$. Then, all we have to do is to show that $x \in \left[-1, -\frac{1}{n}\right]$ for at least one $n \in \{2, 3, 4, \ldots\}$. For that, it is sufficient to show that $x \leq -\frac{1}{n}$ for some $n \in \{2, 3, 4, \ldots\}$ (since we already know that $x \geq -1$).

We can find such n by choosing $N = \left\lceil \frac{1}{|x|} \right\rceil$, where $\lceil t \rceil$ denotes the ceiling function — ie the first integer greater or equal to t. By using the ceiling function we are really just rounding up the value of $\frac{1}{|x|}$. With that choice of N, we know that $x \leq -\frac{1}{N}$ and hence $x \in [-1, \frac{1}{N}]$. Therefore $[-1, 0) \subseteq \bigcup_{n=2}^{\infty} \left[-1, -\frac{1}{n}\right]$.

(f) Since $1 + \frac{1}{n}$ goes to 1 as n goes to infinity, it is tempting to say that the statement is true. Unfortunately[106], this it not correct.

This statement is actually false because, similar to the argument we used in Item a, $1 \in \bigcap_{n=5}^{\infty} \left[0, 1 + \frac{1}{n}\right)$. Thus, $1 \in \bigcap_{n=5}^{\infty} \left[0, 1 + \frac{1}{n}\right)$, but $1 \notin [0, 1)$. Therefore $\bigcap_{n=5}^{\infty} \left[0, 1 + \frac{1}{n}\right) \not\subseteq [0, 1)$.

□

Before we go on to the next example, let's prove a useful lemma.

Lemma 8.5.7 *Let $x \in \mathbb{R}$. If for all $k \in \mathbb{N}$, $x < \frac{1}{k}$ then $x \leq 0$.*

Proof. We prove the contrapositive of this statement. Namely, if $x > 0$ then there is some $k \in \mathbb{N}$ so that $x \geq \frac{1}{k}$. So assume that $x > 0$. Then $0 < \frac{1}{x} \leq \left\lceil \frac{1}{x} \right\rceil = \ell$, where $\ell \in \mathbb{N}$. Then $x \geq \frac{1}{\ell}$ as required. ■

Example 8.5.8 For $k \in \mathbb{N}$ let A_k be the intervals $A_k = [\frac{1}{k+1}, 1 + \frac{1}{k+1})$.

(a) Show that $\bigcup_{k=1}^{\infty} A_k = (0, \frac{3}{2})$.

(b) Show that $\bigcap_{k=1}^{\infty} A_k = [\frac{1}{2}, 1]$

Solution.

Proof. Let us show the two inclusions in turn.

- Let $x \in \bigcup_{k=1}^{\infty} A_k$. Then $x \in A_k$ for some $k \in \mathbb{N}$ so that $\frac{1}{k+1} \leq x < 1 + \frac{1}{k+1}$ from which we get that $0 < x < \frac{3}{2}$, so that $x \in (0, \frac{3}{2})$.

[106]Well, actually it is fortunate. The authors have constructed this example with precisely that in mind. The reader should not give in to the temptation of a quick limit to solve all their set problems.

- Now let $x \in (0, \frac{3}{2})$. Then let us consider two cases, $x \geq \frac{1}{2}$ or $x < \frac{1}{2}$.
  1. First case: Suppose that $x \geq \frac{1}{2}$. Then because of the assumption on x we have $\frac{1}{2} \leq x < \frac{3}{2}$, and so $x \in A_1$, so $x \in \bigcup_{k=1}^{\infty} A_k$.
  2. Second case: Suppose that $x < \frac{1}{2}$. Then if we let $n = \lceil \frac{1}{x} \rceil$ then we have $\frac{1}{x} < n+1$ and so $x > \frac{1}{n+1}$. This is enough to show that $x \in A_n$ with $n \in \mathbb{N}$ and so $x \in \bigcup_{k=1}^{\infty} A_k$.

■

Proof. Again, we prove the two inclusions in turn.

- Let $x \in \bigcap_{k=1}^{\infty} A_k$. Then for any $k \in \mathbb{N}$ we have $x \in A_k$ so that the inequality $\frac{1}{k+1} \leq x < 1 + \frac{1}{k+1}$ holds for any $k \in \mathbb{N}$. In particular, $x \geq \frac{1}{2}$.

  Now we can use Lemma 8.5.7 to show that $x \leq 1$. Since we know that $x - 1 < \frac{1}{k+1}$, Lemma 8.5.7 implies that $x - 1 < 0$ and hence $x \leq 1$.

  So we have now shown that $x \geq \frac{1}{2}$ and $x \leq 1$ and thus $x \in [\frac{1}{2}, 1]$.

- Now let $x \in [\frac{1}{2}, 1]$. So $\frac{1}{2} \leq x \leq 1$. Let $k \in \mathbb{N}$, we can check that $\frac{1}{k+1} \leq \frac{1}{2}$ and $1 + \frac{1}{k+1} > 1$, hence $\frac{1}{k+1} \leq x < 1 + \frac{1}{k+1}$ so $x \in A_k$. In the end, for any $k \in \mathbb{N}$ we have $x \in A_k$, so that $x \in \bigcap_{k=1}^{\infty} A_k$.

■

□

8.6 Exercises

1. Consider the following sets

- $A_1 = \{x \in \mathbb{Z} \colon x^2 < 2\}$,
- $A_2 = \{x \in \mathbb{N} \colon (3 \mid x) \wedge (x \mid 216)\}$,
- $A_3 = \left\{x \in \mathbb{Z} \colon \dfrac{x+2}{5} \in \mathbb{Z}\right\}$,
- $A_4 = \{a \in B \colon 6 \leq 4a + 1 < 17\}$, where $B = \{1, 2, 3, 4, 5, 6\}$,
- $A_5 = \{x \in C \colon 50 < xd < 100 \text{ for some } d \in D\}$, where $C = \{2, 3, 5, 7, 11, 13, \ldots\}$ and $D = \{5, 10\}$,
- $A_6 = \{5, 10, 15, 20, 25, \ldots\}$,
- $A_7 = \{2, 3, 4, 6, 8, 9, 12, 16, 18, 24 \ldots\}$,

Write down the sets below by listing their elements.

(a) $A_2 - A_3$,

(b) $A_5 \cap A_6$,

(c) $\mathcal{P}(A_1))$,

(d) $\mathcal{P}(\mathcal{P}(A_1 - \{-1\}))$,

(e) $A_3 \cap A_4$,

(f) $A_3 - A_7$,

(g) $A_5 \cup A_2$,

(h) $A_2 \cap A_7$.

(i) $A_5 \cap \overline{A_2}$, given the universal set $U = \mathbb{R}$.

(j) Verify whether $(A_4 \times B) \cap (B \times A_4) = A_4 \times A_4$ and $(A_4 \times B) \cup (B \times A_4) = B \times B$.

2. Write down the set $F \cap G$ where

$$F = \left\{(x, x^2 - 3x + 2) \in \mathbb{R}^2 : x \in \mathbb{R}\right\} \qquad \text{and} \qquad G = \left\{(a, a+2) \in \mathbb{R}^2 : a \in \mathbb{R}\right\}$$

by listing out all of its elements. Prove your answer.

3. Prove or disprove the following statement:

Suppose A, B and C are sets. If $A = B - C$, then $B = A \cup C$.

4. Suppose $x, y \in \mathbb{R}$ and $k \in \mathbb{N}$ satisfying, $x, y > 0$ and $x^k = y$. Then prove that $\{x^a \text{ s.t. } a \in \mathbb{Q}\} = \{y^a \text{ s.t. } a \in \mathbb{Q}\}$.

5. Prove or disprove the following statement:

If $m, n \in \mathbb{N}$, then $\{x \in \mathbb{Z} : m \mid x\} \cap \{x \in \mathbb{Z} : n \mid x\} \subseteq \{x \in \mathbb{Z} : mn \mid x\}$.

6. Prove or disprove the following statement:

Let $m, n \in \mathbb{Z}$. Then $\{x \in \mathbb{Z} : mn \mid x\} \subseteq \{x \in \mathbb{Z} : m \mid x\} \cap \{x \in \mathbb{Z} : n \mid x\}$.

7. Let A be a set. Prove or disprove the following statements. If the statement is false in general, determine if there are any sets for which the statement is true.

(a) $A \times \emptyset \subseteq A$.

(b) $A \times \emptyset = A$.

8. Suppose that $A, B \neq \emptyset$, and C are sets such that $A \subseteq B$.

(a) Prove that $A \times C \subseteq B \times C$.

(b) Suppose we have a strict containment $A \subset B$ instead. What additional constraints do we need (if any) to show that

$$A \times C \subset B \times C?$$

Prove your claim.

9. Prove or disprove the following statement:

If A and B are sets, then $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

10. Prove or disprove the following statement:

If A and B are sets, then $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$.

11. Let A be a finite set with $|A| = n$. Prove that $|\mathcal{P}(A)| = 2^n$.

12. Let A and B be sets. Prove or disprove the following statements:

- $\mathcal{P}(A - B) \subseteq \mathcal{P}(A) - \mathcal{P}(B)$, and
- $\mathcal{P}(A) - \mathcal{P}(B) \subseteq \mathcal{P}(A - B)$.

13. Prove that

(a) $\displaystyle\bigcup_{n=3}^{\infty} \left(\frac{1}{n}, 1 - \frac{1}{n}\right) = (0, 1)$

(b) $\displaystyle\bigcap_{n=1}^{\infty} \left(-\frac{1}{n}, 1 + \frac{1}{n}\right) = [0, 1]$

14. Determine what each of the following unions is equal to, and prove your answer.

(a)

$$\bigcup_{n \in \mathbb{N}} [-n, n]$$

(b)

$$\bigcup_{r \in \mathbb{R}, r > 0} B_r$$

where

$$B_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 < r\}.$$

15. Let $S \subset \mathbb{R}$. We say $b \in \mathbb{R}$ is an *upper bound* of S if $s \leq b$ for every $s \in S$. Further, we say $a \in \mathbb{R}$ is the *supremum* (or the *least upper bound*) of S, denoted by $\sup(S)$, if

- a is an upper bound for S, and
- if b is an upper bound for S, then $a \leq b$.

We also call $c \in S$ the *maximum element* of S, denoted by $\max(S)$, if it is the largest element in S. So, $\max(S)$ belongs to S, and is an upper bound of S.

For each of the following sets, determine its maximum and supremum, if they exist. Justify your answers.

(a) $[1, 3] = \{x \in \mathbb{R} \ : \ 1 \leq x \leq 3\}$

(b) $(1,3) = \{x \in \mathbb{R} \ : \ 1 < x < 3\}$

(c) $\{m \in \mathbb{Z} \ : \ |2(m-4)| \leq 15\}$

(d) $\left\{2 - \frac{1}{n} \ : \ n \in \mathbb{N}\right\}$

(e) $\{x \in \mathbb{R} \ : \ \cos(2x) = 1\}$

16. This question involves the supremum, which we first introduced in a previous exercise, Exercise 8.6.15. We recommend that you complete that question before you attempt this one.

Let $S \subset \mathbb{R}$. We say $b \in \mathbb{R}$ is an *upper bound* of S if $s \leq b$ for every $s \in S$. Further, we say $a \in \mathbb{R}$ is the *supremum* (or the *least upper bound*) of S, denoted by $\sup(S)$, if

- a is an upper bound for S, and
- if b is an upper bound for S, then $a \leq b$.

Suppose that S, T are non-empty subsets of $\mathbb{R}$, and $s = \sup(S)$, $t = \sup(T)$, where $s, t \in \mathbb{R}$.

(a) Show that $\sup(S \cup T) = \max\{s, t\}$.

(b) Can you determine $\sup(S \cap T)$?

(c) Define $S + T = \{s + t : s \in S, t \in T\}$. Show that $\sup(S + T) = s + t$.

17. Before completing this question you should look at Exercise 8.6.15 and Exercise 8.6.16. Let $\{a_n\}_{n \in \in \mathbb{N}}$ be a sequence such that $a_{n+1} \geq a_n$ for all $n \in \mathbb{N}$, and such that

$$a = \sup\{a_n : n \in \mathbb{N}\}$$

exists as a real number. Show that

$$\lim_{n \to \infty} a_n = a.$$

Chapter 9

Relations

A great number of equations that we see in mathematics tell us about the relationship between two objects. For example

- $a < b$ — the number a is strictly less than the number b.
- $a|b$ — the number a is a divisor of the number b.
- $a = b$ — the quantities a and b are equal.
- $a \in B$ — the object a is a member of the set B.
- $a \equiv b \pmod{n}$ — a and b have the same remainder when divided by n.

We haven't seen this last one yet, but we will soon — it is a way of generalising the notions of odd and even numbers.

These symbols

$$< \qquad | \qquad = \qquad \in \qquad \equiv$$

all encode relationships between objects. Of course, all the relationships we've stated above are quite different however, there is something to be gained from developing a general theory of how **relations** behave and underline what they have in common.

Consider the symbol that we use to denote divisibility. We say that

$$a|b \iff b = ak \text{ where } k \in \mathbb{Z}$$

You can think of "|" as some sort of operator that takes two objects and declares some relationship between them. Here, both of those objects come from the same set — namely the integers.

Similarly, the symbol we use to denote set membership

$$a \in B$$

tells us that the object a lies inside the object B. Again, this symbol "$\in$" can be an operator that takes two objects and declares a relationship between them. In this case, in contrast with the previous case, the objects need not come from the same set — a could be an integer and B a subset of integers.

In each case, the symbol is declaring a relationship between two objects.

One more. Consider the set $A = \{1, 2, 4, 8\}$, and all the comparisons we can make between those numbers using "is divisible by". Now since there are 4 numbers, we can make 4^2 comparisons:

$1 \mid 1$	$1 \mid 2$	$1 \mid 4$	$1 \mid 8$
$2 \nmid 1$	$2 \mid 2$	$2 \mid 4$	$2 \mid 8$
$4 \nmid 1$	$4 \nmid 2$	$4 \mid 4$	$4 \mid 8$
$8 \nmid 1$	$8 \nmid 2$	$8 \nmid 4$	$8 \mid 8$

Notice a couple of things here:

- The comparisons require an ordered pair of numbers,
- When the relation is true we use "$\mid$", and when it is false, we just draw a line through it and write "$\nmid$".
- The valid comparisons are just a set of ordered pairs — in particular it forms a subset of $A \times A$.

We could form a similar set of comparisons using the "is less than" relation:

$1 \not< 1$	$1 < 2$	$1 < 4$	$1 < 8$
$2 \not< 1$	$2 \not< 2$	$2 < 4$	$2 < 8$
$4 \not< 1$	$4 \not< 2$	$4 \not< 4$	$4 < 8$
$8 \not< 1$	$8 \not< 2$	$8 \not< 4$	$8 \not< 8$

or with the rather silly "starts with an earlier letter when written in German" comparison[107]. We don't have a ready symbol for this comparison, so we'll just use $\mathcal{R}$ and put a slash through it, $\not\mathcal{R}$, to show when the comparison does not hold.

$1 \not\mathcal{R} 1$	$1 \mathcal{R} 2$	$1 \mathcal{R} 4$	$1 \not\mathcal{R} 8$
$2 \not\mathcal{R} 1$	$2 \not\mathcal{R} 2$	$2 \not\mathcal{R} 4$	$2 \not\mathcal{R} 8$
$4 \not\mathcal{R} 1$	$4 \mathcal{R} 2$	$4 \not\mathcal{R} 4$	$4 \not\mathcal{R} 8$
$8 \mathcal{R} 1$	$8 \mathcal{R} 2$	$8 \mathcal{R} 4$	$8 \not\mathcal{R} 8$

In each case the pairs of numbers that satisfy the relation form a subset of $A \times A$.

Since this set is small and finite we could also represent the relation pictorially. Consider the following figure

[107] For the non-germanophone or those without ready access to dictionary or online translation service: 1 = ein, 2=zwei, 4=vier, 8=acht.

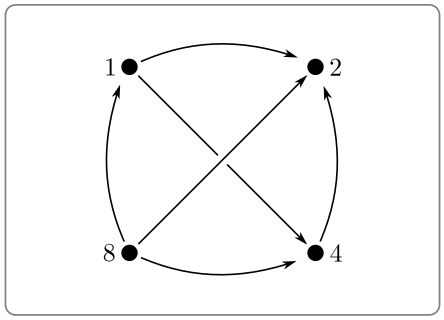


Figure 9.0.1 A pictorial depiction of a silly relation

The dots here denote the elements of the set $A = \{1, 2, 3, 4\}$, and an arrow from x to y denotes $x \mathcal{R} y$. This can be a handy way to visualise things, but really only works when the underlying set is small.

Looking at the above pairs, it should be clear that we can specifiy or *define* the relation using the subset:

$$R = \{(1, 2), (1, 4), (4, 2), (8, 1), (8, 2), (8, 4)\}.$$

More generally we can define *any* relation in this way. This leads us to the formal definition of relation in the next section.

9.1 Relations

Definition 9.1.1 Let A be a set. Then a relation, R, on A is a subset $R \subseteq A \times A$. If the ordered pair $(x, y) \in R$, we denote this as $x \mathcal{R} y$, while if $(x, y) \notin R$ we write $x \not\mathcal{R} y$. ♢

So while we introduced relations in this chapter by starting with relations you already knew — like "is a divisor of" and "is an element of" — the above defines relations as subsets. This allows us much more flexibility and we can use set-builder notation to define specific relations. For example

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

is the relation "=" on the set of real numbers. While

$$S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x - y \in \mathbb{N}\}$$

is the relation ">" on the set of integers.

The definition of relation allows us to take any subset of $A \times A$ to be a relation. For example,

- $R = \varnothing$ gives the relation in which $x \not\mathcal{R} y$ for all $x, y \in A$.
- $R = A \times A$ gives the relation in which $x \mathcal{R} y$ for all $x, y \in A$.

The first of these is sometimes called the **empty relation**, while the latter is called the **universal relation**. Unsurprisingly, the vast majority of other subsets $R \subset A \times A$, won't be particularly interesting or useful or have especially natural or nice definitions. We will, shortly, start to impose additional requirements or properties onto the relations in order to make them more useful and interesting.

For a great many purposes, we define relationships between objects coming from the same set. However, there are situations in which we want to describe relationships between objects from different sets. For example the relation "is an element of", one object will be an element, while the other will be a set. Or, as another example, we could have a set of children and a set of parents, with the relation "is a child of". Consequently, the above definition is often generalised as follows:

Definition 9.1.2 Definition Definition 9.1.1 generalised. Let A, B be sets. Then a relation, R, between A and B is a subset $R \subseteq A \times B$. If the ordered pair $(x, y) \in R$, we denote this as $x \mathcal{R} y$, while if $(x, y) \notin R$ we write $x \not\mathcal{R} y$. $\diamondsuit$

Though the above generalisation will be important when we start to consider **functions**, most of what we will do in this chapter concerns relations that compare elements from a single set, rather than between two sets.

9.2 Properties of relations

Since a relation on A is just a subset of $A \times A$, there are a huge number of possible relations on any given set. As noted above, the vast majority of these will unstructured and be neither useful nor interesting. Typically we require relations to have some additional structure.

Consider the relation "is divisible by" on the set of integers. This has some very useful properties:

- For every $n \in \mathbb{Z}$, it is always true that $n \mid n$,
- If $a \mid b$ and $b \mid c$ then we must have $a \mid c$.

The relation "is less than" on the set of reals, on the other hand, satisfies the second of these, but not the first. These properties (and others) are useful and interesting so let's formalise them.

Definition 9.2.1 Let R be a relation on a set A.

- We say that the relation R is **reflexive** when $a \mathcal{R} a$ for every $a \in A$.
- The relation R is **symmetric** when for any $a, b \in A$, $a \mathcal{R} b$ implies $b \mathcal{R} a$.
- The relation R is **transitive** when for any $a, b, c \in A$, $a \mathcal{R} b$ and $b \mathcal{R} c$ implies $a \mathcal{R} c$.

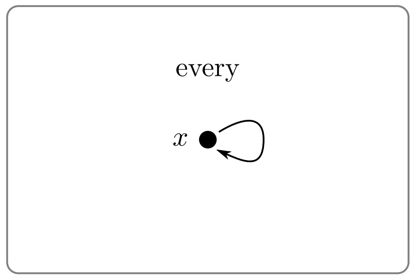
Notice that in the definition of transitive we do not require that a, b, c are different. $\diamondsuit$

Notice that we can write these using quantifiers quite nicely:

reflexive:	$\forall a \in A, (a \mathcal{R} a)$
symmetric:	$\forall a, b \in A, (a \mathcal{R} b) \implies (b \mathcal{R} a)$
transitive:	$\forall a, b, c \in A, (a \mathcal{R} b) \wedge (b \mathcal{R} c) \implies (a \mathcal{R} c)$

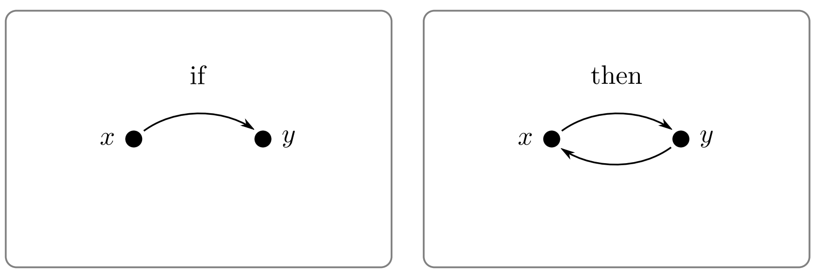
We can visualise these using dot-arrow diagrams (as in Figure 9.0.1). Note that these diagrams are not supposed to represent the entire relation, but rather just enough to illustrate the definitions.

- Reflexive:



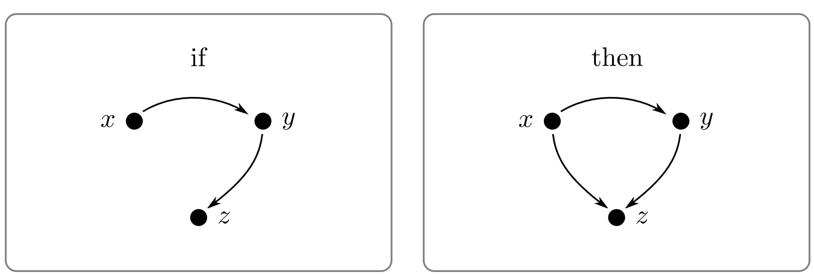
Every element x must have a loop from x back to itself.

- Symmetric:



If there is an arc from x to y then there must also be an arc from y to x.

- Transitive:



If there is an arc from x to y and another from y to z then there must also be an arc from x to z.

With a little work (and some proofs!) we can show that the following table holds for the relations $<, \leq, =, |$ on the set of integers.

R	$<$	$\leq$	$=$	$\mid$
Reflexive	false	true	true	true
Symmetric	false	false	true	false
Transitive	true	true	true	true

Example 9.2.2 Let R be the relation "has the same parity as" on the set of integers. This relation is defined by

$$\begin{aligned} R &= \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a, b \text{ both even or } a, b \text{ both odd}\} \\ &= \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid 2 \mid (a-b)\} \end{aligned}$$

Notice that the second definition is equivalent to the first since

$$(a, b \text{ have same parity}) \iff (2 \mid (a-b)).$$

Prove that this relation is reflexive, symmetric and transitive.

Scratchwork. We explore each in turn:

- Reflexive. We need to show that for every single $a \in \mathbb{Z}$ that $a \mathcal{R} a$. Hence we need to show that for every integer a, that a has the same parity as a. This is pretty obvious, but to write it a little more mathematically — since $a - a = 0$ and $2|0$, we know that $a \mathcal{R} a$.
- Symmetric. We need to show that if $a \mathcal{R} b$ then $b \mathcal{R} a$. So we start by assuming that $a \mathcal{R} b$, so $2 \mid (a-b)$. We need to show that $2 \mid (b-a)$. This, again, is quite obvious, but we can make it more mathematical by saying something like — since $2 \mid (a-b)$ we know that $a - b = 2k$, so $b - a = 2(-k)$, and thus $2 \mid (b-a)$
- Transitive. We need to show that if $a \mathcal{R} b$ and $b \mathcal{R} c$ then $a \mathcal{R} c$. So we assume that $a \mathcal{R} b$ and $b \mathcal{R} a$. This means that $2 \mid (a-b)$ and $2 \mid (b-c)$. So there are integers k, ℓ so that

  $$a - b = 2k \qquad\qquad b - c = 2\ell.$$

  Now we need to show something about $a - c$. It is easy to isolate $a = 2k + b$ and $c = 2\ell + b$, so $a - c = 2k - 2\ell$. Hence $2 \mid (a-c)$ as we need.

We are not done until we write it up nicely. So we do that now.

Solution.

Proof. Let the relation be as defined in the statement. We prove each property in turn.

- Reflexive — Let $a \in \mathbb{Z}$. Since $a - a = 0$ and $2 \mid 0$, we know that $a \mathcal{R} a$.
- Symmetric — Let $a, b \in \mathbb{Z}$ so that $a \mathcal{R} b$. We know that $2 \mid a - b$ and so we can write $a - b = 2k$ for some $k \in \mathbb{Z}$. But then $b - a = 2(-k)$, and so $2 \mid (b-a)$ and thus $b \mathcal{R} a$.

- Transitive — Let $a, b, c \in \mathbb{Z}$ with $a \mathcal{R} b$ and $b \mathcal{R} c$. Thus we know that $a - b = 2k$ and $b - c = 2\ell$ for some integer k, ℓ. But then $a - c = 2(k + \ell)$ and thus $2 \mid (a - c)$. Hence $a \mathcal{R} c$ as required.

■

□

More examples:

Example 9.2.3 Let A be the set of students at UBC, and consider the relation "attended highschool with".

- Reflexive — It is reflexive since every student went to highschool with themselves.
- Symmetric — It is symmetric, because if student a went to highschool with b, then b went to the same highschool as a.
- Transitive — It is not transitive, just because a went to school with b and b went to school with c, it does not mean that a went to school with c. It is possible that b went to two different highschools, one they attended with a and the second they attended with c.

□

Another student flavoured example.

Example 9.2.4 Let A be the set of students in the student union building at 1pm, and let R be the relation "is within 2 metres of".

- Reflexive — It is reflexive since each student is less than 2m from themselves.
- Symmetric — It is symmetric, because if student a is less than 2m from student b, then b is less than 2m from a.
- Transitive — It is not transitive, just because a is 2m from b and b is 2m from c, it does not mean that a is 2m from c. If the students are arranged in a line with 1.5m between each of them, then a is 3m from c.

□

Example 9.2.5 Let R be the relation "is a subset of" on the set of all subsets of the integers.

- Reflexive — The relation is reflexive since for all sets X, we have $X \subseteq X$.
- Symmetric — The relation is not symmetric. Let $X = \emptyset, Y = \{1\}$, then $X \subseteq Y$ but $Y \not\subseteq X$.
- Transitive — The relation is transitive. Assume $A \subseteq B$ and $B \subseteq C$. Now let $a \in A$. Since $A \subseteq B$ we know $a \in B$. And since $B \subseteq C$, we know $a \in C$. Hence $A \subseteq C$ as required.

□

These aren't the only interesting properties of relations. Here are some others we won't really use, except maybe for some examples and exercises.

- A relation is **total** (also called **connex**) when

$$\forall a, b \in A, (a \mathcal{R} b) \vee (b \mathcal{R} a).$$

  The relation $\leq$ on the set of reals is total.

- A relation is **trichotomous** when

$$\forall a, b \in A, \text{ exactly one of } (a \mathcal{R} b) \text{ or } (b \mathcal{R} a) \text{ or } (a = b).$$

  The relation $<$ is trichotomous.

- A relation is **anti-symmetric** when

$$\forall a, b \in A, (a \mathcal{R} b) \wedge (b \mathcal{R} a) \implies a = b.$$

  The relation $\subseteq$ is anti-symmetric, so is $|$ on natural numbers. However $|$ is not anti-symmetric on the set of all integers. If $b = -a$, then $a \mid b$ and $b \mid a$, but $a \neq b$.

- A relation is **dense** when

$$\forall a, b \in A, \exists c \in A \text{ s.t. } (a \mathcal{R} c) \wedge (c \mathcal{R} b).$$

One very important relation on the integers is congruence - recall Definition 5.3.1. It is not hard to prove that congruence has nice properties.

Theorem 9.2.6 *Let $n \in \mathbb{N}$ then congruence modulo n is reflexive, symmetric and transitive.*

Proof. Let n be a fixed natural number. We prove each of the properties in turn.

- Reflexive — Let $a \in \mathbb{Z}$. Then since $a - a = 0$ and $n \mid 0$, we know that $a \equiv a \pmod{n}$.

- Symmetric — Let $a, b \in \mathbb{Z}$ and assume that $a \equiv b \pmod{n}$. Hence we know that $n \mid (a - b)$, and so we can write $a - b = nk$ for some integer k. Thus $b - a = n(-k)$ and so $n \mid (b - a)$ and $b \equiv a \pmod{n}$.

- Transitive — Let $a, b, c \in \mathbb{Z}$ and assume that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. This implies that $n \mid (a - b)$ and $n \mid (b - c)$, and so we can write $(a - b) = nk, (b - c = n\ell)$ for some integers k, l. Consequently $(a - c) = (a - b) + (b - c) = n(k + \ell)$ and $n \mid (a - c)$. Hence $a \equiv c \pmod{n}$.

■

Notice that one immediate consequence of this theorem is that since congruence modulo n is symmetric, we can be a little bit more relaxed when discussing it. In particular, in the examples above we have been very careful to say

- "19 is congruent to 5 modulo 7"
- "11 is congruent to 27 modulo 4"
- "13 is congruent to 7 modulo 5"

where there is a definite *first* number and a definite *second* number in the relation. However since congruence is symmetric, we can instead say

- "19 and 5 *are* congruent modulo 7"
- "11 and 27 *are* congruent modulo 4"
- "13 and 7 *are not* congruent modulo 5"

where the order of the two numbers in the relation no longer matters. Of course we must still be careful with the modulus; we cannot mix that up with the other numbers.

We will return to congruences in more detail shortly.

Another example:

Example 9.2.7 Fractions. Let F be the set of all fractions:

$$F = \left\{ \frac{a}{b} \;\mid\; a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

Consider the following fractions that are *different* elements of F:

$$\frac{2}{4} \qquad \frac{3}{6} \qquad \frac{-7}{-14} \qquad \frac{9}{18}$$

All of these are just different ways of writing "one half" and so correspond to the same single element of $\mathbb{Q}$. We typically avoid this duplication by *representing* each rational number by a single reduced fraction. This is an example of an **equivalence class**, but we will get to those in the next section.

But before that, let us formalise how two fractions are related. We've been doing that since primary school — they are related when they are the same rational number. That is

$$\frac{a}{b} \mathcal{R} \frac{c}{d} \iff \frac{a}{b} = \frac{c}{d}$$

Notice the "=" in the equation on the right *does not* mean that the fractions are *identical* rather it means that they represent the same number. We can make this condition a little more comfortable by writing it as

$$\frac{a}{b} \mathcal{R} \frac{c}{d} \iff ad = bc$$

Let us show that this relation is reflexive, symmetric and transitive.

Proof. We show that the relation on the set of fractions defined above is reflexive, symmetric and transitive.

- Reflexive — Let $\frac{a}{b} \in F$. Then since $ab = ab$, it follows that $\frac{a}{b} \mathcal{R} \frac{a}{b}$. Hence the relation is reflexive.
- Symmetric — Let $\frac{a}{b}, \frac{c}{d} \in F$. Assume that $\frac{a}{b} \mathcal{R} \frac{c}{d}$. Hence $ad = bc$, and so $bc = ad$. Thus $\frac{c}{d} \mathcal{R} \frac{a}{b}$. So the relation is symmetric.
- Transitive — Let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$. Assume that $\frac{a}{b} \mathcal{R} \frac{c}{d}$ and $\frac{c}{d} \mathcal{R} \frac{e}{f}$. Hence we know that
$$ad = bc \qquad \text{and} \qquad cf = de.$$
Multiply the first of these equations by f and the second by b. This gives
$$adf = bcf \qquad \text{and} \qquad bcf = deb$$
Using the transitivity of equality we know that
$$adf = deb$$
and since $d \neq 0$ we have
$$af = eb$$
Thus $\frac{a}{b} \mathcal{R} \frac{e}{f}$ and so the relation is transitive.

■

□

9.3 Equivalence relations and equivalence classes

An important class of relations are those that are similar to "=". We know that "is equal to" is reflexive, symmetric and transitive. Any relation that has these properties acts something like equality does — we call these relations equivalence relations.

Definition 9.3.1 Let R be a relation on a set A. If R is reflexive, symmetric and transitive then R is an equivalence relation. ♢

From our work in the previous section we know that the following relations are equivalence relations

- "is equal to"
- "has same parity as"
- "is congruent to"

Notice that these other two relations are weaker than equality — the underlying objects do not have to be the same in order to be equivalent.

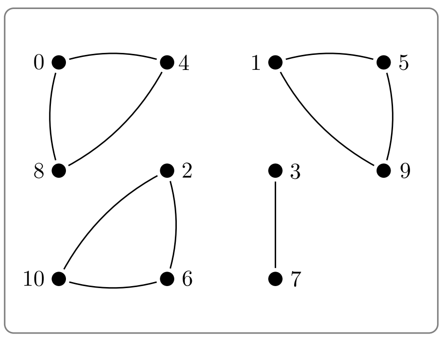
Example 9.3.2 Let A be the set of students at a particular university. Show that the relation "has the same birthday as" is an equivalence relation.
Proof. We need to prove that the relation is reflexive, symmetric and transitive; we prove each in turn.

- Reflexive — Since any person has the same birthday as themselves, the relation is reflexive.
- Symmetric — Let a have the same birthday as b. Then b has the same birthday as a. Hence the relation is symmetric.
- Transitive — Let a have the same birthday as b and b have the same birthday as c. Then it follows that a and c must be born on the same day of the year. Hence a has the same birthday as c.

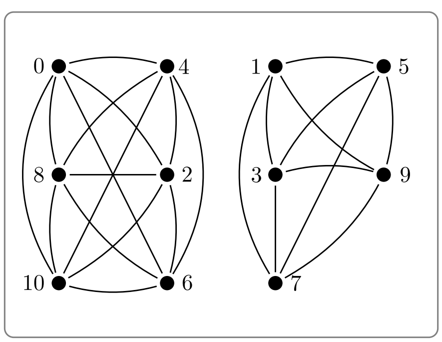
■

□

Consider now the set $A = \{0, 1, 2, 3, \ldots, 10\}$ and consider congruence modulo 4. As we have done a few times, we'll draw a picture of the relation on this set. Not, there could, potentially be a lot of arrows in this figure. To save some space, we can take advantage of the fact that congruence is reflexive, and so we know that if there is an arrow from a to b, there must be one back from b to a. So, instead of drawing two arrows between a and b, we'll just draw a single arc.



We can do exactly the same thing, but now with the relation "has the same parity as"



In each case we should notice that the set of nodes in the pictures fall into a small number of subsets, in which each node is connected to every other node. These connected subsets are examples of equivalence classes.

Definition 9.3.3 Given an equivalence relation R defined on a set A, we define the equivalence class of $x \in A$ (with respect to R) to be the set of elements related to x:

$$[x] = \{y \in A \ : \ y \mathcal{R} x\}$$

This is sometimes also written as "E_x". ♢

So in our "congruent modulo 4" example above, the equivalence classes are

$$\begin{array}{llll} [0] = \{0,4,8\} & [1] = \{1,5,9\} & [2] = \{2,6,10\} & [3] = \{3,7\} \\ [4] = \{0,4,8\} & [5] = \{1,5,9\} & [6] = \{2,6,10\} & [7] = \{3,7\} \\ [8] = \{0,4,8\} & [9] = \{1,5,9\} & [10] = \{2,6,10\} & \end{array}$$

while in our "has the same parity as" example we get

$$\begin{array}{rr} [0] = \{0,2,4,6,8,10\} & [1] = \{1,3,5,7,9\} \\ [2] = \{0,2,4,6,8,10\} & [3] = \{1,3,5,7,9\} \\ [4] = \{0,2,4,6,8,10\} & [5] = \{1,3,5,7,9\} \\ [6] = \{0,2,4,6,8,10\} & [7] = \{1,3,5,7,9\} \\ [8] = \{0,2,4,6,8,10\} & [9] = \{1,3,5,7,9\} \\ [10] = \{0,2,4,6,8,10\} & \end{array}$$

First notice that there are no empty equivalence classes. This follows from the fact that equivalence relations are reflexive:

Lemma 9.3.4 *Let R be an equivalence relation on a set A. Then for any $x \in A$, $x \in [x]$.*

Proof. Let $x \in A$. We know that R is reflexive, so $x \mathcal{R} x$. Since we define

$$[x] = \{a \in A \ : \ a \mathcal{R} x\}$$

we must have that $x \in [x]$. ■

Also notice that there is a lot of repetition in our lists of equivalence classes. Indeed, we could have been listed them as:

$$\begin{array}{cc} [0] = [4] = [8] = \{0,4,8\} & [1] = [5] = [9] = \{1,5,9\} \\ [2] = [6] = [10] = \{2,6,10\} & [3] = [7] = \{3,7\} \end{array}$$

In fact it looks exactly like

$$[x] = [y] \iff x \mathcal{R} y$$

This is an important (and true!) result, so let's call it a theorem and prove it.

Theorem 9.3.5 *Let R be an equivalence relation on A and let $x, y \in A$. Then*

$$x \mathcal{R} y \iff [x] = [y]$$

Proof. We prove each implication in turn.

- ($\Leftarrow$) Assume $[x] = [y]$. From our lemma above, we know $x \in [x]$. Hence $x \in [y]$. But we define $[y] = \{a \in A \ : \ a \mathcal{R} y\}$, and since x is in this set we know that $x \mathcal{R} y$ as required.

- ($\Rightarrow$) Assume $x \mathcal{R} y$. In order to prove that $[x] = [y]$, we prove that each is a subset of the other.

  - Let $a \in [x]$, and so $a \mathcal{R} x$. Now since $x \mathcal{R} y$ and R is transitive, we know that $a \mathcal{R} y$. Consequently $a \in [y]$, and thus $[x] \subseteq [y]$.
  - Now let $b \in [y]$, so $b \mathcal{R} y$. Since R is symmetric, we know that $y \mathcal{R} x$, and because of transitivity, this implies that $b \mathcal{R} x$. Hence $b \in [x]$ and so $[y] \subseteq [x]$

  Thus $[x] = [y]$.

■

Remark 9.3.6 Representing classes — be kind. This result tells us that given any two related elements $x \mathcal{R} y$, their equivalence classes are the same. This can help us choose how we might represent an equivalence class to our reader; since $[x] = [y]$, we might as well choose to write it using which ever of x and y is simpler for the reader. That is, we'll write the class using its simplest **representative**.

In the above example we saw that $[0] = [4] = [8]$, $[1] = [5] = [9]$ and so forth, so when discussing these classes we should pick to represent them as

$$[0] \qquad [1] \qquad [2] \qquad \text{and} \qquad [3].$$

In general it is a good idea to be kind to your reader (and yourself) by representing your equivalence classes using simple members of those equivalence classes.

We can push the above theorem further to show that any two equivalence classes are disjoint or equal. Equivalence classes cannot overlap "just a little" — it is all or nothing. We'll call this result a corollary.

