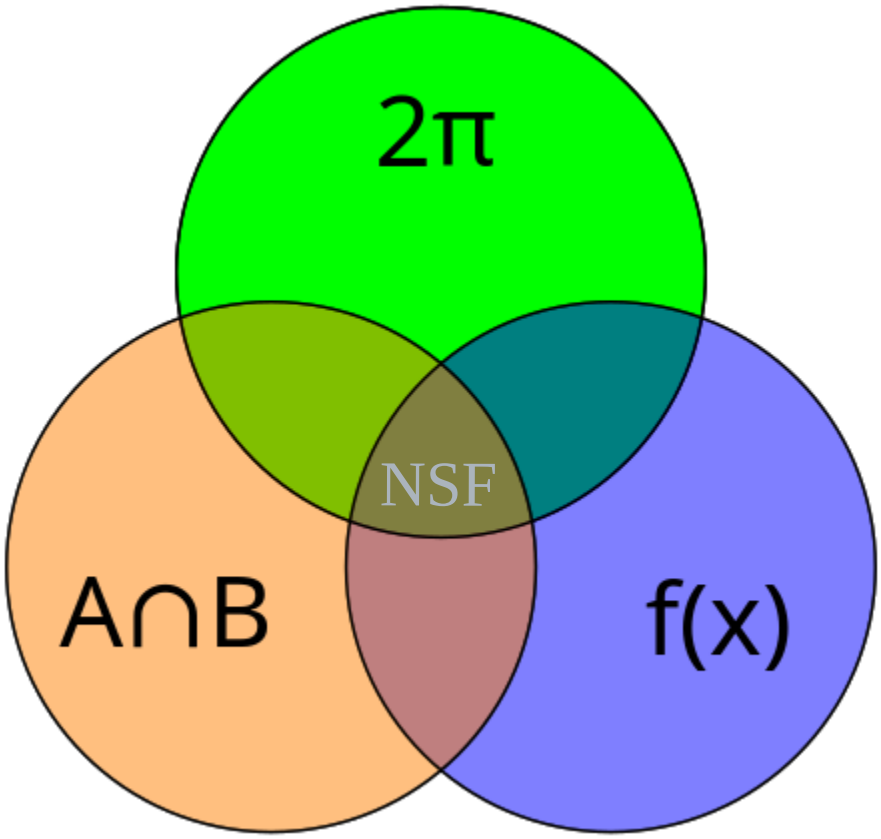
MTH4113/4213: NUMBERS, SETS, AND FUNCTIONS LECTURE NOTES (2025–2026)

DR ARICK SHAO



Queen Mary
University of London

Contents

1. Introduction

Welcome to Numbers, Sets, and Functions (which we will abbreviate as NSF from here on)! As you may already know, this is a required module for all first-year undergraduate students in the *School of Mathematical Sciences*. However, you may be less aware of what NSF is about, and what you will be asked to learn and do for the module.

In short, the main purpose of this module is as an *introduction to university-level mathematics*—in particular to proofs, sets, abstractions, and mathematical rigour in general. For many of you, this may be your first encounter with these concepts. Thus, NSF is intended to smooth the transition from the mathematics you have seen, in secondary school and before, to the material you will encounter as an undergraduate student.

As you will soon see, higher-level rigorous mathematics is, in many ways, a completely different beast than what you have tackled in the past, and you will need to acquire a new way of thinking to successfully navigate this. In NSF, we will begin to develop these skills, in particular the ability to critically reason in a very precise way.

1.1. **Mathematical Thinking.**

What distinguishes mathematics from other academic disciplines? Or, more practically, *what special skills do one acquire from a mathematics degree, in contrast to other degrees*? When asked what makes mathematics special, a common reply might be something like "numbers" or "computations". However, this would not be so accurate, as scientists and engineers (as well as students pursuing such degrees) do plenty of numerical computations—often more than mathematicians! Thus, it is worth spending a few minutes getting to the heart of this question.

At the most basic level, mathematicians are curious people who aim to solve problems. For example, one might wonder what the area of the inside of a unit circle is, or whether a differential equation has a unique solution given certain initial conditions. This is analogous to, say, a scientist asking how a human cell reproduces, or a philosopher inquiring how the moral evaluation of a person should be affected by life circumstances.

What separates mathematics from science, philosophy, and other areas of study is *how its questions are answered*, which in turn determines *the kinds of questions that can be posed*. In science, one cannot simply fabricate any theory and deem it credible. Proposals of a scientific theory must be confirmed repeatedly through experimentation and empirical observations. Analogously, one establishes the truth of a mathematical claim by "proving it"—that is, by providing a *proof* that justifies the claim. This is the fundamental line in mathematics separating a confirmed true statement from mere speculation.

Therefore, the process of devising and writing proofs forms a central pillar of mathematical thinking. Let us now be a bit more precise as to what a proof is:

Definition 1.1. *A proof is a formal logical argument justifying that a mathematical statement is true, by proceeding from given assumptions to the desired conclusion.*

To give just a basic idea, here we present a sample mathematical claim:

Theorem 1.2. *The sum of two even numbers is even.*

We might think it is quite obvious the above statement is true, just by tinkering around with some small numbers. In order for this "fact" to carry actual mathematical weight, however, we must prove it by logically deducing this from existing knowledge:

Proof. Suppose x and y are even numbers. Then, by definition of even numbers, there are numbers (more specifically, integers) k and l such that

$$x = 2k, \qquad y = 2l.$$

But then,

$$x + y = 2k + 2l = 2(k + l).$$

Since $x + y$ is 2 times the number $k + l$, then $x + y$ is even, as desired. □

There is no need to worry if you are not yet comfortable with proofs such as the above, or with how one might come up with such a proof. This is a skill you will gradually learn as you progress through this module, and you will study many more proofs soon.

Many problems that one encounters in mathematics are much more complicated than the above sample, and one needs a combination of knowledge, technical ability, and creativity in order to solve them. The proofs that you find in NSF will be simpler in comparison, thus this module will serve as a playground for you to obtain the background and practice needed to handle more challenging problems and proofs later on.

1.2. **Why Prove Things?** Now, you may wonder why one goes through the formal exercise of writing a proof. After all, the statement that "the sum of even numbers is even" seems obvious enough. The philosophical answer is that, as mentioned before, proofs are how truth is determined in mathematics. Just as one values scientific theories that have been confirmed repeatedly through experiments and observations, one similarly values mathematical statements that have passed the litmus test of being justified through proof.

For example, for the theorem above, you could trying adding a bunch of even numbers to check that the sums are indeed even (e.g. $2 + 6 = 8$ is even). This gives you confidence that the theorem is true, but there is always the possibility that there are some untested even numbers whose sum is not even. However, if you can logically argue that the sum of *any* pair of even numbers is even, then you can reliably put this nagging unease to rest.

Moreover, for more complicated mathematical situations, one may not have reliable intuition for what is true. In some situations, e.g. the famous *Monty Hall Problem*, which models a relatively simple game, the correct solution may go against what your intuition tells you. There are also many problems for which one may have some limited intuition, but a far deeper analysis and proof are needed to determine what is truly the correct result. One common example (of many) is the *four colour theorem*, which is also famous for being one of the earliest (1976) results to be proved partially by computer.

Note. *If you have not heard of the Monty Hall Problem and/or the four colour theorem, then you should definitely look them up!*

There are also mathematical questions for which we have no intuition at all prior to a proof. One example, which we will explore later in this module, is the question of whether there is only one infinite size of sets, or whether there are many different infinite sizes, some larger than others. Such concepts go beyond our ability to visualise, and we will have to resort to logic and proofs to illuminate what is really going on.

The reliability of proofs has also been used in more creative ways. If you have ever written computer programs, then you have spent ample time fixing bugs, yet you would never know for certain if a program has some other hidden error. In computer science, however, there are settings in which one can *prove* a program always runs as intended without errors. One can imagine how useful that might be in critical situations (e.g. missile systems) where any bug could cause an inordinate amount of damage.

While formal verification is a topic well beyond this module, one interesting example worth mentioning comes from the early 1990s, when Intel released a processor containing a subtle bug that led to division errors in some rare circumstances. Though these errors were uncommon, they could be disastrous for research communities that relied on highly precise computations. In the end, the bug grew into a public relations scandal for Intel, and it ultimately cost them hundreds of millions of US dollars to recall and replace the defective processors. Since then, researchers have in some instances preemptively dealt with potential bugs by crafting proofs that verify the hardware will run correctly.

1.3. **Rigorous Mathematics.** Now that we have an idea of what makes mathematical thinking distinct from other disciplines, we can similarly ask *what aspects of mathematical thinking make it distinctly valuable*. One key feature worth highlighting is that of rigour, in that *each mathematical statement has a precise, unambiguous meaning*.

For example, in plain English, the classic example "they all saw her duck" could have unclear meaning, since without more context, the word "duck" could refer to either a bird or to the act of crouching. Moreover, in philosophy or science, one may discuss slippery concepts such as "consciousness" without having a precise definition of what this "consciousness" is (which leads to no shortage of arguments!). In contrast, each mathematical statement—when correctly formulated—will have precise meaning, without any ambiguities such as the ones described above. Thus, when you read any mathematical statement, you should be able to discern *exactly* what it is saying.

Similarly, a mathematical proof, when fully written out, is a sequence of logical steps, each of which has precise meaning and can be checked if it is logically sound. Thus, at least in theory, *one can definitively verify* (up to pesky human errors) *whether a proof is correct or not*. Since proofs are the arbiter of mathematical truth, *one can hence definitively check whether a mathematical statement is true*. Thus, proven mathematical statements are seen as having cleared the bar for the highest standard of reliability.

> **Note.** *Though mathematics is usually grouped with the sciences, its practice is, in certain ways, closer to law. Indeed, legal arguments must be made far more precisely than in other situations; mathematics demands a similarly high level of precision.*

While achieving this precision is nice, it exacts a substantial price—mathematics is restricted to talking only about abstract things in a formal logical universe. In other words, it relinquishes the ability to directly discuss the real world. Indeed, mathematicians study abstract constructs such as numbers and equations, rather than planets, atoms, or consciousness. You should not, however, think this makes maths useless, as these abstractions have been remarkly successful in modelling and predicting the real world. In fact, most of the modern world—the many breakthroughs in science, engineering, and technology—hinge on the reliability and precision of mathematical models.

Thus, if you complete a mathematics degree, then you may not distinguish yourself by having done more "quantitative things" than your peers in science, computing, or engineering. However, a rather exclusive soft skill that you do pick up from a maths degree is an ability to think in a very precise way at an elite level.

1.4. **Contents of NSF.** Before diving into the actual mathematical material, let us conclude this introduction with a brief summary of what this module will cover.

The first part of the module concerns *logic*, which forms the foundations of mathematical reasoning. We aim to gain a more systematic and formal understanding of logic, and we connect this to the informal logical reasoning that you likely already do in your daily lives. At the same time, we also turn our attention toward mathematical proofs, and we explore how such proofs are crafted from individual logical steps. As part of this process, we will look at various simple examples of proofs, some common strategies for devising and writing proofs, and the logical underpinnings of these strategies.

We then turn our attention toward *sets*, which roughly describe "collections of things", and which are used as common building blocks for all kinds of mathematical objects and quantities. In fact, any mathematical object that you will encounter—be it numbers, functions, or anything else—can be formulated in terms of sets! In this part of the module, we will familiarise ourselves with sets and their basic properties, and we will use sets as a minimal testing ground on which we can practice with simple proofs.

Having gained some facility with sets, the next step is to apply our new powers to more interesting mathematical objects. For this, we turn our attention to the various *number systems* that you have studied in your pre-university education—*natural numbers*, *integers*, *rational numbers*, and *real numbers*. We take a deeper, proof-based look at each of these number systems, exploring some interesting properties that you may not have seen before. We will also take a brief look at the "imaginary" and *complex numbers*, as well as why they can be useful despite seeming rather counterintuitive at first glance.

Through numbers, we now have a cornucopia of mathematical objects with which to play. To make things more interesting, however, we need more sophisticated ways describe relationships between these quantities. The common language for doing this revolves around mathematical objects known as *relations* and *functions*, both of which you have already encountered before university. Here, we discuss how relations and functions fit within set theory, and we connect this to what you have previously learned.

For the final part of the module, we study the *cardinality* of sets, which roughly means *the number of elements in a set*. For finite sets, this amounts to counting how many objects are in a set and is the foundation of an area of mathematics known as *combinatorics*. For sets that are not finite, this serves as our first encounter with *infinity*, and it grants us an opportunity to understand this mysterious concept in a precise way.

Again, all the material in NSF is designed to help you pick up a new way of thinking and to ease your progression into more advanced university-level maths. Hopefully, this introduction has convinced you that mathematics is indeed an interesting area of study,

and that it is vastly different from what you have studied before. With all that said, let us not delay any further and jump straight into the module material!

> **Note.** *There will also be some "bonus content" scattered throughout the notes that are related to and supplement the core module material. Though the bonus content will not be examinable, they do contain interesting digressions for those who are curious, and for those who have a stronger mathematical background.*

1.5. **Using the Notes.** These lecture notes contain essentially the same contents as the lectures themselves. Thus, it is recommended that you use the notes and the lecture contents in tandem to supplement each other, though how you ultimately wish to carry this out will depend on what learning style works best for you.

The main advantage of the lecture notes is that they are not bounded by the same time constraints as the lecture sessions. In particular, the notes contain additional explanations and examples that could not be covered in the lectures.

On the other hand, a live lecture format is better suited for demonstrating the mathematical process—having explanations given and examples worked out in real time, alongside the thinking that goes into each individual step. These aspects are more difficult to convey effectively on the static pages of typed notes.

Of course, you should also engage the weekly quizzes and problem sets alongside the lectures and notes. After all, the only way to learn the material for yourself is to practice!

1.6. **Acknowledgments.** I am thankful to Dr Robert Johnson, Dr Matthew Fayers, and Prof Mark Jerrum, who have taught NSF in past years and have handed an ample amount of teaching material down to me. While these notes cover the module topics in a different order than past years, and with more emphasis on logic and proofs, most of the material here is still based on past years' notes. That I was able to get a coherent module running so quickly is a testament to all the existing material I had to work with, and the extensive efforts of my predecessors in curating and organising all this material.

2. Logic and Proofs

As mentioned in the introduction, *a proof is a formal logical argument*. Thus, if we are to become capable with proofs, then we must first gain a better understanding of logic.

Now, you are already quite familiar with logic at a certain level, since you often engage in logical reasoning in your normal life. However, our usual usage of logic in English (or your language of choice) tends to not be very precise. As a common example, if I say "the sky is blue, or the the car is red", then this certainly means one of the two possibilities is true. However, what is not clear is whether both possibilities can be true—whether it is possible the sky is blue *and* the car is red. In plain English, the sentence above could be used to either include or exclude this possibility, depending on context.

Since our mathematical statements must be precise and unambiguous, we must demand the same of our underlying logic. Thus, we turn to formal logic, which refers to an *abstract theory that models the everyday logic that we already do*, except that *all the statements and processes within are completely unambiguous*. In this chapter, we provide a brief introduction to elements of formal logic, as they are commonly used in mathematics.

> **Note.** *For practical reasons, most of our mathematical work will actually be at the semi-formal level. This is because fully formal arguments would be far too long, even for the simple proofs found in NSF. As a result, mathematicians compromise by writing proofs partially in "plain English prose", as was done in the sample from the introduction. From this point of view, the goal of proof writing is to convince the reader that the argument can, at least in principle, be converted to a fully formal proof.*

2.1. Logical Statements.

There are two common perspectives of formal logic:

(1) Boolean logic, roughly the "theory of true and false". This is the perspective often found in computing, since "true/false" reflects the binary nature of computers.
(2) Deductive logic, roughly the "theory of logical arguments". This theory reflects how proofs work, hence this is the viewpoint we will ultimately take.

The Boolean viewpoint tends to be easier and more intuitive for most learners, and you may have already been exposed to this prior to university. As a result, as warm-up, the first parts of this chapter will mostly focus on the Boolean point of view. Once we have built some intuition and momentum, we will then transition to the deductive and "proof-based" perspective in the latter parts of the chapter.

Let us begin our discussion with the most basic logical object, a single statement:

Definition 2.1. *A statement represents an expression that:*

- *is a complete sentence by itself, and*
- *is either true or false.*

Note. *Another common term for "statement" is proposition, which you will find in many texts on logic. However, here we will always use the term "statement", as we will often use "proposition" to mean something different in mathematics.*

Note we have kept our definition of "statement" semi-formal in order to demonstrate its connection to everyday logic. In the purely formal theory:

- A statement is an abstract object, usually denoted by a capital letter (e.g. "A", "B").
- Moreover, in the Boolean perspective of logic, each such statement is assigned a value of *true* or *false*. (You can abbreviate these as "T" and "F", if you wish.)

Of course, the idea is that a formal statement A serves as a proxy for either a statement in everyday English or a mathematical statement.

Example 2.2. *The following plain English sentences are statements:*

- *"Paris is the capital of France."*
- *"Madrid is the capital of Italy."*
- *"I love Numbers, Sets and Functions."*

Note that each of the above is a full sentence, and each is either true or false.

Moreover, from the Boolean point of view, one would assign "true" or "false" to each of the above—the first would be true, the second is false, and the third is up to you!

Example 2.3. *The following mathematical expressions are statements:*

- *"*$1 + 1 = 2$*."*
- *"*3 *is greater than* 4*."*
- *"*$\sqrt{2}$ *is a real number."*

While these contain mathematical symbols, if you read them aloud in English, then you will see that each is indeed a full sentence. Again, each of the above is true or false.

Furthermore, from the Boolean point of view, we would assign "true" to the first and third statements, and "false" to the second statement.

Example 2.4. *The following fail to be statements:*

- *"The capital of Italy": This is not a full sentence (it consists only of a noun).*
- *"Hello.": This is a full sentence, but it fails to be either true or false.*
- *"Do you like NSF?": This is a full sentence, but it fails to be either true or false.*

Note since the first example above is not a full sentence, it is also not true or false.

Example 2.5. *The following all fail to be statements:*

- $1 + 2$*: This is not a full sentence; it is just a number.*
- *"The set of even numbers": This is not a full sentence; it is just a set.*
- $\subseteq A \Leftrightarrow 42$*: This makes no sense whatsoever (and is presumably not a sentence); it is just a sad collection of symbols. Please avoid writing things like this!*

2.2. **Logical Operations.** Now that we have seen some logical statements, let us now see how one can build more complex statements from simpler ones. This is accomplished via *logical operations*, which model aspects of everyday logical reasoning.

For the upcoming discussions, we let P and Q be statements. (You can think of these as being stand-ins for any mathematical or "plain English" statements.)

2.2.1. *Negations.* Our first operation models the logical effect of the English word "not":

Definition 2.6. *The operation* not *associates a statement* P *with its negation, "*not P*".*

In Boolean logic, not P *has precisely the opposite of the truth value of* P*. (If* P *is* true*, then* not P *is* false*, and vice versa.) This can be summarised as follows:*

P	not P
true	false
false	true

The figure at the end of Definition 2.6 is commonly called a truth table. In Boolean logic, truth tables provide a convenient way to summarise all the possible truth values of

compound logical statements. Therefore, you will encounter and work with many more instances of truth tables in the upcoming discussions.

Example 2.7. *Some simple demonstrations of negation are given below:*

- *If* P *represents the statement "it is raining outside", then* not P *represents the statement "it is not raining outside".*
- *If* P *is the statement "Madrid is the capital of Italy", then* not P *represents the statement "Madrid is not the capital of Italy".*

Example 2.8. *Some simple demonstrations of negation are given below:*

- *If* P *is the statement* $x = 2$*, then* not P *is the statement* $x \neq 2$*.*
- *If* P *is the statement* $3 \geq 4$*, then* not P *is the statement* $3 < 4$*.*

Note. *As can be seen from the above examples, whether* P *is true or false (or unknown) is irrelevant;* not P *is always the statement having the opposite truth value to* P*.*

Note. *"*not P*" is also commonly written "*$\neg$P*" in many logic texts. However, to avoid too many notations, we will only use "*not P*" in these lecture notes.*

2.2.2. *Conjunctions.* The next operation models the logic behind the word "and":

Definition 2.9. *The operation* and *associates* P, Q *with their conjunction, "*P and Q*".*

In Boolean logic, P and Q *is true only when both* P *and* Q *are true, and is false otherwise. This is summarised in the following truth table:*

P	Q	P and Q
true	true	true
true	false	false
false	true	false
false	false	false

To better understand this, it is easiest to consider a few basic examples:

Example 2.10. *Consider the following:*

- *Let* P *be the statement "I love maths".*
- *Let* Q *be the statement "I love music".*

Then, P and Q *is the statement "I love maths, and I love music".*

Note that (in the Boolean viewpoint) for P and Q *to be true, one requires both* P *and* Q *must be true, that is, you have to love both maths and music.*

Now, while "I love maths, and I love music" is perfectly acceptable English, it does come across as a bit repetitive, and one would more commonly write this as "I love maths and music". Thus, in practice, you will have to be aware that the precise logical interpretation of "I love maths and music" is as the conjunction of "I love maths" and "I love music".

Example 2.11. *Consider the following:*

- *Let* P *be the statement* $5 < 6$.
- *Let* Q *be the statement* $4 < 5$.

Then, P and Q *is the statement "*$5 < 6$ and $4 < 5$*". Note that as both* $5 < 6$ *and* $4 < 5$ *are individually true, then the conjunction* $5 < 6$ and $4 < 5$ *is true as well.*

Similar to Example 2.10, mathematicians can be a bit lazy and often prefer to abbreviate the above as "$4 < 5 < 6$". Once again, you will have to be aware that the meaning of "$4 < 5 < 6$" is as the conjunction of $4 < 5$ and $5 < 6$.

Example 2.12. *Suppose* P *is the statement "*x *is an even number", and* Q *is the statement "*x *is an odd number". Then,* P and Q *is the statement "*x *is both an even number and an odd number", which is of course always false.*

Note. *"*P and Q*" is also denoted "*$P \wedge Q$*" in many logic texts. Since "*$\wedge$*" is sometimes used for other operations in mathematics, we will exclusively use "*and*" in these notes.*

2.2.3. *Disjunctions.* Next, we consider the formal logic behind the word "or":

Definition 2.13. *The operation* or *associates* P, Q *with their disjunction, "*P or Q*".*

In Boolean logic, P or Q *is true when at least one of* P *and* Q *is true, and is false otherwise. This is summarised in the following truth table:*

P	Q	P or Q
true	true	true
true	false	true
false	true	true
false	false	false

Example 2.14. *Consider the following:*

- *Let* P *be the statement "I pass NSF".*
- *Let* Q *be the statement "I fail NSF".*

Then, P or Q *is simply the statement "either I pass NSF or I fail NSF".*

In Boolean logic, P or Q *is true when one of* P, Q *to be true—that is, you pass or you fail NSF. Thus, once you have your final NSF results, then* P or Q *is necessarily true.*

Note in the above example, the word "either" adds emphasis to the "or", but it does not add any logical meaning. Thus, you should know that the interpretation of "either I pass NSF or I fail NSF" is simply as the disjunction of "I pass NSF" and "I fail NSF".

Example 2.15. *Consider the following:*

- *Let* P *be the statement* $3 < 4$.
- *Let* Q *be the statement* $3 = 4$.

Then, P or Q *is the statement "*$3 < 4$ or $3 = 4$*". Since* $3 < 4$ *is true, then* P or Q *is true, regardless of whether* $3 = 4$ *is true or not (it is not!).*

It is common to abbreviate "$3 < 4$ or $3 = 4$" as $3 \leq 4$; you likely have already been doing this for a while. Again, for our purposes, it will be important to be aware that the logical interpretation of $3 \leq 4$ is as the disjunction of $3 < 4$ and $3 = 4$.

One important point to keep in mind is that by our definition, P or Q *is true when one of* P, Q *is true, as well as when both* P *and* Q *are true.* This is in contrast to the *exclusive or* in computing, in which P xor Q is true only when exactly one of P, Q is true. This tends to

cause some confusion, since in plain English, the word "or" can be interpreted either way, depending on context. In logic and in mathematics (and in this module), we will always interpret "or" as in Definition 2.13—no ambiguities!

Example 2.16. *In Boolean logic, the statement "$3 < 4$ or $4 < 5$" is defined to be true, since both components $3 < 4$ and $4 < 5$ are individually true.*

Note. *"P or Q" is also denoted "$\mathsf{P} \vee \mathsf{Q}$" in many logic texts. Since "$\vee$" is sometimes used for other operations in mathematics, we will exclusively use "*or*" in these notes.*

2.2.4. *Implications.* The next operation models the logical construct "if ..., then ...".

Definition 2.17. *The implication operation associates P, Q with a statement "$\mathsf{P} \Rightarrow \mathsf{Q}$".*

In Boolean logic, $\mathsf{P} \Rightarrow \mathsf{Q}$ is true as long as Q is true whenever P is true; otherwise, $\mathsf{P} \Rightarrow \mathsf{Q}$ is false. This is summarised in the following truth table:

P	Q	$\mathsf{P} \Rightarrow \mathsf{Q}$
true	true	true
true	false	false
false	true	true
false	false	true

$\mathsf{P} \Rightarrow \mathsf{Q}$ is usually written in English as "if P, then Q". The interpretation for this is that if P is true, then Q must necessarily be true as well. (Otherwise, all bets are off!)

Implications $\mathsf{P} \Rightarrow \mathsf{Q}$ are ubiquitous in mathematical statements. In particular, one can view P as assumptions that one makes, and Q the conclusions that follow from P.

Example 2.18. *Consider the following:*

- *Let P be the statement "I revise for the exam".*
- *Let Q be the statement "I will pass the exam".*

Then, $\mathsf{P} \Rightarrow \mathsf{Q}$ is the statement "if I revise for the NSF exam, then I will pass the exam".

In Boolean logic, $\mathsf{P} \Rightarrow \mathsf{Q}$ is false whenever P is true ("I revise for the NSF exam") and Q is false ("I will not pass the exam"). In all other cases, $\mathsf{P} \Rightarrow \mathsf{Q}$ is true.

Example 2.19. *Consider the following:*

- *Let* P *be the statement "*x *and* y *are even numbers".*
- *Let* Q *be the statement "*$x + y$ *is an even number".*

Then, $P \Rightarrow Q$ *is the statement "if* x *and* y *are even numbers, then* $x + y$ *is an even number"—the statement of the sample Theorem 1.2 from the introduction!*

Regarding the truth table in Definition 2.17, one consistent point of confusion is that if P is false, then $P \Rightarrow Q$ is true, which seems quite counterintuitive at first glance. One way to think of this is to consider when the implication $P \Rightarrow Q$ is violated—this only happens when P is true and Q is false, so that Q does not follow from P. We then only assign "false" to $P \Rightarrow Q$ in this particular case when P, Q violate the implication.

To be more concrete, consider Example 2.18, and suppose the statement "if I revise for the exam, then I will pass the exam" is true. All this says is that *if you revise for the exam, then you are guaranteed to pass the exam.* On the other hand, if you do not revise for the exam, then it is possible you fail the exam, or you could still pass the exam anyway—neither possiblity is eliminated by the above implication being true. *The only outcome that is invalidated by the implication is you revising for the exam and then failing the exam.* As a result, only in this invalidating case is the implication considered to be false.

Similarly, in Example 2.19, the implication only guarantees that $x+y$ is even whenever both x and y are even. If it is not the case that x and y are both even (i.e. P is false), then the implication says nothing about $x + y$, and $x + y$ could indeed be even or odd. (For example, $3 + 4 = 7$ is odd, while $3 + 3 = 6$ is even.)

Note. *When one writes* $P \Rightarrow Q$*, the presumption is often that* Q *is causally related to* P *(e.g. passing the exam follows from revising for the exam). However, strictly speaking, one can still construct and analyse the statement* $P \Rightarrow Q$ *when* P, Q *are not causally related whatsoever. For example, the following implications are true in Boolean logic, even though there is no relation between the two respective components:*

- *"*7 *is prime* $\Rightarrow 3 > 2$*"* (true $\Rightarrow$ true*, which is* true*).*
- *"*8 *is prime* $\Rightarrow 3 > 2$*"* (false $\Rightarrow$ true*, which is* true*).*

2.2.5. *Equivalences.* The final operation we discuss concerns whether two statements are logically the same, i.e. whether they carry the same content in terms of truth values:

Definition 2.20. *The equivalence operation associates* P, Q *with a statement "*$P \Leftrightarrow Q$*". In Boolean logic,* $P \Leftrightarrow Q$ *is true when* P *and* Q *have the same truth value, and is false otherwise. This is summarised in the following truth table:*

P	Q	$P \Leftrightarrow Q$
true	true	true
true	false	false
false	true	false
false	false	true

Statements such as $P \Leftrightarrow Q$ rarely come up in everyday English. They are, however, quite common in mathematics, where $P \Leftrightarrow Q$ is often written as "P if and only if Q" (sometimes abbreviated "P iff Q"). Later, we will justify this interpretation.

Example 2.21. *Consider the following:*

- *Let* P *be the statement "*x *is an even number".*
- *Let* Q *be the statement "*$x + 1$ *is an odd number".*

Then, $P \Leftrightarrow Q$ *is the statement "*x *is an even number if and only if* $x + 1$ *is an odd number". Observe that* $P \Leftrightarrow Q$ *is true in Boolean logic, since* P *is true when* Q *is true, and* P *is false when* Q *is false, so that* P, Q *always have the same truth value.*

2.2.6. *Formal vs Natural Language.* A major issue when working with logical statements, which we already alluded to in earlier discussions, is that there are many ways in which one can write a statement in English. For example, the negation of "NSF is fun" can be written "NSF is not fun" or "it is not the case that NSF is fun". While this prevents English writing from being dull and repetitive, it adds some difficulty when we try to interpret the formal logical meaning of a statement written in plain English.

We already mentioned some examples of this in the context of conjunctions and disjunctions, but it is worth listing a few more examples, as interpreting the precise logic behind various statements is an important skill to acquire in mathematics:

Example 2.22. *In the table below are some statements, both plain English and mathematical, given both in common form and in terms of its precise logical meaning:*

Common wording	*Logical meaning*
"Rome and Venice are in Italy"	*"Rome is in Italy"* and *"Venice is in Italy"*
"NSF is not fun"	not *"NSF is fun"*
"Either the sock or the shoe is red"	*"The sock is red"* or *"the shoe is red"*
$x, y > 0$	"$x > 0$ and $y > 0$"
$x \leq y$	"$x < y$ or $x = y$"

In particular, there are many ways that one can write $P \Rightarrow Q$ in English:

- "If P, then Q."
- "P implies Q."
- "Q if P."
- "Q follows from P."
- "P only if Q."
- "P is a sufficient condition for Q."
- "Q is a necessary condition for P."

It is definitely worth taking a few minutes to substitute some simple statements into P, Q above, to convince yourself that all the above have the same interpretation as $P \Rightarrow Q$.

Unfortunately, all the above-mentioned ways to write $P \Rightarrow Q$ are commonly used in mathematics, so you do have to be aware of them and be able to interpret them correctly. (Implications are so common in mathematics, we need many ways to write them in English, in order to keep things spicy!) However, with some practice and experience reading mathematical writing, this will soon become second nature.

Example 2.23. *The following statements all have the same interpretation:*

- *"If I practice, then I will improve."*
- *"I will improve if I practice."*
- *"I practice only if I will improve."*

Indeed, all these correspond to the implication "I practice" $\Rightarrow$ *"I will improve".*

Note. *The last statement in the above example, "I practice only if I will improve", can be quite tricky to parse. The key is the word "only"—what this is really saying is that when "I practice" is true, then "I will improve" must be true.*

2.3. **Logical Properties.** Having discussed how logic operations can be used to combine simple statements into more complicated ones, our next task is to explore various relations between statements defined through these operations. There are many useful relations worth mentioning, and we will explore a few in detail here.

As a first example, let us consider the following question:

Question 2.24. *Given statements* P *and* Q*, is there another way to interpret*

$$\text{not}(P \text{ and } Q)?$$

Example 2.25. *Consider the following mathematical statements:*

- P*:* $x = 2$.
- Q*:* $y = 5$.

Then, $\text{not}(P \text{ and } Q)$ *is the statement, "it's not the case that both* $x = 2$ *and* $y = 5$*".*

Now, if you think about this statement a bit, you can see that this has the same logical meaning as "either $x \neq 2$ *or* $y \neq 5$*". Moreover, this is more precisely interpreted as*

$$\underbrace{(\text{not } P)}_{x \neq 2} \text{ or } \underbrace{(\text{not } Q)}_{y \neq 5}.$$

Thus, in the particular setting of Example 2.25, the statements

$$\text{not}(P \text{ and } Q), \qquad (\text{not } P) \text{ or } (\text{not } Q)$$

are logically equivalent. However, there is nothing special about the statements $x = 2$ and $y = 5$ here—the beauty of formal logic is that *you could replace* P *and* Q *by any statements, and you can still reason in the exact same way that* $\text{not}(P \text{ and } Q)$ *and* $(\text{not } P)$ or $(\text{not } Q)$ *are logically equivalent.* In other words, this is general property relating not, and, or that applies to all statements, and it is commonly known as DeMorgan's Law.

In Boolean logic, one can verify this using a truth table:

P	Q	P and Q	not(P and Q)	not P	not Q	(not P) or (not Q)
true	true	true	false	false	false	false
true	false	false	true	false	true	true
false	true	false	true	true	false	true
false	false	false	true	true	true	true

Note *the two columns in orange always contain the same truth values.* This is the Boolean method of seeing that not(P and Q) and (not P) or (not Q) are the same.

Note. *Another way to state DeMorgan's Law is to observe that the statement*

$$(\text{not}(\text{P and Q})) \Leftrightarrow ((\text{not P}) \text{ or } (\text{not Q}))$$

is always true, for all statements P *and* Q*, and with all possible truth values for each. This justifies the our calling* not(P and Q) *and* (not P) or (not Q) *equivalent.*

Note. *Like in arithmetic, here we use parentheses* (...) *to specify the order that logical operations are carried out. There is not any generally agreed convention for order of logical operations (e.g. addition always comes after multiplication, unless parentheses are present), so we will use parentheses as needed to avoid ambiguities.*

There is an analogous DeMorgan's Law, with the roles of and, or interchanged:

Example 2.26. *Consider the following statements:*

- P*: "I fail NSF".*
- Q*: "I fail Calculus".*

Then, not(P or Q) *is the statement, "it is not the case that I fail NSF or fail calculus", while* (not P) and (not Q) *is the statement, "I pass NSF and pass Calculus". Again, with a bit of reasoning, you can see that the two statements have the same logical meaning.*

In the Boolean viewpoint, we can again demonstrate this via a truth table:

P	Q	P or Q	not(P or Q)	not P	not Q	(not P) and (not Q)
true	true	true	false	false	false	false
true	false	true	false	false	true	false
false	true	true	false	true	false	false
false	false	false	true	true	true	true

Again, the two columns in orange have the same truth values in every possible case.

Next, we look at another logical property concerning implications that will eventually play an important role in constructing proofs. For this, we first introduce a bit of terminology that is commonly used in both logic and mathematics:

Definition 2.27. *Given statements* P, Q, *and the implication* $P \Rightarrow Q$*:*

- *We define the converse of* $P \Rightarrow Q$ *to be the implication* $Q \Rightarrow P$.
- *We define the contrapositive of* $P \Rightarrow Q$ *to be the implication* $(\text{not } Q) \Rightarrow (\text{not } P)$.

Question 2.28. *Is* $P \Rightarrow Q$ *equivalent to its converse or contrapositive?*

As before, in Boolean logic, we can check this directly using a truth table:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(\text{not } Q) \Rightarrow (\text{not } P)$
true	true	true	true	true
true	false	false	true	false
false	true	true	false	true
false	false	true	true	true

Notice the two columns in orange always have the same truth values, while the column in red can have different truth values as the orange columns. From this, we conclude:

- $P \Rightarrow Q$ *is not equivalent to its converse* $Q \Rightarrow P$.
- $P \Rightarrow Q$ *is equivalent to its contrapositive* $(\text{not } Q) \Rightarrow (\text{not } P)$.

You should also look at $P \Rightarrow Q$, as well as its converse and contrapositive, for various concrete statements P and Q, in order to intuitively convince yourself that the above rules hold. We consider a simple mathematical example below:

Example 2.29. *Consider the following mathematical statements:*

- P*:* $x > 2$.
- Q*:* $x^2 > 4$.

Then, we can interpret various implications involving P *and* Q *as follows:*

- $P \Rightarrow Q$ *is the statement "if* $x > 2$*, then* $x^2 > 4$*".*
- *Its converse* $Q \Rightarrow P$ *is the statement "if* $x^2 > 4$*, then* $x > 2$*".*
- *Its contrapositive* $(\text{not } Q) \Rightarrow (\text{not } P)$ *is the statement "if* $x^2 \leq 4$*, then* $x \leq 2$*".*

Note that $P \Rightarrow Q$ *is always true (for any real number* x*), while the converse* $Q \Rightarrow P$ *is not always true. (For example,* $(-3)^2 > 4$ *is true, while* $-3 > 2$ *is false, hence the implication* $(-3)^2 > 4 \Rightarrow -3 > 2$ *is false.) On the other hand, the contrapositive* $(\text{not } Q) \Rightarrow (\text{not } P)$ *is always true (since if* $x^2 \leq 4$*, then* x *must lie between* -2 *and* 2*).*

Thus, in this particular case, we have that $P \Rightarrow Q$ *and its contrapositive have the same truth value, while* $P \Rightarrow Q$ *and its converse may not.*

There are many other similar and useful logical equivalences, however covering them all would be tedious (and would take too much time and space). In the following, we list several common logical equivalences that you will encounter in mathematics:

Name		**Statement**	$\Leftrightarrow$	**Statement**
Commutative Law		P and Q		Q and P
Commutative Law		P or Q		Q or P
Associative Law		P and (Q and R)		(P and Q) and R
Associative Law		P or (Q or R)		(P or Q) or R
DeMorgan's Law		not(P and Q)		(not P) or (not Q)
DeMorgan's Law		not(P or Q)		(not P) and (not Q)
Distributive Law		P and (Q or R)		(P and Q) or (P and R)
Distributive Law		P or (Q and R)		(P or Q) and (P or R)
Equivalence		$P \Leftrightarrow Q$		$(P \Rightarrow Q)$ and $(Q \Rightarrow P)$
Contrapositive		$P \Rightarrow Q$		$(\text{not } Q) \Rightarrow (\text{not } P)$

FIGURE 2.1. Here P, Q, R denote arbitrary statements. In each row of the table, the two statements within are logically equivalent to each other, while the first column gives the common name for this logical property.

Note. *The associative law in Figure 2.1 shows that the order that one takes adjacent* and *operations does not matter. As a result, it makes sense to write either* P and (Q and R) *or* (P and Q) and R *(which are the same!) as simply "*P and Q and R*". By the same logic, we can also write "*P or Q or R*" without ambiguity.*

Example 2.30. *Below is a truth table confirming the equivalence law from Figure 2.1:*

P	Q	$P \Leftrightarrow Q$	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q)$ and $(Q \Rightarrow P)$
true	true	true	true	true	true
true	false	false	false	true	false
false	true	false	true	false	false
false	false	true	true	true	true

Again, the two orange columns always have the same truth values.

It is worth taking a moment to interpret this equivalence law. Observe that this property says that P being equivalent to Q (i.e. P and Q always having the same truth values) is the same as both $P \Rightarrow Q$ and $Q \Rightarrow P$. Thus, *saying that* P *and* Q *being logically equivalent is the same as saying both that* Q *follows from* P *and that* P *follows from* Q. This observation will be of paramount importance once we start studying proofs.

Example 2.31. *The following confirms one of the distributive laws from Figure 2.1:*

P	Q	R	Q and R	P or (Q and R)	P or Q	P or R	(P or Q) and (P or R)
true	true	true	true	true	true	true	true
true	true	false	false	true	true	true	true
true	false	true	false	true	true	true	true
true	false	false	false	true	true	true	true
false	true	true	true	true	true	true	true
false	true	false	false	false	true	false	false
false	false	true	false	false	false	true	false
false	false	false	false	false	false	false	false

Again, you should take some time to think about each of the logical properties in Figure 2.1 to see that each of the equivalences makes intuitive sense.

Note. *We have shown several examples of truth tables, and how they work is mostly self-explanatory. To be more explicit, though, the first columns should contain the basic statements, with a listing of all the possible truth values they may take. The remaining columns list the corresponding truth values of various compound statements.*

For instance, in Example 2.31, the basic statements are P, Q, R, *and we need eight rows to list all the possible truth values that* P, Q, R *together could take; all this is given in the first three columns of the table. The remaining columns display the truth values of compound statements built from* P, Q, R. *Here, our goals are in the orange columns, but we include columns of intermediate steps to make the table easier to check.*

2.4. **Quantifiers.** In mathematics, we will need to work with *statements depending on one or more variables as input.* Formally, these variable-dependent statements will be denoted as before, but with the variables given in parentheses after the statement name:

$$P(x), \qquad Q(y), \qquad R(x, y).$$

Here, P depends on a single variable x, while R depends on two variables x, y. To avoid being too formal, we leave vague what the variables are, but for practical purposes, they could refer to any kind of objects—e.g. days of the week, numbers, sets, animals.

Note. *These variable-dependent statements are commonly called predicates in some logic literature. However, we will avoid using this terminology here.*

Example 2.32. *Let $P(x)$ be the statement "x is a prime number", which depends on a single variable x. We can make use of the variable in two ways:*

- *We can put an formal symbol x in this variable slot. In this case, $P(x)$ says that a formal abstract object x is a prime number.*
- *We can also put a concrete object in the place of x. For example, putting 2 in the place of x, then $P(2)$ is the true statement "2 is a prime number".*

In Example 2.32 above, there is nothing special about the letter "x". We can just as well write $P(y)$ or $P(z)$ to mean the same thing as $P(x)$, as long as x, y, z are all symbols that have not been given additional meaning elsewhere.

Example 2.33. *Let $Q(x, y)$ be the mathematical statement $x^2 \geq y$. Then:*

- *$Q(1, 2)$ is the statement $1^2 \geq 2$.*
- *$Q(x, 3)$ is the statement $x^2 \geq 3$.*
- *$Q(3, z)$ is the statement $3^2 \geq z$.*

Note. *One issue with the statements from Examples 2.32 and 2.33 is that they only make sense when the variable inputs are numbers. Thus, we can say many nonsensical things:*

- *$P(\text{apple})$: "apple is a prime number".*
- *$Q(\text{book}, \text{NSF})$: "$\text{book}^2 \geq \text{NSF}$".*

Ideally, in these cases, we would like to restrict our inputs to numbers. Soon, we will see how to do this in practice, in particular for mathematical statements.

Now, just being able to formulate statements that depend on variables is not that useful on its own. Their real value becomes apparent once we can apply them to make *blanket*

statements over a multitude of variables. For this purpose, we need two additional logical operations—known as quantifiers—that apply to statements depending on variables.

2.4.1. *Universal Quantifiers.* Let $P(x)$ be the statement $x^2 \geq 0$, which we know is true for any x that is real number. Then, a useful statement that we want to make in this instance is of the form "$P(x)$ holds for all real numbers x", that is, "$x^2 \geq 0$ for every real number x". In terms of formal logic, this is accomplished via the following construction:

Definition 2.34. *Let $P(x)$, $Q(x)$ be statements. The universal quantifier, denoted $\forall$, is an operation that associates $P(x)$, $Q(x)$ with the statement "$\forall_{Q(x)}P(x)$".*

In terms of Boolean logic, the statement $\forall_{Q(x)}P(x)$ is true whenever $P(x)$ is true for every variable x such that $Q(x)$ is true; otherwise $\forall_{Q(x)}P(x)$ is false.

In particular, the universal quantifier models the meaning of the English words "for all" (hence the upside-down "$\forall$"). Like in our discussion of implications earlier, there are many different ways to write $\forall_{Q(x)}P(x)$ in English, for instance:

- "$P(x)$ holds for all x such that $Q(x)$".
- "$P(x)$ holds for every x such that $Q(x)$".
- "$P(x)$ holds for any x such that $Q(x)$".
- "For all x such that $Q(x)$, $P(x)$ holds".
- "For every x such that $Q(x)$, $P(x)$ holds".
- "For any x such that $Q(x)$, $P(x)$ holds".

Indeed, universal quantifiers are so common in mathematics that we need more ways to describe them in English to keep our writing from becoming too repetitive!

Example 2.35. *Consider the following statements:*

- *$P(x)$: "$2x$ is even".*
- *$Q(x)$: "x is a natural number".*

Then, applying the universal quantifier to $P(x)$ and $Q(x)$ results in the statement

- *$\forall_{Q(x)}P(x)$: "For any natural number x, $2x$ is even".*

Now, the above is considered poor writing style, since "x, $2x$" could be mistaken for a single mathematical object and cause confusion. Thus, it is often preferable to write

- *$\forall_{Q(x)}P(x)$: "$2x$ is even for every natural number x".*
- *$\forall_{Q(x)}P(x)$: "For all natural numbers x, we have that $2x$ is even".*

Example 2.36. *Consider the following statements:*

- $R(x)$: *"x is sunny".*
- $S(x)$: *"x is a day".*

Then, applying the universal quantifier to $R(x)$ and $S(x)$ yields the statement

- $\forall_{S(x)} R(x)$: *"x is sunny for any day x".*

The above, however, is a terribly clumsy bit of writing, and the more common and natural way to express $\forall_{S(x)} R(x)$ in English is simply "every day is sunny".

Note. *In Definition 2.34 and the examples, there is nothing special about the letter "x". We could replace x by any other unused symbol—for instance, $\forall_{Q(y)} P(y)$ contains exactly the same logical content as $\forall_{Q(x)} P(x)$. Here, the letters "x" and "y" only serve as dummy variables inside the quantifier but have no meaning outside the quantifier.*

This is analogous to how dummy variables are used in integrals and summations, e.g.

$$\int_0^1 f(x)\,dx, \qquad \sum_{k=1}^{100} a_k.$$

In the former case, x is simply a dummy variable representing all the values that are fed into the function f inside the integral. Moreover, the integrals

$$\int_0^1 f(x)\,dx, \qquad \int_0^1 f(y)\,dy,$$

are identical, even though they employ different dummy variables.

The variable x in the quantified statement $\forall_{Q(x)} P(x)$ works in the same way as the above integral. Like for integrals, you should avoid using a dummy variable outside the quantifier where it is used—for example, writing

$$x \geq 2 \text{ and } \forall_{Q(x)}(x < 4),$$

is at best very confusing and at worst nonsense, because x is used in two different ways (as a concrete object in "$x \geq 2$", and as a dummy variable in the quantifier).

Example 2.37. *Consider the following statement:*

- *"Every integer is even."*

Let us now pick apart its precise meaning and write it more formally. (It does not matter that the statement is obviously false, as we are only interested in its logical content.)

First, the word "every" indicates that a universal quantifier $\forall$ is involved. However, the "for all" only applies to all variables x such that x is an integer. Consequently, the above statement can be written more formally as

$$\forall_{n \text{ is an integer}}(n \text{ is even}).$$

Writing "n is an integer" is a bit annoying, we will often shorten this as

$$\forall_{\text{integer } n}(n \text{ is even}).$$

Note. *Later on, when we study set theory, we will encounter ways to write common statements such as "n is an integer" more concisely using symbols.*

Example 2.38. *Consider the following statement:*

- *"Every dog is furry and cute."*

This is similar to Example 2.37, and we can write this as

$$\forall_{x \text{ is a dog}}(x \text{ is furry and cute}).$$

Note "x is furry and cute" is a conjunction of "x is furry" and "x is cute". Thus, combining the above, and shortening what is in the subscript, we can parse our statement as

$$\forall_{\text{dog } x}((x \text{ is furry}) \text{ and } (x \text{ is cute})).$$

Finally, in a few occasions, we will need to employ *universal quantifiers without any restrictions on the variable*. For this purpose, we write "$\forall_x P(x)$" to mean:

- "$P(x)$ holds for all x".
- "For all x, $P(x)$."

This differs slightly from the universal quantifiers in Definition 2.34 in that x can now be any kind of object in our universe—numbers, people, days, etc.

In practice, we will seldom make use of these unrestricted quantifiers, since it is usually quite unnatural to think of a statement holding for every kind of possible object. However, they do come up briefly when we study set theory later on, so we mention them here.

Note. *The statement $\forall_x P(x)$ can also be written in terms of Definition 2.34 as $\forall_{Q(x)} P(x)$, for a statement $Q(x)$ that is always true (so that $Q(x)$ does not put any restriction on x). Thus, unrestricted quantifiers do not introduce any new logic into our system.*

Likewise, a statement $\forall_{Q(x)} P(x)$ can be written in terms of unrestricted quantifiers as

$$\forall_x (Q(x) \Rightarrow P(x)).$$

(You should convince yourself that both statements carry the same meaning.)

2.4.2. *Existential Quantifiers.* Suppose you wish to solve an equation such as $2x+4 = 10$. If you are successful at this (the solution is just $x = 3$, but never mind that), then you would want to declare victory by making a statement such as "the equation $2x + 4 = 10$ has a solution x that is a real number", or in other words, "there exists a real number x such that $2x + 4 = 10$". For this, we will need a different kind of quantifier:

Definition 2.39. *Let $P(x)$, $Q(x)$ be a statement. The existential quantifier, denoted $\exists$, is an operation that associates $P(x)$, $Q(x)$ with the statement "$\exists_{Q(x)} P(x)$".*

In terms of Boolean logic, the statement $\exists_{Q(x)} P(x)$ is true whenever $P(x)$ is true for at least one variable x such that $Q(x)$ is true; otherwise $\exists_{Q(x)} P(x)$ is false.

The existential quantifier models the English phrase "there exists" (hence the upside-down "$\exists$"). Unsurprisingly, there are many ways to write $\exists_{Q(x)} P(x)$ in English, e.g.

- "There exists x satisfying $Q(x)$ such that $P(x)$".
- "There is some x satisfying $Q(x)$ such that $P(x)$".
- "$P(x)$ holds for some x such that $Q(x)$".

Example 2.40. *Consider the following statements:*

- $P(x)$*:* $x^2 = -1$.
- $Q(x)$*: "x is a real number".*

Then, applying the existential quantifier to $P(x)$ and $Q(x)$ yields the statement

- $\exists_{Q(x)} P(x)$*: "There exists a real number x such that $x^2 = -1$".*

Note that another way to write the above is:

- $\exists_{Q(x)} P(x)$*: "$x^2 = -1$ for some real number x".*

Example 2.41. *Consider now the following statements:*

- $R(x)$: *"x is sunny".*
- $S(x)$: *"x is a day".*

Then, applying the existential quantifier to $R(x)$ and $S(x)$ yields the statement

- $\exists_{S(x)} R(x)$: *"x is sunny for some day x".*

It is a bit difficult to write this in natural-sounding English, but you could more smoothly describe $\exists_{S(x)} R(x)$ as "there exists a sunny day" or "there is some sunny day".

Note. *Again, there is nothing special about the letter "x", which is merely a dummy variable. One can write, for instance, $\exists_{Q(y)} P(y)$ to mean the same thing as $\exists_{Q(x)} P(x)$.*

Example 2.42. *Consider the following statement:*

- *"There is a prime number larger than 100."*

Let us now figure out its precise meaning and write it using quantifiers.

First, the phrase "there is" indicates an existential quantifier $\exists$. Since the "there exists" only applies to variables x that are prime numbers, we can write the above as

$$\exists_{p \text{ is a prime number}} (p \text{ is larger than } 100).$$

Shortening "p is a prime number" and using maths symbols, the above becomes

$$\forall_{\text{prime number } p} (p > 100).$$

Example 2.43. *Consider the following statement:*

- *"There is a ball in either the box or the tub."*

This is analogous to Example 2.42, and we can start by writing this as

$$\exists_{x \text{ is a ball}} (x \text{ is in the box or the tub}).$$

We can further decompose "x is in the box or the tub" into a disjunction:

$$\exists_{\text{ball } x} ((x \text{ is in the box}) \text{ or } (x \text{ is in the tub})).$$

In some rare instances, we will need to make use of *existential quantifiers without any restrictions on the variable.* For this, we write "$\exists_x P(x)$" to mean:

- "There exists x such that $P(x)$."
- "$P(x)$ holds for some x".

In contrast to Definition 2.39, here x can be any kind of object without restriction. Again, these seldom occur in practice, but they do come up briefly when studying sets.

Note. *Similar to universal quantifiers, the statement $\exists_x P(x)$ can also be written in terms of Definition 2.39 as $\exists_{Q(x)} P(x)$, for a statement $Q(x)$ that is always true.*

A statement $\exists_{Q(x)} P(x)$ can also be expressed in terms of unrestricted quantifiers as

$$\exists_x (Q(x) \text{ and } P(x)).$$

2.4.3. *Translating Statements with Quantifiers.* Most statements that you will come across in mathematics will involve quantifiers, so an essential skill that you need to have is the ability to translate between formally written mathematical statements and those written in English prose. In particular, given mathematical statements in English, you will have to discern their precise meanings in terms of formal logical language.

We have already seen a few simple examples of this earlier. However, for more complex statements, we can apply quantifiers to statements depending on more than one variable, and we can nest more than one quantifier together:

$$\forall_{Q(x)} P(x,y), \qquad \exists_{Q(y)} P(x,y),$$
$$\forall_{Q(x)} \exists_{R(y)} P(x,y), \qquad \forall_{\text{integer } x} \exists_{\text{integer } y} (x^2 > y).$$

Below, we discuss several concrete examples of such statements and learn to parse their meanings. If you are seeing this for the first time, then there are a quite a few subtleties to keep in mind, so do not feel discouraged if you struggle with this for a while!

Example 2.44. *Consider the following statement:*

- *"The sum of any two even numbers is an even number."*

To make more precise sense of this statement, it is useful to see that what it is really saying is "for any even number x and for any even number y, their sum $x + y$ is even". In particular, there is a universal quantifier over even numbers x, and another universal quantifier over even numbers y. From this more explicit form of the statement, it then

becomes more straightforward to write it more formally:

$$\forall_{\textit{even number } x} \forall_{\textit{even number } y} (x + y \textit{ is an even number}).$$

It is quite common to abbreviate the two quantifiers by combining them together:

$$\forall_{\textit{even numbers } x,\, y} (x + y \textit{ is an even number}).$$

It is fine for you to write either of the two orange statements. The main point you should be aware of is that these two statements have identical meanings.

There are other equivalent ways to parse the statement in Example 2.44, e.g.

- $\forall_{x,\, y \text{ integers}}((x \text{ and } y \text{ are even}) \Rightarrow (x + y \text{ is even}))$
- $\forall_{x,\, y \text{ integers}}(((x \text{ is even}) \text{ and } (y \text{ is even})) \Rightarrow (x + y \text{ is even}))$.

These can be interpreted as "for any integers x and y, if x and y are even, then $x + y$ is even". If you write something similar to one of the above, then that would also be fine. In particular, there is no single correct way to write these statements.

Example 2.45. *Consider the following statement:*

- *"Some student passed NSF, and some student failed Calculus."*

Parsing plain English statements can sometimes be a bit trickier, since it can be a bit ambiguous what should be variables and what should be the basic statements.

Here, one way to approach the above is see that it has the same logical meaning as the more verbose "there exists a student that passed NSF, and there exists a student that failed Calculus". This now readily translates to more formal language as

$$(\exists_{\textit{student } x}(x \textit{ passed NSF}) \text{ and } (\exists_{\textit{student } y}(y \textit{ failed Calculus})).$$

Again, there are other correct ways to write this—some equivalent examples include:

- $(\exists_{\textit{student } x}(x \textit{ passed NSF}) \text{ and } (\exists_{\textit{student } y} \text{not}(y \textit{ passed Calculus}))$.
- $\exists_{\textit{student } x} \exists_{\textit{student } y}((x \textit{ passed NSF}) \text{ and } (y \textit{ failed Calculus}))$.
- $\exists_{\textit{students } x,\, y}((x \textit{ passed NSF}) \text{ and } (y \textit{ failed Calculus}))$.

(The third example simply abbreviated the two quantifiers in the second example.)

Example 2.46. *Consider the following statement:*

- *"For any integer n, there is an integer m that is larger than n."*

For these, it is often easiest to translate in steps. For example, at the highest level is the "for any integer n", which leads to a universal quantifier:

$$\forall_{\textit{integer } n}(\textit{there is an integer } m \textit{ that is larger than } n).$$

We can now expand the part in red, which is led by an existential quantifier:

$$\forall_{\textit{integer } n}(\exists_{\textit{integer } m}(m \textit{ is larger than } n)).$$

Putting the last bit, "m is larger than n", in maths notation yields

$$\forall_{\textit{integer } n}\exists_{\textit{integer } m}(m > n).$$

Example 2.47. *Consider the following statement:*

- *"There is an integer m that is larger than any integer n."*

Here, the leading part is "there is an integer m", indicating an existential quantifier:

$$\exists_{\textit{integer } m}(m \textit{ is larger than any integer } n).$$

Now, the part is red is led by a universal quantifier, "for any n":

$$\exists_{\textit{integer } m}(\forall_{\textit{integer } n}(m \textit{ is larger } n)).$$

As a result, the formal interpretation is given by

$$\exists_{\textit{integer } m}\forall_{\textit{integer } n}(m > n).$$

Notice the formal statements in Examples 2.46 and 2.47 are identical, except for the order of the "$\forall$" and "$\exists$". However, the two statements have vastly different meanings—in particular, the statement in Example 2.46 is true, while the statement in Example 2.47 is false (do take a minute to see why this is)! Thus, *when both universal and existential quantifiers are present, the order that they appear greatly affects the meaning of the statement.*

2.4.4. *Quantifiers and Negation.* There is one last (but not least!) point to address regarding quantifiers, which is what happens when they are negated:

Question 2.48. *Given statements P and Q, are there other ways to interpret*

$$\text{not } \forall_{Q(x)} P(x), \qquad \text{not } \exists_{Q(x)} P(x)?$$

As usual, we approach this question by looking at a couple of examples:

Example 2.49. *Consider the following statement:*

- $P(x)$: *"x likes maths".*

Then, $\forall_{\text{person } x} P(x)$ translates to "all people like maths", or equivalently, "everyone likes maths". Thus, negating this statement, we obtain

- $\text{not } \forall_{\text{person } x} P(x)$: *"Not everyone likes maths".*

Now, if think about this for a bit, then you can see that "not everyone likes maths" has the same logical meaning as "someone does not like maths". But this last statement can be translated as "$\exists_{\text{person } x}(x$ does not like maths$)$", which then becomes

$$\exists_{\text{person } x}(\text{not } P(x)).$$

Thus, in this setting, $\text{not } \forall_{\text{person } x} P(x)$ and $\exists_{\text{person } x}(\text{not } P(x))$ are logically equivalent.

Example 2.50. *Consider again the statement:*

- $P(x)$: *"x likes maths".*

Applying $\exists_{\text{person } x}$ to $P(x)$ and then negating produces the (depressing) statement

- $\text{not } \exists_{\text{person } x} P(x)$: *"There does not exist someone who likes maths".*

Again, with a bit of thought, you can see that the above has the same meaning as "everyone dislikes maths", which can be translated as

$$\forall_{\text{person } x}(\text{not } P(x)).$$

Thus, in this setting, $\text{not } \exists_{\text{person } x} P(x)$ and $\forall_{\text{person } x}(\text{not } P(x))$ are logically equivalent.

Although the above examples only covered a particular statement, the same chain of thought could actually be applied to every statement $P(x)$ (and for every type of variable x, not just people). Therefore, similar to many of the logical properties we discussed earlier, we also have the following, *for any statements* $P(x)$, $Q(x)$:

- *The statements "*$\text{not } \forall_{Q(x)} P(x)$*" and "*$\exists_{Q(x)} \text{ not } P(x)$*" are always equivalent.*
- *The statements "*$\text{not } \exists_{Q(x)} P(x)$*" and "*$\forall_{Q(x)} \text{ not } P(x)$*" are always equivalent.*

(Note these appear similar to DeMorgan's laws, with "$\forall$", "$\exists$" in the places of "and", "or", respectively.) We will revisit these properties later on, in the context of proofs, but these rules are generally quite useful to keep in mind since they are used so often.

Note. *Sadly, as we start considering statements with quantifiers, truth tables become less viable, since we are now dealing with infinitely many statements (which would be hard to list in a table!). Thus, we will have to find other ways to systematically deal with quantifiers. We will explore these when we discuss deductive logic and proofs.*

2.5. **Basic Rules of Proof.** We now shift our focus away from Boolean logic, where one views statements as being true or false, toward *deductive logic*, where statements are used as steps in an argument. In particular, a mathematical proof is, at the formal level, a chain of statements that together form a deductive logical argument.

Assumptions:	P_1, P_2, ... P_n
	⋮ *(steps of the proof)* ⋮
Conclusions:	Q

FIGURE 2.2. The basic structure of a formal proof.

The basic structure of a proof is summarised in Figure 2.2. One begins with the given assumptions, represented by statements $P_1, P_2, \ldots, P_n$. The actual steps of the proof, in blue, consists of various intermediate statements that are deduced from the assumptions. The proof ends when one deduces the desired conclusion, given by the statement Q. As a simple analogy, one can think of this as finding one's way along a maze from the starting point (the assumptions) to the exit (the conclusion).

As a first example, for the sample Theorem 1.2 from the introduction and its subsequent proof, one could formulate the assumptions as follows:

- P_1: "x is an even integer".
- P_2: "y is an even integer".

The conclusion that is the goal of the proof is then:

- Q: "$x + y$ is an even integer".

The proof itself is comprised of several statements obtained along the journey from the assumptions P_1, P_2 to the conclusion Q. Examples of intermediate statements include:

- "$x = 2k$ for some integer k".
- "$y = 2l$ for some integer l".
- "$x + y = 2(k + l)$".

Thus far, we have been vague about the actual steps of a proof. How does one progress from the assumptions $P_1, \ldots, P_n$ to the given conclusion Q? More specifically, *what are the valid steps that one can take in such a deductive argument?*

This is where *formal* deductive logic comes in. Indeed, the formal theory defines various rules of inference that indicate which steps are allowed in an argument. These rules are modelled after various bits of intuitive reasoning that you might do in everyday life. The formalisation serves to make the rules precise, so one can, in principle, check unambiguously whether an argument has followed the rules and is hence valid.

Going back to the maze analogy, the rules of inference would correspond to guidelines saying, for example, that you cannot go through any walls of the maze. Similarly, you can think of these rules as akin to, say, the rules of chess specifying how each piece can and cannot move. Thus, the aim is to reach the maze exit without going through walls, or to checkmate your opponent by only making valid moves with your pieces.

In the remainder of this section, we list some of the foundational rules for deductive logic, and we demonstrate how these rules are used in both mathematical and everyday arguments. Since mathematical proofs are, in practice, only written in semi-formal English prose (a fully formal accounting is too long to be useful!), here we will also be semi-formal in our approach. Indeed, *the main focus of our discussions will be on how the formal rules relate to and are applied to intuitive and mathematical arguments.*

> **Note.** *Similarly, in your reading, you should also focus less on the formal rules themselves. (You could even ignore the formalities, if this is your first go.) The most important point here is the intuitions captured by these rules, and how they are used in proofs.*

To make the discussion more approachable, we begin with some simpler rules that do not involve quantifiers. In the following, we let P, Q, R denote arbitrary statements.

2.5.1. *Rules for Implications.* We start with some simple rules regarding implication. The first, usually known as modus ponens, is (semi-)formally depicted in Figure 2.3:

Assume:	$P \Rightarrow Q, \quad P$
Conclude:	Q

FIGURE 2.3. Proof rule: implication elimination (modus ponens)

Without getting too caught up in the formalities, what the rule essentially says is that *if you know that* $P \Rightarrow Q$ *holds, and you also know that* P *holds, then you can conclude that*

Q *holds*. Now, you should ask *why Figure 2.3 is a proof rule*. The reason is that modus ponens captures a very basic bit of logical reasoning that you do all the time:

Example 2.51. *Consider the following bit of logical reasoning:*

- *Suppose you know that if you revise for the NSF exam, then you will pass the NSF exam. Knowing this, you take the responsible action and you revise for the NSF exam. As a result, you can conclude that you will pass the NSF exam.*

Hopefully, the above simple argument already seems quite natural to you, but let us take a closer look at details. First, the statement in red has the form of an implication $P \Rightarrow Q$*. Then, the statement "you revise for the NSF exam" is simply* P*.*

Since we know both $P \Rightarrow Q$ *and* P *hold, we can conclude by modus ponens that* Q *holds, which is simply that "you will pass the NSF exam".*

Example 2.52. *Another simple example of modus ponens is as follows:*

- *You know from calculus that if a function* f *is differentiable, then it is also continuous. Moreover, suppose you are able to show that* f *is differentiable (e.g. by computing its derivative). Thus, you can conclude that* f *is indeed continuous.*

Here, we used the same colour coding as in Example 2.51 above.

The next formal rule gives the basic template for how to prove an implication:

Assume:	**Assume:** | P
	Conclude: | Q
Conclude:	$P \Rightarrow Q$

FIGURE 2.4. Proof rule: implication introduction

Now, the rule in Figure 2.4 seems complicated at first glance, but it is actually not as bad as it looks. (Here, it is best to ignore the formal rule for now and read ahead first to see how it is used!) What the rule really says is that *if you want to prove an implication* $P \Rightarrow Q$*, then you must assume* P *and proceed to argue that* Q *holds.*

Again, why should Figure 2.4 be a rule of deduction? Intuitively speaking, assuming P and then arguing from this that Q holds is (the inner table in Figure 2.4) basically showing "if P, then Q". As a result, it is natural to then infer $P \Rightarrow Q$ from the above.

As usual, the principle is best demonstrated through more concrete examples:

Example 2.53. *Consider the statement from Theorem 1.2:*

- *If x and y are even integers, then $x + y$ is an even integer.*

In particular, the statement has the form of an implication $P \Rightarrow Q$.

