FUNDAMENTAL CONCEPTS IN MATHEMATICS
Contents

Preface 7

1 Functions, relations and sets 11
1.1 How big is big? 11
1.2 What is a “function” anyway? 11
1.3 A function is a relation 12
1.4 A relation is a set 12
1.5 An aside: naïve set theory 13
1.6 How to start writing proofs 13
1.7 Cardinality fundamentals 15
1.8 Countable and uncountable 20
1.9 Diagonal arguments as two-person games 21
1.10 Aside: What is a number? 25
1.11 Exercises 26

2 From numbers to rings 29
2.1 Divisibility 29
2.2 Prime numbers and canonical factorisation of integers 35
2.3 Aside: how are the primes distributed? 36
2.4 Mersenne primes and perfect numbers 38
2.5 Clock arithmetic 40
2.6 Aside: The RSA algorithm for public-key encryption 45
2.7 Exercises 49
3  **Rings beyond numbers**  53
   3.1  **Rings and fields**  53
   3.2  **Ideals**  55
   3.3  **An important interlude: Equivalence relations, partitions and quotients**  56
   3.4  **A construction of the rational numbers**  59
   3.5  **Geometric things as quotients**  61
   3.6  **Polynomials are like numbers**  61
   3.7  **Irreducibility and factorisation**  65
   3.8  **Gauß's Lemma**  66
   3.9  **Eisenstein's Criterion**  66
   3.10  **Clock arithmetic on polynomials**  67
   3.11  **Congruence modulo a polynomial and ideals**  71
   3.12  **Algebraic versus transcendental**  71
   3.13  **Aside: Constructible numbers**  74
   3.14  **Number-theory type results in ring theory**  75
   3.15  **Exercises**  76

4  **Normed vector spaces**  79
   4.1  **Abstract vector spaces: things that behave like \( \mathbb{R}^n \)**  79
   4.2  **Aside: The Axiom of Choice**  82
   4.3  **Norms**  83
   4.4  **Boundedness**  84
   4.5  **Epsilon versus delta**  86
   4.6  **Continuity for normed vector spaces**  87
   4.7  **Function spaces**  90
   4.8  **Exercises**  92

5  **Metric Spaces**  95
   5.1  **Limit of a function and limit of a sequence are really the same thing**  95
   5.2  **A good definition?**  96
   5.3  **Metrics**  97
   5.4  **Boundedness**  99
   5.5  **Cauchy sequences**  99
   5.6  **Exercises**  101
5.7 Complete metric spaces 102
5.8 The ring of Cauchy sequences 103
5.9 Construction of the real numbers 104
5.10 Arithmetic on $\mathbb{R}$ 105
5.11 What does $0.99999\ldots$ mean? 105
5.12 Aside: other ways to construct $\mathbb{R}$ 106
5.13 The topology of metric spaces 107
5.14 Continuity revisited 109
5.15 Function spaces as metric spaces 109
5.16 Contraction maps 110
5.17 Aside: Iteration Function System 113
5.18 Exercises 113

6 Compactness 115
6.1 From finiteness to compactness 115
6.2 Covers and the definition of compact sets 116
6.3 Closed, bounded and compact 117
6.4 Aside: Brouwer’s fixed-point theorem 119
6.5 Exercises 119

7 The twain shall meet 121
7.1 $p$-adic metric and the $p$-adic numbers 121
7.2 A bit more than what you know 122
7.3 Completing the rationals 123

8 Appendix 125

9 Index 129
Preface

A problem that I face in teaching this course is that I want to teach so much! Alas, I cannot expect a student to understand how much I or one of my colleagues might, but I do not want to short-change the students. There are elements of the fundamentals of mathematics that are truly fascinating and one could spend a whole course just discussing these. For example: “Set theory and logic” could be a thirteen-week course in itself; “Vector spaces” is normally taught in a course dedicated to linear algebra; “Ring theory” normally accompanies a primer on group theory. After a few years of experimenting with a second year course on pure mathematics, the balance has been found. The product is this course: a primer on the fundamental concepts of number systems and ring theory, together with the highlights of real analysis. Along the way, there will be “asides” which expand upon some of the gems we find by the roadside.

Warning: The notes are by no means complete. They are skeletal and it is up to the student to fill in with examples and proofs. This can be achieved either by reading a variety of good books that can be found in the library, or by attending lectures. These notes may not give you the insight in how the writer thought about the proofs or came up with them. This level of insight will be portrayed in lectures.

Theorems, lemmas and corollaries in this course can roughly be categorised into the following, and we will adjoin each result with the respective symbol:

★: The proof is beyond the expected skill level of the student if it were asked of the student to create a proof without ever have read a proof of the result before. However, if the student can recall the “gist” of the proof, or the trick involved, then the student should be able to do it.

†: The proof is beyond the expected skill-level of the student if it were asked of the student to create a proof without ever have read a proof of the result before. The proof is long, tedious or very complex and intricate. The lecturer does not think that being able to accomplish a proof such as this has any value to the students development.

◇: The proof of this result is sufficiently simple that by the end of the course, the student would be expected to be able to prove this result or one of a similar complexity, having never seen it before.

Acknowledgements

I would like to thank Murray Smith for reading drafts of these notes.
Learning outcomes

It is always difficult in mathematics to accurately describe the outcomes of learning this or that in the subject. I will attempt to list here what I think are the things the student should come away with and what they can ideally be able to do.

Proofs

This is really the first course in our undergraduate program where the student learns how to write proofs in a variety of situations. At the very least, the student should be able to do the auto-pilot component of a proof. By this, I mean that the student should know what the necessary steps are in a proof regardless of the difficult and ingenious step that some proofs require. For example, if the student is asked to prove that a function \( f : A \rightarrow B \) is one-to-one, then they must begin the proof with a line like “Suppose we have two elements \( a_1, a_2 \in A \) such that \( f(a_1) = f(a_2) \). We will show that \( a_1 = a_2 \).”

Definitions and examples

It cannot be said enough: mathematics is about clear and precise formulation of ideas. So the student must absolutely know the definitions of every concept in the course. In support of definitions, the student needs to know examples which satisfy a particular definition, and if possible, a non-example. That is, in some situations there is a hierarchy of structures, and there may be subtleties between the layers. For example, do you know of an algebraic number that is not an algebraic integer?

Philosophy of mathematics

From the very beginning of the course, the student will be exposed to the philosophical edge of mathematics. Are there different types of infinities? What does 0.999 \( \cdots \) mean? There is no better way for a student to get a thorough training in critical thinking than to embark on the theory of cardinalities and number systems, and to question the foundations of their subject. The student should know by the end of the course how we can construct the various number systems (e.g., rationals, reals) from the natural numbers, and why this was an important contribution to mathematics over a century ago. We come across diagonal arguments, and non-constructive proofs, and the student will have learnt how to picture difficult abstract ideas by analogy to concrete examples.

An introduction to the basics of abstract algebra

One of the clear goals of this course is as a primer on the basics of abstract algebra. At the heart, the student needs to be au fait with equivalence relations; they are everywhere in algebra! This course leads on to a third year unit in group theory (the mathematics of symmetry) and more ring theory, so some of the basics of ring theory will prepare the students for these two
units. The student must have a very good knowledge of the integers modulo $n$ and of polynomial rings. These are the basic structures of ring theory.

*An introduction to the basics of analysis*

Again, a clear goal of this course is as a primer on some sub-disciplines of the diverse area of *analysis*; the study of the infinite and infinitesimal. We will cover the elementary aspects of convergence and continuity, and the student will come away with a solid background in the theory of metric spaces. Normed vector spaces and metric spaces are the bedrock of functional analysis and geometry, and the student will need to be able to write good old $\delta/\epsilon$-proofs in this basic setting before setting upon the more general unit in third year. By the end of the course, the student will have the preparation need to understand the basics of differential geometry (e.g. manifolds, tangent bundles, etc.) and functional analysis (e.g. operator algebras, Hilbert spaces, etc). So we cover the themes of completeness and compactness, that historically give us the underpinning of modern analysis.
1

Functions, relations and sets

In this chapter we cover relations, basic set theory terminology, Russell’s Paradox, cartesian product of sets, definition of a function, one-to-one, onto, and an introduction to writing proofs.

1.1 How big is big?

For two finite sets, it is straightforward to work out which set is bigger: you simply count the elements of each set. What about infinite sets? Are there some infinite sets that are bigger than other infinite sets? Does it make sense to talk about infinity in the first instance?

Example 1.1.1. A European woman called Grietje counts out a set of numbers as follows, and asserts that there is a pattern that this sequence follows and that it goes on forever:

twee, vier, zes, acht, tien, twaalf, veertien, zestien, achttien, twintig, . . . .

You don’t know the language and so you guess that this person is just counting:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, . . . .

Then it is revealed to you that the language Grietje speaks is dutch and that she was counting the even numbers.

Question 1.1.2. How big is the set of even whole numbers? Is it smaller than the set of whole numbers? If we count the even numbers in a different language, do we see any difference between the even numbers and the whole set of numbers?

We will see that mathematics makes the answer to this question clear and concrete by giving a definition of what the size of a set is. It turns out that the even numbers have precisely the same size as the integers, that the rational numbers have the same size as the integers, and that the real numbers are definitely bigger than the integers.

1.2 What is a “function” anyway?

In secondary school, beyond polynomials we encounter functions that have more complicated descriptions such as log, exp and trigonometric functions. Often these functions were introduced to us passively, described
by association, yet did we really know what they were? What is the cosine of a real number? Next we learn that a function is a rule that assigns one value for every input: there cannot be two values for the same input.

Example 1.2.1. The equation \( f(x)^2 = 1 \) has two solutions: \( f(x) = 1 \) and \( f(x) = -1 \). So writing \( f(x) := \pm \sqrt{x^2} \) does not define a function as it is not single-valued.

Questions such as “what is a function?” were the types of questions some mathematicians of the 19th century were making in their search for a formal treatment of mathematics. We will see that on one hand, formalism was a triumph in mathematical thought, but on the other hand, it brought forth meta-mathematical and philosophical conundrums that shook the foundations of modern mathematics.

1.3 A function is a relation

The relations we will encounter in this course deal with the interactions of two things; they will be binary relations. The archetypical example will be that of friendship on the set of human beings. Given two people, we can establish whether they are friends or not. The reason to abstract and clarify the idea of a relation is simply because they are so fundamental in mathematics and occur so often. For example, we could say that a number is less than another number by

\[ x < y \]

or we could say that golden syrup (i.e. y) tastes better than honey (i.e. x). Notice that we mostly use infix notation for relations. A function is a relation too! When we write

\[ f(x) := x^2 \]

where \( x \) is a real number, what we are actually saying is that \( x \) is related to \( x^2 \). Of course, when we write it has a relation in infix notation, it looks like

\[ x f x^2. \]

This looks very weird, and in the case of functions, we do not really use this notation in practice. Now a function \( f \) from \( X \) to \( Y \) is a relation, where the left-hand things are in \( X \) and the right-hand things are in \( Y \) so that for every element \( x \) of \( X \) there is a unique element of \( Y \) which is \( f \)-related to \( x \).

So what is a relation anyway?

1.4 A relation is a set

Well, it is nothing more than describing a pair of things, each having a left-hand one and a right-hand one. The key devise in making this idea concrete is the notion of the Cartesian product of two sets. Given two sets \( A \) and \( B \), the Cartesian product of \( A \) and \( B \) is the set of all (ordered) pairs \( (a, b) \) with \( a \in A \) and \( b \in B \). We could write this set as

\[ A \times B := \{(a, b) : a \in A, b \in B\}. \]

1 What is a rule?

2 When we define an object, we will use the symbol \( := \). The symbol \( = \) is reserved as a relation comparing pairs of objects.

3 By “infix notation” we mean that the symbol of interest goes between its arguments. So when we write that two things \( x \) and \( y \) are equal, we demonstrate this by \( x = y \).

4 A more formal definition will come later.

5 One of the axioms of Zermelo-Fraenkel Set Theory, the most accepted set of axioms for the fundamentals of mathematics, is called the Axiom of Pairing which allows us to ‘make’ cartesian products of sets. In other words, making pairs is one of the things in mathematics that is necessary to establish as a fundamental construct, and that it does not arise by any simpler construct.
1.5 An aside: naïve set theory

We have come to accept defining sets by a property (or for a fancier word, *predicate*). So for example,

\[ \{ x \in \mathbb{R} : x^2 + 3x + 1 = 0 \} . \]

This set consists of two elements \(-\frac{3}{2} + \sqrt{\frac{5}{2}}\) and \(-\frac{3}{2} - \sqrt{\frac{5}{2}}\), and it might be a different set if we allow \(x\) to be more than a real number (like matrices, for example). But does it make sense to define a set of all sets of size 10?

\[ \{ A : |A| = 10 \} . \]

Note that we have dropped any requirement that \(A\) live in a *universe* of some kind. This can have strange consequences, especially when we allow the ‘set of all sets’ to be a set.

**Example 1.5.1** (The set of non-penguins). *Let \( S \) be the set of all things which are not penguins. Since \( S \) is not a penguin, it is an element of itself:*

\[ S \in S . \]

So we see here an example of a set that is a *member* of itself!

**Example 1.5.2** (The barber paradox). *In a village, there is a male barber who shaves only those men who do not shave themselves. Who shaves the barber?*

**1.5.1 Russell’s paradox**

As we saw in Example 1.5.1, a set can be a *member* of itself; that’s right, a *member* of itself! Bertrand Russell initiated a paradox which shocked the logicians of his time (1901), and it is similar to the barber paradox (Example 1.5.2).\(^7\)

**Example 1.5.3** (Russell’s paradox). *Let \( \mathcal{A} \) be the set of all sets \( S \) such that \( S \notin S \).*

*Is \( \mathcal{A} \) a member of itself?*

If \( \mathcal{A} \) is a member of itself, it would contradict its own definition as a set containing all sets that are not members of themselves. On the other hand, if \( \mathcal{A} \) is not a member of itself, it would satisfy its predicate and hence be a member of itself!

1.6 How to start writing proofs

Mathematics is arguably one of the oldest intellectual disciplines, and since at least antiquity, a part of the doing of mathematics has been establishing truths and collating them into theorems, lemmas and the like. A theorem is a true mathematical statement and its proof relies on established valid statements. Of course, we have to start somewhere, which we alluded to in the previous section on a discussion on the philosophical underpinnings of mathematics. For the student, proofs can be difficult and take some time to
get used to. Some of the fun of doing a proof comes from the completion of a water-tight and elegant proof. However, for most of the formative period, proofs can be frustrating and not enjoyable at all. So we will keep things simple. For at least half of this course we will throw away what I believe is one of the greatest inhibitions to the enjoyment of proofs: the syntax. Syntax, though important in writing clear and elegant proofs, can take a while to master. It often inhibits the new learner in understanding how a proof works and how to recognise whether it is correct or not. In particular, the emphasis early in one’s learning ought to be focussed on the logic of a proof, not whether the right expression was used in conveying an inference or deduction.

1.6.1 Restricted syntax

We will just use one method for doing proofs before embarking on writing out proofs with flair and poetic english language. After we have become comfortable with the structure of a proof, we will then flavour them by introducing more variety into the syntax.

<table>
<thead>
<tr>
<th>Temporary rules:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Only use “Suppose” for initialising statements like “Assume ...”, “Let ..”.</td>
</tr>
<tr>
<td>• Only use “Then” for logical connections like “Hence”, “Thus”, “So”.</td>
</tr>
<tr>
<td>• You can use “Choose ...” if you need to show that something exists.</td>
</tr>
<tr>
<td>• Give a reason for every logical deduction, no matter how trivial it is.</td>
</tr>
<tr>
<td>• Conclude the proof with “Therefore, ...”.</td>
</tr>
</tbody>
</table>

**Example 1.6.1.** We will prove that the sum of two odd numbers is an even number.

**Definitions that you’ll need:**

- An odd number is an integer of the form $2n + 1$ for some integer $n$.
- An even number is an integer of the form $2n$ for some integer $n$.

- **Proof (Restricted Syntax).** Suppose $x$ and $y$ are odd numbers.
  
  Then there are integers $m$, $n$ such that $x = 2n + 1$ and $y = 2m + 1$ 
  Then $x + y = (2n + 1) + (2m + 1)$ 
  Then $x + y = 2n + 2m + 2$ 
  Then $x + y = 2(n + m + 1)$ 
  Then $x + y$ is an even number 
  Therefore, the sum of two odd numbers is an even number. □

Joy and David Morris (University of Lethbridge, Canada) have a similar technique for teaching proofs called “two-column proofs”.

1.7 Cardinality fundamentals

First we return to the definition of a function.

**Definition 1.7.1 (Function).** Let \( A \) and \( B \) be sets and let \( f \) be a subset of \( A \times B \) (i.e., \( f \) is a relation). We say that \( f \) is a function if for every element \( a \in A \), there is a unique element \( b \in B \) such that \((a, b) \in f\). The domain of \( f \) is \( A \), the codomain of \( f \) is \( B \) and the image of \( f \) is

\[
\text{image of } f = f(A) := \{f(a) : a \in A\}.
\]

So a function consists of **three** objects: a domain \( A \), a codomain \( B \), and a relation \( f \).

1.7.1 Kidney diagram of a function

One way to abstractly visualise the definition of a function is by a **kidney diagram**:

![Kidney Diagram](image1.jpg)

Figure 1.1: This diagram depicts what **cannot** happen in the definition of a function.

1.7.2 Special kinds of functions

**Definition 1.7.2 (One-to-one (injective)).** A function \( f \) from \( A \) to \( B \) is one-to-one if for each element of \( b \in B \), there is at most one element \( a \in A \) such that \( f(a) = b \).

**Example 1.7.3.**

- The function \( f \) defined by \( f(x) = x^2 \) is not one-to-one since \( f(-1) = f(1) \) but \( -1 \neq 1 \).
- The identity function on a set \( X \) is one-to-one since for all \( y \in X \), there is just one element, namely itself, that is mapped to \( y \) by the identity function.
- The “blood type” function is not one-to-one.
- Pictorially, a function \( f \) on the reals is one-to-one if every horizontal line drawn on the graph of \( f \) intersects the values of \( f \) at most once. You should picture “\( f(x) = x^2 \)” and imagine drawing horizontal lines on the graph.

In some texts, the word **range** is used instead of image. According to the Oxford English Dictionary, the earliest specific use of the term range (of a function) is found in 1914 in A. R. Forsyth’s, “Theory of Functions of Two Complex Variables”. The term image can be used for the output of a single element under a function.

Equivalently: A function \( f \) from \( A \) to \( B \) is one-to-one if for all \( a_1, a_2 \in A \) such that \( a_1 \neq a_2 \), we have \( f(a_1) \neq f(a_2) \).

The blood-type function has domain the set of all people, and codomain \( \{A, B, AB, O\} \). Never mind the rhesus for this example!
To prove a function \( f : X \rightarrow Y \) is one-to-one:

Suppose \( f(x_1) = f(x_2) \) for some \( x_1, x_2 \in X \). Show that \( x_1 = x_2 \).

**Example 1.7.4.** Show that the function \( f : \mathbb{R}\{0\} \rightarrow \mathbb{R}^+ \) defined by

\[
  f(x) = \sqrt{x + 1}
\]

for all \( x \in \mathbb{R}\{0\} \), is one-to-one.

○ Proof (Restricted Syntax).

Suppose \( x_1, x_2 \in \mathbb{R}\{0\} \) and \( f(x_1) = f(x_2) \).

Then \( \sqrt{x_1 + 1} = \sqrt{x_2 + 1} \) by definition of \( f \).

Then \( x_1 + 1 = x_2 + 1 \) by squaring each side.

Then \( x_1 = x_2 \) by subtracting 1 from each side.

Therefore, \( f \) is one-to-one. \( \square \)

**Definition 1.7.5** (Onto (surjective)). A function \( f : X \rightarrow Y \) is onto, if for each element \( y \in Y \), there is at least one element \( x \in X \) such that \( f(x) = y \). Equivalently: A function \( f : X \rightarrow Y \) is onto if the image \( f(X) \) equals the entire set \( Y \).

**Example 1.7.6.**
• The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ (for all $x \in \mathbb{R}$) is not onto since no element maps to $-1$ under $f$. If however we restricted the definition of $f$ by defining $f : \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$, then it would be onto.

• The “blood-type” function is onto, since for every blood type, there is at least one person in the world who has that blood type.

To prove a function $f : X \to Y$ is onto:

Let $y$ be an element of $Y$. Find an element $x \in X$ such that $f(x) = y$.

Example 1.7.7. Show that the function $f : \mathbb{R}\setminus\{0\} \to [1, \infty)$ defined by $f(x) = \sqrt{x + 1}$ for all $x \in \mathbb{R}\setminus\{0\}$, is onto.

Proof (Restricted Syntax). Suppose $y \in [1, \infty)$.

Choose $x = y^2 - 1$.

Then $f(x) = \sqrt{x + 1}$

Then $f(x) = \sqrt{y^2 - 1 + 1}$

Then $f(x) = \sqrt{y^2}$

Then $f(x) = y$

Therefore, $f$ is onto. □

Remark 1.7.8. In the above proof, the step “Choose $x = y^2 - 1$” was only possible after doing some work on the back of an envelope first. I worked backwards to find an element $x \in \mathbb{R}\setminus\{0\}$ such that $f(x) = y$, and then wrote my proof in the logically correct direction!

1.7.3 Counting

Counting is one of the most central ideas of mathematics, and it wasn’t until Cantor’s work in the 19th century that we began to understand fully what it means to count. To say that one set has more elements then another is a trivial problem in the finite context, but what about infinite sets? Are there more integers than even numbers? What Cantor realised, is that counting can be thought of as pairing elements in a unique and exhaustive way. For example, we can pair up the integers and even numbers in the following way:

$$\ldots, (−6, −3), (−4, −2), (−2, −1), (0, 0), (2, 1), (4, 2), (6, 3), \ldots$$

You can see here that every even number will appear in the first coordinate in precisely one of these pairs and every integer will appear in the second coordinate in just one of these pairs. So what we require is that there is a function from the even numbers to the integers that is one-to-one and onto. We call this a bijection.

Definition 1.7.9 (Bijection). A function is bijective if it is both one-to-one and onto.

The function $f$ from the even numbers to the integers defined by $f(x) = x/2$ is a bijection. So essentially, we think of the integers and even numbers as having the same amount of elements.
Definition 1.7.10 (Equinumerous sets and cardinality). Two sets $X$ and $Y$ are equinumerous, or have the same size/cardinality, if there exists a bijection from $X$ to $Y$. We can express this symbolically as $A \approx B$ or simply $|A| = |B|$.

Example 1.7.11. The unit interval $(0,1)$ and $\mathbb{R}$ are equinumerous, as we shall see. Consider the following function $f : \mathbb{R} \to (0,1)$:

$$f(x) := \frac{1}{\pi} \arctan(x) + \frac{1}{2}.$$  

It can be shown that $f$ is one-to-one and onto, and so $\mathbb{R}$ and $(0,1)$ have the same size!

To prove two functions $f : X \to Y$ and $g : X \to Y$ are equal:

Let $x \in X$. Show that $f(x) = g(x)$. A common mistake made by students is that they prove that two functions are equal for a specific element of $X$. You must prove that they compute the same value for EVERY element of the domain!

1.7.4 Composition of functions

In algebra, we often want to create new things from old things. In this section, we look at a way of creating a function from two old ones. This operation is called function composition.