Corollary 9.3.7 *Let R be an equivalence class on A and let $x, y \in A$. Then either $[x] = [y]$ or $[x] \cap [y] = \varnothing$.*

Proof. Let R be an equivalence relation on A and let $x, y \in A$. Now form the set $B = [x] \cap [y]$. Either this set is empty or not.

- If $B = \varnothing$ then there is nothing left to prove.

- On the other hand, if B is non-empty, then there must be some element $b \in B$. Hence $b \in [x]$, so $b \mathcal{R} x$ and by symmetry of R we know $x \mathcal{R} b$. Now, since $b \in [y]$, we have $b \mathcal{R} y$. By transitivity of R, $x \mathcal{R} y$. The previous theorem then ensures that $[x] = [y]$ as required.

■

Before we go on, let us look at some more examples of equivalence classes.

Example 9.3.8 Let R be congruence modulo 5 on the set of integers. We know from Theorem Theorem 9.2.6 above, that this is an equivalence relation. Now, using Euclidean division Fact 3.0.3, and dividing by 5, we see that any integer n can be written as

$$n = 5q + r \qquad \text{where } r \in \{0, 1, 2, 3, 4\}$$

Hence $n - r = 5q$. So n must be congruent to one of $0, 1, 2, 3, 4$ modulo 5. Thus our equivalence classes are exactly

$$[0] \qquad [1] \qquad [2] \qquad [3] \qquad [4].$$

□

Example 9.3.9 Let S be the set of all students at University of British Columbia. We define a relation on S by

$$a \mathcal{R} b \qquad \iff \qquad a \text{ has the same age as } b.$$

Now this definition is still a little sloppy around the edges. To make it more precise:

- S is the set of all students enrolled on the 1st of October 2019.
- By "age" we mean the age in years rounded down to the nearest integer.

Show that this defines an equivalence relation and determine the equivalence classes.

Solution. We'll first show that this is reflexive, symmetric and transitive and then look at the equivalence classes.

- Reflexive — Let a be a student. Then since a has the same age as a, it follows that $a \mathcal{R} a$ as required.
- Symmetric — Let a, b be students so that a has the same age as b. This means that b has the same age as a and hence $b \mathcal{R} a$ as required.
- Transitive — Let a, b, c be students so that a has the same age as b and b has the same age as c. Then a has the same age as c and so $a \mathcal{R} c$. Hence the relation is transitive.

The equivalence classes are just sets of students with the same age (in years rounded to nearest integer). So there will be an equivalence class full of 18 year-olds, another of 19 year-olds, and so on. We should be a little careful, there may[108] be a very small number of 15 year-olds, 16 year-olds and on up to 75 year old students. □

Example 9.3.10 Let R be a relation defined on $\mathbb{R}^2$ by

$$(a, b) \mathcal{R} (c, d) \iff a + d = c + b$$

Show that is an equivalence relation and determine its equivalence classes.

Solution. We first show that it is an equivalence relation and then we'll look at its equivalence classes.

- Reflexive — Let $(a, b) \in \mathbb{R}^2$, then since $a + b = a + b$, it follows that $(a, b) \mathcal{R} (a, b)$. Hence the relation is reflexive.
- Symmetric — Let $(a, b), (c, d) \in \mathbb{R}^2$ and assume that $(a, b) \mathcal{R} (c, d)$. This implies that $a + d = c + b$. Since equality is symmetric, we know that $c + b = a + d$ and so $(c, d) \mathcal{R} (a, b)$.

[108] See here.

- Transitive — Let $(a,b),(c,d),(e,f) \in \mathbb{R}^2$ and assume that

$$(a,b) \mathcal{R} (c,d) \qquad \text{and} \qquad (c,d) \mathcal{R} (a,b).$$

Hence we know that

$$a+d = c+b \qquad \text{and } c+f = e+d.$$

Rearrange the second of these to give $c = e+d-f$. Substitute this into the first to get

$$\begin{aligned} a+d &= c+b \\ &= \underbrace{e+d-f}_{=c} + b \qquad \text{and so} \\ a+f &= e+b. \end{aligned}$$

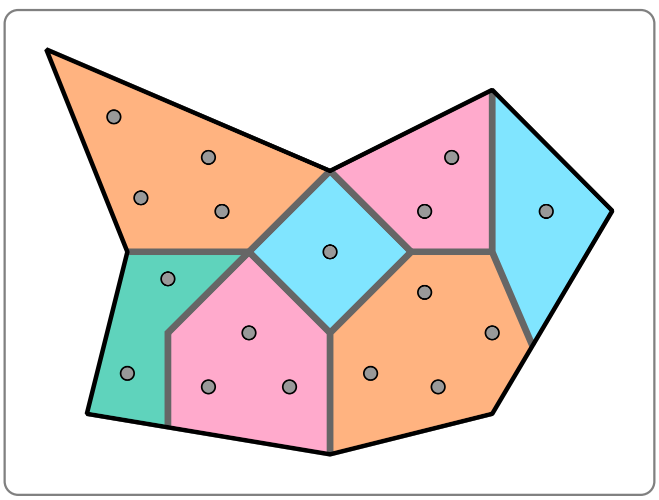
Hence $(a,b) \mathcal{R} (e,f)$ as required.

So what do the equivalence classes look like? Theorem Theorem 9.3.5 tells us that two elements are in the same equivalence class if and only if they satisfy the relation. So let $(a,b) \in \mathbb{R}^2$ and let us examine its equivalence class. The pair $(x,y) \in [(a,b)]$ if and only if $(a,b) \mathcal{R} (x,y)$. That is we must have $a+y = x+b$

$$y = x + (b-a).$$

Hence the equivalence class of (a,b) is the set of points lying on the line with gradient 1 that passes through (a,b). □

Our results above tell us that an equivalence relation cuts a set up into non-empty disjoint pieces, such as is depicted below.



Here we have coloured the different equivalence classes and you can think of the dots in the different subsets as being some elements in those equivalence classes. Notice there is no overlap between the subsets, and the entire set is covered by the subsets — no piece is missing. This separation[109] of a set into disjoint pieces is called a set partition.

Definition 9.3.11 A partition of a set A is a collection $\mathcal{P}$ of non-empty subsets of A, so that

- if $x \in A$ then there exists $X \in \mathcal{P}$ so that $x \in X$, and
- if $X, Y \in \mathcal{P}$, then either $X \cap Y = \varnothing$ or $X = Y$

The elements of $\mathcal{P}$ are then called blocks, parts or pieces of the partition.

An equivalent definition is that a partition of a set A is a collection $\mathcal{P}$ of non-empty subsets of A, so that

- $\bigcup_{X \in \mathcal{P}} X = A$, and
- if $X, Y \in \mathcal{P}$, then either $X \cap Y = \varnothing$ or $X = Y$

Where the union $\bigcup_{X \in \mathcal{P}} X$ is the union of all the sets in the partition $\mathcal{P}$. $\diamondsuit$

Consider our equivalence class examples above, and notice that in each case the equivalence classes form partitions of the underlying set. Rather than just "notice" let us do one (new) example more explicitly.

Given an equivalence relation we can prove that its equivalence classes form a set partition.

Theorem 9.3.12 *Let R be an equivalence relation on A. The set of equivalence classes of R forms a set partition of A.*

Proof. Let $\mathcal{P} = \{[x] \mid x \in A\}$ be the set of equivalence classes.

- Let $x \in A$. Then by Lemma Lemma 9.3.4 above we know that $x \in [x]$, and by definition $[x] \in \mathcal{P}$. Hence for any $x \in A, x \in X$ for some $X \in \mathcal{P}$.
- Let $X, Y \in \mathcal{P}$. Then by Corollary Corollary 9.3.7, we know that either $X = Y$ or $X \cap Y = \varnothing$.

Hence the set of equivalence classes forms a set partition. ■

So an equivalence relation gives equivalence classes that define a set partition. We can also go backwards. A set partition can be used to define equivalence classes that in turn define an equivalence relation. To be more precise, take a set partition $\mathcal{P}$ of a set A. For any two elements $x, y \in A$ we can define

$$x \mathrel{\mathcal{R}} y \iff x, y \text{ are elements of the same part of the partition } \mathcal{P}$$

It is not too hard to prove that this relation is an equivalence relation.

[109] Alternatively, we might say that such a *partitioning* of a set is called a set partition. However that sentence is a bit self-referential. At any rate, the term **set partition** is another on point naming by mathematicians.

Theorem 9.3.13 *Let $\mathcal{P}$ be a set partition on the set A, and define a relation R by*

$$x \mathcal{R} y \iff \big(x, y \in X \text{ for some } X \in \mathcal{P}\big)$$

That is $x \mathcal{R} y$ if and only if they belong to the same piece of the partition.

Then the relation R is an equivalence relation.

Proof. We need to show that R is reflexive, symmetric and transitive.

- Reflexive — Let $x \in A$. Since $\mathcal{P}$ is a set partition, we know that x is an element of some piece of the partition. Hence x is in the same piece of the partition as itself, and so $x \mathcal{R} x$ as required.
- Symmetric — Let $x \mathcal{R} y$, so we know that x, y lie in the same piece of the partition. Hence we must also have $y \mathcal{R} x$.
- Transitive — Let $x \mathcal{R} y$ and $y \mathcal{R} z$. Then there must be $X, Y \in \mathcal{P}$ so that $x, y \in X$ and $y, z \in Y$. Hence $X \cap Y \neq \varnothing$ (since it contains y). Since $\mathcal{P}$ is a partition, we know that $X \cap Y = \varnothing$ or $X = Y$. Hence $X = Y$ and so $x, z \in X$. Thus $x \mathcal{R} z$ as required.

■

9.4 Congruence revisited

One very important relation is congruence modulo n. It is not too hard to show that it is an equivalence relation, and its equivalence classes have some very useful properties. The reader should quickly revisit Section 5.3, Definition 5.3.1 and Theorem 5.3.3.

By Theorem Theorem 9.2.6, congruence modulo n is an equivalence relation and so has equivalence classes. For example, if we fix the modulus as 4, then we can write down the four equivalence classes of integers modulo 4:

$$[0] = \{\dots, -8, -4, 0, 4, 8, \dots\} \qquad [1] = \{\dots, -7, -3, 1, 5, 9, \dots\}$$
$$[2] = \{\dots, -6, -2, 2, 6, 10, \dots\} \qquad [3] = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

Notice that we are *representing* each equivalence class by the smallest non-negative integer in that class.

Warning 9.4.1 Modulo relation and operator. Many of you who have programmed will have encountered the modulo operator; it is usually denoted by the percentage sign, "%". This operator is more correctly called the "integer remainder operator". In particular, if (via Euclidean division) we know that $a = kn + r$ where $0 \leq r < n$, then

$$a\%n = r$$

When we represent the equivalence classes modulo n we typically[110] represent them by the smallest non-negative member of the equivalence class, which is the remainder when divided by n. This can lead to a confusion between the equivalence classes and the remainders.

So while equivalence classes modulo n are related to the effect of this integer remainder operator % — they are not the same. You should avoid thinking of "modulo n" as an operation that is done on integers.

One reason that this equivalence relation, congruence modulo m, is so important is that its equivalence classes interact very nicely with arithmetic giving rise to **modular arithmetic**. We saw this idea back in Theorem 5.3.3. Let us rewrite that result in terms of equivalence classes.

Theorem 9.4.2 Modular arithmetic redux. *Let $n \in \mathbb{N}$, and let $a, b, c, d \in \mathbb{Z}$ so that*

$$c \in [a] \qquad \textit{and} \qquad d \in [b],$$

where $[x]$ denotes the equivalence class of x under congruence modulo n. Then

$$c + d \in [a + b], \qquad c - d \in [a - b] \qquad \textit{and} \qquad c \cdot d \in [a \cdot b]$$

Proof. The proof of this statement is essentially identical to the proof of Theorem 5.3.3. ■

As an illustration of this result, consider the numbers 5 and 7. When we multiply them together we get 35. But now, think about these numbers modulo 4, and the equivalence classes they lie in:

$$5 \in [1] \qquad 7 \in [3] \qquad 35 \in [3]$$

The above theorem tells us that since $5 \equiv 1 \pmod 4$ and $7 \equiv 3 \pmod 4$, their product

$$\underbrace{35}_{5\times 7} \equiv \underbrace{3}_{3\times 1} \pmod 4$$

Notice that this will hold no matter which elements of [1] and [3] we multiply together, we will always get an element of [3]. This suggests (with a little bending of notation and avoiding any confusion with cartesian products):

$$[1] \cdot [3] = [3]$$

and similarly

$$[1] + [3] = [4] = [0].$$

This can be made to work more generally, but first we should define things carefully and then prove things carefully.

Definition 9.4.3 Let $n \in \mathbb{N}$, and let $a, b \in \mathbb{Z}$. Then we define the following arithmetic operations on the equivalence classes modulo n:

$$[a] + [b] = [a + b]$$

[110] This author has gotten into difficulties in a piece of research when their coauthor (for very valid reasons) instead chose to represent equivalence classes by the integer closest to zero.

$$[a] - [b] = [a - b]$$
$$[a] \cdot [b] = [a \cdot b]$$

where we have used "·" to denote multiplication to avoid confusion with the cartesian product of sets. ♢

There is a small problem with this definition — we need to make sure that it makes sense and is **well defined** and that our choice of representative elements a, b does not change the results $[a+b], [a-b], [a \cdot b]$. For example, in our modulo 4 example, we know that

$$[1] = [5] = [-3] \qquad \text{and } [3] = [7] = [-1]$$

so we need to be sure that

$$\underbrace{[1] + [3]}_{[4]} = \underbrace{[5] + [7]}_{[12]} = \underbrace{[-3] + [-1]}_{[-4]} = [0]$$

Thankfully, this is a simple corollary of Theorem 5.3.3 (or Theorem 9.4.2).

Corollary 9.4.4 Modular arithmetic. *Let $n \in \mathbb{N}$, and let $a, b \in \mathbb{Z}$. Then the sets*

$$[a+b] \qquad [a-b] \qquad [a \cdot b]$$

are well defined and do not depend on the choice of representative elements.

Proof. Let a, b, n be as in the statement of the result, and let $c \in [a], d \in [b]$.

By definition $[c] + [d] = [c + d]$. It suffices to show that $[c + d] = [a + b]$. By Theorem Theorem 5.3.3, we know that $c + d \in [a + b]$ and so by Corollary Corollary 9.3.7 $[c + d] = [a + b]$ as required.

The same argument shows that $[c] - [d] = [c - d] = [a - b]$, and that $[c] \cdot [d] = [c \times d] = [a \cdot b]$. ■

This result turns out to be very useful. It tells us that

$$[7] \cdot [9] = [3] \cdot [1] = [3 \cdot 1] = [3].$$

Of course, that one is easy enough to check in our head:

$$7 \times 9 = 63 \qquad \text{and} \qquad 63 \equiv 3 \pmod 4.$$

But (minutely) less easy:

$$[19] \cdot [11] = [3] \cdot [3] = [9] = [1]$$

(which is true since $19 \times 11 = 209 = 208 + 1 = 52 \times 4 + 1$).

Now, just before we switch gears to modulo 10, we should make some notation to emphasise the modulus so that we don't mix equivalence classes from different equivalence relations[111]. We can rewrite the above equivalence classes with the modulus as a subscript:

$$[7]_4 \cdot [9]_4 = [3]_4$$

[111] In some situations it is very helpful to mix results from different moduli, but one does it very deliberately, and not by accident. For a good example of carefully mixing moduli, see Example 9.4.6 below.

This makes it much easier to talk about different modulii without confusing the reader. Of course, if the modulus is clear by context, then we don't need the subscript.

Another, more complicated one, For example, let $a = 17321289, b = 23492871$ and we compute their product as

$$17321289 \times 23492871 = 406926808030718.$$

If you look at this for amoment, you realise that the product is wrong — the last number definitely should not be an "8". We can show this by computing the product modulo 10:

$$[17321289]_{10} \cdot [23492871]_{10} = [9]_{10} \cdot [1]_{10} = [9]_{10}.$$

This is a very simple example of using modular arithmetic as a way of error-checking. Some simple techniques based on modular arithmetic are often used in credit-card numbers and similar.

Example 9.4.5 Checking long numbers — Luhn algorithm. The author is going to assume that everyone has had to either write down a telephone number or a credit card number and messed it up. Very common mistakes are

- Single digit error: $1 \mapsto 2$
- Transposition: $12 \mapsto 21$
- Phonetic errors: $60 \mapsto 16$

Everyone has dialed a wrong number[112], but thankfully, credit card numbers have some built-in checks that prevent simple errors like the above. In particular, a credit card has a "check digit".

Since people rarely mess transcribing up the first or last digit of a long number, one can exploit the last digit to check up on the others. So say you have a long number (like a credit card or phone number), that you want to protect against simple errors, then you should append a single special digit to the end of that number. For example, say we have the first 8 digits of a number "31415926" and we want to make sure that it can be checked when copied down by someone else. A really simple check is to sum up the digits modulo ten:

$$3 + 1 + 4 + 1 + 5 + 9 + 2 + 6 = 31 \equiv 1 \pmod 1)0$$

So we can append "1" to the end of the number to get "31415926***1***".

Now when we read it out to a friend over the phone, they copy down "313159261". They can then compute the check number:

$$3 + 1 + 3 + 1 + 5 + 9 + 2 + 6 = 30 \equiv 0 \pmod 1)0$$

Since $0 \neq 1$ they know there is an error. This will proof against a single-digit substitution error, but it will not be safe against a transposition. If they wrote down "314***51***9261" then the check gives

$$3 + 1 + 4 + 5 + 1 + 9 + 2 + 6 = 31 \equiv 1 \pmod 1)0$$

So the error goes undetected.

However there is a better way. The Luhn algorithm[113] is used in many applications including in credit cards.

- Start with our number $3, 1, 4, 1, 5, 9, 2, 6$.
- Double every second digit (starting from the rightmost): $3, 2, 4, 2, 5, 18, 2, 12$. Notice that our list of digits becomes longer
- Now sum *all*:

$$3 + 2 + 4 + 2 + 5 + (1 + 8) + 2 + (1 + 2) = 30$$

- Multiply the result by 9 and compute the result modulo ten:

$$30 \times 9 = 270 \equiv 0 \pmod 1)0$$

- Append the result as the check digit: "31415926***0***"

Let us try this against the two transcription errors above:

- "31***3***159260" becomes "3,2,3,2,5,18,2,12" which gives

$$3 + 2 + 3 + 3 + 2 + 5 + (1 + 8) + 2 + (1 + 2) = 32.$$

  Multiply by 9 to get $32 \times 9 = 288$ giving check-digit "8". Error detected!
- "314***51***9261" becomes "3,2,4,10,1,18,2,12" which gives

$$3 + 2 + 4 + (1 + 0) + 1 + (1 + 8) + 2 + (1 + 2) = 25.$$

  Multiply by 9 to get 225 giving check-digit "5". Error detected!

This is not too hard to do by hand, but it is very easy for a computer.

This is not perfect, some errors will go undetected. The interested reader should search-engine their way to more information. □

Example 9.4.6 Chinese remainder theorem. You can push this idea further, and instead of doing arithmetic with very large numbers, you can do the same arithmetic modulo several different primes and then reconstruct the big-number result using the results modulo each prime. The piece of mathematics that tells you how to reconstruct the result is called the Chinese Remainder Theorem. It was first stated in the 3rd century AD by the Chinese mathematician Sunzi, but the first real method for this reconstruction is due to Aryabhata (an Indian mathematician of the 6th century AD). It seems to have been rediscovered a few times and seems to have entered European mathematics via Fibonacci in the

[112] I think? Well, the author definitely has

[113] Named for the computer scientist Hans Peter Luhn (1896–1964).

12th century. It's not quite clear when it got its name, but perhaps sometime between 1850 and 1930?

We won't do the Chinese remainder theorem in this course (its a good one to do in a number theory course), but we'll do a few more applications of congruences. □

Example 9.4.7 No integer solutions. Show that the equation

$$x^2 - 4y^2 = 3$$

has no integer solutions.

Scratchwork. A sneaky way to look at this is to realise that if there is an integer solution, then if you look at that solution modulo, say 7, then it will still be a solution. ie

$$(x^2 - 4y^2) \pmod 7 = 3 \pmod 7.$$

Hence if we can prove that the equation has no solution modulo (again say) 7, then it cannot have a solution over the integers (by taking the contrapositive). Notice that the converse is very false — just because we can find a solution modulo 7, does not mean there is an integer solution.

Now, because one of the coefficients in the equation is a 4, it simplifies considerably modulo 4. In particular

$$4y^2 \pmod 4 = 0$$

no matter what y we put in. So modulo 4 the equation simplifies to

$$(x^2 - 4y^2) \pmod 4 = x^2 \pmod 4 = 3 \pmod 4$$

So now we look at squares modulo 4.

$$\begin{array}{lll} 0^2 \pmod 4 = 0 & 1^2 \pmod 4 = 1 & 2^2 \pmod 4 = 0 \\ 3^2 \pmod 4 = 1 & 4^2 \pmod 4 = 0 & 5^2 \pmod 4 = 1 \end{array}$$

So — it looks like squares modulo 4 are either 0 or 1, depending on their parity. If this is true then we are done — there is no solution modulo 4, so there cannot be an integer solution.

Solution.

Proof. The equation either has a solution $x, y \in \mathbb{Z}$ or it does not. If the equation does have a solution, then x is either even or odd.

- If x is even then $x = 2k$ for some $k \in \mathbb{Z}$, and so

  $$x^2 - 4y^2 = 4(k^2 - y^2)$$

  and so $x^2 - 4y^2 \equiv 0 \pmod 4$.

- On the other hand, if x is odd, then $x = 2k + 1$ for some $k \in \mathbb{Z}$ and so

$$x^2 - 4y^2 = 4k^2 + 4k + 1 - 4y^2 = 4(k^2 + 4k - y^2) + 1$$

  and so $x^2 - 4y^2 \equiv 1 \pmod 4$.

In either case $x^2 - 4y^2$ is not congruent to 3 modulo 4. Hence there cannot be a solution. ■

□

Now, noticeably absent from Theorem Theorem 5.3.3 above is any discussion of division. Consider the equation $x = \frac{13}{2}$; here we are really solving the equation $2x = 13$. Consider this equation modulo 4 — find any x so that

$$[2]_4 \cdot [x]_4 = [1]_4$$

(since $[13]_4 = [1]_4$). Similarly modulo 5 we get:

$$[2]_5 \cdot [x]_5 = [1]_5.$$

We can try to solve these equations by brute-force by just writing out the multiplication tables modulo 4 and 5:

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Now - we see that modulo 5 we have a solution since:

$$[2]_5 \cdot [3]_5 = [1]_5$$

but modulo 4 there is no solution since

$$[2]_4 \cdot [x]_4 = [0]_4 \text{ or } [2]_4.$$

The existence of solutions to the equation

$$[a]_n \cdot [x]_n = [1]_n$$

depends on the divisors of a and n.

Lemma 9.4.8 *Let $a \in \mathbb{Z}, n \in \mathbb{N}$. If $d > 1$ divides both a, n then the equation*

$$[a]_n \cdot [x]_n = [1]_n$$

does not have a solution.

Proof. Say that the equation

$$[a]_n \cdot [x]_n = [1]_n$$

has a solution $x = b$. Then for some $k \in \mathbb{Z}$

$$ab + kn = 1.$$

Now if, $d > 1$ divides both a, n the left-hand side is divisible by d. However this does not make sense because the right-hand side is only divisible by ± 1. Hence no such solution can exist. ■

Remark 9.4.9 Bezout and Euclid. The converse of this lemma states that if a, n have no common divisors, then the equation has a solution. To prove this we need to show that if a, n have no common divisors, then we can find b, k so that

$$ab + kn = 1.$$

This is (essentially) Bezout's identity. The values b, k can be computed using the extended Euclidean algorithm. We will discuss all of this in the optional section below.

Example 9.4.10 Pseudo random numbers. Consider the following sequence of numbers

$$1, 10, 7, 8, 4, 9, 0, 3, 2, \ldots$$

The numbers bounce around and look fairly ``random". However, they are not actually random at all; they satisfy the simple relation

$$x_{k+1} \equiv (7x_k + 3) \pmod{11},$$

or, using the % operator (ie integer remainder operator)

$$x_{k+1} = (7x_k + 3)\%11.$$

This is an example of a linear congruent generator; the next term in the sequence is determined by a simple linear equation involving a congruence:

$$x_{k+1} = ax_k + c \pmod{n}$$

If one chooses a and c carefully, then the resulting sequence of numbers will look quite random. However, since the numbers are not actually random, they are usually called **pseudo random** numbers.

Many computer algorithms for generating pseudo random numbers are based on this idea. Of course, one does need to be quite careful and make sure that your pseudo-random numbers are actually fairly random. For example, if we choose $a = 7, c = 5, n = 11$ in the above, then we get the sequence

$$1, 1, 1, 1, \ldots$$

since $7 \cdot 1 + 5 = 12 \equiv 1 \pmod{11}$. Not very random at all.

There is a lot of interesting mathematics to be found in generating pseudo-random numbers and testing their randomness; we recommend that the interested reader take a trip to their favourite search engine. □

9.5 Greatest divisors, Bézout and the Euclidean algorithm

In our (brief) discussion above of division in modular arithmetic we came across the problem of computing **common divisors**. You probably first came across the question of computing common divisors when trying to simplify fractions:

$$\frac{6}{15} = \frac{3 \times 2}{3 \times 5} = \frac{2}{5}$$

We can simplify this fraction because 3 is a divisor of both 6 and 15. In this context we typically want to find the **greatest common divisor** of the numerator and denominator and then factor that out.

Definition 9.5.1 Let $a, b \in \mathbb{Z}$ be non-zero. Then

- The **greatest common divisor** of a, b, denoted $\gcd(a, b)$, is the largest positive integer that divides both a and b.
- If $\gcd(a, b) = 1$ then we say that a and b are **coprime**, or **relatively prime**.
- The **least common multiple** of a, b, denoted $\operatorname{lcm}(a, b)$, is the smallest positive integer that is divisible by both a and b.
- By symmetry, $\gcd(a, b) = \gcd(b, a)$ and $\operatorname{lcm}(a, b) = \operatorname{lcm}(b, a)$.
- Finally, "greatest common divisor" and "least common multiple" are frequently abbreviated to **gcd** and **lcm**.

♢

Remark 9.5.2 What about zero? Notice that in the above defintion if a, b are non-zero then the $\gcd(a, b)$ and $\text{lcm}(a, b)$ are well-defined. We should note that since $0 \times a = 0$, the definition extends to

$$\gcd(a, 0) = a.$$

When both a, b are zero then there is no greatest common divisor since $0 \times n = 0$ for any n. That being said, in some contexts[114] $\gcd(0, 0)$ is *defined* to be zero.

For non-zero a, the $\text{lcm}(a, 0)$ is not well defined since we cannot divide by zero. However, in some contexts $\text{lcm}(a, 0)$ is *defined* to be zero since the only common multiple of a and 0 is zero.

With all of that said, we will only consider $\gcd(a, b)$ when at least one of a, b are non-zero, and only consider $\text{lcm}(a, b)$ when a, b are both non-zero.

Remark 9.5.3 Notice that by definition if c divides both a, b then $c \leq \gcd(a, b)$:

$$(c \mid a) \wedge (c \mid b) \implies c \leq \gcd(a, b).$$

Similarly, if a and b divide m then $\text{lcm}(a, b) \leq m$:

$$(a \mid m) \wedge (b \mid m) \implies m \geq \text{lcm}(a, b).$$

When a, b are small numbers it is not too hard to compute the gcd by hand, typically by thinking about factors. However, there is a much better (and faster) way called Euclid's algorithm. It is based on the following observation.

Lemma 9.5.4 *Let $a, b \in \mathbb{N}$, with $a \geq b$*

$$\begin{aligned} \gcd(a, 0) &= a \\ \gcd(a, b) &= \gcd(b, a - b). \end{aligned}$$

Finally, if $a = qb + r$ for some $q, r \in \mathbb{Z}$, then

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

Remark 9.5.5 Antisymmetry helping equality. To prove the remaining two points we take advantage of the fact that the relation "$\leq$" is antisymmetric. That is

$$(x \leq y) \wedge (y \leq x) \implies x = y$$

This means that we can break down the proof of an equality into proofs of two (potentially easier) inequalities. We have already done this proving set equalities using

$$(A \subseteq B) \wedge (B \subseteq A) \implies A = B.$$

Proof of Lemma 9.5.4. We prove each point in turn.

- Since $a = a \cdot 1$ and $0 = a \cdot 0$, it follows that a is a divisor of both $a, 0$. No number larger than a can divide a, so a must be the greatest common divisor.

[114] Many computer algebra systems define $\gcd(0, 0) = 0$.

As noted above, it is sufficient to show that (say) $\gcd(a,b) \geq \gcd(b,a-b)$ and $\gcd(a,b) \leq \gcd(b,a-b)$ in order to prove that $\gcd(a,b) = \gcd(b,a-b)$.

- We start by showing that $\gcd(a,b) \leq \gcd(b,a-b)$. To do this, we prove that $\gcd(a,b)$ divides both b and $(a-b)$, and hence is a common divisor of b and $(a-b)$. Since it is a common divisor, it cannot be bigger than the largest common divisor (by definition).

  Let $d = \gcd(a,b)$. Since $d \mid a$ and $d \mid b$, we can write $a = kd, b = \ell d$ for some $k, \ell \in \mathbb{Z}$. Thus $b - a = d(k-\ell)$ and so it follows that $d \mid (a-b)$. Hence d is a divisor of b and $a-b$, and so it must be no bigger than the gcd of $b, a-b$.
  $$d \leq \gcd(b,a-b).$$

  Now let us reuse this argument, but now starting from $c = \gcd(b,a-b)$. Since $c \mid b$ and $c \mid (b-a)$, there are $k, \ell \in \mathbb{Z}$ so that $b = ck, (b-a) = c\ell$. It follows that $a = b - (b-a) = c(k-\ell)$ and thus $c \mid a$. And because $c \mid a$ and $c \mid b$ we have
  $$c \leq \gcd(a,b)$$

  But now we have both
  $$\gcd(a,b) \leq \gcd(b,a-b) \qquad \text{and} \qquad \gcd(b,a-b) \leq \gcd(a,b)$$
  and hence $\gcd(a,b) = \gcd(b,a-b)$.

- That $\gcd(a,b) = \gcd(b,r)$ follows by a nearly identical argument. If $d \mid a$ and $d \mid b$, then
  $$d \mid (a-qb) = r$$
  Hence d divides both b and r, and hence
  $$d \leq \gcd(b,r).$$
  And since $c = \gcd(b,r)$ divides both b and r, it must also satisfy
  $$d \mid (qb+r) = a$$
  Thus c divides both b and a, and so
  $$c \leq \gcd(a,b)$$
  Since $\gcd(a,b) \leq \gcd(b,r)$ and $\gcd(b,r) \leq \gcd(a,b)$, we must have that they are equal.

■

Now why is this useful? Well, say $a > b$, then we can compute

$$\gcd(a,b) = \gcd(b,a-b)$$

and now the number $a - b$ is smaller than a. If we keep repeating this, then the numbers in our gcd keep getting smaller and smaller until we have to compute a really simple gcd. This is even faster if we write $a = qb + r$, because then

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

For example

$$\begin{aligned} \gcd(268, 120) &= \gcd(120, 28) & \text{since } 28 = 268 - 2 \times 120 \\ &= \gcd(28, 8) & \text{since } 8 = 120 - 4 \times 28 \\ &= \gcd(8, 4) & \text{since } 4 = 28 - 3 \times 8 \\ &= \gcd(4, 0) & \text{since } 0 = 8 - 2 \times 4 \\ &= 4 \end{aligned}$$

This method of computing the gcd is known as the Euclidean algorithm.

Algorithm 9.5.6 The Euclidean algorithm. *Let $a, b \in \mathbb{Z}$ with $|a| \geq |b|$ and at least one of a, b non-zero. Then $\gcd(a, b)$ can be computed using the following steps:*

1. *If $b = 0$ then the gcd is a, otherwise go on to (2)*
2. *Compute the remainder of a divided by b, that is $a = qb + r$ with $0 \leq r < |b|$.*
3. *Go back to (1) with (a, b) replaced by (b, r).*

Proof. Assume $a, b \in \mathbb{Z}$ as stated.

- If $b = 0$ then we are done since $\gcd(a, 0) = a$ by Lemma Lemma 9.5.4.
- So now we can assume that $b \neq 0$. By Fact 3.0.3 we know that

  $$a = qb + r \qquad \text{with } 0 \leq r < |b|.$$

  By Lemma Lemma 9.5.4 we know that $\gcd(a, b) = \gcd(a, r)$. Hence computing $\gcd(b, r)$ is the same as computing $\gcd(a, b)$.
- Since $0 < r < |b|$ it follows that the value of r will be *strictly* smaller in each iteration. Further, since r is an integer, it follows that r will become zero in a finite number of iterations.

Hence the algorithm described will terminate in a finite number of steps and give the gcd. ■

Let's do another one:

$$\begin{aligned} \gcd(869, 442) &= \gcd(442, 427) & \text{since } 869 = 442 + 427 \\ &= \gcd(427, 15) & \text{since } 442 = 427 + 15 \\ &= \gcd(15, 7) & \text{since } 427 = 15 \cdot 28 + 7 \\ &= \gcd(7, 1) & \text{since } 15 = 2 \cdot 7 + 1 \end{aligned}$$

$$
\begin{aligned}
&= \gcd(1,0) && \text{since } 7 = 7 \cdot 1 + 0\\
&= 1
\end{aligned}
$$

Now notice that at each stage we take linear combinations of the arguments of the gcd to make new arguments.

$$
\begin{aligned}
427 &= 869 - 442\\
15 &= 442 - 427\\
7 &= 427 - 28 \cdot 15\\
1 &= 15 - 2 \cdot 7
\end{aligned}
$$

If we substitute these equations into each other, then we can write our result as some linear combination of our starting arguments. Let $a = 869, b = 442$, then:

$$
\begin{aligned}
427 &= 869 - 442 = a - b\\
15 &= 442 - 427 = b - \underbrace{(a-b)}_{=427} = 2b - a\\
7 &= 427 - 28 \cdot 15 = \underbrace{(a-b)}_{=427} - 28\underbrace{(2b-a)}_{=15} = 29a - 57b\\
1 &= 15 - 2 \cdot 7 = \underbrace{(2b-a)}_{=15} - 2\underbrace{(29a-75b)}_{=7} = 116b - 59a
\end{aligned}
$$

That is

$$\gcd(869, 442) = 1 = 116 \cdot 442 - 59 \cdot 869.$$

That one can write the gcd in this way is quite general and is known as Bézout's Lemma.

Lemma 9.5.7 Bézout's Lemma. *Let $a, b \in \mathbb{Z}$ so that at least one of a, b is non-zero. Then there exist $x, y \in \mathbb{Z}$ so that*

$$\gcd(a, b) = ax + by.$$

Proof. Essentially one follows the Euclidean algorithm backwards just as we have in the example above. However one can also prove this using an induction-like argument which is nearly the same thing.

Consider an execution of the Euclidean algorithm starting from a, b. It builds a finite sequence of equations of the form:

$$
\begin{aligned}
a &= q_1 b + r_1\\
b &= q_2 r_1 + r_2\\
r_1 &= q_3 r_2 + r_3\\
r_2 &= q_4 r_3 + r_4\\
\vdots &= \vdots\\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}
$$

where the gcd will be r_n. We now prove that for each i, there exist $x_i, y_i \in \mathbb{Z}$ so that $r_i = ax_i + by_i$, using an induction-style proof.

Notice that when $i = 1$ we have

$$r_1 = a - q_1 b$$

so we have $x_1 = 1, y_1 = -q_1$. Similarly, when $i = 2$ we have

$$r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = (1 + q_1 q_2)b - q_2 a$$

Hence $x_2 = -q_2, y_2 = 1 + q_1 q_2$.

Now for general i we have that

$$r_{i+1} = r_{i-1} - q_{i+1} r_i$$

So if $r_i = x_i a + y_i b$ and $r_{i-1} = x_{i-1}a + y_{i-1}b$, then

$$r_{i+1} = (x_{i-1}a + y_{i-1}b) - q_{i+1}(x_i a + y_i b) = a(x_{i-1} - q_{i+1}x_i) + b(y_{i-1} - q_{i+1}y_i).$$

Hence

$$x_{i+1} = x_{i-1} - q_{i+1}x_i \qquad y_{i+1} = y_{i-1} - q_{i+1}y_i.$$

So using this recurrence and our starting values of $(x_1, y_1), (x_2, y_2)$ we can find integer $(x_3, y_3), (x_4, y_4)$ and so on up to (x_n, y_n). And hence we can write $gcd(a, b) = x_n a + y_n b$ with $x_n, y_n \in \mathbb{Z}$.

Notice that if we set

$$(x_0, y_0) = (0, 1) \qquad \text{and } (y_0, y_1) = (1, -q_1)$$

then our recurrence gives us

$$x_2 = 0 - q_2 \cdot 1 = -q_2 \qquad y_2 = 1 - q_2 \cdot (-q_1) = 1 + q_1 q_2$$

as required. ■

In the proof of the above lemma we give a construction of a recurrence that gives us the needed x, y to express $\gcd(a, b) = ax + by$. By combining that recurrence and the Euclidean algorithm we get the **extended Euclidean algorithm**.

Algorithm 9.5.8 The extended Euclidean algorithm. *Let $a, b \in \mathbb{Z}$ with $|a| \geq |b|$ and at least one of a, b non-zero. Then $\gcd(a, b)$ can be computed using the following steps:*

1. *If $b = 0$ then the gcd is a else go on to (2)*
2. *Compute the remainder of a divided by b, that is $a = qb + r$ with $0 \leq r < |b|$.*
3. *Go back to (1) with (a, b) replaced by (b, r).*

In the process of computing this we obtain a sequence of n quotients q_i and *remainders r_i. Define sequences x_i, y_i by the inital values*

$$x_0 = 0, x_1 = 1 \qquad \textit{and} \qquad y_0 = 0, y_1 = -q_1$$

and then for $k \geq 1$:

$$x_{k+1} = x_{k-1} - q_{k+1}x_k$$
$$y_{k+1} = y_{k-1} - q_{k+1}y_k$$

Then

$$\gcd(a, b) = ax_n + by_n.$$

Proof. This follows quite directly from Proof 9.5.7.1 of Bézout's lemma above. ■

Returning to our example of $\gcd(869, 442)$ above, we had

$$q_1 = 1 \qquad q_2 = 1 \qquad q_3 = 28 \qquad q_4 = 2$$

which gives $x_0 = 0, x_1 = 1$ and $y_0 = 1, y_1 = -1$

$$x_2 = 0 - 1 = -1 \qquad x_3 = 1 - 28 \cdot (-1) = 29 \qquad x_4 = -1 - 2 \cdot 29 = -59$$
$$y_2 = 1 - 1 \cdot (-1) = 2 \qquad y_3 = -1 - 28 \cdot 2 = -57 \qquad y_4 = 2 - 2 \cdot (-57) = 116$$

and we can verify that

$$-59 \cdot 869 + 116 \cdot 442 = -51271 + 51272 = 1$$

as required.

Bézout's turns out to be a useful result because it allows one to express $\gcd(a, b)$ as a simple equation in a, b which is then easier to manipulate. As an example of its utility, consider the following lemma about division which we attribute to Euclid. This feels like it should be "obvious", but it turns out to be not so easy to prove without invoking unique prime-factorisations of integers — the Fundamental Theorem of Arithmetic. Unfortunately that result is harder to prove than this one. We'll get around to proving the Fundamental Theorem of Arithmetic, but not just yet.