Let us look at a paraphrased excerpt of the proof of Theorem 1.2:

Proof. Assume x and y are even integers.
...(do the actual hard work in the proof) ...
Thus, $x + y$ is even.
This completes the proof of the theorem. □

The point to emphasise here is that our aim is to prove the above implication $P \Rightarrow Q$. To do this, we begin the proof by assuming P holds in the orange statement. The hard work happens in the grey part that is omitted here, but all that matters at the moment is that this leads to the conclusion that Q holds, which is the statement in blue.

By the rule in Figure 2.4, we conclude that $P \Rightarrow Q$ holds, which is the statement we wanted to prove. To emphasise this, you can use a bit of flavour text, such as "this completes the proof of the theorem" above. However, this is often omitted, as experienced proof readers know well to apply the rule automatically.

Example 2.54. *Consider the following statement:*

- *If x is any real number, then $x^2 - 2x + 1 \geq 0$.*

A proof of this statement is given below:

Proof. Suppose x is a real number. Then, x^2-2x+1 can be factored as $(x-1)^2$, which is a perfect square and hence is non-negative. Thus, we conclude $x^2-2x+1 \geq 0$. □

Again, the statement to be proved is of the form $P \Rightarrow Q$. The proof begins by assuming P (in orange) holds. A few short steps later, the proof shows that Q (in blue) holds. Once again, the rule in Figure 2.4 yields that $P \Rightarrow Q$ holds, as desired.

Note. *Often, when proving an implication $P \Rightarrow Q$ (such as in Examples 2.53–2.54), mathematicians will omit writing the first step "assume P holds". This is because this step is implicitly understood by those familiar with proof writing. However, it is fine to always include this step in your writing until you are more comfortable with proofs.*

2.5.2. *Rules for Conjunctions.* Next, we turn to some rules of inference involving conjunctions. First, we give the rule for proving a conjunction:

Assume:	P, Q
Conclude:	P and Q

FIGURE 2.5. Proof rule: conjunction introduction

The rule is as simple as it looks—it says that *if you know that* P *is true, and if you know that* Q *is true, then you can conclude that* P and Q *is true.* Let us now see it in action:

Example 2.55. *Consider the following snippet of logical reasoning:*

- *Suppose you know Venice is in Italy. You then look at a map and find that Rome is in Italy. Then, you can conclude that both Venice and Rome are in Italy.*

To connect this to Figure 2.5, we let P be the statement "Venice is in Italy", and we let Q *denote the statement "Rome is in Italy". Applying Figure 2.5 then yields* P and Q*, which precisely corresponds to "both Venice and Rome are in Italy".*

If you look at the argument in Example 2.55 and think it is extremely obvious, then you would be correct! The rules of inference are intended to model, in a formal and precise way, steps that you would normally do when reasoning logically. Indeed, the rule is Figure 2.5 is one that you probably do very naturally, without even thinking about it.

Let us now introduce an even easier rule for removing a conjunction:

Assume:	P and Q
Conclude:	P, Q

FIGURE 2.6. Proof rule: conjunction elimination

This rule simply says that *if you know* P and Q *holds, then you can conclude that both* P *and* Q *hold individually.* Again, this rule is something that you do automatically without a second thought, but you should take a few seconds to convince yourself that this makes intuitive sense. For completeness, we give a simple example demonstrating the rule:

Example 2.56. *Consider the following snippet of logical reasoning:*

- *I study mathematics and finance. In particular, I study mathematics.*

Note that "I study mathematics and finance" can be interpreted as P and Q*, with:*

- P: *"I study mathematics".*
- Q: *"I study finance".*

By Figure 2.6, from P and Q, *we conclude* P, *i.e. "I study mathematics".*

2.5.3. *Rules for Disjunctions.* We now move on to a rule for proving disjunctions:

Assume:	P
Conclude:	P or Q, Q or P

FIGURE 2.7. Proof rule: disjunction introduction

The idea is that P *holds, then it must be that* P or Q *and* Q or P *must hold.* (This makes sense from the perspective of Boolean logic, since if P is true, then P or Q and Q or P are true regardless of the truth value of Q.) Let us look at one example as well:

Example 2.57. *Consider the following bit of logical reasoning:*

- *Suppose* $x < 3$. *Then,* $x \leq 3$ *as well.*

In particular, if we let P be the statement $x < 3$, *then Figure 2.7 implies that* P or Q *holds. Now, if* Q *is the statement* $x = 3$, *then* P or Q *is precisely the above conclusion,* $x \leq 3$. *(Recall that "*$x < 3$ or $x = 3$*" is commonly written as* $x \leq 3$.*)*

Let us consider another similar rule for introducing a disjunction:

Assume:	*(nothing!)*
Conclude:	P or (not P)

FIGURE 2.8. Proof rule: law of excluded middle

The rule in Figure 2.7 simply captures that *a statement* P *is always either true (*P *holds) or false (*not P *holds).* In particular, no extra assumption is required for this to hold.

Example 2.58. *Consider the following bit of logical reasoning:*

- *Let* x *be an integer. Then,* x *is either even or odd.*

Here, we let P *be the statement "*x *is even". In the above argument, we can conclude for free that* P or (not P) *holds, which is precisely the concluding statement above. (Since* not P *can be interpreted as "*x *is odd", then* P or (not P) *is precisely "*x *is even or odd".)*

Note. *The rule in Figure 2.8 is commonly known as the law of excluded middle, and it serves to capture the Boolean nature of logic. There are other theories of deductive logic that do not adopt the law of excluded middle as a rule; these model "fuzzy" logical systems where statements need not always be either true or false.*

There are also rules for eliminating disjunctions, however demonstrating these tend to be a bit more involved, so we save this for the next section.

2.5.4. *Rules for Equivalences.* We conclude this section by considering a couple basic rules for equivalences. These are based primarily on the *equivalence law* from Section 2.3 that related equivalences and implications; see the table in Figure 2.1.

First, we provide the key rule for proving logical equivalences:

Assume:	$P \Rightarrow Q, \quad Q \Rightarrow P$
Conclude:	$P \Leftrightarrow Q$

FIGURE 2.9. Proof rule: equivalence introduction

The rule in Figure 2.9 states that *if you know that* Q *follows from* P*, and you also know that* P *follows from* Q*, then you can conclude that* P *and* Q *are equivalent* (i.e. P and Q are logically the same). Hopefully, this makes some intuitive sense to you, but you can also think of this as being inspired by our previous knowledge of Boolean logic—that $P \Leftrightarrow Q$ has the same truth values as $(P \Rightarrow Q)$ and $(Q \Rightarrow P)$.

In practice, this provides a *clear two-part plan for proving a statement* $P \Leftrightarrow Q$:

- *Step 1:* Show $P \Rightarrow Q$ holds.
- *Step 2:* Show $Q \Rightarrow P$ holds.

Note we already discussed how to prove implication statements via the rule from Figure 2.4. Thus, to prove an equivalence, we essentially just have to use that rule twice.

Example 2.59. *Let us prove the following simple result:*

- *Let* x *be a real number. Then,* $x > 0$ *if and only if* $2x > 0$.

Proof. First, suppose $x > 0$. Multiplying both sides by 2 then yields $2x > 0$.
Conversely, assume $2x > 0$. Dividing both sides by 2 yields $x > 0$.
This completes the proof of the above statement. □

We can now analyse the structure of the above proof. Consider the statements

- P: $x > 0$.
- Q: $2x > 0$.

Note then that the statement we wish to prove (in red) is just $P \Leftrightarrow Q$. *To show this, the proof above breaks the argument into two separate parts:*

- *In the first line of the proof, we assume* P *(*$x > 0$*), and we proceed to derive* Q *(*$2x > 0$*). This then shows that* $P \Rightarrow Q$ *holds.*
- *In the second line of the proof, we assume* Q *(*$2x > 0$*), and we proceed to derive* P *(*$x > 0$*). This then shows that* $Q \Rightarrow P$ *holds.*

Having now shown both $P \Rightarrow Q$ *and* $Q \Rightarrow P$*, we conclude that* $P \Leftrightarrow Q$ *indeed holds using the rule from Figure 2.9. (The last line of the proof, "this completes the proof...", is not strictly necessary; it is akin to taking an extra victory lap to make clear to the reader that you have done everything needed to complete the proof.)*

Note. *In Example 2.59, the word "conversely" in the second line of proof refers to the fact that this part of the argument is intended to prove* $Q \Rightarrow P$*—the converse of implication* $P \Rightarrow Q$ *that was proved in the previous line.*

Example 2.60. *Let us prove the following simple statement:*

- *Let* x, y *be real numbers. Then,* $x = y$ *if and only if* $x - y = 0$.

Proof. First, assume $x = y$. Subtracting y from both sides then yields $x - y = 0$.
Conversely, suppose $x - y = 0$. Adding y to both sides then yields $x = y$. □

Again, the aim is to prove the equivalence $(x = y) \Leftrightarrow (x - y = 0)$*. For this:*

- *The first line of the proof shows that* $(x = y) \Rightarrow (x - y = 0)$.
- *The second line of the proof shows that* $(x - y = 0) \Rightarrow (x = y)$.

By the rule in Figure 2.9, we can then conclude $(x = y) \Leftrightarrow (x - y = 0)$.

On the other side, we now provide rules for eliminating equivalences:

Assume:	$P \Leftrightarrow Q$, P
Conclude:	Q

Assume:	$P \Leftrightarrow Q$, Q
Conclude:	P

FIGURE 2.10. Proof rule: equivalence elimination

Observe the above rules resemble modus ponens from Figure 2.3. Indeed, the inspiration is again that $P \Leftrightarrow Q$ *should be logically the same as* $P \Rightarrow Q$ *and* $Q \Rightarrow P$. Thus:

- If you know P holds, then applying modus ponens to $P \Rightarrow Q$ gives you Q.
- If you know Q holds, then applying modus ponens to $Q \Rightarrow P$ gives you P.

Example 2.61. *Consider the following snippet of logical reasoning:*

- *Let* x *be an integer. One fact we know is that* x *is even if and only if* x^2 *is even. Assume now that* x^2 *is even. We can then conclude that* x *must also be even.*

To analyse the above, let us consider the statements

- P*: "*x *is even".*
- Q*: "*x^2 *is even".*

Observe that in the above snippet, we are given both $P \Leftrightarrow Q$ *(in red) and* Q *(in blue). Thus, by the rule in Figure 2.10 (the table on the right), we conclude* P *(in orange).*

Note. *An alternative way to state the "equivalence elimination" rules in Figure 2.10 is:*

Assume:	$P \Leftrightarrow Q$
Conclude:	$P \Rightarrow Q, \quad Q \Rightarrow P$

(In fact, one recovers the rules in Figure 2.10 by combining the above with modus ponens.)

2.6. **Proof Strategies.** Previously, we covered various basic rules of inference in deductive logic. Here, we look at some more complicated rules that are connected to common strategies in proofs, as well as some rules that can be derived from other ones.

2.6.1. *Proof by Cases.* Recall that we have not yet mentioned a rule that removes disjunctions from statements. The following provides a mechanism for doing this:

Assume:	P or $Q, \quad P \Rightarrow R, \quad Q \Rightarrow R$
Conclude:	R

FIGURE 2.11. Proof rule: disjunction elimination (proof by cases)

Intuitively, the rule in Figure 2.11 is connected to a common proof strategy, known as proof by cases. Suppose you wish to prove that R holds, but you currently only know that either P or Q holds. The idea is then to break the proof into cases—suppose:

- *Case 1:* You can show that if P holds, then so does R.

- *Case 2:* You can show that if Q holds, then so does R.

Then, since both of the possible cases P, Q lead to R, it follows that R must always be true.

The name "proof by cases" refers to the fact that an argument using this rule is written in English prose as a subdivision into cases. We take a look at some examples below:

Example 2.62. *Let us prove the following simple result:*

- *Let* k *be an integer. Then,* $k^2 + k$ *is even.*

Proof. We know k is either even or odd, and we split the proof into cases:

- First, suppose k is even. Then, $k = 2l$ for some integer l, and hence
$$\begin{aligned} k^2 + k &= 4l^2 + 2l \\ &= 2(2l^2 + l). \end{aligned}$$
Thus, it follows that $k^2 + k$ is indeed even.
- Next, suppose k is odd. Then, $k = 2l + 1$ for some integer l, and hence
$$\begin{aligned} k^2 + k &= (4l^2 + 4l + 1) + (2l + 1) \\ &= 2(2l^2 + 3l + 1). \end{aligned}$$
Thus, it again follows that $k^2 + k$ is even.

Since both cases imply $k^2 + k$ is even, we conclude that $k^2 + k$ is always even. □

To analyse the structure of the above proof, let us consider the statements

- P*: "*k *is even".*
- Q*: "*k *is odd".*
- R*: "*$k^2 + k$ *is even".*

Note that the statement we wish to prove is precisely R*, while we trivially know from the beginning that* P or Q *holds (by Figure 2.8, since* Q *is just* not P*).*

We now break the proof into two cases. In the first case, we assume P *holds (in blue), and we derive from this that* R *holds; this proves* $P \Rightarrow R$*, by the rule from Figure 2.4. Similarly, for the second case, we assume* Q *holds (in pink), and we derive again that* R *holds, proving* $Q \Rightarrow R$*. As a result, all possible cases lead to* R*—i.e. we have shown*

$$P \text{ or } Q, \qquad P \Rightarrow R, \qquad Q \Rightarrow R.$$

Thus, by the rule from Figure 2.11, we conclude R *holds; the last line of the proof, while not completely necessary, simply emphasises this point for clarity.*

Hopefully, when reading the proof in Example 2.62, the logic seems quite natural already. Thus, the "proof by cases" rule just serves to formalise of this bit of everyday logical reasoning. For now, you can again worry less about the computational bits of the proof, as the current emphasis is on the proof's logical structure.

Also, while the rule in Figure 2.11 and Example 2.62 only consider two cases, the principle *extends to decomposing into three or more cases as well.* (Formally, you would do this by applying Figure 2.11 multiple times, but we omit the details.)

Example 2.63. *Let us prove the following simple result:*

- *Let* n *be an integer. Then,* $\frac{n+\frac{1}{2}}{n+\frac{1}{3}} > 0$.

Proof. We know that n must be (strictly) positive, negative, or zero.

- First, if $n > 0$, then both $n + \frac{1}{2}$ and $n + \frac{1}{3}$ must also be positive. Since the quotient of two positive numbers is positive, then $\frac{n+\frac{1}{2}}{n+\frac{1}{3}} > 0$.
- Next, if $n < 0$, then both $n + \frac{1}{2}$ and $n + \frac{1}{3}$ are negative. Since the quotient of two negative numbers is positive, then $\frac{n+\frac{1}{2}}{n+\frac{1}{3}} > 0$.
- Finally, if $n = 0$, then both $n + \frac{1}{2}$ and $n + \frac{1}{3}$ are again positive, so we once again conclude that $\frac{n+\frac{1}{2}}{n+\frac{1}{3}} > 0$.

Since we have covered all the possible cases, the proof is complete. □

Note that in the proof of Example 2.63, the first and third cases could be combined into a single case $n \geq 0$, since both cases are treated in exactly the same way. In particular, this would shorten the proof to only two cases and remove some unnecessary repetition. In practice, you should simplify proofs wherever you can, as this makes the argument more elegant and easier to read, as well as less work for you!

2.6.2. *Proof by Contradiction.* The next rule also encapsulates a common method of proof, though it tends to cause some confusion due to its rather unusual structure:

Assume:	$(\text{not } P) \Rightarrow Q, \quad (\text{not } P) \Rightarrow (\text{not } Q)$
Conclude:	P

FIGURE 2.12. Proof rule: proof by contradiction

In Figure 2.12, the objective is to prove P holds. The unusual (and rather apocalyptic!) aspect, however, is that rather than showing P directly, the idea is to argue that *if* P *does not hold, then the mathematical universe is completely destroyed and ceases to make sense.*

Indeed, the starting point of a proof by contradiction is to *assume the opposite of what you want to prove*, that is, not P. The goal is then given in the two implications in top line of Figure 2.12—we wish to *show that, assuming* not P *holds, we can then derive that both* Q *and* not Q *hold.* Since Q and not Q contradict each other, this is an absurd situation, and our entire logical universe is utterly destroyed! Thus, the only way to avoid the absurd (and save logic and maths like a superhero!) is that P must hold.

Example 2.64. *Let us prove the following statement by contradiction:*

- *Let* $0 < x < 1$ *be a real number. Then,* $\frac{1}{x(1-x)} \geq 4$.

Proof. Suppose, for a contradiction, that $\frac{1}{x(1-x)} < 4$. Rearranging this then yields

$$\begin{aligned} 1 &< 4x(1-x) \\ &= -4x^2 + 4x. \end{aligned}$$

Rearranging the preceding inequality again, we then obtain $4x^2 - 4x + 1 < 0$. However, since $4x^2 - 4x + 1$ can be factored into a perfect square,

$$4x^2 - 4x + 1 = (2x-1)^2,$$

then we also have that $4x^2 - 4x + 1 \geq 0$, and hence we obtain a contradiction. As a result, we conclude that $\frac{1}{x(1-x)} \geq 4$ must hold. □

To analyse the structure of the proof, let us consider the statements

- P: $\frac{1}{x(1-x)} \geq 4$.
- Q: $4x^2 + 4x + 1 < 0$.

Note that P *(in red) is precisely the statement that we wish to prove. The proof, however, begins by assuming instead* not P *(in orange). Then:*

- *From this assumption* not P*, we derive that the statement* Q *(in blue) must hold. This means (from the rule in Figure 2.4) that* $(\text{not P}) \Rightarrow \text{Q}$ *holds.*
- *At the same time, we know (from elementary algebra) that* not Q *(in pink) also holds. Thus, we also have* $(\text{not P}) \Rightarrow (\text{not Q})$.

In particular, Q *and* not Q *together comprise the contradiction that follows from assuming* not P*. More formally, applying the rule in Figure 2.12 to the implications*

$$(\text{not P}) \Rightarrow \text{Q}, \qquad (\text{not P}) \Rightarrow (\text{not Q})$$

established above, we conclude that P *must hold, as desired.*

Example 2.65. *Let us prove the following statement by contradiction:*

- *Let n be an integer. If n^2 is even, then n is also even.*

Proof. Let n be an integer, and assume n^2 is even. Suppose, for a contradiction, that n is odd. Then, $n = 2k + 1$ for some integer k, and hence

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 2(2k^2 + 2k) + 1, \end{aligned}$$

and it follows that n^2 is odd, which contradicts our assumption that n^2 is even. Thus, we conclude that n must be even, which completes the proof. □

For convenience, we label the following statements:

- P: *"n is even".*
- Q: *"n^2 is odd".*

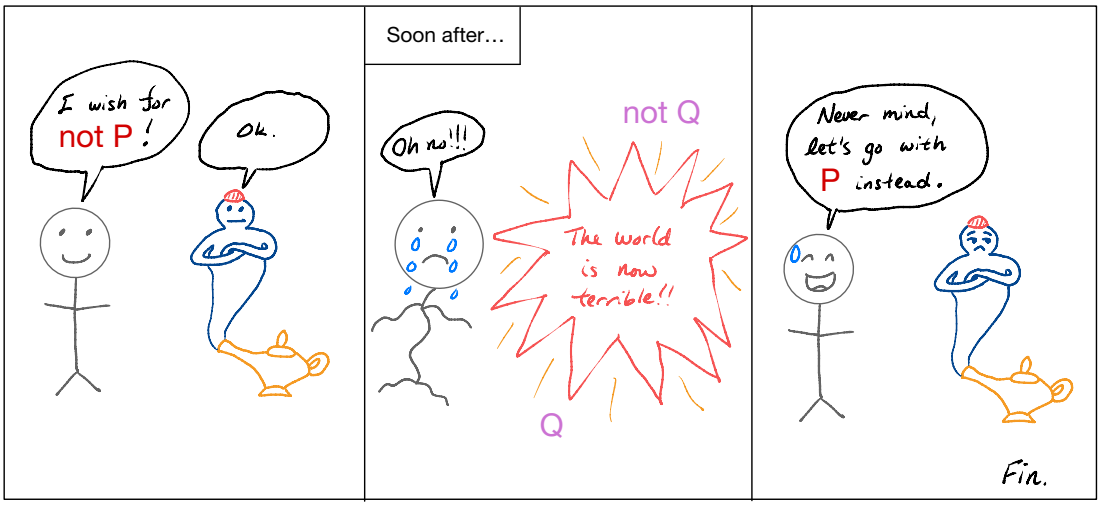
First, the statement we wish to prove is the implication

$$(n^2 \textit{ is even}) \Rightarrow (n \textit{ is even}),$$

thus the proof starts by assuming "n^2 is even" (in pink), with the aim being to show "n is even", i.e. P (in red). We prove P by contradiction—assuming not P *(in orange):*

- *We derive that Q ("n^2 is odd", in blue) holds.*
- *Our starting assumption was* not Q *("n^2 is even", in pink), so this holds too.*

Thus, we have a contradiction, and Figure 2.12 yields that P holds.



2.6.3. *Proof by Contrapositive.* Besides the "foundational" rules of inference that we have already discussed, there are *many additional rules that can be derived from existing ones.* We now discuss some useful derived rules, starting with another common proof strategy:

Assume:	$(\text{not } Q) \Rightarrow (\text{not } P)$
Conclude:	$P \Rightarrow Q$

FIGURE 2.13. Proof rule: proof by contrapositive

Note the rule in Figure 2.13 is closely connected to the property that an implication is equivalent to its contrapositive (see Figure 2.1). Indeed, the rule states that *one can prove an implication* $P \Rightarrow Q$ *by showing that its contrapositive* $(\text{not } Q) \Rightarrow (\text{not } P)$ *holds.* This provides an alternative to the direct method from Figure 2.4 for proving implications.

Example 2.66. *Let us revisit the statement from Example 2.65:*

- *Let* n *be an integer. If* n^2 *is even, then* n *is also even.*

In contrast to Example 2.65, here we prove the statement via the contrapositive.

Proof. Suppose n is odd. Then, $n = 2k + 1$ for some integer k, and hence

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 2(2k^2 + 2k) + 1, \end{aligned}$$

and it follows that n^2 is odd, which completes the proof. □

For convenience, we label the following statements:

- P*: "*n^2 *is even".*
- Q*: "*n *is even".*

In particular, the statement to be proved is precisely $P \Rightarrow Q$*.*

The proof begins by assuming not Q *(in orange). From this assumption, we proceed to derive* not P *(in pink). By the rule from Figure 2.4, this yields* $(\text{not } Q) \Rightarrow (\text{not } P)$*, which is the contrapositive of the implication we want to prove. Finally, applying the rule from Figure 2.13 results in our desired statement* $P \Rightarrow Q$*.*

Note that although the proof by contrapositive in Example 2.66 has a *different structure* from the proof by contradiction of the same statement in Example 2.65, *the two proofs make use of the same mathematical insight* (the square of an odd number must be odd).

In addition, the final logical step of the proof in Example 2.66—applying the rule from Figure 2.13—is often not written, as it is usually obvious to experienced proof readers.

Example 2.67. *Let us prove the following statement via the contrapositive:*

- *Let* a, b, c *be integers. If* $a + b + c$ *is odd, then at least one of* a, b, c *is odd.*

Proof. We prove the contrapositive—suppose a, b, c are all even. Then, by definition, $a = 2k$, $b = 2l$, and $c = 2m$ for some integers k, l, m. As a result,

$$a + b + c = 2(k + l + m)$$

is even, completing the proof. □

The proof structure is analogous to that of Example 2.66. Here, the statement to prove has the form $P \Rightarrow Q$*, where* P *and* Q *can be interpreted as*

- P*: "*$a + b + c$ *is odd".*
- Q*: "(*a *is odd)* or *(*b *is odd)* or *(*c *is odd)".*

Once again, the objective is to prove the contrapositive $(\text{not } Q) \Rightarrow (\text{not } P)$*. The proof begins by assuming the negation of* Q *(recall DeMorgan's laws in Figure 2.1):*

- not Q*: "(*a *is even)* and *(*b *is even)* and *(*c *is even)".*

After a quick computation, one derives not P *(in pink).*

Finally, we mentioned earlier the *proof by contrapositive* rule in Figure 2.13 can be derived from existing rules—in fact, from *proof by contradiction* (Figure 2.12). Thus, it was no accident that the statement in Examples 2.65–2.66 could be proved both ways!

Note. *For those who are more ambitious or wish to toy around a bit more with deductive logic, an informal derivation of Figure 2.13 from Figure 2.12 is provided here:*

Proof. Assume $(\text{not } Q) \Rightarrow (\text{not } P)$ holds; we aim to show $P \Rightarrow Q$ holds. For this, we assume P. Now, if not Q holds, then our first assumption implies not P holds, which contradicts our assumption P. Thus, Q must hold, and we have shown $P \Rightarrow Q$. □

2.6.4. *Other Derived Rules.* We conclude the section by briefly discussing a few other simple rules of inference that are both commonly useful and intuitive.

First, another consequence of proof by contradiction (Figure 2.12) is the following:

Assume:	not(not P)
Conclude:	P

Assume:	P
Conclude:	not(not P)

FIGURE 2.14. Proof rule: double negation

Example 2.68. *Consider the following snippet of logical reasoning:*

- *Suppose it is not the case that* $x \neq 3$*. Then,* $x = 3$*.*

Here, the first sentence is interpreted as the negation of $x \neq 3$*, that is,* $\text{not not}(x = 3)$*. The second line applies the rule from Figure 2.14 to note this is the same as* $x = 3$*.*

Note. *One can derive the first rule in Figure 2.14 from proof by contradiction:*

Proof. Assume $\text{not}(\text{not } P)$ holds; we aim to show P holds. Suppose that not P holds. Then, not P implies both itself (trivially) and $\text{not}(\text{not } P)$ (by the above assumption), so we have a contradiction. Thus, it follows from Figure 2.12 that P holds. □

The next rule—classically known as modus tollens—is a combination of modus ponens (Figure 2.3) and the fact that an implication is equivalent to its contrapositive:

Assume:	$P \Rightarrow Q$, not Q
Conclude:	not P

FIGURE 2.15. Proof rule: contrapositive elimination (modus tollens)

Example 2.69. *Consider the following bit of logical reasoning:*

- *Suppose you know that if you revise for the NSF exam, then you will pass the NSF exam. But, unfortunately, you did not pass the NSF exam. As a result, I know that you did not revise for the NSF exam.*

The structure is very similar to that of Example 2.51. In particular:

- *The statement in red has the form of an implication* $P \Rightarrow Q$*.*
- *The statement in orange is simply* not Q*.*

As a result, we conclude by modus tollens that not P *(in blue) holds.*

The next rule is a variant of proof by cases:

Assume:	P or Q, not P
Conclude:	Q

FIGURE 2.16. Proof rule: disjunctive syllogism

Intuitively, the rule in Figure 2.16 states that if there are two possible cases (P, Q here), and you have eliminated the first case (P here), then the second case (Q) must hold.

Example 2.70. *Let us prove the following simple result:*

- *Let x, y be real numbers. Then, if $xy = 0$ and $x \neq 0$, then $y = 0$.*

Proof. Suppose $xy = 0$ and $x \neq 0$. Since $xy = 0$, we know that either $x = 0$ or $y = 0$. Since $x \neq 0$, it follows that $y = 0$, as desired. □

To analyse the structure of the proof, we consider the statements

- P: "$x = 0$".
- Q: "$y = 0$".

Here, one statement that we take (for simplicity) as "already known" is that if $xy = 0$, then $x = 0$ or $y = 0$—which is P or Q*. However, since we are already given $x \neq 0$ (which is* not P*), then by the rule in Figure 2.16, we conclude that* Q *(i.e. $y = 0$) holds.*

Finally, it turns out *any equivalence from Boolean logic can be established as two reversible rules.* In particular, this means we can create two rules out of each row of the table in Figure 2.1. (There is a reason for this; see the discussion in Section 2.8.) For instance:

Example 2.71. *The following rules arise from DeMorgan's laws in Figure 2.1:*

Assume:	not(P and Q)
Conclude:	(not P) or (not Q)

Assume:	(not P) or (not Q)
Conclude:	not(P and Q)

Example 2.72. *The following rules arise from the commutative laws in Figure 2.1:*

Assume:	P or Q
Conclude:	Q or P

Assume:	Q or P
Conclude:	P or Q

Note. *In fact, we can do far more that what was mentioned above. If two statements* P *and* Q *are equivalent in Boolean logic (e.g. any of the rows in Figure 2.1), then we can replace any instance of* P *within a larger statement by* Q*, and vice versa. Such rules can be derived (rather painstakingly) from the existing rules described in this chapter.*

As just one example, the commutative law in Figure 2.1 yields the following rule:

Assume:	$(P \text{ or } Q) \Rightarrow R$	***Assume:***	$(Q \text{ or } P) \Rightarrow R$
Conclude:	$(Q \text{ or } P) \Rightarrow R$	***Conclude:***	$(P \text{ or } Q) \Rightarrow R$

Here, we replaced P or Q *within a larger statement by the equivalent* Q or R.

2.7. **Proofs with Quantifiers.** Thus far in our discussions of deductive logic, we have studiously avoided any mention of quantifiers. This was primarily to avoid presenting too much information in one iteration by isolating many of the simpler mechanics of proofs. However, it is now time to take the training wheels off and extend our rules of inteference to the full family of statements we will consider, quantifiers included!

2.7.1. *Universal Quantifiers.* At the basic level, we need rules both for introducing quantifiers into statements and for eliminating quantifiers from statements. We begin with the universal quantifier—the simpler rule is the one that removes "$\forall$":

Assume:	$\forall_{Q(x)} P(x)$	
Conclude:	$P(y)$	*(any* y *such that* $Q(y)$ *holds)*

FIGURE 2.17. Proof rule: universal elimination

The rule in Figure 2.17 allows one to remove the "$\forall_{Q(x)}$" from a statement $\forall_{Q(x)} P(x)$ and conclude $P(y)$, where y *stands for any concrete variable such that* $Q(y)$ *holds.*

The intuition behind this is quite simple. Recall that the interpretation for $\forall_{Q(x)} P(x)$ is that "$P(x)$ holds for any x such that $Q(x)$ holds". Thus, if we now take some object y such that $Q(y)$ holds, then it should naturally follow from the above that $P(y)$ should hold. The rule in Figure 2.17 precisely captures this bit of intuitive reasoning.

Example 2.73. *Consider the following snippet of logical reasoning:*

- *We know that* $(x-1)^2 \geq 0$ *for all real numbers* x*. In particular, since* 3 *is a real number, then we conclude that* $(3-1)^2 \geq 0$.

To connect the above to Figure 2.17, we consider the statements

- $P(x)$*: "*$(x-1)^2 \geq 0$*".*
- $Q(x)$*: "*x *is a real number".*

Notice the first sentence of the above can be more precisely parsed as $\forall_{Q(x)} P(x)$*. As for the second sentence, since* $Q(3)$ *holds (that is,* 3 *is a real number), then from the rule in Figure 2.17, we conclude that* $P(3)$ *holds, that is,* $(3-1)^2 \geq 0$.

The more interesting—as well as the more commonly applied—rule for universal quantifiers, however, is the one for proving a statement that contains a "$\forall$". The rule itself can be stated in a semi-formal (though not particularly helpful) manner as follows:

Assume:	$P(y)$ *(*y *arbitrary, such that* $Q(y)$ *holds)*
Conclude:	$\forall_{Q(x)} P(x)$

FIGURE 2.18. Proof rule: universal introduction

Although this rule is actually quite intuitive, it is also rather tricky to describe. The idea is that *if one can show* $P(y)$ *holds for any arbitrary* y*, without restrictions on* y *except that* $Q(y)$ *holds, then one can conclude that* $P(x)$ *holds for every* x *satisfying* $Q(x)$. In essence, this arbitrary y can stand in for any object x such that $Q(x)$ holds. Thus, the argument showing $P(y)$ holds extends also to showing $P(x)$ for any other x satisfying $Q(x)$.

As usual, the rule is far easier to explain via concrete examples:

Example 2.74. *Let us prove the following simple result:*

- $x^2 - 2x + 1 \geq 0$ *for any real number* x.

Proof. Let x be any real number. Then, we can factor $x^2 - 2x + 1 = (x-1)^2$. Since this is a perfect square, we conclude that $x^2 - 2x + 1 \geq 0$, as desired. □

The statement to be proved is similar to those from previous examples, though here we no longer shy away from quantifiers. Observe we wish to prove $\forall_{Q(x)} P(x)$*, where*

- $P(x)$*: "*$x^2 - 2x + 1 \geq 0$*".*
- $Q(x)$*: "*x *is a real number".*

Most crucially, to prove this statement, we begin by letting x *be an arbitrary object satisfying* $Q(x)$ *(the first sentence of the proof, in orange). After a very short computation, we derive that* $P(x)$ *indeed holds for this* x *(the last sentence of the proof, in red).*

Now, since $P(x)$ *holds for this arbitrary* x *satisfying* $Q(x)$ *(i.e. for any real nmber* x*), then by the rule in Figure 2.18, we conclude that "*$P(x)$ *holds for all* x *satisfying* $Q(x)$*", which is precisely the statement we wished to prove.*

Note that the proof in Example 2.74 started by fixing an arbitrary x satisfying $Q(x)$. Strictly speaking, the rule in Figure 2.18 asks that we fix a different symbol y satisfying $Q(y)$. However, when writing proofs in practice, we usually just use the same symbol x, since this does not tend to cause any confusion, and since this keeps us from using an excess number of symbols (which can itself be confusing to read).

Hopefully, Example 2.74 makes the rule in Figure 2.18 more logically intuitive. In practice, the main point to keep in mind is summarised as follows: *in order to prove* $\forall_{Q(x)} P(x)$, *you need to fix an arbitrary* x *such that* $Q(x)$ *holds, and you show* $P(x)$ *holds for this* x.

Example 2.75. *Let us again prove the sample Theorem 1.2:*

- *The sum of any two even integers is an even integer.*

Proof. Let x, y be arbitrary integers, and suppose x and y are even numbers. Then, there are integers k and l such that $x = 2k$ and $y = 2l$. But then,

$$\begin{aligned} x + y &= 2k + 2l \\ &= 2(k + l). \end{aligned}$$

Since $x + y$ is 2 times the number $k + l$, then $x + y$ is even, as desired. □

A more precise interpretation of the statement to be proved is as follows:

$$\forall_{\text{integers } x,\, y}((x, y \text{ are even}) \Rightarrow (x + y \text{ is even})). \tag{2.1}$$

To prove this "for all" statement, we first let x *and* y *be arbitrary integers. The goal is to prove the implication* $(x, y \text{ are even}) \Rightarrow (x + y \text{ is even})$, *since then the rule in Figure 2.18 lets us conclude the statement* (2.1) *we ultimately want to prove.*

Now, to prove this implication, we resort to Figure 2.4—we assume x, y *are even, and we proceed to show via the usual computation that* $x + y$ *is even. Note this part of the proof is identical to what was already demonstrated in Example 2.53.*

Note. *Throughout these lecture notes, we will assign numbers to various equations—for instance, Equation* (2.1) *in Example 2.75. This numbering is useful, since we can more conveniently refer back to these equations later on in the text.*

Example 2.76. *Let us now expand upon Examples 2.65–2.66:*

- *For any integer* n, *we have that* n *is even if and only if* n^2 *is even.*

Proof. Let n be any integer.

- Suppose n is even. Then, $n = 2k$ for some integer k, and a direct computation yields that $n^2 = 2(2k^2)$. As a result, n^2 is also even.

- Conversely, suppose n is odd. Then, $n = 2l + 1$ for some integer l, and we can hence compute $n^2 = 2(2l^2 + 2l) + 1$. Thus, n^2 is odd as well.

In particular, the above shows n is even if and only if n^2 is even, as desired. □

This proof combines several rules. First, the statement to be proved has the form

$$\forall_{\textit{integer } n}((n \textit{ is even}) \Leftrightarrow (n^2 \textit{ is even})). \tag{2.2}$$

Once again, we prove (2.2) *using the rule from Figure 2.18—we fix an arbitrary integer* n*, and we show the equivalence inside the quantifier for this* n*:*

$$(n \textit{ is even}) \Leftrightarrow (n^2 \textit{ is even}). \tag{2.3}$$

Now, to prove (2.3)*, we resort to the rule from Figure 2.9—in other words, we must show that each side of* (2.3) *implies the other side:*

- *The implication* $(n \textit{ is even}) \Rightarrow (n^2 \textit{ is even})$ *is proved in the first bullet point. This is done using Figure 2.4—we assume* n *is even, and we derive* n^2 *is even.*
- *The converse,* $(n^2 \textit{ is even}) \Rightarrow (n \textit{ is even})$*, is proved in the second bullet point by contrapositive (see Figure 2.13)—that is, like in Example 2.66, we prove instead the contrapositive implication* $(n \textit{ is odd}) \Rightarrow (n^2 \textit{ is odd})$.

Lastly, we note that there are analogous rules for *unrestricted* universal quantifiers:

- Assuming $\forall_x P(x)$, we can conclude $P(y)$, with y being any variable.
- Assuming $P(x)$ holds for an arbitrary x, we conclude $\forall_x P(x)$.

Note these can be thought of as simply the rules from Figures 2.17 and 2.18, but with $Q(x)$ now being any statement that is always true.

Note. *In fact, in formal logic, the above rules for unrestricted universal quantifiers are considered the foundational rules. The ones in Figures 2.17 and 2.18 can then be derived from their unrestricted analogoues by interpreting* $\forall_{Q(x)} P(x)$ *as* $\forall_x (Q(x) \Rightarrow P(x))$.

2.7.2. *Existential Quantifiers.* Similar to universal quantifiers, there are two basic rules for dealing with existential quantifiers. We start with the simpler rule for introducing a "$\exists$":

Assume:	$P(y)$ *(any* y *satisfying* $Q(y)$*)*
Conclusion:	$\exists_{Q(x)} P(x)$

FIGURE 2.19. Proof rule: existential introduction

The logical intuition behind Figure 2.19 is simple—*if you know* $P(y)$ *holds for a single* y *for which* $Q(y)$ *holds, then you can conclude "there exists* x *satisfying* $Q(x)$ *such that* $P(x)$ *holds"* (namely, y!). This is precisely how one would naturally interpret "there exists".

Let us demonstrate this via a couple concrete examples:

Example 2.77. *Consider the following snippet of logical reasoning:*

- *Since* 2 *is an integer, and since* $2^2 - 3 \cdot 2 + 1 < 0$*, then we know there exists an integer* x *such that* $x^2 - 3x + 1 < 0$.

To connect the above to Figure 2.19, we consider the statements

- $P(x)$*: "*$x^2 - 3x + 1 < 0$*".*
- $Q(x)$*: "*x *is an integer".*

Now, the first part of the snippet states that $P(2)$ *holds (in orange). Of course, the integer* 2 *here is a variable for which* $Q(2)$ *holds (in pink). As a result, one can then apply the rule from Figure 2.19 to conclude* $\exists_{Q(x)} P(x)$*—the statement at the end of the snippet.*

Example 2.78. *Let us prove the following statement:*

- *There exist real numbers* x *and* y *such that*

$$x + y = 3, \qquad x - y = -1. \tag{2.4}$$

Proof. Setting $x = 1$ and $y = 2$, we can immediately check that

$$1 + 2 = 3, \qquad 1 - 2 = -1.$$

This proves the desired statement. □

Observe that the statement to be proved can be expressed more precisely as

$$\exists_{\text{real number } x} \exists_{\text{real number } y} R(x, y), \tag{2.5}$$

where $R(x, y)$ *is the statement "*$x + y = 3$ and $x - y = -1$*". (Note that the comma in Equation* (2.4) *is interpreted as "*and*".) By substituting real numbers* 1 *into* x *and* 2 *into* y*, we can directly check that* $R(1, 2)$ *holds (in blue in the proof). Thus, applying the rule in Figure 2.19 (twice), we conclude that* (2.5) *holds, completing the proof.*

Regarding Figure 2.19, the main practical point to keep in mind can be summarised as follows: *in order to prove* $\exists_{Q(x)} P(x)$*, you need to find, or solve for, a single* x *satisfying* $Q(x)$

such that $P(x)$ *holds*. In the specific case of Example 2.78, this becomes the common task of solving for two numbers x and y that satisfy a system of linear equations.

(At this point, do take a minute to convince yourself that this is logically different from the corresponding rule in Figure 2.18 for universal quantifiers. Proving $\exists_{Q(x)} P(x)$ amounts to showing $P(x)$ holds *for a single* x satisfying $Q(x)$, while proving $\forall_{Q(x)} P(x)$ amounts to showing $P(x)$ holds *for an arbitrary* x satisfying $Q(x)$.)

We now look at a more involved example involving both types of quantifiers:

Example 2.79. *Let us prove the following calculus statement:*

- *For any real number $\varepsilon > 0$, there exists a real number $\delta > 0$ such that for all real numbers x, we have that $|3x - 3| < \varepsilon$ whenever $|x - 1| < \delta$.*

Proof. Let $\varepsilon > 0$ be any (positive) real number. In addition, let x be any real number. Note that if $|x - 1| < \frac{\varepsilon}{3}$, then a short computation yields

$$\begin{aligned} |3x - 3| &= 3|x - 1| \\ &< 3 \cdot \tfrac{\varepsilon}{3} \\ &= \varepsilon. \end{aligned}$$

Thus, choosing $\delta = \frac{\varepsilon}{3}$, we see the desired statement indeed holds. □

The above proof is short and sweet, but there is a fair amount of logic to unpack here. Again, to see what one should do, one first expresses the statement more precisely as

$$\forall_{\text{real number } \varepsilon > 0} \exists_{\text{real number } \delta > 0} \forall_{\text{real number } x} ((|x - 1| < \delta) \Rightarrow (|3x - 3| < \varepsilon)). \tag{2.6}$$

Whew, three nested quantifiers! While this may look intimidating at first, we just need to deal with them one at a time in the same methodical manner as before.

We begin with the outermost universal quantifier. Indeed, the proof of (2.6) *begins by fixing an arbitrary real $\varepsilon > 0$, so that by Figure 2.18, we need to prove, for this ε,*

$$\exists_{\text{real number } \delta > 0} \forall_{\text{real number } x} ((|x - 1| < \delta) \Rightarrow (|3x - 3| < \varepsilon)). \tag{2.7}$$

Observe now that (2.7) *is headed by an existential quantifier. Thus, by Figure 2.19, we need to find a single, specific $\delta > 0$ such that the statement inside the "$\exists$" holds.*

Using a little bit of calculus wisdom (consult your calculus notes or lecturer!), we can discern that taking $\delta = \frac{\varepsilon}{3}$ will do the trick. Thus, to prove (2.7)*, we must show that*

$$\forall_{\text{real number } x} \left(\left(|x - 1| < \tfrac{\varepsilon}{3} \right) \Rightarrow (|3x - 3| < \varepsilon) \right). \tag{2.8}$$

Since (2.8) is headed by a universal quantifier, then this can be proved by fixing an arbitrary real number x, and then showing, for this x,

$$\left(|x-1| < \tfrac{\varepsilon}{3}\right) \Rightarrow (|3x-3| < \varepsilon). \tag{2.9}$$

Finally, for (2.9), we assume $|x-1| < \frac{\varepsilon}{3}$, and the main computation in the above proof then yields $|3x-3| < \varepsilon$, as desired. And, that is it, proof done!

While there is a lot of logic to break down in Example 2.79, all this can, in practice, be captured in a proof with relatively little writing. This is since most of these steps are very familiar to experienced mathematicians and usually need not be written out explicitly.

Moreover, if you were an especially astute observer, then you may have noticed that the statement which was proved in Example 2.79 simply says that

$$\lim_{x\to 1} 3x = 3,$$

once the limit is expanded into its formal δ-ε-definition. Thus, Example 2.79 provides, in gory detail, the mechanics of a classical δ-ε proof!

Students often find δ-ε proofs especially difficult, as it tends to be their first encounter with logical statements that are complex enough (3 mixed quantifiers!) to be intuitively confusing. However, if you have clear rules that allow you to pick apart all the components, then you know precisely what to do, and there is no reason to be afraid!

We conclude this discussion with the rule for removing an existential quantifier:

Assume:	$\exists_{Q(x)} P(x)$		
Conclude:	$Q(y)$	$P(y)$	*(any unused symbol y)*

FIGURE 2.20. Proof rule: existential elimination

The formal rule looks a bit tricky, but the intuition should be far more apparent. Here, the idea is that *since there exists x satisfying $Q(x)$ such that $P(x)$ holds, then we can use a new symbol y to denote this object that exists, so that $Q(y)$ and $P(y)$ both hold.*

In fact, we have already been secretly using the rule in Figure 2.20 in several proofs from earlier examples. (The logic is so intuitively natural, you may not even have noticed!) Below, we break down one instance where this was used:

Example 2.80. *Consider this familiar bit of logical reasoning:*

- *Let n be an even integer. Then, we can let m be the integer such that $n = 2m$.*

Here, we assumed n is an even integer, but what does this mean? n being even means that it can be written as 2 times something—more precisely,

$$\exists_{\text{integer } k}(n = 2k).$$

Intuitively, we can then simply let m denote this thing that exists—i.e. m is an integer such that $n = 2m$ (the red phrase in the proof). More formally, using the rule in Figure 2.20, we pick an unused symbol—m here—and we can conclude that the statements under and inside the "$\exists$" hold for m, that is, m is an integer and $n = 2m$.

Once again, there are analogous rules for *unrestricted* existential quantifiers:

- Assuming $P(y)$ holds for a single (unrestricted) y, we conclude $\exists_x P(x)$.
- Assuming $\exists_x P(x)$, we can conclude $P(y)$ for an unused symbol y.

Observe that these are analogues of the rules from Figures 2.19 and 2.20, except we now take $Q(x)$ to be any statement that is always true.

Note. *Again, in formal logic, the above rules for unrestricted existential quantifiers are considered the foundational rules. Figures 2.17 and 2.18 can then be derived from these foundational rules by interpreting $\exists_{Q(x)} P(x)$ as $\exists_x(Q(x) \text{ and } P(x))$.*

2.7.3. *Quantifiers and Negation.* Aside from Figures 2.17–2.20, there are also several proof rules involving quantifiers than can be derived from the basic rules. We now look at a few especially useful ones—namely, those pertaining to negations of quantifiers.

Recall that in the end of Section 2.4, we argued:

- The statements "not $\forall_{Q(x)} P(x)$" and "$\exists_{Q(x)}$ not $P(x)$" are logically equivalent.
- The statements "not $\exists_{Q(x)} P(x)$" and "$\forall_{Q(x)}$ not $P(x)$" are logically equivalent.

In fact, we can express these as rules of inference that can, with a bit of work, be derived from the basic quantifier rules in Figures 2.17–2.20 and from earlier rules:

Assume:	not $\forall_{Q(x)} P(x)$
Conclude:	$\exists_{Q(x)}(\text{not } P(x))$

Assume:	$\exists_{Q(x)}(\text{not } P(x))$
Conclude:	not $\forall_{Q(x)} P(x)$

Assume:	not $\exists_{Q(x)} P(x)$
Conclude:	$\forall_{Q(x)}(\text{not } P(x))$

Assume:	$\forall_{Q(x)}(\text{not } P(x))$
Conclude:	not $\exists_{Q(x)} P(x)$

FIGURE 2.21. Proof rules: quantifier negation

As always, the most important point is how these rules are used in mathematical proofs:

Example 2.81. *Consider the statement, "every prime number is odd", that is,*

$$\forall_{\textit{prime number } p}(p \textit{ is odd}).$$

Let us now show that this statement is false—in other words, let us prove

$$\text{not } \forall_{\textit{prime number } p}(p \textit{ is odd}). \tag{2.10}$$

Proving (2.10) *directly is tricky. However, from Figure 2.21, it suffices to prove instead*

$$\exists_{\textit{prime number } p}(p \textit{ is even}). \tag{2.11}$$

On the other hand, (2.11) *is super easy to prove:*

Proof of (2.11). We know that 2 is a prime number and 2 is even, so (2.11) follows immediately (formally, from the rule in Figure 2.19). □

Example 2.82. *Let us now prove the following statement:*

- *There is no largest natural number.*

This can be more formally expressed as

$$\text{not } \exists_{\textit{natural number } n} \forall_{\textit{natural number } m}(m \leq n). \tag{2.12}$$

(Note "$\forall_{\textit{natural number } m}(m \leq n)$" captures that n is the largest natural number.)

Proof. Let n be any natural number. Notice that $n + 1$ is a natural number, and that $n + 1 > n$. Thus, n cannot be the largest natural number. □

While the above proof is intuitive enough in its own right, let us unpack here the background logic. The strategy of the proof is to prove instead the statement

$$\forall_{\textit{natural number } n} \exists_{\textit{natural number } m}(m > n). \tag{2.13}$$

which, by the rules in Figure 2.21, is logically equivalent to the desired (2.12).

To prove (2.13), *we begin by dealing with the universal quantifier (via Figure 2.18)—we fix an arbitrary natural number n (in red), and we show, for this n,*

$$\exists_{\textit{natural number } m}(m > n). \tag{2.14}$$

To prove (2.14), *we simply need to find a single natural number m satisfying $m > n$. For this, the proof simply notes that taking $m = n + 1$ (in blue) accomplishes this task.*

Example 2.83. *We return to the statement in Example 2.82. Let us demonstrate a bit of resourcefulness by proving* (2.12) *using a different logical strategy.*

Proof. Suppose, for a contradiction, there is a largest natural number; let us call this number n_0. But then, $n_0 + 1$ is also a natural number, and moreover $n_0 + 1 > n_0$. This contradicts that n_0 is the largest natural number. □

The above argument now employs a proof by contradiction. The proof begins by assuming the negation of (2.12) *(highlighted in red):*

$$\exists_{\textit{natural number } n} \forall_{\textit{natural number } m} (m \leq n). \tag{2.15}$$

Then, using the rule from Figure 2.20, we can let n_0 *denote this largest natural number:*

$$n_0 \textit{ is a natural number,} \qquad \forall_{\textit{natural number } m} (m \leq n_0). \tag{2.16}$$

Now, we know that, of course, $n_0 + 1 > n_0$*. On the other hand, since* n_0 *is a natural number, the second part of* (2.16) *(and Figure 2.17) yields that* $n_0 + 1 \leq n_0$*. This is the contradiction referenced in the proof;* (2.12) *now follows from the rule in Figure 2.12.*

Note. *Since the rules in Figure 2.21 model equivalences, the note at the end of Section 2.6 applies—one can replace any instance of* $\text{not } \forall_{Q(x)} P(x)$ *and* $\text{not } \exists_{Q(x)} P(x)$ *within a larger statement by* $\exists_{Q(x)} (\text{not } P(x))$ *and* $\forall_{Q(x)} (\text{not } P(x))$*, respectively, and vice versa.*

Note. *For the readers who are curious and wish to play around more with deductive logic, below is an informal derivation of the bottom right rulein Figure 2.21.*

Proof. Assume $\forall_{Q(x)} (\text{not } P(x))$ holds; we aim to show $\text{not } \exists_{Q(x)} P(x)$ holds. Suppose, for a contradiction, that $\text{not not } \exists_{Q(x)} P(x)$ holds; this is the same as $\exists_{Q(x)} P(x)$ (by Figure 2.14). Now, let y be such that $Q(y)$ and $P(y)$ hold (Figure 2.20. However, from the assumption (and Figure 2.17, we also have $\text{not } P(y)$, leading to a contradiction. Thus, we conclude that $\text{not } \exists_{Q(x)} P(x)$ holds. □

2.8. **Final Notes.** In the past few sections, you have seen many examples of proofs. You have likely noticed, especially when comparing the proofs themselves to the surrounding commentary, that proof writing is not an exact science but an art of communication. In

particular, one does not list all the steps of the formal argument; the aim is to present the argument to the reader in a digestible way, so that the reader fill in any missing pieces.

You may wonder which details one should include in or leave out of a proof. There is, unfortunately, no single, neat answer to that question, since this greatly depends on the background of the audience. In general, one would include more details in introductory settings, such as NSF, than in more advanced settings (e.g. later undergraduate or post-graduate modules), where readers have considerably more shared experience. Thus, one must adapt the writing convention to the levels of the presumed readers.

It is ultimately important that you comprehend the underlying logic behind proofs, even if many of the gritty details are not written down in the end. This will critically aid your ability to read and write proofs, especially as the arguments become more complicated and begin to strain your intuitions. Hopefully, this brief survey of formal logic helped to build a more refined understanding of proof structures.

Finally, at this point, you may be anxious that even if you understand the proofs in the examples thus far, you are not still sure how to devise a proof yourself. There is absolutely no need to fret about this now, since we have not covered any mathematical material yet, thus there is little for you to actually prove. Once we begin discussing the maths (in the next chapter) and developing some shared background, then you will gradually see how everything works. Do keep in mind that mathematical reasoning and proof writing are acquired skills—like any worthwhile endeavour, they take time and effort to develop, and you should not feel like you are incapable if you do not pick it up quickly.

2.8.1. *On Learning Proofs.* In NSF and in these lecture notes, we are trying a slightly different approach to learning mathematical proofs. Traditionally, students learn to read and write proofs by being "thrown into the fire"—by encountering many proofs in modules. The successful students are those who are able to "read between the lines" and pick up all the unspoken rules for both the underlying logic and the writing style.

Here, we instead take an "extended detour" through semi-formal logic, with the intention of systematically discussing many of these unspoken rules and making them explicit. On the optimistic side, the hope is this helps to remove some of the common frustrations for beginners that come with not quite knowing what one can or cannot do in a proof. Once you start writing proofs in the next chapter, you can then refer back to our discussions here and discern whether your logic makes sense.

On the other hand, the downside of this approach is that there is a substantial amount of content in this detour, which is extra material you have to take in before properly jumping into proofs. Whether you consider this material to be helpful (if it allows you to

understand things more clearly) or unhelpful (if it is too much information!) depends on your mathematical background and preferred learning style.

If you are in the latter crowd and prefer the more "old-school" approach of just directly diving into proofs, then it is perfectly fine to do just that in the upcoming chapters. Once you gain more experience with proofs, you can then double back to the material here to build that more refined understanding of the underlying logic.

2.8.2. *(Bonus) Boolean and Deductive Logic, Revisited.* Recall that throughout this chapter, we have considered two different perspectives of formal logic:

(1) Boolean logic, where statements are considered either true or false.
(2) Deductive logic, where statements are used as steps in logical arguments.

A deeper question that we have not fully addressed (because it is well beyond the scope of this module) is *how these two perspectives are related.*

If you study more advanced formal logic in the future, then you would encounter two important concepts describing how (1) and (2) are related:

- Soundness: Any statement that can be proved (in (2)) is always true (in (1)).
- Completeness: Any statement that is always true (in (1)) can be proved (in (2)).

What exactly is meant by "can be proved" and "always true" is beyond this module, but hopefully the ideas make some sense. Roughly, *a formal theory is sound when one proves only true statements*, while *a theory is complete when every true statement can be proved.*

The abstract formal logic we have discussed covered here (more specifically, consisting of abstract statements, logical operations, and quantifiers) can be shown to be both sound and complete. (Again, how this is done is beyond the scope of this module.) In this sense, *the Boolean and deductive perspectives of logic are equivalent to each other.*

Now, what is far more interesting (and depressing) is that if we consider more complicated systems—for instance, formal logic plus mathematics—then the above is no longer true. In particular, while these systems remain sound, they fail to be complete. One landmark result is the Gödel incompleteness theorem (1931), which (very) roughly states that *for these complex systems, one can always find statements that cannot be proved true or false.* We will discuss one example of such a statement at the end of this module!

Thus, no matter what assumptions you place on your mathematical universe, there will be things that cannot be proved true or false—and hence are mathematically unknowable. Even if you add more assumptions to your universe, the incompleteness theorem tells you that, like a never-ending game of whack-a-mole, there will always be other statements that remain unprovable. (Sadly, we have to end this chapter on such a depressing note!)

3. Set Theory

Now that we have completed our quick survey of logic and proofs, we are finally prepared to start discussing the mathematical material of the module. The first topic on our agenda is set theory, which obviously refers to the study of sets.

Informally, sets are "collections of things", which you can, for now, roughly think of as a "bag" containing objects inside. (The precise characterization of sets is of course more subtle, but "bag o' stuff" suffices as a starting point.) For example:

- $\{1, 2, 4\}$ is the set (or "bag") containing the numbers 1, 2, 4.
- $\{\text{apple}, \text{orange}\}$ is the set (or "bag") containing "apple" and "orange".
- We can also consider infinite sets, such as the set of all natural or real numbers.

From our perspective, we can view *sets as the foundational objects in mathematics, from which all mathematical quantities are defined.* Indeed, we will think of any collections of quantities as sets, be it collections of numbers, functions, or anything else.

Since sets come before any other mathematical objects, it requires essentially no outside background to study this at the abstract level. Thus, if you feel that your knowledge in secondary-school mathematics is not quite up to par, then this chapter is a great opportunity to let that go and push the reset button. In practice, we will use set theory as a playground to practice the logic and proof skills that we built in the previous chapter.

Here, we will study set theory at a semi-formal level. This is for practical reasons, as this provides an efficient path toward being able to apply this material to other areas of mathematics without being caught up in extra technicalities. There is also a formal set theory, within which everything is very precisely defined, which is interesting in its own right. While we will not need this more formal treatment in practice, there are important reasons for developing such a formal set theory, as we shall discuss later.

Note. *In formal set theory, one takes the "sets as the foundational objects in mathematics" idea to the extreme! It is not just collections of quantities that are sets; rather, every object—including numbers, functions, collections, anything of interest—is a set!*

This may seem counterintuitive, but the philosophical motivation for doing this is to construct the theory with as few definitions and assumptions as possible. In this way, sets already encompass all the quantities of interest, and there is no need to develop separate (and largely redundant) theories to treat "quantities" and "collections".

For this module, however, the formalities of sets are not so important, and it is fine to take a more intuitive approach and simply think of sets as "collections".

3.1. **Descriptions of Sets.** In the semi-formal treatment of sets (often nicknamed "naive set theory"), one avoids the question of what exactly a set is. Instead, we focus on the practical question of *how one describes sets, as well as the elements within a set.*

First, sets are denoted using a wide variety of symbols—including Latin letters (x, y, A, B, etc.), Greek letters (α, β, etc.), familiar symbols with different fonts or highlighting ($\mathbb{R}$, $\mathcal{P}$, $\mathfrak{I}$, etc.), and many unfamiliar symbols. The kinds of symbols that are used usually depend on the context, often on some conventions set by the writer (e.g. lowercase letters for numbers, uppercase letters for sets). You will pick up on many such conventions from these lecture notes, as well as from other modules.

Next, one describes sets according to what objects are in them:

Definition 3.1. *A set is, informally, a collection of objects or quantities. Moreover:*

- *Given a set A, we write $x \in A$ to mean the statement "x is an element of A".*
- *We also write $x \notin A$ as an abbreviation for "$\text{not}(x \in A)$".*

Note. *In mathematics, a definition sets some new terminology in terms of concepts and quantities that we already know about. In practice, we can think of a definition as an additional assumption imposed upon our mathematical universe, which we can refer to and make use of in any statement or argument from there on.*

If we intuitively think of A in Definition 3.1 as a "bag", then $x \in A$ simply means that "x is inside the bag", while $x \notin A$ means that "x is not inside the bag".

One important point from Definition 3.1 is that since "$x \in A$" is a statement, in that it is either true or false, this means that *set membership is binary in nature.* More specifically, this means that either x is in A (i.e. $x \in A$), or x is not in A (i.e. $x \notin A$), and there is no middle ground or more detailed option. In particular:

- There is no concept of multiple copies of x being in A. For instance, the number "0" can be inside or outside the bag, but we cannot stuff two copies of "0" inside.
- There is no ordering of the elements of A, that is, there is no concept of one element of A coming before or after another. Therefore, all the objects inside the bag "A" are "jumbled together" in some undetermined manner.

(Later on, we will consider other types of objects that will take ordering or multiple copies into account, but it is important to keep in mind that sets do not do this!)

Next, let us put our logical knowledge to use and describe when two sets are the same:

Definition 3.2. *We say two sets A and B are equal, denoted $A = B$, iff they contain exactly the same elements. More formally, $A = B$ can be precisely defined as*

$$\forall_x (x \in A \Leftrightarrow x \in B).$$

Moreover, as usual, we will write $A \neq B$ to mean "not$(A = B)$".

As we shall see, sets and logic are quite closely connected. For instance, from Definition 3.2 above, we see that sets A and B having the same elements (that is, $A = B$) is more precisely characterized by $x \in A$ and $x \in B$ being logically equivalent statements (i.e. they must be both true or both false), for every possible x.

Below, we will describe various practical ways in which one can describe sets:

3.1.1. *Listing All Elements.* The most straightforward way to describe a set is to simply list every element that is in that set. The common notation for doing this, which we will use in these notes, is to write out the elements in between two braces "$\{\cdots\}$".

Example 3.3. *We write $\{1, 2, 4\}$ to denote the set containing (only) the numbers 1, 2, and 4. If we wish to be more formal, then we can describe this as*

$$\forall_x (x \in \{1, 2, 4\} \Leftrightarrow (x = 1 \text{ or } x = 2 \text{ or } x = 4)).$$

In particular, this means the following statements hold,

$$1 \in \{1, 2, 4\}, \qquad 2 \in \{1, 2, 4\}, \qquad 4 \in \{1, 2, 4\},$$

while any other quantity will not be an element of $\{1, 2, 4\}$.

Example 3.4. *In Example 3.3, we can replace 1, 2, 4 with other quantities, numerical or otherwise, and we can have lists with more or less than three elements. For instance,*

$$\{3, -2.5, \pi, \{-1, 1\}, \sin\}$$

denotes the set whose elements consists of the natural number 3, the rational number -2.5, the real number π, the set $\{-1, 1\}$, and the sine function. While this would be a rather peculiar set to consider, it is nonetheless perfectly valid.

Notice that nothing prevents a set from being an element of another set—for instance, $\{-1, 1\}$ is an element of the set from Example 3.4.

Note. *Due to the binary nature of set membership, the order in which the elements of a set are listed does not matter. Thus,* $\{1, 2, 4\}$ *is the same set as* $\{2, 4, 1\}$*. (You can also derive this from the formal description of* $\{1, 2, 4\}$ *in Example 3.3.)*

Similarly, since there is no concept of multiple copies of an element in a set, listing some quantity multiple times has no effect. For instance, from the formal description in Example 3.3, one can see that $\{1, 2, 4\}$ *is the same set as* $\{1, 1, 1, 2, 2, 4\}$*.*

3.1.2. *Establishing Patterns.* In many cases, while we may wish to list the elements of a set, it can be impractical (or we are too lazy) to write down every element. To get around this, if we can establish a clear pattern that the elements of a set follows, then we can write "…" in the place of the elements that satisfy this pattern.

Example 3.5. *The set of all natural numbers from* 1 *to* 100 *can be written as*

$$\{1, 2, \ldots, 100\}.$$

In particular, $2 \in \{1, 2, \ldots, 100\}$ *and* $70 \in \{1, 2, \ldots, 100\}$*, but* $102 \notin \{1, 2, \ldots, 100\}$*.*

*In the above, writing "*1*" and "*2*" establishes both that* 1 *is in this set, and it sets the pattern that the following element in the set is always one greater than the previous. The "…" indicates that this "increase by* 1*" pattern continues. Finally, the last element "*100*" shows that the pattern ends once we reach* 100*.*

How many elements of a set you would need to list before a "clear pattern is established" depends on context. For instance, in Example 3.5, if your reader has seen many different patterns, then you may want to list more elements to be extra clear, e.g.

$$\{1, 2, 3, \ldots, 100\}, \qquad \{1, 2, \ldots, 99, 100\}.$$

On the other hand, in some cases, even $\{1, \ldots, 100\}$ would be clear enough.

Example 3.6. *The set of all even integers from* -1000 *to* 2000 *can be written*

$$\{-1000, -998, \ldots, 1998, 2000\}.$$

The same "…" notation can also be used to describe infinite sets whose elements are given by some pattern that continues indefinitely:

Example 3.7. *The set of all natural numbers can be written as*

$$\{1, 2, 3, \dots\}.$$

Since there is no number after the "…", the pattern continues without ever stopping.

Example 3.8. *One can also establish multiple patterns in one set description. For instance, the set of all even integers can be written as*

$$\{\dots, -4, -2, 0, 2, 4, \dots\}.$$

You can also have different types of patterns in one set description, as long as you take care to be precise about what you are saying. For instance, the set of all even positive integers and odd negative integers can be written as

$$\{\dots, -5, -3, -1, 2, 4, 6, \dots\}.$$

3.1.3. *The Empty Set.* The simplest possible set is the one that contains no elements at all. We reserve an exclusive symbol for this special set:

Definition 3.9. *The empty set, denoted $\emptyset$, is the set that has no elements. Formally:*

$$\forall_x (x \notin \emptyset).$$

Note. *The empty set is also often called the null set, and it is often written as $\{\}$. However, in these notes, we will always remain with "empty set" and "$\emptyset$".*

3.1.4. *Common Sets of Numbers.* Next, the following notations for sets containing the different types of numbers are widely used throughout mathematics:

Definition 3.10. *We will adopt the following standard notations:*

- *Let $\mathbb{N}$ denote the set of all natural numbers:*
$$\mathbb{N} = \{1, 2, 3, \dots\}.$$
- *Let $\mathbb{Z}$ denote the set of all integers:*
$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$
- *Let $\mathbb{Q}$ denote the set of all rational numbers (i.e. the set of all fractions).*
- *Let $\mathbb{R}$ denote the set of all real numbers.*
- *Let $\mathbb{C}$ denote the set of all complex numbers.*

Recall the rational numbers consists of all the quotients $\frac{m}{n}$ of two integers m and n. We will give more precise descriptions of the real and complex numbers later on.