Definition 1.7.12 (Function Composition). Let $g$ be a function from a set $A$ to a set $B$ and let $f$ be a function from a set $B$ to a set $C$. Then the composition of $f$ and $g$, denoted $f \circ g$, is the function defined by $(f \circ g)(a) = f(g(a))$ for all $a \in A$.

Example 1.7.13.

- The function $h$ defined by $h(x) = \sin^2(x)$ (for all $x \in \mathbb{R}$) is the composition of the two functions $f$ and $g$ defined by $f(x) = x^2$ and $g(x) = \sin(x)$. So $h = f \circ g$. Note that $g \circ f$ is a completely different function which maps an element $x \in \mathbb{R}$ to $\sin(x^2)$.

- Let $X$ and $Y$ be sets and let $f : X \to Y$ be a function. Then $f \circ \text{id}_X = f$ and $\text{id}_Y \circ f = f$ where $\text{id}_X$ and $\text{id}_Y$ are the identity functions on $X$ and $Y$, respectively.

- Let $\mathbb{R}^+$ denote the positive real numbers, and let $f : \mathbb{R}^+ \to \mathbb{R}^+$ be defined by $f(x) = x^2$ (for all $x \in \mathbb{R}^+$). Let $g : \mathbb{R}^+ \to \mathbb{R}^+$ be defined by $g(y) = \sqrt{y}$ (for all $y \in \mathbb{R}^+$). Then $f \circ g = \text{id}_{\mathbb{R}^+}$ and $g \circ f = \text{id}_{\mathbb{R}^+}$.

1.7.5 Images and inverses

Modern mathematics and its language have evolved into a reasonably stable and uniform state. The words “one-to-one”, “onto”, and “real number” are universally understood. We present here some more notions that are fundamental to the communication of mathematics.
Definition 1.7.14 (Image). Let \( f \) be a function from a set \( X \) into a set \( Y \), and let \( A \subseteq X \). The image \( f(A) \) of \( A \) under \( f \) is the subset
\[
\{ f(a) : a \in A \}
\]
of \( Y \).

Definition 1.7.15 (Preimage). Let \( f \) be a function from a set \( X \) into a set \( Y \), and let \( S \subseteq Y \). Then the preimage of \( S \) under \( f \) is the subset of \( X \) defined by
\[
f^{-1}(S) := \{ x \in X : f(x) \in S \}.
\]

Example 1.7.16. Consider the sine function \( \sin : \mathbb{R} \to \mathbb{R} \). The image of \( \mathbb{R} \) under this function is \( \sin(\mathbb{R}) = [-1, 1] \). The preimage of \( \{0\} \) under sine is the set
\[
\sin^{-1}(\{0\}) = \{ x \in \mathbb{R} : \sin(x) = 0 \} = \{ \pi x : x \in \mathbb{Z} \}.
\]

Definition 1.7.17 (Invertibility). A function \( f : X \to Y \) is said to be invertible if there exists a function \( g : Y \to X \) such that \( f \circ g = \text{id}_Y \) and \( g \circ f = \text{id}_X \). If such a \( g \) exists, we call it the inverse of \( f \), and denote it by \( f^{-1} \).

In order for the notation \( f^{-1} \) to make sense, there has to be just one inverse of an invertible function. We will assume without proof that the operation of function composition is associative\(^9\).

Lemma 1.7.18. Suppose a function \( f : X \to Y \) is invertible. Then there is a unique inverse of \( f \).

Proof (restricted syntax): Suppose there are two inverses \( g : Y \to X \) and \( h : Y \to X \) for \( f \). We will show that \( h = g \).

Then \( h \circ (f \circ g) = (h \circ f) \circ g \)

Then \( h \circ \text{id}_Y = \text{id}_X \circ g \)

Then \( h = g \)

Therefore, \( f \) has a unique inverse. \( \square \)

Example 1.7.19.
• The squaring function from $\mathbb{R}$ to $\mathbb{R}$ is not invertible. However the squaring function on $\mathbb{R}^+$ is invertible!

• The inverse of the identity function is itself, since for any set $X$, $id_X \circ id_X = id_X$.

**Theorem 1.7.20.** A function $f : X \to Y$ is invertible if and only if it is bijective.

⋄ Proof: See the exercises at the end of the chapter. □

1.7.6 The Issue of “Well-Defined”

It is a common trait of mathematicians to “define” a function before actually proving that it is a function. Ideally, we should define a set, show it is a binary relation, and then show it is a function. As you can imagine, this can be quite a cumbersome task in most situations. So mathematicians have become accustomed to writing functions down before verifying that they are indeed functions. When we prove that a binary relation is a binary relation or a function is a function, we say that the object in question is “well-defined”. Not until now have you needed to deal with this issue, but you will find, especially when defining functions with a partition as their domain, that you must take a minute to prove that what you’ve claimed is a function actually is!

**Example 1.7.21.** “Let $f(x) : \mathbb{Q} \to \mathbb{Z}$ be the function defined by $f(q) = a$ where $a$ is the numerator of $q$.”

This is BAD! What we’ve written is not a function, since $f(1/2) = 1$ and $f(2/4) = 2$ but $1/2 \neq 2/4$. We will see in Section 3.4 that the rational numbers are like a partition of $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, and so we must be extra careful when defining functions when there is an equivalence relation hanging about! More of this issue will appear later when we study equivalence relations in Section 3.3.

1.8 Countable and uncountable

Before we saw that the set of even numbers has the same size as the entire set of numbers, and to see this, we showed that there was a bijection between these two sets. If we can embed a set $S$ inside the natural numbers, like we did for even numbers, then we say that $S$ is countable\(^\text{10}\).

**Definition 1.8.1 (Countability).** A set $X$ is countable if there is a one-to-one function $f : X \to \mathbb{N}$. A set is uncountable if it is not countable.

**Lemma 1.8.2.** Every finite set is countable.

⋄ Proof: Let $S$ be a finite set of size $n$. Then we can list the elements as follows:

$$S = \{s_1, s_2, \ldots, s_n\}.$$  

Let $f : S \to \mathbb{N}$ be defined by $f(s_i) := i$. We will show that $f$ is one-to-one. Suppose $f(x) = f(y)$ for two elements $x$ and $y$ of $S$. Then there exist $i, j \in \{1, 2, \ldots, n\}$ such that $x = s_i$ and $y = s_j$. Therefore $f(s_i) = f(s_j)$ and hence $i = j$. So $s_i = s_j$ and $f$ is one-to-one. □

\(^{10}\) We will use a definition that includes finite sets, which differs from some texts such as Martin Liebeck’s book “A concise introduction to pure mathematics”.

Lemma 1.8.3. The set of integers is countable.

★ Sketch: Define the following function $f$ from $\mathbb{N}$ to $\mathbb{Z}$:

$$f(n) := \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n+1}{2} & \text{otherwise} \end{cases}$$

It turns out (exercise!) that $f$ is a bijection. □

Theorem 1.8.4. A countable union of countable sets is countable.

★ Proof: See lectures. □

Theorem 1.8.5. The positive rational numbers are countable.

★ Proof: The main part of the proof is Cantor’s “zigzag” argument:

The rest will be done in lectures. □

Corollary 1.8.6. The rational numbers are countable.

● Proof: The map $f(x) := -x$ is a bijection from $\mathbb{Q}^+$ to $\mathbb{Q}^-$ (exercise) and so by Theorem 1.8.5, $\mathbb{Q}^-$ is countable. The singleton set $\{0\}$ is countable by Lemma 1.8.2, and so by Theorem 1.8.4, $\mathbb{Q}^- \cup \{0\} \cup \mathbb{Q}^+$ is countable. Therefore, $\mathbb{Q}$ is countable. □

1.9 Diagonal arguments as two-person games

Here is a (silly) game we could play that would take a long time to complete. I give you a rational number in the interval $(0, 1)$, and then you give me a different rational number in this interval. Then we continue turn by turn, writing down rational numbers in $(0, 1)$ that we have not mentioned in earlier turns. The person who cannot think of a new rational number or repeats one that has already been said, loses.

Question 1.9.1. Is there a non-losing strategy for one of the players?

The answer is of course yes, but the most elegant answer is to use a diagonal argument. Here’s how it works. Suppose the following ten moves have been made in the game, accurate to ten decimal places:
Now look along the diagonal, after the decimal point. If the number is not equal to 3, then write down next to the row the number 3. Otherwise, write “7”.

Table: 

<table>
<thead>
<tr>
<th>Number</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0125000000</td>
<td>3</td>
</tr>
<tr>
<td>0.1000000000</td>
<td>3</td>
</tr>
<tr>
<td>0.3467891023</td>
<td>3</td>
</tr>
<tr>
<td>0.0041200340</td>
<td>3</td>
</tr>
<tr>
<td>0.9654102948</td>
<td>7</td>
</tr>
<tr>
<td>0.8475839102</td>
<td>7</td>
</tr>
<tr>
<td>0.0194857291</td>
<td>3</td>
</tr>
<tr>
<td>0.3240580293</td>
<td>3</td>
</tr>
<tr>
<td>0.3333333333</td>
<td>7</td>
</tr>
<tr>
<td>0.2121212121</td>
<td>3</td>
</tr>
</tbody>
</table>

Then the new number 0.3333373373 must differ from the first number in the first place, from the second number in the second place, and so on! So we are guaranteed of obtaining a new number!

We can use this argument to show that the real numbers cannot be placed in bijection with the natural numbers.

**Theorem 1.9.2.** The real numbers are uncountable.

**Proof:** Done in lectures. □

Why does this argument not work for rational numbers? Well, the diagonal argument does not produce a rational number since the decimal expression would be forced to be non-periodic.

**Corollary 1.9.3.** The irrational numbers are uncountable.

**Proof:** This is a simple proof by contradiction. Suppose that the irrational numbers \( \mathbb{R} \setminus \mathbb{Q} \) were uncountable. Then by Theorem 1.8.4, \( (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q} \) would be countable. This is a contradiction, since \( (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q} = \mathbb{R} \) and \( \mathbb{R} \) is uncountable by Theorem 1.9.2. Therefore, the irrational numbers are uncountable. □

### 1.9.1 Ordering cardinalities

**Definition 1.9.4.** Let \( A \) and \( B \) be sets. If there exists a one-to-one function from \( A \) to \( B \), we say that \( B \) is at least as numerous as \( A \), and write \( A \preceq B \). If \( A \) and \( B \) are not equinumerous, and \( A \preceq B \), then we write \( A < B \).
Example 1.9.5. So \(\{1, 2, 3\} \prec \{1, 2, 3, 4\}\). How about a more interesting example? Suppose we take the set \(\{1, 2, 3, 4\}\). Now consider all of its subsets:

\[\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 3, 4\}, \{1, 2, 4\}, \{1, 2, 3, 4\}\.

Notice that this set is bigger than \(\{1, 2, 3, 4\}\). We will see that this is also true for infinite sets.

Lemma 1.9.6. Let \(A, B,\) and \(C\) be sets.

(i) If \(A \subseteq B\), then \(A \preceq B\).

(ii) If \(A \preceq B\) and \(B \preceq C\), then \(A \preceq C\).

(iii) \(A \preceq B\) or \(B \preceq A\).

\(\blacksquare\)

Definition 1.9.7. Given a set \(S\) and a subset \(A\) of \(S\), the characteristic function of \(A\) with respect to \(S\) is the map \(\chi_A\) defined by

\[
\chi_A(x) := \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}
\]

The lemma above shows that \(\leq\) is what is known as a partial order (which we do not cover in this course).

Definition 1.9.8 (Power set). For a set \(A\), the power set \(\mathcal{P}(A)\) of \(A\) is the set of all subsets of \(A\). We must be sure that we do not allow the “set of all sets” to be a set here.

Theorem 1.9.9. For any set \(A\), we have \(A \prec \mathcal{P}(A)\).

\(\star\) Proof: First we show that \(A \preceq \mathcal{P}(A)\), and then we will show that \(|A| \neq |\mathcal{P}(A)|\). Let \(f : A \to \mathcal{P}(A)\) be the function defined by

\[
f(a) := \{a\}.
\]
We will show that \( f \) is one-to-one. Suppose \( a, a' \in A \) and \( f(a) = f(a') \). Then \( \{a\} = \{a'\} \), from which it directly follows that \( a = a' \). Therefore, \( f \) is one-to-one and we have shown that \( A \preceq \mathcal{P}(A) \).

Suppose there is a function \( f : A \to \mathcal{P}(A) \). We will show, by contradiction, that \( f \) cannot be onto. So suppose \( f \) is onto. Let

\[
X = \{a \in A : a \notin f(a)\}.
\]

Notice that \( X \) is a subset of \( A \), that is, \( X \in \mathcal{P}(A) \), and so there exists \( a \in A \) such that \( f(a) = X \). Does \( a \in X \) or not? If \( a \in X \), then \( a \notin f(a) \), but \( f(a) = X \); a contradiction. If \( a \notin X \), then \( a \in f(a) \), but again \( f(a) = X \); another contradiction! So \( f \) cannot be onto. \( \square \)

The above proof is actually a “diagonal argument” in disguise. Imagine \( A \) was countable, so that we could actually list its elements. Now consider an array where the elements of \( A \) represent the columns, and the elements of \( \mathcal{P}(A) \) represent the rows. We put a \( T \) for true if the element \( a_i \) of \( A \) belongs to the subset \( A_j \) of \( A \), and a \( F \) (for ‘false’) otherwise. It would look something like this:

\[
\begin{array}{cccccccc}
A & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \ldots \\
\hline
A_1 & T & T & F & T & T & F & F & \ldots \\
A_2 & F & F & T & F & T & T & F & \ldots \\
A_3 & T & F & F & F & T & F & T & \ldots \\
A_4 & T & T & F & T & T & F & F & \ldots \\
A_5 & F & F & F & F & T & F & F & \ldots \\
A_6 & F & F & F & F & F & F & T & \ldots \\
A_7 & F & T & T & F & F & F & F & \ldots \\
\vdots & & & & & & & & \\
\end{array}
\]

The set \( X \) we chose in the proof is what you get when you ‘flip’ the truth values along the diagonal of this array.

\[
\begin{array}{cccccccc}
A & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & \ldots & X \\
\hline
A_1 & T & T & F & T & T & F & F & \ldots & T \\
A_2 & F & F & T & F & T & T & F & \ldots & T \\
A_3 & T & F & F & F & T & F & T & \ldots & T \\
A_4 & T & T & F & T & F & F & F & \ldots & T \\
A_5 & F & F & F & F & T & F & F & \ldots & T \\
A_6 & F & F & F & F & F & F & T & \ldots & T \\
A_7 & F & T & T & F & F & F & F & \ldots & T \\
\vdots & & & & & & & & & \\
\end{array}
\]

Theorem 1.9.10 (Cantor-Berstein-Schröder Theorem). Let \( A \) and \( B \) be two sets. If \( A \preceq B \) and \( B \preceq A \), then \( A \approx B \).

† Proof: A sketch of the proof might be done in lectures (if there is sufficient time). \( \square \)

Theorem 1.9.11. The real numbers and \( \mathcal{P}(\mathbb{N}) \) are equinumerous.
Proof: First we show that \( \mathcal{P}(\mathbb{N}) \preceq \mathbb{R} \). Let \( X \subseteq \mathbb{N} \). Define the real number \( r_X \) by

\[
0.a_1a_2a_3a_4 \ldots
\]

where

\[
a_i := \begin{cases} 
1 & \text{if } i \in X \\
0 & \text{otherwise.} 
\end{cases}
\]

Let \( f : \mathcal{P}(\mathbb{N}) \to \mathbb{R} \) be the function \( X \to r_X \). We will show that \( f \) is one-to-one. Suppose \( X, X' \) are subsets of \( \mathbb{N} \) and \( f(X) = f(X') \). Then \( r_X = r_{X'} \) where \( r_X = 0.a_1a_2a_3a_4 \ldots \) and \( r_{X'} = 0.a'_1a'_2a'_3a'_4 \ldots \) So each \( a_i \) is equal to the corresponding \( a'_i \), and hence \( i \in X \) if and only if \( i \in X' \) (by definition of \( a_i \) and \( a'_i \)). Therefore, \( X = X' \) and \( f \) is one-to-one.

Now we show that \( \mathbb{R} \preceq \mathcal{P}(\mathbb{N}) \). We will use the fact from (reference) that \( \mathbb{R} \approx (0, 1) \) (the unit open interval). Given \( r \in (0, 1) \) written in decimal form \( r = 0.r_1r_2r_3r_4 \ldots \), let \( X_r \) be the set

\[
\{ r_1, r_2 + 10, r_3 + 100, r_4 + 1000, \ldots \}.
\]

Then \( X_r \) is a subset of \( \mathbb{N} \) and no two elements are equal as written above. So let \( g : (0, 1) \to \mathcal{P}(\mathbb{N}) \) be defined by \( g(r) := X_r \). We will leave it as a (simple) exercise for the reader to show that \( g \) is one-to-one. So \( (0, 1) \preceq \mathcal{P}(\mathbb{N}) \), and so by the Cantor-Berstein-Schöder Theorem 1.9.10, \( (0, 1) \approx \mathcal{P}(\mathbb{N}) \). Therefore, since the composition of two bijections is a bijection (see Exercise 1.11.10), we have \( \mathbb{R} \approx \mathcal{P}(\mathbb{N}) \). \( \Box \)

1.9.2 Aside: The Continuum Hypothesis

We have shown above that \( \mathbb{N} \preceq \mathbb{R} \) (see Theorems 1.9.9 and 1.9.11), but is there a set which has size in-between countable and the continuum?\(^{12}\)

The Continuum Hypothesis: Every uncountable subset of the real numbers is equinumerous to the real numbers.

The search for a proof of this statement baffled mathematicians in the first half of the 20th century, and indeed, it was David Hilbert’s first of 23 open problems presented at the 1900 International Congress of Mathematicians. Kurt Gödel in 1940 and Paul Cohen in 1963 showed that the hypothesis can neither be proved nor be disproved using the axioms of Zermelo-Fraenkel set theory, the standard foundation of modern mathematics.

1.10 Aside: What is a number?

There are a number of approaches to formalising the idea of a number, but the one we will briefly go over here is the system introduced by Giuseppe Peano.

Definition 1.10.1 (Peano’s Axioms). There is a set \( \mathbb{N} \) satisfying the following conditions:

1. There is an element called 1 that belongs to \( \mathbb{N} \).
2. There is a function \( S : \mathbb{N} \to \mathbb{N} \), called the “successor function”.

\(^{11}\) This is just the characteristic function for \( X \) written as decimal points behind 0.

\(^{12}\) The continuum is an informal expression in mathematics to express the cardinality of the real numbers.

\(^{13}\) posed by Georg Cantor in 1878
3. For every $x \in \mathbb{N}$, we have $S(x) \neq 1$.

4. $S$ is one-to-one.

5. **Induction:** If $R$ is a subset of $\mathbb{N}$ such that

   (a) $1 \in R$, and

   (b) $x \in R \implies S(x) \in R$,

then $R = \mathbb{N}$.

This definition of $\mathbb{N}$ seems at first to be extremely abstract, but it captures the properties of $\mathbb{N}$ beautifully. For example, these axioms imply the **Well-ordering Principle** of the natural numbers, that every nonempty subset of $\mathbb{N}$ has a least element. The meta-mathematics behind a seemingly innocuous statement is beyond the scope of this course, though you may be surprised if you see if such a statement can be proved for the real numbers!

So is there a set $\mathbb{N}$ with these properties? Here is the well-known example introduced by John Von Neumann that models the properties of $\mathbb{N} \cup \{0\}$, starting only with the empty set.\(^\text{14}\)

- We start with defining 0 to be the empty set $\emptyset$.
- Then 1 is defined to be the set containing 0, that is, $1 := \{\emptyset\}$.
- Then 2 is defined to be the set containing 0 and 1, that is, $2 := \{\emptyset, \emptyset\}$.
- So we have a successor function $S(x) := x \cup \{x\}$.

Addition on $\mathbb{N}$ is then defined inductively:

(i) $x + 1 := S(x)$

(ii) $x + S(y) := S(x + y)$.

As an exercise, you may like to think of how multiplication would be defined . . .

### 1.11 Exercises

**Exercise 1.11.1.** In Google, the three operations of Boolean logic work like this:

```
AND  Whitespace between terms, e.g., "Review" "High School Musical".
OR   Use the word OR, e.g., "Burma" OR "Myanmar".
NOT  Use the minus symbol -, e.g., "Poffertjes recipe" -"sour cream"
```

You can also use brackets to group clauses, and AND has natural precedence over OR.

(a) Give an example of a Google expression which creates a search for

"Madonna" or "Justin Timberlake", but not both.
(b) Write a Google expression with the terms "drink coffee" and "less likely to develop dementia" which represents the following implication:

“If you drink coffee, then you are less likely to develop dementia.”

Exercise 1.11.2 (Quantifiers). For each of the following sentences, rewrite the statement making all the quantifiers\(^{15}\) explicit. Then form the negation of the statement, and convert it back to English.

(a) The skies are not cloudy all day.

(b) The sun never sets on the British Empire.

(c) Every positive integer has a unique prime factorisation.

(d) There is no largest prime.

Exercise 1.11.3. Suppose \(A\) and \(B\) are sets. Give your answers in the notation of logic (not English).

(a) What does it mean to say that \(A\) is a subset of \(B\)?

(b) What does it mean to say that \(A\) is not a subset of \(B\)?

Exercise 1.11.4. Let \(f : \mathbb{Z} \rightarrow \mathbb{Z}\) be the function defined by

\[
f(x) := 3x + 1 \pmod{5}
\]

What is the preimage of 4 under \(f\)?)

Exercise 1.11.5. What can you say about \(f : A \rightarrow B\) if the preimage of every singleton subset \(\{b\}\) of \(B\) is nonempty?

Exercise 1.11.6. Let \(f : A \rightarrow B\) be a function, let \(A' \subseteq A\) and let \(B' \subseteq B\).

1. Show that if \(f\) is one-to-one, then \(f^{-1}(f(A')) = A'\).

2. Show that if \(f\) is onto, then \(f(f^{-1}(B')) = B'\).

Exercise 1.11.7. What can you say about \(f : A \rightarrow B\) if the preimage of every singleton subset \(\{b\}\) of \(B\) is a singleton subset of \(A\)?

Exercise 1.11.8. Prove that a function \(f : A \rightarrow B\) is a bijection if and only if it is invertible (i.e., there exists a function \(g : B \rightarrow A\) such that \(f \circ g = \text{id}_B\) and \(g \circ f = \text{id}_A\)).

Exercise 1.11.9. Let \(f : A \rightarrow B\) be a function and let \(B_1\) and \(B_2\) be subsets of \(B\).

1. Show that \(f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)\).

2. Show that \(f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)\).
Exercise 1.11.10. Let $f : A \to B$ and $g : B \to C$ be functions.

(i) Show that if $f$ and $g$ are one-to-one, then $g \circ f$ is one-to-one.

(ii) Show that if $f$ and $g$ are onto, then $g \circ f$ is onto.

(iii) Show that if $g \circ f$ is one-to-one and $f$ is onto, then $g$ is one-to-one.

(iv) Show that if $g \circ f$ is onto and $f$ is one-to-one, then $f$ is onto.

(v) Let $A = C$. Show that if $g \circ f = \text{id}_A$, then $f$ is one-to-one.

(vi) Let $A = C$. Show that if $f \circ g = \text{id}_B$, then $f$ is onto.

Exercise 1.11.11. Let $A$ and $B$ be countable sets. Show that $A \times B$ is countable. In particular, show that $C$ is uncountable.

Exercise 1.11.12 (Hard). Let $A$ and $B$ be sets. Show that $A \preceq B$ or $B \preceq A$.