Lemma 9.5.9 Euclid's lemma. *Let $a, b, p \in \mathbb{Z}$ so that p is prime, and $p \mid ab$. If $p \nmid b$ then $p \mid a$.*

More generally let $a, b, d \in \mathbb{Z}$ so that $d \mid ab$. If $\gcd(d, b) = 1$ then $d \mid a$.

Via Bézout. Notice that the second statement implies the first statement, since by definition the only divisors of p are $1, p$, and so if $p \nmid b$ then $\gcd(p, b) = 1$.

By assumption, we know that $d \mid ab$, so we can write $ab = dk$ for some $k \in \mathbb{Z}$. Bézout's lemma allows us to write an equation linking b, d. In particular, it guarantees that there are $x, y \in \mathbb{Z}$ so that

$$1 = dx + by$$

Multiply this expression by a to get

$$a = adx + aby$$

But since $ab = dk$, we have

$$a = d(ax + ky)$$

and so $d \mid a$ as required. ■

Implicitly Bézout. Here is an alternative proof — it does not use Bézout's lemma explicitly, but some of the ideas are similar. Let $p \mid ab$ and assume that $p \nmid b$. Then form the set

$$S = \{x \in \mathbb{N} \mid p \mid xa\}$$

We know that S is non-empty since $b \in S$. Further, we also know that $S \subseteq \mathbb{N}$ and so obeys the well-ordering principle that we saw back in Chapter Chapter 7 on induction. It implies that S must have a smallest element, z. If we can show that $z = 1$ we are done because we have shown that $p \mid a$. We first that z divides all elements in S.

Let $x \in S$, then by Euclidean division we know that

$$x = qz + r \qquad \text{with } 0 \leq r < z$$

But we know that $p \mid xa$ and $xa = aqz + ra$. Rewrite this as

$$ra = xa - azq$$

Now by definition of S, we know that $p \mid xa$ and $p \mid az$, so $p \mid ra$. If $r \neq 0$ we have a problem because now $p \mid ra$ and $r < z$ which contradicts z being minimal. Hence we must have $r = 0$ and so $z \mid x$.

How do we now use this to show that $z = 1$? Since $p \mid pa$, we know that $p \in S$. Similarly, since $p \mid ba$, we know that $b \in S$. Hence $z \mid p$ and $z \mid b$. The only divisors of p are 1 and p and since $p \nmid b$, we must have $z = 1$. So finally, we know that $p \mid a$ as required. ■

Remark 9.5.10 Euclid without Bézout. Since Euclid lived around 300BC in ancient Greece and Egypt, and Bézout lived in 18th century France, it is pretty clear that there must be a way to prove the above without using Bézout's lemma. The interested reader should look at this excellent discussion of Euclid's proof[115] by David Pengelley and Fred Richman, and other good articles here[116] and here[117].

Closer to Euclid. The proof we give here is closer to Euclid's original proof. The key to that proof is the fact that if we have a fraction $\frac{a}{b}$ and then we find the smallest fraction equivalent to that, call if $\frac{x}{y}$ (ie where x is as small as possible), then there must be some n so that $a = nx$ and $b = ny$. Now this feels quite obvious. Obvious until you have to prove it.

[115] `web.nmsu.edu/~davidp/euclid.pdf`
[116] `web.nmsu.edu/~davidp/fractions-monthly-final.pdf`
[117] `people.math.harvard.edu/~mazur/preprints/Eva.pdf`

We follow the clever argument given in this excellent article[a] by Barry Mazur. Since the fractions $\frac{a}{b}$ and $\frac{x}{y}$ are equal, we know that

$$ay = bx.$$

If $a = x$ then $n = 1$ and we are done. So choose n to be the largest integer so that $a > nx$. Indeed we must have $a - nx \geq x$ (otherwise we would pick n to be larger). And since $x = \frac{y}{b}a$

$$nx = \frac{ny}{b}a$$

and so we must also have that $ny > b$.

Now consider the fraction $\dfrac{a-nx}{b-ny}$. One can quickly verify by cross-multiplication that

$$\frac{a-nx}{b-ny} = \frac{x}{y}.$$

So we have a new fraction that is also equal to $\frac{a}{b}$ and xy. But now, since $\frac{x}{y}$ was minimal, we must have $a - nx \geq x$, and at the same time, we choose n so that $a - nx \leq x$. Thus we must have $a - nx = x$. In other words

$$a = x(n+1).$$

and so a is a multiple of x. Substituting this back into $ay = bx$ shows that

$$b = y(n+1)$$

also.

This result implies that if we have

$$\frac{a}{b} = \frac{c}{d} = r$$

then there is a unique smallest fraction $\frac{x}{y} = r$ so that

$$\begin{aligned} a &= kx & b &= ky \\ c &= nx & d &= ny \end{aligned}$$

for some integers k, n. That is, the two fractions $\frac{a}{b}, \frac{c}{d}$ reduce to the same[b] fraction $\frac{x}{y}$.

Now let us go back and use this to prove that if $p \mid ab$ and $p \nmid b$ then $p \mid a$. Since $p \mid ab$, we know that $ab = pc$. Hence we have

$$\frac{a}{p} = \frac{c}{b}.$$

From the above, we know that there exist k, n, x, y so that

$$\begin{aligned} a &= kx & c &= nx \\ p &= ky & b &= ny \end{aligned}$$

But we know that p is prime, so either $(k,y)=(p,1)$ or $(k,y)=(1,p)$. The first case implies that $p \mid a$, while the second implies that $p \mid b$. Since $p \nmid b$ by assumption, we know that $p \mid a$. And we are done. ■

[a] people.math.harvard.edu/~mazur/preprints/Eva.pdf

[b] This actually turns out to be a subtle point which is false in other contexts. In particular one can come up with perfectly well behaved sets of numbers, such as $\mathbb{Z}[\sqrt{-5}] = \left\{a+b\sqrt{-5} \mid a,b\in\mathbb{Z}\right\}$ where this result is no longer true. The interested reader should search-engine their way to discussions of "unique factorisation domains" and non-examples.

Here is another example of how Bézout's lemma can be very useful to prove a very useful[118] result linking the gcd and lcm.

Lemma 9.5.11 *The gcd and lcm satisfy the equation*

$$\gcd(a,b)\cdot \operatorname{lcm}(a,b) = |a\cdot b|.$$

Proof. Let $d=\gcd(a,b)$ and let $L=\frac{|ab|}{d}$. We need to show that both

- L is a common multiple of a,b, and
- any other common multiple of a,b is at least as large as L.

We know that, by definition, $d \mid a$ and $d \mid b$. Hence

$$a = dk \qquad \text{and } b = dn$$

which gives $|ab| = |d^2kn|$ and so

$$L = \frac{|ab|}{d} = |dkn| = |an| = |bk|.$$

Thus $a \mid L$ and $b \mid L$ as required.

Let M be a common multiple of a,b. It suffices to show that $L \mid M$ since this means that $|L| \le |M|$. Since M is a common multiple of a,b we know that

$$M = ap = bq$$

for some integer p,q. Now since $dL = ab$, it is easier to compare dM and dL, and we do that via Bézout's lemma. Recall from Bézout's lemma that there are $x,y\in\mathbb{Z}$ so that:

$$d = ax + by$$

This means that

$$\begin{aligned} dM &= aMx + bMy \\ &= a(\underbrace{bq}_{=M})x + b(\underbrace{ap}_{=M})y \\ &= ab(qx+py) \end{aligned}$$

and thus $dL \mid dM$. Hence $L \mid M$ and so $|L| \le |M|$. This means that L is the least common multiple of a,b. ■

[118] and obvious until you have to prove it!

9.6 Uniqueness of prime factorisation

Prime numbers follow very quickly when we learn about multiplication. Soon after that[119] we realise that every positive integer can be written as a product of primes.

$$30 = 5 \times 3 \times 2$$

While we can shuffle those numbers around

$$30 = 2 \times 5 \times 3 = 3 \times 2 \times 5 = \text{ etc}$$

those products will still contain the same number of each prime. Hence we can write it *uniquely* by putting the primes in order, smallest to largest:

$$30 = 2 \times 3 \times 5.$$

This **unique factorisation** of integers[120] into primes is called the "Fundamental theorem of arithmetic", and seems so obvious to us that it is hard to imagine that one even has to prove it! However, while it feels obvious, it needs a proof.

The history of the theorem is not quite as direct as one might think[121]. The result follows quite directly from the results of Euclid we discussed in the previous section, but does not actually appear explicitly in Euclid's Elements[122]. The 13th Century Persian mathematician al-Farisi[123] proved that numbers can be decomposed as products of primes, but not the uniqueness of that decomposition. Prestet, Euler and Lagrange[124] all seem to have been very close to writing it down, but it was actually Gauss[125] who first wrote it down explicitly in 1801.

Theorem 9.6.1 The fundamental theorem of arithmetic. *If $n > 1$ is an integer, then it can be written as a product of primes in exactly one way (up to permutations of the primes).*

[119] If this author is remembering back that far correctly…

[120] Of course we have to make exceptions for zero and one, which are not primes. We also have to agree that when we factor a negative integer we just put a "$(-1)\times$" and then factor the absolute value as usual.

[121] The interested reader can find out more about the history of this result using their favourite search-engine. A very good starting point is this article. It certainly surprises this author that the first explicit formal statement and proof of this fact comes a full century after Newton and Leibniz developed calculus.

[122] `wikipedia.org/wiki/Euclid's_Elements`

[123] Kamal al-Din al-Farisi (1265 – 1318) was a Persian mathematician and physicist who is also famous for his mathematically rigorous description of the formation of rainbows.

[124] Jean Prestet (1648–1690), Leonard Euler (1707 – 1783) and Joseph-Louis Lagrange (1736 –1813). The latter was born Giuseppe Ludovico De la Grange Tournier. Your favourite search engine will get you to much more information, especially about Euler and Lagrange.

[125] Johann Carl Friedrich Gauss (1777 – 1855) made an incredible number of contributions to mathematics and physics. Indeed, we have already come across him in this text back when we were busy computing $1 + 2 + \cdot + n$. His history is well worth a quick trip to your favourite search engine.

With our work in the previous section we are ready to prove this result. It follows quite directly from Euclid's lemma Lemma 9.5.9. Recall that this tells us that

$$(p \mid ab) \implies (p \mid a) \vee (p \mid b).$$

Proof. Let $n \in \mathbb{Z}$ so that $n \geq 2$. We use induction to prove that n can be decomposed as a product of primes. We then show that this decomposition is unique.

We proceed to show the existence of a prime factorisation by strong induction 7.2.2.

- Base case. Since $n = 2$ is prime, it is trivially written as a product of primes.

- Inductive step. Assume that the result holds for all integers $2 \leq k < n$. If n is prime the result holds since the factorisation is trivial. On the other hand, if n is not prime, then (by definition) it can be written as

  $$n = ab \qquad \text{with } 1 < a, b < n.$$

  Since $a, b < n$ we know, by assumption, that

  $$a = p_1 p_2 \cdots p_k \qquad \text{and} \qquad b = q_1 q_2 \cdots q_\ell$$

  where the p_i, q_j are all primes. Hence

  $$n = ab = p_1 p_2 \cdots p_k \cdot q_1 q_2 \cdots q_\ell$$

  is a product of primes as requried.

We must now show that the decomposition is unique. A very standard way to show the uniqueness of a mathematical object is to assume there are two of them and show that the two must be equal. So, let us assume that we can write (please forgive recycling of p's and q's from just above):

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$

If there are any common prime factors between the sides, then divide through by them. Now either that cancels all the factors (in which case we are done), or we are left with an expression as above but with *no* common factors on each side. Well then take the smallest remaining prime on either side, call it z. Since z divides one side, it must, by Euclid's lemma, divide one of the factors on the other. However, since all the factors are prime, the factor z must be on both sides. But this cannot happen since we removed all the common factors. Thus the two factorisations of n must actually be the same. ∎

9.7 Exercises

1. Let $A = \{1, 2, 3, 4, 5, 6\}$. Write out the relation R that expresses "$\nmid$" (does not divide) on A as a set of ordered pairs. That is, $(x, y) \in R$ if and only if $x \nmid y$. Is the relation reflexive? Symmetric? Transitive?

2. Define a relation on $\mathbb{R}$ as $x \mathcal{R} y$ if $|x - y| < 1$. Is R reflexive? Symmetric? Transitive?

3. For each of the following relations, determine whether or not they are reflexive, symmetric, and transitive.

(a) $R = \{(1,1), (2,2), (3,3), (1,2), (2,1), (1,3), (3,1)\} \subseteq \{1,2,3\}\times\{1,2,3\}$

(b) For $a, b \in \mathbb{N}$, $a \mathcal{R} b$ if and only if $a \mid b$.

(c) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Q}\}$

(d) For $A, B \subseteq \mathbb{R}$, $A \mathcal{R} B$ if and only if $A \cap B = \emptyset$.

(e) For functions $f, g : \mathbb{R} \to \mathbb{R}$, $f \mathcal{R} g$ if and only if $f - g$ is linear, that is, there are constants $m, b \in \mathbb{R}$ so that $f(x) - g(x) = mx + b$ for all $x \in \mathbb{R}$. The constants m, b depend on f and g, but not on x.

4. Determine whether the following relations are reflexive, symmetric and transitive. Prove your answers.

(a) On the set X of all functions $\mathbb{R} \to \mathbb{R}$, we define the relation:

$$f \mathcal{R} g \text{ if there exists } x \in \mathbb{R} \text{ such that } f(x) = g(x).$$

(b) Let $\mathcal{S}$ be a relation on $\mathbb{Z}$ defined by:

$$x \mathcal{S} y \text{ if } xy \equiv 0 \pmod 4.$$

5. For each of the following relations, show that they are equivalence relations, and determine their equivalence classes.

(a) $R = \left\{((x_1, y_1), (x_2, y_2)) \in \mathbb{R}^2 \times \mathbb{R}^2 : x_1^2 + y_1^2 = x_2^2 + y_2^2\right\}$

(b) Let L be the set of all lines on the Euclidean plane, $\mathbb{R}^2$. For $\ell_1, \ell_2 \in L$, $\ell_1 \mathcal{R} \ell_2$ if and only if ℓ_1 and ℓ_2 have the same slope, or they are both vertical lines.

(c) Let R be a relation on $\mathbb{Z}^2$ defined by $x \mathcal{R} y$ if and only if $3 \mid x^2 - y^2$.

6. Define a relation on $\mathbb{Z}$ as

$$a \mathcal{R} b \iff 3 \mid (2a - 5b).$$

Is R an equivalence relation? Prove your answer.

7. Let E be a non-empty set and $q \in E$ be a fixed element of E. Consider the relation $\mathcal{R}$ on $\mathcal{P}(E)$ (power set of E) defined as

$$A \mathcal{R} B \iff (q \in A \cap B) \vee (q \in \overline{A} \cap \overline{B}),$$

where for any set $S \subseteq E$, we write $\overline{S} = E - S$ for the complement of S in E. Prove or disprove that $\mathcal{R}$ an equivalence relation.

8. Let R be a relation on $\mathbb{Z}$ defined by $a \mathcal{R} b$ if $7a^2 \equiv 2b^2 \pmod 5$. Prove that R is an equivalence relation. Determine its equivalence classes.

9. Let $n \in \mathbb{N}$ with $n > 1$ and let P be the set of polynomials with coefficients in $\mathbb{R}$. We define a relation, T, on P as follows:

Let $f, g \in P$. Then we say fTg if $f - g = c$ for some $c \in \mathbb{R}$. That is, if there exists a $c \in \mathbb{R}$ such that for all $x \in \mathbb{R}$, $f(x) - g(x) = c$.

Show that T is an equivalence relation on P.

10. Prove or disprove the following statements:

(a) If R and S are two equivalence relations on a set A, then $R \cup S$ is also an equivalence relation on A.

(b) If R and S are two equivalence relations on a set A, then $R \cap S$ is also an equivalence relation on A.

11. Let R be a symmetric and transitive relation on a set A.

(a) Show that R is not necessarily reflexive.

(b) Suppose that for every $a \in A$, there exists $b \in A$ such that $a \mathcal{R} b$. Prove that R is reflexive.

12. Let R be a relation on a nonempty set A. Then $\overline{R} = (A \times A) - R$ is also a relation on A. Prove or disprove each of the following statements:

(a) If R is reflexive, then $\overline{R}$ is reflexive.

(b) If R is symmetric, then $\overline{R}$ is symmetric.

(c) If R is transitive, then $\overline{R}$ is transitive.

13. In this question we will call a relation $R \subset \mathbb{Z} \times \mathbb{Z}$ *sparse* if $(a, b) \in R$ implies that $(a, b+1)$ and $(a+1, b)$ are NOT elements of R.

(a) Prove that for all $n \in \mathbb{N}$ the equivalence relation $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : n \mid (a - b)\}$ is sparse if and only if $n \neq 1$.

(b) Prove or disprove that every equivalence relation R on $\mathbb{Z}$ is sparse.

14. Let A be a non-empty set and $P \subseteq \mathcal{P}(A)$ and $Q \subseteq \mathcal{P}(A)$ partitions of A. Prove that the set R defined as

$$R = \{S \cap T : S \in P,\ T \in Q\} - \{\emptyset\}$$

is also a partition of A.

15. Suppose that $n \in \mathbb{N}$ and $\mathbb{Z}_n$ is the set of equivalence class of congruent modulo n on $\mathbb{Z}$. In this question we will call an element $[u]_n$ *invertible* if it has a multiplicative inverse. That is,

$$[u]_n \text{ is invertible} \iff \text{there exists } [v]_n \in \mathbb{Z}_n \text{ so that } [u]_n[v]_n = [1]_n.$$

Now, define a relation R on $\mathbb{Z}_n$ by

$$[x]_n \; R \; [y]_n \iff [x]_n[u]_n = [y]_n \text{ for some invertible } [u]_n \in \mathbb{Z}_n.$$

(a) Show that R is a equivalence relation.

(b) Compute the equivalence classes of this relation for $n = 6$.

16. Let $n \in \mathbb{Z}$ and $p \geq 5$ be prime.

(a) Prove, using Bézout's identity that if $3 \mid n$ and $8 \mid n$, then $24 \mid n$.

(b) Use the result in part (a) to show that $p^2 \equiv 1 \pmod{24}$.

17.

(a) Let p be a prime number, and suppose that $n \in \mathbb{Z}$ is such that $n \not\equiv 0 \pmod{p}$. Show that there is some $k \in \mathbb{Z}$ so that $nk \equiv 1 \pmod{p}$.

(b) Find an example to show that (a) may not be true if p is not prime. That is, find some composite number p and $n \in \mathbb{Z}$, $n \not\equiv 0 \pmod{p}$ such that $nk \not\equiv 1 \pmod{p}$ for all $k \in \mathbb{Z}$.

18. Let $a, b, d \in \mathbb{Z}$ such that $d \mid ab$. Show that the integer, $\frac{d}{\gcd(a,d)}$, divides b.

19. Let $a, b \in \mathbb{Z}$, at least one of which is non-zero.

(a) Suppose that d divides both a and b. Show that $d \mid \gcd(a, b)$.

(b) Let $m \in \mathbb{N}$. Show that $\gcd(ma, mb) = m \gcd(a, b)$.

(c) Let $c \in \mathbb{Z}$, $c \neq 0$. Show that the statement

$$\gcd(ac, b) = \gcd(a, b) \cdot \gcd(c, b)$$

does not hold in general.

20. A frequently used but false statement is

$$(x + y)^n = x^n + y^n$$

This is sometimes referred to by mathematicians as the "child's binomial theorem" (a quick trip to your search engine will turn up other names). One often sees examples of it such as

$$\sqrt{x + y} = \sqrt{x} + \sqrt{y} \qquad \text{and} \qquad (x + y)^2 = x^2 + y^2.$$

While it is definitely false, there is something here that can be rescued.

Notice that if we take $x, y \in \mathbb{Z}$ and let $n = 2$, then

$$(x+y)^2 = x^2 + 2xy + y^2$$

and so if we look at everything modulo 2 we get

$$(x+y)^2 \equiv (x^2 + 2xy + y^2) \equiv (x^2 + y^2) \pmod 2.$$

Similarly, with $n = 3$ we have

$$(x+y)^3 \equiv (x^3 + 3x^2y + 3xy^2 + y^3) \equiv (x^3 + y^3) \pmod 3.$$

Indeed, one can show that for any prime number p, and integers x, y we have

$$(x+y)^p \equiv x^p + y^p \pmod p.$$

Notice that this is not true for non-prime powers:

$$(1+3)^4 = 4^4 = 256 \equiv 0 \pmod 4$$

while

$$1^4 + 3^4 = 82 \equiv 2 \pmod 4.$$

(a) Use the recurrence in Exercise 7.3.21 (see Pascal's identity), together with the fact that $\binom{n}{0} = \binom{n}{n} = 1$, to prove that the binomial coefficients $\binom{n}{k}$ are integers.

(b) Prove that for prime p and integer $0 < k < p$ the binomial coefficient $\binom{p}{k}$ is a multiple of p, and so

$$\binom{p}{k} \equiv 0 \pmod p \qquad \text{for } 0 < k < p.$$

(c) Then using this and the Binomial Theorem (see Exercise 7.3.21) prove the result

$$(x+y)^p \equiv x^p + y^p \pmod p.$$

Chapter 10

Functions

One of the reasons to introduce relations is because they are nice intermediate mathematical object between sets (which have very little additional structure) and functions (which have quite a lot of structure). Indeed the idea of relations allows us to escape from the idea of a function as being a formula. Arguably, the usual high-school mathematics curriculum (especially the last couple of years of it) is really driving us towards being able to do calculus. And in calculus all the functions we look at are nice formulas that build up more complicated functions by doing arithmetic on simpler functions. At their core, these functions are really very algorithmic:

- Give me an input number x
- I do some arithmetic on x, and maybe look up some values (in a table or via a calculator or computer[126]) of things like sine, or logarithms.
- Then I return to you numerical result y.

Of course to be a function, this procedure has to be well defined — if you give me one input then I return to you one output. And if you give me the same input twice then I'd better return the same output each time.

10.1 Functions

So let's try to strip the idea of a function back as far as we can to make it both simpler and more general. First of all, we should escape from the idea that functions are restricted to have numbers are inputs and outputs; those of you with some programming experience will find this quite natural.

The following is a perfectly good function:

[126] Since doing complicated mathematical computations by hand can be very laborious, people who needed the results of those computations would hire people to do those computations for them. These people were called **computers**.

- Give me the name of a day of the week[127].
- I return to you the first letter of that word.

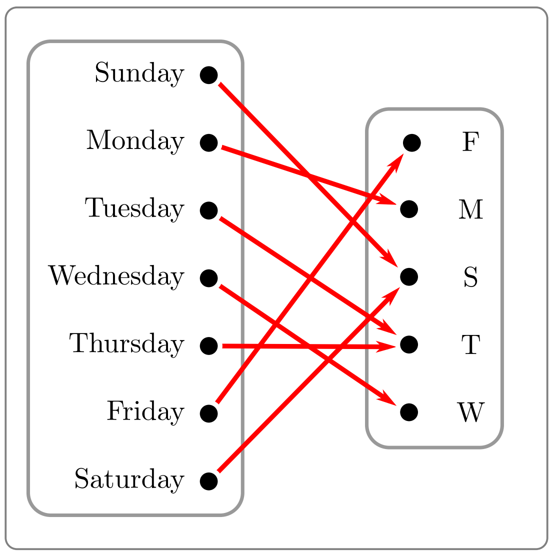
Now this is still quite algorithmic, but we have escaped from the tyranny of numbers — small steps first. The function takes inputs from the set

$$A = \{\text{Sunday}, \text{Monday}, \text{Tuesday}, \text{Wednesday}, \text{Thursday}, \text{Friday}, \text{Saturday}\}$$

and maps them to outputs in the set

$$B = \{F, M, S, T, W\}$$

We can summarise what is happening here by drawing a diagram that illustrates the inputs and outputs.



This is fine when the set of inputs is small, but will clearly become more and more painful as the set of inputs becomes larger. It is also still a quite algorithmic way of thinking about functions, but we can reduce the idea down further:

> Take an element of set A and do *something* to it to get an element of set B.

So we can summarise the function above by the pairs of inputs and outputs:

$$\Big\{(\text{Sunday}, S), (\text{Monday}, M), (\text{Tuesday}, T), (\text{Wednesday}, W),$$
$$(\text{Thursday}, T), (\text{Friday}, F), (\text{Saturday}, S)\Big\}$$

So the set of ordered pairs of inputs and outputs is a subset of $A \times B$ — so it is a relation. However, its not *just any* relation — that is too general. We have extra conditions that a relation must satisfy in order to be a function.

[127]Written in correct — ie. Australian — English. The author might be biased in this assessment.

- We know that a function can only give one output for a given input. That is, if $f(a) = b_1$ and $f(a) = b_2$ then we must have $b_1 = b_2$. We can also express this in terms of relations:

$$((a, b_1) \in R \wedge (a, b_2) \in R) \implies b_1 = b_2$$

- Also everything in the input set has to have an output. That is

$$\forall a \in A, \exists b \in B \text{ so that } f(a) = b.$$

  Notice that this does *not* say that we have to reach *everything* in the output set — rather it just says that every input has to be "legal"; it results in some element in the output set.

Armed with these ideas we can define our new and more abstract idea of a function.

10.2 A more abstract definition

Definition 10.2.1 Let A, B be non-empty sets.

- A **function** from A to B, written $f : A \to B$ is a non-empty subset of $A \times B$ with two further properties
  - for every $a \in A$ there is some $b \in B$ so that $(a, b) \in f$.
  - if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.
- In this context we call the set A the **domain** of f, and the set B is called the **co-domain**.
- If $(a, b) \in f$ then we write $f(a) = b$, and we call b the image of a. We also sometimes say that f maps a to b. With this notation the above two conditions are written as
  - for every $a \in A$ there is some $b \in B$ so that $f(a) = b$.
  - if $f(a) = b$ and $f(a) = c$ then $b = c$.
- We can further refine the co-domain to be exactly the set of elements of B that are mapped to by something in A; this set is called the **range**:

$$\text{rng} f = \{b \in B \mid \exists a \in A \text{ s.t. } f(a) = b\}$$

$\Diamond$

Some things to note

- The condition that if $f(a) = b$ and $f(a) = c$ then $b = c$ just means that the function is well defined. If we apply the function to a given element then we only get 1 result. You might know this from high-school as the "vertical line test" — ie a graph-sketch corresponds to a function provided every vertical line intersects the graph once or not at all.

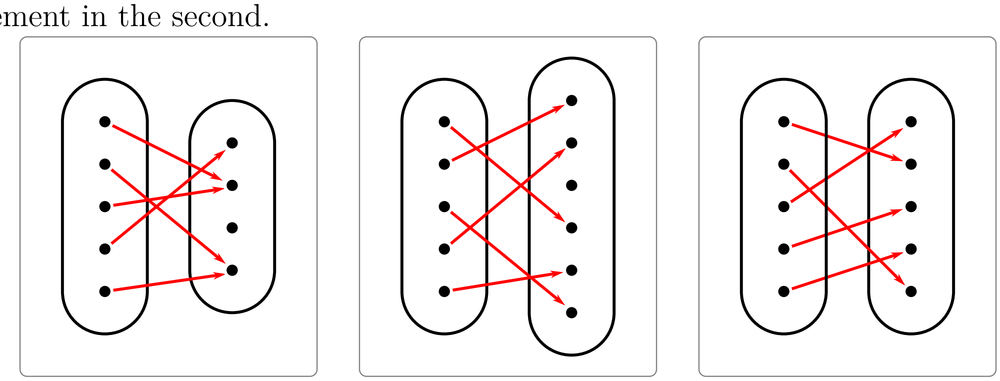
- Two functions $f, g : A \to B$ are equal when $f(a) = g(a)$ for all $a \in A$.
- The range is not (necessarily) the same as the co-domain. The range is always a subset of the co-domain. For example

  $$f : \mathbb{R} \to \mathbb{R} \qquad\qquad f(x) = x^2$$

  has domain $\mathbb{R}$, co-domain $\mathbb{R}$ and range $[0, \infty)$. We make the distinction between the two because sometimes it is really hard to write the range, but it is usually very easy to write the co-domain. We must be able to apply f to every single $a \in A$, but we don't have to arrive at every $b \in B$.

The term "function" only entered mathematics around the 17th century with Leibniz concurrent with the development of calculus and analytical geometry (such as the study of curves in the plane). Before this notions of dependent and independent variables that we are used to when studying $y = f(x)$ were not so well formalised. Arguably there was some work in this direction around the 12th-14th centuries by mathematicians such as Sharaf al-Din al-Tusi (who developed systematic method for numerical approximation of the roots of cubic polynomials) and Nicole Oresme (who first proved that the harmonic series diverges). Around the 19th century developments in mathematics required more general notions of functions and mathematicians, such as Dirichlet, Dedekind and Cantor, pushed away from the notion of a function as a formula and towards more general definitions such as the one above.

Once we have this more general idea of a function, we need ways to represent it. A very natural way (once Descartes introduced it — though it was also developed concurrently by Fermat and much earlier by Oresme) is to plot the function as a curve in the plane. Each point on the curve represents a pair of coordinates (x, y) so that $y = f(x)$. With this more general idea of a function we might try drawing something like we did above for the days-of-the-week example. That is, we might draw two sets of elements and edges between them to indicate that the function applied to that element in the first set gives the corresponding element in the second.



We could also just explicitly write out the mapping. So, for example, if the sets in the first of these functions are

$$A = \{1, 2, 3, 4, 5\} \qquad B = \{a, b, c, d\}$$

then the function can be written as

$$f = \{(1, b), (2, d), (3, b), (4, a), (5, d)\}$$

Both these approaches are reasonably practical when the domain and co-domain of the function are small, but is really not going to work as soon as they get a little bigger.

Example 10.2.2 Consider the sets

$$f = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 3x + 2y = 0\}$$
$$g = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 3x + y = 0\}.$$

Both are subsets of $\mathbb{Z} \times \mathbb{Z}$ and so are (by definition) relations on $\mathbb{Z}$. Only one is a function from $\mathbb{Z}$ to $\mathbb{Z}$.

In order for f to be a function it has to satisfy two conditions:

- For every x in the domain, there must be a y in the co-domain so that $f(x) = y$, and
- If $f(x) = y$ and $f(x) = z$ then $y = z$.

The first of these fails, since if we set $x = 1$, then there is no integer y so that $3 + 2y = 0$. Indeed we require $y = -\frac{3}{2}$. The second condition is satisfied, because if $f(x) = y$ and $f(x) = z$, then we know that

$$3x + 2y = 0 \qquad \text{and} \qquad 3x + 2z = 0$$

then subtract one equation from the other to get

$$2y - 2z = 0$$

and so $y = z$.

The relation g satisfies both conditions:

- Let x be any integer, then we can set $y = -3x \in \mathbb{Z}$ and $3x + y = 0$ as required.
- The second condition is satisfied by the same argument we used for f.

The co-domain of g is the set of integers, but its range $\{n \in \mathbb{Z}$ so that $3|n\}$. □

10.3 Images and preimages of sets

When we defined the function $f : A \to B$, we said that if $f(a) = b$ then we called b the image of a under f. This idea can be extended quite naturally to think of the image of a set of points. Also, given an element $b \in B$, we can ask for all the elements of A that map to it. This latter idea is not quite the inverse function, but it is getting close to it.

We should define these sets more precisely:

Definition 10.3.1 Image and preimage. Let $f : A \to B$ be a function, and let $C \subseteq A$ and let $D \subseteq B$.

- The set $f(C) = \{f(x) : x \in C\}$ is the **image of** C **in** B.
- The set $f^{-1}(D) = \{x \in A : f(x) \in D\}$ is the **preimage of** D **in** A or f**-inverse of** D.

◊

Remark 10.3.2 Preimage of a single element. Note that the preimage of a set containing a single element of B is a (possibly) set of elements of A. For example, consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$. Then

$$f^{-1}(\{0\}) = \{0\} \qquad f^{-1}(\{1\}) = \{-1, 1\} \qquad f^{-1}(\{-1\}) = \varnothing.$$

This shows that the preimage of a set containing a single element is a set that may contain zero, one, two or even more elements. Indeed, it is not hard to construct an example in which the preimage contains infinitely many elements. When our function satisfies very specific conditions, we can ensure that the preimage of a set containing a single element is always set containing a single element. Understanding those conditions is one of the main aims of this chapter and we'll discuss it in detail in the next section. That, in turn, will help us to define the **inverse function**.

You will have noticed that in the preceding paragraph we have had to write "the preimage of a set containing a single element" several times. This becomes quite cumbersome. We will, from here, abuse the definition of the preimage a little to simplify our writing. In particular, we will often write "the preimage of an element x" to mean "the preimage of the set $\{x\}$". While this is modestly incorrect, it does make the writing and reading easier.

The notation for preimage, f^{-1}, is somewhat unfortunate in that we use the same notation to mean the inverse-function. Additionally, it is regularly confused with

$$(f(x))^{-1} = \frac{1}{f(x)}$$

ie the reciprocal. Alas, we are stuck with this notation and must be careful to understand its meaning by context.

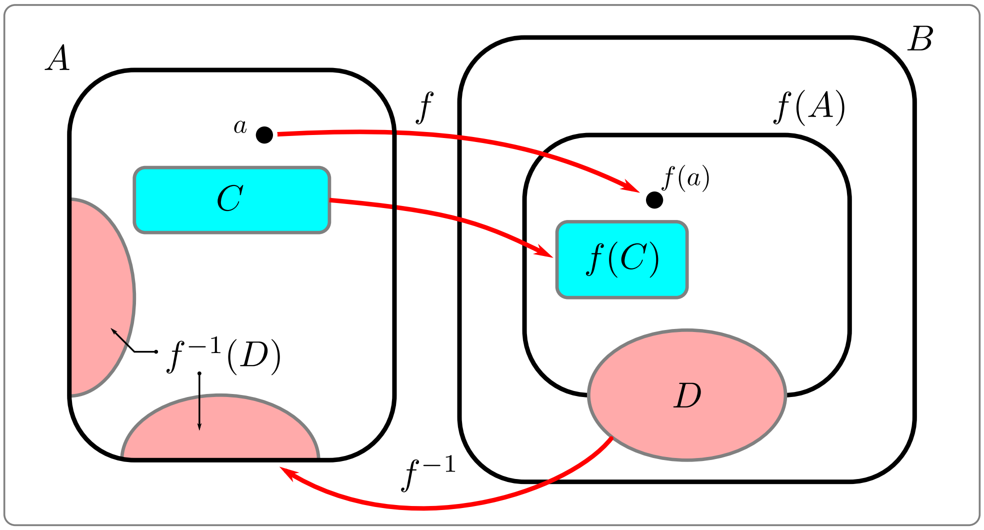
This is an important point, so we'll make it a formal warning:

Warning 10.3.3 Be careful with preimages:

- The preimage f^{-1} is *not* the inverse function.
- If certain special conditions are satisfied, then the inverse function exists and we use the same notation to denote that function.

Consequently, when you see f^{-1} you should think "preimage" and not "inverse function" unless we specifically know that the inverse exists.

After all those warnings and caveats, lets draw a schematic of images and preimages:



Notice in this figure that

- we have drawn $f(A)$ as a subset of B — in fact $f(A)$ is exactly the range of f and so must be a subset of B.
- we have drawn the preimage of D so that it looks like two copies of half of the set D — this is to emphasise the fact that not every element of B has to have a preimage in A. Further, a given point in B might have more than one preimage.

Our quick look at preimages of $f(x) = x^2$ above illustrated this second point. That was a little brief, but the following example looks at this in more detail.

Example 10.3.4 Images and preimages. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Find the following

(a) $f([0, 4])$

(b) $f([-3, -1] \cup [1, 2])$

(c) $f^{-1}(\{0\})$

(d) $f^{-1}(\{1\})$

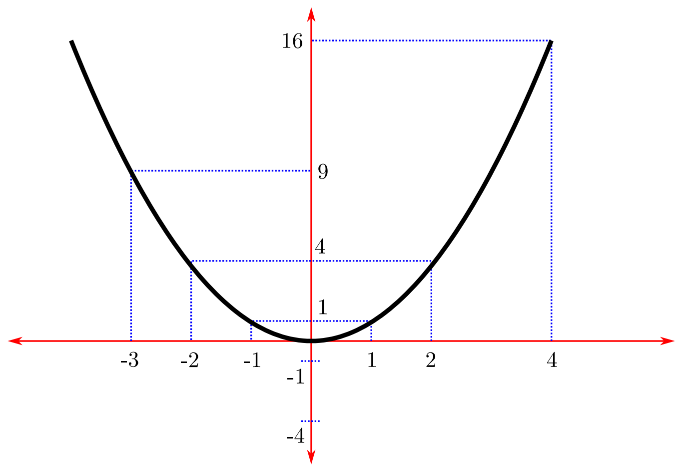
(e) $f^{-1}([0, 4]) = [-2, 2]$

(f) $f^{-1}([1,4]) = [-2,-1] \cup [1,2]$

(g) $f^{-1}(\{-1\})$

(h) $f^{-1}([-4,-1])$

Solution. It will help to make a quick sketch of $y = f(x) = x^2$ and think about the various intervals in the domain and co-domain. That $f(x)$ is decreasing for $x < 0$ and increasing for $x > 0$ does make this exercise a little easier.



(a) The interval $0 \le x \le 4$ maps to $0 \le x^2 \le 16$. So $f([0,4]) = [0,16]$

(b) The interval $-3 \le x \le -1$ maps to $1 \le x^2 \le 9$, and the interval $1 \le x \le 2$ maps to $1 \le x^2 \le 4$. Hence the points in the union $[-3,-1] \cup [1,2]$ map to the interval $[1,9] \cup [1,4] = [1,9]$. Hence $f([-3,-1] \cup [1,2]) = [1,9]$.

(c) To find the preimage of $\{0\}$, we need to solve $f(x) = x^2 = 0$. This only has a single solution, namely $x = 0$, and so $f^{-1}(\{0\}) = \{0\}$

(d) To find the preimage of $\{1\}$, we need to solve $f(x) = x^2 = 1$. This only two solutions, namely $x = \pm 1$, and so $f^{-1}(\{1\}) = \{-1,1\}$

(e) The interval $0 \le x^2 \le 4$ is mapped to by any number in the interval $-2 \le x \le 2$. So $f^{-1}([0,4]) = [-2,2]$.

   We can check this by looking at the above plot, but also by considering $f([-2,0] \cup [0,2])$. The interval $0 \le x \le 2$ maps to $0 \le x^2 \le 4$ and $-2 \le x \le 0$ maps to the same, $0 \le x^2 \le 4$.

(f) The interval $1 \le x^2 \le 4$ is mapped to by any number in the interval $1 \le x \le 2$ or any number in $-2 \le x \le -1$. So $f^{-1}([1,4]) = [-2,-1] \cup [1,2]$.

   Again, we can check this by looking at the above plot, but also by considering $f([-2,-1] \cup [1,2])$. The interval $1 \le x \le 2$ mapes to $1 \le x^2 \le 4$, and $-2 \le x \le -1$ maps to the same.

(g) To find the preimage of $\{-1\}$, we need to solve $f(x) = x^2 = -1$. This has no solutions[128], so $f^{-1}(\{-1\}) = \varnothing$

(h) To find the preimage of $-4 \leq x^2 \leq -1$, we should recall that the square of any real number is non-negative. So there are no values of x that map into that interval. Thus $f^{-1}([-4, -1]) = \varnothing$.