Note. *The strange font for the letters $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ in Definition 3.10 is called "blackboard bold". This came about from the need to write bold letters on a blackboard or a typewriter, and a practical way to do this was to add extra lines at strategic places.*

The notations from Definition 3.10 are useful for making the writing more concise. For instance, the statement "n is a natural number" is equivalent to $n \in \mathbb{N}$, while "x is a real number" is equivalent to $x \in \mathbb{R}$. Since set membership notation is so easy to write, this is the default way of writing that a quantity is a certain kind of number. In fact, we will adopt this style almost exclusively in the remainder of these lecture notes.

This notation is also extra convenient when writing out quantifiers. For instance, rather than writing $\forall_{\text{natural number } n}$ ("for all natural numbers n"), we can instead write the shorter $\forall_{n\in\mathbb{N}}$. The same shorthand can be applied for existential quantifiers as well. As a simple example, the statement "every integer is a difference of two natural numbers" could be expressed in formal logical notation as either of the following:

$$\forall_{a\in\mathbb{Z}}\exists_{m\in\mathbb{N}}\exists_{n\in\mathbb{N}}(a = m - n), \qquad \forall_{a\in\mathbb{Z}}\exists_{m,n\in\mathbb{N}}(a = m - n).$$

3.1.5. *Description via Logical Statements.* The most general way to describe a set is to give a logical statement that precisely characterizes which elements belong in the set:

Definition 3.11. *Given a statement $P(x)$ (depending on a variable x), we write*
$$\{x \mid P(x)\}$$

to denote the set of all x such that $P(x)$ holds.

Formally, the above can be characterised as

$$\forall_a(a \in \{x \mid P(x)\} \Leftrightarrow P(a)).$$

Let $A = \{x \mid P(x)\}$ be the set from Definition 3.11. The main idea is that the statement $P(a)$ serves as the gatekeeper for whether an object a is in A or not:

- If $P(a)$ holds, then $a \in A$.
- If $P(a)$ does not hold, then $a \notin A$.

Example 3.12. *The set of all positive real numbers can be described as*

$$\{x \mid x \in \mathbb{R} \text{ and } x > 0\},$$

that is, the set of all x such that $x \in \mathbb{R}$ (x is a real number) and $x > 0$ (x is positive).

Similarly, the set of all even natural numbers can be written as

$$\{n \mid n \in \mathbb{N} \text{ and } (n \textit{ is even})\}.$$

Now, you may already have noticed from Example 3.12 that "and" shows up quite a bit in various basic set descriptions. Indeed, most sets that you will come across will combine some basic condition (e.g. x is a real number) with some more specialised condition (e.g. x is positive, or y is even). As a result of this, we invent some additional shorthands to make the notation less cumbersome and more intuitive:

Definition 3.13. *Let $P(x)$ and $Q(x)$ be statements. We write*

$$\{Q(x) \mid P(x)\}$$

as a shorthand for the set $\{x \mid Q(x) \text{ and } P(x)\}$.

In plain English, the set $\{Q(x) \mid P(x)\}$ can be interpreted as "the set of all x satisfying $Q(x)$ such that $P(x)$ holds". While the description in quotes seems extra complicated in the abstract, it turns out to be more intuitive in most concrete settings.

Example 3.14. *Let us return to the two sets from Example 3.12:*

- *The set of all positive real numbers can be abbreviated as*

$$\{x \mid x \in \mathbb{R} \text{ and } x > 0\} = \{x \in \mathbb{R} \mid x > 0\}.$$

- *The set of all even natural numbers can be abbreviated as*

$$\{n \mid n \in \mathbb{N} \text{ and } (n \textit{ is even})\} = \{n \in \mathbb{N} \mid n \textit{ is even}\}.$$

Note that the shorthand notations better reflect how we intuitively think of these two sets. Indeed, in practice, we think of the former as the "set of all real numbers that are positive" and the "set of all natural numbers that are even".

Example 3.15. *The open interval* $(0,1)$ *(more specifically, all the real numbers between, but not including,* 0 *and* 1*), can be formulated as a set:*

$$(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

From Definition 3.13, we see that $x \in (0,1)$ *if and only if* $x \in \mathbb{R}$ *and* $0 < x < 1$.

We can offer an analogous set description of the closed interval $[0,1]$*:*

$$[0,1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}.$$

Similarly, $x \in [0,1]$ *if and only if* $x \in \mathbb{R}$ *and* $0 \leq x \leq 1$.

Note. *In the notations* $\{x|P(x)\}$ *and* $\{P(x) \mid Q(x)\}$*, the symbol* x *is once again a dummy variable, in the same sense as for variables showing up under quantifiers.*

In particular, $\{x|P(x)\}$ *and* $\{y|P(y)\}$ *both describe the same set. Furthermore, in this context, neither* x *nor* y *has any meaning outside of the set description.*

Example 3.16. *Recall from Definition 3.10 that the set* $\mathbb{Q}$ *of rational numbers consists of all the fractions, i.e. all possible quotients of integers. Using Definition 3.11, we can give a precise description of this set, at various levels of formality:*

$$\begin{aligned}\mathbb{Q} &= \left\{q \mid q = \tfrac{a}{b} \textit{ for some integer } a \textit{ and nonzero integer } b\right\} \\ &= \left\{q \mid \exists_{a,b\in\mathbb{Z}}(b \neq 0 \text{ and } q = \tfrac{a}{b})\right\}.\end{aligned}$$

Example 3.17. *A point to keep in mind is that adding new conditions in your set description does not necessarily mean that you are defining a novel set. For instance:*

- $\{n \in \mathbb{N} \mid n^2 \in \mathbb{N}\} = \mathbb{N}$, *since* $n^2 \in \mathbb{N}$ *is always satisfied when* $n \in \mathbb{N}$.
- $\{n \in \mathbb{N} \mid n^2 \notin \mathbb{N}\} = \emptyset$, *since* $n^2 \notin \mathbb{N}$ *is never satisfied when* $n \in \mathbb{N}$.

3.1.6. *Additional Shorthands.* There are many more commonly used shorthands to make describing sets easier. While it is not so realistic to list every popular shorthand that exists, here we demonstrate some useful ones via examples:

Example 3.18. *Consider the set of even natural numbers from Example 3.14:*

$$\{n \in \mathbb{N} \mid n \text{ is even}\}.$$

First, by expanding the definition of even numbers, we can expand the above as

$$\{n \in \mathbb{N} \mid \exists_{k \in \mathbb{N}} n = 2k\},$$

that is, the set of all natural numbers that can be written as twice a natural number.

One commonly used abbreviation for the above set is

$$\{2k \mid k \in \mathbb{N}\}.$$

Note this can be interpreted in plain English as "the set of all quantities of the form $2k$ *for some natural number* k*". Aside from being easier to write, the shorthand notation also more closely reflects how we would intuitively think of the set.*

Example 3.19. *To build further on Example 3.18:*

- *We can write the set of all even integers as*

$$\{a \mid \exists_{b \in \mathbb{Z}} a = 2b\} = \{2b \mid b \in \mathbb{Z}\}.$$

- *We can write the set of all odd integers as*

$$\{a \mid \exists_{b \in \mathbb{Z}} a = 2b + 1\} = \{2a + 1 \mid a \in \mathbb{Z}\}.$$

- *We can write the set of all odd natural numbers as*

$$\{n \mid \exists_{k \in \mathbb{N}} n = 2k - 1\} = \{2k - 1 \mid k \in \mathbb{N}\}.$$

On the other hand, note that $\{2k+1 \mid k \in \mathbb{N}\}$ does not describe the set of all odd natural numbers, since 1 is a odd natural number, but 1 does not belong in the above-mentioned set. Thus, you should make sure to give precise and accurate descriptions of your sets!

Example 3.20. *The set P of all squares of real numbers is given by:*

$$\begin{aligned} P &= \{x \in \mathbb{R} \mid \exists_{y \in \mathbb{R}} x = y^2\} \\ &= \{y^2 \mid y \in \mathbb{R}\}. \end{aligned}$$

Note that P can also be characterised as the set of all non-negative real numbers:

$$P = \{x \in \mathbb{R} \mid x \geq 0\}.$$

Example 3.21. *The set $\mathbb{Q}$ of rational numbers (see Example 3.16) can be described as*

$$\mathbb{Q} = \left\{ \tfrac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}.$$

As you can hopefully see, the shorthands from Examples 3.18-3.21 will make describing sets much easier. While the notation is largely self-explanatory and intuitive, for the sake of completeness, we include a precise general characterisation of this shorthand:

Definition 3.22. *Let Y represent a list of one or more variables, let $P(Y)$ be a statement depending on Y, and let $\alpha(Y)$ be an expression that depends on Y. (In particular, $\alpha(Y)$ is a quantity, not a logical statement as in Definition 3.13.) Then, we write*

$$\{\alpha(Y) \mid P(Y)\}$$

as shorthand for the set $\{x \mid \exists_Y (P(Y) \text{ and } x = \alpha(Y))\}$.

3.1.7. *Description in Words.* Finally, one can describe sets using plain English words, provided the writing is clear and unambiguous enough:

Example 3.23. *Consider the following English desription of sets:*

- *The set of integers.*
- *The set of positive rational numbers.*

- *The set of all real numbers x satisfying $-1 < x < 1$.*

Like in the previous chapter, when you encounter a plain English description of a set, you will need to be able to discern the precise meaning of those words.

3.2. **Subsets.** Now that you have seen many different ways to describe a set and its contents, our next aim to discuss relationships between sets. One of the simplest relations is whether one set A is entirely contained within another set B.

Definition 3.24. *Let A and B be arbitrary sets. We say that A is a subset of B, denoted $A \subseteq B$, iff every element of A is also an element of B.*

- *The statement $A \subseteq B$ can be more formally written as one of the following:*

$$\forall_{x \in A}(x \in B), \qquad \forall_x(x \in A \Rightarrow x \in B).$$

- *We can also write $B \supseteq A$ to mean the same as $A \subseteq B$.*

In addition, we say A is a proper subset of B, denoted $A \subset B$, iff $A \subseteq B$ and $A \neq B$.

Recall, from the discussions in Chapter 2, that the two formal statements in Definition 3.24 indeed have the same logical meaning and are equivalent.

Note. *To make life extra confusing, many texts write $A \subset B$ and $A \subsetneq B$ rather than $A \subseteq B$ and $A \subset B$, respectively. (Some of your other modules may even do this!) For this module, we will always use the notations specified in Definition 3.24. In general, though, it is important that you are aware of the conventions being used.*

Example 3.25. *The following subset relations hold:*

- $\{1, 3\} \subseteq \{1, 2, 3\}$. *(This is because every element of the set $\{1, 3\}$—namely, 1 and 3—is also an element of the set $\{1, 2, 3\}$.)*
- $\mathbb{N} \subseteq \mathbb{Z}$. *(This is because every element of $\mathbb{N}$—i.e. every natural number—is a positive integer, and hence is an integer.)*
- $\{x \in \mathbb{Z} \mid x \text{ is even}\} \subseteq \mathbb{Z}$. *(This is because every even integer is an integer.)*

Also, note that all the above relations still hold with "$\subseteq$" replaced by "$\subset$",

$$\{1, 3\} \subset \{1, 2, 3\}, \qquad \mathbb{N} \subset \mathbb{Z}, \qquad \{x \in \mathbb{Z} \mid x \text{ is even}\} \subseteq \mathbb{Z},$$

since none of these pairs of sets are equal to each other.

Next, as warm up, let us bring proofs back in the game. For this, the formal description in Definition 3.24 is quite clarifying. Indeed, given sets A and B, the precise meaning of $A \subseteq B$ can be written as $\forall_{x \in A} x \in B$. Thus, the rule from Figure 2.18 tells us that *to prove* $A \subseteq B$, *we should fix an arbitrary* $x \in A$ *and proceed to show that* $x \in B$ *as well.*

Example 3.26. *Returning to Example 3.25, let us now prove that* $\{1,3\} \subseteq \{1,2,3\}$.

Proof. Fix an arbitrary $x \in \{1,3\}$. This simply means (see Example 3.3) that either $x = 1$ or $x = 3$. Splitting into cases:

- If $x = 1$, then clearly $x \in \{1,2,3\}$ as well, by definition.
- Similarly, if $x = 3$, then again $x \in \{1,2,3\}$.

Thus, we conclude that $x \in \{1,2,3\}$ always holds, completing the proof. □

Now, the above is a higher level of detail than you will be asked to do in this module. However, it is useful to show this once, in order to connect the intuition behind the statement $\{1,3\} \subseteq \{1,2,3\}$ *with a couple of the proof rules.*

3.2.1. *General Properties.* As further practice with logic and abstraction, let us now state and prove some (very) basic general properties involving sets and subsets:

Proposition 3.27. *Let* A *be a set. Then:*

(1) $A \subseteq A$.
(2) $\emptyset \subseteq A$.

Note. *To clarify, theorem (such as Theorem 1.2 in the introduction) is the fancy term for a mathematical fact. When we designate a statement as "theorem", we are staking a formal claim that it is true, and that we will back up this claim with a proof.*

Here, a proposition is functionally the same as a theorem (i.e. a mathematical fact). However, we use "proposition" instead of "theorem" for facts that are minor and less important. Of course, what is considered "less important" is subjective and depends on context, so there is no hard rule on what qualifies as "theorem" or "proposition".

Proof of Proposition 3.27. (1) Given any $x \in A$, this immediately implies $x \in A$ itself. Therefore, by Definition 3.24, it follows that $A \subseteq A$ holds, as desired.

(2) Fix an arbitrary $x \in \emptyset$. Since $x \in \emptyset$ can never hold, then $x \in A$ is vacuously true. As a result, $\emptyset \subseteq A$ holds by Definition 3.24. □

Note the proof of part (1) in Proposition 3.27 has the same structure as Example 3.26—we fix an arbitrary $x \in A$, and we then show $x \in A$. However, since $x \in A$ trivially implies itself, then there is really nothing that needs to be done here!

The proof of part (2) deserves more comment, as the writing in prose differs a bit from what was described in the proof rules. The idea, from Boolean logic, is that an implication $P \Rightarrow Q$ is always true whenever P is false—such an implication is said to be vacuously true. As a result, since $x \in \emptyset$ is always false (since the empty set $\emptyset$ has no elements), then we can always vacuously conclude $x \in A$ from this assumption.

Below, we give an alternate proof of part (2) that is perhaps a bit more complicated structurally but is more in line with the proof rules:

Alternate proof of Proposition 3.27(2). Assume, for a contradiction, that $\emptyset \subseteq A$ does not hold. Then, there exists $x \in \emptyset$ such that $x \notin A$. However, this contradicts that $x \notin \emptyset$ (by definition), hence it immediately follows that $\emptyset \subseteq A$. □

The above is a standard contradiction proof. One point worth further comment is that the proof begins by assuming the negation of $\emptyset \subseteq A$, that is, the negation of $\forall_{x \in \emptyset} x \in A$. From the rules in Figure 2.21, we see that this negation is equivalent to $\exists_{x \in \emptyset} x \notin A$, which is the statement highlighted in red in the proof. Applying Figure 2.20 (i.e. letting x be this element that exists) leads immediately to the contradiction.

The next proposition connects the subset relation with set equality:

Proposition 3.28. *Let A, B be sets. Then, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.*

Proof of Proposition 3.28. Suppose first that $A = B$.

- Given any $x \in A$, since A and B contain the same elements, it follows that $x \in B$ as well. As a result, we conclude $A \subseteq B$.

- Similarly, given any $x \in B$, it follows that $x \in A$. Thus, $B \subseteq A$.

Combining both parts, we obtain, as desired, both $A \subseteq B$ and $B \subseteq A$.

Conversely, suppose both $A \subseteq B$ and $B \subseteq A$. Now, given any x:

- If $x \in A$, then since $A \subseteq B$, it follows that $x \in B$.
- If $x \in B$, then since $B \subseteq A$, it follows that $x \in A$.

Therefore, from the above bullet points, we conclude that $x \in A$ if and only if $x \in B$. Recalling Definition 3.2, we have $A = B$, as desired. □

First, note that Proposition 3.28 gives a template for proving that two sets are equal. Indeed, to show that $A = B$, we must prove two subset relations—$A \subseteq B$ and $B \subseteq A$.

Regarding the proof of Proposition 3.28, since this is an "if and only if" statement (i.e. an equivalence), then by the rule in Figure 2.9, we must show the following:

- If $A = B$, then $A \subseteq B$ and $B \subseteq A$. (This is the first part of the proof.)
- If $A \subseteq B$ and $B \subseteq A$, then $A = B$. (This is the second part of the proof.)

That the above implications hold follows from the definitions of set equality and subsets.

Lastly, note that this equivalence between the statements

$$A = B, \qquad (A \subseteq B) \text{ and } (B \subseteq A)$$

is closely connected to the equivalence between the logical statements

$$P \Leftrightarrow Q, \qquad (P \Rightarrow Q) \text{ and } (Q \Rightarrow P).$$

Indeed, this is simply because set equality is formally defined via an equivalence "$\Leftrightarrow$" (see Definition 3.2), while subsets are formally defined via "$\Rightarrow$" (see Definition 3.24).

3.2.2. *Power Sets.* Before moving on to the next topic, there is one more construction involving subsets that will be useful later in the module:

Definition 3.29. *Let A be a set.*

- *The power set of A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.*
- *Formally, the power set can be expressed as*

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

If you have not seen this before, then the wording here might make your head spin a bit. However, this all makes much more sense after a few basic examples:

Example 3.30. *Consider the set*

$$A = \{1, 2, 3\}.$$

By Definition 3.24, the subsets of A *are precisely those sets* B *for which every element of* B *is in* A*. Since* A *is so simple, one can directly list all the subsets of* A*:*

$$\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}.$$

Then, the power set of A *is just the set containing all the above subsets:*

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Example 3.31. *The set* $E = \{2k \mid k \in \mathbb{N}\}$ *of all even natural numbers is a subset of* $\mathbb{N}$*. As a result, by Definition 3.29, we have that* $E \in \mathcal{P}(\mathbb{N})$*.*

Finally, to see how power sets might come up naturally in mathematics, we recall one example from outside NSF that you will likely find familiar:

Example 3.32. *In probability, a sample space* S *is a set that models all the possible outcomes of some experiment. In the simplest case when* S *is finite:*

- *Any subset of the sample space is called an event.*
- *Thus, the set of all events is precisely the power set* $\mathcal{P}(S)$ *of* S*.*

3.3. **Set Operations.** Our next objective is to define some commonly used set operations, which one can think of as useful ways to construct new sets from existing sets. We begin by giving the precise definitions of these operations:

Definition 3.33. *Let* A *and* B *be any sets:*

- *The union of* A *and* B*, denoted* $A \cup B$*, is defined to be the set*

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

- *The intersection of* A *and* B*, denoted* $A \cap B$*, is defined to be the set*

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

- *The (set) difference of* A *and* B*, denoted* $A \setminus B$*, is defined to be*

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

Intuitively, if we think of A and B as bags with items inside, then:

- $A \cup B$ is the larger bag made by combining all the contents of A and B together.
- $A \cap B$ is the smaller bag made by keeping only the items that are in both A and B.
- $A \setminus B$ is the bag made by taking A and throwing out any items that are in B.

The following concrete examples should make all this much clearer:

Example 3.34. *Consider the following sets:*

$$A = \{1, 2\}, \qquad B = \{2, 3\}.$$

Then, the set operations from Definition 3.33 applied to A *and* B *give:*

- $A \cup B = \{1, 2, 3\}$*, which contains all the elements in* A *or in* B*.*
- $A \cap B = \{2\}$*, which contains all the elements in both* A *and* B*.*
- $A \setminus B = \{1\}$*, which contains all the elements in* A *but not in* B*.*

Example 3.35. *Let* A *and* B *denote the following intervals:*

$$A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}, \qquad B = \{x \in \mathbb{R} \mid 0 < x < 2\}.$$

(Another common way to write the above is $A = [-1, 1]$ *and* $B = (0, 2)$*.)*

The set operations from Definition 3.33 applied to A *and* B *give:*

- $A \cup B = \{x \in \mathbb{R} \mid -1 \leq x < 2\}$*.*
- $A \cap B = \{x \in \mathbb{R} \mid 0 < x \leq 1\}$*.*
- $A \setminus B = \{x \in \mathbb{R} \mid -1 \leq x \leq 0\}$*.*

If you are not sure about any of these, however, then you can dig into the definitions.

For instance, by Definitions 3.13 and 3.33, the set $A \cup B$ *consists of all the real numbers* x *satisfying* $-1 \leq x \leq 1$ *or* $0 < x < 2$*. The numbers for which one of the two conditions above hold are precisely those* x *satisfying* $-1 \leq x < 2$*.*

A similar bit of reasoning shows that $A \cap B$ *consists of all real numbers* x *satisfying both* $-1 \leq x \leq 1$ *and* $0 < x < 2$*. The numbers for which both of the above conditions hold are precisely those* x *that satisfy* $0 < x \leq 1$*.*

Finally, $A \setminus B$ consists of all real numbers x such that $-1 \leq x \leq 1$ holds and such that $0 < x < 2$ does not hold. Now, the latter condition can be rewritten as $x \leq 0$ or $x \geq 2$. You can then quickly convince yourself that the numbers x satisfying both

$$-1 \leq x \leq 1, \qquad x \leq 0 \text{ or } x \geq 2,$$

are precisely those x satisfying $-1 \leq x \leq 0$. (You can draw a picture to help you.)

Example 3.36. *Consider the following sets:*

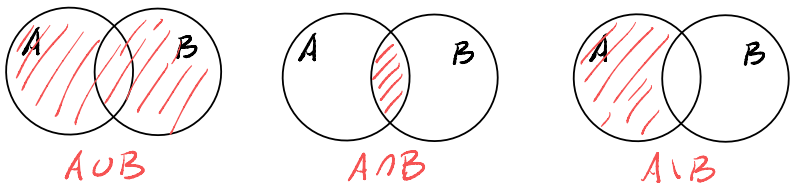
$$A = \{x \in \mathbb{R} \mid 0 \leq x \leq 2\}, \qquad B = \{1, 2, 3\}.$$

The set operations from Definition 3.33 applied to A and B give:

- $A \cup B = \{x \in \mathbb{R} \mid 0 \leq x \leq 2 \text{ or } x = 3\}$.
- $A \cap B = \{1, 2\}$.
- $A \setminus B = \{x \in \mathbb{R} \mid 0 \leq x < 1 \text{ or } 1 < x < 2\}$.
- $B \setminus A = \{3\}$.

Again, if visualisations help, then you can draw a number line to help you.

One handy way to visualise set operations in general is through Venn diagrams, which you may have already seen elsewhere before. The Venn diagram illustrations of unions, intersections, and differences are given in the drawing below:



Note. *Keep in mind that while Venn diagrams can serve as useful visual aids, they do not count as proofs! (A graphic by itself is not a logical argument.) Thus, if a problem asks for a proof, then give a logical argument, not a drawing!*

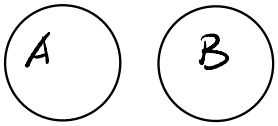
We also remark that the set operations in Definition 3.33 are quite similar to the logical operations discussed in the previous chapter. In particular, unions are analogous to disjunctions (or) in logic, while intersections are analogous to conjunctions (and).

Note. *Be aware that set operations are applied exclusively to sets, while logical operations are applied exclusively to logical statements. Do make sure you do not mix them up! For example, it does not make sense to apply logical operations to sets—if* A *and* B *are sets, then neither "*A and B*" nor "*A or B*" makes any sense.*

3.3.1. *Disjoint Sets.* The following terminology is commonly used:

Definition 3.37. *Sets* A *and* B *are called disjoint iff* $A \cap B = \emptyset$.

Intuitively, *two sets are disjoint iff there are no common elements between them.* The very simple Venn diagram for two disjoint sets is as follows:



There is not much more to be said about this, besides one example for good measure:

Example 3.38. *Consider the following sets:*

$$A = \{1, 2\}, \qquad B = \{2, 3\}, \qquad C = \{3, 4\}.$$

- A *and* B *are not disjoint, since* $A \cap B = \{2\}$ *is not empty.*
- A *and* C *are disjoint, since* $A \cap C = \emptyset$ *has no elements.*

3.3.2. *General Properties.* We now state and prove some basic properties involving unions, intersections, and set differences. The proofs here tend to be relatively simple, with the key mathematical insights given usually by just one or two proof rules. Thus, the following serve as good practice to focus on the structures of the arguments.

Our first family of properties relates our set operations with subsets:

Proposition 3.39. *Let* A *and* B *be any sets. Then:*

(1) $A \subseteq A \cup B$.
(2) $A \cap B \subseteq A$.
(3) $A \setminus B \subseteq A$.

Proof of Proposition 3.39. (1) Fix any $x \in A$. Then, clearly $x \in A$ or $x \in B$ holds, so $x \in A \cup B$ by Definition 3.33. Thus, by Definition 3.24, we conclude $A \subseteq A \cup B$.

(2) Let $x \in A \cap B$. Then, $x \in A$ and $x \in B$, which trivially implies $x \in A$.

(3) Let $x \in A \setminus B$. Then, $x \in A$ and $x \notin B$, which trivially implies $x \in A$. □

Notice that the above proofs have the same structure as those for Proposition 3.27. For (1), we assumed $x \in A$, and we proceeded to show $x \in A \cup B$. That this holds is an immediate consequence of the proof rule from Figure 2.7.

The proofs of (2) and (3) are similar, except that the key mathematical step now comes from the rule in Figure 2.6. Here, we also omitted some of the structural bits of the proof, as these would be clear to any reader who has some experience with subset proofs.

Note. *In general, as we progress further into the notes, we will gradually reduce the level of detail provided for more basic elements, since it is presumed that you will be more familiar with these parts and will need less guidance there.*

Next, we consider some common algebraic properties of unions and intersections. The first properties on this list are the commutative laws:

Proposition 3.40. *Let A and B be sets. Then:*

(1) $A \cup B = B \cup A$.
(2) $A \cap B = B \cap A$.

Proof of Proposition 3.40(1). First, suppose that $x \in A \cup B$. Then, by Definition 3.33, we have either $x \in A$ or $x \in B$. Now, the above is logically equivalent to $x \in B$ or $x \in A$, so by Definition 3.33, we conclude that $x \in B \cup A$.

Conversely, suppose $x \in B \cup A$. By Definition 3.33, we have $x \in B$ or $x \in A$, which we know is equivalent to $x \in A$ or $x \in B$. As a result, $x \in A \cup B$. □

Now, the above proof follows the usual template for proving set equality—we prove $A \cup B$ is a subset of $B \cup A$ (first paragraph), and we then show $B \cup A$ is a subset of $A \cup B$ (second paragraph). That is all fine, but the process is a bit painstaking, and in a rather

repetitive way. In particular, the steps in the second paragraph are precisely the steps in the first paragraph in reverse! This is no accident; the reason is that every step of the proof is actually a logical equivalence, so the implications always go in both directions.

Since the entire proof is just a sequence logical equivalences, here we will allow for an abbreviated writing style that captures this and removes most of the repetition:

Alternate proof of Proposition 3.40(1).

$$\begin{aligned} x \in A \cup B &\Leftrightarrow x \in A \text{ or } x \in B && \text{(definition of } \cup) \\ &\Leftrightarrow x \in B \text{ or } x \in A && \text{(commutative law of or)} \\ &\Leftrightarrow x \in B \cup A && \text{(definition of } \cup) \end{aligned}$$

The above immediately implies that $A \cup B = B \cup A$. □

Note that this alternate proof, written mostly in symbols, consists of a chain of equivalences, with the justification for each "$\Leftrightarrow$" given to its right. The understanding is that *each step in this chain is a logical equivalence and hence is reversible.* Thus, the *logical reasoning can proceed both from top to bottom and from bottom to top*, capturing both paragraphs of the earlier proof and removing the need to do everything twice.

Of course, *this writing style only works when every step of the proof is an equivalence*, so make sure you only use this in situations where it is applicable.

Part (2) of Proposition 3.40 can be proved analogously:

Proof of Proposition 3.40(2).

$$\begin{aligned} x \in A \cap B &\Leftrightarrow x \in A \text{ and } x \in B && \text{(definition of } \cap) \\ &\Leftrightarrow x \in B \text{ and } x \in A && \text{(commutative law of and)} \\ &\Leftrightarrow x \in B \cap A && \text{(definition of } \cap) \end{aligned}$$

□

Note. *We warn that the above is not really a standard style of proof writing. (In particular, avoid using it in your other modules!) However, since a number of basic properties in set theory can be proved this way, we use it here to both shorten the writing and make the logic more apparent. More generally, however, very few proofs consist only of logical equivalences, so the uses of this writing style are rather limited.*

Next, the following associative laws can be similarly proved:

Proposition 3.41. *Let A, B, C be sets. Then:*

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

Proof of Proposition 3.41. (1) The proof follows a sequence of equivalences:

$$\begin{aligned}
x \in (A \cup B) \cup C &\Leftrightarrow (x \in A \cup B) \text{ or } x \in C && \text{(definition of } \cup) \\
&\Leftrightarrow (x \in A \text{ or } x \in B) \text{ or } x \in C && \text{(definition of } \cup) \\
&\Leftrightarrow x \in A \text{ or } (x \in B \text{ or } x \in C) && \text{(associative law)} \\
&\Leftrightarrow x \in A \text{ or } (x \in B \cup C) && \text{(definition of } \cup) \\
&\Leftrightarrow x \in A \cup (B \cup C) && \text{(definition of } \cup)
\end{aligned}$$

(2) The proof is analogous, so we omit some of the more obvious steps:

$$\begin{aligned}
x \in (A \cap B) \cap C &\Leftrightarrow (x \in A \text{ and } x \in B) \text{ and } x \in C && \text{(definition of } \cap) \\
&\Leftrightarrow x \in A \text{ and } (x \in B \text{ and } x \in C) && \text{(associative law)} \\
&\Leftrightarrow x \in A \cap (B \cap C) && \text{(definition of } \cap)
\end{aligned}$$

□

The distributive laws relating unions and intersections can also be similarly proved:

Proposition 3.42. *Let A, B, C be sets. Then:*

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

Proof of Proposition 3.42. (1) The proof follows a sequence of equivalences:

$$\begin{aligned}
x \in A \cup (B \cap C) &\Leftrightarrow x \in A \text{ or } (x \in B \text{ and } x \in C) && \text{(definitions of } \cup, \cap) \\
&\Leftrightarrow (x \in A \text{ or } x \in B) \text{ and } (x \in A \text{ or } x \in C) && \text{(distributive law)} \\
&\Leftrightarrow x \in (A \cup B) \cap (A \cup C) && \text{(definitions of } \cup, \cap)
\end{aligned}$$

(2) The proof is analogous to part (1), with the same justifications:

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

Observe Propositions 3.40, 3.41, and 3.42 can be viewed as analogues of the commutative, associative, and distributive laws for "or" and "and" (see Figure 2.1). Finally, the following properties can be viewed as the analogues of DeMorgan's laws; however, we omit the proofs and leave them as practice problems (i.e. do it yourself!).

Proposition 3.43. *Let A, B, C be sets. Then:*

(1) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.
(2) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

3.4. **Final Notes.** We mentioned, near the start of this chapter, that the semi-formal approach to sets that we have taken here is called naive set theory. Of course, as a critical thinker, you should immediately ask the following question:

Question 3.44. *Why is "naive set theory" naive?*

While there are a number of issues with "naive set theory" (the details go well beyond this module), one fundamental answer to Question 3.44 is that *in naive set theory, we are allowed to create a set out of anything*. For instance, we can construct a set $\{x \mid P(x)\}$ out of *any possible statement* $P(x)$. This is too much power to give to a mathematician!

Question 3.45. *Ahem, what's wrong with too much power?!*

The problem here is this power is enough to easily destroy all of mathematics! In fact, one could, in just a few minutes, and without any mathematical background beyond what we have already studied, break all of maths with a giant contradiction!

In the following, we discuss two ways in which anyone with a "naive" approach can completely wreck our mathematical universe. This will in particular highlight the fundamental need for a formal and precise set theory beyond what was covered here.

3.4.1. *(Bonus) Russell's Paradox.* The first (and rather famous) paradox we will look at is named after British mathematician Bertrand Russell (1872–1970). Its statement is disarmingly simple, yet brutal in its total destructive power:

- *Consider the set* $R = \{x \mid x \notin x\}$.

In naive set theory, R is a perfectly acceptable set, since "$x \notin x$" is a valid statement.

All seems harmless so far. However, let us consider the following simple question:

- *Is* $R \in R$*?*

The answer to this should just be "yes" or "no", depending on whether R satisfies the logical condition that defines R. However, let us take a closer look at this:

- If $R \in R$, then the definition of R tells us that $R \notin R$—this is a contradiction!
- This must mean $R \notin R$, right? However, if $R \notin R$, then R must fail the condition defining R; in other words, $R \in R$. This is also a contradiction!

Therefore, we have a contradiction in all cases—regardless of whether $R \in R$ or $R \notin R$. This very simple contradiction is known as Russell's paradox.

In other words, all of mathematics is a big contradiction, and our entire mathematical universe falls apart thanks to one innocent little definition. Ouch!

While you could gloat about destroying maths, the inconvenient fact is that you just committed yourself for the next several years to studying for a mathematics degree. Thus, from your point of view, the more personally beneficial question to ask is:

Question 3.46. *How do we save mathematics?*

The short answer is that *we need a formal set theory*, where everything is made precise. More specifically, the problem is again that we gave ourselves too much power, as we allowed every logical statement to define a valid set. A formal set theory provides various *axioms*, or rules, *that establish precisely what is allowed to be a set.*

Note. *To clarify, an axiom is a statement that is assumed true without proof. Axioms usually serve as the foundation of a formal theory (e.g. set theory, probability), and they tend to be based on intuitions that are considered "self-evident".*

Functionally, axioms act like definitions, in that both introduce new assumptions into the mathematical universe. In practice, one uses "definition" to set new terminology based on existing ones, while "axiom" is just a statement that is assumed true.

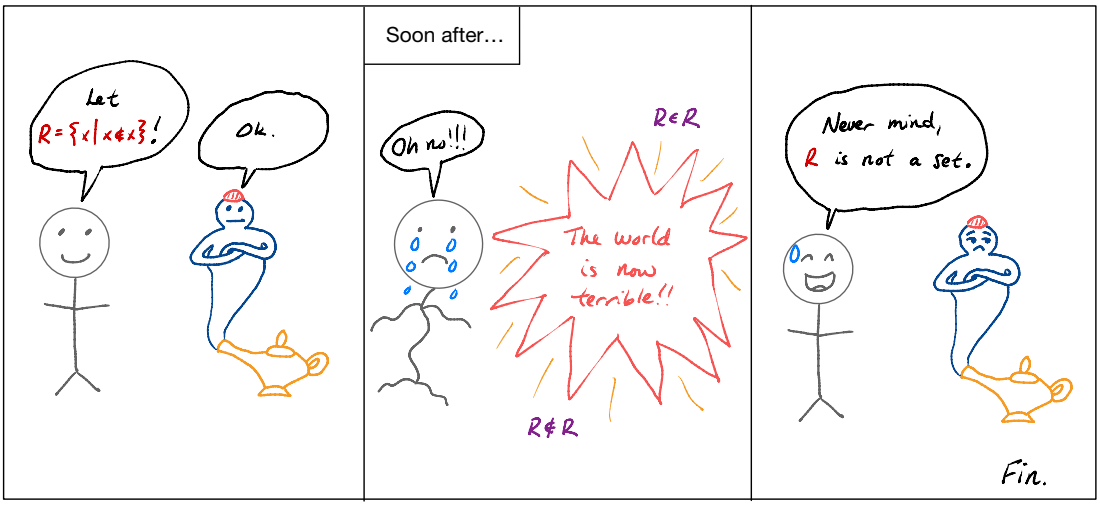
There are many different ways to craft a viable formal set theory that saves mathematics. (Two of the most common theories are due to Zermelo–Fraenkel and Von Neumann–Bernays–Gödel.) In particular, all the formal set theories limit which statements $P(x)$ are allowed to define a set $\{x \mid P(x)\}$. Consequently, Russell's paradox is resolved by showing, through the formal set theory axioms, that R is not a set to begin with. Crisis averted!

Theorem 3.47. *The following hold:*

(1) *Russell's paradox: R is not a set.*
(2) *There is no "set of everything" that contains every object x.*

Part (2) of Theorem 3.47 gives another consequence of formal set theory—in contrast to the empty set (which is a set), there cannot be a set of all things. In other words, if you are "naive" in your approach to sets and allow for a "set of all objects", then, similar to Russell's paradox, things will not end well for you.

Note. *There have been many reformulations of Russell's paradox over the years. One well-known example is the barber paradox, which is the statement "the barber shaves (and only shaves) every man who does not shave himself". You can then ask whether the barber shaves himself—can you find the paradox?*



3.4.2. *(Bonus) Berry's Paradox.* We now discuss another paradox (attributed to librarian G.G. Berry, 1867–1928) that is quite different in nature, but is similarly devastating.

The statement looks simple and innocent enough:

- *Let* B *be the set of natural numbers that can be described in fifty or less English words.*

Now, there are only finitely many English words, so B must contain a finite (albeit very large) number of elements. Thus, there must be a largest number in B, which we call b_0.

However, $b_0 + 1$ can be described, in less than fifty English words, as "one more than the largest element of B". Thus, $b_0 + 1 \in \mathsf{B}$, contradicting that b_0 is the largest element of B! Once again, mathematics is imminently falling apart, all thanks to a one-paragraph contradiction, which is often called the Berry paradox.

To protect the value of your future maths degree, you should ask:

Question 3.48. *How do we save mathematics (again)?*

Here, the problem, as you may have guessed, comes from the plain English phrase "can be described in fifty or less English words". Phrases in English can be ambiguous, and this one is a serious offender, as there is no precise meaning of what it means for a number to be described using English words. Once we allow a bit of self-referencing, in "one greater than the largest element of B", then all hell breaks loose.

Similar to Russell's paradox, the fix is that we need both formal logic and formal mathematical language, as informal descriptions in English can get us in trouble. In particular, we need to restrict what is allowed to be a statement. For instance, in common versions of formal logic, statements must be built exclusively from abstract symbols, logical operations (not, and, or, $\Rightarrow$, $\Leftrightarrow$) and quantifiers ($\forall$, $\exists$). This eliminates the use of ambiguous English phrases, so that we could not define this dangerous set B in the first place.

4. Number Systems

In the previous chapter, we studied sets as the foundational building blocks of mathematics. To really make use of such a theory, we will need to apply it to more mathematically interesting quantities. Most of our concrete examples of sets thus far have involved various types of numbers and some of their simplest properties, things that we can reference without needing to develop any background. But, if we wish to further explore our theory, then we will need to play with numbers in a deeper manner.

The purpose of this chapter is to take an extended safari through the various number systems you know and love, from the natural numbers all the way through the complex numbers. While you are likely already quite familiar with most of these numbers, the aim of the following discussion is to introduce something new and interesting about each one. By the end of this chapter, your expanded knowledge of numbers will provide you a much larger forum in which you can practice your set theory and proof skills.

4.1. **Preliminary Properties.** Similar to the preceding chapter, as we are taking a rather informal approach to mathematical foundations, here we will assume that all the number systems that you have learned about exist as you know them, and they have the usual properties. (In essence, we take these as axioms in our universe.) Thus, you can recall and make use of everything you have learned about these numbers in your previous education.

To be more explicit, let us recall the various sets of numbers and their relations:

$$\underbrace{\mathbb{N}}_{\text{natural numbers}} \subseteq \underbrace{\mathbb{Z}}_{\text{integers}} \subseteq \underbrace{\mathbb{Q}}_{\text{rational numbers}} \subseteq \underbrace{\mathbb{R}}_{\text{real numbers}} \subseteq \underbrace{\mathbb{C}}_{\text{complex numbers}}.$$

Recall Definition 3.10 for the above notations. In particular:

- $\mathbb{N} \subseteq \mathbb{Z}$, since every natural number is a positive integer.
- $\mathbb{Z} \subseteq \mathbb{Q}$, since every integer a is also a fraction $\frac{a}{1}$.
- $\mathbb{Q} \subseteq \mathbb{R}$, since every rational number "lies on the real number line".
- $\mathbb{R} \subseteq \mathbb{C}$, since every real number x is also a complex number $x + i\,0$.

(There is no need to worry if you have not seen complex numbers before. We will cover complex numbers in detail at the end of this chapter.)

Let us now get all the boring material out of the way—we recall the various algebraic properties of the natural numbers, integers, rational numbers, and real numbers that you have learned before, and that we usually take for granted in our everyday use. For practical purposes, you can think of these statements as axioms—assumptions that you can make use of throughout the remainder of this module. (On the other hand, we defer discussing properties of complex numbers until the end of this chapter.)

To make this section slightly more spicy (and less boring) than it otherwise would be, let us state all these properties using formal logical language.

The first property, the closure of addition and multiplication, states that if you add or multiply two of the same kind of number, then the result is also that same kind of number:

Proposition 4.1. *The following statements hold:*

$$\forall_{m,n\in\mathbb{N}}(m+n\in\mathbb{N}), \qquad \forall_{m,n\in\mathbb{N}}(mn\in\mathbb{N}),$$
$$\forall_{a,b\in\mathbb{Z}}(a+b\in\mathbb{Z}), \qquad \forall_{a,b\in\mathbb{Z}}(ab\in\mathbb{Z}),$$
$$\forall_{p,q\in\mathbb{Q}}(p+q\in\mathbb{Q}), \qquad \forall_{p,q\in\mathbb{Q}}(pq\in\mathbb{Q}),$$
$$\forall_{x,y\in\mathbb{R}}(x+y\in\mathbb{R}), \qquad \forall_{x,y\in\mathbb{R}}(xy\in\mathbb{R}).$$

Now, in the upcoming propositions, we will only state the properties for real numbers. However, since every natural number, integer, and rational number is also a real number, these statements automatically cover all four number systems.

Next, recall that both addition and multiplication are commutative, meaning that the order of the two numbers that you add or multiply does not matter:

Proposition 4.2. *The following statements hold:*

$$\forall_{x,y\in\mathbb{R}}(x+y=y+x), \qquad \forall_{x,y\in\mathbb{R}}(xy=yx).$$

Furthermore, both addition and multiplication are associative, meaning that the order in which one applies a sequence of additions or multiplications does not matter:

Proposition 4.3. *The following statements hold:*

$$\forall_{x,y,z\in\mathbb{R}}(\,(x+y)+z=x+(y+z)\,), \qquad \forall_{x,y,z\in\mathbb{R}}(\,(xy)z=x(yz)\,).$$

Recall the special numbers 0 and 1 serve as identities for additional and multiplication, respectively, meaning that both adding 0 and multiplying by 1 do absolutely nothing:

Proposition 4.4. *The following statements hold:*

$$\forall_{x\in\mathbb{R}}(x+0=0+x=x), \qquad \forall_{x\in\mathbb{R}}(x\cdot 1=1\cdot x=x).$$

Next, every real number x has an additive inverse (namely, $-x$) in that adding by this inverse precisely cancels out adding by x. Similarly, each non-zero real number x also has a multiplicative inverse (namely, $\frac{1}{x}$) that cancels out multiplying by x.

Proposition 4.5. *The following statements hold:*

$$\forall_{x\in\mathbb{R}}(\, x + (-x) = (-x) + x = 0\,), \qquad \forall_{x\in\mathbb{R}\setminus\{0\}}\left(x \cdot \tfrac{1}{x} = \tfrac{1}{x} \cdot x = 1\right).$$

(Notice $\mathbb{R} \setminus \{0\}$ is a concise way to describe the "set of all non-zero real numbers". We will use this notation—along with $\mathbb{Z} \setminus \{0\}$, etc.—throughout these notes.)

We also list the distributive property relating addition and multiplication:

Proposition 4.6. *The following statement holds:*

$$\forall_{x,y,z\in\mathbb{R}}(\, x(y+z) = xy + xz\,).$$

Finally, we recall the linear ordering properties of the real numbers (and of the natural numbers, integers, and rational numbers by extension). These are basic properties of "$\leq$" that together can be interpreted as all the real numbers being arranged in a line.

Proposition 4.7. *The following statements hold:*

(1) *Reflexivity:* $\forall_{x\in\mathbb{R}} x \leq x$.
(2) *Antisymmetry:* $\forall_{x,y\in\mathbb{R}}((x \leq y \text{ and } y \leq x) \Rightarrow x = y)$.
(3) *Transitivity:* $\forall_{x,y,z\in\mathbb{R}}((x \leq y \text{ and } y \leq z) \Rightarrow x \leq z)$.
(4) *Linearity/totality:* $\forall_{x,y\in\mathbb{R}}(x \leq y \text{ or } y \leq x)$.

Recall that given $x, y \in \mathbb{R}$, then $x < y$ iff y lies to the right of x. In particular, Properties (2)–(4) in Proposition 4.7 essentially tell us that given $x, y \in \mathbb{R}$ that are distinct (i.e. $x \neq y$), then either "y lies to the right of x", or "x lies to the right of y". As a result, the rough intuition is that all the real numbers can be viewed as lying along a line, rather than in some more complicated shape or configuration.

Given these are all properties that you have encountered before, we will refrain from discussing these further. However, you should use the above as practice for reading and interpreting formal statements. We will also apply some of these properties later on, so make sure you know what each of these statements say.

Note. *From the perspective of formal set theory and foundations of mathematics, assuming all the number systems come prepackaged with all these nice properties is quite undesirable. Even if you believe all this to be self-evident, we saw in the last chapter (in the bonus material) how easily one can generate a contradiction that ends mathematics as we know it, so making this many assumptions is philosophically very risky.*

Thus, what one does in formal set theory is to explicitly construct each of the number systems using the set theory axioms and abstract sets. Once we give precise descriptions of each type of number, we can then define the usual algebraic operations ($+$ and $\times$) and comparison relation ($\leq$). From these, we can then prove that all the properties in Propositions 4.1–4.7 hold. All this is a bit beyond the scope of this module, however we briefly comment on this process in bonus material at the end of Chapter 5.

The upside of this formal approach is that we can recover everything we want about the various number systems using only the basic set theory axioms, hence we need not make any additional risky assumptions at all. The downside, however, is that the formal definitions of the various number systems tend to be quite unintuitive, and proving all the above properties is an extremely painstaking process.

4.2. **Induction.** Our numerical journey begins with the natural numbers

$$\mathbb{N} = \{1, 2, 3, \dots\},$$

which one usually associates with "counting" or "enumerating". For instance, you might count how many hours you revise for the NSF exam (1 hour, 2 hours, etc.), or you might count how many pizza slices you eat (1 slice, 2 slices, etc.). Indeed, natural numbers serve as an abstraction that captures any kind of counting you may do in everyday life.

What features of natural numbers make them special—in particular, suitable for counting? Below are two such properties that are intuitively very obvious but set the natural numbers apart from all the other number systems:

(1) Given any $n \in \mathbb{N}$, there is a unique "next number after n" (namely, $n + 1$).
(2) If you start from $1 \in \mathbb{N}$ (the first natural number), and you iterate through all the "next numbers" in order (i.e. $1, 2, 3, 4, \dots$), then at the end of this infinite process, you will have listed every element of $\mathbb{N}$.

Indeed, the process in (2) of starting from 1 and then repeatedly iterating through the next numbers is precisely what we think of as counting. Furthermore, the properties (1)–(2) form the basis of a beloved proof technique known as induction.

The basic idea behind induction is as follows. Suppose you want to prove the statements $P(n)$ hold for all $n \in \mathbb{N}$. Then, one strategy would be to proceed as follows:

- First, we prove that $P(1)$ holds.
- We then prove "if $P(1)$ holds, then so does $P(2)$" (formally, we show $P(1) \Rightarrow P(2)$). Since we know $P(1)$ holds, this implication tells us that $P(2)$ also holds.
- Next, we then prove "if $P(2)$ holds, then so does $P(3)$" (formally, $P(2) \Rightarrow P(3)$). Since we already have $P(2)$, the above implies that $P(3)$ also holds.
- Similarly, we show $P(3) \Rightarrow P(4)$, and hence $P(4)$.
- Continuing as before, we then prove $P(5)$, $P(6)$, and so on...
- If we can continue this process indefinitely, then $P(n)$ will hold for all $n \in \mathbb{N}$.

While many texts often try to make induction into some complicated and advanced concept, the steps described above is really all that induction is.

Example 4.8. *One concrete example of the above is the following problem:*

- *Prove that* $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ *for all* $n \in \mathbb{N}$.

Note in this case that $P(n)$ *(for* $n \in \mathbb{N}$*) is the statement*

- $P(n)$*:* $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

As a result, the objective here is precisely to show that $P(n)$ *holds for all* $n \in \mathbb{N}$*. Soon, we will demonstrate in detail how to prove this via induction.*

To make this general strategy less abstract, you can think of $P(1), P(2), \ldots$ as dominoes lined up in order, with $P(n-1)$ right before $P(n)$ for each $n \in \mathbb{N}$. In this analogy, proving $P(n)$ holds corresponds to knocking over the n-th domino in the sequence.

The rough idea is that if you tip over the first domino (i.e. you show $P(1)$ holds), then the first domino will tip over the second (i.e. you show $P(1) \Rightarrow P(2)$, so $P(2)$ holds), and then the second will knock over the third (i.e. you show $P(2) \Rightarrow P(3)$, so $P(3)$ holds), and so on. If you let this process run eternally, then at the end of time, every single domino will have fallen over in the end (i.e. you have shown $P(n)$ holds for every $n \in \mathbb{N}$).

On the more abstract side, this strategy can be viewed as another proof rule that can be applied to establish properties involving natural numbers:

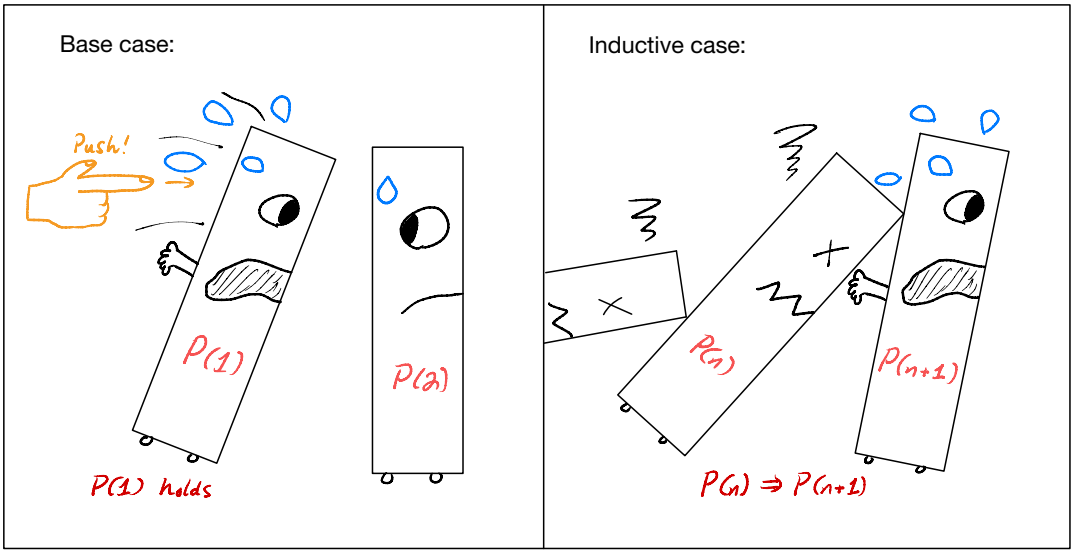
Assume:	$P(1), \quad \forall_{n \in \mathbb{N}}(P(n) \Rightarrow P(n+1))$
Conclude:	$\forall_{n \in \mathbb{N}} P(n)$

FIGURE 4.1. Proof rule: induction

In other words, *to prove* $P(n)$ *holds for all* $n \in \mathbb{N}$ *by induction*, you must show:

- Base case: $P(1)$ holds.
- Inductive case: For any $n \in \mathbb{N}$, if $P(n)$ holds, then $P(n+1)$ holds.

Note that in the domino analogy, proving the base case corresponds to tipping over the first domino, while proving the inductive case corresponds to showing that any falling domino will tip over the next domino in the queue. In practice, the base case is usually relatively easy to show, so the main challenge is in handling the inductive case.



Note. *While we packaged induction as a "proof rule" in Figure 4.1, it is really a feature of the natural numbers, rather than of deductive logic. This is the main reason for presenting induction here, rather than in the earlier discussions on logic.*

4.2.1. *Examples of Induction.* We now present some basic examples of induction proofs. Similar to Chapter 2, for each example, we first write the proof as one normally would in a textbook (or on an exam), and we then provide further commentary below.

Let us begin with the statement from Example 4.8:

Proposition 4.9. *The following holds for every* $n \in \mathbb{N}$*:*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}. \tag{4.1}$$

Note. *Recall that Σ-notation is defined as follows—we write*

$$\sum_{k=a}^{b} x_k.$$

as a shorthand for the summation

$$x_a + x_{a+1} + \cdots + x_{b-1} + x_b.$$

Here, we sum over the x_k's, starting from x_a, with k increasing by one in each successive term, until the sum terminates at x_b. Similar to quantifiers, the index k just serves as a dummy variable that identifies each term in the summation.

In particular, the Σ-summation in Proposition 4.9 expands as

$$\sum_{k=1}^{n} k = 1 + 2 + \cdots + (n-1) + n.$$

Proof of Proposition 4.9. First, the desired equation (4.1) holds for $n = 1$, since

$$\sum_{k=1}^{1} k = 1 = \frac{1(1+1)}{2}.$$

Fix now $n \in \mathbb{N}$, and assume the equation (4.1) holds for n, i.e.

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Then, using the above assumption, we can directly compute

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + (n+1) \\
&= \tfrac{n(n+1)}{2} + (n+1) \\
&= \tfrac{n(n+1)}{2} + \tfrac{2(n+1)}{2} \\
&= \tfrac{(n+1)(n+2)}{2} \\
&= \tfrac{(n+1)((n+1)+1)}{2},
\end{aligned}$$

and hence (4.1) holds, with n replaced by $n+1$.

Finally, by induction, we conclude that (4.1) indeed holds for all $n \in \mathbb{N}$. □

Let us take a closer look at the proof above now. First, here we let $P(n)$ be the statement

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Thus, to proof Proposition 4.9, we must show that $P(n)$ holds for all $n \in \mathbb{N}$.

The first paragraph of the proof (in blue) proves the base case—i.e. $P(1)$ holds:

$$\sum_{k=1}^{1} k = \frac{1(1+1)}{2}.$$

Indeed, the short computation showed that both sides of the above are equal to 1.

The second paragraph tackles the inductive case—showing that

$$\forall_{n\in\mathbb{N}}(P(n) \Rightarrow P(n+1)). \tag{4.2}$$

This begins as you might expect:

- To handle the quantifier in (4.2), we fix an arbitrary $n \in \mathbb{N}$.
- Then, for the implication in (4.2), we begin by supposing that $P(n)$ holds. (This assumption of $P(n)$ is often called the induction hypothesis.)

The above two steps are highlighted in green in the proof.

Next, in the following sequence of equalities (in pink), we proceed to show $P(n+1)$ holds. This suffices to show (see Figures 2.4 and 2.18) that (4.2) indeed holds. Observe that the key feature in showing $P(n+1)$ holds that sets it apart from other proofs is that we make crucial use of the assumption that $P(n)$ holds; this part is highlighted in orange.

Finally, since we have shown both $P(1)$ (the base case) and (4.2) (the inductive case), it follows from the rule in Figure 4.1 that $P(n)$ holds for every $n \in \mathbb{N}$, as desired.

We remark that although newcomers tend to find the structure of proofs by induction confusing, the intent is actually to *make proofs easier*. Rather than having to prove $P(n)$ (for any $n \in \mathbb{N}$) directly, in an induction argument, one needs (aside from the base case) only to prove $P(n+1)$ *while already knowing* $P(n)$. In other words, it is often easier to go up by only one, from n to $n+1$, than to leap directly from nothing to n. Indeed, in the proof of Proposition 4.9, proving $P(n+1)$ from $P(n)$ is a short calculation, but one must be more clever to derive $P(n)$ directly (see if you can do this!).

Example 4.10. *Let us prove by induction that the following holds for all $n \in \mathbb{N}$:*

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}. \tag{4.3}$$

Proof. First, for the base case, we observe that (4.3) holds when $n = 1$:

$$\sum_{k=1}^{1} \frac{1}{k(k+1)} = \frac{1}{2} = \frac{1}{1+1}.$$

Next, we fix $n \in \mathbb{N}$, and we assume (4.3) holds with this n. Then,

$$\begin{aligned}
\sum_{k=1}^{n+1} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} \\
&= \tfrac{n}{n+1} + \tfrac{1}{(n+1)(n+2)} && \text{(by induction hypothesis)} \\
&= \tfrac{n(n+2)+1}{(n+1)(n+2)} \\
&= \tfrac{n^2+2n+1}{(n+1)(n+2)} \\
&= \tfrac{n+1}{n+2} && \text{(since } n^2 + 2n + 1 = (n+1)^2\text{)}.
\end{aligned}$$

As a result, (4.3) holds with n replaced by $n + 1$.

Finally, by induction, we conclude (4.3) indeed holds for all $n \in \mathbb{N}$. □

The structure of the above proof is analogous to that of Proposition 4.9. Here, we let $P(n)$ *denote the statement that* (4.3) *holds, that is,*

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}.$$

The first paragraph of the proof tackles the base case by showing $P(1)$*. The second paragraph handles the inductive case—here, we fix* $n \in \mathbb{N}$ *and assume* $P(n)$ *holds, and we proceed to show* $P(n+1)$*. The last paragraph just applies the rule from Figure 4.1.*

We remark that the last paragraph of the proof in Example 4.10—which applies the induction rule—is often omitted from the writing. This is because it is implicitly understood by readers who are familiar with induction, so it serves no practical function.

Next, to demonstrate the wide applicability of induction, we now prove a rather different type of statement using the same argument structure as before:

Example 4.11. *Let us prove the following statement:*

- $n^2 < 2^n$ *for all* $n \in \mathbb{N}$ *with* $n \geq 5$.

Proof. As the base case, we show the statement holds with $n = 5$:

$$5^2 = 25 < 32 = 2^5.$$

Now, fix a natural number $n \geq 5$, and assume $n^2 < 2^n$. We then have

$$\begin{aligned} 2n + 1 &< 2n + n && \text{(since } n > 1\text{)} \\ &= 3n \\ &< n^2 && \text{(since } n > 3\text{).} \end{aligned}$$

As a result, we conclude that

$$\begin{aligned} (n+1)^2 &= n^2 + 2n + 1 \\ &< n^2 + n^2 && \text{(since } 2n + 1 < n^2\text{)} \\ &< 2^n + 2^n && \text{(induction hypothesis)} \\ &= 2^{n+1} && \text{(since } 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}\text{).} \end{aligned}$$

Thus, by induction, $n^2 < 2^n$ holds for all $n \in \mathbb{N}$. □

Here, the statement under consideration is given by

- $P(n)$: $n^2 < 2^n$.

While the structure of the above proof is essentially identical to those in previous examples, a couple points here do deserve special mention.

The first is we only aim to show $P(n)$ for all natural numbers $n \geq 5$. As a result, for the base case, which kicks off the induction process, we show that $P(5)$ holds. Similarly, for the inductive case, we show $P(n) \Rightarrow P(n+1)$, but only for $n \geq 5$.

The next comment is that the argument for the inductive case is a bit more involved, with some algebraic manipulations that may seem mysterious. The key point to keep in mind is that our only objective is to go from assuming $P(n)$ to proving $P(n+1)$; all we need to do is to find some way to get there. Thus, there is nothing special about these algebraic steps, other than that it is one viable path to go from $P(n)$ to $P(n+1)$.

Note. *Also, there is nothing novel about the fact that the induction process in Example 4.11 starts from $n = 5$ rather than $n = 1$. Indeed, we can just rewrite the statement in Example 4.11 equivalently as "$(n+4)^2 < 2^{n+4}$ for all $n \in \mathbb{N}$", which can be proved using the original induction rule from Figure 4.1.*

There is no need to worry if you do not feel fully comfortable with induction yet. We will see more examples of induction later on as we cover additional material.

4.2.2. *To Induct, or Not to Induct.* As you read examples of induction proofs, you may be wondering *when you should prove a statement by induction, as opposed to directly.* The only general answer is that *you should use whatever methods you need to get the job done, and with the minimum hassle.* Whether this involves induction depends on the statement you wish to prove, as well as what you already know beforehand.

To expand on the above, and to show off a clever trick along the way, let us revisit the statement from Example 4.10 and try proving it directly:

Example 4.12. *Prove (again) that the following holds for all* $n \in \mathbb{N}$*:*

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}.$$

Proof. Recall that by partial fractions, we can write, for each $n \in \mathbb{N}$,

$$\tfrac{1}{k(k+1)} = \tfrac{1}{k} - \tfrac{1}{k+1}.$$

Thus, the original summation can be expanded as

$$\begin{aligned} \sum_{k=1}^{n} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1} \right) \\ &= \left(1 - \tfrac{1}{2}\right) + \left(\tfrac{1}{2} - \tfrac{1}{3}\right) + \left(\tfrac{1}{3} - \tfrac{1}{4}\right) \\ &\quad + \cdots + \left(\tfrac{1}{n-1} - \tfrac{1}{n}\right) + \left(\tfrac{1}{n} - \tfrac{1}{n+1}\right). \end{aligned} \tag{4.4}$$

Note that on the right-hand side, the second part of each term cancels out with the first part of the following term. Thus, after all the cancellations, we obtain

$$\begin{aligned} \sum_{k=1}^{n} \frac{1}{k(k+1)} &= 1 - \frac{1}{n+1} \\ &= \frac{n}{n+1}. \end{aligned}$$

□

Sums such as that of the right-hand side of (4.4)*, which contain successive cancellations in nearby terms, are known as telescoping sums.*

We can now compare the two proofs in Examples 4.10 and 4.12. The main advantage of the induction approach in Example 4.10 is that, once you are familiar with the structure of induction arguments, the proof does not require much cleverness. In the main (inductive) step, once we assume $P(n)$ and apply this inductive hypothesis (highlighted in orange), then $P(n+1)$ follows from a computation that is straightforward to anyone skilled with

adding fractions. In contrast, for the direct proof in Example 4.12, one must somehow find the telescoping structure in the summation in order to apply the cancellations that lead to the final answer; all of this requires an extra level of perceptiveness.

Now, one drawback of the induction proof in Example 4.10 is that *we needed to know the value of the sum before we started the proof.* Indeed, observe that we can complete neither the base nor inductive steps if we did not already know the value of the sum in (4.3) is $\frac{n}{n+1}$. Thus, to prove by induction, you must either have been given this information beforehand, or have guessed the value $\frac{n}{n+1}$ by experimenting around. On the other hand, if you are more clever at the start and proceeded as in Example 4.12, then through that computation, you can arrive at the value $\frac{n}{n+1}$ without knowing it beforehand.

4.3. **Strong Induction.** In the preceding section, we introduced induction as a method of proof for statements involving natural numbers. However, there are some cases where induction, as we presented it, is not quite enough. For a concrete example, let us recall the following famous sequence, which should already be familiar to many of you:

Definition 4.13. *The Fibonacci sequence is defined recursively as follows:*

$$F_1 = 1, \qquad F_2 = 1, \qquad F_{n+1} = F_n + F_{n-1}, \quad n \geq 2.$$

To demonstrate, we can compute the next few values of the Fibonacci sequence,

$$F_3 = F_2 + F_1 = 2,$$
$$F_4 = F_3 + F_2 = 3,$$
$$F_5 = F_4 + F_3 = 5,$$

and so on. A simple property of the Fibonacci sequence is the following:

Proposition 4.14. $F_n < 2^n$ *for any* $n \in \mathbb{N}$.

Suppose now that you wish to prove Proposition 4.14 by induction. The first few cases are easy enough to check directly—for instance,

$$F_1 = 1 < 2^1, \qquad F_2 = 1 < 2^2.$$

For the inductive step, one must then assume $F_n < 2^n$ (for $n \in \mathbb{N}$) and show $F_{n+1} < 2^{n+1}$.

What goes wrong with this effort? In order to prove something about F_{n+1}, we would need to expand $F_{n+1} = F_n + F_{n-1}$. This means that *we need information about both* F_n

and F_{n-1}. However, for our inductive hypothesis, we only assumed $F_n < 2^n$, and nothing about F_{n-1}, so we do not quite have enough to finish the job.

In other words, if we let $P(n)$ denote the statement "$F_n < 2^n$", then due to the way the Fibonacci sequence is defined, we would need to assume both $P(n)$ and $P(n-1)$ in order to say something about $P(n+1)$. In Figure 4.1, however, we make no such assumption about $P(n-1)$, so the prospects of using induction are not so good.

4.3.1. *The Full Power of Induction.* Now, what saves us from impending failure (both in the above example and more generally) is that we have not yet unleashed the full power of induction. This is perhaps best explained by returning to the domino analogy.

Here, one can think of the issue as the $P(n)$-domino falling into the $P(n+1)$-domino, but not being strong enough to tip the $P(n+1)$-domino over. However, the untapped potential comes from the observation that *at the time when the* $P(n)$*-domino is tipping over, we have already knocked over all the dominoes* $P(1), P(2), \ldots, P(n-1)$ *that came before* $P(n)$. Thus, even if the $P(n)$-domino by itself cannot dislodge the $P(n+1)$-domino, then perhaps *the combined strengths of all the fallen dominoes* $P(1), P(2), \ldots, P(n)$ *are enough to knock over* $P(n+1)$. The power of teamwork!

For the special case of Proposition 4.14, we will soon see that the combined strengths of the $P(n)$-domino falling (assuming $F_n < 2^n$) and $P(n-1)$-domino falling (assuming $F_{n-1} < 2^{n-1}$) are enough to tip over the $P(n+1)$-domino (proving $F_{n+1} < 2^{n+1}$).