Exercise 1.11.13. Prove that if $A$ is an infinite set, then $\mathbb{N} \preceq A$. 
2

From numbers to rings

This chapter covers elementary number theory and its analogues in the general theory of rings. We first look at the “Division Rule” for the integers, the greatest common divisor of two numbers, and the Euclidean Algorithm. We then look at the prime numbers, the atoms of the integers. This basic number theory leads to a fundamental number system in abstract algebra, the integers modulo $m$, otherwise known as “clock-arithmetic”.

2.1 Divisibility

Let $x$ and $y$ be two integers. We say that $x$ divides $y$ if there exists another integer $q$ such that

$$y = qx.$$ 

We use the “long bar” notation to denote this relation:

$$x | y.$$ 

From this definition of divisibility we note the following things:

- Any integer $x$ divides 0 since $0 = 0 \cdot x$.
- The number 1 divides any nonzero integer and an integer $x$ divides itself, both because $x = 1 \cdot x$.
- If $a$ and $b$ are positive integers and $a | b$, then\(^2\) $a \leq b$.

**Example 2.1.1** (A lattice of numbers). We can see how the divisibility relation works by drawing a Hasse diagram that displays how the positive divisors of 24 relate to one another.

\(^1\) Synonyms:
- $x$ divides $y$
- $y$ is a multiple of $x$
- $x$ is a factor of $y$

\(^2\) Mini-proof: Since $a | b$, there exists an integer $q$ such that $b = qa$. Now $a$ and $b$ are positive, so $q$ must be positive. So $q \geq 1$ and hence $b \geq 1 \cdot a$. □

A Hasse diagram is a diagram which represents a partially ordered set. Each element of the set is a vertex, and we draw a line segment between vertices $x$ and $y$ whenever $x$ is smaller than $y$ and there is no intermediate element of the set.
2.1.1 “Divides” is transitive

We didn’t point out that what makes the Hasse diagram so neat and tidy is that it is not necessary to put in lines where there are paths; for instance, we don’t need to draw a line between 2 and 12, because if $2 \mid 6$ and $6 \mid 12$ implies that $2 \mid 12$.

Lemma 2.1.2. Let $a$, $b$ and $c$ be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

$\Diamond$ Proof (Restricted Syntax). Suppose $a \mid b$ and $b \mid c$. Then there are integers $m, n$ such that $b = ma$ and $c = nb$.

Then $c = n(ma)$

Then $c = ka$ where $k = nm$

Then $a \mid c$

Therefore, if $a \mid b$ and $b \mid c$, then $a \mid c$. $\square$

Notice that in the above proof, the definition of “divides” had to be the first deduction we made since it was all that we knew, and we reapplied the definition of “divides” in the last deduction we made. So it is almost always true that a mathematician, when devising a proof, constantly reflects on the information known at each step, though being careful not to assume more than what is allowed. At the same time, the mathematician keeps an eye on the prize – the conclusion – and has a feeling of what the final steps need to be.

2.1.2 Ring-like properties of things you know

When we have a binary operation on a set, like addition, and it always produces elements in the same set, we say that the set is closed under this operation.

Example 2.1.3. The set of even numbers $2\mathbb{N}$ is closed under addition since if we add two even numbers, the result is an even number. However, the set of odd numbers is not closed under addition since $3 + 5 = 8$.

Here are some operations on some familiar sets and we summarise when the given set is closed under a particular operation.

<table>
<thead>
<tr>
<th></th>
<th>+</th>
<th>×</th>
<th>−</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2\mathbb{N}$</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>$\mathbb{N}$</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>$\mathbb{Z}$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$\mathbb{Q}$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$\mathbb{R}$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$n \times n$ matrices over $\mathbb{R}$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>invertible $n \times n$ matrices over $\mathbb{R}$</td>
<td>×</td>
<td>✓</td>
<td>×</td>
</tr>
</tbody>
</table>

Table 2.1: Closure and non-closure of some well-known binary operations.

In this course, we will look at other common number systems in mathematics. Some of the sets above (which ones?) have the property that every nonzero element has a multiplicative inverse. That is, we can divide by nonzero elements.
2.1.3 The Division Rule

Below is a very handy result in number theory, which is probably the most fundamental property of the integers. It does not work for the rational numbers or for the real numbers, but we will see later in the course that a similar property holds in other number systems.

**Lemma 2.1.4 (The Division Rule).** Let \( a \) be a positive integer and let \( b \) be an integer. Then there are unique integers \( q \) and \( r \) such that

\[
b = qa + r \quad \text{and} \quad 0 \leq r < a.
\]

⋆ Proof: To be done in lectures. □

We call \( q \) the quotient and \( r \) the remainder. Sometimes we write \( b \pmod{a} \) for the remainder. So for example, if \( a = 5 \) and \( b = 12 \), then \( b = 2a + 2 \) and there is no other way to write \( b \) in terms of \( a \) with the remainder \( r \) satisfying \( 0 \leq r < a \).

**Definition 2.1.5 (Greatest Common Divisor).**

The **greatest common divisor** of two nonzero integers \( x \) and \( y \) is the largest integer that divides both \( x \) and \( y \):

\[
\gcd(x, y) = \max\{i \in \mathbb{N} : i | x \text{ and } i | y\}.
\]

**Example 2.1.6.**

- The divisors of 8 are 1, 2, 4, 8 and the divisors of 20 are 1, 2, 4, 5, 10, 20. So \( \gcd(8, 20) = 4 \).

- \( \gcd(-12, 18) = 6 \).

- The gcd of two distinct primes is always 1.

One way to work out the gcd of 234 and 180, say, is to divide the smaller number into the larger one, take its remainder (which is 54) and then notice that \( \gcd(234, 180) = \gcd(54, 180) \). The next result is the basis for the next section.

**Lemma 2.1.7 (Behind Euclid’s Algorithm).** Let \( a \) and \( b \) be nonzero integers. If \( b = qa + r \) then \( \gcd(b, a) = \gcd(r, a) \).

⋆ Proof (restrictive syntax): Suppose \( d \) is a divisor of both \( a \) and \( b \).

\[
\text{Then } d \text{ divides } b - qa
\]

\[
\text{Then } d \text{ divides } r
\]

\[
\text{Then } d \text{ divides both } r \text{ and } a
\]

Therefore every divisor of both \( a \) and \( b \) is also a divisor of \( r \).

Conversely, suppose \( d \) is a divisor of both \( a \) and \( r \).

\[
\text{Then } d \text{ divides } qa + r
\]

\[
\text{Then } d \text{ divides } b
\]

Therefore every divisor of both \( a \) and \( r \) is also a divisor of \( b \).

\[
\text{Then } \{d \in \mathbb{N} : d \mid a \text{ and } d \mid b\} = \{d \in \mathbb{N} : d \mid a \text{ and } d \mid r\}
\]

Therefore, \( \gcd(b, a) = \gcd(r, a) \)

□
2.1.4 The Euclidean Algorithm in \( \mathbb{Z} \).

In this section we demonstrate a method for finding the gcd of two integers which is attributed to the school of Euclid\(^3\). We show by example the routine.

**Example 2.1.8.** To find the greatest common divisor of 234 and 180, perform the following steps.

(i) **Draw two columns**

(ii) **Write 234 and 180 in the right column, the largest 234 first.**

\[
\begin{array}{c|c}
234 & \\
180 & \\
\end{array}
\]

(iii) **Divide the smaller number 180 into the larger 234, and write the quotient in the left column adjacent to 180, and the remainder below 180.**

\[
\begin{array}{c|c|c}
234 & 180 & 54 \\
1 & 180 & \\
\end{array}
\]

(iv) **Now move down one row and repeat the last step over and over until we get a remainder of 0.**

\[
\begin{array}{c|c|c}
234 & 180 & 54 \\
1 & 180 & \\
3 & 54 & 18 \\
3 & 18 & \\
\end{array}
\]

(v) **The second-last number in the right column is the greatest common divisor of 180 and 234, namely 18.**

**Example 2.1.9.** Consider 558 and 423. Here is the table we get when we do the Euclidean Algorithm:

\[
\begin{array}{c|c|c|c}
558 & 423 & 135 & 9 \\
1 & 423 & 135 & 9 \\
3 & 135 & 18 & \\
7 & 18 & 9 & \\
\end{array}
\]

Then the last non-zero remainder is 9 so \( \text{gcd}(558, 423) = 9 \).

**Lemma 2.1.10** (Bézout’s identity). If \( a \) and \( b \) are nonzero, then there are integers \( m \) and \( n \) such that

\[ \text{gcd}(a,b) = ma + nb. \]

\( \blacklozenge \) **Proof:** Done in lectures. \( \square \)
In fact, Bézout’s identity almost says that the greatest common divisor of \(a\) and \(b\) is the smallest integer linear combination of \(a\) and \(b\). We fill in the details in what follows.

**Corollary 2.1.11.** Let \(a\) and \(b\) be two nonzero integers. Then an integer \(x\) can be expressed as \(ma + nb\) for two integers \(m\) and \(n\) if and only if \(\gcd(a, b)\) divides \(x\).

⋆ **Proof:** We do the “\(\implies\)” direction first. Suppose that \(x\) can be expressed as \(ma + nb\) for some integers \(m\) and \(n\). Let \(d\) be an integer that divides both \(a\) and \(b\). Then by transitivity of the divides relation (Lemma 2.1.2), \(d\) divides \(ma\) and \(d\) divides \(nb\). So \(d\) divides their sum, and hence \(d\) divides \(x\). Therefore, \(\gcd(a, b)\) must divide \(x\), since by definition, \(\gcd(a, b)\) divides both \(a\) and \(b\).

Now for the converse. Suppose \(\gcd(a, b)\) divides \(x\). So there is an integer \(c\) such that \(x = c \cdot \gcd(a, b)\). By Bézout’s identity (Lemma 2.1.10), there exist a pair of integers \(m'\) and \(n'\) such that
\[
\gcd(a, b) = m'a + n'b.
\]
Hence, \(x = (cm')a + (cn')b\) and the result follows by letting \(m = cm'\) and \(n = cn'\). \(\square\)

**Example 2.1.12.** In Example 2.1.9, we showed that \(\gcd(558, 423) = 9\), and Bézout’s identity says that we can express 9 as an integer linear combination of 558 and 423:
\[
9 = 558m + 423n.
\]
Here is how we do it with the table from before:\footnote{This trick is a shorthand for doing the traditional method of reverse substitution:
\[
\begin{align*}
9 & = 135 - 7 \cdot 18 \\
& = 135 - (423 - 3 \cdot 135) \\
& = 22 - 135 - 7 \cdot 423 \\
& = 22 \cdot (558 - 423) - 7423 \\
& = 22 \cdot 558 - 29 \cdot 423 \\
\end{align*}
\]}

\[
\begin{array}{c|c|c|c}
558 & 1 & 0 \\
1 & 423 & 1 & 0 \\
3 & 135 & 0 & 1 \\
7 & 18 & -3 & 135 \\
2 & 9 & -7 & 18 \\
0 & 2 & -2 & 9 \\
\end{array}
\]

We will make a new table with four columns, but retaining the numbers in the left column but making them negative:

\[
\begin{array}{c|c|c|c}
-558 & 1 & 0 \\
-1 & 423 & 1 & 0 \\
-3 & 135 & 0 & 1 \\
-7 & 18 & -3 & 135 \\
-2 & 9 & -2 & 9 \\
\end{array}
\]

To fill out the third column, we take the product of the first and third column in the previous row and add it to the previous value.

\[
\begin{array}{c|c|c|c|c|c|c|c|c}
\text{First step} & \text{Second step} & \text{Third step} \\
558 & 1 & 0 & 558 & 1 & 0 & 558 & 1 & 0 \\
\hline
-1 & 423 & 0 & 1 & -1 & 423 & 0 & 1 & -1 & 423 & 0 & 1 \\
-3 & 135 & 1 & -3 & 135 & 1 & -3 & 135 & 1 \\
-7 & 18 & -3 & -7 & 18 & -3 & -7 & 18 & -3 \\
-2 & 9 & -2 & 9 & -2 & 9 & -2 & 9 & -2 & 9 & 22 \\
\end{array}
\]
Similarly for the fourth column:

<table>
<thead>
<tr>
<th>First step</th>
<th>Second step</th>
<th>Third step</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-1 423 0 1</td>
<td>-1 423 0 1</td>
<td>-1 423 0 1</td>
</tr>
<tr>
<td>-3 135 1 -1</td>
<td>-3 135 1 -1</td>
<td>-3 135 1 -1</td>
</tr>
<tr>
<td>-7 18 -3 4</td>
<td>-7 18 -3 4</td>
<td>-7 18 -3 4</td>
</tr>
<tr>
<td>-2 9 22</td>
<td>-2 9 22</td>
<td>-2 9 22</td>
</tr>
</tbody>
</table>

We just read off from the last row of the table that \( m = 22 \) and \( n = -29 \).

**Definition 2.1.13.** Two nonzero integers are coprime\(^5\) if their gcd is equal to 1.

**Example 2.1.14.**

- 15 and 8 are coprime.
- Any two distinct primes are coprime.

There are some more nice consequences of Bézout’s identity, as we shall see below.

**Corollary 2.1.15.** Two nonzero integers \( a \) and \( b \) are coprime if and only if there exist integers \( m \) and \( n \) such that

\[
1 = ma + nb.
\]

\( \diamond \) **Proof:** This is a direct application of Corollary 2.1.11 and Definition 2.1.13. That is, if we set \( x = 1 \) in the statement of Corollary 2.1.11, we see that 1 can be written as \( ma + nb \) if and only if \( \gcd(a, b) \) divides 1. Now if \( \gcd(a, b) \) divides 1, then it is equal to 1 (because it is divisible by 1) and hence \( 1 = ma + nb \) for some integers \( m \) and \( n \) if and only if \( a \) and \( b \) are coprime. \( \square \)

**Corollary 2.1.16.** Let \( a \) and \( b \) be integers, and let \( c \) be an integer.

(i) If \( a \) and \( b \) are coprime, \( a \mid c \) and \( b \mid c \), then \( ab \mid c \).

(ii) If \( a \) and \( b \) are coprime, and \( a \mid bc \), then \( a \mid c \).

(iii) (Euclid’s Lemma) If \( p \) is prime and \( p \mid ab \), then \( p \mid a \) or \( p \mid b \).

\( \diamond \) **Proof:** To be done in lectures. \( \square \)

Part (i) of Corollary 2.1.16 is really a fact about the least common multiple of two integers.

**Definition 2.1.17.** The least common multiple of two nonzero integers \( x \) and \( y \) is defined by

\[
\text{LCM}(x, y) = \min \{ i \in \mathbb{N} : x \mid i \text{ and } y \mid i \}.
\]
2.2 Prime numbers and canonical factorisation of integers

In the previous section, we already alluded to the prime numbers. These are the indivisible parts of the integers and form the building blocks for all other integers. First and foremost, we will give one of the most beautiful elementary proofs in number theory, that there are infinitely prime numbers.

**Theorem 2.2.1** (Infinitude of primes). There are infinitely many prime numbers.

⋆ Proof: Suppose, for a proof by contradiction, that there are finitely many primes

\[ p_1 < p_2 < p_3 < \ldots < p_n. \]

Let \( N \) be the product of all the primes; \( N := p_1 p_2 \cdots p_n \). Because 2 and 3 are primes, we know at least that \( N > 2 \). Since \( N - 1 > 1 \), it has a prime divisor \( p_i \). Since \( N \) is divisible by every prime, we know that \( p_i \) divides both \( N \) and \( N - 1 \), and so divides their difference. Therefore,

\[ p_i \mid N - (N - 1) = 1 \]

which is a contradiction as \( p_i > 1! \). \( \square \)

Now we will give the most important result of number theory, the “Fundamental Theorem of Arithmetic.”

**Theorem 2.2.2** (The Fundamental Theorem of Arithmetic). Let \( n \) be an integer with \( n \geq 2 \). Then \( n \) can be written uniquely as a product of prime numbers:

\[ n = p_1 p_2 \cdots p_k, \quad p_1 \leq p_2 \leq \cdots \leq p_k. \]

So if \( n = q_1 q_2 \cdots q_k \) where the \( q_i \) are prime numbers, and \( q_1 \leq q_2 \leq \cdots \leq q_k \), then \( k = \ell \) and \( q_i = p_i \) for all \( i \in \{1, \ldots, k\} \).

⋆ Proof: This is an excellent example of a proof by induction.

**Existence:** For \( n \geq 2 \), let \( P(n) \) be the statement

\[ P(n) : \text{“all the positive integers at most } n \text{ can be written as a product of primes.”} \]

Clearly \( P(2) \) is true as 2 is a prime itself.\(^7\) So suppose \( P(k) \) is true for some positive integer \( k \geq 2 \). If \( k + 1 \) is prime, then we are done, so suppose \( k + 1 \) is not prime and that we can write \( k + 1 = ab \) where \( 1 < a, b < k + 1 \). Now by our inductive hypothesis, \( a \) is a product of primes and \( b \) is a product of primes. So \( ab \) is a product of primes! Therefore, \( P(k + 1) \) is true, and hence by the Mathematical Induction, \( P(n) \) is true for every positive integer \( n \geq 2 \).

**Uniqueness:** Suppose we can write \( n \) two ways as a product of primes

\[ n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell \]

For a proof by contradiction, we can suppose that the first factorisation is difference from the second. So without loss of generality, we may suppose that

\[ p_1 p_2 \cdots p_i = q_1 q_2 \cdots q_\ell \]

This proof is attributed to Ernst Kummer (1810–1893).

\(^6\) The Fundamental Theorem of Arithmetic was established at least by the Greeks of the time of Euclid, since it appears in Volume VII of The Elements.

\(^7\) Here we stress that a product of a list of integers \( L \) allows \( L \) to have just one element!
where
\[ \{p_1, p_2, \ldots, p_t\} \cap \{q_1, q_2, \ldots, q_u\} = \emptyset. \tag{2.1} \]

Now \(p_1\) divides both sides, and so \(p_1 \mod q_1 q_2 \cdots q_u\). So from Corollary 2.1.16, we know that \(p_1\) must divide at least one of the \(q_i\), for some \(i\).

This implies that \(p_1 = q_i\), as \(q_i\) is prime, which is a contradiction to 2.1.

Therefore, \(\{p_1, p_2, \ldots, p_k\} = \{q_1, q_2, \ldots, q_\ell\}\). □

This rudimentary property of the integers allows us to have a canonical factorisation of a number, a blueprint of a number in terms of the prime numbers.

**Definition 2.2.3 (Canonical factorisation).** For a positive integer \(n \geq 2\), the canonical factorisation of \(n\) is the unique expression of it as a product of primes:
\[ p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \]
where \(p_1 < p_2 < \cdots < p_k\) and each \(a_i\) is a non-negative integer.

**Remark 2.2.4.** The \(a_i\) are allowed to be zero, though in this case, we do not list the prime in order for the expression to be unique. Since \(n \geq 2\), not all of the \(a_i\) can be zero.

A consequence of the Fundamental Theorem of Arithmetic is that it is not difficult to calculate the greatest common divisor and least common multiple of two integers.

**Lemma 2.2.5.** Let \(x\) and \(y\) be integers, both at least 2, and write them out in their canonical factorisations:
\[ x = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \]
\[ y = p_1^{b_1} p_2^{b_2} \cdots p_\ell^{b_\ell}. \]

Suppose without loss of generality that \(k = \ell\), since we can take the \(a_i\) or \(b_j\) to be 0 so that both factorisations have the same length. Then:
\[ \text{(i) } \gcd(x, y) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)} \]
\[ \text{(ii) } \text{LCM}(x, y) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_k^{\max(a_k, b_k)} \]

Therefore,
\[ \text{LCM}(x, y) = \frac{xy}{\gcd(x, y)}. \]

\[ \diamond \text{ Proof: To be done in lectures.} \] □

### 2.3 Aside: how are the primes distributed?

#### 2.3.1 The prime number function \(\pi(n)\)

There are infinitely primes, but do they occur in a regular way on the number line? Or do they become sparser as the size of the digits gets larger?

One of the first results in this direction is the so-called **Bertrand’s Postulate** and it was proved by the great Russian mathematician Pafnuty Chebyshev.

**Theorem 2.3.1 (Bertrand’s Postulate).** For every integer \(n \geq 2\), there is a prime strictly between \(n\) and \(2n\).
Let $\pi(n)$ be the number of primes that are less than or equal to $n$. For example, $\pi(20) = 8$ as 2, 3, 5, 7, 11, 13, 17 and 19 are the prime numbers less than 20. Another way to express Bertrand’s Postulate is by the inequality

$$\forall n \geq 2 \quad \pi(2n) - \pi(n) \geq 1.$$  

However, Chebyshev proved something much stronger:

$$\forall n \geq 5 \quad \frac{1}{3} \frac{n}{\log n} < \pi(2n) - \pi(n) < \frac{7}{5} \frac{n}{\log n}.$$  

At this point, we have given some indication that the prime numbers occur rather frequently. Here is a simple result which shows that they are also rare.

**Theorem 2.3.2.** For every $k \in \mathbb{N}$, there are $k$ consecutive integers which are not prime.

**Proof:** Let $k \in \mathbb{N}$ and let $N = (k + 1)! + 2$. Note that

$$2 \mid N \quad \text{because } k \geq 1$$
$$3 \mid N + 1 \quad \text{because } k \geq 2$$
$$4 \mid N + 2 \quad \text{because } k \geq 3$$
$$5 \mid N + 3 \quad \text{because } k \geq 4$$
$$\vdots$$

In particular, we know that for $i \in \{0, \ldots, k - 1\}$, we have $i + 2 \mid (k + 1)!$ and hence $i + 2 \mid (k + 1)! + (i + 2) = N + i$. Hence $N, N + 1, N + 2, \ldots, N + k - 1$ are not prime. \hfill \Box

From Bertrand’s Postulate, we know that $\pi(n)$ grows at least as fast as $\log_2(n)$. In fact, Chebyshev attempted to prove something stronger, that the primes grow like $n / \log(n)$.

**Theorem 2.3.3** (The Prime Number Theorem). The limit of $\frac{\pi(n)}{n / \log(n)}$ as $n$ tends to $\infty$ is 1.

This famous theorem was conjectured by Carl Friedrich Gauß (1750’s) and proved independently by Jacques Hadamard and Charles de la Vallée Poussin (1896). Their proof used “complex analysis”, and it wasn’t until 1949 that an elementary proof was given by Paul Erdös and Atle Selberg.

**Remark 2.3.4.** The prime number theorem says that $\pi(n)$ grows asymptotically like $n / \log(n)$, but it says nothing about the difference $\pi(n) - n / \log(n)$.

### 2.3.2 Arithmetic progressions

Consider the following sequence:

$$1, 4, 7, 10, 13, 16, 19, 22, 25, \ldots$$

These are the numbers which are of the form $3k + 1$, where $k \in \mathbb{N} \cup \{0\}$. We have highlighted in bold the prime numbers in this sequence, which is known as an arithmetic progression. In general, if we take $a$ and $b$ to be coprime, we can ask how many primes occur in the arithmetic progression

\[ a, a + b, a + 2b, a + 3b, \ldots \]

\[ \vdots \]

\[ \vdots \]

\[ \vdots \]

\[ \vdots \]

$\vdots$

Why would you take $a$ and $b$ to be coprime? If they had a common factor, would we have a sensible sequence in which to study the occurrence of primes in?
A surprising result to this point was proved by Dirichlet in 1837.