□

This example shows that the preimage of a single element[129] in the co-domain can be empty, or can contain a single element, or can contain multiple elements. As noted above, we want to understand what conditions we can impose on a function so that the preimage of a single point[130] in the co-domain always contains exactly one point in the domain. This will allow us to properly define inverse functions — that is if $f(x) = y$ then how do we define a new function g so that $g(y) = x$.

Before we get to inverses we can do some more exploring of images and preimages. Since these are really operations on sets, we can (and should) ask ourselves how do these new things we can do to sets interact with the other things we can do to sets. So we now explore some of the relationships between subsets and their images and preimages, and also the interplay between functions, unions, intersections and differences.

For example — it is clearly [131] the case that if $C_1 \subseteq C_2 \subseteq A$ then $f(C_1) \subseteq f(C_2)$. Similarly if $D_1 \subseteq D_2 \subseteq B$ then $f^{-1}(D_1) \subseteq f^{-1}(D_2)$. While we've said "clearly", we should really state results carefully and make them a result and prove them. We'll follow this up with a more important result which we'll call a theorem.

Result 10.3.5 *Let $f : A \to B$, and let $C_1 \subseteq C_2 \subseteq A$ and $D_1 \subseteq D_2 \subseteq B$. Then*

$$f(C_1) \subseteq f(C_2) \qquad \textit{and} \qquad f^{-1}(D_1) \subseteq f^{-1}(D_2).$$

Proof. We prove each inclusion in turn.

- Let $b \in f(C_1)$. Then (by the definition of image) there is some $a \in C_1$ so that $f(a) = b$. But since $C_1 \subseteq C_2$, we know that $a \in C_2$. Hence $b = f(a) \in f(C_2)$ as required.

- Let $a \in f^{-1}(D_1)$. Then (by definition of preimage) $f(a) \in D_1$. But since $D_1 \subseteq D_2$, we know $f(a) \in D_2$. Then, by the definition of preimage, we know that $a \in f^{-1}(D_2)$.

■

[130]To be more precise, it has no solutions over the reals, which is the domain of the function.

[129]Recall that we are abusing the definition of preimage here; we really mean "the preimage of a set containing a single element".

[130]Another similar abuse of the definition of preimage in order to keep the language flowing.

[131]This is always a dangerous word when writing mathematics, and the authors include it here as an example of what, perhaps, one should not do. One person's "clearly" is another persons "3 hours of confusion".

Now, while the above proof is not terribly technical, it does require us to know the definitions of image and preimage and to understand how to manipulate them. Even though the statement we have just proved is (arguably) obvious[132], its proof is not so trivial.

Theorem 10.3.6 *Let $f : A \to B$, and let $C \subseteq A$ and $D \subseteq B$. Further, let C_1, C_2 be subsets of A and let D_1, D_2 be subsets of B. The following are true*

(i) $C \subseteq f^{-1}(f(C))$

(ii) $f(f^{-1}(D)) \subseteq D$

(iii) $f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2)$ *— note: need not be equal*

(iv) $f(C_1 \cup C_2) = f(C_1) \cup f(C_2)$ *— note: are equal*

(v) $f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$

(vi) $f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2)$

So what does this theorem tell us? It says that preimages play very nicely with set operations — they are well-behaved:

- The preimage of the intersection is the intersection of the preimages
- The preimage of the union is the union of the preimages

It also tells us that images are *mostly* well-behaved:

- The image of the union is the union of the images
- The image of the intersection is *a subset of* the intersection of the images.

Of course, we should prove these results. We'll do some in the text and leave some of them as exercises. We'll prove (iii) first and then (vi) and leave (i) until last. In the authors' experience, people find (i) quite confusing, so we will tackle it after we've warmed up on the other two.
Proof.

- Proof of (iii):

  We need to show that if an element is in the set on the left then it is in the set on the right. Let $b \in f(C_1 \cap C_2)$. Hence there is $a \in C_1 \cap C_2$ such that $f(a) = b$. This means that $a \in C_1$ and $a \in C_2$. It follows that $f(a) = b \in f(C_1)$ and $f(a) = b \in f(C_2)$, and hence $b \in f(C_1) \cap f(C_2)$.

  The converse is false: $f(C_1) \cap f(C_2) \not\subseteq f(C_1 \cap C_2)$ — another good exercise

[132] "Obvious" is another dangerous word, and is a good example of **emotive conjugation**. "I found it obvious" but "they spent 4 days trying to work out what was going on". This sort of thing often arises in the descriptions that people give their own actions compared with the descriptions of others. The interested reader should search-engine their way to the BBC series "Yes Prime Minister" which has the following example: "I give confidential press briefings; you leak; he's being charged under section 2A of the Official Secrets Act."

for the reader.

- Proof of (vi):

  Let $a \in f^{-1}(D_1 \cup D_2)$ and so $f(a) \in D_1 \cup D_2$. This means that $f(a) \in D_1$ or $f(a) \in D_2$. If $f(a) \in D_1$ it follows that $a \in f^{-1}(D_1)$. Similarly if $f(a) \in D_2$ then $a \in f^{-1}(D_2)$. Since a lies in one of these two sets, it follows that $a \in f^{-1}(D_1) \cup f^{-1}(D_2)$.

  Let $a \in f^{-1}(D_1) \cup f^{-1}(D_2)$. Then a is an element of one of these two sets. If $a \in f^{-1}(D_1)$, then $f(a) \in D_1$. Similarly if $a \in f^{-1}(D_2)$ then $f(a) \in D_2$. In either case $f(a) \in D_1 \cup D_2$ and so $a \in f^{-1}(D_1 \cup D_2)$.

- Proof of (i):

  Let $x \in C$. We need to show that $x \in f^{-1}(f(C))$. So what is this set — by the definition it is $\{a \in A : f(a) \in f(C)\}$. Since $x \in C$ we have, by definition, $f(x) \in f(C)$. Since $f(x) \in f(C)$ it follows that $x \in f^{-1}(f(C))$.

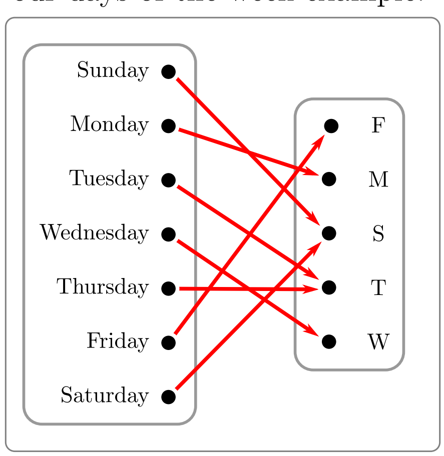
  Note that the converse of this statement is false: $f^{-1}(f(C)) \not\subseteq C$. This makes a good exercise. We also note that (ii) follows a similarly flavoured argument and is another good exercise for the reader.

■

10.4 Injective and surjective functions

We typically think of a function as taking objects from one set, A, doing "stuff" and turning them into elements from another set B. With this in mind, it is quite natural to ask whether or not we can reverse this process; take our result and turn it back into our original object. That is, "when is a given function invertible".

If you think back to our days-of-the-week example:



You can see that if we have arrived at the letter "M" then it is easy to determine that we started at "Monday" — so easy to undo the function. However, if we have arrived at "S" then things are not so simple — we could have started with either “Sunday” or “Saturday”. Obviously this is related to the preimage that we saw before. The good case of “M” worked because the preimage[133] had 1 element in it, “Monday”. The bad case of “S” didn’t work because the preimage[134] had 2 elements in it. More generally the preimage could have any number of elements in it — including zero.

Now, for us to be able to sensibly undo our function, we need the preimage of every element in our co-domain to have exactly one element in it. To be more precise, for any element y in our codomain, there must exist some x in the domain so that the preimage of $\{y\}$ is the set $\{x\}$. If you think about this a little, this means that the domain and co-domain must have the same size[135]. We’ll discuss this more soon. But it should be clear from this discussion that not every function can be undone, and that those that are “undoable” have to satisfy special properties. This brings us to a couple of important definitions.

To get to this we need to define some simple properties that functions can have.

10.4.1 Injections and surjections

Definition 10.4.1 Let $a_1, a_2 \in A$ and let $f : A \to B$ be a function. We say that f is injective or one-to-one when

$$\text{if } a_1 \neq a_2 \text{ then } f(a_1) \neq f(a_2).$$

It is helpful to also write the contrapositive of this condition. We say that f is injective or one-to-one when

$$\text{if } f(a_1) = f(a_2) \text{ then } a_1 = a_2.$$

$\Diamond$

Things to note

- The term injective is, in this author’s opinion, better to use than one-to-one. When we speak (and write) we are sometimes quite sloppy with our use of prepositions like “to” or “on” or “in” or “onto”, so we might accidentally say one-onto-one, for example. The term injective is a nice latin-flavoured word that makes the speaker / writer sound more authoritative [136] .

[133] To be more precise, the preimage of the set $\{\mathrm{M}\}$ is the set $\{\mathrm{Monday}\}$.

[134] Again, being more precise, the preimage of the set $\{\mathrm{S}\}$ is the set $\{\mathrm{Saturday}, \mathrm{Sunday}\}$.

[135] This is perhaps no so hard to see when everything is finite, but harder to see when things are infinite. Indeed, we’ll see examples of just how weird this can be when we get to cardinality later in the text.

[136] Of course that doesn’t mean the speaker knows what they are talking about, just that they sound like it. This is a variation of the “argument from authority” fallacy. Mind you there is the equally, or perhaps even more pernicious, fallacy that because a statement comes from an authority it should be mistrusted. Perhaps an example of an “appeal to common folk” fallacy. “Experts — bah! What would they know?!”

- A very common mistake made with this definition is to get the implications around the wrong way — to give the converse of what is required:
  - The right way — $f(a_1) = f(a_2) \implies a_1 = a_2$. Injective!
  - The wrong way — $a_1 = a_2 \implies f(a_1) = f(a_2)$ — this is just "same input implies same output" which just says the function is *well defined*.

  Be careful of this.
- So when a function is injective, different elements map to different elements.
- When a function is not injective there must be at least one pair $a_1, a_2 \in A$ so that $a_1 \neq a_2 \in A$ but $f(a_1) = f(a_2)$.

As a preview of what is to come when we reach the chapter on cardinality, think about what we can say about the sizes of *finite* sets A, B if there is an injective function between them $f : A \to B$. Each element $a \in A$ has to map to a *different* element $b \in B$. Consequently the set B must have at least as many elements as A. That is $|A| \leq |B|$. We note that when A, B are infinite, these sorts of questions become much less obvious.

Result 10.4.2 *Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 7x - 3$. Then f is injective.*

So — how do we prove this. We have two equivalent conditions

- $a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$
- $f(a_1) = f(a_2) \implies a_1 = a_2$.

Arguably, the second is easier since we have all had much more practice manipulating equalities than manipulating inequalities. So lets run through the argument. Let $a_1, a_2 \in \mathbb{R}$, and assume that

$$\begin{aligned} f(a_1) &= f(a_2) && \text{then we must have} \\ 7a_1 - 3 &= 7a_2 - 3 && \text{and so} \\ 7a_1 &= 7a_2 && \text{and hence} \\ a_1 &= a_2. \end{aligned}$$

That wasn't too bad. Time to write it up as a proof.

Proof of Result 10.4.2. Let $a_1, a_2 \in \mathbb{R}$ and assume $f(a_1) = f(a_2)$. Then $7a_1 - 3 = 7a_2 - 3$ and so $7a_1 = 7a_2$ and thus $a_1 = a_2$. Hence f is injective. ■

Now what about an example that is not injective — we can recycle our x^2 example from above.

Result 10.4.3 *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not injective.*

Injective means

$$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \implies a_1 = a_2$$

and hence non-injective is just the negation of this, namely

$$\exists a_1, a_2 \in A \text{ s.t. } f(a_1) = f(a_2) \wedge a_1 \neq a_2.$$

So we need a counter-example; there exists some pair of distinct $a_1, a_2 \in \mathbb{R}$ that map to the same value. Of course, we could have started with the equivalent contrapositive definition of injective:

$$\forall a_1, a_2 \in A, a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

The negation of that is

$$\exists a_1, a_2 \in A \text{ s.t. } a_2 \neq a_2 \implies f(a_1) = f(a_2)$$

which is the same as we found with the first definition of injective. Of course, this must be the case because the two definitions are equivalent.

Proof of Result 10.4.3. Since $-1, 1$ are in the domain of f and $f(-1) = f(1) = 1$, the function is not injective. ■

Remark 10.4.4 Preimages and injections. Consider an injection $f : A \to B$ and, for any given $b \in B$, the preimage of $\{b\}$:

$$f^{-1}(\{b\}) = \{a \in A \mid f(a) = b\}$$

This set is either empty or contains exactly 1 element. To see this consider $a, c \in f^{-1}(\{b\})$. By definition of the preimage, we know that $f(a) = b$ and $f(c) = b$. Since f is injective, this tells us that $a = c$. So the preimage of a point under an injection contains at most 1 element.

Another important class of functions are surjections.

Definition 10.4.5 Let $f : A \to B$ be a function. We say that f is surjective, or onto, when for every $b \in B$ there is some $a \in A$ such that $f(a) = b$. ◊

Things to note

- This simply means that every element in B is mapped to by some element of A.
- If the function is not surjective then there is some $b \in B$ such that for all $a \in A$, $f(a) \neq b$.
- Again, this author prefers the nice latin "surjective" over the term "onto" because it is less likely to confused with other prepositions.

Again, as a preview of cardinality, think about what we can say about the sizes of *finite* sets A, B if there is an surjection between them $g : A \to B$. Each element $b \in B$ must be mapped to by *at least one* element $a \in A$. Consequently the set A must have at least as many elements as B. That is $|A| \geq |B|$.

Result 10.4.6 *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 7x - 3$ is surjective*

So we need to show that no matter which $y \in \mathbb{R}$ we can always find some $x \in \mathbb{R}$ such that $f(x) = 7x - 3 = y$. So we can just make x the subject giving $x = (y+3)/7$.

Now that we have chosen x, we need to make sure it is actually an element of the domain of the function. In this case it is easy since $(y+3)/7 \in \mathbb{R}$. However, if we consider a similarly function

$$g : \mathbb{Z} \to \mathbb{Z} \qquad g(x) = 7x - 3$$

we would also get $x = \frac{y+3}{7}$, but then x is not always in the domain. Time to write up.

Proof of Result 10.4.6. Let $y \in \mathbb{R}$. Choose $x = (y+3)/7$, then $f(x) = 7 \cdot \frac{y+3}{7} - 3 = y$. Hence f is surjective. ■

Notice that in the proof we *do not* have to explain to the reader how we found the choice of x. It is not necessary to work through solving $y = f(x)$ for x. All we need to do in the proof is tell the reader "Given y we choose this value of x" and then show that $f(x) = y$. This can often be a little frustrating for the reader who can be left thinking "How on earth did they get that?"; a good author might put in a little explanation in the text surrounding the proof, but it is not required for the proof to be valid.

Result 10.4.7 *The function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^2$ is not surjective.*

Since surjective means

$$\forall b \in B, \exists a \in A \text{ s.t. } f(a) = b$$

its negation is

$$\exists b \in B \text{ s.t. } \forall a \in A, f(a) \neq b.$$

So in order to show that g is not surjective, we have to find (at least one) $b \in \mathbb{R}$ (in the co-domain) that is not the image of any $a \in \mathbb{R}$ (in the domain). Sometimes this can be tricky to prove, but for the example above we can use the fact that the square of a real is non-negative.

Proof of Result 10.4.7. Let $b = -1 \in \mathbb{R}$. Since the square of any real number is non-negative, we know that $f(x) = x^2 \geq 0$ for any $x \in \mathbb{R}$. Hence there is no $x \in \mathbb{R}$ so that $f(x) = -1$. Thus the function is not surjective. ■

Remark 10.4.8 Preimages and surjections. Consider a surjection $g : A \to B$ and, for any given $b \in B$, the preimage of $\{b\}$:

$$g^{-1}(\{b\}) = \{a \in A \mid g(a) = b\}$$

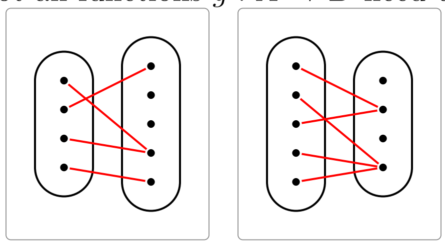
Since g is a surjection, for any given $b \in B$, there must be at least $a \in A$ so that $g(a) = b$. Hence the preimage must contain at least one element.

10.4.2 Bijective functions

Recall that we reasoned (but didn't really prove) that for *finite* sets A, B

- if there is an injection $f : A \to B$ then $|A| \le |B|$, and
- if there is a surjection $g : A \to B$ then $|A| \ge |B|$

Warning 10.4.9 Be careful with your converses. Consider two finite sets A, B. If $|A| \le |B|$ it does *not* mean that all functions $f : A \to B$ will be injections. Similarly if $|A| \ge |B|$ not all functions $g : A \to B$ need to surjections.



The function on the left is not injective (despite its domain being smaller than its co-domain). And the function on the right it not surjective (despite its domain being larger than its co-domain).

So given sets A, B if we can find such an injection and a surjection between them, then $|A| = |B|$. One way to do this is to find one function $h : A \to B$ that is *both* injective and surjective; these functions are called **bijections**. Finding a bijection between two sets is a good way to demonstrate that they have the same size — we'll do more on this in the chapter on cardinality.

Definition 10.4.10 Let $f : A \to B$ be a function. If f is injective and surjective then we say that f is **bijective**, or a **one-to-one correspondence**. ♢

The terms **injective**, **surjective** and **bijective** were coined by Nicholas Bourbaki. Bourbaki was not a person, but the pseudonym of a group of (mostly French) mathematicians who wrote a series of texts in the mid 20th century. The group still exists and published a book in 2016. The central aim of the group was to create a series of complete and self-contained texts on the core of mathematics. The texts strive to be extremely rigorous and very general in their treatment of the material and not without controversy. You can search engine your way to more information on this topic.

Example 10.4.11 Consider the following functions. Determine whether they are injective, surjective or bijective. They all have the same formula, but have different domains and co-domains (and so are different functions).

- $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$. Neither surjective, nor injective.
- $g : \mathbb{R} \to [0, \infty)$ given by $g(x) = x^2$. Surjective, but not injective.
- $h : [0, \infty) \to \mathbb{R}$ given by $h(x) = x^2$. Not surjective, but is injective.
- $\rho : [0, \infty) \to [0, \infty)$ given by $\rho(x) = x^2$. Is bijective.

Solution. All of these functions have the same formula, just different domains and co-domains.

- Think about how these functions can fail to be injective. We can verify that $f(-x) = (-x)^2 = x^2 = f(x)$. Hence these functions will fail to be injective if x and $-x$ are both within the domain. So neither f, g are injective since

$$f(-1) = f(1) = 1 \qquad \text{and} \qquad g(-1) = g(1) = 1$$

  We now prove that h is injective. So let $a_1, a_2 \geq 0$, so that $h(a_1) = h(a_2)$. Hence

$$a_1^2 = a_2^2$$

  Taking square-roots gives

$$a_1 = \pm a_2$$

  However, since neither a_1, a_2 are negative, we must have $a_1 = a_2$ and so h is an injection. The same argument works for ρ.

- Now think about how these functions might fail to be surjective. We know that the square of a real number is non-negative. That is $0 \leq x^2$. So if there is a negative number in the co-domain there is no real number that can map to it. Consequently, neither f nor h are surjections, since there is no $x \in \mathbb{R}$ so that

$$f(x) = -1 \qquad \text{or} \qquad h(x) = -1.$$

  We now prove that g is surjective using the square-root function. Given any y in the codomain of g, pick $x = \sqrt{y}$. Since $y \geq 0$, x is defined and non-negative and so in the domain of g. Further, we know that $g(x) = x^2 = (\sqrt{y})^2 = y$. Thus g is surjective. The argument for ρ is identical.

So to summarise

- f is neither injective, nor surjective,
- g is surjective but not injective,
- h is injective but not surjective, and
- ρ is both injective and surjective, and so bijective.

□

The simplest (useful) bijective function is the identity function.

Definition 10.4.12 Given a non-empty set A we define the identity function $i_A : A \to A$ by $i_A(a) = a$ for all $a \in A$. ◊

The authors are usually loath to use the word "clear", but we hope that it is clear that the identify function is surjective and injective and so bijective. We could prove it if we really had to. We will need the identity function to help us define the inverse of a function.

We need a couple more examples.

Result 10.4.13 *The function $g : \mathbb{R} \to \mathbb{R}$, defined by $7x - 3$, is a bijection.*

Proof. We need to show that g is both injective and surjective.

- Injective: We proved this in Result 10.4.2.
- Surjective: We proved this in Result 10.4.6.

Since the function is both injective and surjective it is bijective. ∎

A more interesting example. Let $a, b, c, d \in \mathbb{R}$ and define

$$h : \mathbb{R} - \left\{ \frac{d}{c} \right\} \to \mathbb{R} - \left\{ \frac{a}{c} \right\} \qquad h(x) = \frac{ax - b}{cx - d}$$

If the constants satisfy $ad \neq bc$, then this is a Möbius transformation[137] Notice that the denominator is zero when $cx = d$, and hence we have removed the point $x = \frac{d}{c}$ from the domain; the function is not defined there. Some similar reasoning can show that there is no $x \in \mathbb{R}$ so that $h(x) = \frac{a}{c}$, so we remove that point from the co-domain. Finally, notice that if $ad = bc$ then

$$\begin{aligned} h(x) &= \frac{ax - b}{cx - d} \\ &= \frac{cax - cb}{c^2x - cd} && \text{since } bc = ad \\ &= \frac{cax - ad}{c^2x - cd} = \frac{a(cx - d)}{c(cx - d)} \\ &= \frac{a}{c} \end{aligned}$$

and so is constant.

Möbius transforms are a good source of non-trivial bijective function examples for authors to give to students. So let us just do this in full generality.

Result 10.4.14 *Let $a, b, c, d \in \mathbb{R}$ with $ad \neq bc$. The function $h : \mathbb{R} - \left\{ \frac{d}{c} \right\} \to \mathbb{R} - \left\{ \frac{a}{c} \right\}$ defined by $h(x) = \frac{ax-b}{cx-d}$ is bijective.*

Scratch work.

- Injective. Let $x, y \in \mathbb{R} - \left\{ \frac{d}{c} \right\}$ and assume $h(x) = h(y)$. Then

$$\frac{ax - b}{cx - d} = \frac{ay - b}{cy - d}$$

[137]Well, we should really take x over complex numbers, but the interested reader should search-engine their way to more on this topic. They are named for August Möbius who was 19th century German mathematician and astronomer. He is perhaps best known for discovering the Möbius strip which is an two-dimensional surface with only 1 side. The Möbius strip was actually discovered slightly earlier by Johann Listing; perhaps "Listing strip" doesn't have quite the same ring to it (sorry for the poor pun).

$$\begin{aligned} (cy-d)(ax-b) &= (ay-b)(cx-d) && \text{since denominator } \neq 0 \\ caxy - cyb - adx + db &= acxy - ady - bcx + bd \\ (ad-bc)y &= (ad-bc)x && \text{so we are done} \end{aligned}$$

- Surjective. Let $y = h(x)$, now find x

$$\begin{aligned} y &= \frac{ax-b}{cx-d} \\ cxy - dy &= ax - b \\ cxy - ax &= dy - b \\ x(cy-a) &= dy - b \\ x &= \frac{dy-b}{cy-a} \end{aligned}$$

  We now need to show that $x \neq \frac{d}{c}$ (and so is in the domain), and we can do so by considering

$$\begin{aligned} x - \frac{d}{c} &= \frac{dy-b}{cy-a} - \frac{d}{c} \\ &= \frac{dcy - bc - dcy + da}{c(cy-a)} \\ &= \frac{ad-bc}{c(cy-a)} \end{aligned}$$

  Now since $ad \neq bc$ and $y \neq \frac{a}{c}$, this is never zero. Hence this choice of x really does lie in the domain of the function.

Proof of Result 10.4.14. We need to show that h is both injective and surjective.

- Let $y \in \mathbb{R} - \frac{a}{c}$. Pick $x = \frac{dy-b}{cy-a} = \frac{d}{c} + \frac{ad-bc}{c(cy-a)}$. Since $\frac{ad-bc}{c(cy-a)} \neq 0$ for any $y \in \mathbb{R} - \left\{\frac{a}{c}\right\}$, this choice of x is in the domain of the function. Now

$$\begin{aligned} h(x) &= \frac{a\frac{dy-b}{cy-a} - b}{c\frac{dy-b}{cy-a} - d} \\ &= \frac{a(dy-b) - b(cy-a)}{c(dy-b) - d(cy-a)} \\ &= \frac{y(ad-bc)}{ad-bc} = y \end{aligned}$$

  Hence for any y in the co-domain, there is an x in the range such that $h(x) = y$. So the function is surjective.

- Now let x, y be two elements of the range such that $h(x) = h(y)$. Hence

$$\frac{ax-b}{cx-d} = \frac{ay-b}{cy-d}$$

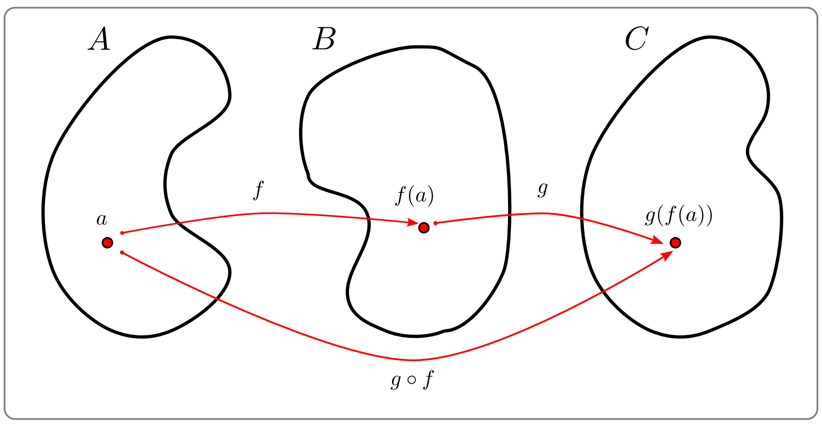
$$\begin{aligned}(cy-d)(ax-b) &= (ay-b)(cx-d) && \text{since denominator} \neq 0\\ cax - cby - dax + db &= acxy - day - bcx + db \\ (ad-bc)y &= (ad-bc)x\end{aligned}$$

Hence $x = y$. Thus if $h(x) = h(y)$ we must have $x = y$ and so h is injective.

Since the function is both injective and surjective, it is bijective as required. ■

10.5 Composition of functions

Our last step before defining inverse functions is to explain a generic way of combining functions. Now since we are dealing with general sets and not just sets of numbers, we can't add or subtract or divide or differentiate or any of the things we usually do with functions in calculus courses. Really the only thing we can with our abstract functions defined on abstract sets is **composition** — that is, take an element, apply the first function and then apply the second function.



Definition 10.5.1 Let $f : A \to B$ and $g : B \to C$ be two functions. The composition of f and g is denoted $g \circ f$ which we read "g of f". It defines a new function

$$g \circ f : A \to C \qquad (g \circ f)(a) = g(f(a)) \qquad \forall a \in A$$

◊

This standard notation for compositions looks a bit backwards — we read things from left to right, but when we actually evaluate the composition we do the rightmost function first.

$$(h \circ g \circ f)(x) = h(g(f(x)))$$

We start with x, apply f, then apply g to the result, and finally apply h to the result of that.

It is important to note that composition is not, in general, commutative:

$$g \circ f \neq f \circ g.$$

But it is associative

Theorem 10.5.2 *Let $f : A \to B$, $g : B \to C$ and $h : C \to D$ be functions. Then $h \circ (g \circ f) = (h \circ g) \circ f$.*

The proof of associativity is not difficult but is quite long; we leave it to the interested reader to work through it. Instead we'll look at the following useful (and nice) theorem. This tells us that composition of functions interacts nicely with injections, surjections and bijections.

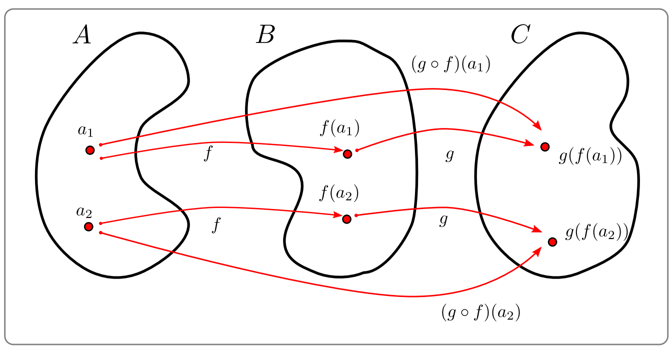
Theorem 10.5.3 *Let $f : A \to B$ and $g : B \to C$ be functions.*

- *If f and g are injective then so is $g \circ f$.*
- *If f and g are surjective then so is $g \circ f$.*

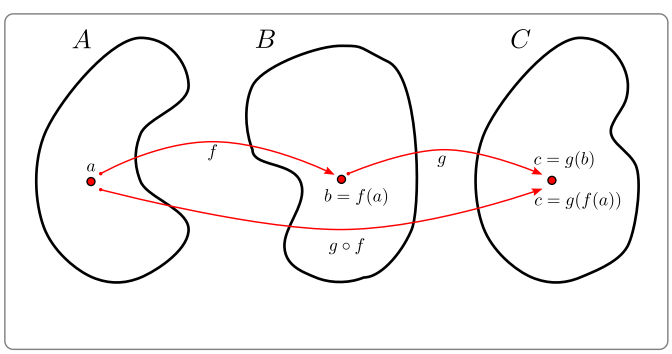
Consequently if f, g are bijective then so is $g \circ f$.

Scratch work:

- Injective: Assume both f and g are injective. So if $a_1 \neq a_2 \in A$ then $f(a_1) \neq f(a_2)$. Similarly if $b_1 \neq b_2$ then $g(b_1) \neq g(b_2)$. We can just put these together. If $a_1 \neq a_2$ then $f(a_1) \neq f(a_2)$ and so $g(f(a_1)) \neq g(f(a_2))$. Thus $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. The diagram below should help.



- Surjective: Assume both f and g are surjective. Then for each $c \in C$ there is some $b \in B$ such that $g(b) = c$. Similarly for each $b \in B$ there is some $a \in A$ such that $f(a) = b$. Thus $g(f(a)) = c$. Again, we refer the reader to the diagram below.



- Bijectiveness follows from surjectiveness and injectiveness. That is, if f, g are both bijective, then they are both injective and surjective. Hence their composition $g \circ f$ is injective and surjective, and so bijective.

We are ready to write things up nicely for the reader.
Proof of Theorem 10.5.3. It suffices to prove the first two points, since the final point follows immediately from them.

- Let f, g be injective functions. And let $a_1, a_2 \in A$ such that $a_1 \neq a_2$. Since f is injective, it follows that $f(a_1) \neq f(a_2)$. And since g is injective it followst that $g(f(a_1)) \neq g(f(a_2))$. Thus $(g \circ f)(a_1) \neq (g \circ f)(a_2)$. Thus $g \circ f$ is injective.
- Let f, g be surjective functions and let $c \in C$. Since g is surjective, $g(b) = c$ for some $b \in B$. Since f is surjective, there is some $a \in A$ such that $f(a) = b$. It follows that $g(f(a)) = c$ and so $g \circ f$ is surjective.

■

Here is another nice result about compositions, injections and surjections. In particular, if we know the composition $g \circ f$ is injective, then what can we say about f, g. Similarly, if $g \circ f$ is surjective, then what can we say about f, g. Similarly

Theorem 10.5.4 *Let $f : A \to B$ and $g : B \to C$ be functions. Then*

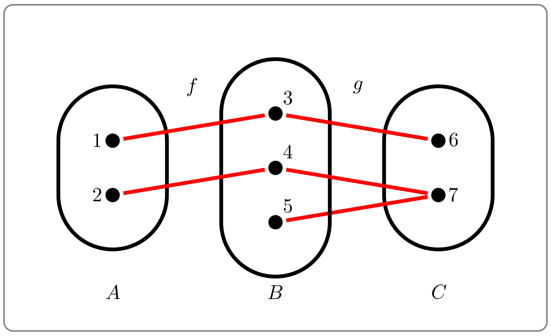
- *If $g \circ f$ is injective then f is injective*
- *If $g \circ f$ is surjective then g is surjective*

Proof. We prove each in turn.

- Assume that $g \circ f$ is injective, and let $a_1, a_2 \in A$ so that $f(a_1) = f(a_2)$. To show that f is injective it suffices to show that $a_1 = a_2$. Since $f(a_1) = f(a_2)$, we know that $g(f(a_1)) = g(f(a_2))$, and since $g \circ f$ is injective we have that $a_1 = a_2$.
- Now assume that $g \circ f$ is surjective and let $c \in C$. To prove that g is surjective it suffices to find $b \in B$ so that $g(b) = c$. Since $g \circ f$ is surjective, we know that there is $a \in A$ so that $g(f(a)) = c$. Now set $b = f(a)$. Then $g(b) = g(f(a)) = c$ as required.

■

Example 10.5.5 The above theorem proves that when $g \circ f$ is injective, we know that f is injective, the following example show that g need not be injective. Further, it also shows that just because $g \circ f$ and g are surjective, we need not have that f is surjective.



Let $A = \{1, 2\}, B = \{3, 4, 5\}, C = \{6, 7\}$ and consider the following functions

$$\begin{array}{ll} f : A \to B & f(1) = 3, \quad f(2) = 4 \\ g : B \to C & g(3) = 6, \quad g(4) = 7, \quad g(5) = 7 \\ g \circ f : A \to C & g(f(1)) = 6, \quad g(f(2)) = 7 \end{array}$$

Notice that f and $g \circ f$ are injective, but g is not injective since $g(4) = g(5)$. Additionally, g and $g \circ f$ are surjective, but f is not surjective. $\square$

10.6 Inverse functions

We now have enough machinery to start working on inverse functions. Consider what an inverse *function* needs to do. If we start with $a \in A$ and apply a function $f : A \to B$ then we obtain some element $b \in B$. We want our inverse to "undo" this and take b back to a. We'll start by defining functions that are *nearly* inverses and give a few examples.

But before we do that, we note that some of the material below is a bit technical. The reader who is interested in these details should continue on. The reader who wishes to just get to the main results should instead skip ahead to Definition 10.6.6 and Theorem 10.6.8

Definition 10.6.1 Recall Definition 10.4.12, and let $f : A \to B$ and $g : B \to A$ be functions.

- If $g \circ f = i_A$ then we say that g is a **left-inverse** of f.
- Similarly, if $f \circ g = i_B$ then we say that g is a **right-inverse** of f.

$\diamondsuit$

So notice that if we start at some point $a \in A$ and apply f to get $b \in B$, then a left-inverse g tells us how to get back from b to a:

$$g(b) = g(f(a)) = a$$

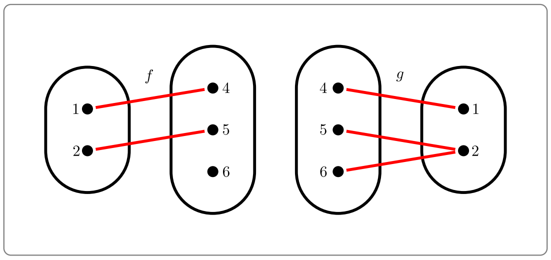
On the other hand, if are trying to get to a particular point $b \in B$ in the codomain using f, then the right-inverse tells you a possible starting point $a \in A$:

$$g(b) = a \qquad \text{so that} \qquad f(a) = f(g(b)) = b$$

Example 10.6.2 Let $A = \{1, 2\}$ and $B = \{4, 5, 6\}$ and define

$$f : A \to B \qquad f(1) = 4, f(2) = 5$$
$$g : B \to A \qquad g(4) = 1, g(5) = 2, g(6) = 2$$

as depicted below.



Then notice that $g \circ f : A \to A$ satisfies

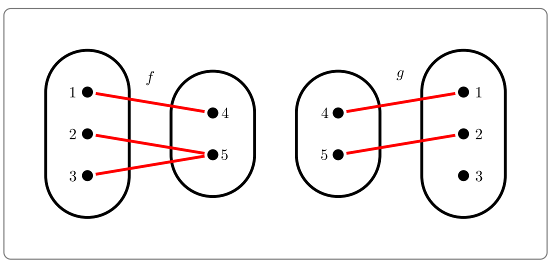
$$g(f(1)) = g(4) = 1 \qquad \text{and} \qquad g(f(2)) = g(5) = 2.$$

That is $g \circ f = i_A$ and so is a left-inverse of f. At the same time, $f \circ g : B \to B$ satisfies

$$f(g(4)) = f(1) = 4 \qquad f(g(5)) = f(2) = 5 \qquad \text{but} \qquad f(g(6)) = f(2) = 5$$

and so g is not a right-inverse of f.

By swapping the roles of f, g in the above we can construct a function that is a right-inverse but not a left-inverse. Consider the functions defined in the image below.



Then we see that

$$g(f(1)) = g(4) = 1 \qquad g(f(2)) = g(5) = 2 \qquad \text{but} \qquad g(f(3)) = g(5) = 2$$

and so g is not a left-inverse of f. And then

$$f(g(4)) = f(1) = 4 \qquad \text{and} \qquad f(g(5)) = f(2) = 5$$

making g a right-inverse of f. □

Notice in the above example, that the function that has a left-inverse is injective, while the function with the right-inverse is surjective. This is not a coincidence as the following two lemmas prove.

Lemma 10.6.3 *Let $f : A \to B$, then f has a left-inverse if and only if f is injective.*

Proof. We prove each implication in turn.

- Assume that f has a left-inverse, g. Now let $a_1, a_2 \in A$ so that $f(a_1) = f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$, but since g is the left-inverse of f, we know that $g(f(a_1)) = a_1$ and $g(f(a_2)) = a_2$. Thus $a_1 = a_2$ and so f is injective.

- Now let f be injective. We construct a left-inverse of f in two steps. First pick any $\alpha \in A$. Then consider the preimage of a given point $b \in B$. That preimage, $f^{-1}(\{b\})$, is empty or not.

  - If $f^{-1}(\{b\}) = \varnothing$, then define $g(b) = \alpha$
  - Now assume that $f^{-1}(\{b\}) \neq \varnothing$. Since f is injective, the preimage $f^{-1}(\{b\})$ contains exactly 1 element. To see why, consider a, c both in the preimage. We must have $f(c) = f(a) = b$ (since they are both in the preimage of b), but since f is an injection, we must have $c = a$. So define $g(b) = a$ the unique element in the preimage.

  To summarise

  $$g(b) = \begin{cases} \alpha & \text{if preimage empty} \\ a & \text{otherwise take unique } a \text{ in the preimage} \end{cases}.$$

  Now let $a \in A$, under f it maps to some $b \in B$ with $b = f(a)$. Hence (as argued above) a is the unique element in the preimage of b, and so $g(f(a)) = g(b) = a$. Thus g is a left-inverse of f.

■

Lemma 10.6.4 *Let $f : A \to B$, then f has a right-inverse if and only if f is surjective.*

Proof. We prove each implication in turn.

- Assume that f has a right-inverse, g. Now let $b \in B$ and set $a = g(b)$. Then $f(a) = f(g(b)) = b$ and so f is surjective.
- Now let f be surjective and let $b \in B$. For the sake of this proof, let us denote the preimage of b as

  $$A_b = \{a \in A \mid f(a) = b\}.$$

  Since f is surjective, we know that $A_b \neq \varnothing$ for every $b \in B$. So now define $g(b)$ to be any[138] element of A_b.