The above discussion leads us to the following "levelled-up" induction strategy:

- First, we prove that $P(1)$ holds.
- We then prove $P(1) \Rightarrow P(2)$. Since we know $P(1)$ holds, this implication tells us that $P(2)$ also holds, hence "$P(1)$ and $P(2)$" holds as well.
- Next, we then prove "$(P(1)$ and $P(2)) \Rightarrow P(3)$". Since we already have $P(1)$ and $P(2)$, the above implies $P(3)$ holds, so "$P(1)$ and $P(2)$ and $P(3)$" follows.
- We then show "$(P(1)$ and $P(2)$ and $P(3)) \Rightarrow P(4)$", and this yields that $P(4)$ holds, as well as "$P(1)$ and $P(2)$ and $P(3)$ and $P(4)$".
- Continuing as before, we prove $P(5)$, $P(6)$, and so on…
- If we can continue this process indefinitely, then $P(n)$ will hold for all $n \in \mathbb{N}$.

This new-and-improved strategy is known as strong induction.

More formally, we can encode strong induction as a proof rule:

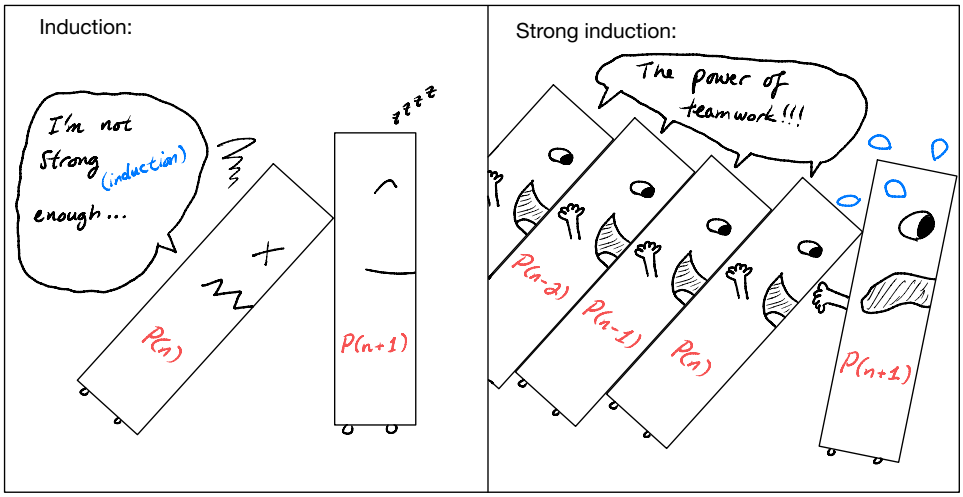
Assume:	$P(1), \quad \forall_{n\in\mathbb{N}}((\forall_{m\in\{1,2,\ldots,n\}} P(m)) \Rightarrow P(n+1))$
Conclude:	$\forall_{n\in\mathbb{N}} P(n)$

FIGURE 4.2. Proof rule: strong induction

Thus, *to prove* $P(n)$ *holds for all* $n \in \mathbb{N}$ *by strong induction*, you must show:

- Base case: $P(1)$ holds.
- Inductive case: For any $n \in \mathbb{N}$, if $P(1), P(2), \ldots, P(n)$ hold, then $P(n+1)$ holds.

Once again, proving the base case corresponds to tipping over the first domino (in practice, usually the first few dominoes). The inductive case now corresponds to showing that all the dominoes up to n falling over will tip over domino $n+1$.



Note. *Observe that induction is nothing but a special case of strong induction. Indeed, we can think of an induction argument as essentially a strong induction argument, except that in the inductive step, we choose only to use information about* $P(n)$*, and not anything before that. Thus, if you do not like remembering so many things, then strong induction is the only concept you really need to know.*

4.3.2. *Examples of Strong Induction.* We now present some examples of strong induction proofs, starting with the proof of Proposition 4.14:

- $F_n < 2^n$ for every $n \in \mathbb{N}$.

Proof of Proposition 4.14. First, by direct computation, we have

$$F_1 = 1 < 2^1, \qquad F_2 = 1 < 2^2.$$

Fix now any natural number $n \geq 2$, and assume $F_k < 2^k$ for all $k \leq n$. Then,

$$F_{n+1} = F_n + F_{n-1}$$

$$\begin{aligned} &< 2^n + 2^{n-1} && \text{(induction hypothesis)} \\ &< 2^n + 2^n && \text{(since } 2^{n-1} < 2^n\text{)} \\ &= 2^{n+1} && \text{(since } 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}\text{).} \end{aligned}$$

Thus, by strong induction, we conclude $F_n < 2^n$ for all $n \in \mathbb{N}$. □

To discuss the above proof in more detail, let us consider the statement

- $P(n)$: $F_n < 2^n$.

The first paragraph of the proof (in blue) covers the base cases by proving $P(1)$ and $P(2)$.

It is in fact quite common for strong induction proofs to have more than one base case. Here, *it is essential that we have two base cases.* This is because we cannot treat F_2 using the recursive formula $F_{n+1} = F_n + F_{n-1}$, since F_0 is not defined. As a result, we have to check that $P(2)$ holds directly, using the definition $F_2 = 1$.

The second paragraph of the proof then treats everything beyond $P(2)$ as the inductive case. We begin by fixing any $n \in \mathbb{N} \setminus \{1\}$, and we then assume (in pink) the inductive hypothesis—that $P(1), P(2), \ldots, P(n)$ hold. The subsequent short computation then proceeds to show that $P(n+1)$ holds (also in pink). Note in particular we applied the induction hypothesis at the part highlighted in orange.

The final sentence of the proof simply applies the rule from Figure 4.2. Again, this is often omitted, as it is implicitly understood by experienced readers.

Note. *Even when an induction proof has multiple base cases, the rule of Figure 4.2 still applies. For instance, in the proof of Proposition 4.14, we can view the second base case $P(2)$ as a trivial inductive case that does not use the inductive hypothesis ($P(1)$ holds).*

On the other hand, it is absolutely essential that one treats $P(2)$ differently than the subsequent $P(n)$'s, $n \geq 2$, in the proof of Proposition 4.14.

Next, while many have seen the Fibonacci sequence before, what is less well-known is that there is a (surprisingly nasty) explicit formula for the values of this sequence:

Proposition 4.15. *The following holds for any $n \in \mathbb{N}$:*

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]. \tag{4.5}$$

Before delving into the proof of Proposition 4.15, one should take a moment to appreciate just how absurd this formula (4.5) is. After all, each F_n, $n \in \mathbb{N}$, is by definition a nice natural number, yet the explicit formula for F_n somehow is full of powers of $\sqrt{5}$!

Proof of Proposition 4.15. For F_1 and F_2, we can these explicitly:

$$\begin{aligned}
\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1\right] &= \frac{1}{\sqrt{5}}\left(\frac{2\sqrt{5}}{2}\right) \\
&= 1, \\
\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2\right] &= \frac{1}{\sqrt{5}}\left[\left(\underbrace{\frac{1}{4}+\frac{\sqrt{5}}{2}+\frac{5}{4}}_{\frac{3}{2}+\frac{\sqrt{5}}{2}}\right) - \left(\underbrace{\frac{1}{4}-\frac{\sqrt{5}}{2}+\frac{5}{4}}_{\frac{3}{2}-\frac{\sqrt{5}}{2}}\right)\right] \\
&= \frac{1}{\sqrt{5}}\left(\frac{2\sqrt{5}}{2}\right) \\
&= 1.
\end{aligned}$$

Thus, the desired formula (4.5) holds for $n = 1$ and $n = 2$.

For the inductive step, fix $n \in \mathbb{N} \setminus \{1\}$, and suppose

$$F_k = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right], \qquad k \leq n.$$

Then, by this inductive hypothesis and the recursive formula for F_{n+1}, we have

$$\begin{aligned}
F_{n+1} &= F_n + F_{n-1} \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \\
&\quad + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right].
\end{aligned}$$

Now, the terms above in red can be combined and simplified as

$$\begin{aligned}
\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} &= \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\underbrace{\frac{1+\sqrt{5}}{2}+1}_{\frac{3}{2}+\frac{\sqrt{5}}{2}=\left(\frac{1+\sqrt{5}}{2}\right)^2}\right) \\
&= \left(\frac{1+\sqrt{5}}{2}\right)^{n+1}.
\end{aligned}$$

Similarly, the terms in blue can be combined and simplified as

$$\left(\frac{1-\sqrt{5}}{2}\right)^{n} + \left(\frac{1-\sqrt{5}}{2}\right)^{n-1} = \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\underbrace{\frac{1-\sqrt{5}}{2}+1}_{\frac{3}{2}-\frac{\sqrt{5}}{2}=\left(\frac{1-\sqrt{5}}{2}\right)^{2}}\right)$$
$$= \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}.$$

Combining all the above, we conclude that

$$F_{n+1} = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} + \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right],$$

which is precisely (4.5), with n replaced by $n+1$.

Finally, by strong induction, we obtain (4.5) for all $n \in \mathbb{N}$, as desired. □

Observe that although the computations in the proof of Proposition 4.15 are considerably more involved, the structure of the proof is identical to that of Proposition 4.14. Indeed, here we let $P(n)$ (for any $n \in \mathbb{N}$) denote the statement in (4.5):

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n} - \left(\frac{1-\sqrt{5}}{2}\right)^{n}\right].$$

The first paragraph of the proof covers the base case; by direct computations, we show both $P(1)$ and $P(2)$ hold. The second paragraph then handles the inductive case. Here, we fix any natural number $n \geq 2$, and we assume $P(1), P(2), \ldots, P(n)$ holds. The ensuing computation then shows $P(n+1)$ holds. (The computation here may be quite complicated, and it requires some extra cleverness, but conceptually, all we are doing here is showing $P(n+1)$.) Thus, by the rule in Figure 4.2, we conclude $P(n)$ holds for all $n \in \mathbb{N}$.

We finish with one more example of a strong induction proof. The argument again has the same structure as before, with the only difference being that we need three base cases. Thus, here we just give the proof without much further comment:

Example 4.16. *Consider the sequence G_n, $n \in \mathbb{N}$, given recursively by*

$$G_1 = 1, \qquad G_2 = 3, \qquad G_3 = 7, \qquad G_{n+1} = G_n + G_{n-1} + G_{n-2}, \quad n \geq 3.$$

Let us now show that the following inequality holds for all $n \in \mathbb{N}$:

$$G_n < 2^n. \tag{4.6}$$

Proof. For G_1, G_2, and G_3, we can check (4.6) directly:

$$G_1 = 1 < 2^1, \qquad G_2 = 3 < 2^2, \qquad G_3 = 7 < 2^3.$$

For the remaining inductive cases, let us fix a natural number $n \geq 3$, and assume

$$G_k < 2^k, \qquad 1 \leq k \leq n.$$

Then, by a direct computation, we see that

$$\begin{aligned} G_{n+1} &= G_n + G_{n-1} + G_{n-2} \\ &< 2^n + 2^{n-1} + 2^{n-2} && \text{(by induction hypothesis)} \\ &= 2^n + \underbrace{2^{n-1} + 2^{n-1}}_{=2\cdot 2^{n-1}=2^n} && \text{(since } 2^{n-2} < 2^{n-1}\text{)} \\ &= 2^n + 2^n \\ &= 2^{n+1}. \end{aligned}$$

Thus, we conclude that $G_{n+1} < 2^{n+1}$, completing the strong induction proof. □

Once again, the chain of equalities and inequalities in the inductive step may seem a bit mysterious and unintuitive, however the only point here is that these manipulations are just enough to prove $G_{n+1} < 2^{n+1}$ from the inductive hypothesis, which is what is required to complete the strong induction argument. In other words, prove just what you need, and nothing more—keep your eyes on the prize!

Again, there is no need to fret if you are not yet fully comfortable with strong induction, as we will see more examples of this later in later sections.

Note. *In these notes, we have essentially presented induction (Figure 4.1) and strong induction (Figure 4.2) as axiomatic rules of proof that we simply accept as valid. However, if one takes a more formal approach and gives a precise definition of the natural numbers, then one can in fact prove, from this construction of $\mathbb{N}$, that induction and strong induction are valid logical steps. Thus, there is no need to accept induction purely on intuition alone, as this is a property that rigorously emerges from the features of $\mathbb{N}$.*

4.4. **Divisibility and Division.** We now turn our attention toward the integers. In the following few sections, we will survey some basic topics in elementary number theory, which is the study of the basic structure and properties of integers.

As you know, the integers satisfy the following closure properties:

- *For any* $a, b \in \mathbb{Z}$*, their sum, difference, and product are also integers:*

$$a + b \in \mathbb{Z}, \qquad a - b \in \mathbb{Z}, \qquad ab \in \mathbb{Z}.$$

However, the story is quite different for division—when $a, b \in \mathbb{Z}$, the quotient $\frac{a}{b}$ needs not be an integer. In fact, we need not look far for an example, since $\frac{1}{2} \notin \mathbb{Z}$! Thus, a large proportion of topics in elementary number theory pertain to division and its complexities.

Along this direction, the most basic questions one can ask are the following:

Question 4.17. *Given* $a, b \in \mathbb{Z}$*:*

- *When can one divide* a *by* b*, that is, when is* $\frac{a}{b} \in \mathbb{Z}$*?*
- *When* $\frac{a}{b} \notin \mathbb{Z}$*, and then how can one divide* a *by* b *"as much as possible"?*

In fact, this is not the first time you are addressing Question 4.17. If you think back to your (much) earlier life, then you should recall that you dealt with these questions when you first studied division in primary school! Here, we revisit these topics in a more rigorous manner, and with an eye toward more interesting applications than just arithmetic.

4.4.1. *Divisibility.* The most fundamental concept regarding integer division is the following, which addresses the first point in Question 4.17:

Definition 4.18. *Given* $a, b \in \mathbb{Z}$*, we write* $b \mid a$ *iff* $a = bk$ *for some* $k \in \mathbb{Z}$*.*

- *More formally,*

$$b \mid a \Leftrightarrow \exists_{k \in \mathbb{N}}(a = bk).$$

- *We also write* $b \nmid a$ *as an abbreviation for "*$\text{not}(b \mid a)$*".*

Furthermore, $b \mid a$ *is often written out in the following ways:*

- b *is a* divisor *of* a*.*
- b *divides* a*.*
- a *is* divisible *by* b*.*

Intuitively, the statement $b \mid a$ (for $a, b \in \mathbb{Z}$) *can be interpreted as "*$\frac{a}{b}$ *is an integer"*. (Indeed, "$a = bk$ for some $k \in \mathbb{Z}$" can also be written as $\frac{a}{b} = k \in \mathbb{Z}$.) The reason for defining $b \mid a$ as we did (rather than as $\frac{a}{b} \in \mathbb{Z}$) is that our definition is expressed purely in terms of integers, without reference to the larger class of rational numbers.

Example 4.19. *The following hold:*

- $3 \mid 15$, *since* $15 = 3 \cdot 5$.
- $12 \mid 156$, *since* $156 = 12 \cdot 13$.
- $3 \nmid 16$, *since* 16 *cannot be expressed as* 3 *times an integer.*
- $15 \nmid 104$, *since* 104 *cannot be expressed as* 15 *times an integer.*

Example 4.20. *Definition 4.18 applies equally well to negative integers. For instance,*

$$-4 \mid 16, \qquad 4 \mid -16, \qquad -4 \mid -16, \qquad 5 \nmid -17.$$

Here, the first three statements hold since

$$16 = (-4) \cdot (-4), \qquad -16 = 4 \cdot (-4), \qquad -16 = (-4) \cdot 4.$$

Example 4.21. *Recall that for any* $a \in \mathbb{Z}$, *we defined* $2 \mid a$ *be the statement*

$$\exists_{k \in \mathbb{Z}} (a = 2k).$$

However, the above is simply the definition of a *being an even integer. Thus:*

- $a \in \mathbb{Z}$ *is even if and only if* $2 \mid a$.
- *Similarly,* $a \in \mathbb{Z}$ *is odd if and only if* $2 \nmid a$.

Note. *The following points tend to cause confusion for new students:*

- *When writing "*$b \mid a$*", one should keep in mind that the number* b *on the left is the smaller one, while the number* a *on the right is the larger one. For instance,* $4 \mid 16$ *is true, while* $16 \mid 4$ *is false—make sure you do not mix them up!*
- *Note also that "*$b \mid a$*" (a statement) and "*$\frac{b}{a}$*" (a rational number) are very different things. Thus, make sure you do not use one when you mean the other!*

Note. *If you take Definition 4.18 literally (you should!), then* $0 \mid 0$ *is clearly true, since* $0 = 0k$ *for every* $k \in \mathbb{Z}$. *On the other hand,* $\frac{0}{0} \notin \mathbb{Z}$, *nor is it even defined.*

Let us also establish a few general properties of divisibility:

Proposition 4.22. *The following hold for any* $a \in \mathbb{Z}$*:*

(1) $a \mid a$.
(2) $1 \mid a$.

Proof of Proposition 4.22. (1) This follows from Definition 4.18, since $a = a \cdot 1$.

(2) This also follows from Definition 4.18, since $a = 1 \cdot a$. □

More specifically, for part (1) of the above proof, $a = a \cdot 1$ implies (see Figure 2.19) that $\exists_{k \in \mathbb{Z}}(a = ak)$, which is precisely the definition of $a \mid a$. The proof of (2) is analogous.

Proposition 4.23. *The following hold for any* $a, b, c \in \mathbb{Z}$*:*

(1) *If* $a \mid b$ *and* $b \mid c$*, then* $a \mid c$.
(2) *If* $a \mid b$ *and* $a \mid c$*, then* $a \mid (b + c)$ *and* $a \mid (b - c)$.

Proof of Proposition 4.23. (1) By the definitions of $a \mid b$ and $b \mid c$, there exist $k, l \in \mathbb{Z}$ such that $b = ak$ and $c = bl$. From this, we then obtain

$$\begin{aligned} c &= (ak)l && \text{(since } b = ak\text{)} \\ &= a(kl). \end{aligned}$$

Since c can be written as a times an integer kl, it follows that $a \mid c$.

(2) Since $a \mid b$ and $a \mid c$, there exist $k, l \in \mathbb{Z}$ so that $b = ak$ and $c = al$. This implies

$$b + c = a(k + l), \qquad b - c = a(k - l).$$

By definition, the above yields both $a \mid (b + c)$ and $a \mid (b - c)$. □

4.4.2. *Divisibility and Induction.* In some cases, divisibility properties can be proved via induction. Such proofs are often found in introductory texts; if you have studied induction before, then you have probably already encountered some of these. We present a couple examples below, as demonstrations of both divisibility and induction.

Example 4.24. *Let us show the following statement holds:*

- $5 \mid (8^n - 3^n)$ *for any* $n \in \mathbb{N}$.

Proof. We prove this by induction. First, for the base case, we note the statement indeed holds for $n = 1$, since $8^1 - 3^1 = 5$, and $5 \mid 5$; see Proposition 4.22 (1).

For the inductive case, we fix any $n \in \mathbb{N}$ and assume $5 \mid (8^n - 3^n)$. Then,

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

By the induction hypothesis above, we have $8^n - 3^n = 5k$ for some $k \in \mathbb{Z}$. Thus,

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

Since $8^{n+1} - 3^{n+1}$ can be written as 5 times an integer, then $5 \mid (8^{n+1} - 3^{n+1})$, which completes the inductive case and the proof altogether. □

Although Example 4.24 is a classic example of induction, if you are a bit more perceptive and recall some factoring tricks, then you can in fact forgo induction altogether:

Example 4.25. *Let us now prove the following statement directly:*

- $5 \mid (8^n - 3^n)$ *for any* $n \in \mathbb{N}$.

Proof. Let $n \in \mathbb{N}$. Recall that $8^n - 3^n$ can be factored as

$$8^n - 3^n = \underbrace{(8 - 3)}_{5} \sum_{k=0}^{n-1} 8^k 3^{n-1-k}.$$

Thus, by definition, it follows that $5 \mid (8^n - 3^n)$. □

Example 4.26. *Let us show the following statement holds:*

- $13 \mid (7^{2n-1} + 6^{2n-1})$ *for any* $n \in \mathbb{N}$.

Proof. We proceed by induction. First, since $13 \mid 13$, and since

$$7^{2 \cdot 1 - 1} + 6^{2 \cdot 1 - 1} = 7^1 + 6^1 = 13,$$

then the desired statement holds for $n = 1$.

Next, fix $n \in \mathbb{N}$, and assume $13 \mid (7^{2n-1} + 6^{2n-1})$. Then,

$$\underbrace{7^{2(n+1)-1} + 6^{2(n+1)-1}}_{7^2 \cdot 7^{2n-1} + 6^2 \cdot 6^{2n-1}} = 49 \cdot 7^{2n-1} + 36 \cdot 6^{2n-1}$$
$$= 36(7^{2n-1} + 6^{2n-1}) + 13 \cdot 7^{2n-1}.$$

By the induction hypothesis, $7^{2n-1} + 6^{2n-1} = 13k$ for some $k \in \mathbb{Z}$, therefore

$$7^{2(n+1)-1} + 6^{2(n+1)-1} = 36(13k) + 13 \cdot 7^{2n-1}$$
$$= 13(36k + 7^{2n-1}).$$

It follows that $13 \mid (7^{2(n+1)-1} + 6^{2(n+1)-1})$, completing the proof. □

Can you prove the statement in Example 4.26 directly, without induction?

4.4.3. *Prime Numbers.* Consider, for the example, the statement $13 \mid 78$, which of course holds since $78 = 13 \cdot 6$. The significance of this statement is that we have now divided (i.e. factored) 78 into two smaller numbers, 13 are 6, which are hence easier to work with. By studying properties of 6 and 13, we can then extract some properties of 78.

On the other hand, there are some numbers that cannot be factored into simpler numbers as above. These are, in terms of division, already in their simplest form. As you have likely seen before, such numbers are commonly referred to as prime:

Definition 4.27. *Let $n \in \mathbb{N} \setminus \{1\}$.*

- *n is prime iff the only positive divisors of n are 1 and n. Formally,*

$$n \text{ is prime} \Leftrightarrow \forall_{m \in \mathbb{N}}(m \mid n \Rightarrow (m = 1 \text{ or } m = n)).$$

- *n is composite iff n is not prime.*

Example 4.28. *The following are all the prime numbers less than 50:*

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.$$

On the other hand, 4, 6, and 15 are not prime, since:

- *4 can be factored into smaller numbers as $4 = 2 \cdot 2$.*
- *6 can be factored into smaller numbers as $6 = 2 \cdot 3$.*

- 15 *can be factored into smaller numbers as* $15 = 3 \cdot 5$.

Note. *Note that the definitions of prime and composite only apply to natural numbers* $n > 1$. *Thus, according to Definition 4.27, the number* 1 *is neither prime nor composite.*

The next basic property states that every number has a prime divisor:

Proposition 4.29. *For any* $n \in \mathbb{N} \setminus \{1\}$, *there exists a prime number* p *such that* $p \mid n$.

Proof of Proposition 4.29. We prove this by strong induction. For convenience, we let $P(n)$ denote the statement "there exists a prime number p such that $p \mid n$".

As the base case, we observe that $P(2)$ holds, since 2 is prime, and $2 \mid 2$.

For the inductive case, suppose $P(2), P(3), \ldots, P(n)$ hold. We now split into cases:

- If $n+1$ is prime, then $P(n+1)$ trivially holds, since $(n+1)|(n+1)$.
- Suppose now $n+1$ is not prime. Note any $k \in \mathbb{N}$ that is a divisor of $n+1$ must satisfy $k \leq n+1$. (This is since if $k > n+1$, then $\frac{n+1}{k}$ cannot be an integer.) Therefore, since $n+1$ is composite, by Definition 4.27, it cannot have only 1 and $n+1$ as divisors, hence it must have another divisor k satisfying

$$1 < k < n+1, \qquad k \mid (n+1).$$

Since $P(k)$ holds (by the inductive hypothesis), there exists a prime number p satisfying $p \mid k$. Since $p \mid k$ and $k \mid (n+1)$, then by Proposition 4.23 (1), we conclude that $p \mid (n+1)$, and hence $P(n+1)$ holds.

As a result, $P(n+1)$ holds in all cases, completing the proof of the inductive case.

From all the above, we conclude $P(n)$ holds for all $n \in \mathbb{N}$, as desired. □

The above proof has the same structure as other strong induction examples. Here, one needs only a single base case, $P(2)$. The inductive case then cover $P(n)$ for all $n > 2$.

For the inductive case, we split into two separate cases (see Figure 2.11)—when $n+1$ is prime (which is trivial), and when $n+1$ is composite (which requires the inductive hypothesis). In the latter case, the idea is simply that the composite number $n+1$ has a strictly smaller factor k, which by the inductive hypothesis must have a prime factor p.

Proposition 4.29 will form the key step for factoring a number into a product of primes, however we will defer that discussion until Section 4.6. For now, we present a fundamental observation about the nature of prime numbers that is attributed to Euclid (ancient Greek mathematician, namesake of "Euclidean geometry"), from approximately 300 B.C.:

Theorem 4.30. *There are infinitely many prime numbers.*

Proof of Theorem 4.30. Suppose, for a contradiction, that there are only finitely many primes, which we denote as $p_1, p_2, \ldots, p_m$. Consider then the number

$$n = (p_1 p_2 \ldots p_m) + 1,$$

i.e. the product of all the (finitely many) primes plus 1.

By Proposition 4.29, there is a prime number p such that $p \mid n$. Since $p_1, p_2, \ldots, p_m$ are all the prime numbers, then $p = p_i$ for some $1 \leq i \leq m$. Thus,

$$p \mid \underbrace{p_1 p_2 \ldots p_m}_{n-1}.$$

Since both $p \mid n$ and $p \mid (n-1)$, then by Proposition 4.23 (2),

$$p \mid \underbrace{(n - (n-1))}_{1}.$$

Since the only numbers p satisfying $p \mid 1$ are $p = +1$ and $p = -1$, this contradicts that p is prime. Thus, we conclude there cannot only be finitely many primes. □

In particular, Theorem 4.30 implies there is no largest prime number.

Although prime numbers are a relatively simple concept that has been studied for millenia, there are still very basic questions involving prime numbers that remain unanswered. One famous example is the following question:

Question 4.31. *Is the following statement true?*

- *For any even $n \in \mathbb{N}$ with $n > 2$, there are primes p, q such that $n = p + q$.*

For example, Question 4.31 is affirmatively answered for $n \in \{4, 6, 8\}$, since

$$4 = 2 + 2, \qquad 6 = 3 + 3, \qquad 8 = 3 + 5.$$

However, does this hold for *every* even $n > 2$? In fact, *the answer to this is not known*!

The statement in Question 4.31 is known as the Goldbach conjecture, and it is one of the most famous unsolved problems in mathematics.

4.4.4. *Integer Division.* The notion of divisibility (Definition 4.18) makes precise the first part of Question 4.17. This still leaves the second half of Question 4.17—what happens when divisibility fails, that is, when one has $a, b \in \mathbb{Z}$ with $a \nmid b$?

The answer to this question is something you have done since primary school:

Example 4.32. *If we divide 80 by 7 like a toddler, then we obtain*

$$80 \div 7 = 11, \text{ remainder } 3.$$

The precise meaning of the above is that we can write 80 as

$$80 = 7 \times 11 + 3, \qquad \tfrac{80}{7} = 11 + \tfrac{3}{7}.$$

Here, 7 is the quotient and 3 is the remainder.

In keeping with the themes of NSF, we will now make this division process rigorous. In the past, we took for granted the fact that we can always divide two integers as in Example 4.32. Below, we will rigorously prove that this can indeed be done.

Theorem 4.33 (Division theorem)**.** *Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then:*

(1) *There exist $q, r \in \mathbb{Z}$ such that the following hold:*

$$a = qb + r, \qquad 0 \leq r < b. \tag{4.7}$$

(2) *q and r from (1) are unique—more precisely, if $q', r' \in \mathbb{Z}$ also satisfy*

$$a = q'b + r', \qquad 0 \leq r' < b, \tag{4.8}$$

then $q = q'$ and $r = r'$.

Proof of Theorem 4.33. (1) Let q denote the largest integer such that $qb \leq a$, and let $r = a - qb$. Then, $r \geq 0$ (since $a \geq qb$), and by definition $a = qb + r$.

Moreover, since $(q+1)b > a$ by the definition of q, the definition of r yields

$$(q+1)b > r + qb.$$

Subtracting qb from both sides yields $r < b$, which completes the proof of (1).

(2) Assume now q, r, q', r' satisfy (4.7) and (4.8). Subtracting (4.8) from (4.7) yields

$$(r - r') + (q - q')b = 0.$$

Since $0 \leq r < b$ and $0 \leq r' < b$, we have

$$\begin{aligned} b &> |r' - r| \\ &= |(q - q')b| \end{aligned}$$

The only way the above can hold is if $q - q' = 0$. Thus, we have $q = q'$, and hence

$$\begin{aligned} r - r' &= b(q' - q) \\ &= 0, \end{aligned}$$

which completes the proof of (2). □

The proof of Theorem 4.33 does not use any fancy strategies. For part (1), we wish to show the existence of quantities q and r (i.e. two existence quantifiers), thus we go out and find numbers q and r that satisfy (4.7). To actually find the numbers, we have to be resourceful and resort to our intuitions about numbers and division. The proof of part (2) is also direct—we assume (4.7)–(4.8), and we proceed to show that $q = q'$ and $r = r'$.

Note. *Recall the proof of Theorem 4.33 (1) began by "taking q to be the largest integer satisfying $qb \leq a$". That such a q always exists is a consequence of what is known as the Archimedean property (named after the ancient Greek mathematician Archimedes), which roughly states that there are no infinitely small numbers. For this module, we can just take this Archimedean property to be an axiom of our number systems. However, this property can also be proved from a formal construction of the number systems.*

We will explore some applications of the division theorem in the next section. For now, we note that through Theorems 4.30 and 4.33, we have seen some more involved proofs that require more effort to read. Even if you cannot come up with these proofs yourself, you should nonetheless be able to make sense of the individual steps within.

4.5. **Greatest Common Divisors.** Our next task is to *compare the divisors of two numbers*, in particular to *identify those divisors that are common to both numbers*. We begin the discussion by providing the basic definitions that we wish to work with below:

Definition 4.34. *Let* $a, b \in \mathbb{Z}$.

- $d \in \mathbb{Z}$ *is a* common divisor *of* a *and* b *iff* $d \mid a$ *and* $d \mid b$.
- *The* greatest common divisor *of* a *and* b *is the largest number* $d \in \mathbb{N}$ *that is a common divisor of* a *and* b. *Formally, this can be expanded as follows:*

$$d = \gcd(a, b) \Leftrightarrow (d \mid a \text{ and } d \mid b \text{ and } \forall_{c \in \mathbb{N}}((c \mid a \text{ and } c \mid b) \Rightarrow c \leq d)).$$

Let us take a minute to unpack the formal definition of $d = \gcd(a, b)$ above, which is a conjunction of three statements. The first two statements, $d \mid a$ and $d \mid b$, simply mean that d is a common divisor of a and b. The last (and more complicated) statement can be interpreted as saying *if any other number* c *is also a common divisor of* a *and* b, *then* c *cannot be larger than* d. This justifies d being the "greatest" common divisor of them all.

Another remark, which should already be intuitively clear, is that *the greatest common divisor of any* $a, b \in \mathbb{Z}$ (almost) *always exists, and there is only one such number*—that is, $\gcd(a, b)$ is uniquely defined. This can be briefly justified as follows:

- 1 is always a common divisor of a and b. Consequently, a and b always have at least one common divisor, so that $\gcd(a, b) \geq 1$.
- Moreover, if d_1 and d_2 are both greatest common divisors of a and b, then by the "greatest" part of the formal definition of gcd, we have both $d_1 \leq d_2$ and $d_2 \leq d_1$. Thus, it follows that $d_1 = d_2$, and hence $\gcd(a, b)$ is uniquely defined.

Note. *The one exception to the preceding discussion is* $\gcd(0, 0)$, *which does not exist. By taking Definition 4.34 very literally (again, you should!), we see that any* $k \in \mathbb{N}$ *is a common divisor of* 0 *and* 0, *hence there cannot be a "greatest" common divisor.*

Let us now get comfortable with Definition 4.34 through a few examples:

Example 4.35. *Some examples of greatest common divisors are below:*

- $\gcd(90, 100) = 10$.
- $\gcd(4, -6) = 2$.

For instance, notice 10 *is a common divisor of* 90 *and* 100 *(i.e.* $10 \mid 90$ *and* $10 \mid 100$*). Moreover, you can directly check that no number greater than* 10 *can be a common divisor of* 90 *and* 100. *Thus, it follows from Definition 4.34 that* $\gcd(90, 100) = 10$.

Moreover, notice that gcd *is not sensitive to the signs of the inputs. For instance, the argument in the preceding paragraph works equally well with* -90 *and* -100 *in the places of* 90 *and* 100*, respectively. As a result, we also obtain*

$$\gcd(-100,-90) = 10,$$
$$\gcd(100,-90) = 10,$$
$$\gcd(-100,90) = 10.$$

Finally, the second example is argued analogously—a quick check shows that 2 *is indeed a common divisor of* 4 *and* -6*, and that no other number larger than* 2 *can also be a common divisor of* 4 *and* -6*. Thus,* $\gcd(4,-6) = 2$*.*

Note. *One can also consider common divisors and greatest common divisors of more than two numbers by directly extending Definition 4.34. For example,*

$$\gcd(6,9,12) = 3, \qquad \gcd(16,-48,31) = 1.$$

Finally, we introduce some terminology for when two numbers share the least possible amount of positive common divisors—namely, only the number 1:

Definition 4.36. $a, b \in \mathbb{Z}$ *are* coprime *(or* relatively prime*) iff* $\gcd(a,b) = 1$.

Example 4.37. 5 *and* 7 *are coprime, since*

$$\gcd(5,7) = 1.$$

Indeed, no number larger than 1 *can be a common factor of* 5 *and* 7*. This is a consequence of the fact that both* 5 *and* 7 *are prime; see Proposition 4.40 (2) below.*

Example 4.38. *Numbers that are not prime can nonetheless be coprime with each other. For instance, neither* 144 *and* 625 *are prime, however* $\gcd(144,625) = 1$.

Next, we prove some elementary properties of greatest common divisors:

Proposition 4.39. *The following properties hold:*

(1) $\gcd(1, a) = 1$ *for any* $a \in \mathbb{Z}$.

(2) $\gcd(a, a) = |a|$ *for any* $a \in \mathbb{Z} \setminus \{0\}$.

Proof of Proposition 4.39. (1) Both $1 \mid 1$ and $1 \mid a$ trivially, so 1 is a common divisor of 1 and a. Moreover, 1 must be the largest common divisor, since $c \nmid 1$ for any integer $c > 1$ (since $\frac{1}{c} \notin \mathbb{Z}$). As a result, $\gcd(1, a) = 1$ by Definition 4.34.

(2) Observe that $|a| \mid a$ (since $|a| = a \cdot 1$ if $a \geq 0$, and $|a| = a \cdot (-1)$ if $a < 0$), hence $|a|$ is a common factor of a and a. In addition, if $c \in \mathbb{N}$ and $c > |a|$, then $c \nmid a$ (since $\frac{a}{c} \notin \mathbb{Z}$). Thus, it follows from Definition 4.34 that $\gcd(a, a) = |a|$. □

Observe that in Proposition 4.39 (2), we must exclude the pathological case $a = 0$, as we noted before that $\gcd(0, 0)$ does not exist. In particular, when $a = 0$, the part of the proof highlighted in red breaks down—if $c \in \mathbb{N}$ and $c > |a| = 0$, then $\frac{a}{c} = 0 \in \mathbb{Z}$.

Proposition 4.40. *The following properties hold:*

(1) *If* $a, b \in \mathbb{Z} \setminus \{0\}$ *and* $b \mid a$, *then* $\gcd(a, b) = |b|$.

(2) *If* p *and* q *are prime numbers and* $p \neq q$, *then* $\gcd(p, q) = 1$.

Proof of Proposition 4.40. (1) First, since $b \mid a$ and $b \mid b$, it follows that $|b|$ is a common divisor of a and b. Furthermore, if $c \in \mathbb{N}$ and $c > |b|$, then $c \nmid b$ (since $\frac{b}{c} \notin \mathbb{Z}$), hence it follows from Definition 4.34 that $\gcd(a, b) = |b|$.

(2) By Definition 4.27, the only positive divisors of p are 1 and p, and the only positive divisors of q are 1 and q. Since $p \neq q$, it follows that the only positive common divisor of p and q is 1, and hence $\gcd(p, q) = 1$. □

Notice that in Proposition 4.40 (1), we must again exclude the case when a or b is zero. Indeed, Proposition 4.40 (1) is false in this special case—for example, $0 \mid 0$, but

$$\gcd(0, 0) \neq 0.$$

The lesson here is that we must be very careful to avoid making incorrect statements.

Moreover, in the proof of Proposition 4.40 (1), the part highlighted in blue skipped a couple steps when concluding $|b|$ is a common divisor of a and b. This is because these steps were already present in earlier proofs. Can you fill in the missing details here?

4.5.1. *Euclid's Algorithm.* Suppose you are asked to compute $\gcd(75, 27)$. Since 75 and 27 are relatively small numbers, you could quite easily do this directly:

- List all the divisors of 75 and 27 individually.
- Identify all the common divisors of 75 and 27.
- Select the largest one for your answer.

Indeed, if you did the above, you would quickly see that 1 and 3 are the only common divisors of 75 and 27, and hence $\gcd(75, 27) = 3$. Not too bad at all.

Now, suppose you are instead asked to find

$$\gcd(149287653924, 3966543772721).$$

While you could theoretically repeat the above process, this would be far less pleasant (and far less practical, in terms of time required). Moreover, for real-world applications, one would need to work with much larger numbers than the above, so that even the newest computer may need longer than the lifetime of the universe to calculate the greatest common divisor directly. (This is not an exaggeration.)

Question 4.41. *Is there a (much) faster way to compute greatest common divisors?*

Fortunately, the answer is "yes"—there is a more clever and efficient method to compute greatest common divisors. The key to this method is the following connection between greatest common divisors and the division theorem (Theorem 4.33):

Proposition 4.42. *Let* $a, q, r \in \mathbb{Z}$ *and* $b \in \mathbb{N}$ *satisfy*

$$a = qb + r, \qquad 0 \leq r < b. \tag{4.9}$$

Then,

$$\gcd(a, b) = \gcd(b, r).$$

Note the relations (4.9) can be interpreted as dividing a by b, in the sense of Theorem 4.33. Thus, Proposition 4.42 states that to compute $\gcd(a, b)$, we need only divide a by b, obtain the remainder r from this division, and then compute $\gcd(b, r)$.

Proof of Proposition 4.42. By Definition 4.34, it suffices to show that b and r have exactly the same common divisors as a and b. Let us fix now $d \in \mathbb{Z}$.

- Suppose first that $d \mid a$ and $d \mid b$. Then, there exist $k, l \in \mathbb{Z}$ such that $a = dk$ and $b = dl$. From (4.9), we can then compute

$$\begin{aligned} r &= \underbrace{a - qb}_{dk - q(dl)} \\ &= d(k - ql), \end{aligned}$$

  and hence $d \mid r$. Thus, we have obtained $d \mid b$ and $d \mid r$.
- Conversely, suppose that $d \mid b$ and $d \mid r$. Then, $b = dk$ and $r = dl$ for some $k, l \in \mathbb{Z}$. Once again, by a direct computation using (4.9), we have

$$\begin{aligned} a &= \underbrace{qb + r}_{q(dk)+dl} \\ &= d(qk + l), \end{aligned}$$

  and hence $d \mid a$. As a result, we have obtained $d \mid a$ and $d \mid b$. □

Regarding the proof of Proposition 4.42, observe that it suffices to prove the statement highlighted in red, since if a, b and b, r have the same common divisors, then they must also have the same largest common divisor. Now, the red statement can be expanded as

$$\forall_{d \in \mathbb{Z}}((d \mid a \text{ and } d \mid b) \Leftrightarrow (d \mid b \text{ and } d \mid r)).$$

This can be proved directly via the usual methods. We first fix an arbitrary $d \in \mathbb{Z}$, and we then prove the equivalence within the "∀". For this, we appeal to Figure 2.9:

- The first bullet point in the proof shows $(d \mid a \text{ and } d \mid b) \Rightarrow (d \mid b \text{ and } d \mid r)$.
- The second bullet point in the proof shows $(d \mid b \text{ and } d \mid r) \Rightarrow (d \mid a \text{ and } d \mid b)$.

Now, Proposition 4.42 leads us to Euclid's algorithm—a new and improved technique for computing greatest common divisors. Again, the idea is that if a and b are very large numbers, then Proposition 4.42 *reduces finding* $\gcd(a, b)$ *to the problem of finding* $\gcd(b, r)$, *for smaller numbers* b *and* r *obtained via division.* This is especially useful, since it is much, much faster to divide large numbers than it is to find their divisors. Furthermore, we can repeat this process over and over again, until we have reduced $\gcd(a, b)$ to the greatest common divisor of two much smaller numbers.

This is most easily demonstrated via a couple concrete examples:

Example 4.43. *Let us apply Euclid's algorithm to compute* $\gcd(75, 27)$*:*

- *First, we divide* 75 *by* 27 *as in Theorem 4.33:*

$$\underbrace{75}_{a} = \underbrace{2}_{q} \times \underbrace{27}_{b} + \underbrace{21}_{r}.$$

Thus, applying Proposition 4.42, we conclude that

$$\gcd(75, 27) = \gcd(27, 21).$$

- *Next, repeat the above process and divide* 27 *by* 21*:*

$$\underbrace{27}_{a} = \underbrace{1}_{q} \cdot \underbrace{21}_{b} + \underbrace{6}_{r}.$$

Thus, by Proposition 4.42,

$$\gcd(27, 21) = \gcd(21, 6).$$

- *Continuing on, we divide* 21 *and* 6*:*

$$\underbrace{21}_{a} = \underbrace{3}_{q} \cdot \underbrace{6}_{b} + \underbrace{3}_{r}.$$

Thus, by Proposition 4.42,

$$\gcd(21, 6) = \gcd(6, 3).$$

- *Dividing* 6 *by* 3*, we obtain*

$$\underbrace{6}_{a} = \underbrace{2}_{q} \cdot \underbrace{3}_{b} + \underbrace{0}_{r}.$$

Since there is no remainder, then $3 \mid 6$*, so by Proposition 4.40 (1),*

$$\gcd(6, 3) = 3.$$

Finally, combining all the above equalities in blue, we conclude $\gcd(75, 27) = 3$.

For clarity, Example 4.43 explained Euclid's algorithm in full detail. However, once you are comfortable, the calculations can be presented in a more streamlined manner:

Example 4.44. *We now apply Euclid's algorithm to compute* $\gcd(144, 112)$*:*

$$144 = 1 \cdot 112 + 32 \quad \Rightarrow \quad \gcd(144, 112) = \gcd(112, 32),$$

$$112 = 3 \cdot 32 + 16 \quad \Rightarrow \quad \gcd(112, 32) = \gcd(32, 16),$$
$$32 = 2 \cdot 16 + 0 \quad \Rightarrow \quad \gcd(32, 16) = 16.$$

Thus, we conclude $\gcd(144, 112) = 16$.

Note the computations in Examples 4.43–4.44 are entirely systematic, in that they can be carried out in mindless autopilot once you know the steps. As a result, Euclid's algorithm can be easily implemented on a computer in a language of your choice (e.g. Python). Here, we give a pseudo-code description of Euclid's algorithm:

Euclid's algorithm		*Comments*
$\gcd(a, b)$:		Assume $a, b \in \mathbb{N}$ and $a \geq b$.
• Find q, r such that $a = qb + r$ and $0 \leq r < b$.		Divide a by b.
• If $r = 0$, then return b.		$b \mid a$, so $\gcd(a, b) = b$.
• If $r \neq 0$, then return $\gcd(b, r)$.		Applying Proposition 4.42.

That's it—super simple. With just a few lines of code, a computer can calculate greatest common divisors of incredibly large numbers very quickly. Try it yourself!

4.5.2. *Bézout's Identity.* Thus far, we have presented Euclid's algorithm as an efficient way to compute greatest common divisors. However, this by itself does not quite unlock the full potential of the algorithm. If we push the process a bit further, then we can extract even more useful information from the greatest common divisor.

To describe this extended algorithm, let us first recall works how Euclid's algorithm computes $\gcd(a_1, a_2)$, for general natural numbers $0 < a_2 \leq a_1$:

- Dividing and applying Proposition 4.42, we obtain
$$a_1 = q_1 a_2 + a_3, \quad 0 < a_3 < a_2, \qquad \gcd(a_1, a_2) = \gcd(a_2, a_3).$$
- Repeating the above with a_2 and a_3, we obtain
$$a_2 = q_2 a_3 + a_4, \quad 0 < a_4 < a_3, \qquad \gcd(a_2, a_3) = \gcd(a_3, a_4).$$
- This process continues...
$$\vdots$$
$$a_{t-2} = q_{t-2} a_{t-1} + a_t, \quad 0 < a_t < a_{t-1}, \qquad \gcd(a_{t-2}, a_{t-1}) = \gcd(a_{t-1}, a_t).$$
- ... until reach a step when the remainder in the divison is zero:
$$a_{t-1} = q_{t-1} a_t + 0, \qquad \gcd(a_{t-1}, a_t) = a_t.$$

We could then conclude $\gcd(a_1, a_2) = a_t$ and call it a day.

But we can do more! In fact, if we reverse the computations that led us to our answer $\gcd(a_1, a_2)$, then we can derive a formula for $\gcd(a_1, a_2)$ in terms of a_1 and a_2. From the last two steps of the preceding computation, we can write

$$\begin{aligned}\gcd(a_1, a_2) &= a_t \\ &= 1 \cdot a_{t-2} - q_{t-2}a_{t-1} \qquad (\text{since } a_{t-2} = q_{t-2}a_{t-1} + a_t).\end{aligned}$$

We have now written $\gcd(a_1, a_2)$ as an integer linear combination of a_{t-2} and a_{t-1}.

If we unwind one more step of Euclid's algorithm (not shown in previous computations), then we can write $\gcd(a_1, a_2)$ as an integer linear combination of a_{t-3} and a_{t-2}:

$$\begin{aligned}\gcd(a_1, a_2) &= 1 \cdot a_{t-2} - \underbrace{q_{t-2}a_{t-1}}_{q_{t-2}(a_{t-3} - q_{t-3}a_{t-2})} \\ &= (1 + q_{t-2}q_{t-3})a_{t-2} - q_{t-2}a_{t-3}.\end{aligned}$$

If we keep unwinding more steps, then we obtain $\gcd(a_1, a_2)$ in terms of a_k and a_{k+1} for successively smaller k's. If we continue all the way to the beginning of Euclid's algorithm, then we obtain $\gcd(a_1, a_2)$ as an integer linear combination of a_1 and a_2:

$$\gcd(a_1, a_2) = ua_1 + va_2, \qquad u, v \in \mathbb{Z}.$$

The above computations lead to a proof of the following property, known as Bézout's identity (after French mathematician Étienne Bézout, 1730–1783):

Theorem 4.45 (Bézout's identity). *For any $a, b \in \mathbb{Z} \setminus \{0\}$, there exist $u, v \in \mathbb{Z}$ with*

$$\gcd(a, b) = ua + vb.$$

To make the discussion more concrete, let us now demonstrate with some examples:

Example 4.46. *Let us first apply Euclid's algorithm to $\gcd(60, 17)$:*

$$\begin{aligned} 60 = 3 \cdot 17 + 9 \quad &\Rightarrow \quad \gcd(60, 17) = \gcd(17, 9), \\ 17 = 1 \cdot 9 + 8 \quad &\Rightarrow \quad \gcd(17, 9) = \gcd(9, 8), \\ 9 = 1 \cdot 8 + 1 \quad &\Rightarrow \quad \gcd(9, 8) = \gcd(8, 1), \\ 8 = 8 \cdot 1 + 0 \quad &\Rightarrow \quad \gcd(8, 1) = 1. \end{aligned}$$

Thus, $\gcd(60, 17) = 1$; in particular, 60 and 17 are coprime.

Unwinding Euclid's algorithm, we then compute

$$\begin{aligned} 1 &= 1 \cdot 9 - 1 \cdot 8 \\ &= \underbrace{1 \cdot 9 - 1 \cdot (17 - 1 \cdot 9)}_{-1 \cdot 17 + 2 \cdot 9} \\ &= \underbrace{-1 \cdot 17 + 2(60 - 3 \cdot 17)}_{2 \cdot 60 - 7 \cdot 17}. \end{aligned}$$

(Here, we have colour-coded the steps to make more clear what was applied at each step.) Thus, we can write $\gcd(60, 17) = 1$ *as an integer linear combination of* 60 *and* 17*:*

$$1 = 2 \cdot 60 - 7 \cdot 17. \tag{4.10}$$

Example 4.47. *Let us revisit the computations for* $\gcd(75, 27) = 3$ *from Example 4.43:*

$$\begin{aligned} 75 = 2 \cdot 27 + 21 \quad &\Rightarrow \quad \gcd(75, 27) = \gcd(27, 21), \\ 27 = 1 \cdot 21 + 6 \quad &\Rightarrow \quad \gcd(27, 21) = \gcd(21, 6), \\ 21 = 3 \cdot 6 + 3 \quad &\Rightarrow \quad \gcd(21, 6) = \gcd(6, 3), \\ 6 = 2 \cdot 3 + 0 \quad &\Rightarrow \quad \gcd(6, 3) = 3. \end{aligned}$$

Reversing the above computations, we can hence write $\gcd(6, 3)$ *as*

$$\begin{aligned} 3 &= 21 - 3 \cdot 6 \\ &= \underbrace{21 - 3(27 - 1 \cdot 21)}_{-3 \cdot 27 + 4 \cdot 21} \\ &= \underbrace{-3 \cdot 27 + 4(75 - 2 \cdot 27)}_{4 \cdot 75 - 11 \cdot 27}. \end{aligned}$$

Thus, we can write $\gcd(75, 27) = 3$ *in terms of* 75 *and* 27 *as*

$$3 = 4 \cdot 75 - 11 \cdot 27. \tag{4.11}$$

Bézout's identity gives one reason that coprimality is desirable. Consider, for instance, the setting of Example 4.46. Since 60 and 17 are coprime, we could write the formula (4.10) thanks to Bézout's identity. One consequence of this is that *we can also write any* $c \in \mathbb{Z}$ *as an integer linear combination of* 60 *and* 17—namely,

$$c = (2c) \cdot 60 - (7c) \cdot 17.$$

One should contrast this with the setting of Example 4.47. Here, because of (4.11), we can write any multiple of $\gcd(75, 27) = 3$ in terms of 75 and 27:

$$3c = (4c) \cdot 75 - (11c) \cdot 27, \qquad c \in \mathbb{Z}.$$

On the other hand, *there is no way to write* 1 *as an integer linear combination of* 75 *and* 27. (To prove this, one can observe that $\gcd(75, 27) = 3$ must be a divisor of any integer linear combination of 75 and 27; see Proposition 4.23.) Thus, unlike 60 and 17, there are limitations to what one can obtain with integer linear combinations of 75 and 27.

You may (should!) wonder *why one would want to work with integer linear combinations in the first place.* While the details are well beyond the scope of this module, such equations do play important roles in cryptography and coding theory. In particular, number theory plays a fundamental role in most modern encryption schemes.

4.5.3. *Least Common Multiples.* We conclude this section discussing a concept that is roughly the direct opposite of greatest common divisors:

Definition 4.48. *Let* $a, b \in \mathbb{Z}$.

- $d \in \mathbb{Z}$ *is a common multiple of* a *and* b *iff* $a \mid d$ *and* $b \mid d$.
- *The least common multiple of* a *and* b *is the smallest number* $d \in \mathbb{N}$ *that is a common multiple of* a *and* b. *Formally, this can written as*

$$d = \operatorname{lcm}(a, b) \Leftrightarrow (a \mid d \text{ and } b \mid d \text{ and } \forall_{c \in \mathbb{N}}((a \mid c \text{ and } b \mid c) \Rightarrow d \leq c)).$$

Note Definition 4.48 is analogous to Definition 4.34 for the greatest common divisor, except the divisibility relations have been reversed. In particular, any common multiple of $a, b \in \mathbb{N}$ is greater than or equal to a and b (as opposed to smaller than or equal to for common divisors). Thus, here it is relevant to take the *least* common multiple.

For small numbers, the least common multiple can be computed directly:

Example 4.49. *By a direct computation, we obtain*

$$\operatorname{lcm}(4, 6) = 12.$$

Notice that 12 *is a common multiple of* 4 *and* 6 *(since* $4 \mid 12$ *and* $6 \mid 12$*). Moreover, you can directly check that no positive number less than* 12 *can be a common multiple of* 4 *and* 6. *Thus, it follows from Definition 4.48 that* $\operatorname{lcm}(4, 6) = 12$.

In addition, lcm *is, like* gcd*, not sensitive to the signs of the inputs, since the above argument still works when* 4 *and* 6 *are replaced by* -4 *and* 6*, respectively. As a result,*

$$\gcd(-4,-6) = 10,$$
$$\gcd(4,-6) = 10,$$
$$\gcd(-4,6) = 10.$$

Example 4.50. *Below are some additional examples of least common multiples:*

- $\operatorname{lcm}(90,100) = 900$.
- $\operatorname{lcm}(75,27) = 675$.

How might one compute least common multiples of larger numbers, in particular when checking for common multiples becomes prohibitively time-consuming? There is actually very little that we need to say here besides the following theorem, which directly relates the least common multiple to the greatest common divisor:

Proposition 4.51. *For any* $a, b \in \mathbb{N}$*, the following formula holds:*

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab. \tag{4.12}$$

Therefore, to calculate $\operatorname{lcm}(a,b)$ efficiently when a and b are large, we need only find $\gcd(a,b)$ using Euclid's algorithm, and then calculate

$$\operatorname{lcm}(a,b) = \tfrac{ab}{\gcd(a,b)}.$$

Before proving Proposition 4.51, let us first give a couple examples:

Example 4.52. *In Example 4.44, we applied Euclid's algorithm to calculate*

$$\gcd(144,112) = 16.$$

As a result, by Proposition 4.51, we immediately obtain

$$\begin{aligned}\operatorname{lcm}(144,112) &= \tfrac{144\cdot 112}{16} \\ &= 1008.\end{aligned}$$

Example 4.53. *In Example 4.47, we used Euclid's algorithm to compute*

$$\gcd(75, 27) = 3.$$

Then, by Proposition 4.51, we obtain

$$\begin{aligned} \operatorname{lcm}(75, 27) &= \tfrac{75 \cdot 27}{3} \\ &= 675. \end{aligned}$$

The proof of Proposition 4.51, given below, is more involved than most others you have seen so far. However, the proof uses the same ideas as before, so it should be accessible with a bit of patience, if you have understood most things up to now.

Proof of Proposition 4.51. For convenience, we define the quantities

$$g = \gcd(a, b), \qquad l = \operatorname{lcm}(a, b). \tag{4.13}$$

Since $g \mid a$ and $g \mid b$, it follows that $\frac{a}{g}, \frac{b}{g} \in \mathbb{N}$. Also, since we can write

$$\tfrac{ab}{g} = a \cdot \tfrac{b}{g} = b \cdot \tfrac{a}{g},$$

it follows that $\frac{ab}{g} \in \mathbb{N}$ is a common multiple of a and b.

Next, we claim there exists $q \in \mathbb{N}$ such that

$$\tfrac{ab}{g} = lq. \tag{4.14}$$

To show this, we apply Theorem 4.33 to write

$$\tfrac{ab}{g} = ql + r, \qquad q, r \in \mathbb{Z}, \quad 0 \le r < l. \tag{4.15}$$

Since $\frac{ab}{g}$ and l are common multiples of a and b, it follows that

$$r = \tfrac{ab}{g} - ql$$

is also a common multiple of a and b (see Proposition 4.23). Now, if $0 < r < l$, then this contradicts that l is the least common multiple of a and b. As a result, we have $r = 0$, hence (4.15) yields $\frac{ab}{g} = lq$. Note also that q is positive, since both $\frac{ab}{g}$ and l are positive; this shows $q \in \mathbb{N}$ and proves the claim (4.14).

Since l is a common multiple of a and b, then $\frac{l}{a}, \frac{l}{b} \in \mathbb{N}$, hence by (4.14),

$$a = qg \cdot \tfrac{l}{b}, \qquad b = qg \cdot \tfrac{l}{a}.$$

The above implies that qg is a common divisor of a and b. Now, if $q > 1$, then this contradicts that g is the greatest common divisor of a and b. As a result, $q = 1$, and we conclude from (4.14) that $\frac{ab}{g} = l$, which is precisely (4.12). □

Note we included a bit less detail in the proof of Proposition 4.51 than before, since you already have some experience with proofs at this point.

4.6. **Prime Factorisations.** To finish off our exploration of the natural numbers and integers, we return once again to factoring numbers. Recall that a composite number n can be factored into the product of two smaller natural numbers,

$$n = kl, \qquad k, l \in \{2, 3, \ldots, n-1\}.$$

Moreover, if k or l is composite, then it can be further factored. Thus, by factoring repeatedly until we cannot continue any further, we could then express n as a product of prime numbers. This process is known as prime factorisation.

Definition 4.54. *Let $n \in \mathbb{N} \setminus \{1\}$. Then, a (finite) product*

$$\prod_{k=1}^{m} p_k = p_1 p_2 \ldots p_m.$$

is called a prime factorisation of n iff the following hold:

- *Each $p_1, p_2, \ldots, p_m$ is a prime number.*
- $n = p_1 p_2 \ldots p_m$.

Note. *As in Definition 4.54, products can generally be expressed using $\prod$-notation:*

$$\prod_{k=a}^{b} x_k = x_a \cdot x_{a+1} \cdot \cdots \cdot x_{b-1} \cdot x_b.$$

This is analogous to Σ-notation, except here we have products rather than sums. Like for Σ-notation, k is a dummy variable that only makes sense within the "$\prod$".

A prime factorisation of $n \in \mathbb{N} \setminus \{1\}$ can be viewed as a decomposition of n into its simplest "atomic" parts. In particular, one can think of a prime factorisation of n as the individual building blocks that make up the number n.

For small numbers, one can compute their prime factorisations by brute force:

Example 4.55. *To factor* 60 *into primes, we write* 60 *as the product of smaller numbers, and we repeat this for each ensuing factor until all the factors become prime:*

$$\begin{aligned} 60 &= 2 \cdot \underbrace{30}_{2\cdot 15} \\ &= 2 \cdot 2 \cdot \underbrace{15}_{3\cdot 5} \\ &= 2 \cdot 2 \cdot 3 \cdot 5. \end{aligned}$$

To save ourselves some writing, we can group together copies of the same prime number:

$$60 = 2^2 \cdot 3 \cdot 5.$$

Example 4.56. *Similarly,* 144 *can be factored into primes in the following way:*

$$\begin{aligned} 144 &= \underbrace{12}_{2\cdot 2\cdot 3} \cdot \underbrace{12}_{2\cdot 2\cdot 3} \\ &= 2^4 \cdot 3^2. \end{aligned}$$

4.6.1. *The Fundamental Theorem of Arithmetic.* Now, you may be wondering *when one can factor a number into a product of primes*, or *how many ways a number can be factored into primes*. The answer to these is given by the theorem below, which is important enough to be known as the fundamental theorem of arithmetic.

Theorem 4.57 (Fundamental theorem of arithmetic)**.** *Let* $n \in \mathbb{N} \setminus \{1\}$. *Then:*

(1) *(Existence)* n *has a prime factorisation,* $n = p_1 p_2 \dots p_m$.
(2) *(Uniqueness) Suppose* $n = q_1 q_2 \dots q_l$ *is another prime factorisation of* n. *Then* $l = m$, *and, after reordering the prime factors* $q_1, \dots, q_l$, *we have that*

$$p_i = q_i \quad \textit{for all } i \in \{1, 2, \dots, m\}.$$

Roughly speaking, Theorem 4.57 states that *every composite number can be factored into a product of prime numbers in exactly one way*. In particular, since there is only one prime factorisation for any $n \in \mathbb{N} \setminus \{1\}$, we can refer to this as *the* prime factorisation of n.

To make the presentation more clear, we will separate the proof of Theorem 4.57 into different parts. We begin by proving the existence of prime factorisations:

Proof of Theorem 4.57 (1). We prove this part by strong induction. First, for the base case, we note that 2 has a trivial prime factorisation:

$$2 = 2.$$

For the inductive case, we fix any $n \in \mathbb{N} \setminus \{1\}$, and we suppose $2, 3, \ldots, n$ all have prime factorisations. Turning now to $n+1$, we see from Proposition 4.29 that there is a prime number p such that $p \mid (n+1)$. Since, $n+1$ and p are both positive, we can write $n+1 = pk$ for some $k \in \mathbb{N}$. We now split into cases:

- If $k = 1$, then $n+1 = p$ is a prime factorisation of $n+1$.
- Otherwise, we have $1 < k < n+1$. (Since $p > 1$, then $k = \frac{n+1}{p} < n+1$.) By the induction hypothesis, k has a prime factorisation,

  $$k = q_1 q_2 \ldots q_m.$$

  As a result, we can factor $n+1$ into primes as

  $$n+1 = p q_1 q_2 \ldots q_m.$$

Thus, $n+1$ has a prime factorisation in call cases, completing the proof. □

The above proof is another example of strong induction. Here, we set

- $P(n)$: "n has a prime factorisation".

The only tricky part is in the inductive case—if $n+1$ is composite, we factor $n+1$ into two smaller numbers, which already have prime factorisations by the induction hypothesis.

Now, before we prove the uniqueness part of Theorem 4.57, we will need the following result, which is quite useful and famous in its own right:

Proposition 4.58 (Euclid's lemma)**.** *Let p be a prime number, and suppose $a, b \in \mathbb{N}$ satisfy that $p \mid (ab)$. Then, either $p \mid a$ or $p \mid b$.*

There are several different ways that one could prove Euclid's lemma. One short and clever method to do this makes use of Bézout's identity:

Proof of Proposition 4.58. First, observe that if $p \mid a$, then we are already done. Thus, we only need to consider the case in which we assume $p \nmid a$.

Since $p \nmid a$, we have that $\gcd(a, p) = 1$. (This follows because the only divisors of p are 1 and p, but p is not a divisor of a.) Consequently, applying Bézout's identity (Theorem 4.45), we see that there exist $u, v \in \mathbb{Z}$ with

$$ua + vp = 1, \qquad uab + vpb = b. \tag{4.16}$$

Since $p \mid (ab)$ by assumption, we have $p \mid (uab)$. Moreover, $p \mid (vpb)$ trivially by definition. As a result, Proposition 4.23 (2) yields $p \mid (uab + vpb)$. From the second part of (4.16), we obtain $p \mid b$, which completes the proof. □

The structure of the above proof may seem a bit unfamiliar due to the wording. However, logically speaking, this is nothing more than a standard proof by cases. Indeed, what is actually happening in the first paragraph is that we split the proof into two cases:

(1) $p \mid a$ *holds.* This case is trivial, since this immediately implies $p \mid a$ or $p \mid b$.
(2) $p \mid a$ *does not hold.* In this case, we use Bézout's identity in a clever way to show that $p \mid b$, which again implies $p \mid a$ or $p \mid b$.

The proof is then complete, since every case leads to the conclusion $p \mid a$ or $p \mid b$.

Euclid's lemma is applied widely throughout number theory. For our purposes, it will be the main tool we need to prove the remaining uniqueness side of Theorem 4.57.

Proof of Theorem 4.57 (2). We proceed by strong induction. For the base case, we note that 2 has only the trivial prime factorisation, $2 = 2$.

For the inductive case, we fix any $n \in \mathbb{N} \setminus \{1\}$, and we suppose $2, 3, \ldots, n$ all have unique prime factorisations (up to reordering of the factors). We now consider $n + 1$—that is, we suppose $n + 1$ can be factored into primes as:

$$n + 1 = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_l. \tag{4.17}$$

From here, the proof splits into two cases.

First, suppose $n + 1$ is prime. Then, the only possible factorisation of $n + 1$ into primes is the trivial one, $n + 1 = n + 1$. In other words,

$$l = m = 1, \qquad p_1 = q_1 = n + 1,$$

so that the prime factorisation of $n + 1$ is unique.

Next, suppose $n + 1$ is composite, so that both $m > 1$ and $l > 1$ in (4.17). Since $p_m \mid (n+1)$, and since $n+1 = q_1 q_2 \ldots q_l$ by (4.17), then by applying Euclid's lemma (Proposition 4.58) multiple times, we conclude that $p_m \mid q_j$ for some $j \in \{1, 2, \ldots, l\}$.

By reordering the factorisation, we can simply assume $p_m \mid q_l$. Moreover, since p_1 and q_1 are prime, then it must follow that $p_m = q_l$.

As a result, we have that $\frac{n}{p_m}$ can be factored into primes as

$$\frac{n}{p_m} = p_1 p_2 \dots p_{m-1} = q_1 q_2 \dots q_{l-1}.$$

By the inductive hypothesis, the prime factorisation of $\frac{n}{p_m}$ is unique—in other words, $m-1 = l-1$, and $p_1, p_2, \dots, p_{m-1}$ and $q_1, q_2, \dots, q_{l-1}$ are the same after reordering. Thus, it follows that $m = l$, and $p_1, p_2, \dots, p_m$ and $q_1, q_2, \dots, q_l$ are also the same after reordering (since $p_m = q_l$). From the above, we conclude that the prime factorisation of $n+1$ is unique, completing the proof of the inductive case. □

The structure of the strong induction in the above proof is the same as the one for Theorem 4.57 (1). The statement we consider here, for all $n \in \mathbb{N} \setminus \{1\}$, is

- $P(n)$: If $n = p_1 p_2 \dots p_m$ and $n = q_1 q_2 \dots q_l$ are prime factorisations, then $m = l$, and $p_1, p_2, \dots, p_m$ and $q_1, q_2, \dots, q_l$ are the same after reordering.