**Theorem 2.3.5 (Dirichlet’s Theorem).** For all \( a, b \in \mathbb{N} \) coprime, the arithmetic progression \( a, a + b, a + 2b, a + 3b, \ldots \) contains infinitely many primes.

† Proof: The proof of this result is beyond the scope of this course. \( \square \)

What about the opposite question? Can we build sequences of primes that have regular gaps between them? Consider the following interesting sequences of primes:

<table>
<thead>
<tr>
<th>Sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>3, 5, 7</td>
</tr>
<tr>
<td>3, 7, 11</td>
</tr>
<tr>
<td>5, 11, 17, 23</td>
</tr>
</tbody>
</table>

The best we seem to be able to do is to list a sequence of 4 primes that are spaced 4 apart. At the time of writing, the best arithmetic progression consisting only of primes is due to Benoît Perichon (2010):

\[
43142746595714191 + k \cdot 23681770 \cdot 223092870
\]

where \( k \in \{0, 1, \ldots, 25\} \). This sequence of primes has length 26 and the distances between them are quite large compared to the sequences we had above. Can we do better than a sequence of length 26? This question was answered by Ben Green and Terence Tao\(^9\) (an Australian!):

**Theorem 2.3.6 (The Green-Tao Theorem).** The primes contain arbitrarily long arithmetic progressions.

Of course, the proof is non-constructive!

### 2.4 Mersenne primes and perfect numbers

We saw in the previous section that there are infinitely many primes, but it was not a constructive proof. That is, we did not create an explicit set of infinitely many primes, we only proved that there cannot be finitely many primes. Mersenne primes are the simplest set of many prime numbers that we know of, and yet, we still do not know if they can produce infinitely many primes.

**Definition 2.4.1 (Mersenne prime).** A prime number of the form \( 2^n - 1 \) is a Mersenne prime.

It turns out (see the Exercises at the end of this chapter) that \( n \) must a prime number in order for \( 2^n - 1 \) to be prime. Not all numbers of this form are prime though:

\[^9\] Terry Tao was awarded a 2006 Fields Medal, the mathematical equivalent of a Nobel Prize. He is the first Australian to have been awarded a Fields Medal.
The largest known Mersenne prime was discovered in 2008 and it is $2^p - 1$ where $p = 43, 112, 609$. We currently know of 47 Mersenne primes. There is a world-wide “Great Internet Mersenne Prime Search” (GIMPS) that uses the CPU power of thousands of home users machines who have volunteered their desktop power to aid in the search for the next Mersenne prime. See www.mersenne.org for more.

The greek civilisation had a particular fascination with what they called perfect numbers, and they knew of four perfect numbers at the time of Nicomachus in 100AD. A number $n$ is perfect if it equal to the sum of its proper divisors. For example, the proper divisors of 6 are 1, 2 and 3, and $6 = 1 + 2 + 3$.

**Example 2.4.2** (Examples of perfect numbers).

<table>
<thead>
<tr>
<th>Perfect number</th>
<th>Proper divisors</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1, 2, 3</td>
</tr>
<tr>
<td>28</td>
<td>1, 2, 4, 7, 14</td>
</tr>
<tr>
<td>496</td>
<td>1, 2, 4, 8, 16, 31, 62, 124, 248, 496</td>
</tr>
<tr>
<td>8128</td>
<td>1, 2, 4, 8, 16, 32, 64, 127, 254, 508, 1016, 2032, 4064</td>
</tr>
</tbody>
</table>

In Euclid’s Elements (Book IX), it was proved that there is a direct connection from Mersenne primes to perfect numbers.

**Theorem 2.4.3** (Euclid). If $2^k - 1$ is a Mersenne prime, then $2^{k-1}(2^k - 1)$ is a perfect number.

⋄ *Proof:* To be done in lectures. □

**Definition 2.4.4** (The sum-of-divisors function). For an integer $n$, let $\sigma(n)$ be the sum of the divisors of $n$.

So a perfect number $n$ satisfies $\sigma(n) = 2n$. Here are some other interesting properties of $\sigma$:

**Lemma 2.4.5.**

(i) If $p$ is a prime and $a$ is a positive integer, then

$$\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}.$$  

(ii) If $a$ and $b$ are coprime, then $\sigma(ab) = \sigma(a)\sigma(b)$.

⋄ *Proof:* For both parts, we simply use the following corollary of the Fundamental Theorem of Arithmetic: if we express a positive integer $x$ in terms of its canonical factorisation $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then every positive divisor of $x$ has canonical factorisation of the form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where for each $i$, we have $b_i \leq a_i$.

(i) Suppose $p$ is a prime and $a$ is a positive integer. Then the divisors of $p^a$ must be of the form $p^i$ for $i \in \{0, \ldots, a\}$. So $\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}$. 

The Greek civilisation had a particular fascination with what they called perfect numbers, and they knew of four perfect numbers at the time of Nicomachus in 100AD. A number $n$ is perfect if equal to the sum of its proper divisors. For example, the proper divisors of 6 are 1, 2 and 3, and $6 = 1 + 2 + 3$.
(ii) Suppose $a$ and $b$ are coprime. Suppose we wrote out their canonical
factorisations as follows

\[
\begin{align*}
  a &= p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k} \\
  b &= q_1^{b_1} q_2^{b_2} \ldots q_ɛ^{b_ɛ}.
\end{align*}
\]

We may assume that $a$ and $b$ are both greater than 1, since the result
would definitely hold in either of these two cases. With this assump-
tion, we may further assume that each of the $a_i$ and $b_i$ are greater than
0 (otherwise we would suppress the term). Then \(\sigma(a) = \prod_i \sigma(p_i^{a_i})\),
and similarly, \(\sigma(b) = \prod_i \sigma(q_i^{b_i})\). Since $a$ and $b$ are coprime, we have
\([p_1, \ldots, p_k] \cap [q_1, \ldots, q_ɛ] = \emptyset\). So the canonical factorisation of $ab$ is simply

\[
\begin{align*}
  p_1^{a_1} & p_2^{a_2} \ldots p_k^{a_k} q_1^{b_1} q_2^{b_2} \ldots q_ɛ^{b_ɛ}.
\end{align*}
\]

and since we can easily read off the divisors of this integer by its
canonical factorisation, it then follows that \(\sigma(ab) = \sigma(a)\sigma(b)\).

\[\square\]

In particular, \(\sigma(2^k) = 2^{k+1} - 1\), which will be used in the following
result, which was first observed by the great mathematician, Leonard Euler.

**Theorem 2.4.6** (Euler, c.a. 1740).

*Every even perfect number is of the form \(2^{k-1}(2^k - 1)\).*

\[\star \text{ Proof: } \] To be done in lectures. \[\square\]

**Question 2.4.7.** *Is there an odd perfect number?*

The best known answer to date to this question (at the point of writing)
is due to Ochem and Rao (2011):

**Theorem 2.4.8** (Ochem and Rao, 2012). *An odd perfect number must be
larger than \(10^{1500}\).*

2.5 Clock arithmetic

Suppose it is 10:02am right now. What is the time 6 hours from now? If
you use a 24-hour convention, then you would say that it is 16:02. But if
you use a 12-hour convention, using “am” or “pm”, then the answer would
be 4:02pm. What were you doing when you are working out that it would
be 4:02 in the clock? You were counting to 12, and then starting back at 0
again. That is, 12 is the *same* as 0.

Here is another example. What day of the week is it on the 10th of the
next month? To work out the answer, you count out the number of days
until the 10th of the next month, divide by 7, and take the remainder. Then
you add this remainder to the day we are currently on.

**Example 2.5.1.** *If it is now Wednesday August 22nd, then there are 19 days
until September 10. Now \(19 = 2 \times 7 + 5\), so there is a remainder of 5 when
dividing 19 by 7. We then count forward by 5 in the days of the week and
discover that September 10 is a Monday.*
What would happen to the examples above if a clock had 13 numbers, or if a week had five days? We would simply change which number that we think of as ‘zero’.

**Definition 2.5.2 (Congruence Modulo n).**

Let \( n \in \mathbb{N} \). Integers \( a \) and \( b \) are said to be congruent modulo \( n \) if \( n \) divides \( a - b \). We denote this relation by \( a \equiv_n b \).

**Example 2.5.3.**

- \( 14 \equiv_5 4 \) since \( 14 - 4 = 10 \) is a multiple of 5.
- \( -7 \equiv_3 2 \) since \( -7 - 2 = -9 \) is a multiple of 3.

The congruence relation is a little bit like the equality relation, but more flexible. It at least has the following properties\(^\text{10}\). Compare the following lemma to Lemma 2.1.2.

**Lemma 2.5.4.** For \( n \in \mathbb{N} \), congruence modulo \( n \) satisfies the following properties:

- **Reflexivity:** For all \( a \in \mathbb{Z} \), \( a \equiv_n a \).
- **Symmetry:** For all \( a, b \in \mathbb{Z} \), if \( a \equiv_n b \) then \( b \equiv_n a \).
- **Transitivity:** For all \( a, b, c \in \mathbb{Z} \), if \( a \equiv_n b \) and \( b \equiv_n c \) then \( a \equiv_n c \).
- **Compatible with addition:** If \( a \equiv_n b \) and \( a' \equiv_n b' \), then \( a + a' \equiv_n b + b' \).
- **Compatible with multiplication:** If \( a \equiv_n b \) and \( a' \equiv_n b' \), then \( aa' \equiv_n bb' \).

\( \qed \)

**Proof:**

**Reflexivity:** Note for all \( a \in \mathbb{Z} \) that \( n \) divides \( a - a = 0 \) and hence \( a \equiv (mod \ n) \).

**Symmetry:** If \( a \equiv b \ (mod \ n) \), then \( n \) divides \( a - b \), which is the same as \( b - a \), and hence \( b \equiv a \ (mod \ n) \).

**Transitivity:** Suppose \( a \equiv b \ (mod \ n) \) and \( b \equiv c \ (mod \ n) \) for some integers \( a, b, \) and \( c \). Then \( n \) divides \( a - b \) and \( n \) divides \( b - c \). So \( n \) divides the sum of \( a - b \) and \( b - c \), which is \( a - c \), and hence \( a \equiv c \ (mod \ n) \).

**Compatible with addition and multiplication:** Suppose \( a \equiv_n b \) and \( a' \equiv_n b' \). Then \( n \) divides \( a - b \) and \( n \) divides \( a' - b' \). So \( n \) divides their sum \( a + a' - b - b' \). Hence, \( a + a' \equiv_n b + b' \).

For multiplication, we need to be more explicit. Write \( a - b = kn \) and \( a' - b' = k'n \) for some \( k, k' \in \mathbb{Z} \). Then

\[
\begin{align*}
aa' &= (b + kn)(b' + k'n) \\
&= bb' + n(bk' + b'k + kk')
\end{align*}
\]

and hence \( n \) divides \( aa' - bb' \).

\( \qed \)

**Corollary 2.5.5.** If \( a \equiv_n b \), then for all positive integers \( k \), we have \( a^k \equiv_n b^k \).
This allows us to make very difficult calculations with ease!

**Example 2.5.6.** Find the remainder of $7^{50}$ when divided by 15.

**Solution:** First notice that $7^2 = 49$ and $49 \equiv_{15} 4$. So

$$7^4 = (7^2)^2 \equiv_{15} 4^2 = 16 \equiv_{15} 1.$$  

Now $7^{50} = 7^{4 \cdot 12 + 2}$ and so

$$7^{50} = (7^4)^{12} \cdot 7^2 \equiv_{15} 1^{12} \cdot 7^2 \equiv_{15} 4.$$  

Therefore, if we divide $7^{50}$ by 15, we end up with a remainder of 4.

The remainder of an integer when we divide by $n$ always gives us a number within a certain range

$$\mathbb{Z}_n := \{0, 1, \ldots, n - 1\}$$

which we call the set of integers modulo $n$. We will see that this set can be equipped with addition-like and multiplication-like operations that makes it into an interesting number system.

**Lemma 2.5.7.** For every integer $x$, there is a unique element $y \in \mathbb{Z}_n$ such that $x \equiv_n y$.

**Proof:** Let $x$ be an integer. By the Division Rule (Lemma 2.1.4), there exist unique integers $q$ and $r$ such that $x = qn + r$ and $0 \leq r < n$. So $r \in \mathbb{Z}_n$. So if we let $y = r$, we see that there is a unique element $y \in \mathbb{Z}_n$ such that $x \equiv_n y$. □

We can make $\mathbb{Z}_n$ into a ring by defining addition and multiplication modulo $n$.

**Definition 2.5.8 (Arithmetic Modulo $n$).**

Let $n \in \mathbb{N}$. Then we define the binary operations $\oplus_n$ and $\otimes_n$ on the integers by

$$x \oplus_n y = (x + y) \pmod{n}$$

$$x \otimes_n y = xy \pmod{n}$$

for all $x, y \in \mathbb{Z}$. The output is always an element of $\mathbb{Z}_n$.

**Example 2.5.9.**

- $5 \oplus_4 3 = 8 \pmod{4} = 0$,
- $-7 \oplus_5 13 = 6 \pmod{5} = 1$,
- $50 \otimes_233 233 = 50 \cdot 233 \pmod{233} = 0$.

We can sometimes ‘cancel’ both sides.

**Lemma 2.5.10.** Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, and suppose $n$ and $a$ are coprime. If $xa \equiv_n ya$, then $x \equiv_n y$.

**Proof:** Suppose $xa \equiv_n ya$. Then $n$ divides $xa - ya = (x - y)a$. Since $n$ and $a$ are coprime, we have by Corollary 2.1.16 that $n$ divides $x - y$. Therefore, $x \equiv_n y$. □
### 2.5.1 Linear diophantine equations

A linear diophantine equation is an equation of the form

\[ ax + by = c \]

where \(a, b, c\) are given integers and we want to solve for integers \(x\) and \(y\). Here is an example that we see often in real life.

**Example 2.5.11.** What amounts of money can you make from \$2 and \$5 denominations? That is, for what values \(c\) can we solve \(2x + 5y = c\)?

We can rephrase a linear diophantine equation \(ax + by = c\) in terms of a solution in one of these variables, giving us a congruence equation:

\[ ax + by = c \text{ has a solution in } x \iff b \mid ax - c \quad (2.2) \]

\[ \iff ax \equiv b \pmod{c} \quad (2.3) \]

**Theorem 2.5.12.** The congruence equation \(ax \equiv b \pmod{c}\) has a solution in \(x \in \mathbb{Z}\) if and only if \(\gcd(a, b) \mid c\).

**Proof:** Done in lectures. \(\square\)

The next question we might ask is, if a linear diophantine solution has a solution, does it have more, and how many more?

**Example 2.5.13.** Suppose \(a = 8, b = 6 \text{ and } c = 14\). Clearly there is a solution to \(ax + by = c\) by taking \(x = y = 1\). Are there more solutions? First of all, from the argument above (2.2), we need \(8x \equiv 14 \pmod{6}\). This equation simplifies to \(x \equiv 3 \pmod{1}\). The set of all integers \(x\) which satisfy \(x \equiv 3 \pmod{1}\) has a special name:

\[ 1 + 3\mathbb{Z} = \{ x \in \mathbb{Z} : x \equiv 3 \pmod{1} \} = \{ \ldots, -8, -5, -2, 1, 4, 7, 10, 13, \ldots \}. \]

**Theorem 2.5.14 (The LDE Theorem).** Suppose \(\gcd(a, b) \mid c\). If \((x_0, y_0)\) is a solution to \(ax + by = c\) (i.e., \(ax_0 + by_0 = c\)), then

\[ \left( x_0 + \frac{b}{\gcd(a, b)}t, y_0 - \frac{a}{\gcd(a, b)}t \right) \]

is a solution to \(ax + by = c\), for all \(t \in \mathbb{Z}\).

In other words, if we fix \(y\), the set of all solutions of \(x\) to \(ax + by = c\) in is infinite if it is non-empty, and it is the congruence class \(x_0 + t\mathbb{Z}\), for all \(t \in \mathbb{Z}\). We will leave the proof as an exercise (see the last section of this chapter).

### 2.5.2 A magic trick and the Chinese Remainder Theorem

Here is how the trick goes. You need four volunteers from the audience. The first three will receive an envelope each containing a piece of paper with a number on it. The fourth, call her Alice, chooses a number between 1 and 1000 and writes it on each of the three volunteers envelopes and secretly passes their envelopes to them. You, nor the rest of the audience know what the number is. Each volunteer has a similar task to complete:
Volunteer 1 works out what their number is modulo 7, call it $a_1$, and writes it on the piece of paper inside the envelope.

Volunteer 2 works out what their number is modulo 11, call it $a_2$, and writes it on the piece of paper inside the envelope.

Volunteer 3 works out what their number is modulo 13, call it $a_3$, and writes it on the piece of paper inside the envelope.

They give you their scribed pieces of paper. With this information you can recover the original number that Alice chose! Let

$$x = -2 \cdot 143 \cdot a_1 + 4 \cdot 91a_2 - 77a_3.$$ 

Alice’s number is then congruent to $x$ modulo 1001. Why 1001? Because $1001 = 7 \cdot 11 \cdot 13$, and we used the proof of the Chinese Remainder Theorem.

**Theorem 2.5.15** (Chinese Remainder Theorem). Let $m_1, m_2, \ldots, m_k$ be positive integers, pairwise coprime, and let $a_1, a_2, \ldots, a_k$ be integers. Then there is a solution $x \in \mathbb{Z}$ of the following simultaneous linear diophantine equations:

$$x \equiv m_1 a_1 \pmod{m_1},$$
$$x \equiv m_2 a_1 \pmod{m_2},$$
$$\vdots$$
$$x \equiv m_k a_k \pmod{m_k}.$$ 

Moreover, two solutions are congruent modulo $m_1m_2 \cdots m_k$.

**Proof:** Let $M = m_1m_2 \cdots m_k$. Now for each $i$, we have that $m_i$ and $M/m_i$ are coprime. By Lemma 2.5.10, for each $i$, there exists $b_i$ such that

$$b_i \left( \frac{M}{m_i} \right) \equiv 1.$$ 

Let $x = \sum_{i=1}^{k} a_i b_i M/m_i$. Then for each $i$, we have $x \equiv m_i a_i b_i M/m_i \equiv m_i a_i$. Therefore, $x$ is a solution to the simultaneous linear diophantine equations.

Now suppose $x'$ is another solution. Then for each $i$, we have $x \equiv m_i a_i$ and hence $m_i$ divides $x - x'$, for each $i \in \{1, \ldots, k\}$. So $M$ divides $x - x'$ by Corollary 2.1.16, and hence

$$x \equiv M x'.$$

The important part of the proof is that it gives us a solution:

$$x = \sum_{i=1}^{k} a_i b_i \frac{M}{m_i}.$$
So in the magic trick above \( m_1 = 7, m_2 = 11 \) and \( m_3 = 13 \). We then work out the inverses of the \( m_i m_j \) modulo the other \( m_k \), and assign them to \( b_k \):

\[
\begin{align*}
  b_1 &: (11 \cdot 13)^{-1} \pmod{7} \rightarrow -2 \\
  b_2 &: (7 \cdot 13)^{-1} \pmod{11} \rightarrow 4 \\
  b_3 &: (7 \cdot 11)^{-1} \pmod{13} \rightarrow -1.
\end{align*}
\]

Of course, we could’ve taken any number to be an inverse as long as it returns 1 under multiplication modulo \( m_i \). For example, in the first case we could have taken \( b_1 = 5 \) since

\[
5 \cdot (11 \cdot 13) = 715 \equiv 1 \pmod{7}.
\]

2.5.3 **Fermat’s Little Theorem**

Fermat’s Little Theorem, and its generalisation by Euler, are the essential ingredients in the RSA-cryptosystem; a commonly used method for transmitting public keys between two parties.

**Theorem 2.5.16** (Fermat’s Little Theorem). Let \( p \) be a prime and let \( a \) be an integer. Then

\[
a^p \equiv_p a.
\]

★ **Proof:** To be done in lectures. \( \square \)

**Example 2.5.17.** Show that for all \( n \in \mathbb{Z} \), \( n^9 - n \) is divisible by 6.

**Solution.** Let \( n \in \mathbb{Z} \). Then \( n^9 = (n^3)^3 \) and so we can apply Fermat’s Little Theorem:

\[
\begin{align*}
  \text{Now } (n^3)^3 &\equiv_3 n^3 \\
  \text{Then } (n^3)^3 &\equiv_3 n \\
  \text{Therefore, } n^9 - n \text{ is divisible by 3.}
\end{align*}
\]

Next we decompose \( n^9 \) into \((n^2)^3\)^2 and use Fermat’s LT for \( p = 2 \):

\[
\begin{align*}
  \text{Now } n^2 &\equiv_2 n \\
  \text{Then } n^4 = (n^2)^2 &\equiv_2 n^2 \equiv_2 n \\
  \text{Then } n^8 = (n^4)^2 &\equiv_2 n^2 \equiv_2 n \\
  \text{Then } n^8 \cdot n &\equiv_2 n \cdot n \text{ Therefore, } n^9 \equiv_2 n \text{ Therefore, } n^9 - n \text{ is divisible by 2.}
\end{align*}
\]

Since 2 and 3 are coprime, we have by Corollary 2.1.16 that \( n^9 - n \) is divisible by 6.

2.6  **Aside: The RSA algorithm for public-key encryption**

For a long time, the world used **private key cryptography** to transmit secret information, until the breakthrough of Diffie and Hellman in the 1970’s. We will see an example of **public key cryptography**, the so-called RSA cryptosystem.

It can often be difficult to find the (multiplicative) inverse of a number modulo \( m \). For example, the inverse of 7 modulo 64 is 55, which may not be easy to guess off-hand. We can use the Euclidean Algorithm to find the inverse modulo \( m \) and we show how this is done by example.

“We in science are spoiled by the success of mathematics. Mathematics is the study of problems so simple that they have good solutions.”

– Whitfield Diffie (1944–)
Example 2.6.1. We want to work out an inverse of $21$ modulo $1430$. The essential property which makes this work is that $21$ and $1430$ have no prime factors in common. By Bézout’s Identity, there are integers $x$ and $y$ such that

$$21x + 1430y = 1.$$ 

So

$$21x \equiv_{1430} 21x + 1430y = 1$$

and hence $x$ will give us the inverse if we can work it out. We will use the Euclidean Algorithm:

<table>
<thead>
<tr>
<th></th>
<th>1430</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>-68</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-10</td>
<td>2</td>
<td>1</td>
<td>-68</td>
</tr>
<tr>
<td>-1</td>
<td>0</td>
<td>-10</td>
<td>681</td>
</tr>
</tbody>
</table>

Therefore, a multiplicative inverse of $21$ is $681$.

Sharing a ‘key’

The previous methods of enciphering depended on knowledge of the key to decipher the message, so the key had to be kept private between Alice and Bob. In the 1970’s a radical new approach to cryptography was borne, public key cryptography. The general way it works is this: Bob has two keys, one private and one public. The public key is used by Alice to encrypt messages sent to Bob, and the private key is used by Bob to decrypt messages.

Here is an analogy where Alice sends a treasure chest to Bob through the post. Alice has a padlock and both Alice and Bob have a key to this padlock. When Alice sends the treasure chest, she puts a padlock on the treasure chest, and then when Bob receives the chest, he opens it with his keys. The problem with this approach is that Alice and Bob need to meet privately to ensure they have identical keys. This is private key cryptography. We can change this example to give an analogy for public key cryptography:

Example 2.6.2. Alice has a treasure chest and padlock, and Bob has a padlock as well, but it is a different padlock. Can you think of a way for Alice to send the treasure chest to Bob so that Bob can open it, but they never meet? (You are allowed to used the postal system more than once!)