  Now let $b \in B$, then under g it maps to some $a \in A$ so that (by construction) $f(a) = b$. Hence $f(g(b)) = f(a) = b$ and thus g is a right-inverse as required.

■

These lemmas tell us that a function has both a left inverse and right inverse if and only if it is bijective. We can go further those one-sided inverses are actually the same function.

Lemma 10.6.5 *Let $f : A \to B$ have a left-inverse, $g : B \to A$ and a right inverse $h : B \to A$, then $g = h$. Further, the function f has a left and right inverse if and only if f is bijective.*

Proof. Let f, g, h be as stated. Then we know that

$$g \circ f = i_A \qquad \text{and} \qquad f \circ h = i_B$$

Now starting with g we can write:

$$\begin{aligned} g &= g \circ i_B \\ &= g \circ (f \circ h) = (g \circ f) \circ h \\ &= i_A \circ h = h \end{aligned}$$

and thus $g = h$ as required.

The last part of the lemma follows by combining the previous two lemmas.

■

So this lemma tells us conditions under which a function will have both a left- and right-inverse, and that those one-sided inverses are actually the same function. A function that is a left- and right-inverse is a (usual) inverse.

Definition 10.6.6 Let $f : A \to B$ and $g : B \to A$ be functions. If $g \circ f = i_A$ and $f \circ g = i_B$ then we say that g is an **inverse** of f.

Note that we will prove that the inverse is unique, and so we *will* be able to

[140]That one can do this is not as obvious as it might seem. In particular, if B is infinite we need the Axiom of Choice in order to make this selection. The interested reader should search engine their way to more information on this. Now in the event that our function f is injective, then A_b contains exactly one element and we don't need the Axiom of Choice to construct our function. Thankfully we apply this result when our function is bijective — phew.

say that g is *the* inverse of f and denote it f^{-1}.

Also note that if a function is an inverse then it is also a left- and right-inverse. ♢

Lemma 10.6.7 *If a function $f : A \to B$ has an inverse, then that inverse is unique.*

Proof. This proof is very similar to the proof of Lemma 10.6.5. Let $g : B \to A$ and $h : B \to A$ both be inverses to the function f. Then

$$\begin{aligned} g &= g \circ i_B \\ &= g \circ (f \circ h) = (g \circ f) \circ h \\ &= i_A \circ h = h \end{aligned}$$

and so $g = h$. Thus the inverse is unique. ■

We can now state our main theorem about inverse functions.

Theorem 10.6.8 *Let $f : A \to B$.*

- *The function f has an inverse function if and only if it is bijective*
- *The inverse of f, if it exists, is unique.*

Proof. We combine some of the lemmas above to prove this result.

- Assume that f has an inverse. Then that inverse is both a left-inverse and a right-inverse. Lemma 10.6.5 then implies that f is both injective and surjective, and so is bijective.

  Now assume that f is bijective. Then Lemma 10.6.5 tells us there exists a function g that is a left-inverse and right-inverse for f. Then, by definition g is an inverse for f.

- The uniqueness of the inverse is proven by Lemma 10.6.7.

■

Theorem 10.6.8 tells us under what circumstances a function has an inverse. However, it does not tell us if that inverse has a nice expression. If the original function is nice enough, then we may be able to state the inverse nicely. Here are a couple of such examples.

Example 10.6.9 The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 7x - 3$ is bijective and so has an inverse function. We proved this in Result 10.4.2 and Result 10.4.2. The inverse is $f^{-1} : \mathbb{R} \to \mathbb{R}$ and we can work out a formula for it by solving $y = f(x)$ for x in terms of y. Notice that we did exactly that when we proved that f was surjective. In particular, we found that

$$f^{-1} : \mathbb{R} \to \mathbb{R} \qquad \text{defined by} \qquad f^{-1}(y) = \frac{y+3}{7}.$$

To verify that this is correct it suffices to show that $f^{-1} \circ f$ is the identity function:

$$f^{-1} \circ f(x) = f^{-1}(7x - 3)$$

$$= \frac{(7x-3)+3}{y} = x$$

as required. □

Example 10.6.10 Möbius continued. In Result 10.4.14 above we saw that a Möbius transformation $h : \mathbb{R} - \left\{\frac{d}{c}\right\} \to \mathbb{R} - \left\{\frac{a}{c}\right\}$ defined by

$$h(x) = \frac{ax-b}{cx-d}$$

is bijective. The above result tells us that it has an inverse function. We can verify that the inverse is $h^{-1} : \mathbb{R} - \left\{\frac{a}{c}\right\} \to \mathbb{R} - \left\{\frac{d}{c}\right\}$ defined by

$$h^{-1}(y) = \frac{dy-b}{cy-a}.$$

(which we computed while proving the result). We simply need to show that $h^{-1} \circ h$ is the identity:

$$\begin{aligned} h^{-1}(h(x)) &= h^{-1}\left(\frac{ax-b}{cx-d}\right) \\ &= \frac{d\frac{ax-b}{cx-d} - b}{c\frac{ax-b}{cx-d} - a} \\ &= \frac{d(ax-b) - b(cx-d)}{c(ax-b) - a(cx-d)} \\ &= \frac{(ad-bc)x}{ad-bc} = x \end{aligned}$$

as required. □

10.7 (Optional) The axiom of choice

Consider the following, not terribly controversial, statement

> Given a non-empty set A, we can pick an element from it.

This is almost trivial. The fact that $A \neq \varnothing$ is equivalent to the statement $\exists a \in A$. So, we can simply take *that* element a, and we are done.

Let's turn up the complexity a little:

> Given two non-empty sets A, B, we can pick one element from each.

This is no harder, since A is non-empty, we can take $a \in A$. And since $B \neq \varnothing$ we can take $b \in B$. And, at this point, we need to start phrasing things a little differently so that we can be a little more formal and a little more careful.

> Given two sets A, B there exists a function $f : \{A, B\} \to A \cup B$

That is, our *choosing* of elements from A and B is really just a function that takes us from the collection $\{A, B\}$ to a specific elements $a, b \in A \cup B$. Similarly, if such a function exists, then we can use it to choose specific elements. We call such functions **choice functions**.

Definition 10.7.1 Choice function. Let $\mathcal{S}$ be a collection of non-empty sets. Then a **choice function** on $\mathcal{S}$ is a function

$$f : \mathcal{S} \to \bigcup_{X \in S} X$$

so that, for any $X \in \mathcal{S}$, $f(X) \in X$. That is, for any set X in our collection $\mathcal{S}$, the **choice function** f chooses an element $f(X) = x \in X$. ◊

This definition allows us to rephrase the above statements as

- A collection of a single set $\{A\}$ always has a choice function, and
- A collection of two sets $\{A, B\}$ always has a choice function.

This is quite easily extended to any finite collection of non-empty sets. Note that while the collection must be finite, the sets in the collection can be infinite.

Result 10.7.2 *Let* $\mathcal{S} = \{A_i \text{ s.t. } i \in \{1, 2, \ldots, n\}\}$ *be a finite collection of non-empty sets. Then there exists a choice function on* $\mathcal{S}$.
Proof. We prove this by induction.

- Let $\mathcal{S} = \{A\}$ consist of a single non-empty set A. Since A is non-empty, there is some $a \in A$. The function

  $$f : \{A\} \to A \qquad f(A) = a$$

  is a choice function on $\mathcal{S}$. Thus the statement is true for $|\mathcal{S}| = 1$.

- Now assume that the statement hold for all collections of k non-empty sets, and let $\mathcal{T} = \{A_i \text{ s.t. } i \in \{1, 2, \ldots, k + 1\}\}$. Since $A_{k+1} \neq \varnothing$ there is some $q \in A_{k+1}$.

  Then, by assumption, the collection $\mathcal{S} = \{A_i \text{ s.t. } i \in \{1, 2, \ldots, k\}\}$ has a choice function f. We can then use this to define the required choice function g:

  $$g(A_i) = \begin{cases} f(A_i) & i = 1, 2, \ldots, k \\ q & i = k + 1 \end{cases}$$

Then, by induction, the statement holds for any finite collection of non-empty sets. ■

The existence of such choice-functions is intuitively quite obvious. I can always grab an element out from a set, so I can grab an element out from each set in turn. Indeed, it is equivalent to the statement that the Cartesian product of a finite number of non-empty sets is also non-empty.

Result 10.7.3 *Let $A_1, A_2, \ldots, A_n$ be non-empty sets. The the collection $\{A_1, \ldots, A_n\}$ has a choice function if and only if the Cartesian product $A_1 \times A_2 \times \cdots \times A_n$ is non-empty.*

Proof. Let the A_i be as stated. We then prove each implication in turn.

Assume that the collection $\{A_1, \ldots, A_n\}$ has a choice function, f. We can use that to select $f(A_i) = a_i \in A_i$ for $i = 1, 2, \ldots, n$. Hence $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$. Thus the product is non-empty.

Similarly, assume that the product $A_1 \times A_2 \times \cdots \times A_n \neq \varnothing$, and hence there is $(a_1, \ldots a_n) \in A_1 \times \cdots \times A_n$. We use that element to define

$$f : \{A_1, \ldots, A_n\} \to \cup A_i \qquad f(A_i) = a_i$$

giving the required choice function. ■

Where things become really very non-trivial, and the consequences very non-intuitive, is when we have infinite collections of sets. Our inductive argument above can't get us there — it cannot make the leap from large, but *finite* collections, to infinite collections.

Of course, if we the sets in our infinite collection are nice and have extra structure, then this might be easy. For example,

- A collection of subsets of $\mathbb{N}$ — just choose the smallest element of each subset (via the well-ordering principle).
- A collection of sets of English words — just choose the words that come first in alphabetic order[139].
- A collection of pairs of shoes — just choose the left shoe of each pair.

This last example is very famous and is due to Bertrand Russell[140]. The second half of the example points out that it is far from obvious how to do the same with an infinite collection of pairs of socks.

Indeed, for an infinite collection of non-empty sets, without extra structure, the existence of a choice function is taken as an axiom — the Axiom of Choice.

Axiom 10.7.4 Axiom of choice. *Let $\mathcal{S}$ be any collection of non-empty sets. Then there exists a choice function on $\mathcal{S}$.*

This statement feels so intuitively true, it was used quite implicitly until 1904 when Zermelo realised that the question of the existence of choice functions was not at all trivial. Indeed, it was subsequently shown that Axiom of Choice cannot be proved or disproved using usual set theory[141]. To be more precise, 1938 Kurt

[139] More formally, we pick the lexicographic least word from each subset. Lexicographic ordering is really useful and the interested reader should search-engine their way to more on this topic.

[140] No footnote can even begin to do justice to the many contributions of Russell to logic and mathematics and many other disciplines. The reader should search-engine their way to more information.

[141] By which we mean Zermelo-Fraenkel set theory, which is, roughly speaking, the formalisation of the usual notions of set theory, including those in this text.

Gödel proved that one can not disprove the existence of such a choice function using the standard axioms of set theory, while in 1963 Paul Cohen proved that the existence cannot be proven either. It is now accepted[142] as a standard part of set theory.

The Axiom of Choice 10.7.4 is equivalent to the statement that the Cartesian product of any collection of non-empty sets is itself non-empty — this seems reasonable and hardly controversial. However, the Axiom of Choice does have some very strange implications.

- Well-ordering theorem — every set can be well-ordered. That is, one can define an ordering of the elements of any set so that any subset has a first element! Cantor conjectured this result in 1883 but it was proved Zermelo in 1904. It was in that proof that the Axiom of Choice was first formalised. It is also known as Zermelo's theorem.
- Banach-Tarski paradox — it is possible to decompose a solid ball into finitely many pieces and reassemble them into two solid balls each having the same volume as the original!
- It allows you to predict the result of coin tosses — see this nice article[143] by Matt Baker. The interested reader should also examine a very nice (and somewhat provocative) paper[144] by Hardin and Taylor push this line of reasoning explaining how you can use the Axiom of Choice to predict future values of real-valued functions[145]. Here[146] is a nice and more accessible description of the result by Michael O'Connor.

The Axiom of Choice is an extremely interesting and complicated topic, and, well beyond the scope of this text; the interested reader should search-engine their way to more information[147].

10.8 Exercises

1. Is the set
$$\theta = \{((x, y), (5y, 4x, x + y)) : x, y \in \mathbb{R}\}$$
a function? If so, what is its domain and its range?

2. For which values of $a, b \in \mathbb{N}$ does the set $\phi = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : ax + by = 6\}$ define a function?

[142] By most mathematicians in most contexts. There is, however, an interesting body of research on what happens when the Axiom of Choice is false. Very strange things happen — the interested reader should search engine their way to more information.

[143] https://mattbaker.blog/2015/01/17/spooky-inference-and-the-axiom-of-choice/

[144] https://www.tandfonline.com/doi/abs/10.1080/00029890.2008.11920502

[145] Such as temperatures, stock-market prices, position of balls on roulette tables, etc.

[146] https://xorshammer.com/2008/08/23/set-theory-and-weather-prediction/

[147] There are many articles out there on this topic, but the authors found this blog to be a very nice discussion of the Axiom of Choice.

3. Let $f : \mathbb{R} \to \mathbb{R}$ be a function which is defined by $f(x) = \dfrac{2x}{1+x^2}$. Show that $f(\mathbb{R}) = [-1, 1]$.

4. Consider the following functions and their images and preimages.

(a) Consider the function $f : \{1, 2, 3, 4, 5, 6, 7\} \to \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ given as

$$f = \{(1, 3), (2, 8), (3, 3), (4, 1), (5, 2), (6, 4), (7, 6)\}.$$

Find: $f\big(\{1, 2, 3\}\big)$, $f\big(\{4, 5, 6, 7\}\big)$, $f(\emptyset)$, $f^{-1}\big(\{0, 5, 9\}\big)$ and $f^{-1}\big(\{0, 3, 5, 9\}\big)$.

(b) Let $g : \mathbb{R} \to \mathbb{R}$ be defined by $g(x) = 4x^2 - x - 3$.

Find: $g\left(\left\{\frac{1}{8}\right\}\right), g^{-1}(\{0\})$, $g((-1, 0) \cup [3, 4])$, and, $g^{-1}([-10, -5))$.

(c) Define $h : \mathbb{R} \to \mathbb{R}$ by $h(t) = \sin(2\pi t)$.

Find: $h(\mathbb{Z})$, $h\left(\left\{\frac{1}{4}, \frac{7}{2}, \frac{19}{4}, 22\right\}\right)$, $h^{-1}(\{1\})$, and $h^{-1}([0, 1))$.

5. Let A, B be sets and $f : A \to B$ be a function from $A$to B. Then prove that if E and F are subsets of B, then

$$f^{-1}(E - F) = f^{-1}(E) - f^{-1}(F).$$

Remember that since we do not know whether or not f is a bijection, f^{-1} denotes the preimage of f not its inverse.

6. Let $f : \mathbb{R} \to \mathbb{R}$ be the function defined by $f(x) = x^2 + ax + b$, where $a, b \in \mathbb{R}$. Determine whether f is injective and/or surjective.

7. Determine all functions $f : \mathbb{N} \to \mathbb{N}$ that are injective and such that for all $n \in \mathbb{N}$ we have $f(n) \leq n$.

8. Prove that $f : [3, \infty) \to [5, \infty)$, defined by $f(x) = x^2 - 6x + 14$ is a bijective function.

9. For $n \in \mathbb{N}$, let $A = \{a_1, a_2, a_3, \cdots, a_n\}$ be a fixed set where $a_j \neq a_i$ for any $i \neq j$, and let F be the set of all functions $f : A \to \{0, 1\}$.

What is $|F|$, the cardinality of F?

Now, for $\mathcal{P}(A)$, the power set of A, consider the function $g : F \to \mathcal{P}(A)$, defined as

$$g(f) = \{a \in A : f(a) = 1\}.$$

Is g injective? Is g surjective?

10. Let $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be defined by $f(n) = (2n + 1, n + 2)$. Check whether this function is injective and whether it is surjective. Prove your answer.

11. Let $f : E \to F$ be a function. We recall that for any $A \subseteq E$ the image of A by f, namely $f(A)$, is defined as

$$f(A) = \{f(x) : x \in A\}.$$

Show that f is surjective if and only if

$$\forall A \in \mathcal{P}(E),\ F - f(A) \subseteq f(E - A).$$

12. Let $f : C \to D$ be a function. Let $A, B \subset C$ be nonempty sets. Prove that if f is injective, then $f(A - B) = f(A) - f(B)$.

13. Consider the function

$$f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad \text{where} \qquad f(x, y) = 2^{x-1}(2y - 1).$$

Prove that f is bijective.

14. Let A, B be nonempty sets. Prove that if there is a bijection $f : A \to B$, then there is a bijection from $\mathcal{P}(A)$, the power set of A, to $\mathcal{P}(B)$, the power set of B.

15. Let $\mathcal{R}$ be the relation on $\mathbb{R}^2$ defined by

$$(x, y)\ \mathcal{R}\ (s, t) \text{ iff } x^2 + y^2 = s^2 + t^2$$

where $(x, y), (s, t) \in \mathbb{R}^2$.

(a) Show that $\mathcal{R}$ is an equivalence relation

(b) Let $\mathcal{S}$ be the set of equivalence classes of the relation $\mathcal{R}$ defined in part (a). Let f be defined by

$$f : \mathcal{S} \to [0, \infty) \qquad \text{with} \qquad f([(x, y)]) = \sqrt{x^2 + y^2}.$$

Prove that

- f is a function, and, further
- f is bijective.

16. Let $n \in \mathbb{N}$ with $n > 1$ and let $\mathbb{Z}_n$ be the set of equivalence classes modulo n. For any $x \in \mathbb{Z}$, let $[x]_n \in \mathbb{Z}_n$ denote its equivalence class modulo n.

Define the function $f : \mathbb{Z}_n \to \{0, 1, \ldots, n - 1\}$ by $f([x]_n) = r$, where r is the remainder of x upon division by n.

(a) Show that f is well-defined, meaning that f is defined on its whole domain and that f does not depend on the choice of representative for each equivalence class; i.e. $[x]_n = [y]_n \implies f([x]_n) = f([y]_n)$.

(b) Show that f is a bijection.

This question explains why when dealing with equivalence classes of integers modulo n, we often consider the set of representatives $\{0, 1, \ldots, n - 1\}$ instead.

17. Consider $f : A \to B$. Prove that f is injective if and only if $X = f^{-1}(f(X))$ for all $X \subseteq A$.

18. Consider $f : A \to B$. Prove that f is surjective if and only if $f(f^{-1}(Y)) = Y$ for all $Y \subseteq B$.

19. We say that a function $f : \mathbb{R} \to \mathbb{R}$ is *strictly increasing* if whenever $x_1 < x_2$ we have $f(x_1) < f(x_2)$. Similarly, a function $g : \mathbb{R} \to \mathbb{R}$ is *strictly decreasing* if whenever $x_1 < x_2$ we have $g(x_1) > g(x_2)$.

(a) Prove that the composition of two strictly increasing functions is strictly increasing.

(b) Prove that the composition of two strictly decreasing functions is strictly increasing.

20. Let f, g, and h be functions from $\mathbb{R} \to \mathbb{R}$. We define the following operations on functions:

- Function addition: $(f + g)(x) = f(x) + g(x)$
- Function division: $\left(\frac{f}{g}\right)(x) = \frac{f(x)}{g(x)}$
- Function composition: $(f \circ g)(x) = f(g(x))$

Note that under this definition, $\left(\frac{1}{f}\right)(x) = \frac{1}{f(x)}$. This is NOT the inverse of $f(x)$.

Prove or give a counterexample to the following statements:

(a) $f \circ (g + h) = f \circ g + f \circ h$ for every $x \in \mathbb{R}$.

(b) $(g + h) \circ f = g \circ f + h \circ f$ for every $x \in \mathbb{R}$.

(c) $\frac{1}{f \circ g} = \frac{1}{f} \circ g$ for every $x \in \mathbb{R}$.

(d) $\frac{1}{f \circ g} = f \circ \frac{1}{g}$ for every $x \in \mathbb{R}$.

21. Find counterexamples to the following statements:

(a) Given a function $f : A \to B$ and subsets $W, X \subseteq A$, we have $f(W \cap X) = f(W) \cap f(X)$.

(b) Given a function $f : A \to B$ and a subset $Y \subseteq B$, we have $f(f^{-1}(Y)) = Y$.

Explain your answers.

22. Let A, B be nonempty sets. Let f, h be functions from A to B, and let g be a function from B to A.

(a) Suppose that g is injective. Prove that if $g \circ f = g \circ h$, then $f = h$.

(b) Suppose that g is surjective. Prove that if $f \circ g = h \circ g$, then $f = h$.

23. Consider the following functions and their compositions.

(a) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x + 1$. Does there exist a function

$g : \mathbb{R} \to \mathbb{R}$ such that $(f \circ g)(x) = (g \circ f)(x)$ for every $x \in \mathbb{R}$?

(b) Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = c$ for some $c \in \mathbb{R}$ (i.e. f is a constant function). Which functions $g : \mathbb{R} \to \mathbb{R}$ have the property $(f \circ g)(x) = (g \circ f)(x)$ for every $x \in \mathbb{R}$?

(c) Let $f : \mathbb{R} \to \mathbb{R}$. Suppose $(f \circ g)(x) = (g \circ f)(x)$ for every $x \in \mathbb{R}$ and for every function $g : \mathbb{R} \to \mathbb{R}$. Show that $f(x) = x$.

24. Let A be a nonempty set and $f : A \to A$ be a function.

(a) Prove that f is bijective if $f \circ f$ is bijective.

(b) Let

$$f : (0, \infty) \to (0, \infty) \qquad f(x) = \log\left(\frac{e^x + 1}{e^x - 1}\right)$$

where $\log(x)$ denotes the natural logarithm of x. Use part (a) to prove that this is a bijective function.

25. Prove that the function

$$f : \mathbb{R} - \{-2\} \to \mathbb{R} - \{1\}, \text{ defined by } f(x) = \frac{x+1}{x+2}$$

is bijective and find its inverse.

26. Let $f : \mathbb{Z} \to \mathbb{Z}$ defined so that $f(n) = -n + 3$ if n is even and $f(n) = n + 7$ if n is odd. Prove that f is bijective and find its inverse, f^{-1}.

27. The following question concerns the triple composition of a function.

(a) Let A be a non-empty set and let $g : A \to A$ be a function that satisfies $g \circ g \circ g = i_A$, where i_A is the identity function on the set A. Prove that g must be bijective.

(b) Let $A = \mathbb{R} - \{0, 1\}$ and let $f : A \to A$ be defined by $f(x) = 1 - \frac{1}{x}$. Show that $f \circ f \circ f = i_A$.

(c) Use part (a) to conclude that f is bijective and determine its inverse function f^{-1}.

Chapter 11

Proof by contradiction

Proof by contradiction is another general proof technique like direct proofs and the contrapositive proofs. When you first encounter proof by contradiction it can seem rather mysterious:

- Assume to be true something we know is false, then
- prove garbage, then
- from this deduce truth!

But after you get the hang of it, proof by contradiction becomes indispensable.

Warning 11.0.1 Not everything is a nail. One of the reasons that the authors have left this topic until quite late in the text is that we find that students try to use this method for *everything*. Remember, contradiction is just another method in our toolbox and just because we have a shiny new hammer, not every result is a nail[148]. Please do not forget the other proof techniques.

With that warning out of the way, what is proof by contradiction and how does it differ from other techniques? Well, roughly speaking, when we use proof by contradiction, we do not seek to prove a statement P to be true, but rather we prove that $(\sim P)$ is false.This might seem to be a delicate and pedantic distinction, but it does make the structure of the resulting proof very different from direct and contrapositive proofs.

Once we know that $(\sim P)$ is false we can deduce that P is true. To do so we rely on the **law of the excluded middle**[149] which states that a statement must either be true or its negation must be true:

$$(P \vee (\sim P)) \text{ is a tautology}$$

[150]Remember the Law of the Instrument (or look it up with your favourite search engine).

[149]Being middle child, one of the authors finds it difficult to not think of the law of the excluded middle as being some sort of analysis of birth-order and family dynamics. The interested reader should continue to the next section of the text in which we discuss it further. "It" being the law of the excluded middle and not anything to do with middle-child syndrome.

and also **modus tollens**[150]. Remember modus ponens is:

$$((P \implies Q) \wedge P) \implies Q$$

Modus tollens is (roughly speaking) applying modus ponens to the contrapositive:

$$((P \implies Q) \wedge \sim Q) \implies (\sim P)$$

So if we know that an implication $P \implies Q$ is true, and the conclusion Q is false, then the hypothesis P must be false[151].

So how do we put these things together to make a proof by contradiction?

11.1 Structure of a proof by contradiction

Say we wish to prove a statement P to be true. Since

$$(P \vee (\sim P)) \text{ is a tautology,}$$

either we must have P is true or $(\sim P)$ is true.

- Tell the reader something like "We will prove this by contradiction" otherwise the next step looks like a mistake.
- We assume that $(\sim P)$ is true, and then show that this leads to a falsehood — a contradiction — garbage.
- That is, we will construct a change of implications like:

$$\begin{aligned}
(\sim P) &\implies P_1 && \text{and} \\
P_1 &\implies P_2 && \text{and} \\
P_2 &\implies P_3 && \text{and} \\
&\vdots \\
P_{n-1} &\implies P_n && \text{and} \\
P_n &\implies \text{CONTRADICTION}
\end{aligned}$$

- The contradiction is a statement that is always false — for example

  $$R \wedge (\sim R).$$

  But which contradiction do we aim for? Let's discuss that shortly.
- Since the contradiction is false, and all of those implications are true, we must have P_n is false (modus tollens).

[150] or "denying the consequent" as it is known in less latin moments.

[151] The skeptical reader should take a quick glimps at the truth table to see why this is so.

- Similarly, since P_n is false, we know P_{n-1} is false (again, modus tollens).
- Keep on moving back up the chain of implications, and we see that $(\sim P)$ must be false.
- Thus[152] P is true.

When when we write this up neatly for the reader we arrive at a proof that looks like the following:
Generic proof-by-contradiction proof. We prove this result by contradiction. So assume, to the contrary $(\sim P)$.

- A chain of implications showing that "$(\sim P) \implies$ contradiction".

Thus we conclude that $(\sim P)$ is false, and so P is true. ■

Warning 11.1.1 What contradiction should we aim for? As we warned earlier, once you are comfortable with the logic of proof by contradiction, it becomes tempting to use it everywhere. However, we caution the reader to use this method after first trying a direct or contrapositive proof. One very good reason for this caution is that a direct or contrapositive proof has a well defined starting point:

- the hypothesis is true,

and a well defined end point:

- the conclusion is true.

By exploring the conclusion in our scratch work we can work out how to make the proof work.

Proof by contradiction starts clearly enough

- the statement is false,

but in contrast with direct and contrapositive proofs, it is not clear what statement we need to generate the contradiction. We know we need *some* contradiction, but *which* contradiction we should reach? How do we know where to aim? This can make it much harder.

We can generate a contradiction for our proof by contradiction is to show that one of our assumptions is both true and false. For example, when we start a proof by contradiction, we assume that the result is actually false and this, in turn, requires us to make an assumption, say, Q. *One* way we can generate a contradiction is to reach a conclusion $(\sim Q)$. However this is not the *only* way to generate a contradiction.

Let us do a small example, in which the contradiction is quite easy to find.

Result 11.1.2 *There is no smallest positive real number.*

[152] By the law of the excluded middle

Proof by contradiction can work very nicely for results of this form "There is no smallest X" or "There is no largest X" (where X is some interesting mathematical object). We can construct the proof by

- assume that there is a smallest X, call it X_1, then
- use X_1 to construct an even smaller X, call it X_2

but then we have

- X_1 is the smallest possible X, and at the same time
- X_2 is smaller that X_1

This gives us a contradiction of the form

$$Q \wedge \sim Q.$$

Let's apply this approach to the above result.

Our scratch work should look something like this:

- We'll try a proof by contradiction
- The negation of the result is "There is a smallest positive real number".
- Hence we assume there is a smallest positive real number — call it r.
- But now the number $r/2$ is a positive real number and $r/2 < r$.
- Contradiction!

Proof of Result 11.1.2. We prove this result by contradiction. Assume the result is false, so there is some smallest positive real number r. But then $0 < r/2 < r$, making $r/2$ is a smaller positive real number. This contradicts our assumption that r was the smallest positive real number. Hence the result must be true. ■

11.2 Some examples

We'll start with a couple of good warm-up examples.

Example 11.2.1 No integer solutions. There are no integers a, b so that $2a + 4b = 1$.

Scratchwork. Now notice that this result hides some universal quantifiers:

$$\forall a, b \in \mathbb{Z}, 2a + 4b \neq 1$$

To prove this using a contradiction we need to assume the negation of this statement. That is, we will assume that

$$\exists a, b \in \mathbb{Z} \text{ s.t. } 2a + 4b = 1.$$

So let a, b be integers so that $2a + 4b = 1$. But from this we have (after a quick division by 2)

$$a + 2b = \frac{1}{2}$$

and this is sufficient to get a contradiction; $a \in \mathbb{Z}$ and $2b \in \mathbb{Z}$ so their sum must be an integer. We just need to write this up nicely[153].

Solution.

Proof. Assume, to the contrary, that there exist integers a, b so that $2a+4b = 1$. This implies that

$$a + 2b = \frac{1}{2}$$

which gives a contradiction because the sum of integers is also an integer. Consequently, there can be no such integer a, b and the result follows. ■

□

Example 11.2.2 Another no integer solutions. There are no integers a, b so that $a^2 - 4b = 3$.

Solution.

Proof. Assume, to the contrary that a, b are integers so that $a^2 - 4b = 3$. Hence $a^2 = 4b + 3$. Consequently a must be odd (otherwise the LHS is even while the RHS is odd). So we can write $a = 2k + 1$ for some integer k. Hence

$$(2k + 1)^2 = 4b + 3$$

and so

$$4k^2 + 4k + 1 = 4b + 3$$

which means that

$$4(k^2 + k - b) = 2.$$

And since $k^2 + k - b \in \mathbb{Z}$, this implies that 2 is divisible by 4. This is clearly false and so we have arrived at a contradiction. Thus there can be no such integers a, b and the result holds. ■

□

Time for something a bit more substantial — a result about irrational numbers. Recall the definition of rational and irrational numbers.

Definition 11.2.3 Let q be a real number. We say that q is rational if it can be written $q = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ with $b \neq 0$. If q is not rational we call it irrational. We will denote the set of irrational numbers as $\mathbb{I}$, and note that $\mathbb{I} = \mathbb{R} - \mathbb{Q}$. ◊

We note that the notation, $\mathbb{I}$, is not standard, and some authors will use $\mathbb{P}$ or $\mathbb{K}$. Unfortunately there is no widely accepted standard notation for the set of irrational numbers. When you do make use of a particular notation for irrational numbers[154], and you are unsure if your reader knows that notation, we

[155]and, of course, make sure we warn the reader that we are using proof by contradiction.

[154]and we do recommend using $\mathbb{I}$ for this course

recommend that you devote a quick short sentence clarifying to explain.

Thus a number q is irrational when (writing it with quantifiers)

$$\forall a, b \in \mathbb{Z}, \left(\frac{a}{b} \neq q\right).$$

So a good way to reach a contradiction when working with irrational numbers, is to show that a number that you have assumed to be irrational can actually be written as a ratio of integers. We use exactly this approach for the next result.

Result 11.2.4 *The sum of a rational number and an irrational number is irrational.*

We start by assuming that the result is actually false and then work our way to a contradiction — namely that the number we assumed to be irrational is actually rational. It pays, especially when starting out with proof by contradiction, to write statements carefully with with quantifiers, so that we can also write down the negation carefully. The original statement is

$$\forall x \in \mathbb{Q}, \forall y \in \mathbb{I}, x + y \in \mathbb{I}$$

and its negation is

$$\exists x \in \mathbb{Q} \text{ s.t. } \exists y \in \mathbb{I} \text{ s.t. } x + y \notin \mathbb{I}$$

We can simplify this a bit because we know that $x+y \in \mathbb{R}$, so if it is not irrational, it must be rational:

$$\exists x \in \mathbb{Q} \text{ s.t. } \exists y \in \mathbb{I} \text{ s.t. } x + y \in \mathbb{Q}.$$

Now we assume *this* statement is true. And hence we can find a rational number, $x = \frac{a}{b}$, and an irrational number, y, and their sum $x + y$ is rational. One way we could get the contradiction, is to leverage the facts we have (by assumption)

$$x \in \mathbb{Q} \qquad y \in \mathbb{I} \qquad \text{and} \qquad x + y \in \mathbb{Q}$$

to reach a contradiction; in this example we'll show that $y \in \mathbb{Q}$.

Since $x \in \mathbb{Q}$ we know that there are integers a, b so that

$$x = \frac{a}{b}.$$

similarly since $x + y \in \mathbb{Q}$ we know that there are integers c, d so that

$$x + y = \frac{c}{d}.$$

But now we can use these to obtain more information about y:

$$\begin{aligned} y &= (x + y) - x \\ &= \frac{c}{d} - \frac{a}{b} = \frac{cb - ad}{bd} \end{aligned}$$

But since all of $a, b, c, d \in \mathbb{Z}$, we've just shown that y is rational — contradiction!

Time to write it up. When we do so we should definitely be careful and show that those denominators are not zero.

Proof of Result 11.2.4. We prove the result by contradiction. Assume that the result is false, and so there is a rational number x and an irrational number y whose sum $z = x + y$ is rational. Since x and z are rational, $x = a/b$ and $z = c/d$ for some $a, b, c, d \in \mathbb{Z}$ with $b, d \neq 0$. But now

$$y = z - x = \frac{cb - ad}{bd}$$

with $bd \neq 0$ and so y must be rational. This contradicts our assumption that y was irrational. Hence the result is true. ■

When we use proof by contradiction to prove an implication, we just have to negate carefully. Say our statement P is of the form

$$P \equiv \Big(\forall x \in S, Q(x) \implies R(x)\Big)$$

Our proof by contradiction needs us to prove that the negation of this statement implies a contradiction. So negating carefully:

$$\begin{aligned}(\sim P) &\equiv \sim \Big(\forall x \in S, Q(x) \implies R(x)\Big)\\ &\equiv \exists x \in S \text{ s.t. } \sim \Big(Q(x) \implies R(x)\Big)\\ &\equiv \exists x \in S \text{ s.t. } \Big(Q(x) \wedge \sim R(x)\Big)\end{aligned}$$

So our proof will start by assuming the existence of some $x \in S$ such that $Q(x)$ is true and $R(x)$ is false. Of course, we should make sure that we alert the reader that we are using proof by contradiction. We might say "Suppose the statement is false" or something similar. Here is example of this in action:

Result 11.2.5 *Let $a, b \in \mathbb{Z}$ with $a \geq 2$. Then a does not divide b or a does not divide $b + 1$.*

This statement has an implication hiding inside and can be written as

$$\forall a, b \in \mathbb{Z}, \Big[(a \geq 2) \implies \big((a \nmid b) \vee (a \nmid (b+1))\big)\Big]$$

so when we negate it we obtain

$$\exists a, b \in \mathbb{Z} \text{ s.t. } \Big[(a \geq 2) \wedge \big((a \mid b) \wedge (a \mid (b+1))\big)\Big]$$

We'll start[155] our proof by assuming that we can find such integers a, b, so that $a \geq 2$ and $a \mid b$ and $a \mid (b+1)$. From this we'll reach a contradiction.

Proof. Assume, to the contrary, that there is some $a, b \in \mathbb{Z}$ so that $a \geq 2$ and a divides both b and $b + 1$. This then implies that there exists $k, \ell \in \mathbb{Z}$ such that $b = ak$ and $(b + 1) = a\ell$.

But then $1 = (b + 1) - b = (\ell - k)a$. Since $\ell - k \in \mathbb{Z}$ this implies that a

[155] Of course, we'll warn the reader that it is a proof by contradiction before we get too far along. Be kind to your reader.

divides 1. This means that $a = 1$ or $a = -1$. This contradicts our assumption that $a \geq 2$. Hence the result is true. ■

This is not the only way to prove the above result and we could give a quick contrapositive proof which as some similarities with our proof above.

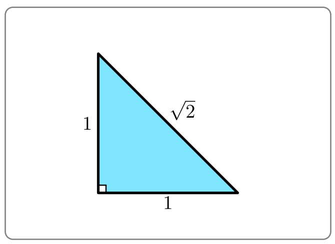
Proof. We prove the contrapositive. So let $a, b \in \mathbb{Z}$ and assume that $a \mid b$ and $a \mid (b+1)$. Then we know that $b = ak, (b+1) = a\ell$ for some $k, \ell \in \mathbb{Z}$. But then this tells us that

$$1 = (b+1) - b = a(k - \ell)$$

and so $a \mid 1$. However the only divisors of 1 are $1, -1$. And thus we know that $a < 2$ as required. ■

11.2.1 The irrationality of $\sqrt{2}$

The existence of a real quantity whose square is 2 follows directly from applying Pythagoras's Theorem to the following simple triangle.



It is, however, much less obvious that $\sqrt{2}$ cannot be expressed as the ratio of two integers; that result is one of the most famous in mathematics. Its proof, and so the proof of the existence of irrational numbers, is generally attributed to a member of the Pythagorean school in the 5th century BC, typically Hippasus of Metapontum. The evidence that exists linking Hippasus to the discovery of irrational numbers suggests that he was not praised for his work, but, rather, that he was expelled from his school. Some accounts indicate that he was even drowned as punishment! At the time the Pythagorean school thought that the positive integers numbers were somehow fundamental and beautiful and *natural*. The natural numbers were almost mystical objects and could be deployed to explain the universe. That such a simple and beautiful geometric object — the hypotenuse of a right-angle triangle — could not be expressed as the ratio of natural numbers was truly shocking. In some sense, it broke the link between number and the world.

Theorem 11.2.6 *The number $\sqrt{2}$ is not rational.*

We prove this result by finding a contradiction — that $\sqrt{2}$ is both rational and irrational. The same proof can be made to work (with minor adjustments) for any prime number. A key part of the proof is understanding that when we write a rational number

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

that we can insist that a, b do not have common factors. If we do have a representation $q = \frac{c}{d}$ where $\gcd(c, d) > 1$, then we can divide both numerator and denominator by that common factor and set

$$q = \frac{c}{d} = \frac{c/\gcd(c,d)}{d/gcd(c,d)} = \frac{a}{b}$$

where the new numerator and denominator, a, b have no common factors. In this way, the resulting a, b are the *smallest* integers whose ratio represents that rational number. Using this idea, our proof works by assuming that $\sqrt{2}$ is rational and so can be represented by a smallest a, b (ie with no common factors). We then obtain a contradiction by showing that the numerator and denominator do have a common factor. Along the way we will make use of a result we proved earlier[156].

> Let $n \in \mathbb{Z}$. Then n^2 is even if and only if n is even.

Proof. We prove the result by contradiction, and so assume that $\sqrt{2}$ is rational. Thus we can write $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and a and b have *no common factors*. Hence $2 = \frac{a^2}{b^2}$, which can be rewritten as $2b^2 = a^2$.

This implies that a^2 is even and so (by the above fact) a must be even. Thus we can write $a = 2c$ for some $c \in \mathbb{Z}$.

Substituting $a = 2c$ into $2b^2 = a^2$ we find $2b^2 = 4c^2$, which implies $b^2 = 2c^2$.Hence b^2 is even and so b must be even.