While $P(n)$ is a complicated statement, the inductive logic is the same as before.

Let us also further clarify how Euclid's lemma was applied in the inductive case. At the start, we used (4.17) to deduce $p_m \mid (q_1 q_2 \dots q_l)$. From here:

- We apply Euclid's lemma to conclude $p_m \mid q_1$ or $p_m \mid (q_2 q_3 \dots q_l)$.
- Applying Euclid's lemma again to the second case in the previous bullet point, we conclude that $p_1 \mid q_1$, $p_m \mid q_2$, or $p_m \mid (q_3 q_4 \dots q_l)$.
- By successively applying Euclid's lemma as before, we finally conclude "$p_m \mid q_1$, $p_m \mid q_2$, ..., $p_m \mid q_{l-1}$, or $p_m \mid q_l$"—i.e. $p_m \mid q_j$ for some $j \in \{1, 2, \dots, l\}$.

4.6.2. *Computational Applications.* Let us now put the fundamental theorem of arithmetic to use by demonstrating how prime factorisations can be used for computations.

First, *from the prime factorisation, we can reconstruct all the divisors of a number.* To see how this works, suppose $n \in \mathbb{N} \setminus \{1\}$ has prime factorisation $n = p_1 p_2 \dots p_m$, and let $d \in \mathbb{N} \setminus \{1\}$ be a divisor of n, with prime factorisation $d = q_1 q_2 \dots q_l$. Then, each q_j, $1 \leq j \leq l$ is a divisor of n, and Euclid's lemma tells us that $q_j = p_i$ for some $1 \leq i \leq m$.

In other words, d cannot contain primes in its factorisation that are not in n. Similarly, one can also see that d cannot contain more copies of a prime than are present in n. Thus, putting it all together, we can deduce that d *is a divisor of* n *if and only if* $q_1, q_2, \dots, q_l$ *is some sublist of the primes* $p_1, p_2, \dots, p_m$ *in* n. (We will not give a formal proof of this here, but the reasoning for that would proceed along the above lines.)

If the above seemed too abstract, then the following examples should clear things up:

Example 4.59. *While it is not difficult to find all the positive divisors of* 40 *directly, let us see how we can do this systematically from its prime factorisation.*

Proceeding as in Examples 4.55–4.56, we can factor 40 *as*

$$40 = 2^3 \cdot 5. \tag{4.18}$$

Then, the divisors of 40 *are given by products of the various prime numbers on the right-hand side of* (4.18)*. All the possible combinations are listed below:*

$2^0 \cdot 5^0 = 1$	$2^1 \cdot 5^0 = 2$	$2^2 \cdot 5^0 = 4$	$2^3 \cdot 5^0 = 8$
$2^0 \cdot 5^1 = 5$	$2^1 \cdot 5^1 = 10$	$2^2 \cdot 5^1 = 20$	$2^3 \cdot 5^1 = 40$

Thus, the following are all the divisors of 40*:*

$$1, 2, 4, 5, 8, 10, 20, 40.$$

By taking the previous example a bit further, *we can use the prime factorisation in a slick way to count how many positive divisors a number* n *has*:

Example 4.60. *Let us return to the number from Example 4.59:*

$$40 = 2^3 \cdot 5.$$

Expressing the work in Example 4.59 more concisely, we see that every divisor of 40 *is exactly of the form* $2^k \cdot 5^l$*, for* $k \in \{0, 1, 2, 3\}$ *and* $l \in \{0, 1\}$*.*

Thus, we need to see how many numbers there are in the above form. Observe that:

- *There are* 4 *different possible values for* k*.*
- *There are* 2 *different possible values for* l*.*

Thus, altogether there are $4 \times 2 = 8$ *possible values in* $2^k \cdot 5^l$ *for* k *and* l*. From this, we conclude that* 40 *has* 8 *positive divisors (which were listed in Example 4.59).*

Example 4.61. *For completeness, let us do a similar computation for* 504*. Note that by a direct computation, the prime factorisation of* 504 *is given by*

$$504 = 2^3 \cdot 3^2 \cdot 7.$$

Then, the divisors of 504 *are those numbers of the form*

$$2^k \cdot 3^l \cdot 7^m, \qquad k \in \{0, 1, 2, 3\}, \quad l \in \{0, 1, 2\}, \quad m \in \{0, 1\}.$$

Observe that there are 4, 3 *and* 2 *possible values for* k, l, *and* m *in the above listing, respectively. As a result, there are in total* $4 \cdot 3 \cdot 2 = 24$ *different possible values for* k, l, *and* m. *We henceforth conclude that* 504 *has* 24 *positive divisors.*

Finally, we can explicitly list all 24 *positive divisors of* 504*:*

$2^0 \cdot 3^0 \cdot 7^0 = 1$	$2^1 \cdot 3^0 \cdot 7^0 = 2$	$2^2 \cdot 3^0 \cdot 7^0 = 4$	$2^3 \cdot 3^0 \cdot 7^0 = 8$
$2^0 \cdot 3^1 \cdot 7^0 = 3$	$2^1 \cdot 3^1 \cdot 7^0 = 6$	$2^2 \cdot 3^1 \cdot 7^0 = 12$	$2^3 \cdot 3^1 \cdot 7^0 = 24$
$2^0 \cdot 3^2 \cdot 7^0 = 9$	$2^1 \cdot 3^2 \cdot 7^0 = 18$	$2^2 \cdot 3^2 \cdot 7^0 = 36$	$2^3 \cdot 3^2 \cdot 7^0 = 72$
$2^0 \cdot 3^0 \cdot 7^1 = 7$	$2^1 \cdot 3^0 \cdot 7^1 = 14$	$2^2 \cdot 3^0 \cdot 7^1 = 28$	$2^3 \cdot 3^0 \cdot 7^1 = 56$
$2^0 \cdot 3^1 \cdot 7^1 = 21$	$2^1 \cdot 3^1 \cdot 7^1 = 42$	$2^2 \cdot 3^1 \cdot 7^1 = 84$	$2^3 \cdot 3^1 \cdot 7^1 = 168$
$2^0 \cdot 3^2 \cdot 7^1 = 63$	$2^1 \cdot 3^2 \cdot 7^1 = 126$	$2^2 \cdot 3^2 \cdot 7^1 = 252$	$2^3 \cdot 3^2 \cdot 7^1 = 504$

In particular, it is far easier to not accidentally miss a divisor with this systematic approach compared to randomly searching for divisors of 504.

From the previous examples, you have hopefully noticed a pattern that can be extrapolated to any number. This is summarised in the following proposition:

Proposition 4.62. *Suppose* $n \in \mathbb{N} \setminus \{1\}$ *has prime factorisation*

$$n = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k} = \prod_{i=1}^{k} p_i^{l_i},$$

where $p_1, p_2, \dots, p_k$ *are distinct primes (that is,* $p_i \neq p_j$ *whenever* $i \neq j$*), and where* $l_1, l_2, \dots, l_k \in \mathbb{N}$. *Then, the total number of positive divisors of* n *is*

$$(l_1 + 1)(l_2 + 1) \dots (l_k + 1) = \prod_{i=1}^{k} (l_i + 1).$$

We can also use prime factorisations to compute greatest common divisors and least common multiples. As before, the process is easiest to demonstrate via examples:

Example 4.63. *Let us compute* $\gcd(24, 84)$ *using prime factorisations.*

First, the prime factorisations of 24 *and* 84 *are*

$$24 = 2^3 \cdot 3^1, \qquad 84 = 2^2 \cdot 3^1 \cdot 7^1.$$

From the relationship between divisors and prime factorisations discussed in Examples 4.60–4.61, we see that the common divisors of 24 *and* 84 *are precisely those obtained by*

multiplying prime numbers that are in the factorisations of both 24 and 84. Thus, the greatest common divisor $\gcd(24, 84)$ *is the number constructed by multiplying all the prime numbers that are in both prime factorisations.*

Now, the prime factors that are in both 24 and 84 are 2^2 *and* 3^1*. As a result,*

$$\begin{aligned}\gcd(24, 84) &= 2^2 \cdot 3^1 \\ &= 12.\end{aligned}$$

Example 4.64. *Let us compute* $\operatorname{lcm}(40, 60)$ *using prime factorisations.*

First, the prime factorisations of 40 and 60 are

$$40 = 2^3 \cdot 5^1, \qquad 60 = 2^2 \cdot 3^1 \cdot 5^1.$$

Observe now that the common multiples of 40 and 60 are precisely those numbers for which their prime factorisation contains all the prime divisors of both 40 and 60. As a result, the least common multiple $\operatorname{lcm}(40, 60)$ *is the number constructed only from the prime divisors of 40 and 60, and containing nothing else.*

To have all the prime divisors of 40 and 60, we need at least 2^3, 3^1, *and* 5^1*. Thus,*

$$\begin{aligned}\operatorname{lcm}(40, 60) &= 2^3 \cdot 3^1 \cdot 5^1 \\ &= 120.\end{aligned}$$

Examples 4.63–4.64 can be systematically adapted to apply to any numbers. For completeness, we summarise the general results in the following proposition:

Proposition 4.65. *Let* $m, n \in \mathbb{N} \setminus \{1\}$*, and suppose* m *and* n *can be written as*

$$m = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}, \qquad n = p_1^{s_1} p_2^{s_2} \dots q_k^{s_k}, \tag{4.19}$$

where $k \in \mathbb{N}$*, where* $p_1, p_2, \dots, p_k$ *are prime numbers, and where*

$$r_1, r_2, \dots, r_k, s_1, s_2, \dots, s_k \in \mathbb{N} \cup \{0\}.$$

Then, the following formulas hold:

$$\gcd(m, n) = p_1^{\min(r_1, s_1)} p_2^{\min(r_2, s_2)} \dots p_k^{\min(r_k, s_k)} = \prod_{i=1}^{k} p_i^{\min(r_i, s_i)},$$

$$\operatorname{lcm}(m,n) = p_1^{\max(r_1,s_1)} p_2^{\max(r_2,s_2)} \dots p_k^{\max(r_k,s_k)} = \prod_{i=1}^{k} p_i^{\max(r_i,s_i)}.$$

Notice that the equations in (4.19) are not necessarily prime factorisations, since any of the exponents r_i, s_i in the right-hand sides of the equations could be zero. Rather, here $p_1, p_2, \dots, p_k$ *represent all the prime numbers in the prime factorisations of either* m *or* n. For example, if p_1 is not in the prime factorisation of n, then $s_1 = 0$.

The upshot of the preceding discussions is that if we have the prime factorisations of numbers, then we could systematically compute many properties of these numbers. The issue, though, is that in applications, we often need to work with very large numbers, for which prime factorisations take impossibly long to compute. Thus, computation methods that use prime factorisations are highly impractical.

While this seems like quite bad news, the silver lining is that the intractability of finding prime factorisations itself leads to important applications, particularly in cryptography. In many encryption schemes used today, the key to decoding a message is the factorisation of an absurdly large number, and what prevents a stranger from snooping is that factoring this absurdly large number takes an incredibly long time! (If you are curious about this, then you can read about RSA encryption or take a cryptography module!)

4.7. **Rational Numbers.** We now turn our attention to the rational numbers, which go beyond the integers to all the fractions. There is not so much that needs to be said here, but we will briefly touch upon two particular points:

(1) How the rational numbers quantitatively differ from the integers.
(2) Why it is important to also look beyond the rational numbers.

On point (1), we recall that the integers are "discrete", in that they are uniformly spaced apart. More specifically, given integers $a, b \in \mathbb{Z}$ that are distinct (i.e. $a \neq b$), then

$$|a - b| \geq 1,$$

that is, a and b are at least one unit apart on the number line. In other words, each integer is isolated on an island apart from every other integer.

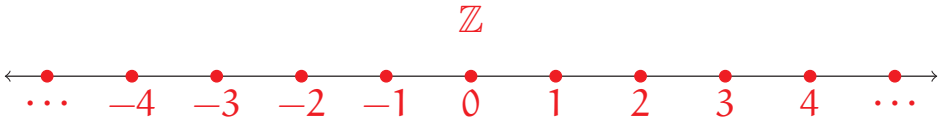


FIGURE 4.3. The integers, drawn as isolated points on the number line.

On the other hand, this "discreteness" no longer holds for $\mathbb{Q}$:

Example 4.66. *Given any rational number $a \in \mathbb{Q}$, the numbers $a + \frac{1}{n}$ are also rational for each $n \in \mathbb{N}$. Moreover, as n becomes arbitrarily large, $a + \frac{1}{n}$ becomes arbitrarily close to a; see Figure 4.4 further below. In other words, unlike for the integers, $a \in \mathbb{Q}$ is "not isolated on an island" apart from all other rational numbers.*

Note. *In the language of calculus, the above can be stated as*

$$\lim_{n \to \infty} \left(a + \tfrac{1}{n}\right) = a.$$

As a consequence of Example 4.66 above, the rational numbers are said to be "dense", meaning roughly that *near any $a \in \mathbb{Q}$, there are infinitely many other rational numbers that are clumped infinitely close to a*. In other words, *in terms of distance, there is no rational number that is isolated from all the other rational numbers.*

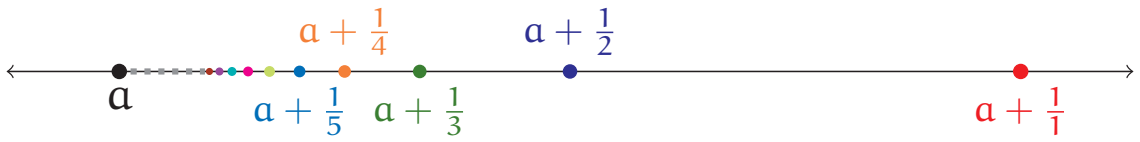


FIGURE 4.4. Illustration of Example 4.66. Given any $a \in \mathbb{Q}$ (in black), there are other rational numbers that are arbitrarily close to a (in various colours).

Another basic observation that also captures the "density" of $\mathbb{Q}$ is the following:

Proposition 4.67. *For any $a, b \in \mathbb{Q}$ with $a < b$, there exists $c \in \mathbb{Q}$ with $a < c < b$.*

Proof of Proposition 4.67. This holds, since $c = \frac{a+b}{2} \in \mathbb{Q}$ satisfies $a < c < b$. □

Intuitively, Proposition 4.67 states that *given any two distinct rational numbers a and b, there is always another rational number c that lies between a and b*. (Note the proof of Proposition 4.67 just chooses c to be the midpoint of a and b.) In particular, the rational numbers are plentiful enough to completely "fill the gaps" between two integers.

4.7.1. *An Irrational Discovery.* We have established that there are many rational numbers, so many that they are infinitely clumped together everywhere. However, does this mean that $\mathbb{Q}$ is large enough to contain every number that we wish to consider?

Spoiler: No!

Question 4.68. *Why is $\mathbb{Q}$ not enough to describe every number we care about?*

One fundamental answer to Question 4.68 is geometric in nature and dates back about 2500 years to ancient Greek mathematicians. Consider a right triangle, whose two perpendicular sides both have length 1, and let x denote the length of the remaining hypotenuse; see Figure 4.5 below. By the Pythagorean theorem, we know that

$$\begin{aligned} x^2 &= 1^2 + 1^2 \\ &= 2. \end{aligned}$$

In other words, the length of the hypotenuse should be "$\sqrt{2}$".

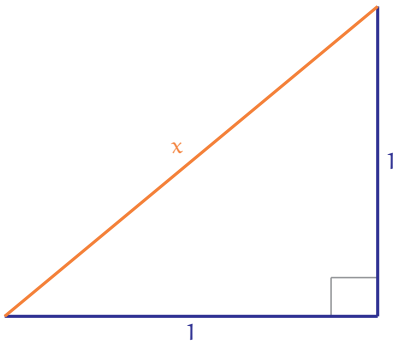


FIGURE 4.5. A right triangle whose two perpendicular sides have length 1. The length x of the hypotenuse cannot be a rational number.

Now, this hypotenuse length x is certainly a very natural quantity to consider. Thus, if the rational numbers are all that we care about, then x should also be rational, that is, a fraction. However, quite shockingly, ancient mathematicians discovered that:

Theorem 4.69. *There does not exist $q \in \mathbb{Q}$ such that $q^2 = 2$.*

Less formally, Theorem 4.69 states that $\sqrt{2}$ *is not a rational number.* Thus, if we are speak about "$\sqrt{2}$", or about the hypotenuse length of the above right triangle, then we will have to look further beyond the rational numbers in order to make sense of this.

Proof of Theorem 4.69. Assume, for a contradiction, that there does exist $q \in \mathbb{Q}$ satisfying $q^2 = 2$. By definition, we can write $q = \frac{a}{b}$, for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Furthermore, we can assume that either a or b is odd. (If both a and b are even, then we can replace a and b by $\frac{a}{2}$ and $\frac{b}{2}$, respectively, without changing the value of q. Moreover, we can repeat this indefinitely until one of a and b is odd.)

Since $q^2 = 2$ and $q^2 = \frac{a^2}{b^2}$, we have

$$a^2 = 2b^2, \tag{4.20}$$

hence a^2 is even. It then follows (see Example 2.65) that a is even as well, hence we can write $a = 2k$ for some $k \in \mathbb{Z}$. But then, recalling (4.20), we can write

$$2b^2 = \underbrace{(2k)^2}_{4k^2}, \qquad b^2 = 2k^2.$$

As a result, b^2 is even, and it follows that b is even.

The above shows that both a and b are even, which contradicts our previous conclusion that a or b is odd. Thus, there cannot be any $q \in \mathbb{Q}$ with $q^2 = 2$. □

The intuitive idea is that even though $\mathbb{Q}$ is "dense", it still has "infinitesimally small holes" everywhere, where there are missing numbers. One example of such a "hole" is at $\sqrt{2}$, but there are many more. (Some other examples include $\sqrt{3}$, $\sqrt[3]{2}$, π, and e, which also cannot be rational numbers.) To make up for this deficiency, we will need to look at the larger class of real numbers, which are designed precisely to "fill in these holes".

4.8. **Real Numbers.** Previously, we were extremely vague in our description of what real numbers are, We have only briefly mentioned the "real number line", but without explaining what this is or where this comes from.

This motivates the question—*how exactly do the real numbers extend the rational number system to fill in the "missing numbers"* (such as $\sqrt{2}$) *described in the previous section*? Now, there are multiple ways to rigorously define the set $\mathbb{R}$ to accomplish this. We now informally describe one intuitive method, which is via *infinite decimal expansions*. (We will look at another method in bonus material at the end of Chapter 5.)

To see how this works, let us apply this to $\sqrt{2}$:

Example 4.70. *Let us construct the infinite decimal expansion for $\sqrt{2}$. Each step below, given by an individual bullet point, provides the expansion to one additional digit:*

- *First, since $1^2 < 2 < 2^2$, we have $1 < \sqrt{2} < 2$. As a result, the leading digit of our decimal expansion for $\sqrt{2}$ must be "1".*
- *Next, since $(1.4)^2 < 2 < (1.5)^2$, we have $1.4 < \sqrt{2} < 1.5$. Therefore, the first two digits of our decimal expansion for $\sqrt{2}$ is "1.4".*
- *Next, since $(1.41)^2 < 2 < (1.42)^2$, we have $1.41 < \sqrt{2} < 1.42$. Thus, the first three digits of our decimal expansion for $\sqrt{2}$ is "1.41".*

By continuing the above, we obtain successively better decimal approximations for $\sqrt{2}$.

The idea is that by running the above process indefinitely, we will obtain an infinite decimal expansion that exactly describes $\sqrt{2}$. In particular, we have

$$\sqrt{2} = 1.414213562\ldots,$$

though for practical reasons, we only list the first few digits of the expansion.

Infinite decimal expansions can also be used to describe other numbers:

Example 4.71. *Any rational number can be described by an infinite decimal expansion. Some simple example of this include the following:*

- $\frac{1}{2} = 0.500000\ldots$.
- $-\frac{1}{3} = -0.333333\ldots$.
- $\frac{322}{5} = 64.40000\ldots$.

Example 4.72. *As we saw earlier, there are many familiar real numbers that we know are not rational (such numbers are called irrational). These can still be described using infinite decimal expansions, though the digits tend to not satisfy any pattern, e.g.*

- $\sqrt{2} = 1.414213562\ldots$.
- $\pi = 3.14159265\ldots$.
- $e = 2.718281828\ldots$.

Since infinite decimal expansions seem to capture the "missing" numbers, the idea is that we now *define the real numbers $\mathbb{R}$ to be the set of all infinite decimal expansions* (though with one caveat, see below). In other words, *by allowing for all infinite decimal expansions, rather than only the expansions corresponding to fractions, we can successfully fill in all the aforementioned "holes" between rational numbers.*

Now, there is a good reason why we did not put the above into a nice, formal definition. This is because this definition does not quite work as written. The issue is that *two different infinite decimal expansions could describe the same number*!

Example 4.73. *The number* 1 *can be described by two different decimal expansions:*

$$1 = 1.0000000\ldots, \qquad 1 = 0.99999999\ldots.$$

The first expansion is clear, but let us see why the second expansion also produces 1*.*

Recalling the meaning of decimal digits (i.e. each digit corresponds to a particular power of 10*), we can write the second decimal expansion as an infinite series:*

$$\begin{aligned} 0.99999999\ldots &= \tfrac{9}{10} + \tfrac{9}{100} + \tfrac{9}{1000} + \ldots \\ &= \sum_{k=1}^{\infty} \underbrace{9 \cdot 10^{-k}}_{\frac{9}{10}\cdot(\frac{1}{10})^{k-1}}. \end{aligned}$$

If you have some calculus experience, then you may recognise this as a geometric series:

$$\begin{aligned} 0.99999999\ldots &= \frac{9}{10} \sum_{k=0}^{\infty} \left(\tfrac{1}{10}\right)^k \\ &= \frac{9}{10} \cdot \frac{1}{1 - \frac{1}{10}} \qquad \textit{(formula for geometric series)} \\ &= 1. \end{aligned}$$

(If you have not seen infinite or geometric series before, then you can skip the above details for now. You will certainly encounter this soon!)

Due to the above, if we are to give a precise and correct definition of the real numbers, then we must *define* $\mathbb{R}$ *to be the set of all infinite decimal expansions, with the caveat that any two expansions that should represent the same number* (such as the pair in Example 4.73) *should be considered "the same"*. Here, for the sake of conciseness, we will avoid giving a full formal definition of $\mathbb{R}$ (though do see the bonus discussion at the end of the chapter); in practice, though, it is fine to just think of real numbers as decimal expansions, as long as you keep exceptions such as Example 4.73 in mind.

Having defined $\mathbb{R}$, in one way or another, we recall one last bit of terminology:

Definition 4.74. *An element of* $\mathbb{R} \setminus \mathbb{Q}$ *is called an irrational number.*

As we saw before, examples of irrational numbers include $\sqrt{2}$, $\sqrt[3]{2}$, π, and e.

4.8.1. *Upper and Lower Bounds.* In the remainder of this section, we present another way to capture this property that *the real number system no longer has the holes that were present in the rational number system.* However, before we can accomplish this, we first require a bit of background material and a few definitions.

We begin our discussion with the following motivating examples:

Example 4.75. *Consider the following sets:*

$$A = \{1, 3, 5, 7\}, \qquad B = \{a \in \mathbb{Z} \mid a < 0\}.$$

- *Observe that* A *has* 7 *as its maximum (i.e. largest) element. This holds because* $7 \in A$*, and because all the other elements of* A *(i.e.* $1, 3, 5$*) are less than* 7*.*
- *Similarly, the set* B *of all negative integers has* -1 *as its maximum element, since* $-1 \in B$*, and since all other elements of* B *are less than* -1*.*

Example 4.76. *On the other hand, the following sets do not have a maximum element:*

$$C = \{q \in \mathbb{Q} \mid q < 0\}, \qquad D = \{x \in \mathbb{R} \mid x < 0\}. \tag{4.21}$$

To see why this is the case, observe that:

- *No element* $q \in C$ *can be the maximum of* C*, since, e.g.,* $\frac{q}{2} \in C$ *and* $q < \frac{q}{2}$*.*
- *Similarly, no* $x \in D$ *can be the maximum of* D*, since* $\frac{x}{2} \in D$ *and* $x < \frac{x}{2}$*.*

Now, although the sets C and D in Example 4.76 do not have a maximum element, they "almost do". Here, the rough idea is that *we can think of* 0 *as "almost the maximum element of* C*"*, since 0 is just barely bigger than every element of C, but $0 \notin C$. By the same reasoning, *we can also view* $0 \notin D$ *as "almost the maximum element of* D*"*.

The above is a bit vague to work with. Thus, in the following, we develop the precise definitions needed to capture this notion of "almost maximum element".

Definition 4.77. *Let* $A \subseteq \mathbb{R}$*, and let* $y \in \mathbb{R}$*.*

- *We say that* y *is an upper bound for* A *iff* $x \leq y$ *for every* $x \in A$*, i.e.*

$$\forall_{x \in A} x \leq y.$$

- *Similarly, y is a lower bound for A iff $x \geq y$ for every $x \in A$, i.e.*

$$\forall_{x \in A} x \geq y.$$

In other words, *an upper bound of A is any number that is larger than or equal to every element of A*. Similarly, *a lower bound of A is any number that is smaller than or equal to each element of A*. Let us now apply this to a few examples:

Example 4.78. *Consider the following set from Example 4.76:*

$$C = \{q \in \mathbb{Q} \mid q < 0\}.$$

- *0 is an upper bound of C. This holds since every $q \in C$ satisfies $q < 0$, so that the condition for upper bound in Definition 4.77 is satisfied.*
- *1 is also an upper bound of C. While this may not be the first number you think of when you see C, the number 1 nonetheless satisfies the condition in Definition 4.77—namely, 1 is larger than every element of C.*
- *-1 is not an upper bound of C. To see this, we simply observe that $-\frac{1}{2} \in C$, but $-\frac{1}{2} > -1$, so that the condition in Definition 4.77 is violated.*

Note that to show $y \in \mathbb{R}$ is *not* an upper bound of $A \subseteq \mathbb{R}$, we must show the negation of the formal statement in Definition 4.77, that is (see Figure 2.21),

$$\exists_{x \in A} x > y.$$

In other words, *we must find an element $x \in A$ that is strictly larger than y*. This is precisely what was done in the last part of Example 4.78 above, with $A = C$ and $y = -1$.

Example 4.79. *The same observations hold for the other set from Example 4.76,*

$$D = \{x \in \mathbb{R} \mid x < 0\}.$$

Indeed, 0 and 1 are upper bounds of D, but -1 is not an upper bound of D.

Example 4.80. *Consider next the set*

$$E = \{q \in \mathbb{Q} \mid q^2 \leq 2\}.$$

By manipulating the condition $q^2 \leq 2$, we see that E is precisely the set of all rational numbers between $-\sqrt{2}$ and $+\sqrt{2}$. As a result:

- *3 is an upper bound of E, since any $q \in E$ satisfies $q \leq 3$.*
- *$\sqrt{2}$ is also an upper bound of E, as again, any $q \in E$ satisfies $q \leq \sqrt{2}$.*
- *0 is not an upper bound of E, since $1 \in E$ and $1 > 0$.*

Example 4.81. *Consider now the set*

$$F = \{x \in \mathbb{R} \mid x > 0\}.$$

Observe that F does not have an upper bound. Indeed, any $y \in \mathbb{R}$ cannot be an upper bound of F, since $z = |y| + 1$ is an element of F, but $z > y$.

Example 4.82. *On the other hand, every $y \in \mathbb{R}$ is an upper bound of the empty set $\emptyset$. This is because the corresponding condition from Definition 4.77,*

$$\forall_{x \in \emptyset} x \leq y,$$

is always (vacuously) true, due to $x \in \emptyset$ always being false.

Note that any of the above examples for upper bounds can be straightforwardly converted to examples for lower bounds by replacing "$\leq$" with "$\geq$". For instance,

- 0 and -1 are lower bounds for $\{q \in \mathbb{Q} \mid q > 0\}$.
- 1 is not a lower bound for $\{x \in \mathbb{R} \mid x > 0\}$.
- $\{q \in \mathbb{Q} \mid q < 0\}$ does not have any lower bounds.

Thus, for brevity, we will, for the most part, restrict our discussions only to upper bounds.

The next definition captures our aforementioned notion of "almost maximum":

Definition 4.83. *Let $A \subseteq \mathbb{R}$. We say that $s \in \mathbb{R}$ is the supremum (alternatively, the least upper bound) of A iff the following conditions both hold:*

(1) *s is an upper bound of A.*
(2) *If t is also an upper bound of A, then $s \leq t$.*

The supremum of A is commonly denoted as $\sup A$.

Observe that condition (2) in Definition 4.83 means that *any other upper bound of* A *must be larger than* s—justifying that s is indeed the least upper bound.

Of course, there is also an opposite notion of "almost minimum":

Definition 4.84. *Let* $A \subseteq \mathbb{R}$. *We say that* $s \in \mathbb{R}$ *is the infimum (or, the greatest lower bound) of* A, *denoted* $\inf A$, *iff the following conditions both hold:*

(1) s *is a lower bound of* A.
(2) *If* t *is also a lower bound of* A, *then* $s \geq t$.

Once again, since Definitions 4.83 and 4.84 are mirror images of each other, we will, for the most part, restrict our discussions to only the supremum.

Note. *By convention, we often also define the following special cases:*

- *If* $A \subseteq \mathbb{R}$ *does not have an upper bound, then we set* $\sup A = +\infty$. *Similarly, if* A *does not have a lower bound, then we set* $\inf A = -\infty$.
- *In addition, we set* $\sup \emptyset = -\infty$ *and* $\inf \emptyset = +\infty$.

However, we will not consider these cases in this module.

Example 4.85. *Observe that by Definition 4.83, the following holds:*

$$\sup\{1, 3, 5\} = 5.$$

- 5 *is clearly an upper bound of* $\{1, 3, 5\}$.
- 5 *is also the smallest upper bound, since if* $x \in \mathbb{R}$ *and* $x < 5$, *then* x *by definition is not an upper bound of* $\{1, 3, 5\}$ *(simply since* $5 > x$*).*

The observations from Example 4.85 can be generalised to other sets:

Proposition 4.86. *If* $A \subseteq \mathbb{R}$ *and* m *is the maximum element of* A, *then* $\sup A = m$.

Proof of Proposition 4.86. First, m is an upper bound of A by Definition 4.77, since by virtue of m being the maximum, we have $x \leq m$ for every $x \in A$.

Furthermore, m must be the least upper bound, since if $y \in \mathbb{R}$ and $y < m$, then y by Definition 4.77 is not an upper bound of A. □

We now confirm our intuitions on the "almost maxima" of the sets in Example 4.76.

Example 4.87. *Let us return once again to the sets*

$$C = \{q \in \mathbb{Q} \mid q < 0\}, \qquad D = \{x \in \mathbb{R} \mid x < 0\}.$$

We claim that $\sup D = 0$. *To see this, we note the following:*

- *We showed in Example 4.78 that* 0 *is an upper bound of* D.
- 0 *is also the smallest upper bound, since if* $x \in \mathbb{R}$ *and* $x < 0$, *then* x *cannot be an upper bound of* D *(since* $\frac{x}{2} \in D$ *and* $\frac{x}{2} > x$*).*

By similar reasoning, one can also show that $\sup C = 0$.

Example 4.88. *The following holds:*

$$\sup\left\{-1, -\tfrac{1}{2}, -\tfrac{1}{3}, \dots\right\} = 0.$$

This is an immediate consequence of the following observations:

- 0 *is an upper bound of the set* $\{-1, -\frac{1}{2}, -\frac{1}{3}, \dots\}$.
- *If* $x \in \mathbb{R}$ *and* $x < 0$, *then* x *is not an upper bound of* $\{-1, -\frac{1}{2}, -\frac{1}{3}, \dots\}$. *(This is because there is a large enough* $n \in \mathbb{N}$ *such that* $-\frac{1}{n} > x$*.)*

Finally, we have thus far been referring to "the supremum" and "the infimum" of a set $A \subseteq \mathbb{R}$. However, this terminology only makes sense if there is only one supremum and one infimum of A. Fortunately, this is indeed always true:

Proposition 4.89. *Let* $A \subseteq \mathbb{R}$.

(1) *If* s *and* s' *are both the supremum of* A, *then* $s = s'$.
(2) *If* s *and* s' *are both the infimum of* A, *then* $s = s'$.

Proof of Proposition 4.89. (1) By Definition 4.83:

- Both s and s' are upper bounds of A.
- Since s is the supremum and s' is an upper bound, then $s \leq s'$.
- Since s' is the supremum and s is an upper bound, then $s' \leq s$.

It follows from the above that $s = s'$.

(2) The proof is analogous to that of (1), so we omit the details. □

4.8.2. *The Supremum Principle.* We had previously advertised all the material regarding upper/lower bounds and suprema/infima as another way of characterising the idea that the real number line "does not have any holes", unlike the rational numbers. We can now make good on this promise. Let us start with a motivating example:

Example 4.90. *Consider the set from Example 4.80:*

$$E = \{q \in \mathbb{Q} \mid q^2 \leq 2\}.$$

We claim that $\sup E = \sqrt{2}$*, which is a consequence of the following:*

- *We already showed in Example 4.80 that* $\sqrt{2}$ *is an upper bound of* E*.*
- *If* $x \in \mathbb{R}$ *and* $0 \leq x < \sqrt{2}$*, then* x *is not an upper bound of* E*. (This is because we can then find some* $q \in \mathbb{Q}$ *satisfying* $x < q < \sqrt{2}$*; see the problem sheets for details. As a result,* $q \in E$ *but* $q > x$*, violating Definition 4.77.)*
- *More trivially, if* $x \in \mathbb{R}$ *and* $x < 0$*, then* x *also cannot be an upper bound of* E*. (This is simply because, e.g.,* $0 \in E$ *and* $0 > x$*.)*

Note, on one hand, *the set* E from Example 4.90 *contains only rational numbers.* On the other hand, $\sup E = \sqrt{2}$ *is not a rational number, but rather is a real number.*

What this tells us is that *had we limited our view to only rational numbers, then we would not have found an "almost maximum" for* E. Indeed, it is *only when we broadened our view from* $\mathbb{Q}$ *to* $\mathbb{R}$ *that we were able to find this "almost maximum"* $\sqrt{2}$. This observation can be interpreted as $\mathbb{Q}$ having a "hole" where the number $\sqrt{2}$ should be; on the real number line, in contrast, the "hole" is filled in by the irrational number $\sqrt{2}$.

In other words, the supremum serves as a tool to "poke for holes" in our number systems. For instance, one detects a hole in $\mathbb{Q}$ whenever a set does not have a supremum in $\mathbb{Q}$. That $\mathbb{R}$ does not have any "holes" would then be demonstrated by the fact that *supremum always exists in* $\mathbb{R}$ (as long as the set has an upper bound to begin with). This is precisely the content of the following fundamental theorem about the real numbers:

Theorem 4.91 (Supremum principle). *Let $A \subseteq \mathbb{R}$ is non-empty, and suppose A has an upper bound $u \in \mathbb{R}$. Then, A has a supremum,* $\sup A \in \mathbb{R}$.

Note. *Recall that when $A = \emptyset$ or A has no upper bound, then* $\sup A$ *is $-\infty$ or $+\infty$, which are not in $\mathbb{R}$. Thus, we have to exclude these cases from Theorem 4.91.*

The proof of Theorem 4.91 makes crucial use of the precise definition of $\mathbb{R}$, which is a bit beyond the scope of this module, hence we omit this proof here. (See, however, the bonus content at the end of the next chapter.) Nonetheless, we can provide some informal intuition for why Theorem 4.91 should be true.

Example 4.92. *Let us consider the particular set*

$$A = \{x \in \mathbb{R} \mid 0 < x < 1\}. \tag{4.22}$$

To systematically obtain the supremum of A, we can carry out the following.

(1a) *Write out each $x \in A$ as an infinite decimal expansion. (For A as in* (4.22)*, each $x \in A$ has a decimal expansion of the form "$0.x_1x_2x_3\ldots$".)*

(1b) *Take the largest leftmost digit attained by elements of A. (For A as in* (4.22)*, the leftmost digit is the x_1-position, and the largest value found there is "9".)*

(1c) *Keep all the elements of A which have this largest leftmost digit, and discard all the others. (For* (4.22)*, we keep all elements in A of the form "$0.9x_2x_3\ldots$".)*

The idea here is that we discard all the elements of A that are "far away" from being an upper bound of A. From the above, we then proceed as follows:

(2a) *Of the remaining elements in A, take the largest value attained in the next digit. (For A as in* (4.22)*, this is the x_2-position, and the largest attained value is "9".)*

(2b) *Keep all the elements of A which have the largest 2 leftmost digits, and discard all others. (For* (4.22)*, we keep all elements in A of the form "$0.99x_3x_4\ldots$".)*

Again, the above steps remove more elements of A that are "far away" from being an upper bound of A. The idea now is to repeat this process for each subsequent digit:

(3) *Of the remaining elements in A, take the largest value attained in the next digit, and keep only the elements which attain this largest value. (For A as in* (4.22)*, we keep all elements in A of the form "$0.999x_4x_5\ldots$".)*

(⋮) ⋮

(∞) *Repeat the above process an infinite number of times, for every remaining digit. (For A as in (4.22), the largest attained value in each digit is 9, so at the end of this infinite process, we have the infinite decimal expansion "0.99999 . . . .")*

The expansion we have generated at the end of this infinite process will be the supremum of A. Thus, for A as in (4.22), we have obtained, as expected,

$$\sup A = 0.999999\cdots = 1.$$

The intuition in Example 4.92 is that after each step, we have discarded more elements of A that are "far away" from an upper bound of A. After running infinitely many steps, the process settles on an infinite decimal expansion, which will "just barely be an upper bound of A", hence this value will be the supremum of A.

Although Example 4.92 only considered the set (4.22), the general algorithm outlined there, which was highlighted in red, will apply to any A in Theorem 4.91, for the same reasons as mentioned before. Thus, with some care, the general algorithm could be converted into a proof of Theorem 4.91, however we omit the details here.

4.9. **Complex Numbers.** Lastly, we turn our attention to the complex numbers, which go even beyond the real number line into the so-called "imaginary numbers".

Before going into details, we should consider why one might want more than the real numbers in the first place. Recall, from Section 4.1, that one can already do many things with real numbers, such as adding, multiplying, exponentiating, and so on. Moroever, the real number system filled in all the holes that were present among the rational numbers. In spite of all this, there are still some very basic things that one cannot do in $\mathbb{R}$, which suggests that the real number line is "missing something fundamental":

Example 4.93. *Let $x \in \mathbb{R}$. Then:*

- *If $x \geq 0$, then its square root $\sqrt{x}$ is well-defined as a real number.*
- *However, if $x < 0$, then there is no well-defined square root $\sqrt{x}$ in $\mathbb{R}$.*

Example 4.94. *A similar issue arises for polynomials with real coefficients:*

- *The quadratic polynomial $x^2 - 1$ can be factored as a product of two linear polynomials $(x-1)(x+1)$. (This is because $x^2 - 1$ has $+1$ and -1 as its roots.)*

- *On the other hand, $x^2 + 1$ cannot be factored as a product of two linear polynomials with real coefficients. (This is since $x^2 + 1$ has no real roots.)*

Examples 4.93–4.94 highlight some rather elementary deficiencies of the real numbers. In fact, both examples revolve around the fact that -1 has no square root that is in $\mathbb{R}$. The main question we should now ask, though, is "*What should we do about this?*"

On one hand, we could just give up and go home, but that would be defeatist and lame, especially for someone studying for a mathematics degree. The other option is that we could just make up our own solution. In other words, we ignore all the naysayers and *invent our own square root of* -1, and we deal with the consequences later.

Proceeding with Option 2, we will into existence a new number i, with the extra condition that i satisfies $i \cdot i = -1$ (i.e. i is a square root of -1). Done! Fantastic! However, once the dust settles, you will see that this is all still a bit pointless, as all we have is merely a new number i that sits apart from the real line.

To accomplish something meaningful, we will also need to *do things* with our shiny new number. For example, it would be nice if we can add and multiply our new number i. Further, our new number i should also be able to interact with our existing real numbers.

Let us now see what else we need in order for all this to work reasonably:

- Given any $y \in \mathbb{R}$, we would like to "multiply y by i". However, there is no existing number that could naturally serve as this product. As a result, we invent yet another new number "yi" to fulfill this purpose.
- Similarly, given $x \in \mathbb{R}$, we would like to "add x to yi". Again, there is no existing number that naturally fits this purpose, so we invent a new number "$x + yi$".

Whew, that is a lot of new numbers! However, the good (and rather interesting) news is that *the above are all the new numbers we need to invent* in order to address the deficiencies in Examples 4.93–4.94, as well as to do the same things we were able to do in $\mathbb{R}$.

We will justify the above statement in the remainder of this chapter. However, let us now define the number system we have just haphazardly created:

Definition 4.95. *The set of complex numbers is defined as*

$$\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}.$$

Moreover, any quantity $yi = 0 + yi$*, for* $y \in \mathbb{R}$*, is called an imaginary number.*

Note. *In engineering, the imaginary number* i *is commonly written as "*j*" instead. However, here we will remain with mathematical conventions and use "*i*".*

4.9.1. *Complex Arithmetic.* While we previously described how to add and multiply some complex numbers, we now need to finish the job and *define sums and products of all complex numbers*. Our guiding principle is that the complex numbers should have the same algebraic properties as the real numbers, as listed in Section 4.1. With that in mind:

- Given complex numbers $z = a + bi$ and $w = c + di$, since we want the commutative, associative, and distributive properties to hold, we would like to have

$$\begin{aligned} z + w &= (a + c) + (bi + di) \\ &= (a + c) + (b + d)i. \end{aligned}$$

- Similarly, given z and w as above, and recalling that our defining property of i is that $i \cdot i$ is -1, we then see that a reasonable value for $z \cdot w$ is

$$\begin{aligned} z \cdot w &= (a + bi)(c + di) \\ &= ac + bci + adi + bd(i \cdot i) \\ &= (ac - bd) + (bc + ad)i. \end{aligned}$$

The above wish list leads us to the following definitions:

Definition 4.96. *Given* $z = a + bi \in \mathbb{C}$ *and* $w = c + di \in \mathbb{C}$*:*

- *We define their sum as*

$$z + w = (a + c) + (b + d)i.$$

- *We define their product as*

$$z \cdot w = (ac - bd) + (bc + ad)i.$$

Example 4.97. *Consider the complex numbers*

$$z = 4 + 3i, \qquad w = 3 + 2i.$$

- *Taking the sum of z and w, we see that*

$$\begin{aligned} z+w &= (4+3\mathrm{i})+(3+2\mathrm{i}) \\ &= (4+3)+(3+2)\mathrm{i} && \textit{(Definition 4.96)} \\ &= 7+5\mathrm{i}. \end{aligned}$$

- *Similarly, taking the product of z and w yields*

$$\begin{aligned} zw &= (4+3\mathrm{i})(3+2\mathrm{i}) \\ &= (4\cdot 3-3\cdot 2)+(3\cdot 3+4\cdot 2)\mathrm{i} && \textit{(Definition 4.96)} \\ &= 6+17\mathrm{i}. \end{aligned}$$

- *In addition, multiplying z by itself, we obtain*

$$\begin{aligned} z^2 &= (4+3\mathrm{i})(4+3\mathrm{i}) \\ &= (4\cdot 4-3\cdot 3)+(4\cdot 3+3\cdot 4)\mathrm{i} \\ &= 7+24\mathrm{i}. \end{aligned}$$

Now, in Example 4.97, the computations were performed directly using the definitions of complex addition and multiplication. However, recall *Definition 4.96 was motivated by assuming $\mathbb{C}$ satisfies the same algebraic rules as $\mathbb{R}$*. Thus, we could derive the same answers as in Example 4.97, and more intuitively, by using these algebraic rules:

Example 4.98. *Consider the complex numbers $4+3\mathrm{i}$ and $3+2\mathrm{i}$ from Example 4.97. Let us now compute the product zw by assuming the usual algebraic identities:*

$$\begin{aligned} (4+3\mathrm{i})(3+2\mathrm{i}) &= 4\cdot 3+3\mathrm{i}\cdot 3+4\cdot 2\mathrm{i}+3\mathrm{i}\cdot 2\mathrm{i} && \textit{(distributive rule)} \\ &= 12+9\mathrm{i}+8\mathrm{i}+6(\mathrm{i}\cdot\mathrm{i}) && \textit{(commutative, associative rules)} \\ &= 6+17\mathrm{i} && \textit{(since } 6(\mathrm{i}\cdot\mathrm{i})=-6\textit{).} \end{aligned}$$

Example 4.99. *Below are a few more examples of complex addition and multiplication:*

$$(-1+\mathrm{i})+(4-3\mathrm{i})=3-2\mathrm{i}, \qquad \mathrm{i}(-3+2\mathrm{i})=-2-3\mathrm{i},$$
$$(-1+\mathrm{i})(4-3\mathrm{i})=-1+7\mathrm{i}, \qquad \mathrm{i}+(-3+2\mathrm{i})=-3+3\mathrm{i}.$$

Example 4.100. *Using Definition 4.96, we can confirm that indeed* $i \cdot i = -1$*:*

$$\begin{aligned} i \cdot i &= (0 + 1 \cdot i)(0 + 1 \cdot i) \\ &= (0 \cdot 0 - 1 \cdot 1) + (0 \cdot 1 + 1 \cdot 0)i \qquad \textit{(definition of multiplication)} \\ &= -1. \end{aligned}$$

Note in addition that

$$i \cdot (-i) = 1, \qquad (-i) \cdot i = 1, \qquad (-i) \cdot (-i) = -1.$$

For completeness, we list explicitly some of the algebraic properties of $\mathbb{C}$:

Proposition 4.101. *The following hold for any* $z, w, u \in \mathbb{C}$*:*

(1) *Commutative property:* $z + w = w + z$*, and* $zw = wz$*.*
(2) *Associative property:* $(z + w) + u = z + (w + u)$*, and* $(zw)u = z(wu)$*.*
(3) *Distributive property:* $z(w + u) = zw + zu$*.*
(4) *Identities:* $z + 0 = 0 + z = z$*, and* $z \cdot 1 = 1 \cdot 1 = z$*.*

Proposition 4.101 can be proved using Definition 4.96 and the algebraic rules for $\mathbb{R}$ in Section 4.1. Since this is rather painstaking, we only prove the first property here:

Proof of Proposition 4.101 (1). Let us write, for $a, b, c, d \in \mathbb{R}$,

$$z = a + bi, \qquad c + di.$$

Then, using Definition 4.96, we have

$$z + w = (a + c) + (b + d)i, \qquad zw = (ac - bd) + (bc + ad)i.$$

Using the commutative properties of $\mathbb{R}$ and Definition 4.96, we then obtain

$$\begin{aligned} z + w &= (c + a) + (d + b)i \qquad \text{(by Proposition 4.2)} \\ &= w + z \qquad\qquad\quad \text{(by Definition 4.96),} \\ zw &= (ca - db) + (cb + da)i \qquad \text{(by Proposition 4.2)} \\ &= wz \qquad\qquad\quad\ \ \text{(by Definition 4.96),} \end{aligned}$$

which are precisely the desired identities. □

We now list a few more commonly used operations on complex numbers:

Definition 4.102. *Given a complex number $z = x + yi$:*

- *We define the real part of z to be $\operatorname{Re} z = x$.*
- *We define the imaginary part of z to be $\operatorname{Im} z = y$.*
- *We define the (complex) conjugate of z to be $\bar{z} = x - yi$.*
- *We define the modulus of z to be $|z| = \sqrt{x^2 + y^2}$.*

We will discuss the interpretations of these operations in the subsequent section. For now, you can just think of these as basic quantities that one can compute.

Example 4.103. *Let $z = 4 - 3i$. Then, by Definition 4.102,*

- $\operatorname{Re} z = 4$.
- $\operatorname{Im} z = -3$.
- $\bar{z} = 4 + 3i$.

Furthermore, the modulus of z is given by

$$\begin{aligned} |z| &= \sqrt{4^2 + (-3)^2} \\ &= 5. \end{aligned}$$

Example 4.104. *Consider the complex numbers $z = 1 + 2i$ and $w = -2 - i$. Then:*

- $z \cdot \bar{w} = -4 - 3i$.
- $\bar{z} \cdot w = -4 + 3i$.
- $|w| = \sqrt{5}$.
- $|z \cdot \bar{w}| = 5$.
- $|\bar{z} \cdot w| = 5$.

The following algebraic property will be useful later on:

Proposition 4.105. *The following holds for any $z \in \mathbb{C}$:*

$$|z|^2 = z \cdot \bar{z}.$$

Proof of Proposition 4.105. Let $z = x + yi$, with $x, y \in \mathbb{R}$. Then, by Definition 4.102,

$$\begin{aligned} z \cdot \bar{z} &= (x + yi)(x - yi) && \text{(Definition of conjugate)} \\ &= (x \cdot x - y \cdot (-y)) + (x \cdot (-y) + y \cdot x)i \\ &= x^2 + y^2 \\ &= |z|^2 && \text{(Definition of modulus).} \end{aligned}$$

□

4.9.2. *Subtraction and Division.* Recall that on $\mathbb{R}$, one can "undo" the effects of adding and multiplying; this is done by subtracting and dividing, respectively. One can then ask *whether one can similarly "undo" addition and multiplication on* $\mathbb{C}$, that is, *whether one can make sense of subtracting and dividing complex numbers.*

To define these operations, we set the following:

Definition 4.106. *Let $z, w \in \mathbb{C}$.*

(1) *We define the additive inverse of z to be*

$$-z = (-1) \cdot z.$$

We then define subtraction of complex numbers by

$$w - z = w + (-z).$$

(2) *If $z \neq 0$, then we define the multiplicative inverse of z to be*

$$\frac{1}{z} = \frac{\bar{z}}{|z|^2}.$$

We then define division of complex numbers by

$$\frac{w}{z} = w \cdot \frac{1}{z}.$$

Note. *To clarify, in the above, we should interpret $\frac{\bar{z}}{|z|^2}$ as the real number $\frac{1}{|z|^2}$ multiplied by the complex number $\bar{z}$, which is carried out as in Definition 4.96.*

In order to justify Definition 4.106, we must show that subtraction and division actually do reverse the effects of addition and multiplication. In other words, we must show:

Proposition 4.107. *The following hold for any $z \in \mathbb{Z}$:*

(1) $z - z = 0$.

(2) *If $z \neq 0$, then $\frac{z}{z} = 1$.*

The story for subtraction is short, as this works for the same reason as for $\mathbb{R}$:

Proof of Proposition 4.107 (1). By Definition 4.106 and Proposition 4.101, we have

$$\begin{aligned} z - z &= \underbrace{z}_{1 \cdot z} + (-1) \cdot z \\ &= (1 - 1) \cdot z && \text{(distributive property)} \\ &= 0. \end{aligned}$$

□

Division is a bit more subtle. Here, the insight is to rewrite Proposition 4.105 as

$$\begin{aligned} 1 &= \tfrac{z \cdot \bar{z}}{|z|^2} \\ &= z \cdot \tfrac{\bar{z}}{|z|^2}. \end{aligned}$$

Since we naturally want $z \cdot \frac{1}{z} = 1$, the above suggests that $\frac{1}{z}$ should be equal to $\frac{\bar{z}}{|z|^2}$. This is the motivation for our formula for $\frac{1}{z}$ in Definition 4.106.

Proof of Proposition 4.107 (2). By Definition 4.106 and Proposition 4.105, we have

$$\begin{aligned} \tfrac{z}{z} &= z \cdot \tfrac{1}{z} \\ &= z \cdot \tfrac{\bar{z}}{|z|^2} && \text{(by Definition 4.106)} \\ &= 1 && \text{(by Proposition 4.105).} \end{aligned}$$

□

To consolidate this discussion, we give a few simple examples:

Example 4.108. *Let $z = 2 + \mathrm{i}$ and $w = 4 + 3\mathrm{i}$.*

- *Using Definition 4.106 directly, we compute*

$$z - w = \underbrace{z}_{(2+\mathrm{i})} + \underbrace{(-w)}_{(-4-3\mathrm{i})}$$

$$= (2-4) + (1-3)\mathrm{i}$$
$$= -2 - 2\mathrm{i}.$$

- *Similarly, we can compute*

$$w - z = (4-2) + (3-1)\mathrm{i}$$
$$= 2 + 2\mathrm{i}.$$

Example 4.109. *Again, let* $z = 2 + \mathrm{i}$ *and* $w = 4 + 3\mathrm{i}$.

- *Let us first compute* $\frac{1}{w}$. *By Definitions 4.102 and 4.106, we have*

$$\frac{1}{w} = \frac{\bar{w}}{|w|^2}$$
$$= \frac{4-3\mathrm{i}}{4^2+3^2}$$
$$= \frac{4}{25} - \frac{3}{25}\,\mathrm{i}.$$

- *Next, let us compute* $\frac{z}{w}$. *By Definition 4.106 and the above,*

$$\frac{z}{w} = \underbrace{z}_{(2+\mathrm{i})} \cdot \underbrace{\frac{1}{w}}_{(\frac{4}{25} - \frac{3}{25}\mathrm{i})}$$
$$= \left[2 \cdot \tfrac{4}{25} - 1 \cdot \left(-\tfrac{3}{25}\right)\right] + \left[1 \cdot \tfrac{4}{25} + 2 \cdot \left(-\tfrac{3}{25}\right)\right]\mathrm{i}$$
$$= \frac{11}{25} - \frac{2}{25}\,\mathrm{i}.$$

Example 4.110. *One could also divide two complex numbers directly, without first computing the multiplicative inverse. For instance,*

$$\frac{1+\mathrm{i}}{1-2\mathrm{i}} = \frac{(1+\mathrm{i}) \cdot (\overline{1-2\mathrm{i}})}{|1-2\mathrm{i}|^2}$$
$$= \frac{(1+\mathrm{i})(1+2\mathrm{i})}{1^2 + (-2)^2}$$
$$= -\frac{1}{5} + \frac{3}{5}\,\mathrm{i}.$$

4.10. **The Complex Plane.** Recall that $\mathbb{R}$ can be visually represented as a line, with the various real numbers being individual points along the line. We can hence ask whether there is a natural way to intuitively describe the complex numbers.

Question 4.111. *How would one visualise $\mathbb{C}$?*

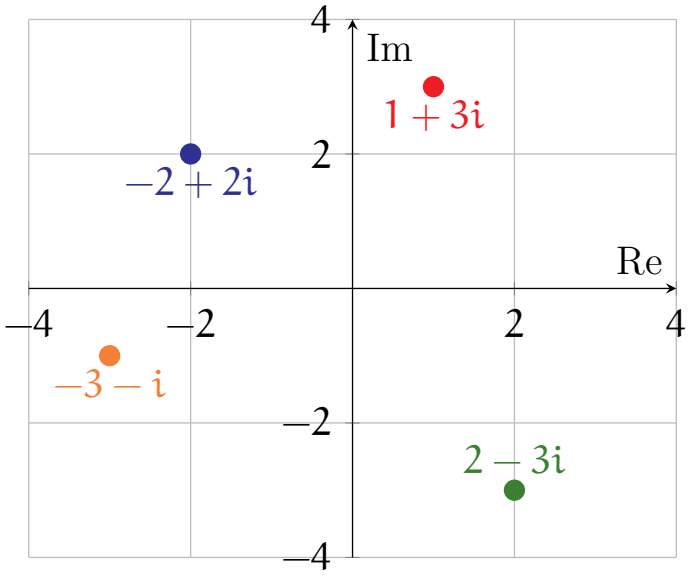
The answer to Question 4.111 is remarkly simple. After all, any $z \in \mathbb{C}$ can be represented uniquely by two real numbers, $z = x + yi$, with $x, y \in \mathbb{R}$. Then, it may be natural to think of the real part x as coordinate along the x-axis, and the imaginary part y as a coordinate along the y-axis. More specifically, *we could view z as a point on a plane, with its Cartesian coordinates given by its real and imaginary parts.*

Consequently, just as $\mathbb{R}$ is sometimes called the "real line", we often refer to $\mathbb{C}$ as the complex plane when we want to highlight its geometric features.

Example 4.112. *In the figure below, we plot the following onto the complex plane:*

$$1 + 3i, \qquad -2 + 2i, \qquad -3 - i, \qquad 2 - 3i.$$

The real and imaginary parts correspond to the x and y coordinates, respectively.



While it is nice that we can draw complex numbers as points on a plane, this would only be useful if the usual things we can do with complex numbers have meaningful geometric interpretations. As a result, it is important that we ask:

Question 4.113. *What do the usual operations on $\mathbb{C}$ look like on a plane?*

First, recall that for $z = x + yi \in \mathbb{C}$, its conjugate is given by

$$\bar{z} = x - yi,$$

that is, we simply negate the imaginary part of z. Since the imaginary part corresponds to the y-coordinate of the plane, *conjugation on the complex plane simply negates the y-coordinate of the given point*, or in other words, *reflects the point across the x-axis.*

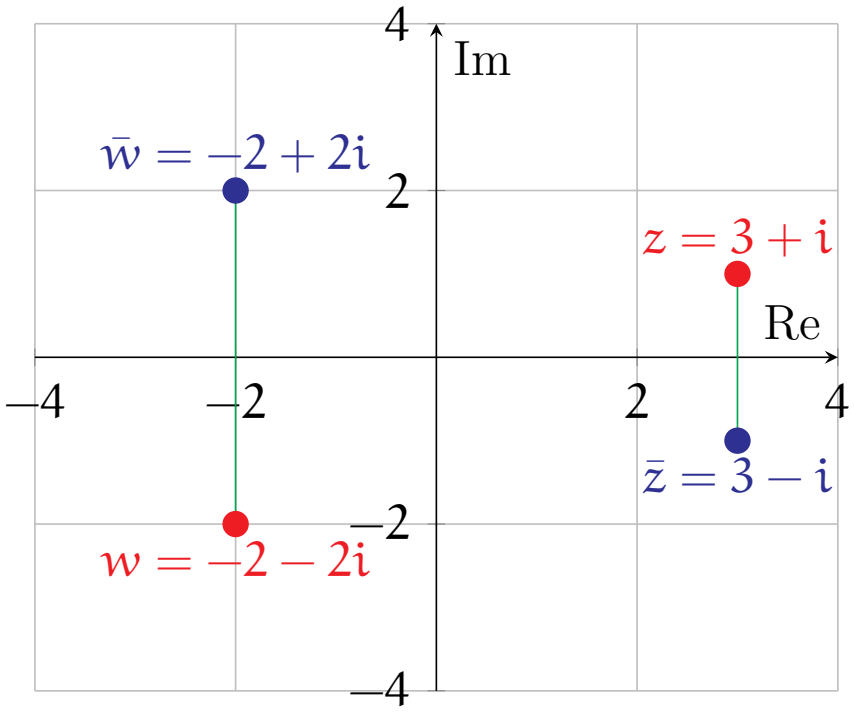


FIGURE 4.6. The above plot illustrates conjugation on the complex plane. The numbers $z, w \in \mathbb{C}$ are drawn in red, while their conjugates $\bar{z}, \bar{w}$ are in blue.

Next, recall that for complex numbers $z = x + yi$ and $w = a + bi$, their sum is

$$z + w = (x + a) + (y + b)i,$$

that is, one adds the respective real parts and imaginary parts, which correspond to the x and y coordinates on the plane. Now, this should look very much like something else you have seen before, namely, vector addition! Indeed, when adding two-dimensional vectors, you also just sum the respective x-components and y-components.

Thus, addition of complex numbers and planar vectors are functionally equivalent, so it is unsurprising that both have the same geometric meaning. Indeed, the depiction of addition on the complex plane is identical to the usual drawing of vector addition:

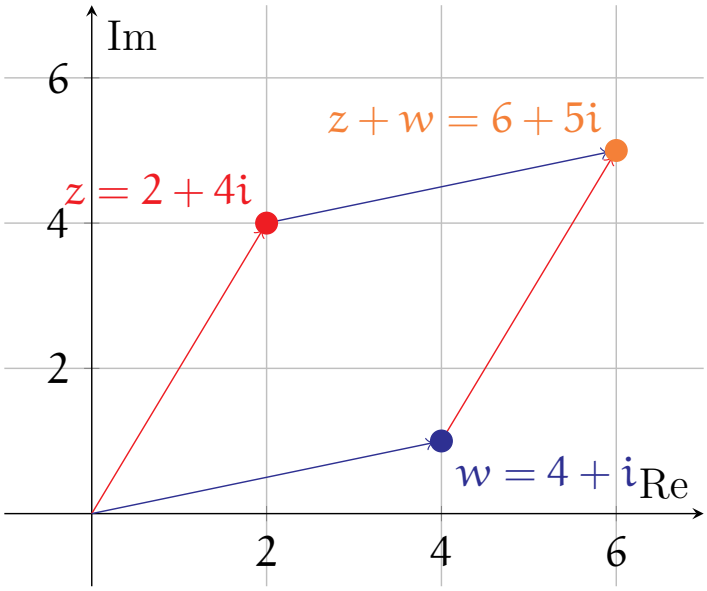


FIGURE 4.7. The above plot illustrates addition on the complex plane. Note this is identical to the usual visualisation of vector addition on a plane.

The more interesting operation with regards to Question 4.113 is multiplication, which has a novel interpretation that is different from what you have seen before. Before elaborating on this, however, we will require a bit more background.

4.10.1. *Polar Form.* Given any nonzero point $z = x + yi$ on the complex plane, we can also describe its position using polar coordinates (r, θ), where:

- r denotes the distance between the point z and the origin.
- θ denotes the anticlockwise angle that the line segment connecting the origin and the point z makes with the positive x-axis.

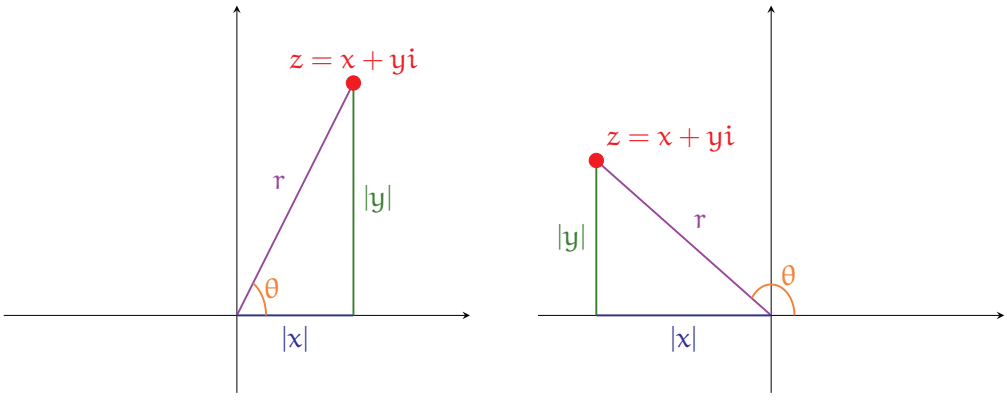


FIGURE 4.8. The above illustrates polar coordinates for points $z = x + yi \in \mathbb{C}$.

In particular, since x and y represent the horizontal and vertical positions of z, respectively, one can observe from the above illustrations that:

- By the Pythagorean theorem, the coordinate r is given by

$$r = \sqrt{x^2 + y^2}. \tag{4.23}$$

- Moreover, by the definitions of the trigonometric functions, we have

$$\cos\theta = \tfrac{x}{r}, \qquad \sin\theta = \tfrac{y}{r}, \qquad \tan\theta = \tfrac{y}{x}, \tag{4.24}$$

Combining (4.23) and (4.24), we see that $z = x + yi$ can be rewritten as

$$z = r\cos\theta + r\sin\theta\, i.$$

Summarising the above, we arrive at the following definition:

Definition 4.114. *Let $z = x + yi \in \mathbb{C} \setminus \{0\}$. We define the polar form of z to be*

$$z = r(\cos\theta + i\sin\theta),$$

where r (i.e. the modulus) and θ (i.e. the argument) satisfy

$$r = \sqrt{x^2 + y^2} = |z|, \qquad \tan\theta = \tfrac{y}{x} = \tfrac{\operatorname{Im} z}{\operatorname{Re} z}.$$

There is one additional bit of common notation that you should be aware of:

Definition 4.115. *Given any $\theta \in \mathbb{R}$, we define the imaginary exponential $e^{i\theta}$ by*

$$e^{i\theta} = \cos\theta + i\sin\theta. \tag{4.25}$$

As a result, given any $z \in \mathbb{C} \setminus \{0\}$, its polar form can be abbreviated as

$$z = re^{i\theta}, \qquad r = |z|, \qquad \tan\theta = \tfrac{\operatorname{Im} z}{\operatorname{Re} z}.$$

The equation (4.25) is known as Euler's formula. For this module, you can simply view Euler's formula as a convenient abbreviation, but it actually has much deeper meaning.