Solution: Alice locks the chest with her padlock and sends it to Bob. Bob then places his padlock on the chest and sends it back to Alice. We now have two padlocks on the treasure chest. Alice takes her padlock off and sends it back to Bob. Then Bob can open the treasure chest by removing his padlock.

One-way functions

Just as we saw in the previous example, the main idea in public key cryptography is a one-way function. A function $f$ is said to be one-way if given $x$ it is “easy” to compute $f(x)$, but given $y$, it is “hard” to determine an $x$.
such that \( f(x) = y \). The mathematics behind “easy” and “hard” is well beyond the scope of this course, but if you’re interested, there is plenty on the web about it, and related to this question is one of the biggest problems in mathematics; is \( P = \text{NP} \)? Diffie and Hellman were the first to conceive of the idea of using one-way functions in cryptography, and they actually constructed one, although it is not as good as the one we will see below.

**The RSA cryptosystem**

The RSA cryptosystem is named after the three mathematicians who invented it around 1978: Ron Rivest, Adi Shamir and Leonard Adleman. It was found out much later, that the same cryptosystem was discovered in top-secret work by the GCHQ in the early seventies (by Clifford Cocks).

Before a message can be sent, a public key is set up by the receiver (Bob) that everyone has access to.

- Choose two different primes \( p \) and \( q \).
- Compute \( n = pq \) and \( \varphi = (p − 1)(q − 1) \). (The symbol \( \varphi \) is the greek letter \( \phi \)).
- Choose \( e \) such that \( e \) has an inverse modulo \( \varphi \), and let \( d \) be this inverse.
- The encryption function is \( E_{n,e}(x) = x^e \pmod{n} \).
- The decryption function is \( D_{n,d}(x) = x^d \pmod{n} \).

Bob then has the following:

<table>
<thead>
<tr>
<th>Public Key</th>
<th>((n, e))</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Key</td>
<td>(d)</td>
</tr>
</tbody>
</table>

**Example 2.6.3.** The two chosen prime numbers are \( p = 47 \) and \( q = 59 \). So

\[
n = 47 \times 59 = 2773, \quad \varphi = 46 \times 58 = 2668.\]

Now we need an integer \( e \) such that

\[
de \equiv 1\pmod{\varphi}
\]

for some \( d \). It turns out that \( e = 157 \) is one of many choices for \( e \). In fact,

\[
17 \times e = 2669 \equiv 2668 \pmod{\varphi}.
\]

So \( d = 17 \).

**Public Key:** \((n, e) = (2773, 157)\).

Alice then converts her message to a sequence of integers between 0 and \( n − 1 \), and then encrypts them with

\[
E_{n,e}(x) = x^e \pmod{n}.
\]
So for example, Alice sends the number 5 by encrypting it:

\[ 5^{137} \pmod{n} = 1044. \]

Bob then applies his decryption function \( D_{n,d}(x) = x^d \pmod{n} \):

\[ 1044^{17} \pmod{2773} = 5. \]

**Why it works: Fermat’s Little Theorem**

First we give a simple corollary of Fermat’s Little Theorem.

**Corollary 2.6.4.** Let \( p \) and \( q \) be different prime numbers and let \( a \) be an integer which is not divisible by \( p \) or \( q \). Then

\[ a^{(p-1)(q-1)} \equiv_{pq} 1. \]

**Proof.** By Fermat’s Little Theorem (2.5.16), \( a^{p-1} \equiv_p 1 \), and so

\[ a^{(p-1)(q-1)} \equiv_p 1^{q-1} = 1. \]

Similarly, \( a^{q-1} \equiv_q 1 \) and so

\[ a^{(p-1)(q-1)} \equiv_q 1^{p-1} = 1. \]

Therefore, both \( p \) and \( q \) divide \( a^{(p-1)(q-1)} - 1 \) and so \( pq \) divides this number. Hence \( a^{(p-1)(q-1)} \equiv_{pq} 1. \) \( \square \)

Let’s see what happens when we decrypt something that’s been encrypted:

\[ D_{n,d} \left( E_{n,e}(x) \right) = (x^e)^d \pmod{n}. \]

So in order for decryption to give us the same thing back again, we need to show that

\[ x^{de} \equiv_n x. \]

Now \( d \) was chosen so that \( de \equiv_p 1 \), that is, \( de = 1 + m\phi \) for some \( m \). Hence

\[ x^{de} = x^{1 + m\phi} = x \cdot (x^\phi)^m. \]

Now \( x^\phi = x^{(p-1)(q-1)} \) and so \( x^\phi \equiv_{pq} 1 \) (by the Corollary above). It then follows that

\[ x^{de} \equiv_n x. \]

**Further questions on RSA for you to ponder**

- Why is it computationally easy to carry out the calculations involved such as finding \( d \) and computing powers modulo \( n \)?
- Why cannot another user discover the sent message when they know the public key?
- How much extra information do you need to to crack a message sent with RSA?
2.7 Exercises

1. Show that \( n \) must a prime number in order for \( 2^n - 1 \) to be prime.

2. Find the set of all integer solutions in \( x \) to the following set of simultaneous linear diophantine equations:

\[
\begin{align*}
    x &\equiv_6 2 \\
    x &\equiv_7 1 \\
    x &\equiv_{11} 3.
\end{align*}
\]

3. Use the Euclidean Algorithm to find the greatest common divisor of 56 and 1430, and find integers \( s \) and \( t \) such that

\[
\gcd(56, 1430) = 56s + 1430t.
\]

4. Let \( n \) be an odd integer. Prove that \( n^2 \equiv 1 \pmod{4} \).

5. Let \( n \geq 2 \) be an integer. Suppose that for every prime \( p \leq \sqrt{n} \), \( p \) does not divide \( n \). Prove that \( n \) is a prime.

6. Let \( q \) be an odd positive integer and let \( x \in \mathbb{Z} \). Show that \( x + 1 \) divides \( x^q + 1 \).

7. Show that if \( k \geq 1 \) such that \( 2^k + 1 \) is a prime then \( 2^k = 2^n \) for some \( n \geq 0 \).

8. Let \( U_n \) be the nonzero elements of \( \mathbb{Z}_n \) which have a multiplicative inverse and let \( a \in U_n \). Prove

\[
a^{\mid U_n \mid} \equiv 1 \pmod{n}.
\]

What do you notice when \( n \) is prime?

9. Are the following true or false?

   (a) \( 4 \equiv_{13} 17 \)
   
   (b) \( 6 \equiv_{7} 42 \)
   
   (c) \( -1 \equiv_{4} 11 \)
   
   (d) \( 11 \equiv_{4} -1 \)
   
   (e) \( -5 \equiv_{8} -21 \)

10. Find the remainder \( r \) (between 0 and 6) that we get when we divide \( 6^{82} \) by 7.

11. Calculate the following:

   (a) \( 2 \oplus_5 4 \)
   
   (b) \( -4 \oplus_3 10 \)
   
   (c) \( 25 \otimes_9 94 \)
   
   (d) \( -2 \otimes_3 7 \)
   
   (e) \( 25634578912 \otimes_2 65 \).
12. John H. Conway once said that 91 is the smallest integer which looks like a prime, but isn’t. Use Fermat’s Little Theorem to show that 91 is not prime. (Hint: Decompose 90 into binary: $90 = 64 + 16 + 8 + 2$).