Since both a and b are even, they must have a common factor of 2. This contradicts our assumption that a and b have no common factors. Hence the result is true and $\sqrt{2} \notin \mathbb{Q}$. ■

Here is another result with a similar proof.

Result 11.2.7 *Let a, b, c be odd integers. Then the polynomial $ax^2 + bx + c$ has no rational zeros.*

Proof. Assume, to the contrary, that there are odd a, b, c and rational x so that $ax^2 + bx + c = 0$. Since x is rational, we know that $x = \frac{k}{n}$ for some integers k, n with $n \neq 0$. Further, we can assume that k, n have no common factors; if they do have common factors, remove them. Then

$$a\left(\frac{k}{n}\right)^2 + b\left(\frac{k}{n}\right) + c = 0$$

and so (multiplying through by n^2)

$$ak^2 + bkn + cn^2 = 0$$

Now consider the parity of k and n. There are four possibilities

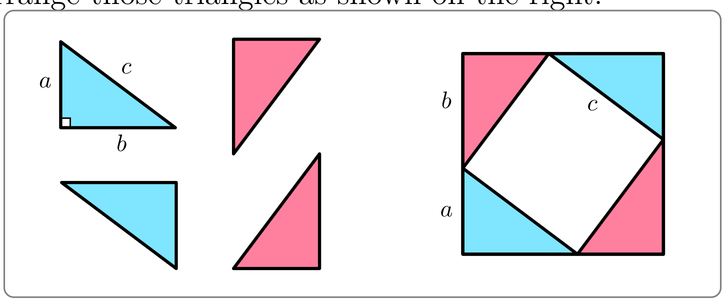
- If k, n are both odd, then since a, b, c are odd, the LHS is also odd, and so cannot equal zero.

[156] Lemma 5.1.5 is logically equivalent to the statement "The number n^2 is even iff n is even" (just take the contrapositive of both implications).

- If k is even and n is odd, then ak^2 and bkn are even, and cn^2 is odd. Hence the LHS is odd and so cannot equal zero.
- Similarly, if n is even and k is odd, then bkn and cn^2 are even and ak^2 is odd. Again this implies the LHS is odd and so cannot equal zero.
- Finally, if k, n are both even, then this contradicts our assumption that k, n have no common factors.

Thus there cannot exist such k, n and hence there is no such rational x. ■

Remark 11.2.8 Pythagoras' Theorem. There are a great many proofs of this famous theorem, but here is a pictorial argument that the authors particularly like (and we include here for completeness[157]). It is attributed to the 12th century mathematician and astronomer Bhaskara[158]. Construct a right-angle triangle with sides a, b, c, and then make another 3 copies, each rotated by 90 degrees, and then rearrange those triangles as shown on the right.



Now notice that the outer-square has area $(a+b)^2$, and the inner rotated square has area c^2. The four triangles have total area $2ab$. Equating the areas gives $(a+b)^2 = c^2 + 2ab$. But since $(a+b)^2 = a^2 + b^2 + 2ab$, subtracting $2ab$ from each side gives

$$c^2 = a^2 + b^2.$$

11.2.2 The infinitude of primes

Here is wonderful result about a fundamental property of numbers — that there are an infinite number of primes. The first recorded proof of this is due to Euclid in his Elements[159] from around 300 BC. The result does not rely on unique prime

[159] and because we can! We hope the reader will agree that it is pretty cool.

[160] Bhāskara, made many contributions to mathematics, including understanding some of the central ideas of differential calculus around 500 years before Newton and Leibniz. The interested reader should use their search engine to discover more. We note that Bhāskara is also known as Bhāskara II to distinguish him from Bhāskara I. Bhāskara I was a 7th Century mathematician and astronomer, who amongst other acheivements helped to develop the positional notation we use for representing numbers including a circle symbol for zero. He is also worth a trip to your favourite search engine. Both Bhāskara have satellites named after them by the Indian Space Research Organisation.

[159] This 13 book work on mathematics has been called the most famous and influential textbook in history. Indeed, it was *the* standard textbook for university students for many centuries. The interested reader should search-engine their way to more information.

factorisations, but it does require the fact that every integer greater than 1 has a prime divisor. We prove this first via strong induction — in fact we did this back in Example 7.2.20.

Result 11.2.9 *Let $n \in \mathbb{N}$ so that $n \geq 2$. Then n is divisible by a prime number.*

Proof. See Example 7.2.20. ■

Armed with this result, we can prove that the set of primes is not finite.

Theorem 11.2.10 Euclid — 300 BC. *There are infinitely many primes.*

We will prove this using a "proof by contradiction". We assume that there are only a finite number of primes and then deduce a contradiction. If there are a finite number of primes, we can list them out $\{p_1, p_2, \dots p_r\}$ and we can form the new number $N = p_1 p_2 \dots p_r$ — Now $N + 1$ is not on our list and it is not divisible by any of the primes. This will be the source of the contradiction (with a little more work).

Proof. Assume there are a finite number of primes. Since the primes are finite, we can write a finite list containing all of them — $p_1, p_2, \dots, p_n$. Now let $N = (p_1 p_2 \dots p_r)$ be a product of all the primes. Since the list of primes is finite, we know that N is finite. Now either $N + 1$ is prime or not.

- If $N + 1$ is prime then since $N + 1$ is bigger than all the primes on the list, $N + 1$ is not in our list of prime numbers. This gives a contradiction since our list was assumed to be *all* the primes.

- If $N+1$ is not prime then, by the above result, it must be divisible by one of the primes in our list — say $p_k \mid (N + 1)$. Hence we can write $N + 1 = p_k a$ for some $a \in \mathbb{N}$. Similarly we can write $N = p_k b$ for some $b \in \mathbb{N}$. But then

  $$1 = (N + 1) - N = p_k(a - b).$$

  This implies that 1 is divisible by p_k which is clearly false.

  Thus $N + 1$ is not divisible by any prime on our list and so there must be some prime that is not contained in our list. Again this gives a contradiction since our list as assumed to contain *all* primes.

In both cases a contradiction is obtained and hence the result is true. ■

11.3 Exercises

1. Prove that there is no integer a that simulataneously satisfies

$$a \equiv 2 \pmod{6} \qquad \text{and} \qquad a \equiv 7 \pmod{9}.$$

2. Let $a, b, c \in \mathbb{Z}$. If $a^2 + b^2 = c^2$, then a or b is even.

3. Let $n \in \mathbb{N}$. Suppose that $a \in \mathbb{Z}$ is such that $\gcd(a, n) > 1$. Show, by contradiction, that there is no $k \in \mathbb{Z}$ so that $ak \equiv 1 \pmod{n}$. This statement implies that $[a]_n$ is not invertible, which is a concept defined in Exercise 9.7.17.

4. Let $n \in \mathbb{N}$, $n \geq 2$, and $a, b \in \mathbb{Z}$. Prove that if $ab \equiv 1 \pmod{n}$, then $\forall c \in \mathbb{Z}, c \not\equiv 0 \pmod{n}$ we have $ac \not\equiv 0 \pmod{n}$.

5. Prove that there do not exist $x, y \in \mathbb{Z}$ that satisfy the equation $5y^2 - 4x^2 = 7$.

6. Prove each of the following statements:

(a) There is no smallest positive rational number.

(b) There is no smallest positive irrational number.

7. Two irrationality proofs.

(a) Prove that $\sqrt{6}$ is an irrational number.

(b) Prove that $\sqrt{2} + \sqrt{3}$ is irrational.

8. Prove that $\sqrt[3]{25}$ is irrational.

9. Prove that if k is a positive integer and $\sqrt{k}$ is not an integer, then $\sqrt{k}$ is irrational.

10. Let $r, x \in \mathbb{R}$, with $r \neq 0$. Prove by contradiction that if r is rational and x is irrational, then rx must be irrational.

11. Consider the following statements about preserving irrationality under addition and multiplication.

(a) Consider the following faulty proof of the statement, "If $x, y \in \mathbb{R}$ are irrational, then xy is irrational."

Faulty proof. Let $x, y \in \mathbb{R}$ be irrational. Then there are no $m, n, p, q \in \mathbb{Z}$ such that $x = m/n$ and $y = p/q$. Hence for any $m, n, p, q \in \mathbb{Z}$,

$$xy \neq \frac{mp}{nq}.$$

Since $mp, nq \in \mathbb{Z}$, we see that xy cannot be written as a fraction, and so xy is irrational. ∎

Show by counterexample that the statement above is false.

(b) Prove or disprove the following statement: If $x, y \in \mathbb{R}$ are irrational, then $x + y$ is irrational.

12. Let $x \in \mathbb{R}$ satisfy $x^7 + 5x^2 - 3 = 0$. Then prove that x is irrational.

13. Consider the following questions about the irrationality of logarithmic values.

(a) Prove that 5^k is odd for all $k \in \mathbb{N}$.

(b) Prove that $\log_2(5)$ is irrational.

(c) Determine for which $n \in \mathbb{N}$ is $\log_2(n)$ irrational. Prove your answer. You may assume the following statement:

For any $n \in \mathbb{N}$, there is some $a \in \mathbb{Z}$, $a \geq 0$ and $b \in \mathbb{Z}$ that is odd, so that $n = 2^a b$.

For this question, you may assume the following properties about the logarithm:

- if $x > 1$, then $\log_2(x) > 0$;
- for any $x, y > 0$,
$$\log_2(xy) = \log_2(x) + \log_2(y);$$

14. Consider the subset of rational numbers
$$A = \left\{x \in \mathbb{Q} \text{ s.t. } x \leq \sqrt{2}\right\}$$
Prove that it does not have a maximum.

See also Exercise 8.6.15 and Exercise 8.6.16.

15. Prove that there do not exist $a, n \in \mathbb{N}$ such that $a^2 + 35 = 7^n$.

16. Let $x \in (0, 1)$. Show that
$$\frac{1}{2x(1-x)} \geq 2$$

(a) by contradiction, and

(b) by a direct proof.

17. Consider the following statement: For all $x, y \in \mathbb{R}$ with $x, y > 0$ and $x \neq y$
$$\frac{x}{y} + \frac{y}{x} > 2.$$

(a) Prove the statement directly.

(b) Prove the statement by contradiction.

(c) How does the statement change if we remove the assumption $x \neq y$? That is: For all $x, y \in \mathbb{R}$ with $x, y > 0$, what can we say about $\frac{x}{y} + \frac{y}{x}$?

18. Let $a, b \in \mathbb{R}$ with $a, b > 0$. Show that
$$\frac{2}{a} + \frac{2}{b} \neq \frac{4}{a+b}$$

(a) using a contradiction, and

(b) using a direct proof.

19. Recall the *Intermediate Value Theorem:*

Let $g : U \to \mathbb{R}$ where $U \subseteq \mathbb{R}$. Suppose g is continuous on

$[a, b] \subseteq U$, and

$$f(a) \geq c \geq f(b) \quad \text{OR} \quad f(a) \leq c \leq f(b),$$

then there exists $x_0 \in [a, b]$ such that $g(x_0) = c$.

Let $f : \mathbb{R} \to \mathbb{R}$ be a continuous, bijective function. Using the Intermediate Value Theorem, prove that f is strictly increasing or strictly decreasing. See Exercise 10.8.19 for the definitions of strictly increasing and decreasing.

Chapter 12

Cardinality

This last chapter of the text brings together many of the ideas and techniques that we have learned to make sense of cardinality — the size of a set. When a set is finite the cardinality is a very intuitive concept — just[160] count up the elements:

$$|\{1,3,7,18,53\}| = 5.$$

By carefully describing how we count elements in finite sets in terms of **bijections** we can extend our understanding of cardinality to infinite sets. This allows us to make sense of statements such as

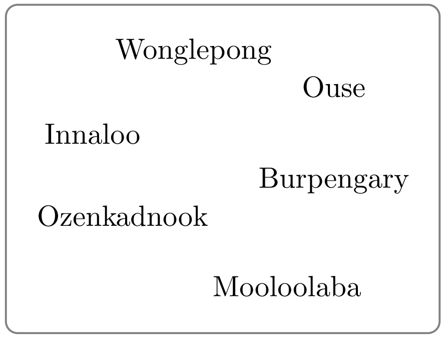
$$|\mathbb{Q}| = |\mathbb{Z}|$$

which are, to say the least, quite counter-intuitive. This also enables us to prove Cantor's Theorem 12.4.3. This result is arguably one of the most important pieces of mathematics that can be proven in undergraduate mathematics. It tells us something fundamental about the nature of infinity: not only are there different sorts of infinities, but there are an infinite number of different infinities!

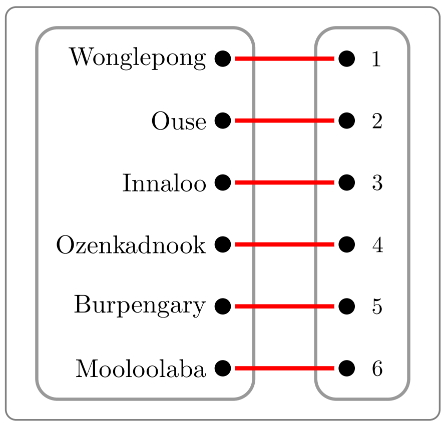
12.1 Finite sets

Consider the following set of place names from Australia:

[160]The reader is right to be a little skeptical of the use of the word "just" here; counting up the elements of a finite set can sometimes be quite difficult. Here we have listed out all the elements quite explicitly, but somes a set will be defined more *implicitly*, and then counting the elements can be quite challenging. The interested reader should search-engine their way to a description of enumerative combinatorics which is the mathematics of counting.



Think about what you do when you *count* the elements of that set. Now obviously[161] there are 6 elements in the set. However, think about how you count up those elements. Indeed, think about how we learn to count when we are very young. Typically we count by pointing at each element in turn (either physically pointing, or just pointing in our mind's eye), and counting off "one, two, three,…".



So what we are really doing here is constructing a function that takes us from the set of objects that we are counting to a subset $\{1, 2, 3, \dots, n\}$. This function is both

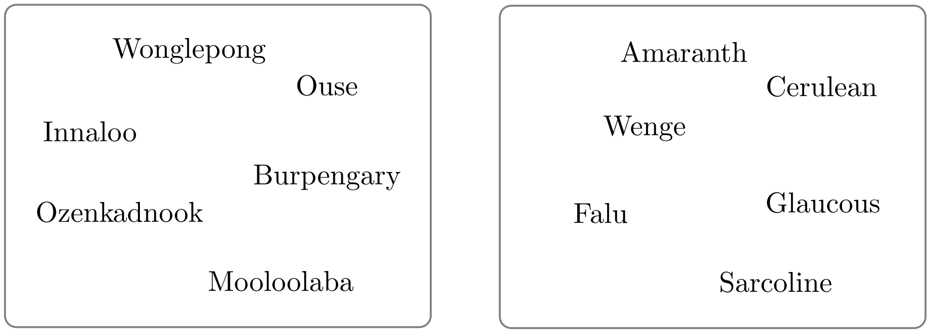
- injective — since different objects will be *counted* by different numbers, and
- surjective — since every number is used to *count* an object.

Hence when we count the objects in a finite set A we are really constructing a bijection from A to a subset of the natural numbers, $\{1, 2, 3, \dots, n\}$.

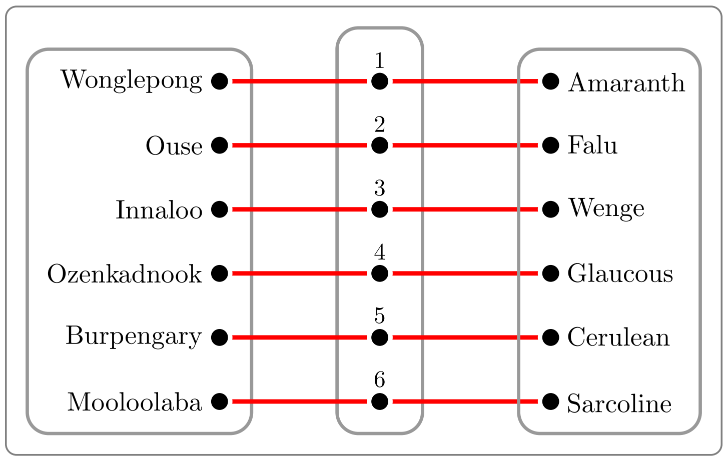
Now notice also that if we consider the following two sets[162]:

[161]While it is generally a good idea to avoid this word, it is probably safe to use it here. Clearly it is obviously safe to leave a decision on the use of this word to the reader who may edit their copy of the text accordingly.

[162]The same set of place names, and a set of "interesting" colour names.



Then we see that there are the same number of elements in each. We can do this in two ways, one is to count up as we did in the previous figure, but we could also simply establish a bijection between them.



These are actually equivalent. If there is a bijection, f from the set of place names to the set $\{1,2,3,4,5,6\}$, and another g from the set of colours to the set $\{1,2,3,4,5,6\}$, then g^{-1} is a bijection, and the composition $g^{-1} \circ f$ will be a bijection from the set of place names to the set of colours. In this way, two sets have the same size when there is a bijection between them.

In the above discussion we have tried to leverage the language of functions in order to compare the sizes of sets. Using functions allows us to extend the idea of "these sets are the same size" from finite sets to *infinite* sets. That is the main aim of this part of the text.

12.1.1 Equinumerous sets, bijections and pigeons

Oof! There are a lot of ideas above, so let's set them down slowly, carefully and rigorously.

Definition 12.1.1 Two sets A, B are said to have the same **cardinality** (or same **cardinal number**), written $|A| = |B|$, if either $A = B = \varnothing$ or there is a bijection from A to B. If A and B have the same cardinality then we say they are **equinumerous**[163]. Finally, if A and B are not equinumerous, we write $|A| \neq |B|$, and this is equivalent to saying that there is no bijection between them. ♢

This definition allows us to understand cardinality in terms of functions; this is critical for our understanding the size of infinite sets.

- When we write $|A| = n \in \mathbb{N}$, we are really stating that there is a bijection

$$f : A \to \{1, 2, 3, \ldots, n\}$$

  From our work on functions (see Theorem 10.6.8), we know that this also implies that there is a bijection back from $\{1, 2, \ldots, n\}$ to A — just the inverse function f^{-1}.

- And when $A = \varnothing$ we write $|A| = 0$. This is a special case that we have to treat separately; we cannot define a function with empty domain.

Example 12.1.2 Finite non-equinumerous sets. Say we have two finite sets A, B, so that they are not equal in size, $|A| \neq |B|$. Then there cannot be a bijection between them. We will shortly prove this in general, but suppose (for the sake of this discussion) that $|A| = 5$ and $|B| = 3$. So we can write our sets as

$$A = \{a_1, a_2, a_3, a_4, a_5\} \qquad B = \{b_1, b_2, b_3\}$$

First consider trying to construct a function $f : A \to B$. It is easy to construct a surjection:

$$f(a_1) = b_1, f(a_2) = b_2, f(a_3) = f(a_4) = f(a_5) = b_3.$$

However it is impossible to construct an injection. Once we have assigned $f(a_1), f(a_2), f(a_3)$ to three distinct values in B, it is impossible to assign $f(a_4)$ without repeating one of the values from B — making our function non-injective.

Now try construct a function $g : B \to A$. It is easy to construct an injection:

$$g(b_1) = a_1, g(b_2) = a_2, g(b_3) = a_3$$

However it is impossible to construct a surjection. Once we have assigned $g(b_1), g(b_2), g(b_3)$, there will still be two elements of A that have no preimage in B. □

The reasoning in the previous example is formalised by the **Pigeonhole Principle**[164].

[165]or "numerically equivalent", but "equinumerous" is a nicer word.

[164]While this is intuitively obvious, mathematicians like to make sure that obvious things are actually true. And if that obvious thing is really useful, then it should get a good name. Dirichlet was the first to formalise this idea in the 19th century and called it (in German) the

Theorem 12.1.3 Pigeonhole principle — Dirichlet's Schubfachprinzip. *If $n > 0$ objects are placed in $k > 0$ boxes then*

- *if $n < k$ then at least one box has zero objects in it, and*
- *if $n > k$ then at least one box has at least two objects in it.*

*In the second case, we can be more precise: at least one box contains at least $\lceil \frac{n}{k} \rceil$ objects, where $\lceil x \rceil$ is the **ceiling** of x and denotes the smallest integer larger or equal to x.*

Proof. We prove the contrapositive of the first statement, and then prove the second by contradiction.

- Assume each box has at least one element in it, then there must be at least k objects. Hence the number of objects is at least as large as the number of boxes.
- Assume, to the contrary, that every box contains at most $\lceil \frac{n}{k} \rceil - 1$ objects, then the total number of objects is

$$k \cdot \left(\left\lceil \frac{n}{k} \right\rceil - 1 \right) = k \left\lceil \frac{n}{k} \right\rceil - k < n,$$

  where we have used the fact that $\lceil x \rceil - 1 < x \leq \lceil x \rceil$. This gives a contradiction. Hence at least one box contains at least $\lceil \frac{n}{k} \rceil$ objects.

■

An immediate corollary is the following result for *finite* sets that formalises the last example.

Corollary 12.1.4 *Let A, B be finite sets and let $f : A \to B$ be a function. Then*

- *If $|A| > |B|$ then f is not an injection.*
- *If $|A| < |B|$ then f is not a surjection.*

Proof. We prove each in turn. Assume that A, B are finite.

- Assume that $|A| > |B|$. Then when the images of elements of A are placed into B by the function, there must, by the pigeonhole principle, be at least one element of B which is the image of $\left\lceil \frac{|A|}{|B|} \right\rceil > 1$ elements of A. Hence f is not injective.
- Assume that $|A| < |B|$. Then when the images of elements of A are placed into B by the function, there must, by the pigeonhole principle, be at least one element of B which is not the image of any element of A. Hence f is not surjective.

drawer-principle — Schubfachprinzip. Since Dirichlet's father was a postmaster, it is perhaps an imperfect translation of his idea that led to "pigeonholes" in the sense of a small open drawer or shelf used to sorting or storing letters (slightly antiquated in these days of tweeting (pun!), email, and social media updates). This imperfect English translation has been imported into other languages, including back into German. No pigeons are involved.

■

We should notice the contrapositive of the results in the above corollary. Let A, B be finite sets and $f : A \to B$ be a function, then

- if f is an injection then $|A| \leq |B|$, and
- if f is a surjection then $|A| \geq |B|$.

Notice that one can do much more with the pigeonhole principle than just put objects in boxes — a little trip to your favourite search engine will turn up many many examples. We'll give a few examples, most quite standard, and one definitely not.

Example 12.1.5 Fix $n \in \mathbb{N}$ and let $S = \{1, 2, \cdots, 2n-1\}$ and let $A \subseteq S$ so that $|A| = n+1$. Prove that there are two elements of A whose sum is $2n$.

Solution.

Proof. We can write $2n$ as the following sums of pairs from S:

$$2n = (2n-1) + 1 = (2n-2) + 2 = \cdots = (n+1) + (n-1)$$

Notice that the number n cannot be used in such a pair.

So split the set S up into 2 element subsets and $\{n\}$:

$$\{1, 2n-1\}, \{2, 2n-2\}, \ldots, \{n-1, n+1\}, \{n\}$$

There are n sets in this list. Consequently, when we choose n elements it is possible to choose one element from each of the above subsets, however when we choose one more, we must choose a second element from one of those two element subsets. The two elements from the two element-subset sum to $2n$ as required.

■

□

Example 12.1.6 Let $S = \{1, 2, \cdots, 20\}$ and let $A \subseteq S$ so that $|A| = 11$. That is, A contains 11 distinct integers from between 1 and 20 (inclusive). Then there exist $a, b \in A$ so that $a \mid b$.

Solution.

Proof. First notice that we can write any natural number as the product of an odd number and a power of 2.

$$\forall n \in \mathbb{N}, \exists k, \ell \in \mathbb{N} \text{ s.t. } n = (2k+1) \cdot 2^{\ell}$$

So we can take any $n \in A$ keep dividing by 2 until you get an odd number. When you do so the resulting odd number must be in the set $\{1, 3, 5, \cdots, 19\}$. Since this set contains 10 distinct elements, there must be two numbers in A that result the same odd number in $\{1, 3, 5, \cdots, 19\}$. We can write these numbers as

$$a = (2k+1)2^i \qquad \text{and} \qquad b = (2k+1)2^j$$

where $i \neq j$. If $i > j$ then $b \mid a$ and if $i < j$ then $a \mid b$. In either case there must be a pair of integers in A for which one divides the other. ■

□

Example 12.1.7 Spurious correlations. An excellent illustration of the pigeonhole principle is given by the database of "spurious correlations" — see the fantastic website and book by Tyler Vigen[165].

It goes roughly like this — consider how many simple (ie not-too wiggly) graphs you can draw whose horizontal axis is the last 100 years. There might be (say) a hundred such "simple" graphs. Now build a big database of any statistics you can think of — diary production in Quebec, deaths by lightning, number of twins born in a particular city, etc etc. There are thousands and thousands of such statistics.

Now — associate each of these statistics to the curve that best approximates it. Since there are only (say) a hundred such curves, and many thousands of statistics, there must — by the pigeonhole principle — be at least one curve which corresponds to many statistics. In practice, there are many statistics for each curve. This means that those statistics are correlated. In this way you can see that, say, the number of mathematics PhD's awarded is highly correlated with the quantity of uranium stored at US power plants. Is there any causal link — nope[166].

This can be a source of fun (well, mathematician fun), but it can also create problems. The idea of making use of "Big data" to solve problems is getting a lot attention. People even announcing that analysis of huge data sets will replace[167] the scientific method! However, given enough data, you will find correlations everywhere. It is just a matter of putting objects in boxes — the pigeonhole principle at work. □

12.1.2 Comparing with functions

In the previous section we started to link cardinality of sets A, B and the types of functions that can be constructed between them. For example, we saw that

- If $f : A \to B$ is an injection then $|A| \leq |B|$,
- If $g : A \to B$ is a surjection then $|A| \geq |B|$, and
- If $h : A \to B$ is a bijection then $|A| = |B|$

In this section we demonstrate that this way of comparing sizes of sets is well-defined. For example, we should have that equality of cardinality behaves just like equality of integers:

$$|A| = |A|$$

and

$$(|A| = |B|) \implies (|B| = |A|)$$

[167] `tylervigen.com/spurious-correlations`
[168] We hope not.
[169] This was a big headline article in Wired magazine in 2008.

and

$$(|A| = |B|) \wedge (|B| = |C|) \implies (|A| = |C|)$$

That is, we need to show that equinumerous is an equivalence relation.

Theorem 12.1.8 *Let A, B and C be sets. Then*

- $|A| = |A|$ *(reflexive).*
- *If* $|A| = |B|$ *then* $|B| = |A|$ *(symmetric).*
- *If* $|A| = |B|$ *and* $|B| = |C|$ *then* $|A| = |C|$ *(transitive).*

Proof.

- The identity function on A, $i_A : A \to A$ is a bijection and thus $|A| = |A|$.
- Assume $|A| = |B|$. Then there is a bijection $f : A \to B$. Since f is bijective the inverse function $f^{-1} : B \to A$ exists and is bijective. Thus there is a bijection from B to A and so $|B| = |A|$.
- Assume $|A| = |B|$ and $|B| = |C|$, so there are bijections $f : A \to B$ and $g : B \to C$. Since the composition of bijections is bijective, it follows that $h : A \to C$ defined by $h = g \circ f$ is bijective. Thus $|A| = |C|$.

■

This result is very useful. In order to show that two sets have the same size we can show they are equinumerous with a third set.

Remark 12.1.9 Cardinality inequalities. In addition to proving the above properties of equality of cardinalities, we should also prove analogous results for inequalities of cardinalities. In particular, we should also show that

$$|A| \leq |A|$$

and

$$(|A| \leq |B|) \wedge (|B| \leq |A|) \implies (|A| = |B|)$$

and

$$(|A| \leq |B|) \wedge (|B| \leq |C|) \implies (|A| \leq |C|)$$

Notice that the first follows immediately since the identity function on A is an injection. The last one follows because the composition of injections is itself an injection (this is exactly Theorem 10.5.3). The middle one is the Cantor-Schröder-Bernstein theorem and its proof is quite involved — see Section 12.5. It is reasonably easy to prove for finite sets, however. Maybe we'll set that as an exercise.

12.1.3 Infinite sets are strange.

When we deal with finite sets everything above is pretty clear cut — we can put things into a bijection with $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. We did exactly this with our place-names and colours example at the start of this chapter. However, when we get to non-finite sets, things get much more interesting and weird.

Here is a very telling example. Consider the positive even numbers

$$E = \{2, 4, 6, 8, \dots\}$$

Now it is clear that E is a proper subset of $\mathbb{N}$; it only contains ever second number. So it should[168] be half the size. But we have to be careful; consider the following function

$$f : \mathbb{N} \to E \qquad\qquad f(n) = 2n$$

This function is a bijection from $\mathbb{N}$ to E:

- Injective because if $n_1 \neq n_2$ then $f(n_1) = n_1 \neq n_2 = f(n_2)$.
- Surjective because for any $b \in E$, we know that $b = 2k$ for $k \in \mathbb{N}$, and $f(k) = 2k = b$.

So the set of natural numbers is equinumerous with a proper subset of the natural numbers! No finite set can do this because of the pigeonhole principle, but an infinite set can. This is actually one way of defining when a set is infinite:

Definition 12.1.10 We say that a set A is **infinite** when there is a bijection between A and a proper subset of A. ♢

This definition was introduced by Dedekind in the late 19th century. Notice that this way of defining infinity does not rely on the natural numbers. When we first learn of the existence of infinity as children it is usually in the context of having learned to count

$$1, 2, 3, 4, \dots$$

and we ask ourselves (or our teacher, or our parent[169]) — what is the biggest number? And we realise that we can go on counting forever without stopping. This idea of infinity as being somehow intimately related to the natural numbers is hard to shake. But we will a little later in this chapter.

The apparent paradox[170] in Dedekind's definition of infinite sets goes back at least as far as Galileo, and is often called Galileo's paradox. In his "Two new sciences" Galileo imagines a conversation between two people, Simplicio and

[168] "Should" is another one of those dangerous words like "clearly" and "obviously" and "just". It should (ha!) set off alarm bells.

[169] Perhaps repeatedly?

[170] It is a veridical paradox. That is, a paradox that seems absurd but is actually true. Another good example, for the paradoxically inclined, is the Monte Hall problem. The interested reader can (and should) search-engine their way to that particular example.

Salviati[171] . Simplicio brings up the bijection[172] between the natural numbers at the squares:

$$f : \{1, 2, 3, \dots\} \mapsto \{1, 4, 9, \dots\} \qquad\qquad f(n) = n^2$$

and the apparent paradox of something larger being equinumerous with something smaller. After some discussion Salviati concludes that one cannot compare cardinalities of infinite sets. That restriction stayed until the 19th century work of Cantor and others.

Georg Cantor developed modern set theory (especially between about 1874 and 1884) — he developed the finer understanding of infinite sets we now have. Before him, there were finite sets, and a somewhat loosely defined idea of infinity. Cantor's work on infinity was not well received by the maths community of the 19th century and a number of big names in mathematics very publically criticised him — "corrupter of youth" was one of many insults[173] . It is worth search-engining your way to a biography of him and the intersection between his work on infinity and many ideas in the philosophy of mathematics and theology. Not light stuff to be summarised here in a quick paragraph.

12.2 Denumerable sets

As described above, our intuitive notion of an infinite set (or any infinite thing), is a process that keeps on going. We never get to the end because we can always take another step. What we are really doing when we think of infinity in this way is setting up a bijection between it and the set of natural numbers. There is some infinite process — we start at the beginning (the number 1) and then we take a step $n \mapsto n + 1$, and then another step, and another step and, ... This is the first type of infinity that we will encounter — sets that are in bijection with $\mathbb{N}$. We call these sets denumerable because we can think of counting off the elements via the bijection.

---

[171]Salviati is named after one of Galileo's friends, while Simplicio is likely modelled on one of his philosophical opponents, or perhaps is intended to represent Galileo's beliefs early in his lief. Both characters appear in Galileo's work "Dialogue Concerning the Two Chief World Systems" which discusses the relative merits of the Copernican (heliocentric) and Ptolemaic (geocentric) models of the solar system. That book was subsequently banned by the Catholic Church for over 200 years.

[172]He doesn't call it a bijection — that term didn't come into mathematics until the middle of the 20th century with the work of Bourbaki.

[173]Henri Poincaré called his work on infinities a "grave disease" infecting the discipline of mathematics, while Leopold Kronecker described Cantor as a charlatan and a renegade as well as the famous epithet "corrupter of youth" and "I don't know what predominates in Cantor's theory — philosophy or theology, but I am sure that there is no mathematics there." Kronecker is reputed to have said that "God created the natural numbers; all else is the work of man." — making him (arguably) a proponent of mathematical finitism. It's an interesting topic and well worth a quick trip to your favourite search-engine.

Definition 12.2.1 Let A be a set.

- The set A is called **denumerable** if there is a bijection $f : \mathbb{N} \to A$.
- The cardinal number of a denumerable set is denoted $\aleph_0$ (read “aleph naught” or “aleph null”).
- The set A is called **countable** if it is finite *or* denumerable.
- The set A is **uncountable** if it is not countable.

◊

Notice that

- At this stage it is not clear that there is something out there that is “uncountable” — the existence of uncountable sets was highly controversial when Cantor proved it in 1874[174].
- There is a bijection from $\mathbb{N}$ to A if and only if there is a bijection from A to $\mathbb{N}$.
- Finally, a very nice property of denumerable sets is that even though they are infinite, we can still “list out the elements”.

This last point is both very important and also is a little counter-intuitive, so we’ll make it more precise. Consider a denumerable set A. By definition there is a bijection $f : \mathbb{N} \to A$. Now we can think of f as a relation

$$f = \{(1, f(1)), (2, f(2)), (3, f(3)), \dots\}$$

Hence we can write A as

$$\begin{aligned} A &= \{f(1), f(2), f(3), \dots\} && \text{or equivalently} \\ A &= \{a_1, a_2, a_3, \dots\} && \text{with } a_i = f(i). \end{aligned}$$

Notice that this list has a couple of special properties.

- Since f is injective, our list does not repeat — different indices give different elements of A.
- Also, since f is surjective, any given element of A — say q — is mapped to by some integer $n_q \in \mathbb{N}$. Since n_q is finite, this means that any given element of A appears on the list in some finite position.

We can also go backwards — if we can list out the elements of some infinite set B, then B is denumerable. Say we have listed out our elements as $\{b_1, b_2, b_3, \dots\}$, so that

[174] It first appeared in an article called “On a Property of the Collection of All Real Algebraic Numbers”. He did not use his famous diagonal-argument (we do it a little later in the text); that argument appeared 17 years later in a 1891 paper titled “On an elementary question of the theory of manifolds.”

- the list does not repeat, and
- any given element of B appears at some finite position on the list.

Now we can define a function $g : \mathbb{N} \to B$ by $g(j) = b_j$. That is, just map any natural number to the element at that position in the list. The two conditions we have placed on the list then mean that g is injective and surjective, so g is a bijection. Hence B is denumerable.

Let's formalise this idea that denumerable means listable in a lemma. The proof is given by the argument above.

Lemma 12.2.2 Listing elements of denumerable sets. *Let A be a set. If A is denumerable then we can construct an infinite list, $a_1, a_2, a_3, \ldots$, of all its elements so that*

- *the list does not repeat any element of A, and*
- *any given element, $a \in A$ appears at some finite position in the list*

The converse of this statement is also true. Namely, if we can construct such a list of the elements of A, then A is denumerable.

Proof. Let A be denumerable. Then, by definition, there exists a bijection $f : \mathbb{N} \to A$. For any $n \in \mathbb{N}$, define the n^{th} element of our list to be $a_n = f(n)$. Then

- Since f is injective, we know that for $j \neq k$, $a_j = f(j) \neq f(k) = a_k$. So the items on our list are distinct.
- Since f is surjective, we know that for any $x \in A$ there exists $n \in \mathbb{N}$ so that $f(n) = x$. Thus the element $x = a_n$ is the n^{th} item on the list, and so appears at a finite position in the list.

Now assume such a list exists. Then for any $n \in \mathbb{N}$ define $g(n) = a_n \in A$. Since the list is infinite this defines a function $g : \mathbb{N} \to A$. Then

- Let $x \in A$. By assumption, the element x appears at some finite position in the list. So there is $n \in \mathbb{N}$ so that $x = a_n = g(n)$. Thus g is surjective.
- Since the list does not repeat we can take the items from the j^{th} and k^{th} positions on the list, namely a_j, a_k with $j \neq k$. Then we know that $a_j \neq a_k$ which in turn gives $g(j) \neq g(k)$. Thus g is injective.

Hence there is a bijection $g : \mathbb{N} \to A$ and so A is denumerable. ∎

This infinite-but-listable way of looking at denumerable sets makes it much easier to work with them. Especially because, as we have seen with our even numbers example above, infinite sets are very counter-intuitive. Here is counter-intuitive result that is also a very important result.

Theorem 12.2.3 *The set of all integers is denumerable.*

Proof sketch. We will sketch out how to prove this result but leave the formal proof to the reader. It suffices to find a "nice way" to list out all the elements of $\mathbb{Z}$ (since this nice list is really a bijection). We can't just do $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ — which each integer appears on the list, it is not clear that any given integer appears at some finite position in the list. This sort of infinite list is typically called bi-infinite, since it extends to infinity in both direction.

On the other hand, if we write out the integers as

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$$

then we can see that every integer will appear once, and that any given integer will appear at some finite position in the list. Indeed, this list, carefully described, is a proof of the result.

We can, in this case, make the bijection very explicit in this case and define a function

$$f = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & -1 & 2 & -2 & \cdots \end{array}$$

With a bit of juggling this becomes

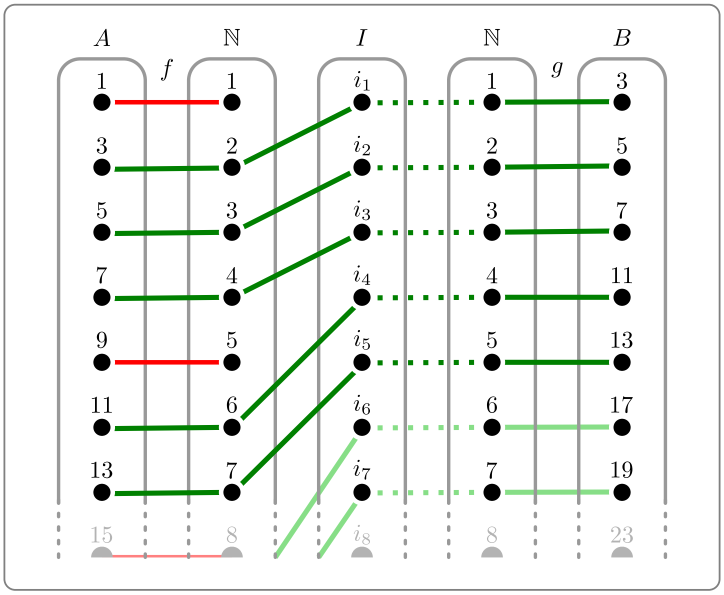
$$f(n) = \begin{cases} \frac{1-n}{2} & n \text{ is odd} \\ \frac{n}{2} & n \text{ is even} \end{cases} = \frac{1 + (-1)^n(2n-1)}{4}$$

It is not hard to show this is bijective — in fact, we'll make this an exercise. ■

So again we have produced an example of a strict subset having the same cardinality: $\mathbb{N} \subset \mathbb{Z}$ but $|\mathbb{N}| = |\mathbb{Z}|$. This is quite general; a subset of a denumerable set is either finite or itself denumerable.