Example 4.116. *Let us write $1 + i$ in polar form.*

Observe that here, r and θ are given by

$$r = \sqrt{1^2 + 1^2} = \sqrt{2}, \qquad \theta = \tan^{-1}\left(\tfrac{1}{1}\right) = \tfrac{\pi}{4}.$$

As a result, the polar form of $1+i$ *is given by*

$$1+i=\sqrt{2}e^{\frac{\pi}{4}i}.$$

Example 4.117. *Let us now write* $1-\sqrt{3}i$ *in polar form.*

Observe that its polar coordinates are given by

$$r=\sqrt{1+3}=2, \qquad \theta=\tan^{-1}\left(\tfrac{-\sqrt{3}}{1}\right)=-\tfrac{\pi}{3}.$$

Thus, the polar form of $1-\sqrt{3}i$ *is*

$$1-\sqrt{3}i=2e^{-\frac{\pi}{3}i}.$$

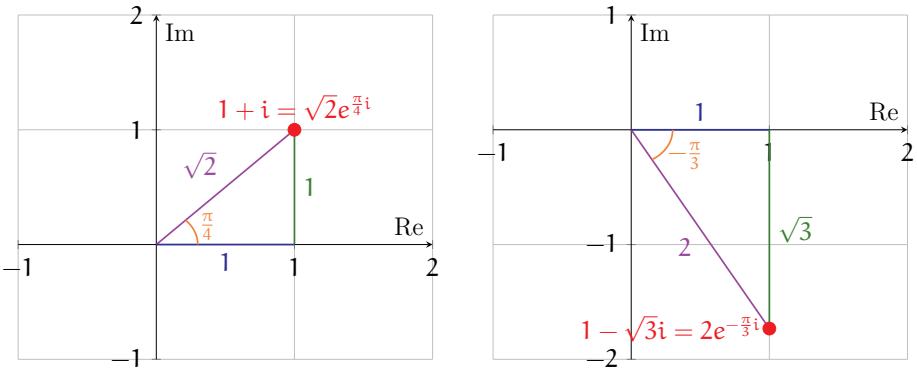


FIGURE 4.9. The above plots illustrate the polar form computations from Example 4.116 (left) and Example 4.117 (right).

Finally, recall that both sin and cos are periodic, with period 2π. This means that

$$\sin(t+2\pi k)=\sin t, \qquad \cos(t+2\pi k)=\cos t$$

for any $t\in\mathbb{R}$ and $k\in\mathbb{Z}$. Euler's formula (4.25) immediately implies

$$e^{i(\theta+2\pi k)}=e^{i\theta}, \qquad \theta\in\mathbb{R}, \quad k\in\mathbb{Z}. \tag{4.26}$$

In particular, *the polar form of a complex number is not unique, as there are infinitely many possible values of* θ *that can be associated with any number.*

Example 4.118. *Recall that we compute in Example 4.116 that*

$$1+i=\sqrt{2}e^{\frac{\pi}{4}i}.$$

Applying (4.26)*, we see that we could also write* $1+i$ *as*

$$1+i=\sqrt{2}e^{(\frac{\pi}{4}+2\pi k)i},\qquad k\in\mathbb{Z}.$$

In particular, by taking $k=1$ *and* $k=-1$ *(respectively), we obtain the polar forms*

$$1+i=\sqrt{2}e^{\frac{9\pi}{4}i},\qquad 1+i=\sqrt{2}e^{-\frac{7\pi}{4}i}.$$

Note. *You may be wondering where Euler's formula comes from, as the particuilar form of* (4.25) *seems quite mysterious at first glance. One way to justify Euler's formula is via calculus, through Taylor series. If you have learned about this before, then you can recall the Taylor series for the exponential and the trigonometric functions,*

$$e^t=\sum_{k=0}^{\infty}\frac{t^k}{k!},\qquad \cos t=\sum_{k=0}^{\infty}\frac{(-1)^k t^{2k}}{(2k)!},\qquad \sin t=\sum_{k=0}^{\infty}\frac{(-1)^k t^{2k+1}}{(2k+1)!},$$

which hold for all $t\in\mathbb{R}$*. Extending the series to complex numbers yields*

$$e^{i\theta}=\sum_{k=0}^{\infty}\frac{(i\theta)^k}{k!},$$

$$\cos\theta+i\sin\theta=\sum_{k=0}^{\infty}\frac{(-1)^k\theta^{2k}}{(2k)!}+i\sum_{k=0}^{\infty}\frac{(-1)^k\theta^{2k+1}}{(2k+1)!}.$$

Doing a bit of algebra, you can see that the right-hand sides of the above are the same! This suggests the most natural way to define $e^{i\theta}$ *is indeed as* $\cos\theta+i\sin\theta$*.*

Finally, the preceding discussion shows that widening our perspective from real to complex numbers could reveal some surprising connections. In terms of real numbers, the exponential function exp and the trigonometric functions sin and cos seem entirely unrelated. However, *from the point of view of complex numbers,* exp*,* sin*, and* cos *are actually different aspects of a single "complex exponential" function*!

Indeed, exponential and trigonometric functions are often seen together in various parts of mathematics, and our understanding of complex numbers helps us to see why this is the case. One very simple example of this is in the differential equations

$$y''(t)+c\cdot y(t)=0,\qquad c\in\mathbb{R}. \tag{4.27}$$

One can verify that (4.27) has solutions $y(t)=e^{+\sqrt{c}\,t}$ and $y(t)=e^{-\sqrt{c}\,t}$ when $c>0$, and solutions $y(t)=\sin(\sqrt{c}\,t)$ and $y(t)=\cos(\sqrt{c}\,t)$ when $c<0$. These seemingly different

looking solutions can be unified from the point of view of complex numbers, as we can always view the solutions of (4.27) as "$e^{+\sqrt{c}t}$" and "$e^{-\sqrt{c}t}$"; when $c < 0$, the square roots of c become imaginary, leading to sin and cos via Euler's formula.

4.10.2. *Multiplication Revisited.* We now return to the question of how multiplication of complex numbers can be geometrically interpreted on the plane. Here, the key observation arises from the following trigonometric computation:

Proposition 4.119. *The following formulas hold:*

(1) $e^{ti} \cdot e^{si} = e^{(t+s)i}$ *for any* $t, s \in \mathbb{R}$.

(2) *De Moivre's formula:* $(e^{ti})^n = e^{nti}$ *for any* $t \in \mathbb{R}$ *and* $n \in \mathbb{N}$.

Proof of Proposition 4.119. (1) Recalling Euler's formula (4.25), we compute

$$\begin{aligned} e^{ti} \cdot e^{si} &= (\cos t + i \sin t)(\cos s + i \sin s) \\ &= (\cos t \cos s - \sin t \sin s) + i(\cos t \sin s + \sin t \cos s). \end{aligned}$$

Combining the above with the standard angle addition formulas,

$$\begin{aligned} \cos(t+s) &= \cos t \cos s - \sin t \sin s, \\ \sin(t+s) &= \cos t \sin s + \sin t \cos s, \end{aligned}$$

we obtain our desired formula:

$$\begin{aligned} e^{ti} \cdot e^{si} &= \cos(t+s) + i \sin(t+s) \\ &= e^{(t+s)i} \qquad \text{(Euler's formula).} \end{aligned}$$

(2) This follows immediately from applying the result of (1) repeatedly:

$$\begin{aligned} (e^{ti})^n &= \underbrace{e^{ti} \cdot e^{ti} \cdot \cdots \cdot e^{ti}}_{n \text{ times}} \\ &= e^{\underbrace{ti+ti+\cdots+ti}_{n \text{ times}}} \qquad \text{(iteration of (1))} \\ &= e^{nti}. \end{aligned}$$

□

Most importantly, Proposition 4.119 leads us to the following geometric characterisation of complex multiplication, in particular addressing Question 4.113:

Corollary 4.120. *Let $z, w \in \mathbb{C} \setminus \{0\}$ have polar forms*

$$z = re^{\theta i}, \qquad w = se^{\sigma i}.$$

Then, the following hold:

(1) *zw has polar form $zw = (rs)e^{(\theta+\sigma)i}$.*
(2) *z^n has polar form $z^n = r^n e^{n\theta i}$ for any $n \in \mathbb{N}$.*

Note. *A corollary is a mathematical fact that is an immediate consequence of another result. Functionally, a "corollary" is the same as a "theorem" or "proposition", except that it can also be quickly proved from a previous result. (What counts as "quickly proved" is subjective and is up to the author's judgment.)*

Proof of Corollary 4.120. (1) Using Proposition 4.119 and the algebraic properties of multiplication (see Proposition 4.101), we can immediately compute

$$\begin{aligned} zw &= (re^{\theta i})(se^{\sigma i}) \\ &= (rs)(e^{\theta i}e^{\sigma i}) \\ &= (rs)e^{(\theta+\sigma)i} \qquad \text{(by Proposition 4.119 (1).)} \end{aligned}$$

(2) Again, by Proposition 4.119 and the algebraic properties of multiplication,

$$\begin{aligned} z^n &= (re^{\theta i})^n \\ &= r^n(e^{\theta i})^n \\ &= r^n e^{n\theta i} \qquad \text{(by Proposition 4.119 (2).)} \end{aligned}$$

□

Observe that Corollary 4.120 gives the following description of multiplication of complex numbers z and w in terms of polar coordinates:

- The r-value (modulus) of zw is the product of the r-values of z and w.
- The θ-value (argument) of zw is the sum of the θ-values of z and w.

In other words, *zw is the point on the complex plane whose distance from the origin is the product of the distances from the origin of z and w, and whose (signed) angle from the positive x-axis is the sum of the (signed) angular values of z and w.*

Example 4.121. *On one hand, we can directly compute the product*

$$(1+\mathrm{i})(1-\sqrt{3}\mathrm{i}) = (1+\sqrt{3}) + (1-\sqrt{3})\mathrm{i}.$$

Next, let us find the polar form of the above.

Recall from Examples 4.116 and 4.117 that we have the polar forms

$$1+\mathrm{i} = \sqrt{2}\,e^{\frac{\pi}{4}\mathrm{i}}, \qquad 1-\sqrt{3}\mathrm{i} = 2\,e^{-\frac{\pi}{3}\mathrm{i}}.$$

Consequently, by Corollary 4.120, we conclude

$$\begin{aligned}(1+\sqrt{3}) + (1-\sqrt{3})\mathrm{i} &= \sqrt{2}e^{\frac{\pi}{4}\mathrm{i}} \cdot 2e^{-\frac{\pi}{3}\mathrm{i}} \\ &= 2\sqrt{2}\,e^{(\frac{\pi}{4}-\frac{\pi}{3})\mathrm{i}} \\ &= 2\sqrt{2}\,e^{-\frac{\pi}{12}\mathrm{i}}.\end{aligned}$$

Example 4.122. *Sometimes, Corollary 4.120 can be used to simplify computations that may otherwise be very cumbersome. As an example, suppose we wish to find*

$$(1+\mathrm{i})^{2025}.$$

Recalling from Example 4.116 the polar form

$$1+\mathrm{i} = \sqrt{2}\,e^{\frac{\pi}{4}\mathrm{i}},$$

and applying Corollary 4.120, we conclude that

$$\begin{aligned}(1+\mathrm{i})^{2025} &= (\sqrt{2})^{2025}\,e^{2025\cdot\frac{\pi}{4}\mathrm{i}} \\ &= 2^{1012}\sqrt{2}\,e^{(\frac{\pi}{4}+506\pi)\mathrm{i}}.\end{aligned}$$

Now, since by (4.25),

$$\begin{aligned}e^{506\pi\mathrm{i}} &= \cos\left(\tfrac{\pi}{4}+506\pi\right) + \mathrm{i}\sin\left(\tfrac{\pi}{4}+506\pi\right) \\ &= \cos\tfrac{\pi}{4} + \mathrm{i}\sin\tfrac{\pi}{4} \\ &= \tfrac{1}{\sqrt{2}} + \tfrac{1}{\sqrt{2}}\,\mathrm{i},\end{aligned}$$

we conclude that

$$\begin{aligned}(1+\mathrm{i})^{2024} &= 2^{1012}\sqrt{2}\left(\tfrac{1}{\sqrt{2}} + \tfrac{1}{\sqrt{2}}\,\mathrm{i}\right) \\ &= 2^{1012}(1+\mathrm{i}).\end{aligned}$$

Finally, we can describe division in terms of polar coordinates as well:

Proposition 4.123. *If $z \in \mathbb{C} \setminus \{0\}$ has polar form $z = re^{\theta i}$, then $\frac{1}{z}$ has polar form*

$$\frac{1}{z} = \frac{1}{r}e^{-\theta i}.$$

Proof of Proposition 4.123. Since by Corollary 4.120, we have

$$\begin{aligned} z \cdot \left(\tfrac{1}{r}e^{-\theta i}\right) &= (re^{\theta i}) \cdot \left(\tfrac{1}{r}e^{-\theta i}\right) \\ &= 1, \end{aligned}$$

it follows that $\frac{1}{z}$ must be equal to $\frac{1}{r}e^{-\theta i}$. □

Example 4.124. *Recall from Example 4.117 the polar form*

$$1 - \sqrt{3}i = 2\,e^{-\frac{\pi}{3}i}.$$

- *Computing directly, we have that*

$$\begin{aligned} \tfrac{1}{1-\sqrt{3}i} &= \tfrac{1+\sqrt{3}i}{|1+\sqrt{3}|^2} \\ &= \tfrac{1}{4} + \tfrac{\sqrt{3}}{4}i. \end{aligned}$$

- *Applying Proposition 4.123, we can also compute the polar form of the above:*

$$\frac{1}{1-\sqrt{3}i} = \frac{1}{2}e^{\frac{\pi}{3}i}.$$

Note. *Defining negative exponents by $z^{-n} = (\frac{1}{z})^n$ for any $n \in \mathbb{N}$, one can then directly extend de Moivre's formula to all integer exponents:*

- $(e^{ti})^k = e^{kti}$ *for all $t \in \mathbb{R}$ and $k \in \mathbb{Z}$.*

4.10.3. *Roots of Unity.* Using polar forms, we can address another related question:

Question 4.125. *For any $n \in \mathbb{N}$, find all the complex n-th roots of 1. More specifically, find all $z \in \mathbb{C}$ satisfying the equation $z^n = 1$.*

The complex n-th roots of 1 are commonly called the n-th roots of unity. (In algebra, "unity" is a fancy term for the abstraction of "1".) In particular, we wish to contrast the answer to Question 4.125 with the real-valued n-th roots of 1.

To get to the bottom of this, let us write $z \in \mathbb{C} \setminus \{0\}$ in polar form

$$z = re^{\theta i}.$$

Then, by Corollary 4.120, we want to find all such z such that

$$\begin{aligned} 1 &= z^n \\ &= r^n e^{n\theta i}. \end{aligned} \tag{4.28}$$

Taking the modulus of (4.28), we see that $r^n = 1$, and (4.28) then becomes

$$\begin{aligned} 1 &= e^{n\theta i} \\ &= \cos(n\theta) + i\sin(n\theta). \end{aligned} \tag{4.29}$$

Now, (4.29) holds only when $\cos(n\theta) = 1$ and $\sin(n\theta) = 0$, and a bit of trigonometry shows that this holds precisely when $n\theta = 2\pi m$ for some $m \in \mathbb{Z}$.

To summarise, since $r > 0$, then the only solution of $r^n = 1$ is given by $r = 1$. Moreover, rearranging the equation $n\theta = 2\pi m$ yields $\theta = \frac{2\pi m}{n}$ for some $m \in \mathbb{Z}$. Putting these values of r and θ into the polar form of z leads to the following results:

Proposition 4.126. *The complex n-th roots of unity are precisely given by*

$$z = e^{\frac{2\pi m}{n} i}, \qquad m \in \mathbb{Z}. \tag{4.30}$$

Proof of Proposition 4.126. First, notice that for z as in (4.30), we have

$$\begin{aligned} z^n &= (e^{\frac{2\pi m}{n} i})^n \\ &= e^{2\pi m i} && \text{(by Corollary 4.120)} \\ &= 1. \end{aligned}$$

Thus, the values z in (4.30) are indeed n-th roots of unity.

Furthermore, the computation preceding the statement of the proposition shows that the values (4.30) are the only n-th roots of unity, i.e. that there can be no other n-th roots of 1. This completes the proof of the proposition. □

Therefore, Proposition 4.126 provides formulas for all the n-th roots of unity. Let us now see what these numbers look like for various values of n.

To simplify the upcoming computations, we can observe the following. Given $\theta \in \mathbb{R}$, the complex number $e^{\theta i} = 1 \cdot e^{\theta i} \in \mathbb{C}$, expressed in polar form, has modulus $r = 1$ and argument θ. It follows that $e^{\theta i}$ *is the point on the complex plane that is of distance* 1 *from the origin and of angle* θ *from the positive* x*-axis*; see the illustration below.

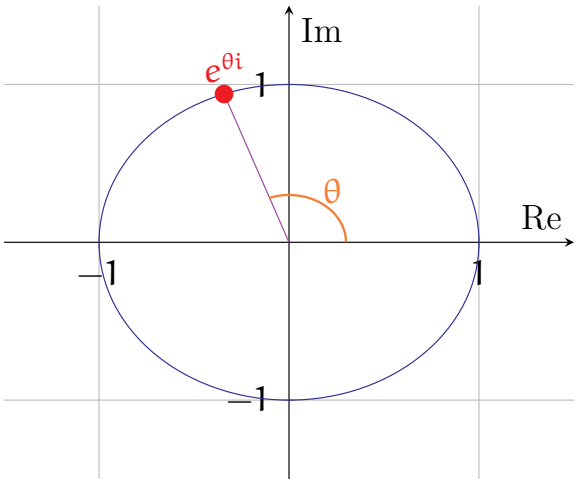


FIGURE 4.10. A plot of the point $e^{\theta i}$ on the complex plane. The blue (unit) circle is the set of all points of distance 1 from the origin. $e^{i\theta}$ is the point on this blue circle, with (signed) angle θ from the positive x-axis.

Example 4.127. *We first consider* $n = 2$*, i.e. all the complex square roots of* 1*. By Proposition 4.126, the square roots of* 1 *are given by*

$$e^{\frac{2\pi m}{2} i} = e^{m\pi i}, \qquad m \in \mathbb{Z}.$$

By putting in various values of m*, we can see what these square roots are:*

- *When* $m = 0$*, we obtain* $e^0 = 1$*.*
- *When* $m = 1$*, we have* $e^{\pi i} = -1$*. (Recall from the preceding discussion that* $e^{\pi i}$ *has distance* 1 *from the origin and angle* $\pi = 180^\circ$ *from the positive* x*-axis.)*
- *When* $m = 2$*, we have* $e^{2\pi i} = 1$*.*
- *For larger values* $m > 2$*, the values of* $e^{m\pi i}$ *repeat. More specifically,* $e^{m\pi i} = 1$ *when* m *is even, while* $e^{m\pi i} = -1$ *when* m *is odd.*
- *The same pattern holds for negative values of* m*—once again,* $e^{m\pi i} = 1$ *when* m *is even, and* $e^{m\pi i} = -1$ *when* m *is odd.*

From the above, we see there are two distinct complex square roots of 1*:*

$$e^{0\pi i} = +1, \qquad e^{1\pi i} = -1.$$

The left part of Figure 4.11 illustrates the square roots of 1 *on the complex plane. Note, in particular, the complex square roots of* 1 *are the same as the real square roots of* 1*.*

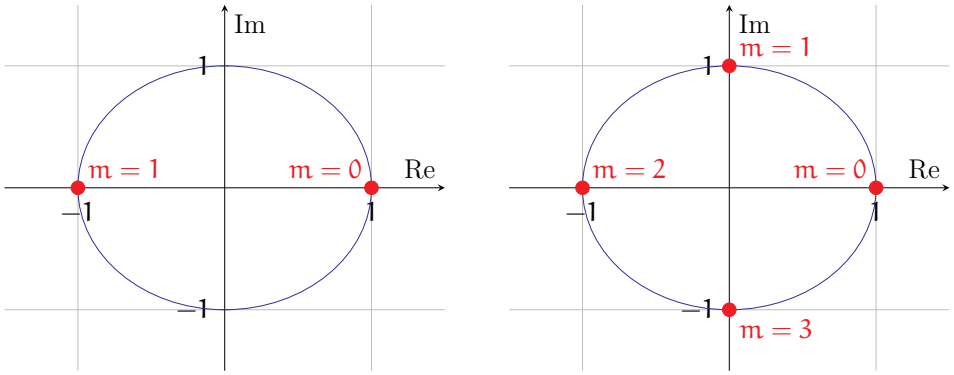


FIGURE 4.11. The red dots in the above graphics indicate all of the n-th roots of unity $e^{\frac{2\pi m}{n}i}$, for $n = 2$ (left) and $n = 4$ (right).

Example 4.128. *Next, consider* $n = 4$*, i.e. all the complex fourth roots of* 1*.*

By Proposition 4.126, the fourth roots of 1 *are*

$$e^{\frac{2\pi m}{4}i} = e^{\frac{m\pi}{2}i}, \qquad m \in \mathbb{Z}.$$

- *When* $m = 0$*, we obtain* $e^0 = 1$*.*
- *When* $m = 1$*, we obtain* $e^{\frac{\pi}{2}i} = i$*.*
- *When* $m = 2$*, we obtain* $e^{\pi i} = -1$*.*
- *When* $m = 3$*, we obtain* $e^{\frac{3\pi}{2}i} = -i$*.*
- *For* $m = 4$*, we have* $e^{2\pi i} = 1$*, so that we have returned to the same value as for* $m = 0$*. For* $m > 4$*, as well as for* $m < 0$*, the above values repeat (since* sin *and* cos *are periodic), so we do not obtain any new numbers.*

As a result, we obtain four distinct complex fourth roots of 1*:*

$$e^{\frac{0\pi}{2}i} = +1, \qquad e^{\frac{1\pi}{2}i} = +i, \qquad e^{\frac{2\pi}{2}i} = -1, \qquad e^{\frac{3\pi}{2}i} = -i.$$

Two of these $(+1, -1)$ *are just the real fourth roots of* 1*, while the other two* $(+i, -i)$ *can only be found by looking at the complex plane; see the right half of Figure 4.11.*

Example 4.129. *Let us now consider $n = 3$, i.e. all the complex cube roots of 1.*

Once again, by Proposition 4.126, the cube roots of 1 are

$$e^{\frac{2\pi m}{3}i}, \qquad m \in \mathbb{Z}.$$

- *When $m = 0$, we obtain $e^0 = 1$.*
- *When $m = 1$, we obtain $e^{\frac{2\pi}{3}i} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$.*
- *When $m = 2$, we obtain $e^{\frac{4\pi}{3}i} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$.*
- *When $m \geq 3$ or $m < 0$, the above values are repeated.*

As a result, there are three distinct complex cube roots of 1:

$$e^{\frac{0\pi}{3}i} = 1, \qquad e^{\frac{2\pi}{3}i} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \qquad e^{\frac{4\pi}{3}i} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

In particular, one of the above (namely, 1) is the usual real cube root of 1, while the other two can only be found by looking at the complex plane; see the left half of Figure 4.12.

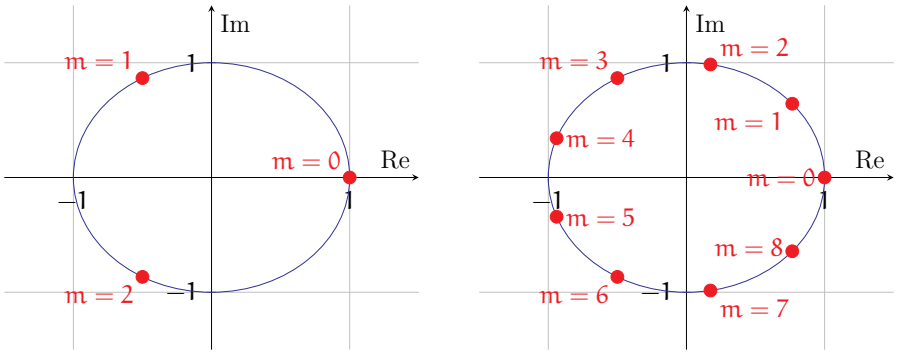


FIGURE 4.12. The red dots in the above graphics indicate all of the n-th roots of unity $e^{\frac{2\pi m}{n}i}$, for $n = 3$ (left) and $n = 9$ (right).

From Examples 4.127–4.129, one can start to see a pattern. Indeed, the computations from these examples extend to n-th roots of unity, for any $n \in \mathbb{N}$.

To summarise, the n-th roots of unity are given by

$$e^{\frac{2\pi m}{n}i}, \qquad m \in \mathbb{Z}.$$

The above numbers take on n distinct values, given by $m = \{0, 1, \ldots, n-1\}$. (The values repeat once $m \geq n$ and $m < 0$.) By examining the polar forms of these numbers, we can conclude that *there are n distinct n-th roots of unity*, and that on the complex plane, *these roots are equally spaced apart on the unit circle about the origin.*

Finally, the right part of Figure 4.12 shows all the 9-th roots of unity.

4.10.4. *The Fundamental Theorem of Algebra.* From the previous discussion, we derived that given any $n \in \mathbb{N}$, there are exactly n distinct n-th roots of unity:

$$e^{\frac{2\pi m}{n}i}, \qquad m \in \{0, 1, 2, \ldots, n-1\}.$$

In other words, the above values are precisely the solutions of the polynomial equation

$$z^n - 1 = 0.$$

One consequence of this is that *we can fully factor* $z^n - 1$ *as*

$$z^n - 1 = \prod_{m=0}^{n-1} \left(z - e^{\frac{2\pi m}{n}i}\right), \tag{4.31}$$

that is, as a product of linear polynomials. When $n = 2$, as in Example 4.127, we obtain the same factorisation as one would when working only with the real numbers:

$$z^2 - 1 = (z-1)(z+1).$$

However, for $n > 2$, we can do more with complex numbers than with real numbers:

Example 4.130. *Consider the case* $n = 4$. *In terms of* $\mathbb{R}$, *one can only factor*

$$\begin{aligned} x^4 - 1 &= (x^2 - 1)(x^2 + 1) \\ &= (x-1)(x+1)(x^2+1). \end{aligned}$$

In particular, the factor $x^2 + 1$ *cannot be reduced any further.*

However, in terms of $\mathbb{C}$, *then by* (4.31) *and Example 4.128, we can fully factor*

$$z^4 - 1 = (z-1)(z+1)(z-i)(z+i).$$

One way to think of this is that $\mathbb{R}$ *is "missing some numbers", which prevents us from fully factoring* $x^4 - 1$. *In contrast, those missing numbers (namely,* $+i$ *and* $-i$*) are found in* $\mathbb{C}$, *so that* $z^4 - 1$ *could now be fully factored using complex numbers.*

Example 4.131. *Similarly, consider* $n = 3$. *In terms of* $\mathbb{R}$, *one can only factor*

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

However, in $\mathbb{C}$, *we can fully factor (see* (4.31) *and Example 4.129)*

$$z^3 - 1 = (z-1)\left(z + \tfrac{1}{2} - \tfrac{\sqrt{3}}{2}i\right)\left(z + \tfrac{1}{2} + \tfrac{\sqrt{3}}{2}i\right).$$

Once again, the numbers missing from the real line, which prevented us from fully factoring $x^3 - 1$, can be found on the complex plane.

The idea behind Examples 4.130 and 4.131 extends to any $n \in \mathbb{N}$. Whenever $n > 2$, one cannot fully factor $x^n - 1$ in terms of real numbers. However, once we expand our perspective to complex numbers, then $z^n - 1$ can be fully factored as in (4.31).

Now, all of the previous discussion concerned only the particular polynomial $z^n - 1$. However, what is far more incredible is that the same conclusions actually apply to *every complex polynomial*. This observation is of such importance in mathematics that it has earned the lofty nickname of fundamental theorem of algebra.

Theorem 4.132 (Fundamental theorem of algebra)**.** *Any complex polynomial*

$$f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0,$$

where $n \in \mathbb{N}$, and where $a_0, a_1, \ldots, a_{n-1} \in \mathbb{C}$, can be fully factored as

$$f(z) = \prod_{k=1}^{n} (z - \lambda_k),$$

for some $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{C}$.

The fundamental theorem of algebra suggests $\mathbb{C}$ is quite "complete", as there are no "missing numbers" preventing us from doing algebraic things, e.g. factoring polynomials.

Note. *There are many different proofs of the fundamental theorem of algebra, though these are beyond the scope of this module. (One relatively simple proof uses complex analysis, which you will see later on in your degree.) What is rather amusing is that despite the theorem name, none of the elementary (i.e. accessible at the undergraduate level) proofs is actually based on algebraic methods!*

Finally, while we have motivated complex numbers in terms of overcoming deficiencies in the real number line, they also have many other important applications. For instance, complex numbers are widely used in a number of fields, ranging from electromagnetism to electronic circuits to quantum mechanics. In particular, it is often more convenient to represent various physical quantities in terms of complex numbers, and one can sometimes simplify algebraic computations by doing so.

5. Relations and Functions

At this point, we have described several types of quantities, such as sets and various types of numbers. However, for all this to be useful, we must also describe *relationships* between such quantities. While we have already accomplished this in a few special cases (e.g. greatest common divisors of integers, modulus of complex numbers), we next develop the language to discuss these relationships in a general and systematic manner.

This will be accomplished through abstract notions such as *relations* and *functions*, with which you should already have some familiarity. In this chapter, we study both concepts in detail, both abstractly and in various concrete settings.

5.1. Ordered Pairs.

Before getting to relations or functions, we must first construct the basic objects representing two quantities that are "related to each other"—namely, *ordered pairs*. Recall that due to how sets are defined, there is no concept of "order of elements" in a set. As a result, to make sense of ordered pairs, we will need a new type of object:

Definition 5.1. *We let* (a, b) *denote the ordered pair containing the quantities* a *and* b *(in that order). The defining property of ordered pairs is as follows:*

- *For any* a, b, c, d, *we have* $(a, b) = (c, d)$ *if and only if both* $a = c$ *and* $b = d$.

More formally, the above can be precisely described as follows:

$$\forall_{a,b,c,d}[(a, b) = (c, d) \Leftrightarrow (a = c \text{ and } b = d)].$$

Again, the key feature of ordered pairs, in contrast to sets, is that the order in which the quantities appear in these pairs now matters.

Example 5.2. *The following pairs are not the same:*

$$(1, 2) \neq (2, 1).$$

In particular, in the context of Definition 5.1, we have

$$a = 1, \qquad b = 2, \qquad c = 2, \qquad d = 1.$$

Thus, since $a \neq c$ *and* $b \neq d$ *in the above, it follows that indeed,* $(1, 2) \neq (2, 1)$.

Observe that the above is in direct contrast to the nature of sets, since $(1, 2)$ *and* $(2, 1)$ *are distinct quantities*, while $\{1, 2\}$ *and* $\{2, 1\}$ *describe the same set.*

Example 5.3. *Similarly, ordered pairs are considered to be different from "non-pair quantities". For instance, by our construction, we have that* $(1,1) \neq 1$.

Note. *In Definition 5.1, we established ordered pairs as a brand new kind of object that is distinct from sets. However, this is philosophically unpleasant, since one must make a substantial assumption that such objects exist in our mathematical universe.*

An alternative approach is to define ordered pairs by making clever use of existing quantities. One commonly used formal definition (due to Kuratowski) is given by

$$(a,b) = \{\{a\},\{a,b\}\}. \tag{5.1}$$

On one hand, the definition (5.1) *is flagrantly non-intuitive, and no one would ever think of an ordered pair this way. However, one can prove that if one defines* (a,b) *as in* (5.1)*, then this satisfies the key property of ordered pairs in Definition 5.1. Thus, the philosophical advantage of the definition* (5.1) *is that one can make sense of ordered pairs without imposing additional axioms in our formal theory.*

5.1.1. *Cartesian Products.* Having defined ordered pairs, the next task is to consider various sets of ordered pairs. The simplest examples of such sets are as follows:

Definition 5.4. *Let* A *and* B *be sets. The Cartesian product of* A *and* B *is defined as*

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

In other words, $A \times B$ *is the set of all possible ordered pairs* (a,b)*, such that the first component* a *is in* A *and the second component* b *is in* B.

Example 5.5. *As a simple example, consider the sets*

$$A = \{1,2\}, \qquad B = \{1,2,3\}.$$

Then, the Cartesian product $A \times B = \{1,2\} \times \{1,2,3\}$ *consists of all pairs* (a,b)*, such that* a *is* 1 *or* 2*, and such that* b *is* 1*,* 2*, or* 3*. As a result, we have*

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

Example 5.6. *The Cartesian product*

$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\}$$

is the set of all ordered pairs of real numbers. For instance, we have

$$(1, 1), (5.2, -2.7), \left(\pi^2, -\tfrac{7}{3}\right) \in \mathbb{R} \times \mathbb{R}.$$

In particular, if we think of the components x and y of an ordered pair $(x, y) \in \mathbb{R} \times \mathbb{R}$ as horizontal and vertical coordinates, respectively, then we can geometrically interpret $\mathbb{R} \times \mathbb{R}$ as the set of all points on the Euclidean plane.

It is customary to abbreviate the Cartesian product $\mathbb{R} \times \mathbb{R}$ as $\mathbb{R}^2$. (Similar conventions hold even when one replaces "$\mathbb{R}$" by any other set.) We will avoid doing so in this module, but you may have already seen such notations elsewhere, such as in calculus.

Example 5.7. *We can also mix and match sets. For instance,*

$$\mathbb{R} \times \mathbb{Z} = \{(x, k) \mid x \in \mathbb{R} \text{ and } k \in \mathbb{Z}\}$$

is the set of all ordered pairs (x, k), with x a real number and k an integer.

Note. *Definition 5.1 can be directly extended to "ordered n-tuples" for any $n \in \mathbb{N}$. For instance, when $n = 3$, the defining property of ordered triples is as follows:*

$$(a, b, c) = (d, e, f) \Leftrightarrow (a = d \text{ and } b = e \text{ and } c = f).$$

Similarly, given sets A, B, C, we can define the triple Cartesian product by

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

Next, for arbitrary $n \in \mathbb{N}$, the defining property of ordered n-tuples is

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \Leftrightarrow \forall_{i \in \{1,2,\ldots,n\}} a_i = b_i.$$

The corresponding Cartesian product can also be analogously defined.

5.2. **Relations.** Recall that an ordered pair (a, b) is used to represent some existing "relationship" between a and b. Thus, in order to describe connections between quantities, we will want to study more elaborate sets of ordered pairs. This leads us to the following:

Definition 5.8. *Let A and B be sets.*

- *Any subset R of $A \times B$ is called a relation from A to B.*
- *As a special case, any subset R of $A \times A$ is called a relation on A.*

Furthermore, given a relation R from A to B:

- *We often write "$a \ R \ b$" as shorthand for the statement $(a, b) \in R$.*
- *Similarly, we write "$a \not R \ b$" as shorthand for $(a, b) \notin R$.*

Example 5.9. *Let $A = \{1, 2, 3, 4, 5\}$ and $B = \{2, 3, 5\}$. Then, then set*

$$R = \{(1, 2), (2, 3), (4, 5), (5, 5)\}$$

is a relation from A to B, since $R \subseteq A \times B$. Moreover:

- *Since $(1, 2) \in R$, we can write $1 \ R \ 2$.*
- *Since $(3, 3) \notin R$, we can also write $3 \not R \ 3$.*

The next example shows that "$\leq$ defines a relation on $\mathbb{R}$":

Example 5.10. *Consider the set*

$$L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}.$$

(L is the set of all pairs of real numbers, in which the first component is less than or equal to the second.) Note that L is a relation on $\mathbb{R}$, since $L \subseteq \mathbb{R} \times \mathbb{R}$.

Observe that for any $x, y \in \mathbb{R}$, we have, from Definition 5.8, that

$$\begin{aligned} x \ L \ y &\Leftrightarrow (x, y) \in L \\ &\Leftrightarrow x \leq y. \end{aligned}$$

In other words, L can be equivalently described as follows:

- *L is the relation on $\mathbb{R}$ satisfying $x \ L \ y$ if and only if $x \leq y$, for all $x, y \in \mathbb{R}$.*

Note that L contains exactly the same content as the "$\leq$" relationship on $\mathbb{R}$.

Following from Example 5.10, if we think a bit less formally, we can then view L and "$\leq$" as essentially the same object, since both capture the same content. As a result, in practice, we tend to think of "$\leq$" itself as a relation on $\mathbb{R}$.

Note. *By replacing "$\mathbb{R}$" in Example 5.10 by $\mathbb{Q}$, $\mathbb{Z}$, or $\mathbb{N}$, we can also see, from an analogous argument, that "$\leq$" defines relations on $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{N}$.*

Next, by analogous reasoning, we can show that "$=$" also defines relations:

Example 5.11. *Let A be any set, and let*

$$\begin{aligned} E &= \{(x, y) \in A \times A \mid x = y\} \\ &= \{(x, x) \mid x \in A\}. \end{aligned}$$

Similar to Example 5.10, we have that E is a relation on A, since $E \subseteq A \times A$.

An equivalent way to describe E is as follows:

- *E is the relation on A satisfying $x \mathrel{E} y$ if and only if $x = y$, for all $x, y \in A$.*

Thus, the relation E contains exactly the same content as "$=$" on A.

Examples 5.10 and 5.11 show that many familiar concepts which signify relationships, such as "$\leq$" and "$=$", can be described via relations. In other words, the concept of relations is general enough to encompass "$\leq$" and "$=$", along with many more possibilities.

Example 5.12. *Consider the relations $D_{\mathbb{Z}}$ on $\mathbb{Z}$ and $D_{\mathbb{N}}$ on $\mathbb{N}$, given by*

$$\begin{aligned} D_{\mathbb{Z}} &= \left\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \;\middle|\; a \mid b\right\}, \\ D_{\mathbb{N}} &= \left\{(m, n) \in \mathbb{N} \times \mathbb{N} \;\middle|\; m \mid n\right\}. \end{aligned}$$

Note $D_{\mathbb{Z}}$ and $D_{\mathbb{N}}$ can be equivalently defined as:

- *$D_{\mathbb{Z}}$ is the relation on $\mathbb{Z}$ satisfying $x \mathrel{D_{\mathbb{Z}}} y$ if and only if $x \mid y$, for all $x, y \in \mathbb{Z}$.*
- *$D_{\mathbb{N}}$ is the relation on $\mathbb{N}$ satisfying $x \mathrel{D_{\mathbb{N}}} y$ if and only if $x \mid y$, for all $x, y \in \mathbb{N}$.*

Both $D_{\mathbb{Z}}$ and $D_{\mathbb{N}}$ contain the same information as divisibility (i.e. "$\mid$" from Definition 4.18). Note, however, that the relation $D_{\mathbb{Z}}$ describes divisibility on all the integers, while $D_{\mathbb{N}}$ restricts this notion to only the natural numbers.

Example 5.13. *Consider the following relation on $\mathbb{Q}$:*

$$R = \{(p, q) \in \mathbb{Q} \times \mathbb{Q} \mid pq \in \mathbb{Z}\}.$$

An equivalent description of R *is the following:*

- R *is the relation on* $\mathbb{Q}$ *satisfying* $p\ R\ q$ *if and only if* $pq \in \mathbb{Z}$*, for all* $p, q \in \mathbb{Q}$*.*

In particular:

- *Both* $1\ R\ 3$ *and* $3\ R\ 1$ *hold, since* $1 \cdot 3 = 3 \cdot 1 \in \mathbb{Z}$*.*
- *Both* $\frac{1}{2} \not R\ \frac{7}{3}$ *and* $\frac{7}{3} \not R\ \frac{1}{2}$ *hold, since* $\frac{1}{2} \cdot \frac{7}{3} = \frac{7}{3} \cdot \frac{1}{2} \notin \mathbb{Z}$*.*
- *Both* $4\ R\ (-\frac{7}{2})$ *and* $(-\frac{7}{2})\ R\ 4$ *hold, since* $4 \cdot (-\frac{7}{2}) = (-\frac{7}{2}) \cdot 4 \in \mathbb{Z}$*.*

Example 5.14. *Let* A *be any set. Then, the following defines a relation on* $\mathcal{P}(A)$*:*

$$S = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid X \subseteq Y\}.$$

(Recall $\mathcal{P}(A)$ *denotes the power set of* A*, that is, the set of all subsets of* A*; see Definition 3.29.) Moreover, an equivalent description of* S *is:*

- S *is the relation on* $\mathcal{P}(A)$ *satisfying* $X\ S\ Y \Leftrightarrow X \subseteq Y$*, for all* $X, Y \in \mathcal{P}(A)$*.*

In particular, S *contains the same information as the notion of subset (i.e. "*$\subseteq$*").*

To be more concrete, consider the special case $A = \mathbb{N}$*, and let*

$$C_2 = \{2k \mid k \in \mathbb{N}\}, \qquad C_3 = \{3k \mid k \in \mathbb{N}\}, \qquad C_4 = \{4k \mid k \in \mathbb{N}\}.$$

Then, the following statements hold:

- $C_4\ S\ C_2$*, since* C_4, C_2 *are both subsets of* $\mathbb{N}$*, and* $C_4 \subseteq C_2$*.*
- $C_2 \not S\ C_4$*, since* C_2 *is not a subset of* C_4*.*
- $C_3 \not S\ C_2$*, since* C_3 *is not a subset of* C_2*.*
- $C_2\ S\ \mathbb{N}$*, since* $C_2, \mathbb{N}$ *are both subsets of* $\mathbb{N}$*.*

5.2.1. *Properties of Relations.* There are several useful properties that are satisfied by many relations. For convenience, these properties are given names, which are widely used in mathematics. In the following, we discuss a few especially common properties:

Definition 5.15. *Let* A *be a set, and let* R *be a relation on* A*.*

(1) R *is reflexive iff* $a\ R\ a$ *for all* $a \in A$*.*
(2) R *is symmetric iff* $a\ R\ b$ *implies* $b\ R\ a$ *for any* $a, b \in A$*.*
(3) R *is antisymmetric iff* $a\ R\ b$ *and* $b\ R\ a$ *together imply* $a = b$ *for all* $a, b \in A$*.*
(4) R *is transitive iff* $a\ R\ b$ *and* $b\ R\ c$ *together imply* $a\ R\ c$ *for all* $a, b, c \in A$*.*

Note. *For clarity, we can rewrite Definition 5.15 using more precise language:*

- R *is reflexive iff* $\forall_{a \in A}(a \mathrel{R} a)$.
- R *is symmetric iff* $\forall_{a,b \in A}(a \mathrel{R} b \Rightarrow b \mathrel{R} a)$.
- R *is antisymmetric iff* $\forall_{a,b \in A}((a \mathrel{R} b \text{ and } b \mathrel{R} a) \Rightarrow a = b)$.
- R *is transitive iff* $\forall_{a,b,c \in A}((a \mathrel{R} b \text{ and } b \mathrel{R} c) \Rightarrow a \mathrel{R} c)$.

Note. *In spite of what the names may suggest, "antisymmetric" does not mean the same as "not symmetric". In particular, a relation could be both antisymmetric and symmetric. Similarly, a relation could also be neither antisymmetric nor symmetric.*

Let us now see how Definition 5.15 applies to various examples of relations.

Example 5.16. *Consider the relation "$\leq$" on $\mathbb{R}$ that was discussed in Example 5.10. (To have more intuitive notation, we will write "$\leq$" in the place of "L".) Then:*

- *"$\leq$" is reflexive, since $x \leq x$ holds for all $x \in \mathbb{R}$. (See Proposition 4.7 (1).)*
- *"$\leq$" is antisymmetric, since given any $x, y \in \mathbb{R}$, if both $x \leq y$ and $y \leq x$ hold, then it must be that $x = y$. (See Proposition 4.7 (2).)*
- *"$\leq$" is transitive, since given any $x, y, z \in \mathbb{R}$, if both $x \leq y$ and $y \leq z$ hold, then $x \leq z$ must hold. (See Proposition 4.7 (3).)*
- *On the other hand, "$\leq$" is not symmetric. To see this, one can observe, for example, that $1 \leq 2$, but $2 \not\leq 1$. (Do take a minute to understand how the above achieves the negation of the definition for "symmetric"!)*

In fact, any relation on a set A that is reflexive, antisymmetric, and transitive is known as a partial ordering of A. This terminology comes from the fact that any relation satisfying all three properties behaves qualitatively similarly to "$\leq$".

Example 5.17. *Let A be any set, and consider the relation "$\subseteq$" on $\mathcal{P}(A)$ from Example 5.14. (Again, for ease of notation, we will write "$\subseteq$" in the place of "S".) Then:*

- *"$\subseteq$" is reflexive, since $X \subseteq X$ holds for all $X \in \mathcal{P}(A)$. (See Proposition 3.27 (1).)*
- *"$\subseteq$" is antisymmetric, since given any $X, Y \in \mathcal{P}(A)$, if both $X \subseteq Y$ and $Y \subseteq X$ hold, then $X = Y$ holds. (See Proposition 3.28.)*

- *"$\subseteq$" is transitive, since given any $X, Y, Z \in \mathcal{P}(A)$, if both $X \subseteq Y$ and $Y \subseteq Z$ hold, then $X \subseteq Z$ holds. (This was a problem sheet exercise.)*
- *If $X \neq \emptyset$, then "$\subseteq$" is not symmetric. This follows since $\emptyset \subseteq X$, but $X \not\subseteq \emptyset$.*

In particular, Example 5.17 shows that "$\subseteq$" is also a partial ordering (of $\mathcal{P}(A)$). Qualitatively speaking, this shows that "$\subseteq$" is "similar in nature to $\leq$", in that *"$\subseteq$" provides what could be thought of as an ordering or ranking of all the subsets of A.*

Example 5.18. *Consider now the divisibility relation "$\mid$" on $\mathbb{Z}$ from Example 5.12. (For ease of notation, we will write "$\mid_{\mathbb{Z}}$" in the place of "$D_{\mathbb{Z}}$".) Then:*

- *"$\mid_{\mathbb{Z}}$" is reflexive, since $a \mid a$ holds for all $a \in \mathbb{Z}$. (See Proposition 4.22 (1).)*
- *"$\mid_{\mathbb{Z}}$" is transitive, since given any $a, b, c \in \mathbb{Z}$, if both $a \mid b$ and $b \mid c$ hold, then $a \mid c$ also holds. (See Proposition 4.23 (1).)*
- *"$\mid_{\mathbb{Z}}$" is not symmetric, since, e.g. $2 \mid 4$ but $4 \nmid 2$.*
- *"$\mid_{\mathbb{Z}}$" is not antisymmetric, since, e.g. $2 \mid (-2)$ and $(-2) \mid 2$, but $2 \neq -2$.*

Example 5.19. *Consider now the relation "$\mid$" on $\mathbb{N}$ instead, i.e. $D_{\mathbb{N}}$ from Example 5.12. (To distinguish from Example 5.18, we denote this relation by "$\mid_{\mathbb{N}}$".) Then:*

- *By the same reasonings as Example 5.18, we deduce that "$\mid_{\mathbb{N}}$" is both reflexive and transitive, and that "$\mid_{\mathbb{N}}$" is not symmetric.*
- *In contrast to Example 5.18, however, "$\mid_{\mathbb{N}}$" is antisymmetric.*

Proof that $\mid_{\mathbb{N}}$ is antisymmetric. Let $a, b \in \mathbb{N}$, and assume $a \mid b$ and $b \mid a$. Then, since $a, b > 0$, we have that both $a \leq b$ and $b \leq a$, which implies $a = b$. □

Examples 5.18 and 5.19 together show that the *properties of a relation can be sensitive to the set that the relation acts on.* Indeed, divisibility fails to be antisymmetric when we consider all the integers, while divisibility becomes antisymmetric once we restrict its scope to only the natural numbers. Consequently, it is important that *when describing a relation, we also specify the underlying set that the relation acts on.*

Example 5.20. *Consider the relation R on $\mathbb{Q}$ from Example 5.13:*

- *$p \mathrel{R} q$ if and only if $pq \in \mathbb{Z}$, for all $p, q \in \mathbb{Q}$.*

Once again, we can check which properties are satisfied by R*:*

- R *is not reflexive, since, e.g.* $\frac{1}{2} \not R \frac{1}{2}$ *(as* $\frac{1}{2} \cdot \frac{1}{2} \notin \mathbb{Z}$*).*
- R *is not transitive. To see this, one can simply observe that* $\frac{1}{2}\ R\ 4$ *(since* $\frac{1}{2} \cdot 4 \in \mathbb{Z}$*) and* $4\ R\ \frac{1}{4}$ *(since* $4 \cdot \frac{1}{4} \in \mathbb{Z}$*), however* $\frac{1}{2} \not R \frac{1}{4}$ *(since* $\frac{1}{2} \cdot \frac{1}{4} \notin \mathbb{Z}$*).*
- R *is not antisymmetric. To see this, one can observe that both* $\frac{1}{2}\ R\ 2$ *and* $2\ R\ \frac{1}{2}$ *hold (since* $\frac{1}{2} \cdot 2 = 2 \cdot \frac{1}{2} \in \mathbb{Z}$*), however* $\frac{1}{2} \neq 2$*.*
- R *is symmetric. To prove this, let* $p, q \in \mathbb{Q}$*, and suppose* $p\ R\ q$*. Then,* $pq \in \mathbb{Z}$*, and hence* $qp = pq \in \mathbb{Z}$ *as well, which implies* $q\ R\ p$*.*

Example 5.21. *Consider the relation* R *on* $\{1, 2, 3\}$ *that is given by*

$$R = \{(1,1), (1,2), (1,3), (2,2), (3,3)\}.$$

(Unlike preceding examples, there is no convenient description of R *of the form "*$x\ R\ y$ *if and only if ...", so we will have make do with the above set description.)*

Let us check which properties are satisfied by R*:*

- R *is reflexive, since the above definition of* R *yields that* $1\ R\ 1$*,* $2\ R\ 2$*, and* $3\ R\ 3$ *all hold (that is,* $a\ R\ a$ *for every* $a \in \{1, 2, 3\}$*).*
- R *is not symmetric, since* $1\ R\ 2$*, but* $2 \not R\ 1$*.*
- R *is transitive. You will have to check all the cases carefully, however you can see from the definition of* R *that given any* $a, b, c \in \{1, 2, 3\}$*, if both* $a\ R\ b$ *and* $b\ R\ c$ *hold, then* $a\ R\ c$ *must always hold as well.*
- R *is antisymmetric. Again, you need to check all cases carefully, but you can see that given* $a, b \in \{1, 2, 3\}$*, both* $a\ R\ b$ *and* $b\ R\ a$ *hold only when* $a = b$*.*

5.3. **Equivalence Relations.** In this section, we focus on a special class of relations:

Definition 5.22. *Let* A *denote a set. A relation on* A *that is reflexive, symmetric, and transitive is called an equivalence relation on* A*.*

Example 5.23. *Let* A *be any set, and consider the relation "*$=$*" on* A *from Example 5.11. (Here, we write "*$=$*" in the place of "*$\in$*".) Then:*

- *"*$=$*" is reflexive, since* $x = x$ *holds for all* $x \in A$*.*

- *"$=$" is symmetric, since for any $x, y \in A$, if $x = y$, then $y = x$.*
- *"$=$" is transitive, since for all $x, y, z \in A$, if $x = y$ and $y = z$, then $x = z$.*

As a result, "$=$" is an equivalence relation on A by Definition 5.22.

(Note in addition that "$=$" is antisymmetric. This follows trivially from the definition—given $x, y \in A$, if $x = y$ and $y = x$, then clearly $x = y$.)

"$=$", from Example 5.23 is the prototypical example of an equivalence relation. In fact, an equivalence relation R on a set A can be viewed as R behaving similarly to "$=$". Given any $x, y \in A$, *we can interpret the statement* $x \mathrel{R} y$ *as* x *"being the same as"* y.

In this way, equivalence relations serve as an abstraction of this notion of "sameness". Through this, we have broad flexibility in what we prescribe as "the same":

Example 5.24. *Let T be the relation on $\mathbb{R}$ defined by the condition*

- $x \mathrel{T} y$ *if and only if $x - y \in \mathbb{Z}$, for any $x, y \in \mathbb{R}$.*

Let us confirm that T is an equivalence relation on $\mathbb{R}$:

- *T is reflexive, since $x - x = 0 \in \mathbb{Z}$ for any $x \in \mathbb{R}$.*
- *T is symmetric, since for all $x, y \in A$, if $x - y \in \mathbb{Z}$, then*

$$y - x = (x - y) \in \mathbb{Z}.$$

- *T is transitive, since for all $x, y, z \in A$, if $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$, then*

$$x - z = (x - y) + (y - z) \in \mathbb{Z}.$$

Thus, we conclude that T is indeed an equivalence relation on $\mathbb{R}$.

In the setting of Example 5.24, two real numbers are considered "the same" (via T) if and only if their difference is an integer. Thus, with respect to T, the numbers 1.34, 3.34, and -12.34 would be considered "the same", while 109.45 and -7.5 are considered "different".

In the upcoming discussions, it will be useful to group together all the elements that are considered "the same" via an equivalence relation:

Definition 5.25. *Let R be an equivalence relation on a set A, and let $a \in A$. We then define the (R-)equivalence class of a, denoted $[a]_R$, to be the set*

$$[a]_R = \{b \in A \mid a \mathrel{R} b\}.$$

Example 5.26. *Let A be any set, and consider the relation "$=$" on A from Examples 5.11 and 5.23. Then, given any $a \in A$, its equivalence class, with respect to "$=$", is*

$$\begin{aligned}[a]_= &= \{b \in A \mid a = b\} \\ &= \{a\}.\end{aligned}$$

In other words, $[a]_=$ is the set containing only a itself.

Example 5.27. *Consider the relation T on $\mathbb{R}$ from Example 5.24:*

- *$x \mathrel{T} y$ if and only if $x - y \in \mathbb{Z}$.*

Then, for any $x \in \mathbb{R}$, its T-equivalence class is

$$\begin{aligned}[x]_T &= \{y \in \mathbb{R} \mid x \mathrel{T} y\} \\ &= \{y \in \mathbb{R} \mid x - y \in \mathbb{Z}\}.\end{aligned}$$

To be more concrete, let us compute a few equivalence classes:

- *For $x = 0$, we have $[0]_T = \{y \in \mathbb{R} \mid -y \in \mathbb{Z}\}$. Note the latter set is nothing more than the set of integers, hence we have $[0]_T = \mathbb{Z}$.*
- *For $x = 2.14$, we have $[2.14]_T = \{y \in \mathbb{R} \mid 2.14 - y \in \mathbb{Z}\}$. Note this set consists of all the numbers whose decimal part is 0.14—e.g. $3.14, 0.14, -2.14 \in [2.14]_T$. As a result, this equivalence class can be more clearly written as*

$$[2.14]_T = \{k + 0.14 \mid k \in \mathbb{Z}\}.$$

5.3.1. *Modular Arithmetic.* Next, we apply the language of equivalence relations to construct some new number systems. The starting points for this are the following relations:

Definition 5.28. *Given any $n \in \mathbb{N}$, we define the following relation on $\mathbb{Z}$:*

$$M_n = \left\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \,\middle|\, n \mid (b - a)\right\}.$$

Note that M_n can be equivalently described as:

- *$a \mathrel{M_n} b$ if and only if $n \mid (b - a)$, for any $a, b \in \mathbb{Z}$.*

Notice that *one can interpret the statement* $a \mathrel{M_n} b$, for any $a, b \in \mathbb{Z}$, *as* a *and* b *having the same remainder when both numbers are divided by* n.

Note. *The more common notation for "$a\ M_n\ b$", which you may have seen before, is*

$$a \equiv b \pmod{n}.$$

However, we will not need to use this notation within this module.

Proposition 5.29. *M_n is an equivalence relation on $\mathbb{Z}$ for any $n \in \mathbb{N}$.*

Proof of Proposition 5.29. Let $n \in \mathbb{N}$. In order complete the proof, it suffices by Definition 5.22 to show that M_n is reflexive, symmetric, and transitive.

First, given any $a \in \mathbb{Z}$, we have that $a\ M_n\ a$ holds, since $a - a = 0$, and since $n \mid 0$ by definition. Therefore, it follows that M_n is reflexive.

Next, let $a, b \in \mathbb{Z}$, and suppose $a\ M_n\ b$. Then, by definition, we have $n \mid (b - a)$. Since $a - b = -1(b - a)$, we also have $n \mid (a - b)$ (see Proposition 4.23 (1)), and hence $b\ M_n\ a$. As a result, we obtain that M_n is symmetric.

Finally, suppose $a, b, c \in \mathbb{Z}$, and suppose $a\ M_n\ b$ and $b\ M_n\ c$. Then, $n \mid (b - a)$ and $n \mid (c - b)$ both hold. Since $c - a = (c - b) + (b - a)$, it then follows (from Proposition 4.23 (2)) that $n \mid (c - a)$, and hence $a\ M_n\ c$. Thus, M_n is transitive. □

Let us now delve further into the structure of M_n and its equivalence classes. To make the upcoming discussions more concrete, we restrict to the special case $n = 12$. (However, the arguments here will directly extend to any $n \in \mathbb{N}$).

First, note from Definitions 4.18 and 5.28 that for any $a, b \in \mathbb{Z}$,

$$\begin{aligned} a\ M_{12}\ b &\Leftrightarrow 12 \mid (b - a) \\ &\Leftrightarrow \exists_{k \in \mathbb{Z}}(b = a + 12k). \end{aligned} \tag{5.2}$$

From the above, we immediately obtain, for instance, that

- $0\ M_{12}\ 12$, since $12 = 0 + 12 \cdot 1$.
- $1\ M_{12}\ 13$, since $13 = 1 + 12 \cdot 1$.
- $(-1)\ M_{12}\ 11$, since $11 = -1 + 12 \cdot 1$.
- $35\ M_{12}\ (-1)$, since $-1 = 35 + 12 \cdot (-3)$.

These should provide a bit of basic intuition on how M_{12} works.

Recalling Definition 5.25 and (5.2), we see for each $a \in \mathbb{Z}$ that

$$\begin{aligned}[a]_{M_{12}} &= \{b \in \mathbb{Z} \mid a \; M_{12} \; b\} \\ &= \{b \in \mathbb{Z} \mid \exists_{k \in \mathbb{Z}} (b = a + 12k)\} \\ &= \{a + 12k \mid k \in \mathbb{Z}\}.\end{aligned}$$

From the above, we can explicitly compute the various equivalence classes:

$$\begin{aligned}[0]_{M_{12}} &= \{\ldots, -36, -24, -12, 0, 12, 24, 36, \ldots\}, \\ [1]_{M_{12}} &= \{\ldots, -35, -23, -11, 1, 13, 25, 37, \ldots\}, \\ [2]_{M_{12}} &= \{\ldots, -34, -22, -10, 2, 14, 26, 38, \ldots\}, \\ [3]_{M_{12}} &= \{\ldots, -33, -21, -9, 3, 15, 27, 39, \ldots\}, \\ &\vdots \\ [10]_{M_{12}} &= \{\ldots, -26, -14, -2, 10, 22, 34, 46, \ldots\}, \\ [11]_{M_{12}} &= \{\ldots, -25, -13, -1, 11, 23, 35, 47, \ldots\}.\end{aligned} \tag{5.3}$$

So far, so good. However, the interesting bit happens once we go beyond 11:

$$\begin{aligned}[12]_{M_{12}} &= \{\ldots, -24, -12, 0, 12, 24, 36, 48 \ldots\} \\ &= [0]_{M_{12}}.\end{aligned}$$

This pattern continues for successively higher inputs:

$$[12]_{M_{12}} = [0]_{M_{12}}, \qquad [13]_{M_{12}} = [1]_{M_{12}}, \qquad [14]_{M_{12}} = [2]_{M_{12}}, \qquad \ldots. \tag{5.4}$$

By similar computations, we obtain a similar repetition for negative inputs:

$$[-1]_{M_{12}} = [11]_{M_{12}}, \qquad [-2]_{M_{12}} = [10]_{M_{12}}, \qquad [-3]_{M_{12}} = [9]_{M_{12}}, \qquad \ldots. \tag{5.5}$$

From (5.3)–(5.5), we obtain a good idea of the structure of the M_{12}-equivalence classes. In particular, the M_{12}-equivalence classes form a new number system:

$$\ldots, [-1]_{M_{12}} = [11]_{M_{12}}, [0]_{M_{12}}, [1]_{M_{12}}, \ldots, [10]_{M_{12}}, [11]_{M_{12}}, [12]_{M_{12}} = [0]_{M_{12}}, \ldots.$$

Observe that this number system is *finite*, and *its values resemble the numbers on a clock*:

- There are 12 distinct "numbers", ranging from $[0]_{M_{12}}$ to $[11]_{M_{12}}$ (inclusive).
- Beyond the above range, the numbers then loop back to the opposite end.

Therefore, if one counts upward, then after 11, one loops back down to 0, and the numbers repeat. Similarly, counting downward, then before 0, one loops back up to 11.

While the details are a bit beyond the scope of this module, one can also make sense of the usual algebraic operations on this "clock" number system. For instance,

- $[5]_{M_{12}} + [4]_{M_{12}} = [9]_{M_{12}}$.
- $[6]_{M_{12}} + [9]_{M_{12}} = [15]_{M_{12}} = [3]_{M_{12}}$.
- $[5]_{M_{12}} - [7]_{M_{12}} = [-2]_{M_{12}} = [10]_{M_{12}}$.
- $[5]_{M_{12}} \cdot [7]_{M_{12}} = [35]_{M_{12}} = [-1]_{M_{12}}$.
- $[-2]_{M_{12}} \cdot [9]_{M_{12}} = [-18]_{M_{12}} = [6]_{M_{12}}$.

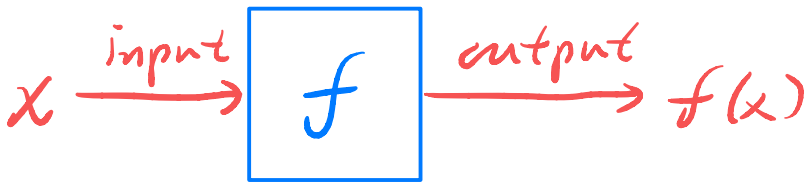
To be more specific, observe that the above operations are identical to those for the integers, except we also take into account that the numbers start repeating after 12 values.

Algebraic computations in the above number system are often nicknamed "clock arithmetic", as this resembles how one might operate with time on a clock. For example, the equation $[6]_{M_{12}} + [9]_{M_{12}} = [3]_{M_{12}}$ mentioned above can be interpreted as follows: "if it is 6 o'clock now, and 9 hours pass, then the time will be 3 o'clock."

Finally, while we worked only with M_{12} for the sake of concreteness, everything here still works if we replace "12" by any other $n \in \mathbb{N}$. The finite number systems created from these M_n-equivalence classes, along with their algebraic operations, are together referred to as modular arithmetic. These number systems play a major role in number theory and cryptography, and you will learn more about them in future algebra modules.

5.4. **Functions.** We now turn our attention to functions, one of the most fundamental concepts in mathematics. At this point, you are likely already quite familiar with functions and do not require much introduction to the intuitions behind them.

Nonetheless, we recall that a function f essentially takes some input, say x, and then produces some output $f(x)$. The most common illustration of functions is to portray one as a "machine", into which one feeds the input, and out of which comes the output. A poorly drawn "machine" is provided below for your entertainment:



Now, the first question we face is *how one should model functions in mathematics.* There are many ways to do this—for example, we can define a new kind of formal object that is a function, similarly to how we constructed ordered pairs. An alternative method, however, is to make use of machinery that we already have—namely, relations.

More specifically, we can think of functions as a special case of relations. Recall that relations model some "relationship" between pairs of quantities. Here, we can *view functions as a special kind of "relationship"*, in particular *between the given input value and the resulting output value.* All this leads to our official definition of functions:

Definition 5.30. *Let* A, B *be arbitrary sets. We say* f *is a function from* A *to* B*, denoted* $f : A \to B$*, iff both of the following statements hold:*

- f *is a relation from* A *to* B *(i.e.* $f \subseteq A \times B$*).*
- *For any* $a \in A$*, there exists a unique* $b \in B$ *such that* $(a, b) \in f$*.*

Definition 5.30 deserves further comment, since it seems quite different, at first glance, from how one usually views functions. First, since f is a relation, it is a set consisting of ordered pairs. The connection to our usual perspective of functions is that *given any pair* $(a, b) \in f$*, we interpret* a *as the input into* f*, and* b *the resulting output that is received from* f. Thus, the second condition in Definition 5.30 means *that every* $a \in A$ *is a valid input into* f*, and putting* $a \in A$ *into* f *results in exactly one output from* B.

Note. *It is rather tricky to express the condition "there exists a unique* $b \in B$ *such that* $(a, b) \in f$*" in a precise manner. The formal representation of this statement is*

$$\exists_{b \in B}((a, b) \in f \text{ and } \forall_{c \in B}((a, c) \in f \Rightarrow c = b)).$$

Since this is a bit cumbersome, and since "uniqueness" comes up often enough in mathematics, one often writes $\exists!_{b \in B}((a, b) \in f)$ *as a shorthand for the above statement.*

From here, we can connect the set-theoretic interpretation of functions in Definition 5.30 to the more standard notations for describing functions:

Definition 5.31. *Let* A, B *be sets, and let* $f : A \to B$*.*

- *Given* $a \in A$*, we let* $f(a)$ *be the unique element of* B *with* $(a, f(a)) \in f$*.*
- *The above can precisely described as "*$f(a) = b$ *if and only if* $(a, b) \in f$*".*

Letting f be as in Definition 5.31, since $f(a)$ by construction satisfies $(a, f(a)) \in f$, then the preceding interpretation yields that $f(a)$ *is output obtained from* f *when* a *is given as the input*, which is precisely how we have always viewed functions.