13. We will do a magic trick starting with 27 cards (the joker, the diamonds and the hearts), and the audience member selects 4 cards. The assistant hides one card and you, the magician, will use the other three cards to figure out what the fourth card is. First we assign a number from 0 up to 26 to each card.

```
Joker A 2 3 4 5 6 7 8 9 10 J Q K A 2 3 4 5 6 7 8 9 10 J Q K
-       ⋮      ⋮      ⋮      ⋮      ⋮      ⋮      ⋮      ⋮      ⋮
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

The audience member selects four cards, and the assistant hides one of the cards. The three cards that the magician can see are:

\[
\begin{pmatrix}
3 \\
7 \\
10
\end{pmatrix}
\]

(a) Convert these cards to numbers from \{0, \ldots, 26\} and find the remainder of their sum \(s\) when divided by 4.

(b) There are 24 possibilities for the hidden card. How many numbers are there from \{0, \ldots, 23\} which are congruent to \(s\) modulo 4?

(c) From the last question, you know that there are \(N\) numbers from \{0, \ldots, 23\} that are congruent to \(s\) modulo 4. The assistant wants to somehow give you a number from 0 up to \(N - 1\) which will give rise to the number that gives away the hidden card for you.

The assistant lays out the three cards to you in this order ...

\[
\begin{pmatrix}
7 \\
10 \\
3
\end{pmatrix}
\]

i. When represented as numbers from \{0, \ldots, 26\}, let \(d_i\) be the number of displayed cards appearing to the right of the \(i\)-th card that are smaller than it. Find \(d_1\) and \(d_2\).

ii. Compute \(p = 2d_1 + d_2\). You should get a number from \{0, \ldots, N - 1\}.

iii. Now find \(R = 4p + (-s \mod 4)\). The hidden card is the \(R\)-th possible card. Be careful to start counting at 0 and to skip over the three cards we already have; the hidden card may not be the \(R\)-th card from the deck. Which card do you get?

14. Prove that a number is divisible by three if and only if the sum of its digits is divisible by three. (Hint: The first step is to express the unknown number \(N\) as some unknown sum of multiples of powers of 10.)

15. Find the day of the week you were born on by using the following formula:

\[
W = (D + \lfloor 2.6((M + 9) \mod 12) + 2.4 \rfloor - 2C + \lfloor 5Y/4 \rfloor + \lfloor C/4 \rfloor - \lfloor ((M + 9) \mod 12)/10 \rfloor) \mod 7
\]

where
• $D$ is the day (1 to 31),
• $M$ is the month (1 to 12),
• $C$ is the century (2011 has $C = 20$),
• $Y$ is the year (2011 has $Y = 11$),
• $W$ is the week day (Sunday=0,…,Saturday=6).

The symbol $\lfloor x \rfloor$ means the “integer part” of $x$ (i.e., round down to the nearest integer).
3

Rings beyond numbers

We investigate polynomial rings and their properties, to see which of those for the integers also hold for polynomials. We finish with algebraic numbers and the famous impossible problems of antiquity. In the middle, we come across one of the most important themes of this course: equivalence relations. From this chapter until the end of the notes, the idea of an equivalence relation will crop up continuously (no pun intended for Chapter 2).

3.1 Rings and fields

By doing some elementary number theory first, we will have some motivation to study the greater context; the theory of rings. The study of rings really began in the work of Richard Dedekind in his seminal work Vorlesungen über Zahlentheorie (1879, 1894) and was invented as a generalisation of different algebraic systems with common properties, and the early beginnings in the theory of rings were very much inspired by the quest to prove Fermat’s Last Theorem. The term ring was later coined by David Hilbert.

In the definition we use below, we will always assume that a ring has a unit; sometimes these are known specially as unital rings. It seems the definition is very long, but once the student learns what a group is (in a later course) it becomes much simpler.

Definition 3.1.1 (Ring). A ring is a set $R$ equipped with two associative binary operations $+$ and $\cdot$ called addition and multiplication, satisfying the following axioms:

$(R, +)$ is an abelian group

- Addition is commutative.
- There is an additive identity called $0$ in $R$, such that for all $a \in R$ we have $a + 0 = a$.
- Every element has an additive inverse. That is, for each element $a \in R$, there is an element $b \in R$ such that $a + b = 0$.

$(R \setminus \{0\}, \cdot)$ is a monoid

- There exists a multiplicative identity called $1$ in $R$ such that for all elements $a \in R$ we have $a \cdot 1 = a$.

Distributive laws

We use 0 and 1 informally for the additive and multiplicative inverses for a ring. Of course, we might use other notion in a particular context, for example, $O$ and $I$ in a matrix ring.
• For all \( a, b, c \in \mathbb{R} \), the equation \( a \cdot (b + c) = (a \cdot b) + (a \cdot c) \) holds.

• For all \( a, b, c \in \mathbb{R} \), the equation \( (a + b) \cdot c = (a \cdot c) + (b \cdot c) \) holds.

**Example 3.1.2.**

• The set of integers form a ring, and the set of \( n \times n \) matrices over \( \mathbb{R} \) form a ring with the usual addition and multiplication operations.

• However, \( \mathbb{N} \) is not a ring as no element has an additive inverse, nor is there an additive identity!

• Under the operations of \( \oplus_n \) and \( \otimes_n \), the set \( \mathbb{Z}_n \) forms a ring.

• Later we will see how polynomials form a ring. Polynomial rings are the bread-and-butter of algebraic number theory and algebraic geometry, and their influence and application to 20th-century mathematics cannot be understated.

A **field** is a ring where there is extra multiplicative structure. The applied mathematicians use the word **field** to mean something entirely different!

**Definition 3.1.3** (Field). A field is a ring \((F, +, \cdot)\) such that \((F \setminus \{0\}, \cdot)\) is an abelian group. That is,

• \( \cdot \) is commutative: \( a \cdot b = b \cdot a \) for all \( a, b \in F \).

• Every element has a **multiplicative inverse**. That is, for each element \( a \in F \), there is an element \( b \in R \) such that \( a \cdot b = 1 \).

**Example 3.1.4.** The set of real numbers \( \mathbb{R} \) and the set of complex numbers \( \mathbb{C} \) are both fields, and so too is the set of rational number \( \mathbb{Q} \). The integers \( \mathbb{Z} \), however, do not form a field since \( 2 \) does not have a multiplicative inverse. The invertible \( n \times n \) matrices over \( \mathbb{R} \) only form a field if \( n = 1 \), since matrix multiplication is not commutative.

The ring and field properties can be explained by looking at their addition and multiplication tables (particularly if they are finite!).

**Example 3.1.5.** Consider \( \mathbb{Z}_4 \). It is a ring and we can write out its addition and multiplication tables as follows:

<table>
<thead>
<tr>
<th>( \oplus_4 )</th>
<th>0 1 2 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 1 2 3</td>
</tr>
<tr>
<td>1</td>
<td>1 0 3 2</td>
</tr>
<tr>
<td>2</td>
<td>2 3 0 1</td>
</tr>
<tr>
<td>3</td>
<td>3 2 1 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( \otimes_4 )</th>
<th>0 1 2 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0 0 0 0</td>
</tr>
<tr>
<td>1</td>
<td>0 1 2 3</td>
</tr>
<tr>
<td>2</td>
<td>0 2 0 2</td>
</tr>
<tr>
<td>3</td>
<td>3 0 2 1</td>
</tr>
</tbody>
</table>

For the left-hand table for \( \oplus_4 \), we see that it is symmetric about the diagonal, so this operation is **commutative**. We also see that it is a Latin square\(^2\) and so every element has an additive inverse (and it is unique). On the other-hand the table for \( \otimes_4 \) is symmetric, but not a Latin square. So some elements here have multiplicative inverses, and some don’t, even if we are careful to only look at the nonzero elements. If the nonzero elements form a Latin square for \( \otimes_4 \), then this is the same as saying that the ring is a field.

\(^2\) Recall from your school days that an \( n \times n \) square made up of \( n \) numbers is a Latin square if every number appears exactly once in each row and column.
**Question 3.1.6.** When do we get Latin squares?

When \( n \) is not prime, can we decide if an element of \( \mathbb{Z}_n \) has a multiplicative inverse? Such elements are called *units* of \( \mathbb{Z}_n \). For example, in \( \mathbb{Z}_4 \) the units are just 1 and 3; there is no element \( s \) such that \( 2 \otimes s = 1 \).

**Definition 3.1.7 (Units of a ring).** A nonzero element \( r \) of a ring \( R \) is a *unit* if there exists an element \( s \) such that \( r \cdot s = 1 \). That is, \( r \) has a multiplicative inverse.

**Lemma 3.1.8.** An element \( a \in \mathbb{Z}_n \) is a unit if and only if gcd\((a,n)\) = 1.

*Proof:* To be done in lectures.

**Corollary 3.1.9.** \( \mathbb{Z}_n \) is a field if and only if \( n \) is prime.

*Proof:* To be done in lectures.

\[ \Box \]

### 3.2 Ideals

The term *ideal* was introduced by Dedekind at the birth of the theory of rings. An ideal is a special sub-ring of a ring which in some sense absorbs elements of the ring when they are multiplied by elements inside the ideal. First, let us consider the simplest ring, the ring of integers \( \mathbb{Z} \).

**Example 3.2.1.** Consider the even numbers \( 2\mathbb{Z} \) of \( \mathbb{Z} \). It is closed under addition and multiplication and so forms ring; that is, \( 2\mathbb{Z} \) is a subring of \( \mathbb{Z} \). Now let \( 2x \) be a typical element of \( 2\mathbb{Z} \), and take another element of \( \mathbb{Z} \), say \( z \). Then \( 2x \cdot z \) is divisible by 2 and hence the product of \( 2x \) with \( z \) is an even number. So we have the property that

\[ (\forall z \in \mathbb{Z})(\forall y \in 2\mathbb{Z}) \ x \cdot y \in 2\mathbb{Z}. \]

So \( 2\mathbb{Z} \) is what we call an ideal of \( \mathbb{Z} \).

Are there other ideals of \( \mathbb{Z} \), and why do we care about them? We will see in a later section that we can form a new ring from an ideal, which in some sense inherits the basic properties of the original ring but we collapse the ideal so that anything in it is treated like “zero”.

**Example 3.2.2 (A more elaborate example).** *Take all of the integers 7\( \mathbb{Z} \) that are multiples of 7.* Again, if we multiply something inside of 7\( \mathbb{Z} \) with something outside of 7\( \mathbb{Z} \), the result lies inside 7\( \mathbb{Z} \). But there is more we can do with this interesting set of numbers. We can consider all translates of this set:

\[
\begin{align*}
1 + 7\mathbb{Z} := \{\ldots, -13, -6, 1, 8, 15, 22, \ldots\} \\
2 + 7\mathbb{Z} := \{\ldots, -12, -5, 2, 9, 16, 23, \ldots\} \\
3 + 7\mathbb{Z} := \{\ldots, -11, -4, 3, 10, 17, 24, \ldots\} \\
4 + 7\mathbb{Z} := \{\ldots, -10, -3, 4, 11, 18, 25, \ldots\} \\
5 + 7\mathbb{Z} := \{\ldots, -9, -2, 5, 12, 19, 26, \ldots\} \\
6 + 7\mathbb{Z} := \{\ldots, -8, -1, 6, 13, 20, 27, \ldots\} \\
7 + 7\mathbb{Z} := \{\ldots, -7, 0, 7, 14, 21, 28, \ldots\}
\end{align*}
\]

Notice that the last example gives us 7\( \mathbb{Z} \) back again, and they will keep repeating when we use higher values for the translate. For example
15 + 7\mathbb{Z} is the same as 1 + 7\mathbb{Z}, since 15 \equiv 1 \mod 7.

These sets themselves form a ring\(^3\) if we consider the following operations:

**Addition:** \((a + 7\mathbb{Z}) \oplus (b + 7\mathbb{Z}) := (a \oplus_7 b) + 7\mathbb{Z}\)

**Multiplication:** \((a + 7\mathbb{Z}) \otimes (b + 7\mathbb{Z}) := (a \otimes_7 b) + 7\mathbb{Z}\)

You might notice here that what we end up with is really not a new ring at all: it looks and behaves just like \(\mathbb{Z}/7\mathbb{Z}\)! The idea of rings being the same is pursued further in a later course.

**Lemma 3.2.3.** The only ideals of \(\mathbb{Z}\) are of the form \(n\mathbb{Z}\) for some integer \(n \geq 2\).

\(^*\)\ **Proof:** To be done in lectures. \(\square\)

We will come back to ideals later once we have done equivalence relations and polynomial rings.

### 3.3 An important interlude: Equivalence relations, partitions and quotients

We saw in the previous section an example of a partition of a set. A more common example is the division of the population of Australia into states and territories.

**Definition 3.3.1 (Partition).** Let \(\mathcal{P}\) a collection of non-empty subsets of a set \(S\). We say that \(\mathcal{P}\) is a partition of \(S\) if it satisfies the following:

- **Covers \(S\):** Every element of \(S\) lies in some element of \(\mathcal{P}\). In other words, \(S = \bigcup \mathcal{P}\).

- **Disjointness:** For every pair \(P_1, P_2 \in \mathcal{P}\), we have \(P_1 \cap P_2 = \emptyset\). That is, different elements of \(\mathcal{P}\) are disjoint.

The elements of the partition are sometimes called **cells** or **parts** of the partition.

**Example 3.3.2.** The even and odd integers form a partition of the integers. As a partition, we would write it as

\(\{E, O\}\)

where \(E\) is the set of even integers and \(O\) is the set of odd integers. So a partition\(^4\) is a “set of sets”. So in this sense, the set of integers is like the population of Australia, only we divide it up according to West Australians and non-West Australians!

**Example 3.3.3.** The singleton subsets \([s]\) of a set \(S\) form a partition, and we would write it as

\(\mathcal{P} := \{[s] : s \in S\}\).

For example, the collection of singleton subsets of \(\{1, 2, 3, 4, 5\}\) are

\(\{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}\).

\(^3\) This is the first time you’ve really seen some high-order abstractness!

\(^4\) One of the most common difficulties we see in this course is that the student does not understand that a partition is a set of sets. That is why I deliberately used the term “collection” in the definition to make this clear.
The whole set $S$ itself gives a partition with just one part!

$$P := \{ S \}.$$ 

These two examples are considered the trivial partitions of a set.

**Example 3.3.4.** The translates of an ideal of a ring form a partition of the ring. For the example we saw in the last section, we have that

$$\{ 7\mathbb{Z}, 1 + 7\mathbb{Z}, 2 + 7\mathbb{Z}, 3 + 7\mathbb{Z}, 4 + 7\mathbb{Z}, 5 + 7\mathbb{Z}, 6 + 7\mathbb{Z} \}$$

is a partition of $\mathbb{Z}$ with seven parts, and each part is an infinite subset.

Recall that the “disjointness” part of the definition of a partition requires us to prove that if $P_1 \neq P_2$, then $P_1 \cap P_2 = \emptyset$. The contrapositive of this statement is equivalent: If $P_1 \cap P_2 \neq \emptyset$, then $P_1 = P_2$. I have found it is easier to prove the contrapositive statement than the original one! You will see when you try it.

Now we will look at particular relations known as equivalence relations. But first, some examples and some jargon. Let $\sim$ be a relation on a set $X$. Then:

- **is reflexive if**: $x \sim x$ for all $x \in X$;
- **is symmetric if**: $x \sim y$ implies $y \sim x$ (for all $x, y \in X$);
- **is transitive if**: $x \sim y$ and $y \sim z$ implies $x \sim z$ (for all $x, y, z \in X$).

**Example 3.3.5.**

- “friendship” is an equivalence relation (at least it should be!), since everyone is a friend of themselves (reflexivity), if I’m a friend of you then you’re a friend of me (symmetry), and a friend of a friend is a friend (transitivity).
- “$<$” is not an equivalence relation on $\mathbb{R}$ as it is not reflexive.
- “$\leq$” is not an equivalence relation on $\mathbb{R}$ as it is not symmetric (but it is reflexive and transitive!).
- By Lemma 2.5.4, $\equiv_n$ is an equivalence relation.
- Equality is an equivalence relation.

**Definition 3.3.6** (Equivalence classes). Let $\sim$ be a relation on a set $X$. Then for each $x \in X$, the equivalence class containing $x$ is the set

$$[x] := \{ y \in X : y \sim x \}.$$
Example 3.3.7.

- For the “friendship” is equivalence relation the equivalence class containing you is the set of all your friends.
- For congruence modulo 7, we have the following congruence classes:

\[
\begin{align*}
[0] & = 7\mathbb{Z}, \\
[1] & = 1 + 7\mathbb{Z}, \\
& \cdots \\
[6] & = 6 + 7\mathbb{Z}.
\end{align*}
\]

Notice in this example that we could write \([7]\) for \([0]\), we could write \([-13]\) for \([1]\). There are many ways to write down any equivalence class.

Example 3.3.8 (Example: Spokes-people of soccer teams). Suppose we have a soccer competition with 12 teams. So the set of S players in the competition, is split up into 12 teams, or in other words, the teams are a partition of S. Each team has a spokes person who does nothing more than say “we’ll take one week at a time” and “the boys tried really hard today”. To identify a team you could just identity the spoke-person. For example, “Tom Richards” team is the same as saying “the Numbats”. But one day, Tom Richards is deposed of being spokes-person, and another person, from his team, Bill Bates, is put in his place. It doesn’t matter much because this spokes-person can also recite the same things that Tom says every week. So to identify the “the Numbats” I could also say “Bill Bates’ team”.

The tale above is about representatives of an equivalence class. The equivalence relation here is “being in the same team”. So we see that a partition gives rise to an equivalence relation, and vice-versa. In the mathematical example we see above, the congruence modulo 7 relation gives us a partition of Z. This phenomenon is one of the most important concepts in pure mathematics.

Theorem 3.3.9 (The Equivalence Relation Theorem). The equivalence classes of an equivalence relation on a set X forms a partition of X. Conversely, a partition \(\mathcal{P}\) of X yields an equivalence relation on X defined by \(x_1 \sim_{\mathcal{P}} x_2\) if and only if \(x_1\) and \(x_2\) belong to the same part of \(\mathcal{P}\).

\[\text{Proof:}\] To be done in lectures.

Lemma 3.3.10. Let \(\sim\) be an equivalence class on a set X, and let \(x, y \in X\). Then the following are equivalent:

(i) \(x \sim y\)

(ii) \(x \in [y]\)

(iii) \([x] = [y]\).

\[\text{Proof:}\] We will show that (iii) \(\implies\) (ii) \(\implies\) (i) \(\implies\) (iii).

(iii) \(\implies\) (ii): Suppose \([x] = [y]\). By reflexivity, \(x \in [x]\) and so \(x \in [y]\).

(ii) \(\implies\) (i): Suppose \(x \in [y]\). Then, by definition of \([y]\), we have \(x \sim y\).
(i) \(\implies\) (iii): Suppose \(x \sim y\). In order to show that \([x] = [y]\), we need to show that \([x] \subseteq [y]\) and \([y] \subseteq [x]\). Let \(z \in [x]\). Then \(z \sim x\), and so by transitivity, \(z \sim y\). Therefore, \(z \in [y]\) and \([x] \subseteq [y]\). Conversely, if \(w \in [y]\), we have \(w \sim y\). By symmetry, \(y \sim x\) and then by transitivity \(w \in x\). Therefore, \(w \in [x]\) and \([y] \subseteq [x]\). Thus, \([x] = [y]\).

\[\blacksquare\]

**Definition 3.3.11 (Quotient).** The set of all equivalence classes of an equivalence relation \(\sim\) of a set \(X\) is called the quotient of \(X\) by \(\sim\).

We will see a classical example of a quotient in the next section.

### 3.4 A construction of the rational numbers

Let \(X\) be equal to the Cartesian product \(Z \times (Z \setminus \{0\})\). This is the set of all ordered pairs \((a, b)\) of integers where \(b \neq 0\). Let \(\sim\) be the relation on \(X\) defined by

\[(a, b) \sim (a', b') \iff ab' = a'b.\]

It turns out that \(\sim\) is an equivalence relation:

**Reflexivity:** Let \((a, b) \in X\). Then \(ab\) is certainly equal to itself, and hence \((a, b) \sim (a, b)\).

**Symmetry:** Let \((a, b), (a', b') \in X\) and suppose that \((a, b) \sim (a', b')\). Then \(ab' = a'b\). Since ‘\(=\)’ is symmetric, we know that \(a'b = ab'\). Therefore, \((a', b') \sim (a, b)\).

**Transitivity:** Let \((a, b), (a', b'), (a'', b'') \in X\) and suppose that \((a, b) \sim (a', b')\) and \((a', b') \sim (a'', b'')\). Then \(ab' = a'b\) and \(a'b'' = a''b'\). Now we can multiply the first of these equations through by \(b''\) and obtain

\[ab'b'' = a''b'b.\]

We can then use the second equation to substitute \(a''b'\) in for \(a'b''\):

\[ab'b'' = a''b'b = (a'b'')b = (a''b')b.\]

Since \(b'\) is nonzero, we can divide each side by \(b'\):

\[ab'' = a''b.\]

Therefore, \((a, b) \sim (a'', b'')\).

So all three properties of an equivalence relation are satisfied. It will be interesting now to compute a few equivalence classes.

\[
\begin{align*}
[[1, 1]] &= \{(a, b) \in X : a = b\} = \{(a, a) : a \in Z \setminus \{0\}\} \\
[[1, 2]] &= \{(a, b) \in X : 2a = b\} = \{(a, 2a) : a \in Z \setminus \{0\}\} \\
[[3, 5]] &= \{(a, b) \in X : 5a = 3b\} = \{(3a, 5a) : a \in Z \setminus \{0\}\}
\end{align*}
\]

Perhaps we could write down a convenient shorthand for an equivalence class \([a, b]\)? How about

\[[(a, b)] \rightarrow \frac{a}{b}\]

Voilé! We see that the rational numbers are nothing else but the quotient of \(X\) by the equivalence relation \(\sim\).
3.4.1 Addition and multiplication on the rationals

In primary school we learnt how to add fractions:

\[
\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{cd}.
\]

We can see by our construction in the previous section what this looks like in terms of an operation on equivalence classes:

\[
[(a, b)] + [(c, d)] := [(ad + bc, cd)].
\]

Likewise for multiplication:

\[
[(a, b)] \times [(c, d)] := [(ac, bd)].
\]

3.4.2 The field of fractions of a ring

The construction of the reals in the previous section is an example of the construction of the field of fractions of a ring \( R \).

**Definition 3.4.1** (Field of fractions). Let \( R \) be a ring that has no zero-divisors\(^5\). Let \( X = R \times R \setminus \{0\} \) and let \( \sim \) be the equivalence relation defined by

\[
(a, b) \sim (a', b') \iff ab' = a'b.
\]

Define \( \text{Frac}(R) \) to be the set of equivalence classes of \( \sim \) equipped with the following operations:

**Addition**: \( [(a, b)] + [(c, d)] := [(ad + bc, cd)] \).

**Multiplication**: \( [(a, b)] \times [(c, d)] := [(ac, bd)] \).

It turns out (see Exercise 3.15.2) that the operations of addition and multiplication on \( \text{Frac}(R) \) are well-defined and that \( \text{Frac}(R) \) is in fact a field! The multiplicative identity is \( [(1, 1)] \), where 1 is the multiplicative identity of \( R \), and a non-zero element \( [(a, b)] \) has multiplicative inverse \( [(b, a)] \). Notice that \( a \) and \( b \) need not have multiplicative inverses in \( R \)! So we saw that the rational numbers are realised as \( \text{Frac}(\mathbb{Z}) \), where we make a shorthand notation for the element \( [(a, b)] \) be writing a fraction \( \frac{a}{b} \). Here are some other examples.

**Example 3.4.2.**

- If \( R \) is a field, then \( \text{Frac}(R) \) gives us a field that is equivalent to the original field \( R \). So \( \text{Frac}(\mathbb{Q}) \) is the same as \( \mathbb{Q} \) and \( \text{Frac}(\mathbb{R}) \) is the same as \( \mathbb{R} \).

- Let \( \mathbb{R}[x] \) be the set of polynomials with real coefficients. Then \( \text{Frac}(\mathbb{R}[x]) \) is the set of rational functions.

- We will see in the last chapter another interesting construction, whereby the \( p \)-adic rationals are the field of fractions of the \( p \)-adic integers.
### 3.5 Geometric things as quotients

Let $I$ be the unit interval $[0, 1]$. These are the real numbers $x$ satisfying $0 \leq x \leq 1$. Now take the Cartesian product $I \times I$. We can see this geometrically in the Cartesian plane.

Consider the following relation $\sim$ on $I \times I$:

$$(x, y) \sim (x', y') \iff y = y' \text{ and } (x = x' \text{ or } |x - x'| = 1).$$

It turns out that $\sim$ is an equivalence relation! Let’s see what it means geometrically. We see that if we take a point on the left-hand side of the square, then it is equivalent to a point on the right-hand side of the square at the same longitude. So what we are doing is identifying the sides of the square. We can think of curling the plane until the sides of the square meet; we end up with a cylinder! So geometrically, we can model the quotient of $I \times I$ by $\sim$ with a cylinder.

We can also model some other surfaces with equivalence relations, and this will be explored in the Appendix.

### 3.6 Polynomials are like numbers

We have seen polynomials in high school, such as

$$x^3 + 3x^2 + 1$$

and the emphasis there was to understand their sets of values, to draw graphs of these values and find out when they are zero. We will not be so interested in their values, rather, we will be interested in polynomials as objects themselves and their entirety. This is what we have been doing with numbers; we are not interested in single numbers on their own, rather about the properties of numbers in general and how they interact.

**Definition 3.6.1 (Polynomial).** A polynomial over a ring $R$ is an expression

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where the $a_i$ are elements of $R$, called the coefficients of the polynomial.

So in other words, the powers of $x$ are essentially place holders for the coefficients. We could have easily defined polynomials as $(n + 1)$-tuples $(a_n, a_{n-1}, \ldots, a_1, a_0)$, but as we shall see later, there are some advantages in having easily digestible notation for polynomials.

**Example 3.6.2.**

**Constant polynomials** We will use the functional notation $a$ for the constant function $x \mapsto a$, where $a$ is a fixed element of a given ring. We will also use this notation for the constant polynomial.

**Polynomials of matrices** Recall that the set of $n \times n$ matrices over a ring $R$ form another ring $M_{n \times n}(R)$. We can then consider polynomials of matrices. For example, the characteristic polynomial of

$$\begin{pmatrix} 2 & 0 \\ -1 & 1 \end{pmatrix}$$

is $x^2 - 3x + 2$. 
Now we can add polynomials simply by adding corresponding coefficients, and multiplying polynomials is just like you did in high school. For example,
\[(x^2 + 3)(x + 1) = x^3 + x^2 + 3x + 3.\]
So the polynomials have an addition operation and a multiplication operation, we also have a zero polynomial, and multiplying by the constant polynomial \(1\) does not change a polynomial.

**Definition 3.6.3 (Polynomial ring).** The set of all polynomials \(R[x]\) over \(R\) is a ring, called the polynomial ring of \(R\).

Here are some technical things we need to care about, to avoid confusion. The largest number \(i\) such that \(a_i \neq 0\) is called the degree of the polynomial \(f = a_0x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0\) and the shorthand notation is \(\deg(f)\). If \(a_i = 0\), we ignore writing this term of the polynomial down. We will also write \(x^i\) when the coefficient is 1.

As a convention, the degree of the zero polynomial is \(-1\), whereas it is 0 for all other constant polynomials.

**Example 3.6.4.** Let \(R\) be a ring and let \(P\) be the set of elements of \(R[x]\) that have degree 0 or \(-1\). Then \(P\) is just like \(R\)! The function
\[
a_0 \mapsto a_0
\]
is a bijection from \(P\) to \(R\). Not only is it a bijection, but it is compatible with the operations of each ring\(^6\).

Earlier, we asked the question of which elements of \(\mathbb{Z}_n\) had multiplicative inverses (i.e., units). Similarly, some polynomial rings have nonzero elements which do not have multiplicative inverses.

**Example 3.6.5.** Recall that in \(\mathbb{Z}_6\), the elements 1 and 5 are units since \(1 \otimes_6 1 = 1\) and \(5 \otimes_6 5 = 1\). However, none of the other elements do! For example, there is no element \(b \in \mathbb{Z}_6\) such that \(2 \otimes_6 b = 1\), and so 2 is not a unit of \(\mathbb{Z}_6\).

By Lemma 3.1.8, \(x \in \mathbb{Z}_n\) is a unit if and only of \(\gcd(x, n) = 1\). What happens for polynomials?

**Example 3.6.6.** Consider the degree 1 polynomial \(x\) in \(R[x]\). Is it a unit? If it was a unit, then there would exist a nonzero polynomial \(g\) such that \(x \cdot g = 1\). Let us suppose that\(^7\)
\[
g := a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0.
\]
Then \(x \cdot g\) would be
\[
a_nx^{n+1} + a_{n-1}x^n + \cdots + a_1x^2 + a_0x
\]
and so would have degree \(n + 1\). Since 1 has degree 0, it follows that \(n = -1\) and so \(g\) is the zero polynomial – a contradiction! Therefore, \(x\) is not a unit in \(R[x]\).

\(^6\) Aside: A function \(f\) from a ring \(R_1\) to a ring \(R_2\) is a homomorphism if for all \(r, r' \in R\), we have
\[
\bullet \quad f(r + r') = f(r) + f(r').
\]
\[
\bullet \quad f(r \cdot r') = f(r) \cdot f(r').
\]
If \(f\) is also a bijection, then we say that \(R_1\) and \(R_2\) are isomorphic (greek: same shape), which means that \(R_1\) and \(R_2\) are essentially the same up to re-labelling.

\(^7\) It is wrong to divide by \(x\) here! I have seen before in this course that students feel compelled to work with this equation as it is presented to them. So they will often write “thus \(g = 1/x\)”. This assumes that we can do division in \(R[x]\), and the point of this example, is that we can’t.
The main theme of this section is to explore number-theoretic analogues of polynomial rings. It is remarkable how number-like the polynomials behave. The fundamental relation that we need in order to understand the multiplicative structure of a polynomial ring is divisibility; as was the case for the integers in order to establish important properties such as Bézout’s identity and the canonical factorisation into products of primes.

**Definition 3.6.7** ("Divides" relation). Let $g$ and $h$ be two polynomials in $R[x]$, where $R$ is a ring. We say that $g$ divides $h$, and write $g \mid h$, if there exists a polynomial $k \in R[x]$ such that

$$gk = h.$$ 

**Example 3.6.8.** Consider $x + 1, x^2 - 1$ in $\mathbb{Q}[x]$. Since $(x + 1)(x - 1) = x^2 - 1$, we see that $x + 1 \mid x^2 - 1$.

### 3.6.1 Long division

One of the most important things we learn, or should be learning, in school is long division. There are a number of reasons for this: (i) it is the only true mathematical algorithm we learn in school, (ii) long division works for the integers and not the real numbers (because of the Division Rule, Lemma 2.1.4), (iii) to get a grip on what a rational number is as a decimal expansion.

I will not revise long division of numbers here, but rather show how it is done with polynomials, by example.

**Example 3.6.9.** We would like to divide $x^4 + 4x^3 - x + 5$ by $x^2 + 2x - 1$ to find a remainder and quotient. (Write this out in the box below).

---

**Lemma 3.6.10** (The Division Rule for polynomials). Let $f, g \in F[x]$ where $F$ is a field. Then there exist elements $q, r \in F[x]$ satisfying

$$f = qg + r$$

and

$$\deg(r) < \deg(g).$$

**Proof:** The proof essentially is an application of long division. See the lectures.  

---

\* Why is a field necessary and why does it not work for rings? See Exercise 3.15.3.
A polynomial is \textit{monic} if its leading coefficient is 1.

\textbf{Definition 3.6.11} (Greatest common divisor for polynomials). The greatest common divisor \( \gcd(f, g) \) of two polynomials \( f, g \) of a polynomial ring \( F[x] \) (where \( F \) is a field) is the (unique) monic polynomial \( d \in F[X] \) such that:

(i) \( d \mid f, d \mid g; \)

(ii) if \( h \mid f \) and \( h \mid g \), then \( h \mid d. \)

The \textit{uniqueness} part of the definition follows from Lemma 3.6.10.

\textbf{Example 3.6.12.} Let \( R = \mathbb{Q} \) and consider \( f = x^3 + x - 2 \) and \( g = x^4 - 1. \) Then \( \gcd(f, g) = x - 1. \)

How did we find the greatest common divisor of \( f \) and \( g \) in the last example? Well, the Euclidean Algorithm works for polynomials just as it did for integers.

\textbf{Lemma 3.6.13} (Behind Euclid’s Algorithm for polynomials). Let \( F \) be a field and let \( f \) and \( g \) be elements of \( F[x]. \) If \( f = qg + r \) then \( \gcd(f, g) = \gcd(r, g). \)

\( \diamond \) \textbf{Proof:} The proof is similar to its analogue, Lemma 2.1.7. Suppose \( d \) is a divisor of both \( f \) and \( g. \) Then \( d \) divides \( f - qg \) and so \( d \) divides both \( r \) and \( g. \) Therefore every divisor of both \( f \) and \( g \) is also a divisor of \( r. \) Conversely, suppose \( d \) is a divisor of both \( g \) and \( r. \) Then \( d \) divides \( qg + r \) and hence \( d \) divides \( f. \) Therefore every divisor of both \( g \) and \( r \) is also a divisor of \( f. \) Moreover, the monic polynomials that divide \( f \) and \( g \) are the same set of monic polynomials that divide \( r \) and \( g. \) Therefore, \( \gcd(f, g) = \gcd(r, g). \)

\( \square \)

\textbf{Example 3.6.14.} We will now use the Euclidean Algorithm, but with polynomials as input, to find the greatest common divisor of \( f = x^3 + x - 2 \) and \( g = x^4 - 1. \) (We implicitly use long division throughout).

\[
\begin{array}{c|c|c}
  x & x^4 - 1 & x^3 + x - 2 \\
  -x - 2 & -x^2 + 2x - 1 & \\
  -\frac{1}{4}x + \frac{1}{4} & 4x - 4 & 0 \\
\end{array}
\]

So the last remainder here is \(-\frac{1}{4}x + \frac{1}{4}, \) which we can simply scale by \(-4\) to obtain a monic polynomial dividing both \( f \) and \( g. \) That is, \( \gcd(f, g) = x - 1. \)

In the last example, we saw rational numbers that are not integers appearing in the left-hand column. This is why it is necessary for the polynomial ring to be defined over a field. It would not ‘work’ if we used \( \mathbb{Z} \) instead of \( \mathbb{Q} \) in the last example.

A consequence of the Euclidean Algorithm for polynomials is a Bézout identity for polynomials.
Lemma 3.6.15 (Bézout for polynomials). Let \( f, g \) be two polynomials in \( F[x] \). Then there exist two polynomials \( m, n \in F[x] \) such that

\[
\gcd(f, g) = m \cdot f + n \cdot g.
\]

The next theorem gives us a way to easily check for affine divisors of polynomials.

Theorem 3.6.16 (The Factor Theorem). Let \( f \in F[x] \) and let \( c \in F \). Then \( f(c) = 0 \) if and only if the polynomial \( x - c \) divides \( f \).

\[ \text{Proof: To be done in lectures.} \]

Corollary 3.6.17. If \( f \in F[x] \) has degree \( d \), then \( f \) has at most \( d \) zeroes in \( F \).

\[ \text{Proof: To be done in lectures.} \]

3.7 Irreducibility and factorisation

Throughout this section, \( F \) will be a field. The irreducible polynomials are to \( F[x] \) what prime numbers are to \( \mathbb{Z} \).

Definition 3.7.1 (Irreducible polynomial). A polynomial \( p \in F[x] \) whose only divisors are constant polynomials and constant multiples of itself is said to be irreducible (over \( F \)).

Example 3.7.2. It is important what the field is that we are referring to. For example, \( x^2 + 2 \) is irreducible when considered as an element of \( \mathbb{Q}[x] \), however, it is reducible if we consider it as an element of \( \mathbb{R}[x] \):

\[
x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).
\]

Lemma 3.7.3 (Euclid’s Lemma for polynomials). Let \( p \in F[x] \) be irreducible over \( F \) and let \( f, g \in F[x] \). If \( p \mid f \cdot g \) then \( p \mid f \) or \( p \mid g \).

\[ \text{Proof: Suppose } p \text{ divides } f \cdot g \text{ but } p \text{ does not divide } f. \text{ Then } \gcd(p, f) \text{ is the constant polynomial } 1, \text{ since } \gcd(p, f) \text{ is a monic polynomial properly dividing the irreducible polynomial } p. \text{ So by Lemma 3.6.15 there exist polynomials } m, n \in F[x] \text{ such that}
\]

\[
1 = m \cdot f + n \cdot p.
\]

If we multiply through by \( g \), we see that

\[
g = m \cdot (f \cdot g) + n \cdot p \cdot g
\]

and we know that \( p \) divides the bracketed term above. So \( p \) divides the right-hand side and hence \( p \) divides \( g \). Therefore, if \( p \) does not divide \( f \), then \( p \) divides \( g \) (which is logically equivalent to proving “\( p \) divides \( f \) or \( p \) divides \( g \)”).

\[ \text{Proof: To be done in lectures.} \]

Theorem 3.7.4 (Fundamental Theorem of Polynomial Arithmetic). The factorisation of a polynomial in \( F[x] \) into irreducible factors is unique up to ordering and constant factors.

We will not prove this result as it is almost identical to the Fundamental Theorem of Arithmetic, with just polynomials put in place of integers and “irreducible” put in place of “prime” (Theorem 2.2.2).
3.8 Gauß’s Lemma

Here we look at when polynomials are irreducible over the integers.

**Definition 3.8.1** (Content of a polynomial). The content $I(f)$ of a polynomial $f \in \mathbb{Z}[x]$ is the greatest common divisor of its coefficients.

**Example 3.8.2.** So $I(30x^3 - 18x^2 + 9) = 3$.

**Theorem 3.8.3** (The Content Theorem). If $f, g \in \mathbb{Z}[x]$, then $I(fg) = I(f)I(g)$.

**Proof:** Let $f' = f/I(f)$ and $g' = g/I(g)$. Notice that these new polynomials both have integer coefficients, because the gcd of the coefficients divides each coefficient. Hence $I(f') = I(g') = 1$. Now $f \cdot g = f' \cdot g' I(f)I(g)$, and so

$$I(f \cdot g) = I(f')I(g')I(f)I(g).$$