Theorem 12.2.4 *Let A be a denumerable set and let $B \subseteq A$. Then B is countable.*

Now this proof is a little fiddly around the edges so we'll just give a proof sketch. Before we get started with the proof, consider the specific case of A being the set of positive odd numbers, and B being the set of odd prime numbers.



On the right-hand side of the figure we've drawn the set of odd primes, B, and the natural numbers and the bijection g between them. On the left-hand side we've given the set of odd numbers, A and next to it we've drawn the set of natural numbers $\mathbb{N}$ and the bijection f between them. Notice that we've drawn some edges in red and some in green. The red edges correspond to the elements of A that are not in B, while the green edges correspond to the elements in A that are in B. Notice that the red edges stop, while the green edges trace through a set I (described in the proof sketch below), and then another copy of $\mathbb{N}$ and then finally to the set B. Keep this picture in mind when you read the proof sketch below.

Actually just a sketch of a proof. Let B be a subset of a denumerable set A.

- If B is finite then we are done, because a finite set is countable.

- Assume B is infinite. There is a bijection $f : \mathbb{N} \to A$, and we can write $A = \{a_1, a_2, \ldots\}$ and $f(n) = a_n$. Now define $I = \{n \in \mathbb{N} \mid a_n \in B\}$ — ie the indices of elements that are in B. Notice that $I \subseteq \mathbb{N}$ and so we can write the indices in order[a]

  Hence we can write the set of these indices as $I = \{i_1, i_2, i_3, \ldots\}$. Now define a function $g : \mathbb{N} \to B$ by

  $$g(n) = a_{i_n}$$

  That is, for any input number n, look up the n^{th} index in I, and then return that element of A. By construction that is an element of B.

  We can trace this though our odd-primes figure above. In that case $g(3) = 7$ because $i_3 = 4$ and $f(4) = 7$. Similarly, $g(5) = 13$ since $i_5 = 7$ and $f(7) = 13$.

- Now that we have this function, we need to prove it is bijective.

- Injective — Assume that $g(n) = g(m)$, then $a_{i_n} = a_{i_m}$. Since the original function f is bijective, this implies that $i_n = i_m$. Hence $n = m$.
- Surjective — Let $b \in B$. Then since $B \subseteq A$, we know $b \in A$. Since f is surjective, there is some n so that $f(n) = a_n = b$. Hence $n \in I$. Hence there is some $1 \leq k \leq n$ so that $g(k) = a_n = b$.

- Thus there is a bijection from $\mathbb{N}$ to B, and so B is denumerable.

■

[a]This bit actually requires a bit of thought — one can use the well-ordering principle to find the smallest thing in the set I and call it i_1.Then remove that from the set and find the next smallest, call it i_2. etc etc.

Let's generalise our result above positive even numbers being in bijection with the naturals; we'll also do Galileo's paradox the same way. Using the above theorem we don't have to establish explicit bijections, we just need to show that they are infinite subsets of a denumerable set.

Result 12.2.5 *Let $k \in \mathbb{N}$, then the sets*

$$k\mathbb{Z} = \{kn \mid n \in \mathbb{Z}\} \qquad k\mathbb{N} = \{kn \mid n \in \mathbb{N}\} \qquad \left\{n^2 \mid n \in \mathbb{N}\right\}$$

are denumerable.

Proof. Let $k \in \mathbb{N}$. Then above sets all subsets of $\mathbb{Z}$. Hence by the previous theorem they are countable. All of the sets are infinite, so they must be denumerable. ■

One can show that the union of denumerable sets is denumerable and that the Cartesian product is too.

Result 12.2.6 *Let A and B be denumerable sets, then $A \times B$ is denumerable.*

Proof. It suffices to find a bijection from $\mathbb{N}$ to $A \times B$. Since A and B are denumerable we can write $A = \{a_1, a_2, \dots\}$ and $B = \{b_1, b_2, \dots\}$. Construct the following (infinite) table

	b_1	b_2	b_3	$\dots$
a_1	(a_1, b_1)	(a_1, b_2)	(a_1, b_3)	$\dots$
a_2	(a_2, b_1)	(a_2, b_2)	(a_2, b_3)	$\dots$
a_3	(a_3, b_1)	(a_3, b_2)	(a_3, b_3)	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

We form the function $f : \mathbb{N} \to A \times B$ by sweeping successive diagonals $\swarrow \swarrow \cdots$.

$$\begin{array}{llll} f(1) = (a_1, b_1) & & & \\ f(2) = (a_1, b_2) & f(3) = (a_2, b_1) & & \\ f(4) = (a_1, b_3) & f(5) = (a_2, b_2) & f(6) = (a_3, b_1) & \\ f(7) = (a_1, b_4) & f(8) = (a_2, b_3) & f(9) = (a_3, b_2) & f(10) = (a_4, b_1) \end{array}$$

and so forth. Since any given ordered pair is reached eventually (ie after a finite number of diagonal sweeps of finite length), the function is surjective. Since we never repeat an ordered pair, the function is injective. Thus f is bijective. ■

Notice that if we tried to list out the elements by reading out each column (or each row), then the resulting function would not be surjective — it would take an infinite time to reach the second column. Hence the preimage under that function of an element in the second column would not be a natural number.

Very similarly we arrive at the following very counter-intuitive result

Theorem 12.2.7 *The set of positive rational numbers $\mathbb{Q}^+$ is denumerable.*

Proof. Form the following table of positive rationals

	1	2	3	...
1	1/1	1/2	1/3	...
2	2/1	2/2	2/3	...
3	3/1	3/2	3/3	...
⋮	⋮	⋮	⋮	⋱

List things out in the same sweeping diagonal order $\swarrow \swarrow \cdots$ we used previously:

$$\begin{array}{lllll}
\frac{1}{1}, & & & & \\
\frac{1}{2}, & \frac{2}{2}, & & & \\
\frac{1}{3}, & \frac{2}{2}, & \frac{3}{1}, & & \\
\frac{1}{4}, & \frac{2}{3}, & \frac{3}{2}, & \frac{4}{1}, & \\
\frac{1}{5}, & \frac{2}{4}, & \frac{3}{3}, & \frac{4}{2}, & \frac{5}{1}, \\
\vdots & & & &
\end{array}$$

This list gives a surjective function, since any given positive rational number would appear at some finite positive position on the list. For example, we have $f(1) = \frac{1}{1}, f(2) = \frac{1}{2}, f(5) = \frac{2}{2}$, and so on. However, the list repeats rationals, so it is not injective.

Thankfully this is quite easy to fix, we can simply skip those rationals that have already appeared[a]:

$$\begin{array}{lllll}
\frac{1}{1}, & & & & \\
\frac{1}{2}, & \frac{2}{1}, & & & \\
\frac{1}{3}, & \cdot & \frac{3}{1}, & & \\
\frac{1}{4}, & \frac{2}{3}, & \frac{3}{2}, & \frac{4}{1}, & \\
\frac{1}{5}, & \cdot & \cdot & \cdot & \frac{5}{1},
\end{array}$$

where we have used a dot to indicate a fraction we have skipped. Define $f : \mathbb{N} \to \mathbb{Q}^+$ by $f(n)$ is the nth term of the list. So $f(1) = \frac{1}{1}, f(3) = \frac{2}{1}, f(5) = \frac{3}{1}, f(7) = \frac{2}{3}$ and so on.

Since every positive rational number appears on the list (at some finite position), f is surjective. Since no number is repeated, f is injective. Thus f is bijective and so $|\mathbb{N}| = \mathbb{Q}^+$. ■

[a] Notice that we do not have to be able to do this efficiently, we just need to be able to do it! Mind you, it is not too hard to work out that a given ratio $\frac{a}{b}$ has already appeared on the list when a, b have a common divisor.

An alternative proof. We can also prove this result using our previous theorem, by constructing a bijection from $\mathbb{Q}^+$ to an infinite subset of $\mathbb{N} \times \mathbb{N}$.

Recall that we can write any $q \in \mathbb{Q}^+$ uniquely as $\frac{a}{b}$ where a, b are natural numbers with no common divisors. Then we can define $f : \mathbb{Q}^+ \to \mathbb{N} \times \mathbb{N}$ by

$$f(q) = (a, b) \qquad \text{where } q = \frac{a}{b}$$

and $a, b \in \mathbb{N}$ with no common divisors. We claim that this function is an injection.

Let $p, q \in \mathbb{Q}^+$ so that $p \neq q$. Now if $f(p) = f(q) = (a, b)$ we must have $p = q = \frac{a}{b}$. Thus we must have $f(p) \neq f(q)$.

The injection f can be specialised to a bijection $\hat{f} : \mathbb{Q} \to \operatorname{rng}(f)$ by reducing its codomain to exactly the range of f. Since $\operatorname{rng}(f)$ is an infinite subset of $\mathbb{N} \times \mathbb{N}$, it must be denumerable. Hence $\mathbb{Q}^+$ is denumerable. ■

Now say that the above order gives

$$\mathbb{Q}^+ = \{q_1, q_2, q_3, \dots\}$$
$$\mathbb{Q}^- = \{-q_1, -q_2, -q_3, \dots\}$$

Then we can write

$$\begin{aligned}\mathbb{Q} &= \{0\} \cup \mathbb{Q}^+ \cup \mathbb{Q}^- \\ &= \{0, q_1, -q_1, q_2, -q_2, \dots\}\end{aligned}$$

And so by using this sneaky way of listing the rationals, we get

Corollary 12.2.8 *The set of all rational numbers is denumerable.*

This is really weird. While the natural numbers and the integers feel very similar; there are nice discrete unit steps between numbers. The rational numbers, however, appear to be very different objects. Most striking being that they are dense — between any two rationals we can find another rational number. But despite that, the rationals are the same size as the integers!

The trick we used above to prove this corollary is a good one and can be extended to a more general result:

Result 12.2.9 *Let A, B be countable sets. Then the union $A \cup B$ and intersection $A \cap B$ are also countable.*

Proof.

- The intersection $A \cap B \subseteq A$, so if A is finite then so is the intersection. While if A is denumerable, then our previous theorem tells us that all its subsets are countable. So we are done.

- Now consider the union. Since A, B are countable, we can list out their elements as

$$A = \{a_1, a_2, a_3, \dots\} \qquad B = \{b_1, b_2, b_3, \dots\}$$

 Assume, for the moment that $A \cap B = \varnothing$.

 - If both A, B are finite then their union is finite.
 - If both A, B are infinite, then write the union as

$$A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, \dots\}$$

 This listing of the elements of the union demonstrates that the union is denumerable.

 - If one of A, B is finite, but the other infinite, then we can write

$$A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, \dots, a_n, b_n, a_{n+1}, a_{n+2}, a_{n+3}, \dots\} \quad \text{or}$$
$$A \cup B = \{a_1, b_1, a_2, b_2, a_3, b_3, \dots, a_\ell, b_\ell, b_{\ell+1}, b_{\ell+2}, b_{\ell+3}, \dots\}$$

 depending on which of A, B are finite. This demonstrates that the union is denumerable.

 Thus the union of two disjoint countable sets is countable.

 Now assume that $A \cap B \neq \varnothing$, then write $C = B - A$, so that

$$C \subseteq B \qquad A \cap C = \varnothing \qquad A \cup C = A \cup B.$$

 These are quite straight-forward to prove:

 - If $x \in C$ then $x \in B - A$ and so $x \in B$.
 - Let $x \in A$. Then we must have that $x \notin B - A$, and thus $x \notin C$. Hence $A \cap C$ must be empty.
 - Since $C = B - A = B \cap \bar{A}$, we have

$$A \cup C = A \cup (B \cap \bar{A}) = (A \cup B) \cap (A \cup \bar{A}) = (A \cup B) \cap U = A \cup B$$

 where U denotes the universal set.

 Now, since B is countable we know that C is countable. The reasoning used for disjoint sets above, then shows that $A \cup C$ is countable, and thus $A \cup B$ is countable.

■

12.3 Uncountable sets

We are now ready to move on to one of the nicest results of the course and arguably one of nicest in Mathematics. We will prove that there is no bijection between the natural numbers and the reals and so that the reals are uncountable. It is due to Georg Cantor. He proved the result first in 1873, and again by a simpler method in 1891. We will do the second version here, since it is easier. We give Cantor's first proof as an optional section 12.6 later in this chapter.

The proof works by a contradiction and also relies on some facts about decimal expansions of real numbers.

- Every rational number has a repeating decimal expansion
  - eg $1/3 = 0.333333333...$
  - eg $2/11 = 0.1818181818181...$
- Some rational numbers have two repeating expansions
  - eg $1/2 = 0.500000... = 0.499999999...$
  - eg $1/5 = 0.2... = 0.1999999999...$
- One can show that a rational number p/q (reduced) has two expansions if only if q is a product of powers of 2 and 5. In this case the expansions terminate either with 9's or 0's.
- Every irrational number has a unique (non-repeating) decimal expansion

None of the above is too hard to prove, but we won't do it here. We want to get on to this very important result.

Theorem 12.3.1 Cantor 1891. *The open interval* $(0, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$ *is uncountable.*

From this result we could prove that all of $\mathbb{R}$ is uncountable by constructing a suitable bijection (which we will do so at the end of this section). Alternatively, and perhaps more usefully, we can argue that because $(0, 1)$ is a subset of $\mathbb{R}$, then $\mathbb{R}$ cannot be denumerable. By our previous theorem, if $\mathbb{R}$ were denumerable, then it could not have an uncountable subset. This observation is a pretty important one, so let us write it down as its own theorem.

Theorem 12.3.2 *Let A, B be sets with $A \subseteq B$. If A is uncountable then B is uncountable.*

Proof. Prove the contrapositive. If B is countable, then it is either finite or denumerable. If B is finite, then A must be finite. On the other hand if B is denumerable then all its subsets must be denumerable. In either case A must be countable. ■

So — how do we prove the uncountability of $(0, 1)$. This comes down to showing that there cannot be a bijection from $\mathbb{N}$ to $(0, 1)$. Showing the non-existence of an object is often most easily done by contradiction and that is the approach we will take (following in Cantor's footsteps).

So we assume that $(0,1)$ is denumerable meaning there is some bijection $f : \mathbb{N} \to (0,1)$. But this means that we can make a big list of all the numbers in $(0,1)$ (just like we did with the even numbers or the squares or … above). For example, we might have:

$$\begin{aligned} f(1) &= 0.78304492\ldots \\ f(2) &= 0.21892653\ldots \\ f(3) &= 0.15206327\ldots \\ &\vdots \end{aligned}$$

As we construct our list, if we come across a number in $(0,1)$ that has two expansions (like $1/2 = 0.49999 = 0.50000$) then we write down the expansion that ends in all zeros. To complete the proof we need to find a contradiction. We do so by finding a real number in $(0,1)$ that is not on our list. This implies that f is not a bijection and so — contradiction!

To build the number we use a very slick argument[175] argument. Consider the figure below.

$f(1) =$	0.	7	8	3	0	4	4	9	2	$\cdots$
$f(2) =$	0.	2	1	8	9	2	6	5	3	$\cdots$
$f(3) =$	0.	1	5	2	0	6	3	2	7	$\cdots$
$f(4) =$	0.	5	4	3	6	2	9	1	2	$\cdots$
$f(5) =$	0.	8	9	7	5	1	7	5	9	$\cdots$
$f(6) =$	0.	0	3	4	8	0	4	2	5	$\cdots$
$f(7) =$	0.	7	4	3	7	5	8	1	2	$\cdots$
$f(8) =$	0.	3	0	7	0	6	9	6	8	$\cdots$
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$\Delta =$	0.	7	1	2	6	1	4	1	8	$\cdots$
$z =$	0.	1	2	1	1	2	1	2	1	$\cdots$

We have listed out the (hypothetical) values of each number in our list in order: $f(1), f(2), f(3) \ldots$. For each number we have carefully written out its decimal expansion so that all the digits are arranged neatly in an array. Now ignore the leading "0." and focus on those numbers down the diagonal.

[175] Cantor was very very clever. This argument is now called "Cantor's diagonal argument" and it has been used in many places in mathematics. One famous application of the idea is to show that the Halting Problem is not solvable. The interested reader should search-engine their way to more information.

From those digits down the diagonal, we can construct a new number Δ:

$$\Delta = 0.d_1 d_2 d_3 \cdots$$

so that

- The first digit d_1 is first digit of $f(1)$.
- The second digit d_2 is second digit of $f(2)$.
- The third digit d_3 is third digit of $f(3)$.
- $\vdots$
- The n^{th} digit d_n is the n^{th} digit of $f(n)$.
- and so on.

Now because the digits of Δ agree with some of the digits of each of the $f(k)$, it is possible that Δ appears somewhere on our list — so this doesn't give us the contradiction. However, Cantor realised that from Δ, one can construct a number, z, that is definitely not on the list. In particular, construct z so that each digit of z is different from the corresponding digit of Δ.

This means that

- The first digit of z must be different from the first digit of $f(1)$ — so $z \neq f(1)$.
- The second digit of z must be different from the second digit of $f(2)$ — so $z \neq f(2)$.
- The third digit of z must be different from the third digit of $f(3)$ — so $z \neq f(3)$.
- $\vdots$
- The n^{th} digit of z must be different from the n^{th} digit of $f(n)$ — so $z \neq f(n)$.
- and so on.

So if we make the digits of z in this way, it follows that our number z cannot be any number of the list since it has a different expansion[176] . Contradiction!

Let us be more precise about this and make a proof.

Proof. Assume, to the contrary, that $(0,1)$ is countable. Since it is finite, it must be denumerable and so there is a bijection $f : \mathbb{N} \to (0,1)$. Hence we can write $(0,1) = \{x_1, x_2, x_3, \ldots\}$ where $x_i = f(i)$. Now each of these x's has an infinite

[176]We should be a little careful about 9's and 0's when we do this — and we will avoid those two digits when we do this in our proof.

decimal expansion, so we can write a big array as follows:

$$\begin{aligned} x_1 &= 0.a_{11}a_{12}a_{13}\cdots, \\ x_2 &= 0.a_{21}a_{22}a_{23}\cdots, \\ x_3 &= 0.a_{31}a_{32}a_{33}\cdots, \\ \vdots &= \vdots \end{aligned}$$

where each $a_{ij} \in \{0, 1, \ldots, 9\}$.

Now we construct a number z that is not on the list. Write $z = 0.b_1b_2b_3\cdots$. And set

$$b_n = \begin{cases} 1 & \text{if } a_{nn} \neq 1 \\ 2 & \text{if } a_{nn} = 1 \end{cases}$$

and since each digit[a] of z is either $1, 2$ we know that

$$\frac{1}{9} = 0.111111\ldots < z < 0.222222\cdots = \frac{2}{9}$$

and hence $z \in (0, 1)$.

Of course, since f is a bijection, our number z must appear somewhere on our list. So let us assume that it is the k^{th} number on the list, namely that $z = x_k$. But, by construction, the k^{th} digit of z is not the same as the k^{th} digit of x_k. So $z \neq x_k$. In this way, there is no k such that $z = x_k$ and z is not in the list — a contradiction since f must be a bijection.

Hence there is no bijection from $\mathbb{N}$ to the set $(0, 1)$, and thus $(0, 1)$ is uncountable. ■

[a]Note that we could have used any two digits except 9, in order to avoid the problem of representing the same number with two different expansions.

So this Theorem proves that there is more than one type of ∞ — something that is really not at all obvious[177] . Let us push through to all reals now.

Corollary 12.3.3 *The set $\mathbb{R}$ of real numbers is uncountable.*

Proof. If $\mathbb{R}$ were countable, then all its subsets must be denumerable. Since $(0, 1)$ is uncountable, it follows that $\mathbb{R}$ is uncountable. ■

Note that the cardinality of the reals is denoted c, for continuum. That is $|\mathbb{R}| = c$. Since $c \neq \aleph_0$ and $\mathbb{N} \subseteq \mathbb{R}$, we must have $\aleph_0 < c$. Of course, to give a concrete meaning to the symbol "<" in the context of cardinalities of infinite sets, we have to do some work. That is the subject of our next section.

[177]This is a really beautiful result about the nature of the infinite! The author still finds it incredible that one can prove such a deep statement about the universe in a one term course. Remember, we started out with truth tables, and sets and we've just demonstrated that there is not just one infinity! Amazing!

12.4 Comparing cardinalities

12.4.1 Extending to the infinite

So really all[178] we have been able to do so far is show that $|A| = |B|$ and, after borrowing some cunning from Cantor, that $|A| \neq |B|$. Now we will try to understand and give meaning to $|A| \leq |B|$ and $|A| < |B|$. As before, we will try to translate these statements whose meaning are quite simple for finite sets, into statements about functions. From there we can extend them to make sense of infinite sets. This, in turn, will enable us to prove that there is no biggest set and so there an infinite number of infinities!

Let us go back to finite sets for a moment. Consider the sets

$$A = \{a, b, c\} \qquad\qquad S = \{x, y, z, w\}$$

Of course we know $|A| < |B|$. How can we describe this in terms of functions.

- Is there an injection from A to B? — Yes, for example:

$$f(a) = x \qquad\qquad f(b) = y \qquad\qquad f(c) = z$$

- Is there a surjection from A to B? — No — by the pigeonhole principle.
- Since there is no surjection there cannot be a bijection.

In fact this was a corollary of the pigeonhole principle — Corollary 12.1.4.

In the same way that extended the equivalence between the existence of bijections and sets being equinumerous, from finite sets to infinite sets, we extend the above ideas from finite sets to all sets.

Definition 12.4.1 Let A and B be sets.

- We write $|A| \leq |B|$ if there is an injection from A to B.
- Further, we use $|A| < |B|$ to mean that $|A| \leq |B|$ and $|A| \neq |B|$.
- That is, we write $|A| < |B|$ and say A has a smaller cardinality than B if there is an injection from A to B but no bijection.

◊

So with this definition we can now sensibly[179] state that

$$\aleph_0 = |\mathbb{N}| < |\mathbb{R}| = c$$

There are two different infinities — the infinity of the integers, and the larger infinity of the reals.

This inequality prompts two questions.

[178]Mind you we did quite a lot with "just" this.
[179]Well — perhaps "precisely" is a better word than "sensibly".

- Are there more[180] infinities?
- Is there some infinity that lies between α_0 and c?

This first question we can answer and will do so shortly. The second question is due to Cantor and remains unanswered; it now stated as a conjecture called the "continuum hypothesis".

Conjecture 12.4.2 The continuum hypothesis. *There is no set A such that $\aleph_0 < |A| < c$.*

This is generally believed to be true. It is still an active area of research and people have shown quite a bit about what might happen if this result is true and if it is false. In particular — it has been proved that one cannot disprove this using standard set theory (by Gödel 1931). It was then proved that one cannot prove it to be true either (by Cohen 1963).

12.4.2 Cantor's Theorem and infinite infinities

Back to the number of infinities. One relatively easy result shows that there is a set bigger than the reals. We do this by considering a set and its power set. This result, now known as Cantor's theorem, has very interesting consequences.

Theorem 12.4.3 Cantor's theorem. *Let A be a set. Then $|A| < |\mathcal{P}(A)|$.*

For finite sets this result is quite easy. One can prove (using induction, for example) that if $|A| = n$ then $|\mathcal{P}(A)| = 2^n$, and that $n < 2^n$ for any integer n. For infinite sets things are much less obvious.

We start by showing that there is an injection from A to $\mathcal{P}(A)$. An easy one is

$$f : A \to \mathcal{P}(A) \qquad \text{defined by} \qquad f(a) = \{a\}$$

another one is

$$h : A \to \mathcal{P}(A) \qquad \text{defined by} \qquad h(a) = A - \{a\}.$$

We can then show there is no bijection by showing that no function from A to its power set can be surjective. We do this using a proof by contradiction.

Before we do that, let us study these two functions, f and h, a little more. Consider $A = \{1, 2, 3\}$, then we have

$$\begin{array}{lll} f(1) = \{1\} & f(2) = \{2\} & f(3) = \{3\} \\ h(1) = \{2,3\} & h(2) = \{1,3\} & h(3) = \{1,2\} \end{array}$$

[180] Once you show that something isn't unique, it is only reasonable to ask "Well - how many are there?". This was no small part of the controversy that Cantor's work generated. Some Christian theologians thought his results were challenging the notion that the Christian God is unique and absolute. You can certainly find much interesting reading on the implications of Cantor's work.

Notice that f, h take elements of A and turn them into subsets of A.

Look a little more closely at f and you see that $1 \in f(1)$, $2 \in f(2)$ and $3 \in f(3)$. That is

$$\forall a \in A, a \in f(a)$$

Looking at h we see that $1 \notin h(1), 2 \notin h(2)$ and $3 \notin h(3)$. That is

$$\forall a \in A, a \notin h(a)$$

More generally, if we have some function, g, that takes us from A to its power set, then we can try to understand which elements map into their image and which do not. In particular, for which $x \in A$ is $x \in g(x)$, and for which $y \in A$ is $y \notin g(y)$. Understanding those sets of elements will be key to the proof.

So, assume, to the contrary, that there is a surjection (call it g) from A to its power set. Hence the function g takes an element, $x \in A$ and maps it to a subset of $g(x) \subseteq A$. As we noted above, it is possible that when we apply g to an element x we'll get a subset of A that *contains* x. So now let us say that

- an element x is "good" if $x \in g(x)$, and
- an element x is "bad" if $x \notin g(x)$.

So we can now define the set of all good elements, G, and the set of all bad elements, B:

$$G = \{x \in A \mid x \in g(x)\}$$
$$B = \{x \in A \mid x \notin g(x)\}$$

Now both of these are subsets of A and so $G, B \in \mathcal{P}(A)$. Further we see that each element of A must be in exactly one of G, B, and thus

$$G \cap B = \varnothing \qquad \text{and} \qquad G \cup B = A$$

As is often the case, the set of good things is not as interesting as the set of bad things. So though we have defined G, we won't use it further. Instead concentrate on B. By assumption g is surjective, so there must be some element of A that maps to B. That is, there should be $q \in A$ so that

$$g(q) = B$$

We get the contradiction[181] by examining whether or not $q \in B$.

- If $q \in B$, then since $g(q) = B$ we must have (by definition of G) that $q \in G$. However, this is a contradiction — $q \in B$ and $q \notin B$.
- If $q \notin B$, then since $g(q) = B$ we must have (by definition of B) that $q \in B$. However, this is a contradiction — $q \notin B$ and $q \in B$.

In either case we get a contradiction, so no such surjection exists.

[181]This contradiction is reminiscent of Russell's paradox (due to Russell in 1901 and also by Zermelo in 1899). Consider the set of all sets that do not contain themselves. That is $R = \{X \mid X \notin X\}$. One realises the paradox when you try to decide whether $R \in R$ or not. If $R \in R$, then my definition of the set, it cannot be. While if $R \notin R$ then, by definition of the set, it must be. There is much of interest here for a reader armed with a good search-engine.

Proof. We split the proof into three steps.

- We show that the result holds when $A = \varnothing$
- We show that $|A| \leq |\mathcal{P}(A)|$ by giving an injection from A to $\mathcal{P}(A)$.
- Finally, we show that there cannot be a surjection from A to $\mathcal{P}(A)$.

Either A is empty or not. If $A = \varnothing$ then $0 = |A| < |\mathcal{P}(A)| = 1$. So in what follows we can assume $A \neq \varnothing$.

We now construct an injection $f : A \to \mathcal{P}(A)$. Define

$$f(x) = \{x\} \qquad \text{for all } x \in A.$$

To show that this function is injective, let $x_1, x_2 \in A$ and assume $f(x_1) = f(x_2)$. Then $\{x_1\} = \{x_2\}$ and thus $x_1 = x_2$. So f is injective. Thus $|A| \leq |\mathcal{P}(A)|$.

We prove there cannot be a bijection between A and $\mathcal{P}(A)$ by showing that there cannot be a surjection. We do this by contradiction. Assume, to the contrary, that there is a surjection $g : A \to \mathcal{P}(A)$. We then partition A into two subsets

$$G = \{x \in A \mid x \in g(x)\} \qquad \text{and} \qquad B = \{x \in A \mid x \notin g(x)\}.$$

Notice that $B \subseteq A$ and so $B \in \mathcal{P}(A)$.

Since g is, by assumption, a surjection, and B is an element of the codomain of g, there must be $q \in A$ so that $g(q) = B$. Now either $q \in B$ or $q \notin B$.

- If $q \in B$, then since $g(q) = B$ we have that $q \in g(q)$. But then definition of B implies that $q \notin B$, giving a contradiction.
- Similarly, if $q \notin B$, then since $g(q) = B$ we have that $q \notin g(q)$. But then definition of B implies that $q \in B$, again giving a contradiction.

In either case we get a contradiction, and so we must conclude that no surjection g can exist. Thus there is no surjection from $A \to \mathcal{P}(A)$, and thus there is no bijection from $A \to \mathcal{P}(A)$. ■

We can immediately apply Cantor's theorem to the natural numbers to see that

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$$

so we have 2 infinities! But, of course, we can do it again to get another infinity:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))|$$

and again!

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))|$$

And we can keep going and going to get the following corollary.

Corollary 12.4.4 *There are an infinite number of different infinities.*

Proof. Starting with $\mathbb{R}$, we can form $\mathcal{P}(\mathbb{R})$, which is not equinumerous, by Cantor's theorem. But then we can take the power set of that to obtain a yet larger infinite set $\mathcal{P}(\mathcal{P}(\mathbb{R}))$. Continuing in this fashion gives an infinitely long sequence of infinite sets none of which are equinumerous. ■

So we have at least a denumerable number of infinites! In fact there are even more than that! But we'll let you search-engine your way to discussions of that result.

12.4.3 Congratulations are in order

At this point we invite the reader to take stock of what we — ie you! — have managed to do by following along the text. We started by looking at very basic ideas of sets, statements and truth-tables, and have now just proved something fundamental and highly-non-trivial about the nature of infinity! This is no small achievement!

12.4.4 One more question

There is one little question left in this section. From Theorem 12.3.1 we know that

$$|\mathbb{N}| < |\mathbb{R}|$$

and from Theorem 12.4.3 we know that

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$$

but we have not yet compared

$$|\mathcal{P}(\mathbb{N})| \stackrel{?}{=} |\mathbb{R}|$$

One can show that these sets are equinumerous, but constructing an explicit bijection between them is quite difficult. Instead one can prove that

$$|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}| \qquad \text{and } |\mathbb{R}| \leq |\mathcal{P}(\mathbb{N})|$$

by finding injections between those sets. However in order to show that the existence of those injections implies the existence of a bijection, ie

$$(|A| \leq |B|) \wedge (|B| \leq |A|) \implies (|A| = |B|)$$

we need the Cantor-Schröder-Bernstein theorem.

The proof of the Cantor-Schröder-Bernstein theorem is quite involved, so *the proof* is not typically covered in a first course in proof. That being said, the result itself is useful and we do make use of it in some of the exercises for this chapter. Accordingly we encourage the reader to read about the result, skip over the proof, and see how Cantor-Schröder-Bernstein is used to show that $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

The interested reader is, of course, encouraged to read the proof — it is a nice piece of mathematics.

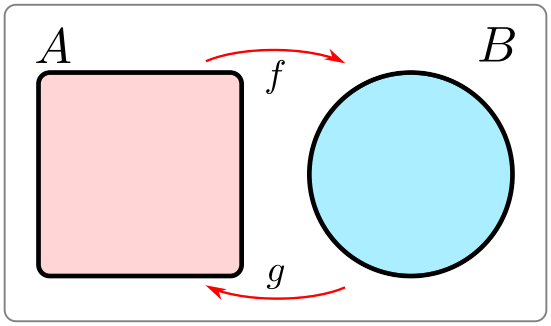
12.5 More comparisons of cardinalties

At this point, we have given extra meaning to the symbols "≤" and '<' so that they can be used to handle cardinalities of infinite sets. In that context do they still behave the same way as they do in the context of (say) comparing real numbers? So, for example, does the following hold:

if $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$

This is equivalent to

If there is an injection from A to B and an injection from B to A, then there is a bijection from A to B.

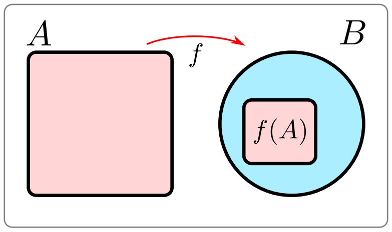


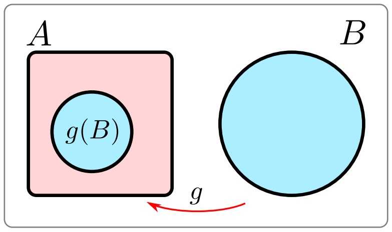
This result is the Cantor-Schröder-Bernstein[182] Theorem

12.5.1 The Cantor-Schröder-Bernstein theorem

Theorem 12.5.1 Cantor-Schröder-Bernstein (and also Dedekind). *Let A, B be sets. If there is an injection $f : A \to B$ and an injection $g : B \to A$, then there is a bijection $h : A \to B$. Equivalently, if $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.*

The proof is by no means trivial; we have some work to do. First up — let us assume that we have those injections $f : A \to B$ and $g : B \to A$.





[182]This was first published without proof by Cantor in 1887. In the same year it was proved by Dedekind, but not published. Schröder gave a proof sketch in 1896, but it was found to be incorrect. Then in 1897, almost simultaneously, Schröder and Bernstein gave correct proofs. At this time, Bernstein was 19 years old! Dedekin proved it again later that year. Why Dedekin doesn't get more credit for this theorem remains mysterious.

We can think of f injecting a copy of A into B — namely $f(A)$. It is not hard to show that by restricting the codomain we can build a function

$$\hat{f} : A \to f(A) \qquad \text{defined by } \hat{f}(a) = f(a)$$

is a bijection. So that looks like a good place to start making our bijection from A to B. We can similarly restrict the codomain of g to construct

$$\hat{g} : B \to g(B) \qquad \text{defined by } \hat{g}(b) = g(b)$$

Since this is also a bijection, its inverse is a bijection — giving us another bijection

$$\hat{g}^{-1} : g(B) \to B$$

This should give us some hope because by restricting codomains we have

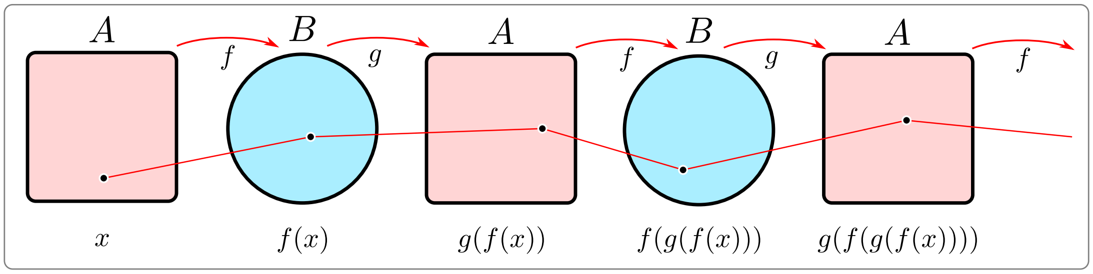
- a bijection, $\hat{f}$, from all of A to some (but not all) of B, and
- a bijection, $\hat{g}^{-1}$ from some (but not all) of A to all of B.

So perhaps we can build a bijection from all of A to all of B by carefully choosing between these two depending on our input.

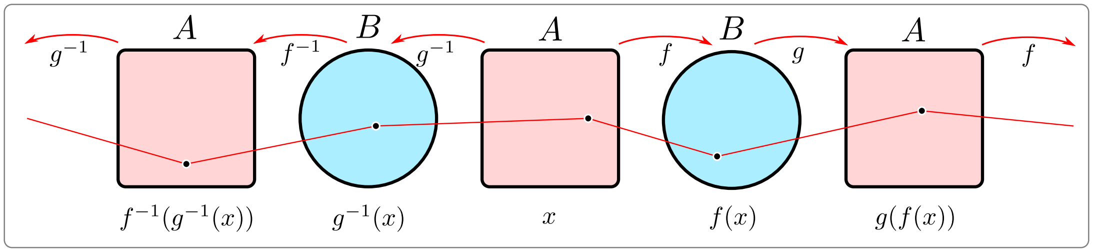
To investigate things a bit further, we should think about what happens when we compose f and g. Let $x \in A$ and consider the image of x under f — we get some element $f(x) \in B$. We cannot do much with this, but we can apply g to it, giving us $g(f(x))$. This, in turn, is some element of A, so we can apply f to it, etc etc. In this way, we can think of the trajectory of x under these two injections.

$$x \mapsto f(x) \mapsto g(f(x)) \mapsto f(g(f(x))) \mapsto \cdots$$

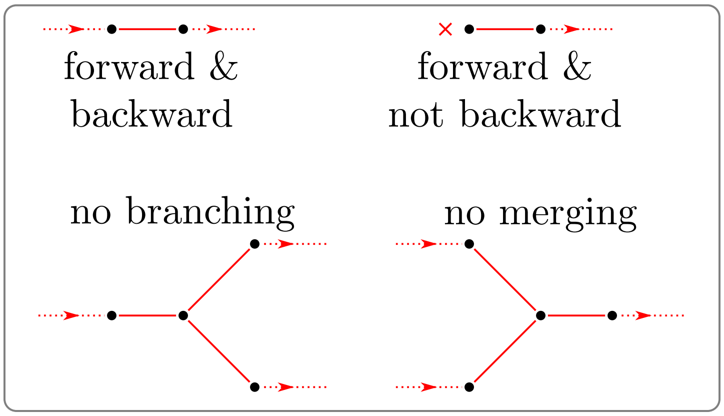
What we have here is the *forward* trajectory of x under f and g.



But we could also go backwards. For any $x \in A$, we can compute the preimage of $g^{-1}(\{x\})$. Since g is injective, we know that that this set is either empty or contains precisely 1 element (otherwise g would fail to be injective). We can make a similar argument about any $y \in B$, its preimage $f^{-1}(\{y\})$ is either empty or contains exactly 1 element. Hence we can extend this trajectory backwards via unique preimages — unless we get stuck at an element whose preimage is empty.

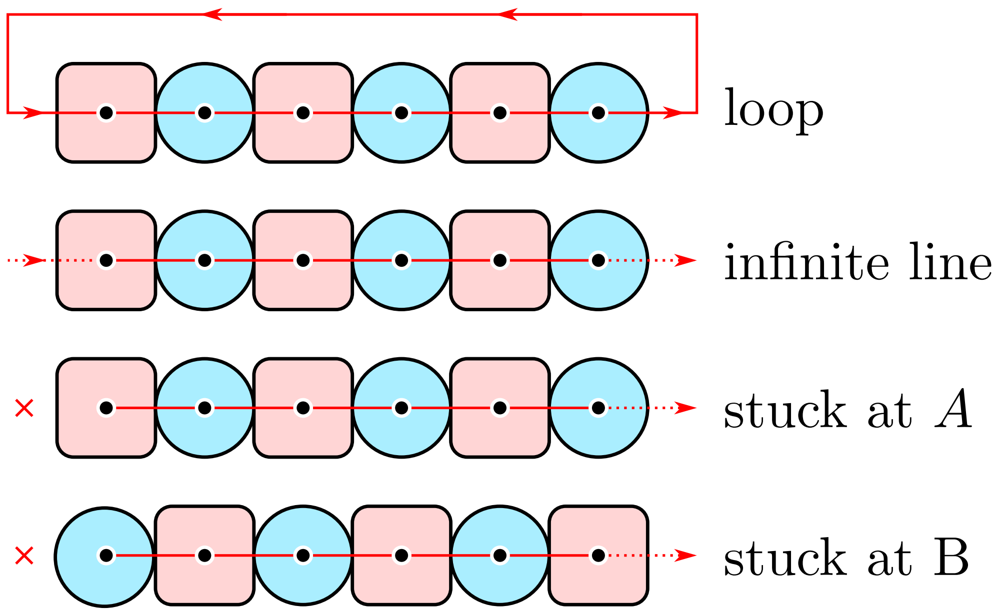


Each element has a unique forward step along its path by applying f or g as appropriate. Similarly, when we step back along the trajectory, we move to a unique element (due to injectivity) by application of f^{-1} or g^{-1}, or the preimage is empty and cannot move any further back. So two trajectories cannot merge, nor can a trajectory branch:



Because of this, the trajectory of any point x can be of 4 types:

- the trajectory forms an infinite line
- the trajectory is a loop
- the trajectory goes forward forever, but going backwards we get stuck at an element of A, or
- the trajectory goes forward forever, but going backwards we get stuck at an element of B.