Example 5.32. *As a first example, let* $A = \{1, 2, 3\}$*, and consider the set*

$$f = \{(1, 2), (2, 3), (3, 1)\},$$

which is clearly a relation from A *to* A*. Observe, in addition, that*

- *For* $1 \in A$*, there is exactly one* $a \in A$ *with* $(1, a) \in f$*, namely,* $a = 2$*.*
- *For* $2 \in A$*, there is exactly one* $a \in A$ *with* $(2, a) \in f$*, namely,* $a = 3$*.*
- *For* $3 \in A$*, there is exactly one* $a \in A$ *with* $(3, a) \in f$*, namely,* $a = 1$*.*

In summary, each "input" in A *is paired with exactly one "output" in* A*, so it follows from Definition 5.30 that* f *is a function from* A *to* A*.*

Now, the above gives the set-theoretic description of f*. In terms of the more widely used "function notation",* f *can be characterised as follows:*

- *"*$f : \{1, 2, 3\} \to \{1, 2, 3\}$ *is given by* $f(1) = 2$*,* $f(2) = 3$*, and* $f(3) = 1$*".*

In particular, $f(1) = 2$ *holds since* $(1, 2) \in f$*, and similarly for* $f(2)$ *and* $f(3)$*.*

Example 5.33. *Consider the function given (in terms of function notation) by*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2.$$

The above means that f *maps any input* $x \in \mathbb{R}$ *to the output* $f(x) = x^2 \in \mathbb{R}$*, e.g.*

$$f(0) = 0, \qquad f(1) = f(-1) = 1, \qquad f\left(-\tfrac{3}{2}\right) = \tfrac{9}{4}.$$

Observe also that f *can be described as a set by*

$$f = \{(x, x^2) \mid x \in \mathbb{R}\}.$$

Example 5.34. *One can split a function definition into cases. Consider, for instance,*

$$s : \mathbb{R} \to \mathbb{R}, \qquad s(x) = \begin{cases} -1 & \text{if } x < 0, \\ 1 & \text{if } x \geq 0. \end{cases}$$

The meaning of the above is rather self-explanatory, but for completeness:

- $s(x)$ *is defined to be* -1 *whenever* $x \in \mathbb{R}$ *and* $x < 0$*.*
- $s(x)$ *is defined to be* 1 *whenever* $x \in \mathbb{R}$ *and* $x \geq 0$*.*

Note in particular that $s(0) = s(1) = 1$*, while* $s(-2) = -1$*.*

More formally, s *can be described as a set by*

$$s = \{(x, -1) \mid x \in \mathbb{R} \text{ and } x < 0\} \cup \{(x, 1) \mid x \in \mathbb{R} \text{ and } x \geq 0\}.$$

In practice, we will, for the most part, use the more common "function notation" to describe functions in the upcoming discussions, simply because the common notation tends to be far more intuitive than the set-theoretic description of functions.

5.4.1. *Domains and Codomains.* Returning to the definition of functions, we introduce some additional terminology that will be useful in upcoming discussions:

Definition 5.35. *Let* A, B *be sets, and let* $f : A \to B$. *In this setting:*

- A *is called the domain of* f.
- B *is called the codomain of* f.

Recalling Definition 5.30 and its interpretation, we see that *the domain of a function* f *represents the set of all possible inputs values into* f. Furthermore, *the codomain of* f *can be interpreted as a set of potential output values of* f.

To be more specific, suppose $f : A \to B$ as in Definition 5.35. Then, every input x that one feeds into f must be an element of its domain A, while every output value $f(x)$ of f (for $x \in A$) must be an element of its codomain B.

Now, in Examples 5.33–5.34, we considered functions for which both the domain and codomain were just $\mathbb{R}$. While such functions are commonly studied in calculus and pre-calculus, there is no reason at all to restrict our scope to only real numbers.

Example 5.36. *Consider next the function*

$$g : \mathbb{N} \to \mathbb{N}, \qquad g(n) = n^2.$$

Notice g *is defined by the same formula as* f *in Example 5.33, but the domain of* g *is* $\mathbb{N}$ *rather than* $\mathbb{R}$. *This means we are only allowed to feed natural numbers as input into* g:

- *Just like for* f, *we have* $g(0) = 0$ *and* $g(1) = 1$.
- *On the other hand,* $g(-1)$ *and* $g(-\frac{3}{2})$ *are not defined, since* $-1, -\frac{3}{2} \notin \mathbb{N}$.

Examples 5.33 and 5.36 show that the domain is a critical part of the description of a function. *To fully define a function, one must specify not only the rule associating the input*

to the output, but also which inputs are allowed in the first place. Thus, *if you have not specified a function's domain, then you have not adequately defined that function*!

Next, we can consider functions whose domain is a Cartesian product, that is, a set of ordered pairs. These functions can hence be thought of taking a pair of inputs. In fact, we have already seen examples of this in the previous chapter.

Example 5.37. *The greatest common divisor (of positive integers) can be expressed as a function* $\gcd : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. *Indeed,* gcd *takes a pair of natural numbers* (m, n) *as input, and it gives their greatest common divisor* $\gcd(m, n) \in \mathbb{N}$ *as output.*

Recall from Definition 4.34 that greatest common divisors can be defined for pairs of integers, hence gcd *could also be formulated with an even larger domain. However, one must be a bit careful here, since* $\gcd(0, 0)$ *is not defined (see the note below Definition 4.34). Thus, this "extended"* gcd *should be expressed as a function*

$$\gcd : (\mathbb{Z} \times \mathbb{Z}) \setminus \{(0, 0)\} \to \mathbb{N}.$$

Note the output of this gcd *is still always a natural number.*

Next, the inputs to functions need not be numbers. The following is a simple example of a function which takes sets as both input and output.

Example 5.38. *Consider the function*

$$H : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N}), \qquad H(A) = \mathbb{N} \setminus A.$$

Observe H *takes as input any subset* $A \subseteq \mathbb{N}$ *(that is, any* $A \in \mathcal{P}(\mathbb{N})$*). The corresponding output* $H(A) = \mathbb{N} \setminus A$ *is then the set of all natural numbers not in* A.

Recall we had mentioned that the domain is a critical property of any function. On the other hand, *the same is not true for the codomain.* To explain this, observe that for a function declaration $f : A \to B$, the only requirement for the codomain B is that every output of f lies in B, that is, $f(x) \in B$ for all $x \in A$. However, there are many such sets B that satisfies this condition, so the codomain is not uniquely defined.

For instance, in Example 5.36, we declared the codomain of g to be $\mathbb{N}$, since we know from the formula for g that every output value is an element of $\mathbb{N}$. However, since $\mathbb{N} \subseteq \mathbb{Z}$, it would have been equally valid to say that every output of g is in $\mathbb{Z}$. Thus, it would have been just as correct to write $g : \mathbb{N} \to \mathbb{Z}$ (or even $g : \mathbb{N} \to \mathbb{R}$) in Example 5.36.

As a result, *the codomain is not really an essential part of a function's definition.* It is mainly given as an aid to the reader, to make clear which kinds of values a function can take. In any function declaration, there is never one single "correct" codomain.

Nonetheless, mathematicians do aim to make the codomain declaration as informative as possible. For instance, in Example 5.36, since we know all the outputs of g are positive, it is more useful to write $g : \mathbb{N} \to \mathbb{N}$ rather than $g : \mathbb{N} \to \mathbb{Z}$, even if both are correct.

Example 5.39. *Consider now the setting of probability theory. Let S be a finite sample space, so that its power set $\mathcal{P}(S)$ is the corresponding set of events. A probability measure in this setting is then given by a function $\mathbb{P} : \mathcal{P}(S) \to \mathbb{R}$.*

In fact, we can be more informative about the codomain, since all probabilities lie between 0 and 1 (inclusive). Thus, letting $[0, 1]$ denote the closed interval

$$[0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\},$$

we can then more helpfully write $\mathbb{P} : \mathcal{P}(S) \to [0, 1]$.

Example 5.40. *Let us remain in the setting of Example 5.39. A random variable X on this finite sample space S can then be viewed as a function $X : S \to \mathbb{R}$.*

5.4.2. *How Not to Define Functions.* In practice, functions are usually defined using the conventions found in Examples 5.33–5.40. First, one specifies, in "$f : A \to B$", the function's name (f), domain (A), and codomain (B). One then defines the function's values via some formula (e.g. "$f(x) = \dots$") or some longer description in English.

However, this writing style leads to many potential pitfalls, and some additional care is needed to ensure a function description is actually valid. Below, we provide a few basic examples of how function definitions can go wrong.

Example 5.41. *Consider the function "defined" by*

$$f : \mathbb{N} \to \mathbb{N}, \qquad f(n) = n - 1.$$

What goes wrong with this definition?

First, since the domain of f is $\mathbb{N}$, every natural number is a valid input into f. Moreover, for any input $n \in \mathbb{N}$, the output $f(n) = n - 1$ makes sense. However, note that if

$1 \in \mathbb{N}$ is the input, then the output $f(1) = 0$ is not in the given codomain $\mathbb{N}$! Thus, this codomain $\mathbb{N}$ is not large enough to include all possible outputs of f.

There are multiple ways to correct the above definition:

- *The most straightforward fix is to simply expand the codomain:*

$$f : \mathbb{N} \to \mathbb{Z}, \qquad f(n) = n - 1.$$

If one wishes to be more specific with the codomain, then one could also take

$$f : \mathbb{N} \to \mathbb{N} \cup \{0\}, \qquad f(n) = n - 1.$$

- *The other option, if one insists on the codomain being $\mathbb{N}$, is to restrict the domain. Since $f(n) \notin \mathbb{N}$ only when $n = 1$, we could cut 1 from the set of inputs:*

$$f : \mathbb{N} \setminus \{1\} \to \mathbb{N}, \qquad f(n) = n - 1.$$

Example 5.42. *Next, we turn to a "classical" example:*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = \tfrac{1}{x}.$$

Here, though we have specified that every real number is a valid input into f, the above formula does not adequately define $f(0) = \frac{1}{0}$ as an element of the codomain $\mathbb{R}$!

One straightforward way to fix this is to cut 0 from the domain altogether:

$$f : \mathbb{R} \setminus \{0\} \to \mathbb{R}, \qquad f(x) = \tfrac{1}{x}.$$

Alternatively, if the domain must be all of $\mathbb{R}$, then we could define $f(0)$ differently:

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = \begin{cases} \frac{1}{x} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

Example 5.43. *Consider next the function "definition"*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = \begin{cases} 4 & \text{if } x < 1, \\ 3 & \text{if } x > 1. \end{cases}$$

Note the above formula specified $f(x)$ when $x < 1$ and when $x > 1$. However, $f(1)$ was left undefined, hence the above is an incomplete description of f.

To fix this, we would need to attach some value to $f(1)$*, for instance,*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = \begin{cases} 4 & \text{if } x \leq 1, \\ 3 & \text{if } x > 1. \end{cases}$$

In this corrected definition, we have now set $f(1) = 4$*.*

Example 5.44. *Similarly, consider the "definition"*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = \begin{cases} 4 & \text{if } x \leq 1, \\ 3 & \text{if } x \geq 1. \end{cases}$$

This suffers from the opposite problem from Example 5.43:

- *From the first case above (for* $x \leq 1$*), we have set* $f(1) = 4$*.*
- *From the second case above (for* $x \geq 1$*), we have set* $f(1) = 3$*.*

As a result, we have assigned two different values to $f(1)$*!*

To fix this, we must again make sure to only attach one value to $f(1)$*, e.g.*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = \begin{cases} 4 & \text{if } x \leq 1, \\ 3 & \text{if } x > 1. \end{cases}$$

There are many more examples of bad function definitions that we could give here. In general, the main point to keep in mind to avoid these pitfalls is to *make sure that your function definition maps every point in the domain to exactly one point in the codomain.* Indeed, each of the errors in Examples 5.41–5.44 was fixed by doing exactly this.

Note. *Here, we reiterate that a function is not adequately defined until its domain is specified. For example, "*$f(x) = x^2$*" by itself is not a valid definition, since it only provide a rule associating input to output without specifying the domain. In particular, the above fails to make clear what "*x*" is, and what kinds of "*x*" are allowed. (The definition of* f *above can be completed as in either Example 5.34 or Example 5.36.)*

Note. *For* $f : A \to B$*, a common point of notational confusion is the following:*

- *The symbol "f" refers to the function itself.*
- *"$f(x)$" refers to the output of f (an element of B), when $x \in A$ is given as input.*

It is common to mistakenly write "$f(x)$" (the output value) when one intends "f" (the function). Make sure you do not write one when you mean the other!

5.5. **Images and Inverse Images.** Previously, we noted that the codomain of a function f represents the set of all its *potential* output values. In some cases, however, we will be interested in the *actual* output values of f. This leads us to the following:

Definition 5.45. *Let A, B be sets, and consider the function $f : A \to B$. We then define the range of f (or alternatively, the image of f) to be the following set:*

$$\operatorname{range}(f) = \{f(a) \mid a \in A\}.$$

Observe that the range of a function f is precisely the set of all output values of f. Unlike the codomain, *the range of f represents the actual* (rather than potential) *outputs of f*.

Example 5.46. *Consider the function from Example 5.33:*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2.$$

Observe that although the codomain was set to be $\mathbb{R}$, all the output values of f must in fact be non-negative, since $x^2 \geq 0$ for every $x \in \mathbb{R}$. In fact, we have

$$\operatorname{range}(f) = \{y \in \mathbb{R} \mid y \geq 0\}. \tag{5.6}$$

For completeness, we give a detailed proof of this below:

Proof of (5.6). For convenience, we set

$$Y = \{y \in \mathbb{R} \mid y \geq 0\}.$$

Then, to prove (5.6), it suffices to show both $\operatorname{range}(f) \subseteq Y$ and $Y \subseteq \operatorname{range}(f)$.

First, suppose $y \in \operatorname{range}(f)$. Then, by Definition 5.45, we have that $y = f(x)$ for some $x \in \mathbb{R}$. But then, by the above definition of f,

$$\begin{aligned} y &= x^2 \\ &\geq 0, \end{aligned}$$

and it follows that $y \in Y$. This proves that $\text{range}(f) \subseteq Y$.

Conversely, suppose $y \in Y$, that is, $y \in \mathbb{R}$ and $y \geq 0$. Then, we have $\sqrt{y} \in \mathbb{R}$, and

$$f(\sqrt{y}) = y.$$

This implies $y \in \text{range}(f)$, and it follows that $Y \subseteq \text{range}(f)$. □

Example 5.47. *Next, consider the function from Example 5.36:*

$$g : \mathbb{N} \to \mathbb{N}, \qquad g(n) = n^2.$$

Thus, by Definition 5.45 and the above, the range of g satisfies

$$\begin{aligned} \text{range}(g) &= \{g(n) \mid n \in \mathbb{N}\} \\ &= \{n^2 \mid n \in \mathbb{N}\}, \end{aligned}$$

that is, the range of g is the set of all the natural numbers that are perfect squares.

Example 5.48. *Remaining with natural numbers, we next consider the following:*

$$w : \mathbb{N} \to \mathbb{N}, \qquad w(n) = n + 1.$$

We claim that the range of w is given by

$$\text{range}(w) = \mathbb{N} \setminus \{1\}. \tag{5.7}$$

Proof of (5.7). First, suppose $m \in \text{range}(w)$, so that $m = w(n) = n + 1$ for some $n \in \mathbb{N}$. It follows from the above that $m = n + 1$ satisfies both $m \in \mathbb{N}$ and $m > 1$, hence $m \in \mathbb{N} \setminus \{1\}$. This proves that $\text{range}(w) \subseteq \mathbb{N} \setminus \{1\}$.

Conversely, suppose $m \in \mathbb{N} \setminus \{1\}$. Then, since $m > 1$, we have $m - 1 \in \mathbb{N}$ and $w(m - 1) = m$. It follows that $m \in \text{range}(w)$, and hence $\mathbb{N} \setminus \{1\} \subseteq \text{range}(w)$. □

Example 5.49. *We now turn to the function from Example 5.34:*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = \begin{cases} -1 & \text{if } x < 0, \\ 1 & \text{if } x \geq 0. \end{cases}$$

By the above formula, f *takes exactly three values:* -1 *and* 1*. As a result,*

$$\operatorname{range}(f) = \{-1, 1\}.$$

Example 5.50. *Finally, consider the function from Example 5.38:*

$$H : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N}), \qquad H(A) = \mathbb{N} \setminus A.$$

In fact, the range of H *is all of* $\mathcal{P}(\mathbb{N})$*:*

$$\operatorname{range}(H) = \mathcal{P}(\mathbb{N}). \tag{5.8}$$

To obtain (5.8)*, it suffices to observe that*

$$H(\mathbb{N} \setminus B) = \mathbb{N} \setminus (\mathbb{N} \setminus B) = B \tag{5.9}$$

holds for any $B \in \mathcal{P}(\mathbb{N})$*. (The proof of* (5.9) *is left as an exercise in the problem sheets.) Thus, any* $B \in \mathcal{P}(\mathbb{N})$ *can be achieved as an output value of* H*, leading to* (5.8)*.*

5.5.1. *Partial Images.* Sometimes, we may not be interested in all of the output values of a function (which was described by the range). Instead, we may only want some of the achieved values, arising from a restricted set of inputs. This motivates the following:

Definition 5.51. *Let* A, B *be any sets, let* $C \subseteq A$*, and consider the function* $f : A \to B$*. The image of* C *under* f *is then defined to be the set*

$$f(C) = \{f(a) \mid a \in C\}.$$

Note that the image described Definition 5.51 is essentially the range described in Definition 5.45, except that we restrict the input values of f to elements of C. Thus, $f(C)$ can be interpreted as *the set of achieved ouptuts of* f *corresponding to inputs in* C.

Example 5.52. *Consider the function given as a set by*

$$f = \{(1, 2), (2, 3), (3, 3), (4, 1)\}.$$

Equivalently, f *can be given in the "standard" notation by*

$$f : \{1, 2, 3, 4\} \to \{1, 2, 3\}, \qquad f(1) = 2, \quad f(2) = f(3) = 3, \quad f(4) = 1.$$

Let us compute a few images involving this f.

For a set with a single element, its image is clear from Definition 5.51:

$$\begin{aligned} f(\{1\}) &= \{f(a) \mid a \in \{1\}\} \\ &= \{f(1)\} \\ &= \{2\}. \end{aligned}$$

The process is similar for sets with multiple elements. For instance,

$$\begin{aligned} f(\{1,2\}) &= \{f(a) \mid a \in \{1,2\}\} \\ &= \{f(1), f(2)\} \\ &= \{2,3\}, \end{aligned}$$

while an analogous computation yields

$$\begin{aligned} f(\{1,2,3\}) &= \{f(1), f(2), f(3)\} \\ &= \{2,3\}. \end{aligned}$$

It is worth noting that given any function $f : A \to B$ and any subset $C \subseteq A$, *the image* $f(C)$ *will always be a subset of the codomain* B.

Example 5.53. *Consider the function from Examples 5.33 and 5.46:*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2.$$

First, similar to Example 5.52, we have

$$\begin{aligned} f(\{1,2,3\}) &= \{f(1), f(2), f(3)\} \\ &= \{1,4,9\}. \end{aligned}$$

Next, for a more complicated image, we claim the following holds:

$$f(\{x \in \mathbb{R} \mid x \geq 2\}) = \{y \in \mathbb{R} \mid y \geq 4\}. \tag{5.10}$$

To see this, we first recall Definitions 3.11 and 5.51 to obtain

$$\begin{aligned} f(\{x \in \mathbb{R} \mid x \geq 2\}) &= \{f(z) \mid z \in \{x \in \mathbb{R} \mid x \geq 2\}\} \\ &= \{f(x) \mid x \in \mathbb{R} \text{ and } x \geq 2\} \\ &= \{x^2 \mid x \in \mathbb{R} \text{ and } x \geq 2\}. \end{aligned}$$

Now, since $x \geq 2$ holds if and only if $x^2 \geq 4$, it follows that

$$\{x^2 \mid x \in \mathbb{R} \text{ and } x \geq 2\} = \{y \in \mathbb{R} \mid y \geq 4\}.$$

(We could give a detailed proof of the above identity in the same manner as in Example 5.46, however we omit the details here.) Combining all the above results in (5.10).

In addition, we claim that

$$f(\{x \in \mathbb{R} \mid x \leq 1\}) = \{y \in \mathbb{R} \mid y \geq 0\}. \tag{5.11}$$

To see this, we first observe, as before, that

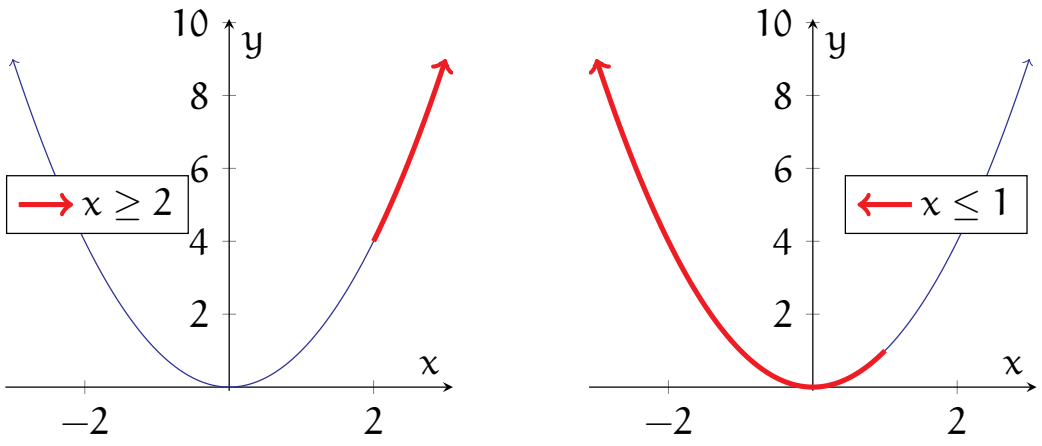
$$f(\{x \in \mathbb{R} \mid x \leq 1\}) = \{x^2 \mid x \in \mathbb{R} \text{ and } x \leq 1\}.$$

Now, the idea is that taking x^2 for every $x \leq 0$ yields all the non-negative real numbers. Furthermore, for $0 \leq x \leq 1$, the values x^2 are redundant and just repeat all the real numbers between (and including) 0 and 1. As a result, it follows that

$$\{x^2 \mid x \in \mathbb{R} \text{ and } x \leq 1\} = \{y \in \mathbb{R} \mid y \geq 0\}$$

(again, this can be proved in more detail if you wish), and (5.11) *follows.*

There is a visual way to see what the images in Example 5.53 should be, if you find graphing functions easier. Recall when one graphs a function, such as f in Example 5.53, the input values are given by the horizontal (x-)coordinate, while the output values are given by the vertical (y-)coordinate. Thus, the image corresponds to all the y-coordinates covered by the part of the graph whose x-coordinates lie in the given set.



The two figures above illustrate the graph of f from Example 5.53 (in blue).

- The left figure highlights, in red, the part of the graph whose x-coordinate corresponds to the region $x \geq 2$. Note that this portion of the graph covers all y-coordinates satisfying $y \geq 4$, confirming the identity (5.10).
- Similarly, the right figure highlights the part of the graph whose x-coordinates corresponds to the region $x \leq 1$. Observe that this part of the graph covers all non-negative y-coordinates, hence this confirms the identity (5.11).

Note. *Keep in mind that drawing a graph does not qualify as a proof, as this is not a logical argument! Nonetheless, it is a useful method for gaining intuition.*

Example 5.54. *Next, consider the function from Example 5.48:*

$$w : \mathbb{N} \to \mathbb{N}, \qquad w(n) = n + 1.$$

Images of w can be computed in a manner similar to Example 5.52:

$$\begin{aligned} w(\{1,2,3,4,5\}) &= \{w(1), w(2), w(3), w(4), w(5)\} \\ &= \{2,3,4,5,6\}. \end{aligned}$$

The same process applies to infinite sets, for instance,

$$\begin{aligned} w(\{1,3,5,7,\dots\}) &= \{w(1), w(3), w(5), w(7), \dots\} \\ &= \{2,4,6,8,\dots\}. \end{aligned}$$

Example 5.55. *Consider the function*

$$G : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \qquad G(a,b) = |a - b|.$$

Let us find the images of the following sets under G:

$$A_1 = \{(a,a) \mid a \in \mathbb{Z}\}, \qquad A_2 = \{(0,a) \mid a \in \mathbb{Z}\}.$$

First, for A_1, we can compute, as before,

$$\begin{aligned} G(A_1) &= \{G(a,a) \mid a \in \mathbb{Z}\} \\ &= \{|a - a| \mid a \in \mathbb{Z}\} \end{aligned}$$

$$= \{0\}.$$

In particular, $G(A_1)$ *is the set of all values* $G(a, a) = |a - a|$*, for all* $a \in \mathbb{Z}$*. Since any such* $|a - a|$ *is always zero, then* $G(A_1)$ *is just* $\{0\}$*.*

Similarly, for A_2*, we have,*

$$\begin{aligned} G(A_2) &= \{G(0, a) \mid a \in \mathbb{Z}\} \\ &= \{|0 - a| \mid a \in \mathbb{Z}\} \\ &= \{|a| \mid a \in \mathbb{Z}\} \\ &= \mathbb{N} \cup \{0\}. \end{aligned}$$

In other words, $G(A_2)$ *is the set of all values* $G(0, a) = |a|$*, for all* $a \in \mathbb{Z}$*. This covers every non-negative integer, the set of which can be written as* $\mathbb{N} \cup \{0\}$*.*

5.5.2. *Inverse Images.* In many cases, it will be more pertinent to consider the "opposite" of the purpose of images from Definition 5.51, that is, to *find all the input values that lead to some given output values.* For this, we define the following:

Definition 5.56. *Let* A, B *be any sets, let* $D \subseteq B$*, and consider the function* $f : A \to B$*. The inverse image of* D *under* f *is then defined to be the set*

$$f^{-1}(D) = \{a \in A \mid f(a) \in D\}.$$

In particular, $f^{-1}(D)$ in Definition 5.56 can be interpreted as *the set of all the input values for which the corresponding output lies in the set* D. Furthermore, it is worth noting that *the inverse image* $f^{-1}(D)$ *will always be a subset of the domain* A.

Example 5.57. *Consider the function from Example 5.54:*

$$w : \mathbb{N} \to \mathbb{N}, \qquad w(n) = n + 1.$$

Inverse images of w *can be obtained using Definition 5.51. For instance,*

$$\begin{aligned} w^{-1}(\{7, 9, 11\}) &= \{n \in \mathbb{N} \mid w(n) \in \{7, 9, 11\}\} \\ &= \{n \in \mathbb{N} \mid n + 1 \in \{7, 9, 11\}\} \\ &= \{6, 8, 10\}. \end{aligned}$$

A similar computation yields

$$\begin{aligned} w^{-1}(\{1,2,3,4,5\}) &= \{n \in \mathbb{N} \mid n+1 \in \{1,2,3,4,5\}\} \\ &= \{1,2,3,4\}. \end{aligned}$$

For the second part, notice that while there do exist $n \in \mathbb{N}$ such that $w(n)$ equals 2, 3, 4, and 5, there is however no $n \in \mathbb{N}$ with $w(n) = 1$. This is why $w^{-1}(\{1,2,3,4,5\})$ only has four elements, even though $\{1,2,3,4,5\}$ has five.

Example 5.58. *Consider again the function from Example 5.53:*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2.$$

First, similar to Example 5.57,

$$\begin{aligned} f^{-1}(\{1,4,9\}) &= \{x \in \mathbb{R} \mid x^2 \in \{1,4,9\}\} \\ &= \{1,2,3,-1,-2,-3\}. \end{aligned}$$

Notice $f^{-1}(\{1,4,9\})$ has twice as many elements as $\{1,4,9\}$, since there are two input values for f that lead to each desired output 1, 4, 9 (e.g. $f(1) = f(-1) = 1$).

Next, we claim that the following holds:

$$f^{-1}(\{y \in \mathbb{R} \mid y \geq 4\}) = \{x \in \mathbb{R} \mid x \geq 2 \text{ or } x \leq -2\}. \tag{5.12}$$

To see this, we first recall Definition 5.56 to obtain

$$\begin{aligned} f^{-1}(\{y \in \mathbb{R} \mid y \geq 4\}) &= \{x \in \mathbb{R} \mid x^2 \in \{y \in \mathbb{R} \mid y \geq 4\}\} \\ &= \{x \in \mathbb{R} \mid x^2 \geq 4\}. \end{aligned}$$

Now, for any $x \in \mathbb{R}$, we have that $x^2 \geq 4$ holds if and only if $x \geq 2$ or $x \leq -2$, hence

$$\{x \in \mathbb{R} \mid x^2 \geq 4\} = \{x \in \mathbb{R} \mid x \geq 2 \text{ or } x \leq -2\},$$

and (5.12) now follows immediately from the above.

Similarly, we claim the following holds:

$$f^{-1}(\{y \in \mathbb{R} \mid y \leq 1\}) = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}. \tag{5.13}$$

For this, we first observe that

$$f^{-1}(\{y \in \mathbb{R} \mid y \leq 1\}) = \{x \in \mathbb{R} \mid x^2 \in \{y \in \mathbb{R} \mid y \leq 1\}\}$$

$$= \{x \in \mathbb{R} \mid x^2 \leq 1\}.$$

Since $x^2 \leq 1$ (where $x \in \mathbb{R}$) holds if and only if $-1 \leq x \leq 1$, we obtain

$$\{x \in \mathbb{R} \mid x^2 \leq 1\} = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\},$$

so that combining the above results in (5.13).

Lastly, we claim that

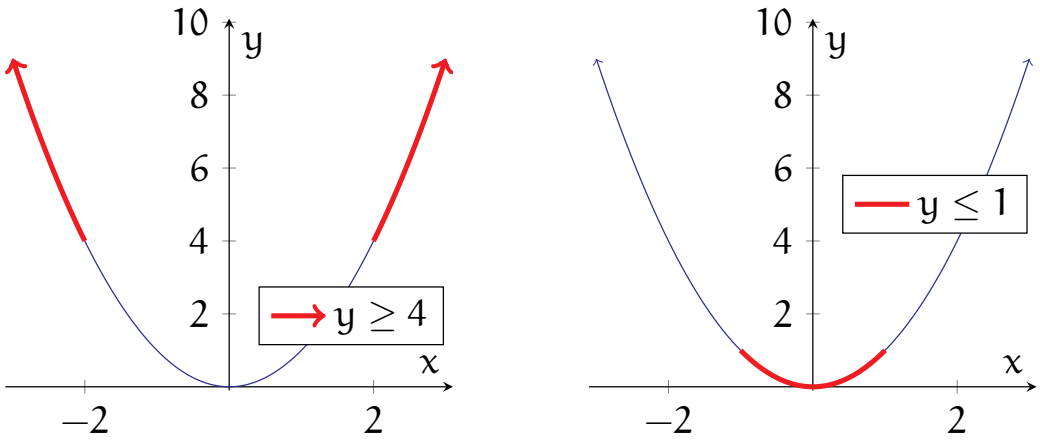
$$f^{-1}(\{y \in \mathbb{R} \mid y < 0\}) = \emptyset.$$

To see this, we note that

$$f^{-1}(\{y \in \mathbb{R} \mid y < 0\} = \{x \in \mathbb{R} \mid x^2 < 0\}.$$

Since there is no $x \in \mathbb{R}$ such that $x^2 < 0$, the above must be the empty set.

We can also use graphs to see what the inverse images in Example 5.58 ought to be. Since the input and output values of f are given by the x- and y-coordinates (respectively) of the graph of f, it follows that the inverse image corresponds to all the x-coordinates covered by the part of the graph whose y-coordinates lie in the given set.



The two figures above illustrate the graph of f from Example 5.58 (in blue).

- The left figure highlights (in red) the part of the graph whose y-coordinate corresponds to the region $y \geq 4$. Note that this portion of the graph covers all x-coordinates satisfying $x \geq 2$ or $x \leq -2$, which confirms (5.12).
- Similarly, the right figure highlights the part of the graph whose y-coordinates corresponds to the region $y \leq 1$. Observe that this part of the graph covers all x-coordinates satisfying $-1 \leq x \leq 1$, which confirms (5.13).

Example 5.59. *Consider the following function:*

$$H : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, \qquad H(a) = (a, a^2).$$

Let us find the inverse images under H *of the following:*

$$B_1 = \{(c, 1) \mid c \in \mathbb{Z}\}, \qquad B_2 = \{(c, c) \mid c \in \mathbb{Z}\}, \qquad B_3 = \{(c, d) \in \mathbb{Z} \times \mathbb{Z} \mid d \geq 0\}.$$

First, for B_1*, we use Definition 5.56 to obtain*

$$\begin{aligned} H^{-1}(B_1) &= \{a \in \mathbb{Z} \mid H(a) = (c, 1) \text{ for some } c \in \mathbb{Z}\} \\ &= \{a \in \mathbb{Z} \mid (a, a^2) = (c, 1) \text{ for some } c \in \mathbb{Z}\}. \end{aligned}$$

Note the above set contains precisely all the $a \in \mathbb{Z}$ *such that* $a^2 = 1$*. Therefore,*

$$\begin{aligned} H^{-1}(B_1) &= \{a \in \mathbb{Z} \mid a^2 = 1\} \\ &= \{1, -1\}. \end{aligned}$$

Next, for B_2*, we have*

$$\begin{aligned} H^{-1}(B_2) &= \{a \in \mathbb{Z} \mid H(a) = (c, c) \text{ for some } c \in \mathbb{Z}\} \\ &= \{a \in \mathbb{Z} \mid (a, a^2) = (c, c) \text{ for some } c \in \mathbb{Z}\}. \end{aligned}$$

Since the above set contains precisely all the $a \in \mathbb{Z}$ *with* $a = a^2$*, we conclude*

$$\begin{aligned} H^{-1}(B_2) &= \{a \in \mathbb{Z} \mid a = a^2\} \\ &= \{0, 1\}. \end{aligned}$$

Finally, by the definition of B_3*, we see that* $H^{-1}(B_3)$ *is the set of all* $a \in \mathbb{Z}$ *such that the second (right) component of* $H(a)$ *(that is,* a^2*) is non-negative. In other words,*

$$\begin{aligned} H^{-1}(B_3) &= \{a \in \mathbb{Z} \mid a^2 \geq 0\} \\ &= \mathbb{Z}. \end{aligned}$$

Finally, we observe that inverse images pop up in other areas of mathematics:

Example 5.60. *First, we turn to probability; consider a sample space* S *and a random variable* $X : S \to \mathbb{R}$*. Here, one might study events of the form*

$$\{X > 1\}, \qquad \{X \leq -2\}, \qquad \{-1 \leq X < 5\}.$$

Even though the notational conventions tend to be different in probability, the above sets are actually inverse images in disguise! In particular, using the notations of Definition 5.56, we can more clearly rewrite the above sets in terms of inverse images as follows:

- $\{X > 1\} = X^{-1}(\{y \in \mathbb{R} \mid y > 1\})$.
- $\{X \leq -2\} = X^{-1}(\{y \in \mathbb{R} \mid y \leq -2\})$.
- $\{-1 \leq X < 5\} = X^{-1}(\{y \in \mathbb{R} \mid -1 \leq y < 5\})$.

Note. *Continuous functions (as one studies in calculus) can also be characterised using inverse images. A precise statement of this is given in the following:*

Theorem. *$f : \mathbb{R} \to \mathbb{R}$ is continuous if and only if given any open interval $I \subseteq \mathbb{R}$, its inverse image $f^{-1}(I)$ can be expressed as a union of open intervals.*

Further discussions or a proof of the above theorem lie a bit beyond the scope of this module, however you will come across these ideas if you study real analysis (i.e. a rigorous development of the ideas from calculus). Additionally, in more abstract settings (e.g. in topology), one actually defines continuity using inverse images.

5.5.3. *Properties of Images.* We now turn our attention to proving some basic properties of images and inverse images. In this process, we also make some comparisons between the behaviours of images and inverse images.

Let us begin our discussion with the most trivial properties:

Proposition 5.61. *Let A, B be sets, and let $f : A \to B$. Then:*

(1) $f(A) = \text{range}(f)$.
(2) $f(\emptyset) = \emptyset$.

Proof of Proposition 5.61. (1) This follows immediately from Definitions 5.45 and 5.51, as both $f(A)$ and $\text{range}(f)$ are defined to be the set $\{f(a) \mid a \in A\}$.

(2) Suppose, for a contradiction, that $f(\emptyset) \neq \emptyset$. Then, there is some $b \in f(\emptyset)$, and Definition 5.51 implies there exists $a \in \emptyset$ with $f(a) = b$. However, the statement $a \in \emptyset$ contradicts that $\emptyset$ has no elements. Thus, we conclude $f(\emptyset) = \emptyset$. □

Proposition 5.62. *Let A, B be sets, and let $f : A \to B$. Then:*

(1) $f^{-1}(B) = A$.
(2) $f^{-1}(\emptyset) = \emptyset$.

Proof of Proposition 5.62. (1) This identity is an immediate consequence of Definition 5.56, since every $a \in A$ satisfies $f(a) \in B$.

(2) Suppose instead that $f^{-1}(\emptyset) \neq \emptyset$. Then, there is some $a \in f^{-1}(\emptyset)$, and Definition 5.56 implies that $f(a) \in \emptyset$, contradicting that $\emptyset$ is empty. □

In spite of what the names "image" and "inverse image" may suggest, these operations need not in fact be inverses of each other—*an inverse image operation needs not undo a previous image*, and *an image operation needs not undo a previous inverse image.*

Example 5.63. *Consider the function from Examples 5.53 and 5.58,*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2,$$

and consider the following sets:

$$C = \{x \in \mathbb{R} \mid 1 \leq x \leq 2\}, \qquad D = \{y \in \mathbb{R} \mid -1 \leq y \leq 1\}.$$

Taking the image of C under f yields

$$\begin{aligned} f(C) &= \{x^2 \mid x \in \mathbb{R} \text{ and } 1 \leq x \leq 2\} \\ &= \{y \in \mathbb{R} \mid 1 \leq y \leq 4\}. \end{aligned}$$

The inverse image of this resulting set is then

$$\begin{aligned} f^{-1}(f(C)) &= \{x \in \mathbb{R} \mid 1 \leq x^2 \leq 4\} \\ &= \{x \in \mathbb{R} \mid 1 \leq x \leq 2 \text{ or } -2 \leq x \leq -1\}. \end{aligned}$$

In particular, we see that $f^{-1}(f(C)) \neq C$.

Similarly, the inverse image of D under f is

$$\begin{aligned} f^{-1}(D) &= \{x \in \mathbb{R} \mid -1 \leq x^2 \leq 1\} \\ &= \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}. \end{aligned}$$

Taking the image of the above then yields

$$\begin{aligned} f(f^{-1}(D)) &= \{x^2 \mid x \in \mathbb{R} \text{ and } -1 \leq x \leq 1\} \\ &= \{y \in \mathbb{R} \mid 0 \leq y \leq 1\}. \end{aligned}$$

In particular, we once again have that $f(f^{-1}(D)) \neq D$.

In the following, we state and prove some basic properties that pertain to how images behave with regards to the standard set operations:

Proposition 5.64. *Let* A, B *be sets, let* $f : A \to B$*, and let* $C, D \subseteq A$*. Then:*

(1) $f(C \cup D) = f(C) \cup f(D)$.
(2) $f(C \cap D) \subseteq f(C) \cap f(D)$.
(3) $f(C \setminus D) \supseteq f(C) \setminus f(D)$.

Proof of Proposition 5.64. (1) First, suppose $b \in f(C \cup D)$. Then, by definition, there exists $a \in C \cup D$ such that $f(a) = b$. We can then split this into two cases:

- If $a \in C$, then $b = f(a) \in f(C)$, and hence $b \in f(C) \cup f(D)$.
- If $a \in D$, then $b = f(a) \in f(D)$, and hence $b \in f(C) \cup f(D)$.

Thus, $b \in f(C) \cup f(D)$ in every case, and we conclude $f(C \cup D) \subseteq f(C) \cup f(D)$.

Conversely, suppose $b \in f(C) \cup f(D)$. We can again split into cases:

- If $b \in f(C)$, then there exists $a \in C$ such that $f(a) = b$. But then, $a \in C \cup D$ as well, and hence $b = f(a) \in f(C \cup D)$.
- If $b \in f(D)$, then there exists $a \in D$ such that $f(a) = b$. But then, $a \in C \cup D$ as well, and hence $b = f(a) \in f(C \cup D)$.

Thus, $b \in f(C \cup D)$ in all cases, and we conclude that $f(C) \cup f(D) \subseteq f(C \cup D)$.

Combining the above with Proposition 3.28 yields $f(C \cup D) = f(C) \cup f(D)$.

(2) Suppose $b \in f(C \cap D)$. Then, there exists $a \in C \cap D$ such that $f(a) = b$. Now, since $a \in C$, then $b = f(a) \in f(C)$. Moreover, since $a \in D$, then $b \in f(D)$ as well. Thus, it follows that $b \in f(C) \cap f(D)$, and hence $f(C \cap D) \subseteq f(C) \cap f(D)$.

(3) Suppose $b \in f(C) \setminus f(D)$. Since $b \in f(C)$, there exists $a \in C$ with $f(a) = b$. Now, if $a \in D$, then $b = f(a) \in f(D)$, contradicting that $b \in f(C) \setminus f(D)$. Therefore,

we have $a \notin D$, and it hence follows that $a \in C \setminus D$. Finally, the above implies that $b = f(a) \in f(C \setminus D)$, which yields $f(C) \setminus f(D) \subseteq f(C \setminus D)$. □

In addition, subset relations are the best that one can prove in (2) and (3) of Proposition 5.64. The following example shows that equality cannot hold in general:

Example 5.65. *Consider the function from Examples 5.53 and 5.58,*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2,$$

and consider the sets

$$C = \{-1\}, \qquad D = \{1\}.$$

Observe that $C \cap D = \emptyset$ *and* $f(C) = f(D) = \{1\}$. *As a result,*

$$f(C \cap D) = \emptyset, \qquad f(C) \cap f(D) = \{1\}.$$

In particular, in this case, $f(C \cap D) \neq f(C) \cap f(D)$.

Furthermore, observe that $C \setminus D = \{-1\}$ *and* $f(C) = f(D) = \{1\}$, *and hence*

$$f(C \setminus D) = \{1\}, \qquad f(C) \setminus f(D) = \emptyset,$$

so once again, $f(C \setminus D) \neq f(C) \setminus f(D)$.

Somewhat surprisingly, the following proposition shows that inverse images demonstrate better behaviour than images with respect to the usual set operations.

Proposition 5.66. *Let* A, B *be sets, let* $f : A \to B$, *and let* $C, D \subseteq B$. *Then:*

(1) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.
(2) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.
(3) $f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$.

Proof of Proposition 5.66. (1) The most straightforward method to prove this is via a series of equivalent statements, similar to proofs in Section 3.3. For any x, we have

$$\begin{aligned} x \in f^{-1}(C \cup D) &\Leftrightarrow f(x) \in C \cup D && \text{(definition of } f^{-1}\text{)} \\ &\Leftrightarrow f(x) \in C \text{ or } f(x) \in D && \text{(definition of } \cup\text{)} \end{aligned}$$

$$\Leftrightarrow x \in f^{-1}(C) \text{ or } x \in f^{-1}(D) \quad \text{(definition of } f^{-1}\text{)}$$
$$\Leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D) \quad \text{(definition of } \cup\text{)}.$$

(2) The process is analogous to the proof of (1)—for any x, we have

$$x \in f^{-1}(C \cap D) \Leftrightarrow f(x) \in C \cap D \quad \text{(definition of } f^{-1}\text{)}$$
$$\Leftrightarrow f(x) \in C \text{ and } f(x) \in D \quad \text{(definition of } \cap\text{)}$$
$$\Leftrightarrow x \in f^{-1}(C) \text{ and } x \in f^{-1}(D) \quad \text{(definition of } f^{-1}\text{)}$$
$$\Leftrightarrow x \in f^{-1}(C) \cap f^{-1}(D) \quad \text{(definition of } \cap\text{)}.$$

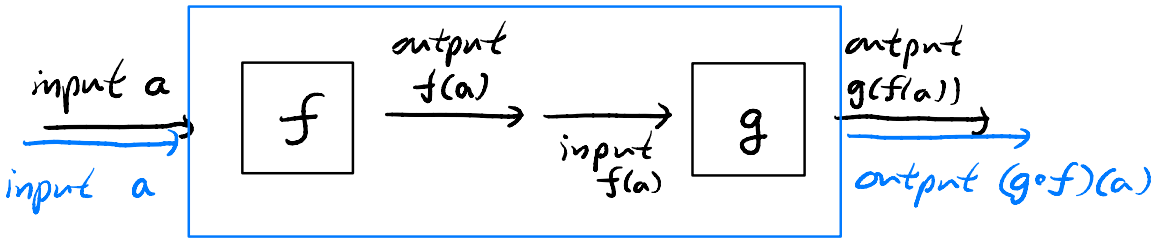
(3) For any x, we have

$$x \in f^{-1}(C \setminus D) \Leftrightarrow f(x) \in C \setminus D \quad \text{(definition of } f^{-1}\text{)}$$
$$\Leftrightarrow f(x) \in C \text{ and } f(x) \notin D \quad \text{(definition of } \setminus\text{)}$$
$$\Leftrightarrow x \in f^{-1}(C) \text{ and } x \notin f^{-1}(D) \quad \text{(definition of } f^{-1}\text{)}$$
$$\Leftrightarrow x \in f^{-1}(C) \setminus f^{-1}(D) \quad \text{(definition of } \cap\text{)}. \qquad \square$$

5.6. **Function Composition.** Next, we consider a common operation on functions that "chains together" their effects in succession. We begin with the precise definition:

Definition 5.67. *Let A, B, C be sets, and consider functions $f : A \to B$ and $g : B \to C$. We define the composition of g and f, denoted $g \circ f$, to be the function*

$$g \circ f : A \to C, \qquad (g \circ f)(a) = g(f(a)).$$



Assume for the moment the setting of Definition 5.67. A simple illustration of the inner workings of $g \circ f$ is given above. Here, the blue box represents $g \circ f$, while the black boxes inside demonstrate the intermediate steps taken when computing values of $g \circ f$.

In particular, for any input $a \in A$, the composition $g \circ f$ has the following effect:

- f is applied to the input a, which yields the output $f(a)$.
- $f(a)$ is then fed as the input into g.

The resulting output $g(f(a))$ is taken as the final output of $g \circ f$.

Note that the choice of sets in Definition 5.67 is important, since the codomain of f must match the domain of g. This is because any potential output of f must be a valid input for g in order for the defining formula of $g \circ f$ to make sense.

Example 5.68. *Consider the functions* $f : \mathbb{R} \to \mathbb{R}$ *and* $g : \mathbb{R} \to \mathbb{R}$ *given by*

$$f(x) = x + 4, \qquad g(x) = 2x.$$

Let us now consider their compositions. Note that both $g \circ f$ *and* $f \circ g$ *are well-defined, since the codomain of* f *coincides with the domain of* g*, and since the codomain of* g *coincides with the domain of* f*. (In particular, all four sets are equal to* $\mathbb{R}$*.)*

Let us now determine the composition $g \circ f : \mathbb{R} \to \mathbb{R}$*. By Definition 5.67, we can directly compute the output value* $(g \circ f)(x)$ *for any input* $x \in \mathbb{R}$*:*

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) && \text{(by Definition 5.67)} \\ &= g(x + 4) && \text{(definition of } f\text{)} \\ &= 2(x + 4) && \text{(definition of } g\text{).} \end{aligned}$$

As a result, we conclude that $g \circ f$ *is the function*

$$g \circ f : \mathbb{R} \to \mathbb{R}, \qquad (g \circ f)(x) = 2x + 8.$$

Similarly, we can find $f \circ g$*—for any* $x \in \mathbb{R}$*, we have*

$$\begin{aligned} (f \circ g)(x) &= f(g(x)) && \text{(by Definition 5.67)} \\ &= f(2x) && \text{(definition of } g\text{)} \\ &= 2x + 4 && \text{(definition of } f\text{).} \end{aligned}$$

As a result, $f \circ g$ *is the function*

$$f \circ g : \mathbb{R} \to \mathbb{R}, \qquad (f \circ g)(x) = 2x + 4.$$

From Example 5.68, we see that $g \circ f$ and $f \circ g$ need not be the same. (In fact, they will generally be quite different.) Of course, one or both of $g \circ f$ and $f \circ g$ may not be defined, if the relevant domains and codomains do not match.

Example 5.69. *Consider the functions* $p : \mathbb{N} \to \mathbb{Z}$ *and* $q : \mathbb{Z} \to \mathbb{N}$ *given by*

$$p(n) = 1 - n, \qquad q(a) = 1 + |a|.$$

Again, both $q \circ p$ *and* $p \circ q$ *are well-defined, since the codomain of* p *equals the domain of* q *(both are* $\mathbb{Z}$*), and the codomain of* q *equals the domain of* p *(both are* $\mathbb{N}$*).*

To find $q \circ p$*, we see that given any* $n \in \mathbb{N}$*, we have*

$$\begin{aligned}(q \circ p)(n) &= q(p(n)) \\ &= q(1 - n) \\ &= 1 + |1 - n|.\end{aligned}$$

Moreover, since $1 - n \leq 0$*, we have that* $|1 - n| = n - 1$*, hence*

$$\begin{aligned}(q \circ p)(n) &= 1 + (n - 1) \\ &= n.\end{aligned}$$

Consequently, the composition $q \circ p$ *can be described as*

$$q \circ p : \mathbb{N} \to \mathbb{N}, \qquad (q \circ p)(n) = n,$$

that is, $q \circ p$ *takes any input* $n \in \mathbb{N}$ *and does absolutely nothing to it.*

Next, for $p \circ q$*, we compute, for any* $a \in \mathbb{Z}$*,*

$$\begin{aligned}(p \circ q)(a) &= p(q(a)) \\ &= p(1 + |a|) \\ &= 1 - (1 + |a|) \\ &= -|a|.\end{aligned}$$

Thus, the composition $p \circ q$ *is described as*

$$p \circ q : \mathbb{Z} \to \mathbb{Z}, \qquad (q \circ p)(a) = -|a|.$$

Example 5.70. *Consider* $F : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ *and* $G : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \times \mathbb{N}$*, given by*

$$F(a) = (a, -a), \qquad G(a, b) = (|b| + 1, |a| + 2).$$

Note in particular that $G \circ F$ *is well-defined, but the opposite composition* $F \circ G$ *is not (since the codomain* $\mathbb{N} \times \mathbb{N}$ *of* G *does not match the domain* $\mathbb{Z}$ *of* F*).*

Let us now compoute $G \circ F$. *For this, we note that for any* $a \in \mathbb{Z}$,

$$\begin{aligned}(G \circ F)(a) &= G(F(a)) \\ &= G(a, -a) \\ &= (|-a| + 1, |a| + 2) \\ &= (|a| + 1, |a| + 2).\end{aligned}$$

More specifically, $G \circ F$ *is the function described as*

$$G \circ F : \mathbb{Z} \to \mathbb{N} \times \mathbb{N}, \qquad (G \circ F)(a) = (|a| + 1, |a| + 2).$$

5.6.1. *Inverse Functions.* We next consider functions that "undo" the effects of another function. This is analogous to how subtraction and division reverse the effects of addition and multiplication, respectively, except we extend this idea to functions in general.

We begin with the precise definition of these "undo" functions, more officially known as inverses. However, one issue to keep in mind is that such an inverse may not necessarily exist, and this possibility must also be worked into the definition.

Definition 5.71. *Let* A, B *be sets, and let* $f : A \to B$. *We say that* f *is* <u>invertible</u> *iff there exists a function* $g : B \to A$ *such that the following holds:*

- $(g \circ f)(a) = a$ *for all* $a \in A$.
- $(f \circ g)(b) = b$ *for all* $b \in B$.

Furthermore, when f *is invertible, the function* $g : B \to A$ *satisfying the above two conditions is called the* <u>inverse</u> *of* f *and is commonly denoted as* f^{-1}.

You probably already have some familiarity with finding inverses of functions involving real numbers. However, similar to the concepts we have studied earlier, this idea of inverses works equally well for any choice of domain and codomain.

Example 5.72. *Consider the function*

$$h : \mathbb{R} \to \mathbb{R}, \qquad h(x) = 2x + 3.$$

We claim that the following function is the inverse of h:

$$H : \mathbb{R} \to \mathbb{R}, \qquad H(y) = \tfrac{1}{2}(y - 3).$$

To see this, first note that, as required by Definition 5.71, the codomain of h *matches the domain of* H*, and the domain of* h *matches the codomain of* H *(all four sets are just* $\mathbb{R}$*). It remains to check that the two bullet point conditions in Definition 5.71 hold, with* h *and* H *in the places of* f *and* g*, respectively. Both points are direct computations:*

- *For any* $x \in \mathbb{R}$*, we have*

$$\begin{aligned}(H \circ h)(x) &= H(h(x)) && \text{(definition of } \circ\text{)}\\ &= H(2x+3) && \text{(definition of } h\text{)}\\ &= \tfrac{1}{2}[(2x+3)-3] && \text{(definition of } H\text{)}\\ &= x.\end{aligned}$$

- *Similarly, for any* $y \in \mathbb{R}$*, we calculate*

$$\begin{aligned}(h \circ H)(y) &= h(H(y)) && \text{(definition of } \circ\text{)}\\ &= h\big(\tfrac{1}{2}(y-3)\big) && \text{(definition of } H\text{)}\\ &= 2 \cdot \frac{1}{2}(y-3)+3 && \text{(definition of } h\text{)}\\ &= y.\end{aligned}$$

Thus, Definition 5.71 implies h *is indeed invertible, and its inverse is* H*:*

$$h^{-1} : \mathbb{R} \to \mathbb{R}, \qquad h^{-1}(y) = \tfrac{1}{2}(y-3).$$

Note also the conditions in Definition 5.71 are symmetric in the two functions f and g. This means that *if* g *satisfies the conditions for being the inverse of* f*, then* f *also satisfies the conditions for being the inverse of* g. Therefore, in Example 5.72, we can additionally conclude from our computations that H *is invertible, and that* $H^{-1} = h$.

Example 5.73. *Consider next the functions*

$$f : \mathbb{N} \to \mathbb{N} \cup \{0\}, \qquad f(n) = n-1,$$
$$F : \mathbb{N} \cup \{0\} \to \mathbb{N}, \qquad F(m) = m+1.$$

First, note the codomain of f *matches the domain of* F *(both are* $\mathbb{N} \cup \{0\}$*), and the domain of* f *matches the codomain of* F *(both are* $\mathbb{N}$*). Next, for any* $n \in \mathbb{N}$*, we have*

$$(F \circ f)(n) = F(n-1) \qquad \text{(definitions of } \circ \text{ and } f\text{)}$$

$$= (n-1)+1 \qquad \textit{(definition of } F\textit{)}$$
$$= n,$$

while for any $m \in \mathbb{N} \cup \{0\}$,

$$(f \circ F)(m) = f(m+1) \qquad \textit{(definitions of } \circ \textit{ and } F\textit{)}$$
$$= (m+1)-1 \qquad \textit{(definition of } f\textit{)}$$
$$= m.$$

Thus, Definition 5.71 implies that f *is invertible, and its inverse is* F*:*

$$f^{-1} : \mathbb{N} \cup \{0\} \to \mathbb{N}, \qquad f^{-1}(m) = m+1.$$

By symmetry, we can also conclude that F *is invertible, with inverse* f*:*

$$F^{-1} : \mathbb{N} \to \mathbb{N} \cup \{0\}, \qquad F^{-1}(n) = n-1.$$

In both Examples 5.72 and 5.73, we were told beforehand by the lecture notes oracle what the inverses of h and f should be. However, what if we were not given these inverses ahead of time? Then, *how can we find out what the inverses are*?

For concreteness, we assume the setting of Example 5.72. Let us also *suppose we already know that* h *is invertible.* (We will address this point later on.) The idea is that if we set $y = h(x)$ for an arbitrary given $x \in \mathbb{R}$, then this gives us the equation

$$y = 2x + 3.$$

We can then "flip the above equation around" by solving for x in terms of y:

$$2x = y - 3, \qquad x = \tfrac{1}{2}(y-3).$$

Now, by Definition 5.71, we have $x = h^{-1}(h(x)) = h^{-1}(y)$, so the above becomes

$$h^{-1}(y) = \tfrac{1}{2}(y-3),$$

which is precisely the formula for H in Example 5.72.

The same process can be applied to Example 5.73, if we already know f is invertible. Setting $m = f(n) = n-1$ for an arbitrary $n \in \mathbb{N}$, we then have

$$n = m+1.$$

Since $n = f^{-1}(m)$, we obtain the formula for F in Example 5.73:

$$f^{-1}(m) = m+1.$$

Note. *We should caution that the informal process described above only works when the function under consideration is invertible. If the opposite is true, then one will either fail to obtain a formula, or the formula will fail to produce an inverse.*

Example 5.74. *Consider now the function*

$$g : \{1,2,3\} \to \{1,2,3\}, \qquad g(1) = 3, \quad g(2) = 2, \quad g(3) = 1.$$

We claim that the function g itself is the inverse of g!

To see this, we note that the domain and codomain of g match. Moreover,

- $(g \circ g)(1) = g(3) = 1.$
- $(g \circ g)(2) = g(2) = 2.$
- $(g \circ g)(3) = g(1) = 3.$

Thus, Definition 5.71 is indeed satisfied, and $g^{-1} = g$.

Example 5.75. *Consider the function*

$$M : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N}), \qquad M(A) = \mathbb{N} \setminus A.$$

We again claim that M itself is the inverse of M.

The key observation is that the following holds for any $A \in \mathcal{P}(\mathbb{N})$:

$$\mathbb{N} \setminus (\mathbb{N} \setminus A) = A. \tag{5.14}$$

(We leave this as an exercise in the problem sheet, but (5.14) can be proved using the same methods as in Chapter 3.) Using (5.14), we then obtain, for any $A \in \mathcal{P}(\mathbb{N})$,

$$\begin{aligned}(M \circ M)(A) &= M(\mathbb{N} \setminus A)\\ &= \mathbb{N} \setminus (\mathbb{N} \setminus A)\\ &= A,\end{aligned}$$

and it follows that M is indeed the inverse of itself: $M^{-1} = M$.

Finally, as mentioned before, a function may not have an inverse to begin with. Thus, though we defer a detailed discussion of what makes functions non-invertible until later, we conclude here by looking at one example of a non-invertible function:

Example 5.76. *Consider the function from Example 5.33:*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2.$$

Let us look at a couple reasons why f *is not invertible.*

First, assuming f *is invertible, then its inverse must have the form* $f^{-1} : \mathbb{R} \to \mathbb{R}$*. In particular,* -1 *is a valid input into* f^{-1}*. By Definition 5.71, we must also have*

$$\begin{aligned} -1 &= f(f^{-1}(-1)) \\ &= (f^{-1}(-1))^2. \end{aligned}$$

However, this immediately leads to a contradiction, since the square of a real number cannot be -1*. Thus, we see that* f *could not possibly be invertible.*

For yet another defect preventing f *from being invertible, observe that*

$$f(1) = 1 = f(-1).$$

As a result, if f *is assumed to be invertible, then applying* f^{-1} *to the above yields both:*

- $f^{-1}(1) = f^{-1}(f(1)) = 1$.
- $f^{-1}(1) = f^{-1}(f(-1)) = -1$.

Thus, $f^{-1}(1)$ *must be defined to be two different values,* 1 *and* -1*, which is a contradiction, so we again conclude that* f *could not be invertible.*

5.7. **Properties of Functions.** Our next task is to look at a few properties that are common to many functions of interest. Similar to our previous discussions abour relations, it is convenient to assign names to these common properties:

Definition 5.77. *Let* A, B *be sets, and let* $f : A \to B$*:*

- f *is injective iff* $f(a_1) = f(a_2)$ *implies* $a_1 = a_2$ *for all* $a_1, a_2 \in A$.
- f *is surjective iff for any* $b \in B$*, there exists* $a \in A$ *such that* $f(a) = b$.
- f *is bijective iff* f *is both injective and surjective.*

Note. *The following terminology are also commonly used:*

- *"*f *is injective" is also written "*f *is an injection" or "*f *is one-to-one".*
- *"*f *is surjective" is also written "*f *is a surjection" or "*f *is onto".*

- *A bijective function is also called a bijection or a one-to-one correspondence.*

Thus, you should be aware of the above alternative names and what they mean.

Let us make some more intuitive sense of Definition 5.77. First, for injectivity, while the given condition in Definition 5.77 is usually easier to work with in practice, the contrapositive statement tends to be more understandable:

- *For any* $a_1, a_2 \in A$, *if* $a_1 \neq a_2$, *then* $f(a_1) \neq f(a_2)$.

The above shows that f being injective is equivalent to the condition that *different inputs always map to different outputs*. In other words, no output of f is attained more than once. Consequently, f being injective is equivalent to the following:

- *Every element of the codomain* B *is mapped to at most once.*

Next, for surjectivity, the condition in Definition 5.77 states that every element $b \in B$ is achieved as an output value of f. Recall now that the range of f is precisely the set of all outputs of f. Thus, f being surjective is equivalent to the following:

- $\text{range}(f) = B$.

Yet another way of stating the above mirrors our last description of injectivity—that is, f being surjective is equivalent to the following statement:

- *Every element of the codomain* B *is mapped to at least once.*

Finally, since f being bijective means that f is both injective and surjective, the above discussions yield that f being bijective is equivalent to:

- *Every element of the codomain* B *is mapped to exactly once.*

In the following, we apply Definition 5.77 to some basic examples of functions:

Example 5.78. *Consider the function from Example 5.33:*

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = x^2.$$

We claim that f *is not injective, not surjective, and not bijective.*

To see that f *is not injective, we can use that* $f(-1) = 1 = f(1)$. *More specifically, by taking* $x_1 = -1$ *and* $x_2 = 1$, *we have that* $f(x_1) = f(x_2)$, *but* $x_1 \neq x_2$. *As a result, the condition for injectivity in Definition 5.77 is violated, hence* f *is not injective.*

Next, for surjectivity, observe that $x^2 \neq -1$ *for any* $x \in \mathbb{R}$. *Thus, taking* $y = -1$, *we see that there does not exist any* $x \in \mathbb{R}$ *such that* $f(x) = y$, *hence violating the condition for surjectivity in Definition 5.77. As a result,* f *is not surjective.*

Finally, since f is neither injective nor surjective, then f is also not bijective.

Example 5.79. *Consider the function from Example 5.36:*

$$g : \mathbb{N} \to \mathbb{N}, \qquad g(n) = n^2.$$

We claim that g is injective, not surjective, and not bijective.

The analysis of g is analogous similar to that of f in Example 5.78, except that we only consider input and output values in $\mathbb{N}$, rather than in $\mathbb{R}$.

First, for injectivity, let $n, m \in \mathbb{N}$ be arbitrary, and suppose $g(n) = g(m)$, which by the definition of g implies $n^2 = m^2$. As we are now only considering positive integers, square roots become unique. Thus, taking square roots of $n^2 = m^2$ yields $n = m$, so the condition in Definition 5.77 is satisfied, and hence g is injective.

Next, for surjectivity, observe that there is no $n \in \mathbb{N}$ such that $g(n) = n^2 = 2$. Thus, the condition in Definition 5.77 is violated, and f is not surjective.

Lastly, since f is not surjective, then f is also not bijective.

Examples 5.78 and 5.79 also demonstrate why it is important to specify the domains of functions. Although f and g are defined by the same rule, they have different properties due to their different domains—g is injective, but f is not.

Example 5.80. *Consider the function from Example 5.73:*

$$f : \mathbb{N} \to \mathbb{N} \cup \{0\}, \qquad f(n) = n - 1.$$

We claim that f is injective, surjective, and bijective.

To prove that f is injective, we let $n, m \in \mathbb{N}$ and suppose $f(n) = f(m)$. The definition of f then yields $n - 1 = m - 1$, and adding 1 to both sides yields $n = m$. Therefore, applying Definition 5.77, we conclude that f is injective.

To show that f is surjective, we fix $m \in \mathbb{N} \cup \{0\}$. Then, we have $m + 1 \in \mathbb{N}$, and

$$\begin{aligned} f(m+1) &= (m+1) - 1 \\ &= m. \end{aligned}$$

Thus, the condition for surjectivity in Definition 5.77 is satisfied, hence f is surjective.

Finally, since f is both injective and surjective, f is also bijective.

The above examples should give you a basic idea of what is involved in checking for injectivity and surjectivity. We give a few more examples below, but with less details.

Example 5.81. *Consider the function from Example 5.72:*

$$h : \mathbb{R} \to \mathbb{R}, \qquad h(x) = 2x + 3.$$

We claim that h *is injective, surjective, and bijective.*

First, suppose $x, y \in \mathbb{R}$ *and* $h(x) = h(y)$*. Then, by definition of* h*,*

$$2x + 3 = 2y + 3.$$

Subtracting 3 *from both sides yields* $2x = 2y$*, and dividing both sides by* 2 *yields* $x = y$*. It follows from the above and Definition 5.77 that* h *is injective.*

Next, let $y \in \mathbb{R}$*. Then,* $\frac{1}{2}(y - 3) \in \mathbb{R}$ *as well, and a direct computation shows*

$$\begin{aligned} h\left(\tfrac{1}{2}(y-3)\right) &= 2 \cdot \tfrac{1}{2}(y-3) + 3 \\ &= y. \end{aligned}$$

It then follows, from Definition 5.77, that h *is surjective.*

Since h *is both injective and surjective, then* h *is also bijective.*

Note in the proof of surjectivity in Example 5.81, we were helped along by already knowing that $h(\frac{1}{2}(y-3)) = y$ for any $y \in \mathbb{R}$. However, in practice, one may not be able to see this beforehand. In this case, one could deduce the above by *first solving*

$$y = h(x) = 2x + 3$$

for $x \in \mathbb{R}$, which yields the desired input $x = \frac{1}{2}(y - 3)$. (The above is also closely related to the inverse of h, computed in Example 5.72.)