We cannot have more complicated shapes. Let us call the first three types "good" and the last type — that gets stuck at B — "bad".

Now, define a function $h : A \to B$ by

$$h(x) = \begin{cases} f(x) & \text{if the trajectory of } x \text{ is good, and} \\ g^{-1}(x) & \text{if the trajectory of } x \text{ is bad.} \end{cases}$$

To see that this is actually function — take any element of $a \in A$. We can always form $f(a)$, since f is a function. If a lies on a bad trajectory, then we know we can go backwards until we get stuck at some element of B — thus the preimage of $g^{-1}(a)$ must contain exactly 1 element — which we take to be $h(a)$.

Oof. Now we "just" have to prove this is a bijection.

h is a surjection. Let $b \in B$. Examine the trajectory on which b lies — it is either "good" or "bad".

- If b lies on a good trajectory, then (by moving back one step along the trajectory) there is some $x \in A$ so that $f(x) = y$. This x must also lie on a good trajectory and so $h(x) = f(x) = y$.

- If b lies on a bad trajectory, then (by moving forward one step along the trajectory) we set $x = g(b)$. We know that x also lies on a bad trajectory, so $h(x) = g^{-1}(x) = g^{-1}(g(y)) = y$.

In either case, by moving forward or backward one step along the trajectory of y we find an $x \in A$ so that $h(x) = y$. ■

h is an injection. Let $a, c \in A$, and assume that $h(a) = h(c)$. Notice that by construction, $h(x)$ lies on the same trajectory as x. Thus $a, c, h(a)$ and $h(c)$ must all lie on the same trajectory. That trajectory is either good or bad.

- If the trajectory is good, then $h(a) = f(a)$ and $h(c) = f(c)$ and so $f(a) =$

$f(c)$. Since f is an injection, we know that $a = c$.

- If the trajectory is bad then $h(a) = g^{-1}(a)$ and $h(c) = g^{-1}(c)$. So $g^{-1}(a) = g^{-1}(c)$ — since g is an injection, that preimage contains exactly one element, so we must have $a = c$.

In either case, we have that $a = c$. ■

12.5.2 Applications

The Cantor-Schröder-Bernstein theorem makes proving the following results much easier.

Result 12.5.2 *The sets* $(0, 1), [0, 1), (0, 1]$ *and* $[0, 1]$ *are all equinumerous.*

Proof. By Cantor-Schröder-Bernstein it suffices to construct injections from $(0, 1)$ to $[0, 1)$ and vice-versa to show that they are equinumerous.

- Let $f : (0, 1) \to [0, 1)$ be defined by $f(x) = x$. This is an injection since if $x_1 \neq x_2$ then $f(x_1) = x_1 \neq x_2 = f(x_2)$.
- Let $g : [0, 1) \to (0, 1)$ be defined by $g(x) = 0.1(1+x)$ (there are many similar choices). Again, this is an injection since if $x_1 \neq x_2$ then $g(x_1) \neq g(x_2)$.

We can then show that the second and third sets are equinumerous via the explicit bijection

$$f :[0, 1) \to (0, 1] \qquad\qquad f(x) = 1 - x$$

This is injective since if $f(x_1) = f(x_2)$ then $1 - x_1 = 1 - x_2$ so $x_1 = x_2$. It is surjective since for any $y \in (0, 1]$ pick $x = 1 - y \in [0, 1)$. Then $f(x) = 1 - (1 - y) = y$ as required.

Finally we can prove that the first and last sets are equinumerous by very similar injections to those we used to prove that the first and second sets are equinumerous.

- Let $f : (0, 1) \to [0, 1]$ be defined by $f(x) = x$. It is (immediately) injective by the same argument used above.
- Let $g : [0, 1] \to (0, 1)$ be defined by $g(x) = 0.1(1 + x)$. It is injective by similar arguments.

So by CSB we have that $|(0, 1)| = |[0, 1]|$. ■

This can also be proved without CSB, but it is definitely more work — we'll demonstrate that the first two sets are equinumerous. The approach is to split the set $(0, 1)$ into the set $\left\{\frac{n}{n+1} \mid n \in \mathbb{N}\right\}$ and everything else. Then things of the form $\frac{n}{n+1}$ are mapped to $\frac{n-1}{n}$, so that

$$f(1/2) = 0 \qquad f(2/3) = 1/2 \qquad f(3/4) = 2/3 \qquad f(4/5) = 3/4$$

This way we can map something to 0 while not forgetting or missing any other element.
Proof. Let $f : (0,1) \to [0,1)$ be defined by

$$f(x) = \begin{cases} \frac{n-1}{n} & \text{if } x = \frac{n}{n+1}, n \in \mathbb{N} \\ x & \text{otherwise} \end{cases}$$

We then need to show that this is both injective and surjective.

- Injective — Let $a, b \in (0,1)$ and assume $f(a) = f(b)$. If $f(a) = f(b) = \frac{n-1}{n}$ for some $n \in \mathbb{N}$, then we must have $a = \frac{n}{n+1} = b$. On the other hand if $f(a) = f(b)$ is not of this form then $f(x) = x$, so $a = b$.
- Surjective — Let $y \in (0,1)$. If $y = \frac{n-1}{n}$ for some $n \in \mathbb{N}$, then set $x = \frac{n}{n+1}$. Otherwise set $x = y$. In either case $f(x) = y$ as required.

■

12.5.3 Proof that $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$

From Cantor's theorem we saw that $|\mathbb{N}| < \mathcal{P}(\mathbb{N})|$, and by Cantor's diagonal argument we also saw that $|\mathbb{N}| < |\mathbb{R}|$. It is not unreasonable to ask to compare these two uncountable sets. The following really beautiful result shows that they are actually equinumerous.

Theorem 12.5.3 *The sets $\mathbb{R}$ and $\mathcal{P}(\mathbb{N})$ are equinumerous.*
Proof. By the Cantor-Schröder-Bernstein theorem it suffices to construct injections from $\mathcal{P}(\mathbb{N})$ to $\mathbb{R}$ and vice-versa.

- We define an injection $g : \mathcal{P}(\mathbb{N}) \to \mathbb{R}$. Let $X \in \mathcal{P}(\mathbb{N})$, we can then construct $y = g(X)$ by constructing its decimal expansion. In particular, write $y = 0.y_1y_2y_3y_4\cdots$, and then

  $$y_n = \begin{cases} 1 & \text{if } n \in X \\ 0 & \text{if } n \notin X \end{cases}$$

  Now if we take $X_1, X_2 \in \mathcal{P}$ with $X_1 \neq X_2$, then

  - there is $n_1 \in X_1$ so that $n_1 \notin X_2$, or
  - there is $n_2 \in X_2$ so that $n_2 \notin X_1$, or both.

  In either case, this means that corresponding expansions differ at either y_{n_1} or y_{n_2}, and so $g(X_1) \neq g(X_2)$.

- It is easier to construct an injection from $[0,1)$ to $\mathcal{P}(\mathbb{N})$ rather than from $\mathbb{R}$ to $\mathcal{P}(\mathbb{N})$. However, since we have proved that $|[0,1)| = |(0,1)| = |\mathbb{R}|$, we know there is a bijection between $\mathbb{R}$ and $[0,1)$. So if we compose that bijection with the injection we are about to construct, we get the required injection from $\mathbb{R}$ to $\mathcal{P}(\mathbb{N})$.

Given any $x \in [0,1)$ we write its decimal expansion as $x = 0.x_1x_2x_3\ldots$. As noted above we can make this expansion unique by avoiding any expansion that ends in an infinite sequence of 9's. Using this expansion we can define $h : [0,1) \to \mathcal{P}(\mathbb{N})$ by

$$h(x) = h(0.x_1x_2x_3\ldots) = \left\{x_1, 10x_2, 100x_3, \ldots, 10^{n-1}x_n, \ldots\right\} \subseteq \mathbb{N}$$

So, for example,

$$\begin{aligned} h\left(\frac{1}{4}\right) &= h(0.25) = \{2, 50\} \\ h\left(\frac{1}{3}\right) &= h(0.333\ldots) = \{3, 30, 300, 3000, \ldots\} \\ h\left(\frac{2}{11}\right) &= h(0.181818\ldots) = \{1, 80, 100, 8000, \ldots\} \end{aligned}$$

Now if $x \neq z$ then their decimal expansions must differ at least one digit. Consequently their images will be different subsets of $\mathbb{N}$. Hence the function h is an injection from $[0,1)$ to $\mathcal{P}(\mathbb{N})$, and so there is an injection from $\mathbb{R}$ to $\mathcal{P}(\mathbb{N})$ as required.

■

12.6 (Optional) Cantor's first proof of the uncountability of the reals

For completeness we include Cantor's first proof that $|\mathbb{N}| < |\mathbb{R}|$. This, proved in 1874, is more involved than his very famous diagonal argument which was published in 1891. Despite this it is still accessible to the tools developed in this text.

Like the diagonal argument, this first proof also is a proof by contradiction. We assume the existence of a bijection from $\mathbb{N}$ to an interval of the real-line and then show that this leads to a contradiction. However, rather than relying on decimal expansions of real numbers, it instead relies on the supremum — the least upper bound property. The reader should take a moment to examine Exercise 8.6.15 and Exercise 8.6.16, and also revise Section 6.4 before continuing.

Axiom 12.6.1 Least upper bound property of the reals. *Let $A \subseteq \mathbb{R}$ be bounded above. That is, there is some $M \in \mathbb{R}$ so that $a \leq M$ for all $a \in A$. Then the supremum of A exists and is a real number.*

This is the critical difference between the reals and the rationals — the rationals do not satisfy the least upper bound property. For example, one can take the set of truncated decimal expansions of $\sqrt{2}$:

$$\begin{aligned}\{1.0, 1.4, 1.41, 1.414, 1.4142, \dots\} &= \left\{\frac{1}{1}, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}, \dots\right\} \\ &= \left\{\lfloor 10^n \sqrt{n} \rfloor \cdot 10^{-n} \text{ s.t. } n \in \mathbb{N}\right\} \\ &\subseteq \mathbb{Q}\end{aligned}$$

The least upper bound of this set is $\sqrt{2}$ which is not a rational number 11.2.6.

We can use the least upper bound property to prove[183] that increasing sequences of real numbers that are bounded above must converge to a real limit.

Lemma 12.6.2 *Let (a_n) be a sequence of real numbers that*

- *is bounded above by some real number M, and*
- *satisfies $a_k \leq a_{k+1}$ for all k.*

Then the sequence a_n converges as $n \to \infty$.

Proof. See Exercise 8.6.17. ■

Now we are ready to get into the proof. Let $[a, b]$ be an interval of the real line with $a < b$. Then assume to the contrary, that there is a bijection

$$g : \mathbb{N} \to [a, b]$$

This bijection defines an infinite sequence via $x_n = g(n)$ for any $n \in \mathbb{N}$. Notice that all the terms of this sequence must be distinct since g is injective.

The proof works by finding some $q \in [a, b]$ so that q is not part of the sequence. Hence there is no $n \in \mathbb{N}$ so that $g(n) = q$, and so g is not surjective and hence not bijective.

We construct two new sequences (a_n) and (b_n) from the sequence (x_n).

- Find the first two x_n lying strictly inside the interval, that is $a < x_n < b$. These two terms must be distinct and let a_1 be the smaller and b_1 be the larger.
- Similarly, find the first two terms of the sequence that lie inside (a_1, b_1) — call the smaller a_2 and the larger b_2.
- Keep repeating this to define (a_3, b_3), (a_4, b_4) and so on.

Notice that

- for any n we must have $a_n < b_n$, and
- the sequences of a's and b's satisfy

  $$a < a_1 < a_2 < a_3 < \ldots < b_3 < b_2 < b_1 < b$$

  and so the sequence (a_n) is increasing and bounded above by b, while the sequence (b_n) is decreasing and bounded below by a.

183 This is a nice and intuitive result; in fact it is such a nice result we set it as an exercise 8.6.17.

- the sequences of a's and b's may or may not be infinite.
- for any n, the terms $x_1, x_2, \dots, x_{2n}$ do not lie inside the interval (a_n, b_n).

This last point can be proved quite readily using induction on n.

Lemma 12.6.3 *The interval* (a_n, b_n) *does not contain the sequence terms* $x_1, x_2, \dots, x_{2n}$.
Proof. We prove the result by induction on n.

- Notice that x_1, x_2 must belong to $\{a, b, a_1, b_1\}$ (by construction). Thus $x_1, x_2 \notin (a_1, b_1)$ since the open interval exludes the endpoints.
- Now assume that the result holds for $n = k$, and so $x_1, x_2, \dots x_{2n}$ are lie outside the interval (a_n, b_n). Then either x_{2n+1}, x_{2n+2} lie outside this interval, or, if they lie inside the interval they are one or both of a_{n+1}, b_{n+1}. Consequently they lie outside (a_{n+1}, b_{n+1}).

Hence the result holds for all $n \in \mathbb{N}$. ■

The sequences $(a_n), (b_n)$ may or may not be infinite. So initially assume that they are finite. That is, the final interval is (a_N, b_N). Now notice that there cannot be two or more x_n inside the interval (a_N, b_N) because otherwise we would use those to define another interval (a_{N+1}, b_{N+1}). Thus there are either zero or one more term of the sequence (x_n) lying inside (a_N, b_N). But this means that any other number inside (a_N, b_N) is not part of the sequence (x_n). That is, there is some $q \in (a_N, b_N)$ so that $q \neq x_n = g(n)$ for any $n \in \mathbb{N}$.

Now instead, assume that the sequences of a's and b's are infinite. Since the sequence of a's is increasing and bounded above by b, Lemma 12.6.2 implies that it converges to a limit. The same argument (applied to $-b_n$) shows that the sequence of b's also converges to a limit. So define

$$\lim_{n\to\infty} a_n = \alpha \qquad \lim_{n\to\infty} b_n = \beta.$$

Notice that we cannot have $\beta < \alpha$ (otherwise we would have $a_k > b_k$ for some k), and so either $\alpha < \beta$ or $\alpha = \beta$.

- If $\alpha < \beta$, then every $q \in (\alpha, \beta)$ is not in the sequence of x's. If $q = x_n$ for some n, then this would contradict Lemma 12.6.3 above, since it would imply that $q = x_n \in (\alpha, \beta) \subseteq (a_n, b_n)$.
- On the other hand, if $\alpha = \beta$, then $q = \alpha$ is not in the sequence of x's. If $q = \alpha = x_n$ for some n, then again this would contradict Lemma 12.6.3 since it would imply that $q = x_n = \alpha \in (a_n, b_n)$.

Thus even when the sequences of a's and b's are infinite, there is always some $q \in [a, b]$ that is not in the sequence of x's. Hence the function $g : \mathbb{N} \to [a, b]$ is not a surjection, contradicting our initial assumption that it is bijective.

12.7 Exercises

1. Show that each of the following sets are denumerable, by construction a bijection between them and the natural numbers.

(a) $\mathbb{N} \cup \{0\}$

(b) $\{5, 6, 7, 8, \dots\}$

(c) $\{1, 3, 3^2, 3^3, \dots\}$

(d) $\mathbb{Z} \setminus \{0\}$

2. Suppose $A = \{(m, j) \in \mathbb{N} \times \mathbb{R} : j = \pi m\}$. Is it true that $|\mathbb{N}| = |A|$?

3. Let $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the function

$$f(m, n) = 2^{m-1}(2n - 1).$$

Can you use this f to conclude that $\mathbb{N} \times \mathbb{N}$ is denumerable?

4. Describe a partition of $\mathbb{N}$ that divides $\mathbb{N}$ into $\aleph_0$ countably infinite subsets. That is, partition $\mathbb{N}$ into an infinite number of subsets, each of which is itself infinite.

5. Theorem 12.2.3 states that $\mathbb{Z}$ is denumerable. We claimed that $f : \mathbb{N} \to \mathbb{Z}$ given by

$$f(n) = \begin{cases} \frac{1-n}{2} & n \text{ is odd} \\ \frac{n}{2} & n \text{ is even} \end{cases}$$

is a bijection. Prove this now.

6. Determine if each of the following sets is denumerable.

(a) The set of irrational numbers, $\mathbb{I}$

(b) $[0, 1] \cap \mathbb{Q}$

(c) $\{\pi + q : q \in \mathbb{Q}\}$

(d) $\{a + q : q \in \mathbb{Q}\}$ for some fixed $a \in \mathbb{R}$

(e) $\{\pi q : q \in \mathbb{Q}\}$

(f) $\{aq : q \in \mathbb{Q}\}$ for some fixed $a \in \mathbb{R}$

7. Prove that the set of all irrational numbers is uncountable. You may assume the fact that the set of real numbers is uncountable.

8. Prove that $(-\infty, -\sqrt{29})$ and $\mathbb{R}$ are equinumerous by constructing an explicit bijection between them.

9. Let S be the set of all functions $f : \mathbb{N} \to \{0, 1\}$. Prove that S is uncountable.

Notice that the codomain of these functions is the set that contains just two elements, zero and one. It is not the set of all reals between 0 and 1.

10. Show that $\mathbb{R}$ and $(0, 1)$ are equinumerous by giving two different explicit bijections.

11. Show that the two given sets have equal cardinality by describing a bijection from one to the other. Describe your bijection with a formula (not as a table).

(a) $\mathbb{R}$ and $(\sqrt{2}, \infty)$

(b) The set of even integers and the set of odd integers

(c) $\mathbb{Z}$ and $S = \{x \in \mathbb{R} : \sin x = 1\}$

(d) $\{0, 1\} \times \mathbb{N}$ and $\mathbb{Z}$

12. Let A, B, C, D be any nonempty sets. Suppose that $A \cap C = \emptyset$ and $B \cap D = \emptyset$, and that $|A| = |B|$ and $|C| = |D|$. Show that $|A \cup C| = |B \cup D|$.

13. Construct an explicit bijection between the sets $(0, \infty)$ and $(0, \infty) - \{1\}$ to show that $|(0, \infty)| = |(0, \infty) - \{1\}|$.

You must prove that your function is a bijection.

14. Show that the following pairs of sets are equinumerous.

(a) $(0, 1) \times (0, 1)$ and $(0, 1)$

(b) $\mathbb{R}^2$ and $\mathbb{R}$

15. Let A and B be equinumerous sets. Show that $|\mathcal{P}(A)| = |\mathcal{P}(B)|$.

16. Prove or disprove: The set $\{(a_1, a_2, a_3, \ldots) : a_i \in \mathbb{Z}\}$ of infinite sequences of integers is countably infinite.

17. Let A and B be sets. Let P be a partition of A, and let Q be a partition of B. Suppose that we have a bijection between the partitions, $h\colon P \to Q$, with the additional property that $|X| = |h(X)|$ for every set $X \in P$.

Prove that the underlying sets, A and B, have the same cardinality.

18. Let A, B, and C be sets.

(a) Suppose that $|A| \le |B|$ and $|B| \le |C|$. Show that $|A| \le |C|$.

(b) Show that the following statement is equivalent to the Cantor-Schröeder-Bernstein 12.5.1:

Suppose that $|A| \le |B| \le |C|$, and that $|A| = |C|$. Then $|A| = |B| = |C|$.

19. Let $F_n = \{X \subset \mathbb{N} \colon |X| = n\} \subseteq \mathcal{P}(\mathbb{N})$.

(a) Prove that for every $n \in \mathbb{N}$, $|F_n| = |\mathbb{N}|$.

(b) Also show that $\left| \bigcup_{n \in \mathbb{N}} F_n \right| = |\mathbb{N}|$.

(c) Does the result in part (b) contradict the fact that $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$?

Explain why or why not (you do not need to give a formal proof).

20. Consider the following questions about countable unions of countable sets.

(a) Let $A_1, A_2, A_3, \ldots$ be denumerable sets, and suppose that $A_m \cap A_n = \emptyset$ whenever $m \neq n$. Show that

$$\bigcup_{n=1}^{\infty} A_n$$

is denumerable as well.

(b) Now suppose $A_1, A_2, A_3, \ldots$ are countable sets, and suppose that $A_m \cap A_n = \emptyset$ whenever $m \neq n$. Show that

$$\bigcup_{n=1}^{\infty} A_n$$

is countable as well.

(c) Redo part (b), but without the assumption that $A_m \cap A_n = \emptyset$ whenever $m \neq n$.

21. In the following exercises, you may use the result from Exercise 12.7.20 and the Fundamental Theorem of Algebra: a degree n polynomial has at most n real solutions.

(a) Let $m \in \mathbb{N}$. Define P_m to be the set of degree m polynomials with rational coefficients. That is,

$$P_m = \{a_0 + a_1 x + \cdots + a_m x^m \mid a_i \in \mathbb{Q} \text{ for all } i \in \{0, 1, \ldots, m\},\ a_m \neq 0\}.$$

Show that P_m is countable.

(b) Now, define P to be the set of all polynomials with rational coefficients. That is,

$$P = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N} \text{ and } a_i \in \mathbb{Q} \text{ for all } i \in \{0, 1, \ldots, n\},\ a_n \neq 0\}.$$

Prove that P is countable.

(c) Define A to be the set of all real numbers that are the roots of a polynomial in P. That is,

$$A = \{x \in \mathbb{R} \mid \exists f \in P \setminus \{0\} \text{ s.t. } f(x) = 0\}.$$

Prove or disprove: $|A| = |P|$.

Appendix A

Hints for Exercises

1 · Sets

1.4 · Exercises

1.4.2.

(a) No hint.

(b) No hint.

(c) The elements of the set are close to other numbers that may be easier to find connection between.

(d) Can you see a connection between the numerators and the denominators? The previous question may give you a hint.

(e) What do the elements have in common?

(f) What do the elements have in common?

1.4.5. Pay close attention to notation! For part (h), this is an issue you would only come across if you are typing your math in a program such as LaTeX.

1.4.9. Try writing out the first few terms of each set.

2 · A little logic

2.7 · Exercises

2.7.9. Carefully determine what is the hypothesis and what is the conclusion of each implication, and then refer to the truth table of the implication.

2.7.14. What is the only situation in which an implication is false?

2.7.15. Is the conclusion of the implication true or false? What does that tell you?

2.7.16. You don't have to use truth tables to determine the answer (although you could).

3 · Direct proofs
3.5 · Exercises

3.5.1. Think about what does being even mean and how we can use it.

3.5.2. Think about what being odd means and how we can use it.

3.5.6. Think about what it means for n to divide a and b, and how we can use that information.

3.5.7. Think about the divisors of 1 and how you might use that.

3.5.8. Think about how we can get from 2 and 3 to 6.

3.5.9. Think about what it means for 3 to divide an integer and how we can use that information.

3.5.13. Try writing down different integer roots and check whether their product is also an integer root.

3.5.16. Try writing the inequality in a different way, the difference of squares might help.

4 · More logic
4.3 · Exercises

4.3.2. Refer back to Exercise 2.7.5 and use Theorem 4.2.3.

5 · More proofs
5.5 · Exercises

5.5.3. What is the contrapositive of this statement?

5.5.4. What is the contrapositive of the statement?

5.5.5. What is the contrapositive of the statement?

5.5.9. Think carefully about the parity of n.

5.5.10. The ideas used in the solution of Exercise 3.5.8 may be useful.

5.5.11. Try proving by cases.

5.5.12. Think carefully about the contrapositive.

5.5.13. What is the contrapositive of the statement?

5.5.15. If we assume the hypothesis is true, then what do we know about q?

5.5.16. Expand the cubes and simplify the sum

5.5.17. Modular arithmetic makes this much easier.

5.5.18. You may want to look at cases for $x \in \mathbb{R}$ to get rid of the absolute values.

5.5.21.

- Notice that the statement is equivalent to proving

$$-|x-y| \leq |x| - |y| \leq |x-y|.$$

- Use the triangle inequality!

5.5.22. Try sketching the function.

6 · Quantifiers
6.6 · Exercises

6.6.1. You can think about the division algorithm and cases for n. Also try factoring things.

6.6.2. Try to eliminate n. What does this tell you about k? What else do you know about k?

6.6.3. What can you say about a^2 modulo 4 for all $a \in \mathbb{Z}$?

6.6.6. Try playing around with some simple functions.

6.6.7. If you are unsure if the statement is true or not, then explore its negation — it might be easier to understand.

6.6.9. Which primes are even?

6.6.11. Think carefully about the truth table of the implication. Also, negate carefully. Finally, be careful with your inequalities.

6.6.12. Be careful of the order of quantifiers; make sure you pick variables in the correct order.

6.6.13. Start with a few simple functions you know well. Sketch them and try to decide if they are type A or type B or neither. Also, you should write out the negations of these definitions; what does it mean if a function is not type A? what does it mean if it is not type B?

6.6.19. Can you bound $\sin(1/x)$ by a simpler function?

6.6.20. Carefully negate the definition of convergence. Also, explore the first few terms of the sequence.

6.6.23. Split the sequence at some large N, so that when $n \geq N$, we know that a_n is really close to L. We can use this to bound $|a_n|$ when $n \geq N$. That leaves us to bound only finitely many of the terms $|a_n|$, the terms for which $n < N$. While we cannot take the maximum of an infinite set of values, we can find the maximum of a finite set of values and it will be finite. See Exercise 7.3.16 which explores this point.

6.6.24. For part (c), the contrapositive can help. Also, see Exercise 4.3.1 (c).

6.6.25. For part (b), try some of the sequences we have seen that converge with the Euclidean distance, and see whether they converge under this new distance? Choosing your ε satisfying $0 < \varepsilon < 1$, would be very useful in understanding the convergence of a sequence.

7 · Induction
7.3 · Exercises

7.3.2. Write out the statement for $n = k$ and $n = k + 1$ and try to work out how to make the left-hand side of the first statement look like the left-hand side of the second statement.

7.3.4. How can we get from z^{2n+1} to $z^{2(n+1)+1}$?

7.3.5. The even-ness of the exponent is required, otherwise the statement is simply not true:

$$3^3 - 1 = 27 - 1 = 26$$

and 8 definitely does not divide 26. Rephrase things to take advantage of what you know about even numbers.

7.3.10. The sum $\sum_{k=1}^{n} k$ is a very standard result and is in the main text. You can use that result without proof.

7.3.11. Be careful when you expand $(n + 1)^3$ and $(n + 1)^4$.

7.3.13.

- Take the first few derivatives and see if you can find a pattern.
- The factorial will be helpful. Recall that for any $n \in \mathbb{N}$,

  $$n! = n \cdot (n - 1) \cdot (n - 2) \cdots 2 \cdot 1$$

  and also the double-factorial $n!!$

  $$n!! = \begin{cases} n \cdot (n-2) \cdot (n-4) \cdots 2 & \text{when } n \text{ is even} \\ n \cdot (n-2) \cdot (n-4) \cdots 3 \cdot 1 & \text{when } n \text{ is odd} \end{cases}$$

7.3.14. Factoring a cubic can be painful. Perhaps write down the cubics you need and then expand them out. This might help with some of the arithmetic.

7.3.15. Adding to the end of the series will get you intro trouble. Try adding to the beginning instead. You might have to think about that a little.

7.3.17. For (b) try integration by parts.

7.3.19. Notice that every number is of the form

$$100 \underbrace{1 \cdots 1}_{n \ 1s} 7$$

Also useful is the fact that if $d \mid a$ and $d \mid b$, then $d \mid (a + b)$.

7.3.20. The proof of Result 7.2.18 works because 5 is a Fibonacci number. See how you might generalise what is happening in the proof.

7.3.21.

- For Pascal's identity, rewrite the binomials as factorials and juggle carefully.
- For the binomial theorem, expand and group carefully. The following might

also be handy

$$\binom{n}{0} = \binom{n}{n} = 1.$$

Also, be careful around the edges of your expanded sums.

7.3.22. Integrate by parts!

7.3.23. As a base case, consider $n = 0$ and $n = 1$. This means that your inductive hypothesis can include both the $n - 1$ and n cases.

7.3.25. Shops will not be intimidated by excess purchasing power; even though you have lots of money, this fictional mathematical country does not allow you to overpay for an item.

7.3.27. Strong induction helps, as does the parity of the number.

7.3.28. You can simplify the analysis of the floor function by studying even and odd values separately.

7.3.29. Be careful as to how you can go from $k = n+1$ stones to $k \leq n$ stones in your inductive step and see whether different splittings change the calculations. Try playing this game with 5 or 6 stones to get a better understanding of how this works.

8 · Return to sets

8.6 · Exercises

8.6.3. Revise the definition of set-differences and then try to make a small example.

8.6.9. Remember that the power set is the set of subsets. That is

$$X \in \mathcal{P}(A) \iff X \subseteq A.$$

8.6.11. You may need to use mathematical induction on the size of A.

8.6.12. Try some small examples of sets A, B to gain some intuition.

8.6.13. Recall that

- $x \in \bigcup_{i \in I} A_i$ if and only if there is some $i \in I$ so that $x \in A_i$, and
- $x \in \bigcap_{i \in I} A_i$ if and only if for every $i \in I$ we have $x \in A_i$.

8.6.15. In order to prove that a is the supremum of a set S, it suffices to show that a is an upper bound for S, and that if $b < a$, then b is not an upper bound of the set. The latter statement may be rephrased as follows: if $b < a$, then there is some $s \in S$ with $s > b$.

If you want to show instead that S has no maximum, prove that any $s \in S$ is not an upper bound of the set. That is, for any $s \in S$, there is some $t \in S$ with $t > s$.

8.6.16. Suppose we are trying to prove that a is the least upper bound of a set S. Then we need prove that the two defining properties of the supremum hold for a. In order to prove the statement "if b is an upper bound for S, then $a \leq b$," it may be easier to show the contrapositive, "if $b < a$, then b is not an upper bound for S." In order to prove that contrapositive, we need to show that for any $b < a$, there is some $s \in S$ so that $s > b$. Then b will not be an upper bound for S, by definition.

8.6.17. For any ε, we know that $a - \varepsilon$ is not an upper bound of the set $\{a_n : n \in \mathbb{N}\}$.

9 · Relations

9.7 · Exercises

9.7.7. You can first look at the relation R for $E = \{1, 2, 3, 4\}$, and $q = 1$ to understand the relation better. Also, recall that $\overline{A} \cap \overline{B} = \overline{A \cup B}$.

9.7.10. Try looking at examples of relations on a small set, like $A = \{1, 2, 3\}$.

9.7.11. For part (a), try looking at examples of relations on a small set, like $A = \{1, 2, 3\}$.

9.7.12. Try some simple examples on small sets. Also, modus-tollens might help.

9.7.13. For the first part, the result in Exercise 3.5.7 will be useful.

9.7.14. Remember that every element of the set R is the intersection of two elements of P and Q. Also, read the definition of partitions carefully.

9.7.15. For the second part, start by finding the invertible elements in $\mathbb{Z}_6$

9.7.16.

(a) Bézout's identity tells you about the greatest common divisor of two numbers. What does it tell you about some of the numbers in the statement of the question? How can you use that information to get an equation for n?

(b) When a prime is at least 5 what do you know about its remainder when you divide by 3 or 8 or 24? And how can you turn the congruence we want to prove into a statement about divisibility? And how can we use (a) to reduce the number of cases we need to check?

9.7.17. Try using Bézout's identity.

9.7.18. Try modifying the proof of Euclid's lemma 9.5.9.

9.7.19.

- For part (a), try using Bézout's identity.
- For part (b), we can show that the two quantities are equal by showing that $m \gcd(a, b) \leq \gcd(ma, mb)$ and $\gcd(ma, mb) \leq m \gcd(a, b)$. Also, for any $d, e \in \mathbb{N}$, one way to show that $d \leq e$ is to prove that $d \mid e$.

- For part (c), some small numbers will help you build a counter-example.

9.7.20.

(a) The recurrence for the binomial coefficients is just adding integers.

(b) Think about prime factors.

(c) What coefficients in the sum are not divisible by p?

10 · Functions

10.8 · Exercises

10.8.1. The question asks for the range, not the codomain.

10.8.2. Remember that a function has to give a valid output for every valid input — why does this tell you about the y-values?

10.8.3. How do we show that two sets are equal?

10.8.5. Recall that

$$x \in f^{-1}(D) \iff f(x) \in D.$$

Also, modus tollens 2.5.2 can help you.

10.8.6. Completing squares may help with the answer (to be honest, completing squares will help you with almost everything quadratic functions related, cherish it).

Also, try choosing some small a, b values and sketch the function.

10.8.7. Can you determine $f(n)$ for small $n \in \mathbb{N}$?

10.8.8. This is a good example as to why when we want to determine whether a function is injective and/or surjective, we shouldn't only look at `what kind' of a function it is, but also consider the domain and the codomain of the function as well.

Remember, a function is not just a formula!

10.8.9.

- You can start the problem with a small set, say $A = \{1, 2, 3\}$, to understand the set F and the function g.
- To find $|F|$, think about how many different images there are there for each element in A.

10.8.11. For one side of the implication, think about how we can express the surjectivity in terms of the codomain and the range.

10.8.13. Think how an integer factors.

10.8.14.

- You need to do a lot of work mapping elements and subsets. We recommend that you use (say) x, y to denote elements of A and B, and (say) X, Y to denote subsets of A, B (which makes X, Y elements of $\mathcal{P}(A), \mathcal{P}(b)$).

- Try this with two small sets. For example, take $A = \{1, 2, 3\}$ and $B = \{10, 20, 30\}$. Construct a simple bijection from A to B and then use that to make a bijection from $\mathcal{P}(A)$ to $\mathcal{P}(B)$.

10.8.15.

- What do the equivalence classes of $\mathcal{R}$ look like?

- How can we show that f is, indeed, a function?

10.8.16. To show that an integer is zero, one can show that it is small and divisible by a bigger integer.

10.8.17. Be careful, the symbol f^{-1} denotes the preimage not the inverse-function. It only denotes the inverse-function when the function is bijective.

Also, see Theorem 10.3.6 and its proof.

10.8.18. Be careful, the symbol f^{-1} denotes the preimage not the inverse-function. It only denotes the inverse-function when the function is bijective.

Also, see Theorem 10.3.6 and its proof.

10.8.20. To show that two functions with same domains and codomains are different, it suffices to show that there is a single point at which they differ. To show that they are the same, you must show they are equal on every point of the domain.

10.8.21. Try to construct counterexamples on small sets (eg. $\{1, 2, 3\}$) rather than on $\mathbb{R}$.

10.8.22. Two functions are equal when they are equal at all points in their domains.

10.8.23. Your observations from part (b) can be helpful in solving part (c).

10.8.24.

- You may need to show that if $f \circ g$ is injective then g is injective, and then show that if $f \circ g$ is surjective then f is surjective.

- Combining part (a) with Theorem 10.5.3, we know that f is bijective if and only if $f \circ f$ is bijective.

- For part (b), it might help to compute $(f \circ f)(x)$.

10.8.26. Observe that f takes even numbers to odd numbers and odd numbers to even numbers. Considering that, what should the inverse of f look like?

Also - there are some very *handy* lemmas in Section 10.6.

10.8.27. Make good use of the fact that

$$g(g(g(x))) = (g \circ g)(g(x)) = i_A(x) = x.$$

11 · Proof by contradiction

11.3 · Exercises

11.3.1. If a were to satisfy both congruences, then we get 2 equations. Combining them helps.

11.3.3. Remember that 1 is not divisible by very many integers!

11.3.5. Modular arithmetic can really help with problems like this since they take all the infinite possible integers down to a small finite set of equivalence classes. Consider the equation modulo 4.

11.3.6. Try adapting the proof of Result 11.1.2.

11.3.7.

(a) Remember that $2 \mid 6$.

(b) The result from (a) can help you with (b). How can we manipulate $(\sqrt{2}+\sqrt{3})$ to somehow get an expression involving $\sqrt{6}$? Or, alternatively, how can we use that expression to say something about $\sqrt{2}$?

11.3.8. Please observe that $25 \mid 5^3$.
Euclid and the prime-ness of 5 also help.

11.3.9. Prove this by contradiction, but negate the statement carefully. Then, to get more information, Bézout's identity could be very useful.

11.3.12. What would the equation look like if x were a rational number?

11.3.14. If A were to have a maximum, what is the difference between $\sqrt{2}$ and that? It is not a rational number, but how can we use it to make a rational number that is still in A?

11.3.15.

- This may look like an induction question, but it's not!
- Euclid's lemma 9.5.9 should be useful, which tells us that if a prime p divides ab, then $p \mid a$ or $p \mid b$.
- What power of 7 divides 35?

11.3.19. What would happen if the function weren't strictly increasing or decreasing?

12 · Cardinality

12.7 · Exercises

12.7.4.

- Splitting $\mathbb{N}$ into even and odd doesn't work because it is a partition into only two parts.
- Similarly, splitting $\mathbb{N}$ as $\{\{n\} \,|n \in \mathbb{N}\}$ doesn't work because the parts are all finite.

12.7.6. Your answers for (d) or (f) may depend on (a).

12.7.8. Can you think of a bijection from $(0, \infty)$ to $\mathbb{R}$ How can we use that function in this question?

12.7.9. Question 13 in Section 10 may be useful.

12.7.10. Try sketching the graph of potential bijections from $(0, 1)$ to $\mathbb{R}$.

12.7.12. The sets do not have to be finite.

12.7.13. The explicit bijection in the proof of {*Result 12.5.2*} may be useful.

12.7.14. For part (a), try to define an injection from each set to the other; you can then use Cantor-Schröder-Bernstein 12.5.1 to infer there is a bijection between the sets. For the function from $(0, 1) \times (0, 1)$ to $(0, 1)$, consider the decimal representation of elements in $(0, 1)$.

12.7.15. Remember that the sets A and B may be infinite!

12.7.16.

- Any $x \in \mathbb{R}$ can be written as $x_0.x_1x_2x_3x_4\ldots$ where $x_0 \in \mathbb{Z}$ and $x_i \in \{0, 1, \ldots, 9\}$ for $i \geq 0$. For example, if $x = 3.141592\ldots$ then

$$\begin{array}{llll} x_0 = 3 & x_1 = 1 & x_2 = 4 & x_3 = 1 \\ x_4 = 5 & x_5 = 9 & x_6 = 2 & \cdots \end{array}$$

- We need to be careful! Notice that $0.25000000\cdots = 0.24999999\ldots$.

12.7.17.

- The function h is not a from A to B, it is a function from the partition P to the partition Q.
- What does it mean for X and $h(X)$ have the same cardinality?
- Corollary 9.3.7 may be useful.

12.7.20. Try using the diagonal sweeping argument given in the proof of Result 12.2.6. For part (c), try defining new sets B_n such that

$$\bigcup_{n=1}^{\infty} A_n = \bigcup_{n=1}^{\infty} B_n$$

and $B_n \cap B_m = \emptyset$ for $m \neq n$. Then apply part (b).