Example 5.82. *Consider the function*

$$G : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}, \qquad G(x, y) = (x + y,\ x - y).$$

We claim that G *is injective, surjective, and bijective. (Here, the domain and codomain are a bit more complicated, but the ideas and the process are the same as before.)*

First, let $(x_1, y_1), (x_2, y_2) \in \mathbb{R} \times \mathbb{R}$*, and suppose* $G(x_1, y_1) = G(x_2, y_2)$*, that is,*

$$(x_1 + y_1,\ x_1 - y_1) = (x_2 + y_2,\ x_2 - y_2).$$

By Definition 5.1 for ordered pairs, the above is equivalent to the two equations

$$x_1 + y_1 = x_2 + y_2, \qquad x_1 - y_1 = x_2 - y_2. \tag{5.15}$$

From here, we observe the following:

- *Adding the two equations in* (5.15) *yields* $2x_1 = 2x_2$*, and hence* $x_1 = x_2$*.*
- *Subtracting the two equations in* (5.15) *yields* $2y_1 = 2y_2$*, and hence* $y_1 = y_2$*.*

Recalling Definition 5.1 again, we conclude $(x_1, y_1) = (x_2, y_2)$*, hence* G *is injective.*

Next, given any $(x, y) \in \mathbb{R} \times \mathbb{R}$*, a direct computation yields*

$$\begin{aligned} G\left(\tfrac{1}{2}(x+y),\, \tfrac{1}{2}(x-y)\right) &= \left(\tfrac{1}{2}(x+y) + \tfrac{1}{2}(x-y),\, \tfrac{1}{2}(x+y) - \tfrac{1}{2}(x-y)\right) \\ &= (x, y), \end{aligned}$$

and it follows that G *is indeed surjective.*

Finally, since G *is injective and surjective, it is also bijective.*

Example 5.83. *Consider the function*

$$G_* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, \qquad G_*(a, b) = (a + b,\, a - b).$$

(In particular, G_* *is defined using the same rule as for* G *in Example 5.82, however we restrict the inputs for* G_* *to only the integers.)*

One can show that G_* *is still injective, but* G_* *is neither surjective nor bijective. (We save the details as an exercise in the problem sheets.) This is yet another example that the properties of a function are sensitive to its domain and codomain.*

5.7.1. *Invertibility Revisited.* Previously, we had given examples of inverses of functions, as well as discussed how the inverse can be computed if the function is known to be invertible. However, we had left answered the following question:

Question 5.84. *Given a function* $f : A \to B$*, when is* f *invertible?*

We now have enough background to give a tidy answer to Question 5.84. For a bit of intuition, we can look at some of the previous examples:

- Recall Examples 5.72 and 5.73 provided two functions that were invertible. It was also shown in Examples 5.80 and 5.81 that both functions were bijective.

- Moreover, Example 5.76 gives a simple function that fails to be invertible, while Example 5.78 showed that this function was neither injective nor surjective.

Although these examples alone constitute too small a sample size, they do suggest some connection between the properties of Definition 5.77 and invertibility.

The following theorem rigorously confirms this suggestion, and it provides a practical way to check whether a given function is invertible:

Theorem 5.85. *Let A and B be arbitrary sets, and consider any function $f : A \to B$. Then, f is invertible if and only if f is bijective.*

Proof of Theorem 5.85. Since the statement to be proved is an equivalence, it suffices to show that each part of the equivalence implies the other.

First, let us assume f is invertible, so that the inverse $f^{-1} : B \to A$ exists. We now claim that f is both injective and surjective:

- Let $a_1, a_2 \in A$, and suppose $f(a_1) = f(a_2)$. Applying f^{-1} to this yields

$$\begin{aligned} a_1 &= f^{-1}(f(a_1)) && \text{(by Definition 5.71)} \\ &= f^{-1}(f(a_2)) \\ &= a_2 && \text{(by Definition 5.71),} \end{aligned}$$

  and it follows from Definition 5.77 that f is injective.
- Let $b \in B$. Then, Definition 5.71 implies that

$$f(f^{-1}(b)) = b,$$

  and it follows, again from Definition 5.77, that f is surjective.

From the above, we conclude that f is bijective, as desired.

Conversely, assume f is bijective. We can then define $g : B \to A$ as follows:

- Given $b \in B$, there exists $a \in A$ such that $f(a) = b$ (since f is surjective). Moreover, we know that this $a \in A$ is unique (if $a' \in A$ and $f(a') = b$, then $a' = a$, since f is injective). We can thus unambiguously define $g(b) = a$.

Now, to show that f is invertible, we must show that for any $a \in A$ and $b \in B$,

$$g(f(a)) = a, \qquad f(g(b)) = b.$$

- Given $b \in B$, we immediately have, from the definition of g, that $f(g(b)) = b$ (since $g(b)$ is defined to be the unique element of A that maps to b via f).
- Given $a \in A$, the definition of g implies that

$$f(g(f(a))) = f(a),$$

since $g(f(a))$ is the unique element of A that maps to $f(a)$ via f. Since f is injective, it follows that $g(f(a)) = a$, as desired.

From the above and Definition 5.71, we conclude that f is invertible. □

Thus, to check whether a function $f : A \to B$ is invertible, we need only determine if f is bijective. While this is not always an easy task, Examples 5.78–5.82 show that this can often be done through systematic applications of Definition 5.77.

Furthermore, the second half of the proof of Theorem 5.85 tells us what the inverse of f must be. Indeed, Definition 5.71 also implies that $f^{-1} = g$, *where* g *is the function that maps each* $b \in B$ *to the unique element* $a \in A$ *such that* $f(a) = b$.

Example 5.86. *Both the function from Example 5.80,*

$$f : \mathbb{N} \to \mathbb{N} \cup \{0\}, \qquad f(n) = n - 1,$$

and the function from Example 5.81,

$$h : \mathbb{R} \to \mathbb{R}, \qquad h(x) = 2x + 3,$$

were shown to be bijective. Therefore, Theorem 5.85 implies both f *and* h *are invertible. Indeed, both inverses were already computed in Examples 5.72 and 5.73.*

Example 5.87. *Consider the function from Example 5.79,*

$$g : \mathbb{N} \to \mathbb{N}, \qquad g(n) = n^2,$$

as well as the function from Example 5.83,

$$G_* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, \qquad G_*(a, b) = (a + b,\ a - b).$$

It was shown in Examples 5.79 and 5.83 that both g *and* G_* *fail to be surjective, thus Theorem 5.85 implies that neither* g *nor* G_* *is invertible.*

Example 5.88. *Consider the function from Example 5.82,*

$$G : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}, \qquad G(x, y) = (x + y,\ x - y).$$

Recall Example 5.82 showed G *is bijective, hence Theorem 5.85 implies* G *is invertible.*

To determine the inverse of G*, recall from Example 5.82 that*

$$G\left(\tfrac{1}{2}(x + y),\ \tfrac{1}{2}(x - y)\right) = (x, y),$$

for any $x, y \in \mathbb{R}$*. In other words,* $(\frac{1}{2}(x + y), \frac{1}{2}(x - y))$ *is the element in* $\mathbb{R} \times \mathbb{R}$ *that maps to* (x, y) *via* G*. Thus, it follows that the inverse* G^{-1} *is given by*

$$G^{-1} : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}, \qquad G^{-1}(x, y) = \left(\tfrac{1}{2}(x + y),\ \tfrac{1}{2}(x - y)\right).$$

We can confirm by direct computation that the above truly is the inverse:

- *Given any* $(x, y) \in \mathbb{R} \times \mathbb{R}$*, we have*

$$\begin{aligned} G^{-1}(G(x, y)) &= G^{-1}(x + y,\ x - y) \\ &= \left(\tfrac{1}{2}((x + y) + (x - y)),\ \tfrac{1}{2}((x + y) - (x - y))\right) \\ &= (x, y). \end{aligned}$$

- *Similarly, given any* $(x, y) \in \mathbb{R} \times \mathbb{R}$*, we have*

$$\begin{aligned} G(G^{-1}(x, y)) &= G\left(\tfrac{1}{2}(x + y), \tfrac{1}{2}(x - y)\right) \\ &= (x, y). \end{aligned}$$

Example 5.89. *Consider the following function:*

$$f : \mathbb{Z} \to \mathbb{N}, \qquad f(k) = \begin{cases} 2k & \text{if } k > 0, \\ 1 - 2k & \text{if } k \leq 0. \end{cases}$$

Before we do any rigorous proving, let us first "play around a bit" to get some intuition on what f *is doing. Computing* f *for some small positive integers yields*

$$f(1) = 2, \qquad f(2) = 4, \qquad f(3) = 6, \qquad f(4) = 8.$$

Similarly, computing f *some small non-positive integers yields*

$$f(0) = 1, \qquad f(-1) = 3, \qquad f(-2) = 5, \qquad f(-3) = 7.$$

From the above, a pattern emerges—the positive integers map to all the even natural numbers, while the non-positive integers map to all the odd natural numbers.

In particular, we expect f *to map to each* $m \in \mathbb{N}$ *exactly once, that is, we expect that* f *will be bijective, and hence invertible. Let us now rigorously confirm these statements.*

To cover all our bases, though, let us first confirm our definition of f *is valid:*

Claim 1: f *is well-defined, i.e.* $f(k) \in \mathbb{N}$ *for every* $k \in \mathbb{Z}$*. Furthermore,* $f(k)$ *is even when* $k > 0$*, and* $f(k)$ *is odd when* $k \leq 0$*.*

Proof of Claim 1. This follows immediately from the following observations:

- When $k > 0$, we have $f(k) = 2k$, which is both even and positive.
- When $k \leq 0$, we have $f(k) = 1 - 2k$, which is odd and positive. □

Next, we show that f *is indeed bijective:*

Claim 2: f *is bijective.*

Proof of Claim 2. First, let $a, b \in \mathbb{Z}$, and suppose $f(a) = f(b) = m$.

- If m is even, then it follows that $a, b > 0$. (By the previous claim, if $a \leq 0$, then $f(a)$ is odd, and similarly for b.) Thus, by the definition of f, we have
$$f(a) = 2a, \qquad f(b) = 2b.$$
As a result, $2a = 2b = m$, and dividing this by 2 yields $a = b$.
- If m is odd, then it follows (again from the previous claim) that $a, b \leq 0$, so
$$f(a) = 1 - 2a, \qquad f(b) = 1 - 2b.$$
It then follows that $1 - 2a = 1 - 2b$. Subtracting 1 from both sides of the above and dividing by -2, we again obtain $a = b$.

Thus, in all cases, we obtain $a = b$, hence we conclude f is injective.

Next, let $m \in \mathbb{N}$, and consider the following cases:

- If m is even, then $\frac{m}{2} \in \mathbb{N}$, and it follows that $f(\frac{m}{2}) = m$.
- Similarly, if m is odd, then $\frac{1-m}{2}$ is an integer. Since $m \geq 1$, we also have $\frac{1-m}{2} \leq 0$. Thus, by the definition of f,
$$\begin{aligned} f\left(\tfrac{1-m}{2}\right) &= 1 - 2 \cdot \tfrac{1-m}{2} \\ &= m. \end{aligned}$$

Thus, in all cases, there exists $k \in \mathbb{Z}$ with $f(k) = m$, hence f is surjective.

Finally, since f is injective and surjective, it is also bijective. □

Thus, by the claim and by Theorem 5.85, we conclude that f is invertible. Finally, let us determine what the inverse $f^{-1} : \mathbb{N} \to \mathbb{Z}$ should be.

For this, we need only look at the preceding proof that f is surjective:

- *Recall that if $m \in \mathbb{N}$ is even, then $f(\frac{m}{2}) = m$. Thus, $f^{-1}(m) = \frac{m}{2}$.*
- *Recall that if $m \in \mathbb{N}$ is odd, then $f(\frac{1-m}{2}) = m$. Thus, $f^{-1}(m) = \frac{1-m}{2}$.*

Combining the above observations, we conclude that the inverse of f is given by

$$f^{-1} : \mathbb{N} \to \mathbb{Z}, \qquad f^{-1}(m) = \begin{cases} \frac{m}{2} & \text{if } m \text{ is even,} \\ \frac{1-m}{2} & \text{if } m \text{ is odd.} \end{cases}$$

5.8. **Final Notes.** In these notes, we have taken the informal view that all the number systems we have studied exist in our mathematical universe, and they have all the properties studied in Section 4.1. As we have mentioned before, this is philosophically undesirable, as this adds a long list of facts that we must take as mere assumptions, or axioms.

Instead, what we would like to do is to assume as little as possible, and to then *prove* all the desired properties as logical consequences of our minimal assumptions. In particular, with regards to our various number systems, we aim to:

- Rigorously *construct* all the sets of numbers that we have studied ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) from more elementary objects—that is, from abstract sets.
- Define the usual algebraic and ordering operations on these constructed sets, and *prove* that these number systems have all the properties listed in Section 4.1.

There are multiple ways to accomplish the above, however a full accounting of any method is beyond the scope of these notes (and is rather long and painstaking).

Nonetheless, in the remainder of this section, we provide, as bonus content, some key ideas behind how each set of numbers could be rigorously defined.

5.8.1. *(Bonus) Construction of $\mathbb{N}$.* For some concrete intuition on how the natural numbers can be defined, let us construct the first few numbers:

- $0 = \emptyset$: To start, we define 0 to be the empty set.
- $1 = \{0\} = \{\emptyset\}$: Next, we define 1 to be the set containing 0.
- $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$: We then define 2 to be the set containing 0 and 1.

In general, given $n \in \mathbb{N} \cup \{0\}$, we define its successor n_* to be

$$n_* = \{0, 1, 2, \ldots, n\}.$$

(This successor n_* is really just $n + 1$, but we have yet not defined "$+$" at this point.) In other words, $\mathbb{N}$ can be *constructed inductively* by *defining each natural number to be the set of all natural numbers (and zero) less than itself.*

Again, no one would intuitively think of natural numbers in this convoluted manner. The point here is that this way, we need not assume $\mathbb{N}$ exists with all the familiar properties. Instead, we build $\mathbb{N}$ from more basic sets and prove it has the right properties.

Now, there are a few advantages to defining $\mathbb{N}$ in this particular manner:

- It is clear that *the numbers we have constructed are distinct.* More specifically, our numbers, as defined above, satisfy $1 \neq 2$, $2 \neq 3$, $1 \neq 3$, and so on.
- Our construction allows for a very convenient definition of "less than" ("$<$"). Indeed, since each number contains every number less than itself, then given any $m, n \in \mathbb{N} \cup \{0\}$, we can simply define $m < n$ to hold iff $m \in n$ holds.

The next step is to define the algebraic operations "$+$" and "$\times$" on $\mathbb{N} \cup \{0\}$. Similarly to our preceding construction, this can be done inductively for any $n \in \mathbb{N} \cup \{0\}$:

- As base cases, we first define
$$n + 0 = n, \qquad n \times 0 = 0.$$
- Next, once $n + m$ and $n \times m$, where $m \in \mathbb{N} \cup \{0\}$, are defined, we then set
$$n + m_* = (n + m)_*, \qquad n \times m_* = (n \times m) + n,$$
where $(n + m)_*$ denotes the successor of $n + m$.

By induction, the above defines $n + m$ and $n \times m$ for all $n, m \in \mathbb{N} \cup \{0\}$.

Using the above definitions, we can then prove, as theorems, all the properties of $\mathbb{N}$ listed in Section 4.1. This is not all that difficult to do, but the process is quite lengthy, with many painstaking inductions, so we omit the details here.

5.8.2. *(Bonus) Construction of $\mathbb{Z}$.* We next turn our attention to constructing the integers, using only the natural numbers $\mathbb{N}$ and the basic tenets of set theory.

The main idea is to *model an integer $a \in \mathbb{Z}$ as a difference $n - m$ of two natural numbers $n, m \in \mathbb{N}$.* However, since we have not yet defined "$-$", we must represent this differently. In particular, we use an *ordered pair* (n, m) to model this "difference $n - m$". (See the discussion below Example 5.3 for a formal construction of ordered pairs.)

To make this more clear, we consider some concrete examples:

- The pair $(4, 1)$ models the integer $4 - 1 = 3$.
- The pair $(1, 5)$ models the integer $1 - 5 = -4$.
- The pair $(7, 7)$ models the integer $7 - 7 = 0$.

In this way, we can capture the negative numbers alongside the non-negative ones.

Now, there is one major issue with the above characterisation—*there are multiple pairs that model the same integer*! For instance, by our descriptions, both $(4,1)$ and $(6,3)$ would model the same integer 3, while both $(1,2)$ and $(5,6)$ would represent the same integer -1. As a result, a reasonable construction of $\mathbb{Z}$ would have to view the pairs $(4,1)$ and $(6,3)$ as "the same", and similarly for $(1,2)$ and $(5,6)$.

Fortunately for us, we have just the tool for capturing "sameness"—*equivalence relations*! Thus, we would like to define the (equivalence) relation R on $\mathbb{N} \times \mathbb{N}$ as follows:

$$(n_1, m_1)\ R\ (n_2, m_2) \text{ if and only if } n_1 - m_1 = n_2 - m_2.$$

However, we cannot do the above, as have not yet made sense of "$-$". Fortunately, since we have defined "$+$" on $\mathbb{N}$, we can rearrange the above into a usable definition:

$$(n_1, m_1)\ R\ (n_2, m_2) \text{ if and only if } n_1 + m_2 = n_2 + m_1.$$

We can now *define the set $\mathbb{Z}$ of integers to be the of all equivalence classes of R*:

$$\mathbb{Z} = \{\, [(n, m)] \mid n, m \in \mathbb{N} \,\}.$$

Note this precisely has the effect of aggregating all the pairs (n, m) that represent the same integer into a single object. For instance, the integer 3 is represented by the equivalence class $[(4,1)]$, while -2 is represented by the equivalence class $[(1,3)]$.

Finally, having constructed $\mathbb{Z}$, we can then define the standard algebraic operations ("$+$" and "$\times$") and order relation ("$<$") on $\mathbb{Z}$. Without getting into details, we summarise these below—see if you can see why these definitions are reasonable:

- Addition: $[(n_1, m_1)] + [(n_2, m_2)] = [(n_1 + n_2, m_1 + m_2)]$.
- Multiplication: $[(n_1, m_1)] \times [(n_2, m_2)] = [(n_1 n_2 + m_1 m_2, n_1 m_2 + n_2 m_1)]$.
- Ordering: $[(n_1, m_1)] < [(n_2, m_2)]$ if and only if $n_1 + m_2 < n_2 + m_1$.
- Negation: $-[(n, m)] = [(m, n)]$.

Using the above definitions, one can then (very painstakingly) prove that all the relevant properties listed throughout Section 4.1 hold for the integers.

5.8.3. *(Bonus) Construction of $\mathbb{Q}$.* Recall that each rational number is, in essence, a fraction $\frac{a}{b}$, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus \{0\}$. However, we cannot directly define rational numbers in this way, as we have not yet made sense of division and fractions at this point.

We get around this obstacle in a similar manner as in our construction of $\mathbb{Z}$—the key idea is to *model each fraction $\frac{a}{b}$ as an ordered pair* $(a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. For instance:

- The pair $(1,3)$ represents the rational number $\frac{1}{3}$.
- The pair $(2,1)$ represents the rational number $\frac{2}{1} = 2$.

- The pair $(-9, 5)$ represents the rational number $-\frac{9}{5}$.

The above scheme, however, has the same deficiency as in our previous discussion for $\mathbb{Z}$—*there are multiple pairs that model the same rational number.* For instance, both $(2, 1)$ and $(4, 2)$ model the same rational number 2, while $(-2, 6)$ and $(1, -3)$ both model $-\frac{1}{3}$. We again get around this by introducing an appropriate equivalence relation R.

Ideally, we would like to define R by:

(a_1, b_1) R (a_2, b_2) *if and only if* $\frac{a_1}{b_1} = \frac{a_2}{b_2}$.

However, the above does not quite work, as have not yet defined "$\div$". Nonetheless, the above can be reformulated in terms of integer multiplication (which has been defined):

(a_1, b_1) R (a_2, b_2) *if and only if* $a_1 b_2 = a_2 b_1$.

We can now *define the set* $\mathbb{Q}$ *of rational numbers via equivalence classes of* R:

$$\mathbb{Q} = \{\, [(a, b)] \mid a \in \mathbb{Z} \text{ and } b \in \mathbb{Z} \setminus \{0\} \,\}.$$

The next step is to define the usual algebraic and order relations on $\mathbb{Q}$. Once again, we simply summarise the definitions below; can you see why these are reasonable?

- Addition: $[(a_1, b_1)] + [(a_2, b_2)] = [(a_1 b_2 + a_2 b_1, b_1 b_2)]$.
- Multiplication: $[(a_1, b_1)] \times [(a_2, b_2)] = [(a_1 a_2, b_1 b_2)]$.
- Ordering: $[(a_1, b_1)] < [(a_2, b_2)]$ if and only if $a_1 b_2 < a_2 b_1$, when $b_1, b_2 > 0$.
- Negation: $-[(a, b)] = [(-a, b)]$.
- Reciprocal: $[(a, b)]^{-1} = [(b, a)]$, when $a \neq 0$.

Once again, using these definitions, one can then (again painstakingly) prove that all the relevant properties in Section 4.1 hold for the rational numbers.

5.8.4. *(Bonus) Construction of* $\mathbb{R}$. Turning to the real numbers, recall we previously informally defined $\mathbb{R}$ in terms of infinite decimal expansions, that is, using an infinite sequence of digits and a decimal point. This can all be made precise and rigorous with some work, however this approach tends to be quite troublesome, since different decimal expansions could represent the same real number, and any formal definition would have to take careful account of this. Consequently, here we take another popular approach that is, in many ways, more convenient for theoretical purposes.

The key intuition in this endeavour, summarised in one sentence, is that *we model each real number* $x \in \mathbb{R}$ *as "the set of all rational numbers less than* x*".* To get a better picture of how this works, let us apply this to a couple of concrete numbers:

- For a rational number, say $\frac{1}{2}$ or -3, we model $\frac{1}{2}, -3 \in \mathbb{R}$ as

$$\left\{ q \in \mathbb{Q} \mid q < \tfrac{1}{2} \right\}, \qquad \{ q \in \mathbb{Q} \mid q < -3 \}, \tag{5.16}$$

that is, the set of all rational numbers less than $\frac{1}{2}$ and -3, respectively.

- The above scheme covers all the rational numbers, but we can actually do more! Consider, for example, the irrational number $\sqrt{2}$. This can also be modelled as the set of all rational numbers less than $\sqrt{2}$ in the following manner:

$$\{q \in \mathbb{Q} \mid q < 0 \text{ or } q^2 < 2\}. \tag{5.17}$$

As a result, our idea is capable of capturing not only the rational numbers, but also the (not yet defined) irrational numbers sitting in-between the rational numbers!

More precisely, we define a Dedekind cut to be any $A \subseteq \mathbb{Q}$ satisfying the following:

(1) $A \neq \emptyset$ and $A \neq \mathbb{Q}$.
(2) Given any $y \in A$ and $x \in \mathbb{Q}$, if $x < y$, then $x \in A$ as well.
(3) For any $x \in A$, there exists $y \in A$ such that $y > x$.

Notice in particular that the sets (5.16) and (5.17) are Dedekind cuts. The intuition is that Dedekind cuts are precisely the "sets of rationals that are less than some number". It follows then that *every* real number should be represented as such a Dedekind cut:

- We *define* $\mathbb{R}$ *to be the set of all Dedekind cuts.*

On one hand, Dedekind cuts are far less intuitive than decimal expansions. Nonetheless, as a theoretical construction, Dedekind cuts do have some key advantages:

- For example, via Dedekind cuts, it is exceptionally easy to define the order relation "$\leq$". Indeed, given $x, y \in \mathbb{R}$ (i.e. two Dedekind cuts x and y), we can define $x \leq y$ to hold if and only if $x \subseteq y$ holds. (This is simply because x is represented as the set of all rationals less than x, and similarly for y.)
- In addition, the Supremum Principle (Theorem 4.91) is exceptionally easy to prove using Dedekind cuts. Indeed, given $A \subseteq \mathbb{R}$ as in Theorem 4.91, the union

$$\bigcup_{x \in A} x = \{z \mid \exists_{x \in A}(z \in x)\}$$

is itself a Dedekind cut, and this union is in fact the supremum of A!

Finally, the main disadvantage of using Dedekind cuts is that the algebraic operations "$+$" and "$\times$" require more effort to define. Moreover, while proving the algebraic properties of real numbers in Section 4.1 is not so difficult, it is a painfully long and painstaking procedure. We will mercifully omit the details here. :)

5.8.5. *(Bonus) Construction of* $\mathbb{C}$. Let us save the easiest portion for last! Since each complex number $z \in \mathbb{C}$ is just a pair of real numbers,

$$z = x + yi, \qquad x, y \in \mathbb{R},$$

we can simply model each $x + yi \in \mathbb{C}$ as an ordered pair $(x, y) \in \mathbb{R} \times \mathbb{R}$.

As a result, we can define $\mathbb{C}$ as

$$\begin{aligned}\mathbb{C} &= \mathbb{R} \times \mathbb{R} \\ &= \{(x, y) \mid x, y \in \mathbb{R}\}.\end{aligned}$$

(In other words, the complex plane is defined to be the Euclidean plane.) From here, one can define the usual algebraic operations on $\mathbb{C}$ as before, for instance,

- Addition: $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, x_2 + y_2)$.
- Multiplication: $(x_1, y_1) \times (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$.

6. Cardinality

In the final chapter of these notes, we turn our attention to cardinality. Roughly speaking, the cardinality of a set A refers to the "number of elements in A".

For most of this chapter, our focus will be on finite sets, for which we can provide a precise, formal definition of "number of elements". Along the way, we will look at some basic results in combinatorics, which deals with counting the cardinalities of finite sets.

Finally, at the end of the chapter, we will briefly turn toward infinite sets. In particular, we will explore how we can make sense of infinite cardinalities, and we will conclude the notes by highlighting some surprising consequences of this theory.

6.1. **Finite Sets.** Let us start with an easy question for toddlers:

Question 6.1. *How many elements are in the set* $A = \{-2, -1, 0, 1, 2\}$*?*

Of course, you would immediately know the answer to this question—A has 5 elements. But how did you arrive at "5"? Well, all you had to do was to *count all the elements of* A!

But, what does it mean exactly to "count the elements of A"? If you break things down, then you probably listed these elements in a manner similar to the following:

- Element 1 $\mapsto$ -2.
- Element 2 $\mapsto$ -1.
- Element 3 $\mapsto$ 0.
- Element 4 $\mapsto$ 1.
- Element 5 $\mapsto$ 2.

Since we have now exhausted all the elements of A, and since labelling of the elements stopped at "5", we would then conclude that A indeed has 5 elements.

The one (non-toddler-level) insight to take from all this is that the counting done in the above bullet points looks suspiciously like a function. In fact, the process can be modelled by the function $f : \{1, 2, 3, 4, 5\} \to A$ satisfying the following:

$$f(1) = -2, \quad f(2) = -1, \quad f(3) = 0, \quad f(4) = 1, \quad f(5) = 2.$$

Furthermore, this f is bijective, since it maps to each element of A exactly once.

Consequently, "counting the elements of A" is represented by this bijective function $f : \{1, 2, 3, 4, 5\} \to A$. However, there is nothing special about the set A, and the counting of any finite set can be analogously modelled by bijective functions. This leads us to our first definition, which makes rigorous the notion of "number of elements" of finite sets:

Definition 6.2. *Let A be a set, and let $n \in \mathbb{N}$.*

- *We say that A has cardinality n, written more concisely as $|A| = n$, iff there exists a bijective function $f : \{1, 2, \ldots, n\} \to A$.*
- *The empty set is defined to have cardinality 0, i.e. $|\emptyset| = 0$.*

Example 6.3. *From our preceding discussion, since we have found a bijective function*

$$f : \{1, 2, 3, 4, 5\} \to \{-2, -1, 0, 1, 2\},$$

it follows from Definition 6.2 that

$$|\{-2, -1, 0, 1, 2\}| = 5.$$

Example 6.4. *Consider next the set*

$$B = \{p \in \mathbb{N} \mid (p \text{ is prime}) \text{ and } (p \leq 20)\}.$$

Observe that B can be more explicitly written as

$$B = \{2, 3, 5, 7, 11, 13, 17, 19\}.$$

From the above, it is easy to see that $|B| = 8$. For a rigorous confirmation of this, one can, for instance, construct a bijective function $f : \{1, 2, \ldots, 8\} \to B$ as follows:

$$f(1) = 2, \quad f(2) = 3, \quad f(3) = 5, \quad f(4) = 7,$$
$$f(5) = 11, \quad f(6) = 13, \quad f(7) = 17, \quad f(8) = 19.$$

Throughout these notes, we have often thrown around the terms "finite" and "infinite" without defining them precisely. We can now finally address this shortcoming:

Definition 6.5. *Let A be a set.*

- *A is finite iff $|A| = k$ for some $k \in \mathbb{N} \cup \{0\}$.*
- *A is infinite iff A is not finite.*

6.1.1. *Comparing Cardinalities.* Our next topic is to compare cardinalities of finite sets, that is, to see which of two finite sets has more elements.

Before jumping into this, let us first mention some preliminary properties of function compositions that will be needed in upcoming proofs:

Proposition 6.6. *Let A, B, C be sets, and let $f : A \to B$ and $g : B \to C$.*

(1) *If f and g are both injective, then $g \circ f$ is injective.*
(2) *If f and g are both surjective, then $g \circ f$ is surjective.*
(3) *If f and g are both bijective, then $g \circ f$ is bijective.*

Proof. (Parts (1) and (2) are left as questions in the last tutorial sheet.)

Part (3) an immediate consequence of (1), (2), and Definition 5.77. □

We begin by considering when two finite sets have the same cardinality. Similar to Definition 6.2, the answer to this can be given in terms of bijective functions:

Theorem 6.7. *Let A, B be non-empty finite sets. Then, $|A| = |B|$ (i.e. A, B have the same cardinality) if and only if there exists a bijective function $g : A \to B$.*

Proof of Theorem 6.7. First, suppose $|A| = |B| = n$, where $n \in \mathbb{N}$. Then, from Definition 6.2, we see that there exist bijective functions

$$f_A : \{1, 2, \ldots, n\} \to A, \qquad f_B : \{1, 2, \ldots, n\} \to B.$$

Moreover, since f_A is invertible by Theorem 5.85, it follows that

$$g = (f_B \circ f_A^{-1}) : A \to B$$

is a bijective function, by Proposition 6.6(3).

Conversely, suppose $g : A \to B$ is bijective, and let $n = |A|$. Then, there exists a bijective function $f : \{1, 2, \ldots, n\} \to A$. By Proposition 6.6(3), we see that

$$g \circ f : \{1, 2, \ldots, n\} \to B$$

is a bijective function, hence $|B| = n$ by Definition 6.2. □

Next, a related but more subtle fact is that *inequalities* between cardinalities of finite sets can be characterised in terms of injective and surjective functions:

Theorem 6.8. *Let A, B be non-empty finite sets.*

(1) $|A| \leq |B|$ *if and only if there exists an injective* $g : A \to B$.

(2) $|A| \geq |B|$ *if and only if there exists a surjective* $g : A \to B$.

Proof of Theorem 6.8. Throughout the proof, we set $n = |A|$ and $m = |B|$ for convenience. Recall that by Definition 6.2, there exist bijective functions

$$f_A : \{1, 2, \ldots, n\} \to A, \qquad f_B : \{1, 2, \ldots, m\} \to B.$$

(1) First, suppose $|A| \leq |B|$, that is, $n \leq m$. Consider the restriction

$$\tilde{f}_B : \{1, 2, \ldots, n\} \to B, \qquad \tilde{f}_B(k) = f(k).$$

(Note in particular the above is a valid function definition, since $n \leq m$.) Since f_B is injective, it follows that $\tilde{f}_B$ is also injective. As a result, using Proposition 6.6(1), we see that the composition $g = \tilde{f}_B \circ f_A^{-1} : A \to B$ is an injective function.

Conversely, suppose $g : A \to B$ is injective. Since f_A and f_B are injective, then

$$h = f_B^{-1} \circ g \circ f_A : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$$

is injective as well, by Proposition 6.6(1). Now, since h can map to each element in $\{1, 2, \ldots, m\}$ at most once, one can see that the above is only possible when $n \leq m$. (For brevity, we omit a detailed proof of this, but hopefully it makes intuitive sense.)

(2) Suppose first that $|A| \geq |B|$. Since $n \geq m$ and $B \neq \emptyset$, we can define

$$\hat{f}_B : \{1, 2, \ldots, n\} \to B, \qquad \tilde{f}_B(k) = \begin{cases} f_B(k) & \text{if } 1 \leq k \leq m, \\ f_B(1) & \text{if } m < k \leq n. \end{cases}$$

Since f_B is surjective, it follows that $\hat{f}_B$ is also surjective. Thus, by Proposition 6.6(2), the composition $g = \hat{f}_B \circ f_A^{-1} : A \to B$ gives us a surjective function.

Conversely, suppose $g : A \to B$ is surjective. Since f_A and f_B are surjective, then

$$h = f_B^{-1} \circ g \circ f_A : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$$

is also surjective, by Proposition 6.6(2). Now, each element of $\{1, 2, \ldots, m\}$ is mapped to by h to at least once, but this is only possible when $n \geq m$. □

Note. *In fact, both Theorems 6.7 and 6.8 hold for all finite sets, even when A or B is empty. We restricted the theorem statement to non-empty finite sets only to simplify the proof, since the empty set must otherwise be treated separately as a special case.*

In particular, observe that when $A = B = \emptyset$, we have $|A| = |B| = 0$. In this case, $\emptyset$ itself is a bijective function from $A = \emptyset$ to $B = \emptyset$. (As strange as that sounds, you can check from definitions that $\emptyset$ is indeed a bijective function.)

While Theorems 6.7 and 6.8 are simple properties that one can prove for finite cardinalities, we will only see their true significance later, once we discuss *infinite* sets.

6.2. **Combinatorics.** To further build upon our newly defined notion of finite cardinality, we take a brief stroll into the field of combinatorics—roughly, the study of counting. We begin by surveying some of the most basic results in combinatorics, which many of you will have already seen before. In the end, we will give one example of how combinatorial ideas can be applied to other parts of mathematics!

6.2.1. *Counting Pairings.* For our first combinatorics result, consider the following "real world" problem, loosely based on this very module.

Question 6.9. *Suppose there are m students in NSF tutorial group A and n students in NSF tutorial group B. The students are now giving team presentations, with each team consisting of a pair of students, one from group A and one from group B. How many possible teams can one form from groups A and B?*

One can reformulate the above more precisely and mathematically in terms of cardinalities of sets. For instance, we can let A represent the set of students from group A, and B represent the set of students in group B. Moreover, each team is then modelled by a pair $(a, b) \in A \times B$, that is, satisfying $a \in A$ and $b \in B$.

With the above in mind, Question 6.9 is then equivalent to the following:

Question 6.10. *Let A, B be finite sets. If $|A| = m$ and $|B| = n$, then what is $|A \times B|$?*

The key to answering Question 6.10 is that *each $a \in A$ can be paired with n elements of B*, i.e. there are n pairs for which the first component is a. Since this holds for each of the m elements of A, *the total number of pairs in $A \times B$ is $m \cdot n$*:

Proposition 6.11. *If A, B are non-empty finite sets, and if $|A| = m$ and $|B| = n$, then*

$$|A \times B| = m \cdot n.$$

While the preceding discussion already gives the key insight behind Proposition 6.11, with a bit more care, we can also formulate a rigorous proof of this:

Proof of Proposition 6.11. By Definition 6.2, there exist bijective functions

$$a : \{1, 2, \ldots, m\} \to A, \qquad b : \{1, 2, \ldots, n\} \to B.$$

Moreover, by Definition 6.2, it suffices to construct a bijective function

$$g : \{1, 2, \ldots, mn\} \to A \times B.$$

One such bijective g can be defined by setting

$$g(kn + l) = (a(k), b(l)),$$

for any $k \in \{0, 2, \ldots, m - 1\}$ and $l \in \{1, 2, \ldots, n\}$. (Notice that the above is a valid function definition, as any $p \in \{1, 2, \ldots, mn\}$ can be written uniquely in the form $kn + l$, with k, l as above; this can be proved using Theorem 4.33.) □

Example 6.12. *Suppose there are 12 students in tutorial group A and 11 students in tutorial group B. Then, by Proposition 6.11, the number of possible presentation teams, with one member from group A and one member from group B, is $12 \cdot 11 = 132$.*

Note. *Proposition 6.11 still holds even when either A or B is empty. In this case, Definition 5.4 implies $A \times B$ is the empty set, so $|A \times B| = 0$.*

6.2.2. *Counting Subsets.* Next, we consider the following "real world" combinatorics problem, which we once again set in the land of NSF:

Question 6.13. *In a class of n NSF students, some attend the lecture, while others skip. In how many possible groups of students could have attended the lecture?*

One can again find a more precise mathematical formulation of the above. Let A be the set of students in NSF, so that $|A| = n$. Then, the group of students who actually attended the lecture can be represented by a subset $B \subseteq A$. As a result, Question 6.13 is essentially asking how many different subsets of A there are. Since the power set $\mathcal{P}(A)$ is the set of all subsets of A, Question 6.13 is equivalent to the following:

Question 6.14. *Let A be a finite set. If $|A| = n$, then what is $|\mathcal{P}(A)|$?*

The main idea behind answering Question 6.14 is as follows. First, we label the elements of A as $a_1, a_2, \ldots, a_n$. Then, all the possible subsets of A can be listed as follows:

- a_1 is either in or not in A (there are 2 possibilities).
- a_2 is either in or not in A (there are 2 possibilities).
- $\vdots$
- a_n is either in or not in A (there are 2 possibilities).

In other words, *each additional element of A doubles the total number of subsets of A* (all the possibilities for the previous elements remain, while the newest element can either be in or not in A). As a result, the total number of subsets of A is

$$\underbrace{2 \cdot 2 \cdot \cdots \cdot 2}_{n \text{ times}} = 2^n.$$

This leads us to the following result:

Proposition 6.15. *If A is a non-empty finite set, and if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.*

Proof of Proposition 6.15. (This is left as an exercise in the problem sheets.) □

Note. *Proposition 6.15 still holds when $A = \emptyset$, that is, when $|A| = 0$. In particular, in this case, we have $\mathcal{P}(\emptyset) = \{\emptyset\}$, hence $|\mathcal{P}(\emptyset)| = 1 = 2^0$.*

Example 6.16. *Suppose there are 205 NSF students in the class. Then, by Proposition 6.15, there are 2^{205} possible groups of students who could have attended the lecture.*

6.2.3. *Permutations.* For our next problem, we consider the following:

Question 6.17. *Suppose n NSF students need to give a presentation in class, and we need to determine an order in which these students will present. In how many different ways can we order the student presentations?*

For a more precise formulation, let A be the set of NSF students, so that $|A| = n$. Now, to order the students, one needs to choose which element of A goes first, second, and so on. The key observation is that this ordering be modelled using a bijective function

$$f : \{1, 2, \ldots, n\} \to A.$$

In particular, $f(1)$ is the student who presents first, $f(2)$ is the student who presents second, and so on. More generally, $f(k)$, for any $k \in \{1, 2, \ldots, n\}$, is the k-th presenter.

As a result, we can equivalently state Question 6.17 as follows:

Question 6.18. *Let A be a non-empty, finite set. If $|A| = n$, then what is*

$$\left|\{f : \{1, 2, \ldots, n\} \to A \mid f \text{ is bijective}\}\right| ?$$

Note. *In combinatorics, an ordering of the elements of A is called a permutation.*

To answer Question 6.18, the main observation is as follows:

- There are n possibilities for choosing the first element in our order.
- Once the first element has been chosen, then there are $n-1$ remaining possibilities in choosing the second element in our order.
- $\vdots$
- Once the $(n-1)$-th element has been chosen, then there is 1 remaining possibility in choosing the last (n-th) element in our order.

As a result, for the full ordering of A, the total number of possibilities is

$$n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 = \prod_{k=1}^{n} k.$$

Many readers will already be aware that the above product, which arises often in combinatorics, is called a factorial and has a convenient shorthand:

Definition 6.19. *Given $n \in \mathbb{N}$, we define the abbreviation*

$$n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1.$$

In addition, by convention, we define $0! = 1$.

Note. *While the convention $0! = 1$ may seem strange at first glance, one justification is that with this, we now have $n! = n \cdot (n-1)!$ for all $n \in \mathbb{N}$.*

Combining all the above, we arrive at the following answer to Question 6.18:

Proposition 6.20. *If A is a non-empty finite set, and if $|A| = n$, then*

$$\left|\{f : \{1, 2, \ldots, n\} \to A \mid f \text{ is bijective}\}\right| = n!.$$

Example 6.21. *Suppose 8 NSF students are giving a presentation in class. Then, from Proposition 6.20, there are $8! = 40320$ orders in which the students could present.*

Note. *In the context of probability and statistics, Question 6.17–6.18 are often referred to as "ordered sampling without replacement". When ordering the elements of A, we are choosing its elements one by one, in a manner in which the order of the choice matters, and in which any element that we have already chosen cannot be picked again.*

6.2.4. *Combinations.* Our final "real world" problem is the following:

Question 6.22. *In a class of n NSF students, k lucky students are selected to give a presentation in front of the class. In how many ways can these students be chosen?*

Once again, let A represent the set of NSF students, with $|A| = n$. The k special students that are chosen to give a presentation can then be represented by a subset $B \subseteq A$ satisfying $|B| = k$. Thus, we must count all the subsets of A that have cardinality k.

The above implies Question 6.22 can be equivalently stated as follows:

Question 6.23. *Let A be a finite set. If $|A| = n$ and $k \in \{0, 1, \ldots, n\}$, then what is*

$$\left|\{B \subseteq A \mid |B| = k\}\right|?$$

Note. *In combinatorics, a selection of k elements of A is called a k-combination.*

To answer Question 6.23, we want to count all the subsets $\{a_1, a_2, \ldots, a_k\} \subseteq A$ having cardinality k. For this, we observe the following:

- There are n possibilities for choosing a_1.
- Once a_1 has been chosen, there are then $n - 1$ possibilities for a_2.
- $\vdots$
- Once a_{k-2} has been chosen, there are then $n - k + 2$ possibilities for a_{k-1}.
- Once a_{k-1} has been chosen, there are then $n - k + 1$ possibilities for a_k.

Thus, to choose $a_1, a_2, \ldots, a_k$ altogether, the number of possibilities is

$$n \cdot (n-1) \cdot \cdots \cdot (n-k+1) = \frac{n \cdot (n-1) \cdot \cdots \cdot (n-k+1) \cdot (n-k)!}{(n-k)!} = \frac{n!}{(n-k)!}. \tag{6.1}$$

Notice, however, that *in the above process, we overcounted*! Indeed, here we chose a_1 *first*, a_2 *second*, and so on. On the other hand, in a subset $\{a_1, a_2, \ldots, a_k\}$, the ordering of all the a_i's does not matter. As a result, *each subset $\{a_1, a_2, \ldots, a_k\}$ has been counted multiple times—in fact, as many times as the number of orderings of $a_1, a_2, \ldots, a_k$.*

Now, recalling Proposition 6.20, we know there are exactly $k!$ different orderings of $a_1, a_2, \ldots, a_k$. As a result, our figure from (6.1) should be divided by $k!$ in order to account for our overcounting, leading to a revised total of

$$\frac{n!}{k!(n-k)!}.$$

This quantity also arises often in combinatorics, hence we adopt a shorthand:

Definition 6.24. *Given $n, k \in \mathbb{N} \cup \{0\}$, we define the binomial coefficient*

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

Note. *The binomial coefficient* $\binom{n}{k}$ *is read as "*n *choose* k*".*

From the above, we obtain the following answer to Question 6.23:

Proposition 6.25. *If* A *is a finite set,* $|A| = n$*, and* $k \in \{0, 1, \ldots, n\}$*, then*

$$\left|\{B \subseteq A \mid |B| = k\}\right| = \binom{n}{k}.$$

Note. *The formula in Proposition 6.25 continues to hold even when* $k > n$*, since there are no subsets of* A *with more than* n *elements.*

Example 6.26. *Suppose there are* 205 *NSF students, of which* 3 *are chosen to give a presentation. Then, the number of ways these* 3 *students can be selected is*

$$\begin{aligned}\binom{205}{3} &= \frac{205!}{3!202!} \\ &= 1414910.\end{aligned}$$

Note. *In the context of probability and statistics, Question 6.22–6.23 are often referred to as "unordered sampling without replacement". Here, we are choosing elements of* A*, in a manner in which the order of the choice does not matter, and in which any element that we have already chosen cannot be picked again.*

6.2.5. *The Binomial Theorem.* We conclude our brief survey of combinatorics by demonstrating how its results can be applied to other parts of mathematics. Here, we present a famous example of one application of Propositions 6.15 and 6.25.

The key point is that there are two ways to count the subsets of $\{1, 2, \ldots, n\}$, where $n \in \mathbb{N}$. First, recall that since $\{1, 2, \ldots, n\}$ has cardinality n, Proposition 6.15 yields

$$|\mathcal{P}(\{1, 2, \ldots, n\})| = 2^n, \tag{6.2}$$

that is, *there are* 2^n *different subsets of* $\{1, 2, \ldots, n\}$.

Alternatively, we can classify the subsets of $\{1, 2, \ldots, n\}$ according to their cardinalities. Since subsets of $\{1, 2, \ldots, n\}$ could have cardinalities ranging from 0 to n (inclusive), then we can also decompose the total number of subsets of $\{1, 2, \ldots, n\}$ as a sum:

$$\begin{aligned}|\mathcal{P}(\{1, 2, \ldots, n\})| &= (\text{number of subsets of } \{1, 2, \ldots, n\}) \\ &= \sum_{k=0}^{n} (\text{number of subsets of } \{1, 2, \ldots, n\} \text{ having cardinality } k).\end{aligned}$$

Recalling now Proposition 6.25, the above then becomes

$$|\mathcal{P}(\{1, 2, \ldots, n\})| = \sum_{k=0}^{n} \binom{n}{k}. \tag{6.3}$$

Combining equations (6.2) and (6.3), we obtain the following:

Proposition 6.27. *The following holds for any $n \in \mathbb{N} \cup \{0\}$:*

$$\begin{aligned}2^n &= \sum_{k=0}^{n} \binom{n}{k} \\ &= \sum_{k=0}^{n} \frac{n!}{k!(n-k)!}.\end{aligned}$$

Note the equation in Proposition 6.27, which involves a sum containing many factorials, is not so easy to derive directly. However, by observing that all the quantities have combinatorial interpretations that can be linked to each other, as we did in the above, we obtained a quick derivation of Proposition 6.27 that required very little computation.

In fact, Proposition 6.27 is a special case of a more general formula:

Theorem 6.28 (Binomial theorem). *For any $n \in \mathbb{N} \cup \{0\}$ and $x, y \in \mathbb{R}$, we have*

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

Note that by setting $x = y = 1$ in Theorem 6.28, we recover the formula from Proposition 6.27. Moreover, taking other values of x and y leads to other useful formulas.

Though we omit the proof of Theorem 6.28 here, it is actually not so difficult. There are, in fact, many different ways to prove this—for example, Theorem 6.28 could be derived using an induction on n, along with some basic properties of the binomial coefficients.

Note. *The more standard definition of $\binom{n}{k}$ is as the coefficient of the $x^{n-k}y^k$-term of $(x+y)^n$; this is the reason for the name "binomial coefficient".*

From this point of view, Theorem 6.28 becomes the definition of the binomial coefficients, while Definition 6.24 becomes the property to be proved.

6.3. **Infinite Sets.** In this final section of the lecture notes, we turn to infinite sets and their cardinalities. However, we immediately run into a fundamental question:

Question 6.29. *What does it even mean to measure cardinalities of infinite sets?*

For a finite set A, we can measure its cardinality by "counting" the number of elements in A. However, if A is infinite, and we adopt the same strategy, then we will be counting for an eternally long time—not a very practical solution, unfortunately. Thus, if we want to make any sense of cardinalities of infinite sets in the first place, then we will already need to be considerably more clever in our approach.

The main insight for this comes from Theorem 6.7, which characterises two finite sets A, B having the same cardinality in terms of bijective functions from A to B. The clever observation here is that *although "counting" no longer makes sense for infinite sets, bijective functions make perfect sense for any sets, finite or infinite.* This gives us a natural method to extend our cardinality theory for finite sets to infinite sets.

More specifically, we can use the conclusion of Theorem 6.7 as the *definition* for comparing infinite cardinalities. This leads us to the following:

Definition 6.30. *Let A, B be sets (either finite or infinite). We say that A and B have the same cardinality, denoted $|A| = |B|$, iff there exists a bijective function $f : A \to B$.*

In addition, though we will not really make use of this in these notes, we can also build upon Theorem 6.8 to define *inequalities* of cardinalities:

Definition 6.31. *Let A, B be sets (either finite or infinite). We say that $|A| \leq |B|$ holds iff there exists an injective function $f : A \to B$.*

Having a precise way to compare infinite cardinalities leads to the following:

Question 6.32. *Do all infinite sets have the same cardinality? Or, are there different infinite cardinalities—can some sets be "more infinite than others"?*

In the following, we explore Question 6.32 by studying the cardinalities of some basic infinite sets—namely, the various sets of numbers from Chapter 4.

Note. *To keep the ensuing discussions brief, we will avoid giving full, precise proofs of most of the upcoming results. Instead, we opt for semi-formal arguments that demonstrate the main ideas behind why these results hold.*

6.3.1. *Countable Infinity.* Let us begin with the natural numbers $\mathbb{N}$. First, to get the obvious part out of the way, we establish that $\mathbb{N}$ is indeed infinite:

Theorem 6.33. *$\mathbb{N}$ is infinite.*

Proof of Theorem 6.33. According to Definition 6.5, since clearly $\mathbb{N} \neq \emptyset$ (thus $|\mathbb{N}| \neq 0$), in order to show $\mathbb{N}$ is not finite, we must prove that $|\mathbb{N}| \neq n$ for any $n \in \mathbb{N}$—that is, there is no bijective function from $\{1, 2, \ldots, n\}$ to $\mathbb{N}$. In other words, we must show that *every function* $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ *fails to be bijective.*

Consider now an arbitrary $f : \{1, 2, \ldots, n\} \to \mathbb{N}$. Since

$$\operatorname{range}(f) = \{f(1), f(2), \ldots, f(n)\}$$

is finite, then it has a maximum value $m = f(k)$ for some $k \in \{1, 2, \ldots, n\}$. But then, $m + 1 \notin \operatorname{range}(f)$, so f is not surjective and hence is also not bijective. □

Next, consider the integers $\mathbb{Z}$. A natural question to ask is the following:

Question 6.34. *Are $|\mathbb{N}|$ and $|\mathbb{Z}|$ the same? Or, is $|\mathbb{N}| < |\mathbb{Z}|$?*

On one hand, $\mathbb{Z}$ consists of not only the natural numbers, but also zero and the negative integers, the latter of which could be viewed as yet another "copy" of $\mathbb{N}$. Thus, it might seem that there should be many more integers than natural numbers.

However, is this actually the case? To answer this, we will need to explore what Definition 6.30 gives us, as it is only through this precise definition that we can even make sense of comparing the cardinalities of $\mathbb{N}$ and $\mathbb{Z}$. Fortunately for us, we have already secretly answered Question 6.34 earlier without realising it! Indeed, the main insight comes from Example 5.89, and the result that follows is rather surprising:

Theorem 6.35. $|\mathbb{Z}| = |\mathbb{N}|$.

Thus, though it might seem at first glance that there are far more integers than natural numbers, our precise Definition 6.30 tells us $\mathbb{N}$ *and* $\mathbb{Z}$ *actually have the same cardinality*!

Proof of Theorem 6.35. Example 5.89 yields a bijective function

$$f : \mathbb{Z} \to \mathbb{N}, \qquad f(k) = \begin{cases} 2k & \text{if } k > 0, \\ 1 - 2k & \text{if } k \leq 0. \end{cases}$$

between $\mathbb{N}$ and $\mathbb{Z}$. Thus, the desired conclusion follows from Definition 6.30. □

Let us now go even "bigger" and consider the rational numbers $\mathbb{Q}$, which consists of not only the integers, but all the fractions that fill in the spaces between integers. Once again, this seems like we have added many new numbers! But, is it the case that $\mathbb{Q}$ has larger cardinality than $\mathbb{N}$ and $\mathbb{Z}$? More specifically, we ask the following:

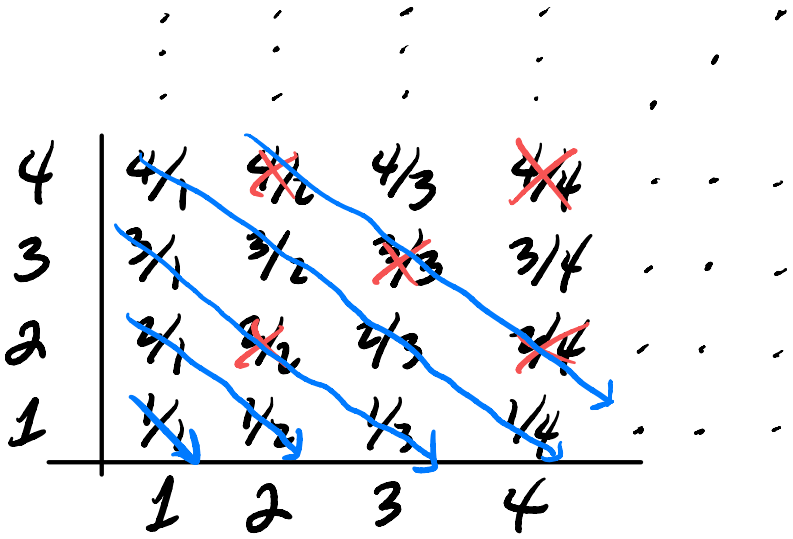
Question 6.36. *Are* $|\mathbb{N}|$ *and* $|\mathbb{Q}|$ *the same? Or, is* $|\mathbb{N}| < |\mathbb{Q}|$*?*

The answer to Question 6.36 again comes as a surprise and strains our intuitions:

Theorem 6.37. $|\mathbb{Q}| = |\mathbb{N}|$.

Ideas behind Theorem 6.37. To make the explanations simpler, let us construct instead a bijective function $f : \mathbb{Q}_+ \to \mathbb{N}$, where $\mathbb{Q}_+$ is the set of all *positive rational numbers*; Definition 6.30 would then give us $|\mathbb{Q}_+| = |\mathbb{N}|$. (Once we have this, it is then not so difficult to show that $\mathbb{Q}$ and $\mathbb{Q}_+$ also have the same cardinality.)

The ideas for constructing this f can be found in the table illustrated below:



Here, we arranged all the positive fractions in an "infinite table", with the rows representing the numerator values and the columns representing the denominator values. Notice the fractions are not uniquely represented—for example, $\frac{1}{1}$, $\frac{2}{2}$, and $\frac{3}{3}$ all represent the same number. To get around this issue, we crossed out in red all the fractions in the table that are not in simplest form. (Any crossed out number is equal to its representation in simplest form, which is elsewhere in the table.)

Now, the clever trick is to list all the positive fractions in the table in a specific order—starting from the bottom left corner, we traverse along each downward-and-rightward diagonal of the table (drawn in blue), and we then go upwards through all the diagonals. If we list these positive fractions (but skipping those that are crossed out in red) while traversing these blue diagonals in the above-mentioned order, then we will hit every positive fraction exactly one time.

Finally, to define f, all we have to do is to match all the natural numbers to elements of $\mathbb{Q}_+$ according to this ordering. More specifically:

- Starting from the bottom left diagonal, we define $f(\frac{1}{1}) = 1$. .
- Moving to the next diagonal, we then set $f(\frac{2}{1}) = 2$ and $f(\frac{1}{2}) = 3$.
- Similarly, for the third diagonal, we set $f(\frac{3}{1}) = 4$, we skip $\frac{2}{2}$ (which is crossed out in red), and we define $f(\frac{1}{3}) = 5$.
- The remaining values of f are defined by continuing this pattern indefinitely.

Observe, most importantly, that the above defines a bijective function $f : \mathbb{Q}_+ \to \mathbb{N}$! As a result, by Definition 6.30, we conclude that $|\mathbb{N}| = |\mathbb{Q}_+|$. □

Note. *Using the same argument as in the proof of Theorem 6.37, one can also show that* $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$. *Furthermore, since* $\mathbb{N}$ *and* $\mathbb{Q}$ *have the same cardinality, then* $|\mathbb{Q}\times\mathbb{Q}| = |\mathbb{N}|$ *as well. Continuing along these lines, we can build progressively "larger-looking" sets that turn out to have the same cardinality as* $\mathbb{N}$*!*

6.3.2. *Uncountable Infinity.* Thus far, all the infinite sets we have considered have the same cardinality as $\mathbb{N}$. Although this is a small sample size, we could already wonder whether our infinite mathematical landscape is as boring as the above suggests:

Question 6.38. *Do all infinite sets have the same cardinality?*

To investigate Question 6.38, let us move on to the next number system—the real numbers $\mathbb{R}$. Here, we come across our second major plot twist, which was first discovered by mathematician Georg Cantor in 1874. In particular, Cantor proved the following:

Theorem 6.39. $|\mathbb{N}| \neq |\mathbb{R}|$.

Furthermore, the following function is clearly injective,

$$i : \mathbb{N} \to \mathbb{R}, \qquad i(n) = n,$$

so Definition 6.31 yields $|\mathbb{N}| \leq |\mathbb{R}|$. Theorem 6.39 hence gives us that $|\mathbb{N}| < |\mathbb{R}|$.

Thus, in a sharp contrast to Theorems 6.35 and 6.37, *there are more real numbers than there are natural numbers (and, by extension, also integers and rational numbers)*! The key insight behind this is an ingenious argument that is now commonly known as "Cantor diagonalisation". We give an informal description of this process below:

Ideas behind Theorem 6.39. To simplify the exposition, let us show instead

$$|\mathbb{N}| \neq |(0,1)|, \tag{6.4}$$

where $(0,1)$ denotes the standard open interval

$$(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

(Once (6.4) is in hand, it is not so hard to show that $|(0,1)| = |\mathbb{R}|$.)

Similar to the proof of Theorem 6.33, according to Definition 6.30, we must show there is no bijective function from $\mathbb{N}$ to $(0,1)$. In other words, it suffices to show:

- *Every function* $f : \mathbb{N} \to (0,1)$ *fails to be bijective.*

For this, let us consider an arbitrary $f : \mathbb{N} \to (0,1)$. The idea is to then write each output value of f as an infinite decimal expansion:

$$\begin{aligned} f(1) &= 0.x_{11}x_{12}x_{13}x_{14}\ldots, \\ f(2) &= 0.x_{21}x_{22}x_{23}x_{24}\ldots, \\ f(3) &= 0.x_{31}x_{22}x_{33}x_{34}\ldots, \\ f(4) &= 0.x_{41}x_{42}x_{43}x_{44}\ldots, \\ &\vdots \end{aligned} \tag{6.5}$$

Here, each x_{ij} is a digit, i.e. one of the numbers $0, 1, \ldots, 9$.

Now, the brilliant insight is to look at the "diagonal digits" $x_{11}, x_{22}, x_{33}, \ldots$ in (6.5); these are highlighted in pink. The idea, for each $n \in \mathbb{N}$, is to *alter the diagonal digit* x_{nn} *to a new digit* $d_n \neq x_{nn}$. (For example, if $x_{11} = 5$, then we could choose $d_1 = 6$ or $d_1 = 4$; similarly, if $x_{33} = 0$, then we could take $d_3 = 4$ or $d_3 = 7$.) We can then define a new real number $y \in (0,1)$ via the infinite decimal expansion

$$y = 0.d_1d_2d_3d_4\ldots.$$

Observe that the following holds for y:

- Since $d_1 \neq x_{11}$, it follows that y and $f(1)$ have different first digits after the decimal point. As a result, we have that $y \neq f(1)$.
- Since $d_2 \neq x_{22}$, it follows that y and $f(2)$ differ in the second digit after the decimal point. As a result, we have $y \neq f(2)$.
- Similarly, since $d_3 \neq x_{33}$, we obtain that $y \neq f(3)$.

Continuing this process indefinitely, we derive $y \neq f(n)$ for every $n \in \mathbb{N}$!

Since y differs from *every* output of f, we conclude $y \in (0,1)$ is not in the range of f. As a result, f is fails to be surjective and hence bijective, proving (6.4).

(One extra pitfall in this argument is that some numbers have more than one decimal expansion; for example, $0.129999\ldots$ and $0.13000\ldots$ represent the same real number. However, we can circumvent this danger by never choosing any d_n to be 9 or 0, since two distinct decimal expansions can represent the same number only when there are infinitely repeating 9's and 0's involved.) □

In particular, Theorem 6.39 tells us *there is more than one infinite cardinality*:

- First, we have $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, which are said to be countably infinite. (The name arises from this being the cardinality of $\mathbb{N}$, which is associated with counting.)
- On the other hand, we have $\mathbb{R}$, which is said to be uncountable.

Note. *In addition to Theorem 6.39, we can also derive that there are more irrational numbers than natural numbers and rational numbers, i.e.*

$$|\mathbb{N}| < |\mathbb{R} \setminus \mathbb{Q}|, \qquad |\mathbb{Q}| < |\mathbb{R} \setminus \mathbb{Q}|.$$

(The rough idea is that if $|\mathbb{Q}| = |\mathbb{R} \setminus \mathbb{Q}|$, then we can view $\mathbb{R}$ as "two copies of $\mathbb{Q}$", which together will have the same cardinality as $\mathbb{Q}$.) Thus, even though most numbers that you might think of or encounter are rational, the unsettling truth is that the rational numbers form only a vanishingly small proportion of the real numbers.

Note. *With a bit more effort, one can also show that*

$$|\mathbb{R}| = |\mathbb{R} \times \mathbb{R}|.$$

In other words, the cardinality of the real line is the same as the cardinality of the Euclidean plane! Thus, increasing the dimension of your space does not actually increase the cardinality—a bit counterintuitive, but true!

Now that we have found an uncountable cardinality, namely $|\mathbb{R}|$, it is natural to ask if there are other, even larger uncountable cardinalities:

Question 6.40. *Does there exist a set A with $|\mathbb{R}| < |A|$?*

Furthermore, if the answer to Question 6.40 is affirmative, then we can be even more ambitious and ask just how large cardinalities can be:

Question 6.41. *Is there a "largest" cardinality?*

Both Questions 6.40 and 6.41 were definitively answered by Georg Cantor. In particular, Cantor proved in 1891 the following striking result:

Theorem 6.42. *Let X be a set. Then, $|X| < |\mathcal{P}(X)|$.*

The proof of Theorem 6.42 seems quite tricky at first glance, but it is actually analogous to the proof of Theorem 6.39. Indeed, the argument is a clever reworking of the Cantor diagonalisation trick behind Theorem 6.39. We omit the proof here, but this is left as an exercise (with hints) in the problem sheets for the more ambitious readers.

Proof of Theorem 6.42. (See the problem sheets.) □

In particular, Theorem 6.42 provides a negative answer to Question 6.41:

- *There is no largest cardinality.*

Indeed, given any set X, no matter how large its cardinality, we can always construct its power set $\mathcal{P}(X)$, which will have even larger cardinality!

Furthermore, Theorem 6.42 goes above and beyond answering Question 6.40, as *we can construct infinitely many distinct cardinalities larger than* $|\mathbb{R}|$:

$$|\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < |\mathcal{P}(\mathcal{P}(\mathbb{R}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{R})))| < \dots.$$

Note. *In fact, with some additional effort, one can also prove that*

$$|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|.$$

6.4. **Final Notes.** Finally, we mention a couple closely related topics that are related to infinite cardinalities. These, however, do go beyond the scope of this module, so we avoid discussing them in detail in these lecture notes.

6.4.1. *(Bonus) The Continuum Hypothesis.* Consider the following:

- *There exists a set A such that $|\mathbb{N}| < |A| < |\mathbb{R}|$.*

This seemingly innocent statement is known as the continuum hypothesis, and it simply claims that there is a set whose cardinality is between that of $\mathbb{N}$ (countably infinite) and $\mathbb{R}$ (uncountable). We can then ask the following simple question:

Question 6.43. *Is the continuum hypothesis true or false?*

This seems harmless enough—such a statement should be either true or false, and we just need to figure out which one it is. However, things do not proceed according to plan:

- In 1940, Kurt Gödel proved (roughly speaking) that, *assuming the standard axioms of set theory, one cannot prove that the continuum hypothesis is false.*

Fantastic, the continuum hypothesis must then be true, right? Well, not so fast:

- Later, in 1963, Paul Cohen proved (roughly speaking) that, *assuming the standard axioms of set theory, one cannot prove that the continuum hypothesis is true.*

To make sense of this, recall the *Gödel incompleteness theorem* from Section 2.8, which roughly stated that for a sufficiently complex axiomatic system (e.g. "logic plus set theory"), there always exists some statement that cannot proved true or false. The continuum hypothesis is hence a concrete instance of this that is remarkably easy to state.

As a result, to establish the continuum hypothesis as true or false, we must impose additional axioms on our mathematical universe that tilt the playing field in one direction or the other. (For example, we could impose an axiom that simply assumes the continuum hypothesis true, though it is not philosophically clear *why* we should do this.) However, the Gödel theorem tells us that no matter how many more axioms we impose, there will always be some other statement that cannot be proved true or false.

6.4.2. *(Bonus) Cardinal Numbers.* Recall for a finite set A, we could actually assign a *number* $n \in \mathbb{N} \cup \{0\}$ to its cardinality $|A|$. For infinite sets, however, Definition 6.30 merely allows us to compare infinite cardinalities. On the other hand, we have not assigned any well-defined numerical value to $|\mathbb{N}|$, $|\mathbb{R}|$, $|\mathcal{P}(\mathbb{R})|$, and so on.

While the details are beyond this module, one can in fact construct a system of "infinite numbers" that extend beyond $\mathbb{N}$ and that can be assigned as cardinalities of infinite sets. These new numbers, along with 0 and $\mathbb{N}$, are together called the cardinal numbers.

For example, $|\mathbb{N}|$ is assigned a cardinal number that is commonly denoted as "$\aleph_0$". (The symbol "$\aleph$" is the Hebrew letter "aleph".) The larger cardinalities $|\mathbb{R}|$, $|\mathcal{P}(\mathbb{R})|$, etc. are then formally assigned even larger cardinal numbers.

Finally, just as one can add and multiply natural numbers, one can also make sense of adding and multiplying infinite cardinal numbers. These can be described more precisely as follows—given any sets A and B (finite or infinite), we define:

- Cardinal addition: $|A| + |B| = |(\{0\} \times A) \cup (\{1\} \times B)|$.
- Cardinal multiplication: $|A| \cdot |B| = |A \times B|$.

While we omit details here, see if you can make sense of the above definitions!