So it suffices to show that $I(f' \cdot g') = 1$. Suppose $f' = a_m x^m + \cdots + a_1 x + a_0$ and $g' = b_n x^n + \cdots + b_1 x + b_0$, and suppose for a proof by contradiction that there is some prime number $p$ dividing $I(f' \cdot g')$. That is, $p$ divides each coefficient of $f' \cdot g'$. Now the contents of $f'$ and $g'$ are both equal to 1, so there is a least $i$ and a least $j$ such that $p$ does not divide $a_i$ and $p$ does not divide $b_j$. However, the coefficient of $x^{i+j}$ in $f' \cdot g'$ is not divisible by $p$, and this coefficient is

$$a_i b_{i+j} + a_i b_{i+j-1} + \cdots + a_i b_j + a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0.$$

This is a contradiction since $p$ divides all terms above, except $a_i b_j$. Therefore, $I(f' \cdot g') = 1$. □

**Lemma 3.8.4** (Gauß’s Lemma). Let $g$ and $h$ be two monic polynomials in $\mathbb{Q}[x]$. If $g \cdot h$ has integer coefficients, then so too have $g$ and $h$. That is, $g \cdot h \in \mathbb{Z}[x] \implies g, h \in \mathbb{Z}[x]$.

**Proof:** To be done in lectures. □

So this means that if a polynomial with integer coefficients is reducible over $\mathbb{Q}$, then it is also reducible over $\mathbb{Z}$. Moreover, the factorisation of a polynomial over $\mathbb{Z}$ into irreducibles is unique up to order and signs (multiplying by $-1$).

3.9 Eisenstein’s Criterion

There is an industry of “computational number theory” behind finding ways to determine if an integer is a prime number or not, and it has applications to cryptography and information security. One of the most basic “primality tests” comes from Fermat’s Little Theorem: to determine if a number $n$ is prime, we choose random integers $a$ satisfying $1 \leq a < p$ and test to see if $a^{n-1} \equiv 1$ holds. In this section, we look at one of the most basic tests for the irreducibility of a polynomial.
**Theorem 3.9.1** (Eisenstein’s Irreducibility Criterion). If \( f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \) and \( p \) is a prime number dividing each coefficient \( a_i \) where \( i \in \{0, 1, \ldots, n-1\} \), but \( p^2 \) does not divide \( a_0 \), then \( f \) is irreducible over \( \mathbb{Q} \).

\( \diamond \) Proof: To be done in lectures. \( \square \)

**Example 3.9.2.** The polynomial \( x^4 + 3x^2 + 15x + 6 \) is irreducible over \( \mathbb{Q} \), since 3 divides each non-leading coefficient, but 9 does not divide the constant coefficient.

**Example 3.9.3.** It is not difficult to prove that \( x^3 - 3x - 1 \) is irreducible over \( \mathbb{Q} \) by noticing that if it was reducible, then it would have a linear factor, and then we simply observe that there are no rational roots of this polynomial, and then we apply the Factor Theorem (3.6.16). There is another way, and it involves substitution.

**Lemma 3.9.4.** Let \( f \) be a polynomial in \( \mathbb{Z}[x] \) of the form
\[
f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0
\]
and let \( g \) be another polynomial in \( \mathbb{Z}[x] \) of the form \( g = x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \). Let \( f \circ g \) be the polynomial where we have substituted \( g \) for the indeterminate \( x \) of \( f \), to obtain another a monic polynomial of \( \mathbb{Z}[x] \) of degree \( mn \). If \( f \circ g \) is irreducible over \( \mathbb{Q} \), then so too is \( f \).

\( \diamond \) Proof: We will prove the contrapositive. Suppose \( f \) is reducible over \( \mathbb{Q} \). Then \( f = a \cdot b \) for two polynomials \( a, b \in \mathbb{Q}[x] \). We see than that \( f \circ g \) would factorise as \( a \circ g \) and \( b \circ g \), and hence \( f \circ g \) is reducible over \( \mathbb{Q} \). \( \square \)

**Example 3.9.5.** Let \( f = x^3 - 3x - 1 \). We substitute \( g = x + 1 \) to create a polynomial \( f \circ g \) that we can apply Eisenstein’s Criterion to:
\[
f \circ g = (x + 1)^3 - 3(x + 1) - 1 = x^3 + 3x^2 + 3x + 1 - 3x - 3 - 1 = x^3 + 3x^2 - 3.
\]
So we see that 3 divides the non-leading coefficients and 9 does not divide the constant coefficient. Therefore, by Eisenstein’s Criterion (Theorem 3.9.1), \( f \circ g \) is irreducible over \( \mathbb{Q} \), and so by Lemma 3.9.4, \( f \) is also irreducible over \( \mathbb{Q} \).

3.10 Clock arithmetic on polynomials

So far, we have seen that polynomials behave a little bit like numbers: we have a Division Rule for \( F[x] \), we have the greatest common divisor function and the Euclidean Algorithm, and we have a notion of prime numbers (i.e., the irreducible polynomials). We will now look at clock arithmetic on \( R[x] \) and an analogue of the ring \( \mathbb{Z}_n \) of integers modulo \( n \).

**Definition 3.10.1** (Congruence modulo a polynomial). Let \( p \) be a polynomial in \( R[x] \). Define \( \equiv_p \) on \( R[x] \) by
\[
f \equiv_p g \iff p \mid f - g.
\]

**Lemma 3.10.2.** \( \equiv_p \) is an equivalence relation on \( R[x] \).
Proof:

Reflexivity: Let $f \in R[x]$. Clearly, $p$ divides the zero polynomial, and so $f \equiv_p f$.

Symmetry: Suppose $f \equiv_p g$. Then $p$ divides $f - g$, and hence $p$ divides $-(f - g) = g - f$. Therefore, $g \equiv_p f$.

Transitivity: Suppose $f \equiv_p g$ and $g \equiv_p h$. Then $p$ divides $f - g$ and $p$ divides $g - h$. So $p$ divides the sum of $f - g$ and $g - h$, and hence $p$ divides $f - h$. Therefore, $f \equiv_p h$. □

Recall that the quotient of $R[x]$ by $\equiv_p$ is the set of equivalence classes of $\equiv_p$, the congruence classes modulo $p$. We will write $R[x]/\equiv_p$ for this quotient. We can also define addition and multiplication on $R[x]/\equiv_p$ in the following natural way:

Definition 3.10.3 (Addition and multiplication on $R[x]/\equiv_p$). For all polynomials $a, a' \in R[x]$, let:

Addition: $[a] \oplus [a'] := [a + a']$;

Multiplication: $[a] \otimes [a'] := [aa']$.

We leave it as an exercise (see the Exercises at the end of this chapter) that the addition and multiplication operations defined above, are well-defined. Moreover,

Lemma 3.10.4. $R[x]/\equiv_p$ with the operations of addition and multiplication defined above (3.10.3) forms a ring.

The proof of this result is simple, but perhaps a little tedious, so we leave it to the reader to verify that it is a true statement.

Example 3.10.5. It is important now to give an example of how this all works, as we have probably presented the most abstract idea in this course; a quotient of a polynomial ring. Consider $R[x]$, the of polynomials with real coefficients, and let $p$ be the polynomial $x^2 + 1$. What does a congruence class modulo $p$ look like?

Let’s take the polynomial $f := x^5 + 3x^2 - 2$. When we do long division to $f$ modulo $p$, we find that

$$x^5 + 3x^2 - 2 = (x^3 - x + 3) \cdot p + x - 5.$$ 

In other words, we have a remainder of $x - 5$ when dividing $f$ by $p$. So $f \equiv_p x - 5$, or in other words,

$$[f] = [x - 5].$$

In fact, we will always obtain a remainder that is a constant polynomial or a linear polynomial, since the degree of the remainder has to be less than the degree of $p$. So every congruence class modulo $p$ is of the form

$$[ax + b]$$
for some \( a, b \in \mathbb{R} \). This quotient ring has a very interesting property. Consider the congruence class \([x]\) and multiply it by itself:
\[
[x] \otimes [x] = [x^2].
\]

Now \( p \) clearly divides the difference of \( x^2 \) and the constant polynomial \(-1\), so \( x^2 \equiv_{p} -1 \) and hence
\[
[x] \otimes [x] = [-1].
\]

Does this look familiar? Yes, there is a natural bijection\(^9\) between the quotient \( \mathbb{R}[x]/\equiv_p \) and the complex numbers given by:
\[
(ax + b) \mapsto b + ai.
\]

**Example 3.10.6** (A field with 4 elements). Consider the field \( \mathbb{Z}_2 \) consisting of the two elements 0 and 1. This itself is a quotient ring of \( \mathbb{Z} \), where 0 represents the even numbers and 1 represents the odd numbers. Recall that \( \mathbb{Z}_2 \) has the interesting property that \( 1 + 1 = 0 \). This makes the polynomial ring \( \mathbb{Z}_2[x] \) particularly interesting. Consider all of the quadratic polynomials of \( \mathbb{Z}_2[x] \):
\[
x^2, \quad x^2 + 1, \quad x^2 + x, \quad x^2 + x + 1.
\]

Clearly the first and third are reducible since \( x \) divides both of these. The second one also turns out to be reducible:
\[
(x + 1)(x + 1) = x^2 + x + x + 1 = x^2 + (1 + 1)x + 1 = x^2 + 0x + 1 = x^2 + 1.
\]

Now consider the polynomial \( x^2 + x + 1 \). If we do long division with each of the degree 1 polynomials\(^10\) of \( \mathbb{Z}_2[x] \), we will find that:
\[
x^2 + x + 1 = x(x) + x + 1
\]
\[
x^2 + x + 1 = x(x + 1) + 1.
\]

The denominators of our division are in the brackets above. So \( x^2 + x + 1 \) is irreducible. Call this polynomial \( p \). We will now look at the quotient of \( \mathbb{Z}_2[x] \) by \( \equiv_p \). Here are the equivalence classes of \( \equiv_p \):
\[
[0], \quad [1], \quad [x], \quad [x + 1]
\]

Notice, for example, that every polynomial of \( \mathbb{Z}_2[x] \) belongs to one of these equivalence classes. If we do long division by \( p \) we will always have a remainder that has degree 0 or 1, and the representatives of these equivalence classes above are precisely these polynomials. Note what happens when we add two equivalence classes:
\[
[x] \otimes_p [x + 1] = [x + x + 1] = [(1 + 1)x + 1] = [0x + 1] = [1].
\]

When we multiply, we must remember to take the remainder after dividing by \( p \):
\[
[x] \otimes_p [x + 1] = [x^2 + x] = [x^2 + x + 1 + 1] = [p + 1] = [1].
\]

Let us now look at the addition and multiplication tables of \( \mathbb{Z}_2[x]/\equiv_p \):

---

\(^9\) You can check that this really does work. If you add \([ax + b]\) and \([a'x + b']\), you get \([(a + a')x + (b + b')]\), and their product is \([(aa' + a'b')x + (ab' + a'b') + b'b']\).

\(^10\) The only degree 1 polynomials in \( \mathbb{Z}_2[x] \) are \( x \) and \( x + 1 \).
Notice that the multiplication tables are very different from the table we got for \( \mathbb{Z}_4 \) (see Example 3.1.5). First of all, if we delete the first row and column, we get a Latin square! In other words, \( \mathbb{Z}_2[x]/\equiv_p \) is a field.

**Theorem 3.10.7.** Let \( p \) be a polynomial in \( F[x] \), where \( F \) is a field. Then the quotient ring \( F[x]/\equiv_p \) is a field if and only if \( p \) is irreducible over \( F \).

\[ \begin{array}{c|cccc} \oplus_p & 0 & 1 & x & x+1 \\ \hline 0 & 0 & 1 & x & x+1 \\ 1 & 1 & 0 & x+1 & x \\ x & x & x+1 & 0 & 1 \\ x+1 & x+1 & x & 1 & 0 \\ \end{array} \]

\[ \begin{array}{c|cccc} \otimes_p & 0 & 1 & x & x+1 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & x & x+1 \\ x & x & x+1 & 1 & 1 \\ x+1 & 0 & x+1 & 1 & x \\ \end{array} \]

**Proof:** The multiplication operation \( \otimes_p \) on \( F[x]/\equiv_p \) is commutative, so in order to show that \( F[x]/\equiv_p \) is a field, we only need to show that every element has a multiplicative inverse. We prove the \( \Leftarrow \) direction first.

Suppose \( p \) is irreducible over \( F \), and let \( [f] \) be a nonzero equivalence class of \( \equiv_p \) (i.e., an element of \( F[x]/\equiv_p \)). To be nonzero, we mean that \( f \not\equiv_p 0 \), or in other words, \( p \) does not divide \( f \).

By Bézout’s identity for polynomials (Lemma 3.6.15), there exist polynomials \( m \) and \( n \) in \( F[x] \) such that

\[
\gcd(f, p) = m \cdot f + n \cdot p.
\]

Now \( \gcd(f, p) \) is a divisor of \( p \), and \( p \) is irreducible, so there are two possibilities:

(i) \( \gcd(f, p) = k \cdot p \) for some nonzero \( k \in F \), or

(ii) \( \gcd(f, p) \) is a constant polynomial, say \( k \).

The first case is impossible, since otherwise, we would have \( p \) dividing \( f \). Therefore, \( \gcd(f, p) = k \) and moreover, \( k \neq 0 \). So we divide through by the constant \( k \) and find that

\[
1 = \left(\frac{1}{k}m\right) \cdot f + \left(\frac{1}{k}n\right) \cdot p,
\]

or in other words, \( \left(\frac{1}{k}m\right) \cdot f \equiv_p 1 \). So \( \left(\frac{1}{k} \cdot m\right) \) is the multiplicative inverse of \( [f] \), and we have thus shown that \( F[x]/\equiv_p \) is a field.

Conversely, suppose \( p \) is NOT irreducible. Then there exist polynomials \( a, b \in F[x] \) such that \( p = a \cdot b \) and the degrees of \( a \) and \( b \) are smaller than the degree of \( p \). In particular, \( a \) and \( b \) are not divisible by \( p \) and so \( [a] \) and \( [b] \) are nonzero elements of \( F[x]/\equiv_p \). However,

\[
[a] \otimes_p [b] = [p] = [0]
\]

which shows that \( F[x]/\equiv_p \) has zero divisors. Therefore, \( F[x]/\equiv_p \) is not a field.

All up, we have shown that the quotient ring \( F[x]/\equiv_p \) is a field if and only if \( p \) is irreducible over \( F \). \( \square \)
3.11 Congruence modulo a polynomial and ideals

Here we see that there is a direct relationship between the equivalence classes of \( \equiv_p \) and the ideal generated by \( p \). The fancy term for this is a principal ideal.

**Definition 3.11.1 (Principal Ideal of \( R \)).** Let \( p \) be an element of a commutative ring \( R \). Then the following subset \( \langle p \rangle := \{ r \cdot p : r \in R \} \) is an ideal of \( R \) and is called the principal ideal generated by \( p \).

**Lemma 3.11.2.** Let \( p \) be an element of \( R[x] \), where \( R \) is a commutative ring. Then the equivalence classes of \( \equiv_p \) can be written as translates of the principal ideal \( \langle p \rangle \):

\[
[f] = f + \langle p \rangle.
\]

So the quotient \( R[x] / \equiv_p \) can be realised in the usual sense in ring theory, that it is a quotient \( R/I \) of a ring by an ideal. This is not an emphasis of this course, but will be in a later course on ring theory.

3.12 Algebraic versus transcendental

One the triumphs of abstract algebra was the solution to the famous three problems of antiquity. Using the basic constructions of Euclidean geometry, we can make numbers from old ones. If we are given a unit length, we can make the integers with a straight-edge and compass. In recent times, this beautiful part of mathematics has left the Australian secondary school curriculum, where in the past we enjoyed learning how to construct surds like \( \sqrt{5} \) using Euclidean geometry.

The three problems are about constructions in Euclidean geometry that use only a straight-edge and compass, and there are more details in Section 3.13.

**Doubling the cube (Eratosthenes 240 BC):**
Can we construct a cube whose volume is twice that of a given cube? \(^{12}\)

**Trisecting an arbitrary angle (at least Hippocrates 450 BC):**
Given an arbitrary angle, such as \( \pi/3 \), can we construct a third of this angle?

**Squaring the circle (Rhind papyrus 1650 BC):**
Can we construct a square whose area is equal to that of a given circle?

These problems can be rephrased in terms of algebraic numbers, and will be pursued in Section 3.13.

**Definition 3.12.1 (Algebraic number).** Let \( a \in \mathbb{C} \). If there is a nonzero polynomial \( f \in \mathbb{Q}[x] \) with \( f(a) = 0 \), then \( a \) is algebraic. Otherwise, \( a \) is transcendental.

**Example 3.12.2.**
- \( \sqrt{2} \) is algebraic since it is a zero of \( x^2 - 2 \).
- The complex number \( i \) is algebraic since it is a zero of \( x^2 + 1 \).

\(^{11}\) This is just a ring where the multiplication operation is commutative: \( a \cdot b = b \cdot a \) for all \( a, b \in R \).

\(^{12}\) Given the unit cube, a doubling would produce a cube with side length \( \sqrt[3]{2} \).
• The Golden Ratio \( \frac{1 + \sqrt{5}}{2} \) is algebraic since it is a zero of \( x^2 - x - 1 \).

• \( e \) and \( \pi \) are transcendental.\(^{13} \)

• Every rational number \( \frac{a}{b} \) is algebraic since it is a zero of \( x - \frac{a}{b} \).

It is still not known whether \( \pi + e \) or \( \pi \cdot e \) is transcendental, but we do know (see Exercise 3.15.7) that one of them is transcendental.

In the definition of an algebraic number, we can assume \( f \) is monic.

Lemma 3.12.3. Let \( f \in \mathbb{Q}[x] \) and \( c \in \mathbb{C} \) such that \( f(c) = 0 \). Then there is a unique monic irreducible polynomial \( m(x) \in \mathbb{Q}[x] \) such that \( m(x) = 0 \). Moreover, \( m | f \).

\* Proof: To be done in lectures. \( \square \)

The polynomial \( m(x) \) in Lemma 3.12.3 is called the minimal polynomial of \( c \).

Example 3.12.4. Let \( \alpha = 1 + \sqrt{2} \) and take \( f = x^2 - 2x - 1 \). Notice that \( \alpha^2 = 3 + 2\sqrt{2} \) and so \( \alpha \) is a zero of \( f \). How do we know if \( f \) is irreducible over \( \mathbb{Q} \)?

First way: Since \( f \) is quadratic, we know that it is reducible if it has a linear factor. So by Theorem 3.6.16 (see Exercise 3.15.4), we only need to look at the zeros of \( f \) and see if they are rational. Indeed, \( 1 + \sqrt{2} \) and \( 1 - \sqrt{2} \) are irrational!

Second way: We can use Eisenstein’s Criterion (Theorem 3.9.1) and Lemma 3.9.4. Substitute the polynomial \( g = x - 1 \) to obtain the polynomial \( f \circ g = (x - 1)^2 - 2(x - 1) - 1 = x^2 - 4x + 2 \). So we see that 2 divides the non-leading coefficients but 4 does not divide the constant coefficient. Hence, \( f \circ g \) is irreducible over \( \mathbb{Q} \), and so too is \( f \).

3.12.1 How big are the algebraic numbers?

Let \( \mathbb{A} \) be the set of algebraic numbers. In the Exercise 1.11.11 at the end of the last chapter, we saw there that \( \mathbb{C} \) is uncountable by noting that there is a bijection from \( \mathbb{R} \times \mathbb{R} \) to \( \mathbb{C} \), and the Cartesian product of uncountable sets yields an uncountable set. The rational numbers are a countable subset of \( \mathbb{A} \), and we see below that the size of \( \mathbb{A} \) is no bigger than the size of \( \mathbb{Q} \).

Theorem 3.12.5. \( \mathbb{A} \) is countable.

\* Proof: To be done in lectures. \( \square \)

Corollary 3.12.6. The set of transcendental numbers \( \mathbb{C} \setminus \mathbb{A} \) is uncountable.

\* Proof: Suppose the opposite, that \( \mathbb{C} \setminus \mathbb{A} \) is countable. Then by Theorem 1.8.4, we would have that \( (\mathbb{C} \setminus \mathbb{A}) \cup \mathbb{A} \) is countable, which is a contradiction as this set is \( \mathbb{C} \). \( \square \)

An important subset of the algebraic numbers, especially in algebraic geometry and group representation theory, is the set of algebraic integers.

Definition 3.12.7 (Algebraic integer). A zero of a monic polynomial of \( \mathbb{Z}[x] \) is called an algebraic integer.
Example 3.12.8.

- \( \sqrt{-2} \) is an algebraic integer as it is a zero of \( x^2 + 2 \) (whose coefficients are integers).
- Integers are algebraic integers\(^{14}\).
- \( \frac{1}{2} \) is not an algebraic integer.

**Lemma 3.12.9.** The rational algebraic integers are integers.

★ **Proof:** Let \( y \) be a rational algebraic integer, and write it in reduced form: \( y = \frac{m}{n} \) where \( \gcd(m, n) = 1 \). By definition of an algebraic integer, there exists a monic polynomial \( f \in \mathbb{Z}[x] \) such that \( f(y) = 0 \). Suppose \( f \) has degree \( k \). Then when we evaluate \( n^k \cdot f \) at \( \frac{m}{n} \), we get an expression of the form

\[
0 = m^k + a_{k-1} m^{k-1} n + \cdots + a_1 m n^{k-1} + a_0 n^k.
\]

Therefore, \( n \) divides \( m^k \) and hence\(^{15}\) \( n = 1 \). So, \( y \) is an integer. \( \square \)

Now we see how these sets of complex numbers behave under the usual arithmetic operations.

**Theorem 3.12.10.** The algebraic numbers \( A \) form a field and the algebraic integers form a ring.

† **Proof:** What we haven’t seen in this course is that we can describe algebraic numbers as eigenvalues of matrices with rational entries. Suppose \( c \) is an algebraic number with minimal polynomial \( f \). If we write \( f = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \), then it turns out that the minimal polynomial of \( f \) is in fact the characteristic polynomial of the following matrix:

\[
\begin{bmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 1 \\
-a_0 & -a_1 & -a_2 & \cdots & -a_{n-1}
\end{bmatrix}
\]

This matrix is known as the *companion matrix* of \( f \). So we use the following facts:

(i) \( c \) is an algebraic number if and only if \( c \) is an eigenvalue of a matrix over \( \mathbb{Q} \);

(ii) \( c \) is an algebraic integer if and only if \( c \) is an eigenvalue of a matrix over \( \mathbb{Z} \).

The Kronecker product \( A \otimes B \) of two matrices has \((i, j)\)-entry \( a_{ij} B \) where \( a_{ij} \) is the \((i, j)\)-entry of \( A \). For example

\[
\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \otimes \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 5 & 6 & 10 & 12 \\ 7 & 8 & 14 & 16 \\ 15 & 18 & 20 & 24 \\ 21 & 24 & 28 & 32 \end{bmatrix}
\]
This operation on matrices is particularly nice as it is compatible with matrix multiplication:

\[(A \otimes B)(C \otimes D) = AC \otimes BD.\]

In particular, \(C\) and \(D\) can be row vectors if we think of them as \(1 \times n\) matrices.

Let \(a\) and \(b\) be algebraic numbers. Then \(a\) is an eigenvalue of a matrix \(A\) over \(\mathbb{Q}\), and \(b\) is an eigenvalue of a matrix \(B\) over \(\mathbb{Q}\). It turns out that:

- \(a + b\) is an eigenvalue of \(A \otimes I + I \otimes B\), where \(I\) is an identity matrix of the appropriate size.
- \(a \cdot b\) is an eigenvalue of \(A \otimes B\).

We leave the details of these calculations to the interested reader. So we can show using the Kronecker product of matrices that the algebraic numbers are closed under addition and multiplication, and likewise for the algebraic integers. It then needs to be observed that the nonzero elements of the algebraic numbers have multiplicative inverses (just their reciprocal value).

\[\square\]

3.13 Aside: Constructible numbers

Here are the rules of the game:

1. We have an initial position of points \(\{P_0, P_1, P_2, \ldots, P_m\}\)

2. **Operation 1**: Draw a line through two old points \(P_i\) and \(P_j\) to get new points where this line intersects other lines and circles.

3. **Operation 2**: Draw a circle with centre at an old point \(P_i\) and radius equal to the distance between two old points \(P_j\) and \(P_k\) to get new points from intersections with other circles and lines.

Then a real number \(\lambda\) is **constructible** if we can construct points \(P_i\) and \(P_j\) whose distance apart is \(|\lambda|\) units by starting from an initial set of points \(\{P_0, P_1\}\) whose distance apart is 1 unit and then performing a finite number of Operations 1 and 2. It turns out, that the following is true\(^{16}\).

**Theorem 3.13.1.** All constructible real numbers come from repeated square roots and field operations starting from numbers in \(\mathbb{Q}\).

**Corollary 3.13.2.** Every constructible number is an algebraic number.\(^ {17}\)

The interesting thing about constructible numbers is that they have limited values for their **degree**. This quantity is defined as the degree of their minimal polynomial. For example:

- \(\sqrt{2}\) has degree 2 (since the minimal polynomial is \(x^2 - 2\));
- \(\sqrt{2} + \sqrt{3}\) has degree 4 (since the minimal polynomial is \(x^4 - 10x^2 + 1\));
- \(\cos(2\pi/17)\) has degree 8.

\(^{16}\) See Section 5.6 of John Stillwell’s book “Elements of Algebra”.

\(^{17}\) Actually, this result requires us knowing that the algebraic numbers are algebraically closed, which is beyond the scope of this course.
The last of these has minimal polynomial
\[ x^8 + \frac{1}{2}x^7 - \frac{7}{4}x^6 - \frac{3}{4}x^5 + \frac{15}{16}x^4 + \frac{5}{16}x^3 - \frac{5}{32}x^2 - \frac{1}{32}x + \frac{1}{256}. \]

Using the theory of field extensions\(^\text{18}\) the following can be proved:

**Theorem 3.13.3.** If \( \lambda \) is constructible, then \( \deg(\lambda) = 2^i \) for some \( i \geq 0 \).

**Example 3.13.4.** \( \sqrt[3]{5} \) is not constructible as its minimal polynomial is \( x^3 - 5 \).

So the famous problems of antiquity become:

**Doubling the cube:** Is \( \sqrt[3]{2} \) constructible?

**Squaring the circle:** Is \( \sqrt{\pi} \) constructible?

**Trisecting \( \beta/3 \):** Is \( \cos(\pi/9) \) constructible?

It turns out that each of these problems is impossible to solve:

\[
\deg(\sqrt[3]{2}) = 3 \quad (\text{min. poly.} \ X^3 - 2) \\
\implies \sqrt[3]{2} \text{ is NOT constructible.}
\]

\[
\pi \text{ is transcendental} \implies \sqrt{\pi} \cdot \sqrt{\pi} \text{ is not constructible} \\
\implies \sqrt{\pi} \text{ is NOT constructible.}
\]

\[
\deg(\cos(\pi/9)) = 3 \quad (\text{min. poly.} \ X^3 - \frac{3}{4}X - \frac{1}{8}) \\
\implies \cos(\pi/9) \text{ is NOT constructible.}
\]

### 3.14 Number-theory type results in ring theory

Below is a table that summarises one of the goals of this course: the synthesis of results in number theory to polynomial rings. Each row states a result in number theory aligned with its analogue in polynomial rings. The right-most column states the category of rings for which a more general result holds, that the reader can pursue at their own interest.

<table>
<thead>
<tr>
<th></th>
<th>Integers</th>
<th>Polynomials</th>
<th>Generally holds in ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Division Rule</td>
<td>Lemma 2.1.4</td>
<td>Lemma 3.6.10</td>
<td>Euclidean domains</td>
</tr>
<tr>
<td>Euclidean Algorithm</td>
<td>Lemma 2.1.7</td>
<td>Lemma 3.6.13</td>
<td>Euclidean domains</td>
</tr>
<tr>
<td>Factorisation</td>
<td>Theorem 2.2.2</td>
<td>Theorem 3.7.4</td>
<td>Unique factorisation domains</td>
</tr>
<tr>
<td>Euclid’s Lemma</td>
<td>Corollary 2.1.16(c)</td>
<td>Lemma 3.7.3</td>
<td>Integral domains</td>
</tr>
<tr>
<td>Bézout’s identity</td>
<td>Lemma 2.1.10</td>
<td>Lemma 3.6.15</td>
<td>Principal ideal domains</td>
</tr>
<tr>
<td>When a quotient is a field</td>
<td>Corollary 3.1.9</td>
<td>Theorem 3.10.7</td>
<td>Commutative rings</td>
</tr>
</tbody>
</table>

What of the following results?
### 3.15 Exercises

**Exercise 3.15.1.** For each of the following pairs of polynomials \( f(x), g(x) \in \mathbb{Q}[x] \), find the quotient \( q(x) \) and remainder \( r(x) \) when \( f(x) \) is divided by \( g(x) \).

(i) \( f(x) = x^2 + x - 1, g(x) = x - 1 \)
(ii) \( f(x) = x^4 - 1, g(x) = -x^2 + 2 \).
(iii) \( f(x) = 2x^5 - 3x^2 + 2x + 1, g(x) = x - 2 \).

**Exercise 3.15.2.** Show that addition and multiplication on \( \mathbb{R}[x]/\equiv_p \), as given in Definition 3.10.3, is well-defined.

**Exercise 3.15.3.** Show that the Division Rule (Lemma 2.1.4) does not hold in the polynomial ring \( \mathbb{Z}[x] \).

**Exercise 3.15.4.** Let \( F \) be a field and let \( f \in F[x] \). Show that if \( f \) has degree at most 3 and is reducible\(^{19} \), then it has a factor with degree 1.

**Exercise 3.15.5.** Show that if \( f, g \in F[x] \), then \( \deg(f \cdot g) = \deg(f) + \deg(g) \).

**Exercise 3.15.6.** Find the minimal polynomial over \( \mathbb{Q} \) for the following numbers:

(i) \( 1 + i \),
(ii) \( 2 + 3i \),
(iii) \( e^{2\pi i}/5 \).

**Exercise 3.15.7.** By using the fact that the algebraic numbers form an algebraically closed field\(^{20} \), show that one of \( \pi + e \) or \( \pi \cdot e \) is transcendental.

**Exercise 3.15.8.** State and prove an analogue of the LDE Theorem 2.5.14 for the polynomial ring \( F[x] \).

---

First of all, the LDE Theorem does have a direct analogue and we do this in Exercise 3.15.8. The Chinese Remainder Theorem has an analogue in the direct factorisation of a quotient ring \( R/I \) by coprime ideals. Gauß’s Lemma holds when taking the field of fractions:

If a polynomial with coefficients in a ring \( R \) is reducible over \( \text{Frac}(R) \), then it is also reducible over \( R \).

Eisenstein’s Irreducibility Criterion works for a commutative ring \( R \) with unit:

If \( f = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in R[x] \) and \( p \) is a prime in \( R \) dividing each coefficient \( a_i \) where \( i \in \{0, 1, \ldots, n-1\} \), but \( p^2 \) does not divide \( a_0 \), then \( f \) is irreducible over \( \text{Frac}(R) \).

---

\(^{19}\) This is not true if we consider polynomials of degree 4. The polynomial \((x^2 + 1)^2\) in \( \mathbb{Q}[x] \) is reducible but has no factors of degree 1.

\(^{20}\) A field \( F \) is algebraically closed if every non-constant polynomial has a root.
In the following, we will see how we can extend the integers to a particular lattice of the complex plane. It forms a ring, but it doesn’t have the nice properties like the other rings we’ve seen so far ...

3.15.1  A different type of number system and its arithmetic: \(\mathbb{Z}(\sqrt{-5})\)

This is the set of all formal sums of the form

\[ a + b\sqrt{-5} \]

where \(a, b \in \mathbb{Z}\). We will simply write \(a\) for \(a + 0\sqrt{-5}\). We can define addition and multiplication of such numbers:

**Addition**

\[(a + b\sqrt{-5}) + (a' + b'\sqrt{-5}) = (a + a') + (b + b')\sqrt{-5} \]

**Multiplication**

\[(a + b\sqrt{-5}) \cdot (a' + b'\sqrt{-5}) = (aa' - 5bb') + (ab' + a'b)\sqrt{-5} \]

**Exercise 3.15.9.** For \(z = a + b\sqrt{-5} \in \mathbb{Z}(\sqrt{-5})\) define the norm \(N(z) = z \cdot \bar{z}\) where, \(\bar{z} = a - b\sqrt{-5}\). Prove that

\[ N(z \cdot z') = N(z) \cdot N(z') \]

for any \(z, z' \in \mathbb{Z}(\sqrt{-5})\).

**Exercise 3.15.10.** A unit of \(\mathbb{Z}(\sqrt{-5})\) is an element \(u\) such that there exists an element \(v\) such that \(u \cdot v = 1\). What are the units of \(\mathbb{Z}(\sqrt{-5})\)? (Hint: You know that \(N(z \cdot z') \geq N(z)\) for any \(z, z' \in \mathbb{Z}(\sqrt{-5})\).)

**Exercise 3.15.11.** An irreducible in \(\mathbb{Z}(\sqrt{-5})\) is a non-unit which cannot be written as a product of two non-units. Show that 3 and \(1 + \sqrt{-5}\) are irreducible.

**Exercise 3.15.12.** How many ways can 6 be written as a product of irreducibles in \(\mathbb{Z}(\sqrt{-5})\)?

**Exercise 3.15.13.** A prime in \(\mathbb{Z}(\sqrt{-5})\) is a nonzero element \(p\), that is not a unit, satisfying the following:

given \(x\) and \(y\) in \(\mathbb{Z}(\sqrt{-5})\) such that \(p\) divides \(x \cdot y\), then \(p\) divides \(x\) or \(y\).

Show that every prime is an irreducible, but the converse is not true.
4

Normed vector spaces

In this chapter we look at a generalisation of Euclidean space that encapsulates ‘spaces of functions’ and other objects whereby we can measure the difference between things as we would the vectors of $\mathbb{R}^n$.

4.1 Abstract vector spaces: things that behave like $\mathbb{R}^n$

Gregory H. Moore wrote an interesting piece in Historia Mathematica\(^1\) that describes how the idea of a vector space was developed to include the many mathematical objects we study today. Here, we reproduce the abstract of his article:

Modern linear algebra is based on vector spaces, or more generally, on modules. The abstract notion of vector spaces was first isolated by Peano (1888) in geometry. It was not influential then, nor when Weyl rediscovered it in 1918. Around 1920 it was rediscovered again by three analysts – Banach, Hahn, and Weiner – and an algebraist, Noether. Then the notion developed quickly, but in two distinct areas: functional analysis, emphasizing infinite-dimensional normed vector spaces, and ring theory, emphasizing finitely generated modules which were often not vector spaces. Even before Peano, a more limited notion of vector space over the reals was axiomatized by Darboux (1875).

So what does Moore mean by ‘axiomatize’? We will motivate the axiomatic definition of a (normed) vector space by exploring a few examples.

**Example 4.1.1** (Euclidean space). In $\mathbb{R}^n$, we can add two elements to get another element of $\mathbb{R}^n$, and we also have another operation called scalar multiplication:

$$\lambda(u_1, u_2, \ldots, u_n) := (\lambda u_1, \lambda u_2, \ldots, \lambda u_n).$$

We can take subsets which are closed under these two operations, and we call them subspaces. For example, the set of elements $(u_1, u_2, \ldots, u_n)$ whose sum $\sum u_i$ is zero forms a subspace. We can also define a basis of $\mathbb{R}^n$ so that we can write every element as linear combinations of the basis elements. For example, the vectors $(1,0,\ldots,0)$, $(0,1,0,\ldots,0)$, $\ldots$, $(0,\ldots,0,1)$ form a linearly independent spanning set for $\mathbb{R}^n$.

**Example 4.1.2** (Vector space of code words). Let’s take the smallest field, $\mathbb{Z}_2$, with just the two elements 0 and 1. Much of the theory of codes is


This is not a binary operation. Rather each element of $\mathbb{R}$ defines a unary (‘one’) operation $\mathbb{R}^n \to \mathbb{R}^n$.\n
about strings of 0’s and 1’s, of a common length, say \( n \). We can add code words, with the rule that 1 + 1 = 0. For example:

\[
0011001 + 1001111 = 1010110.
\]

Scalar multiplication by elements of \( \mathbb{Z}_2 \) is not very interesting here since multiplying by 0 and 1 just annihilates or preserves the codewords respectively. This example is really just like the previous example where we replace \( n \)-tuples of real numbers with \( n \)-strings of elements from a different field \( \mathbb{Z}_2 \).

**Example 4.1.3** (Vector space of functions). Consider the set of all functions \( V^X \) from a set \( X \) to a vector space \( V \) (think of \( \mathbb{R}^n \) if you like). We can add functions by the so-called point-wise addition of functions, and we can also define scalar multiplication on functions:

\[
(f + g)(x) := f(x) + g(x) \\
(\lambda f)(x) := \lambda f(x).
\]

There are subsets of \( V^X \) that are closed under this operation, such as the constant functions. Can we write every element of \( V^X \) as a linear combination of a distinguished set of functions?

**Example 4.1.4** (Vector space of polynomials). Consider the polynomial ring \( \mathbb{R}[x] \). We can add polynomials and multiply them by elements of \( \mathbb{R} \) to give us more elements of \( \mathbb{R} \). If \( f, g \in \mathbb{R}[x] \) and \( \alpha, \beta \in \mathbb{R} \), then \( \alpha \cdot f + \beta \cdot g \in \mathbb{R}[x] \). There are subsets of \( \mathbb{R}[x] \) that are closed under these operations, such as the polynomials which have degree at most a given number, such as 5 say. We can write every element of \( \mathbb{R}[x] \) as a linear combination of the polynomials

\[
1, x, x^2, x^3, x^4, \ldots
\]

All of these examples satisfy the axioms\(^2\) of a vector space.

**Definition 4.1.5** (Vector space). Let \( V \) be a set and \( F \) be a field, and suppose there is a binary operation ‘+’ on \( V \), and a map which takes an element \( \lambda \in F \) and an element \( v \in V \) and returns an element \( \lambda \cdot v \) of \( V \) (we call this scalar multiplication). We call \( V \) a vector space if these operations satisfy the following axioms:

1. For all \( u, v \in V \) we have \( u + v = v + u \).
2. For all \( u, v, w \in V \) we have \( (u + v) + w = u + (v + w) \).
3. There is an element 0 \( \in V \) , such that for all \( v \in V \) , we have \( v + 0 = v \).
4. For every \( v \in V \) , there is an element \( -v \in V \) such that \( v + (-v) = 0 \).
5. For every \( v \in V \) , we have \( 1 \cdot v = v \).
6. For all \( u, v \in V \) and \( \lambda \in F \) , we have \( \lambda(u + v) = \lambda u + \lambda v \).
7. For all \( v \in V \) and \( \lambda, \mu \in F \) , we have \( (\lambda + \mu)v = \lambda v + \mu v \).
8. For all \( v \in V \) and \( \lambda, \mu \in F \) , we have \( \lambda(\mu v) = (\lambda \mu)v \).

\(^2\) What we are demonstrating now is typical of pure mathematics; the distilling of the properties of interesting and widely studied examples in order to create a framework where all of these entities can be studied with an over-arching theory.
This seems like a lot to remember! However, if we use some of the
jargon of abstract algebra, we can cluster some of these axioms together
to make it easier to remember\(^3\). The first four just say that \(+\) is associative
and commutative, there is an additive identity, and every element has an
additive inverse. In third year, we would say that \((V, +)\) is an abelian
group. The rest basically says that the field \(F\) acts as automorphisms on the
group\(^4\) \(V\).

All of the examples we had before satisfy this definition. So what? Well,
from this abstract and very general definition, we can do linear algebra
in a similar way to what you did in first year mathematics with \(\mathbb{R}^n\). We
can study subspaces, spanning sets, bases, linear maps, eigenvalues and
so on. We do not need to spend much time on this generalised version of
linear algebra, since you can more or less assume that whatever property
you learnt about of \(\mathbb{R}^n\) has a direct analogue in a vector space \(V\). The main
difference that you will see is that we can have vector spaces which do not
have a finite basis: infinite-dimensional vector spaces.

### 4.1.1 Vector spaces from fields

Recall that a subset \(S\) of a ring \(R\) is a subring if it itself is a ring under the
induced operations of \(R\). Likewise, a subset \(K\) of a field \(F\) is a subfield if it
itself is a field. For example, we have the following lattice of fields:

```
    C                     
   /   \                    
  /     \                   
 R     A  \                 
       / \                 
      /   \                
 R \cap A  \               
       \                 
         Q
```

If we take two of these fields, we can define a vector space.

**Lemma 4.1.6.** Let \(F\) be a field and let \(K\) be a subfield of \(F\). Define ‘scalar
multiplication’ on \(F\) by the multiplication by elements of \(K\). Then the add-
tion operation on \(F\) together with scalar multiplication by elements of \(K\)
forms a vector space on \(F\).

† **Proof:** To check all the axioms of a vector space can be quite tedious. In
this case, many of them follow simply from the definition of field: e.g. (1) –
(4) follow immediately. It just suffices to check the axioms (5)-(8), but we
will leave this to the reader. \(\square\)

**Example 4.1.7.** Consider \(F = \mathbb{C}\) and \(K = \mathbb{R}\). This setup defines a two-
dimensional vector space on \(F\). Why? Because, every element of \(F\) can be
written as \(a + b \cdot i\) for two elements \(a, b \in \mathbb{R}\). That is, \([1, i]\) forms a basis for
\(F\) (over \(K\)).

**Example 4.1.8.** Consider \(F = \mathbb{R}\) and \(K = \mathbb{Q}\). This time, we end up with
an infinite-dimensional vector space! We will see this as a proof by contra-
diction. Suppose there was a finite basis for \(F\) over \(K\): \([e_1, e_2, \ldots, e_n]\). Then

\(^3\) I don’t expect you to remember them.

\(^4\) You will understand this once you see “group actions” in third year.
every element of $\mathbb{R}$ could be written as a linear combination

$$q_1 \cdot e_1 + q_2 \cdot e_2 + \cdots + q_n \cdot e_n$$

where $q_1, q_2, \ldots, q_n \in \mathbb{Q}$. In fact, this implies that there is a bijection\(^5\) $f$ from $\mathbb{R}$ to the Cartesian product $\mathbb{Q}^n$ defined by

$$f(q_1 \cdot e_1 + q_2 \cdot e_2 + \cdots + q_n \cdot e_n) := (q_1, q_2, \ldots, q_n).$$

So the cardinality of $\mathbb{R}$ is the same as the cardinality of $\mathbb{Q}^n$; which is a contradiction as $\mathbb{R}$ is uncountable by Theorem 1.9.2, $\mathbb{Q}$ is countable by 1.8.6, and $\mathbb{Q}^n$ is countable by (repeated application of) Exercise 1.11.11.

4.2 Aside: The Axiom of Choice

Is there a basis for the vector space $\mathbb{R}$ over $\mathbb{Q}$? Does every vector space have a basis?

We have already seen Russell’s Paradox and the Continuum Hypothesis as fundamental philosophical questions in mathematics that stirred the minds of early 20th century mathematicians. There is another taboo subject in mathematics, and it is the acceptance or non-acceptance of the Axiom of Choice.

**Axiom of choice:** For any collection $\mathcal{S}$ of nonempty sets, there exists a function $f$ that assigns to each set $S$ in $\mathcal{S}$ an element $f(S)$ of $S$.

The function $f$ here is called a choice function, a map which selects one element from an infinite collection of sets. If we can always assume that such a function exists, then the real numbers would be well-ordered\(^6\), that is,

there is a total order $\preceq$ such that every nonempty subset of the real numbers has a minimum element (with respect to $\preceq$).

This seems like nonsense: how can we order the real numbers so that any open interval has a minimum element? Another reason to dislike the Axiom of Choice is the Banach-Tarski paradox in measure theory. In 1924 Stefan Banach and Alfred Tarski proved the following remarkable result: It is possible to take a solid ball in 3-dimensional space, cut it up into finitely many pieces and, moving them using only rotation and translation, reassemble the pieces into two balls of the same radius as the original. In other words, we get two spheres exactly the same size as the original sphere merely by cutting and shifting! Alternatively, we can cut up a ball the size of a pea and reassemble it into a ball the size of the sun. This theorem has come to be known as The Banach-Tarski Paradox not because it is a logical paradox (like that of Russell), but rather because it goes against our intuition about how the world works.

There are many, many results such as these that follow from assuming the Axiom of Choice, so why do we bother with it at all? It turns out that certain extremely useful results rely on an equivalent version of the Axiom of Choice known as Zorn’s Lemma\(^7\). However, here are some of the results which follow from Zorn’s Lemma:

\(^5\) Mini-proof that $f$ is a bijection: In Exercise 4.8.1, we show that $f$ is well-defined. Suppose $f(q_1 \cdot e_1 + \cdots + q_n \cdot e_n) = f(q'_1 \cdot e_1 + \cdots + q'_n \cdot e_n)$. Then $(q_1, \cdots, q_n) = (q'_1, \cdots, q'_n)$ and hence $q_i = q'_i$ for each $i \in \{1, \ldots, n\}$. Therefore, $q_1 \cdot e_1 + \cdots + q_n \cdot e_n = q'_1 \cdot e_1 + \cdots + q'_n \cdot e_n$ and $f$ is one-to-one. Now for an element $(q_1, q_2, \ldots, q_n) \in \mathbb{Q}^n$, notice that $f(q_1 \cdot e_1 + \cdots + q_n \cdot e_n) := (q_1, \ldots, q_n)$, so $f$ is clearly onto.

\(^6\) I’ll suppress the details here.

\(^7\) Zorn’s Lemma: Suppose a partially ordered set $\mathcal{P}$ has the property that every totally ordered subset has an upper bound in $\mathcal{P}$. Then the set $\mathcal{P}$ contains at least one maximal element.
(i) Every vector space has a basis.

(ii) The Hahn-Banach Theorem; one of the fundamental theorems of functional analysis which is fundamental to quantum mechanics.

(iii) Every field has an algebraic closure.

(iv) Tychonoff’s Theorem: An arbitrary product of compact sets is compact.

(v) Every subgroup of a free group is free.

There are ways around the Axiom of Choice (such as the Axiom of Determinateness) that eliminate the bad stuff and keep the good, but this is getting way beyond this course.

4.3 Norms

In high-school, the Euclidean norm is introduced in the context of problems in physics, where we would like to calculate the magnitude of a vector. So given a vector \( \mathbf{v} := (a_1, a_2, \ldots, a_n) \in \mathbb{R}^n \) the norm of \( \mathbf{v} \) is the square root of the sum of the squares of its coordinates:

\[
\| \mathbf{v} \| := \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}.
\]

Another length-function appears in coding theory, the so-called Hamming weight, and it has similar properties to the Euclidean norm.

Example 4.3.1 (Hamming weight). Given an n-string \( \mathbf{v} \) of elements of \( \mathbb{Z}_p \), the Hamming weight \( w(\mathbf{v}) \) is the number of nonzero positions. For example,

\[
w(000130520) = 4.
\]

There are three properties of this function which share analogous properties with the Euclidean norm on \( \mathbb{R}^n \):

Non-degeneracy: \( w(\mathbf{v}) = 0 \) if and only if \( \mathbf{v} \) is the string of all 0’s. (Just like the zero vector).

Positivity: \( w \) always returns a non-negative number.

Triangle inequality: \( w(\mathbf{u} + \mathbf{v}) \leq w(\mathbf{u}) + w(\mathbf{v}) \), for all \( \mathbf{u}, \mathbf{v} \).

We will be looking at vector spaces were the scalars are the real numbers, since there is a natural ordering on \( \mathbb{R} \).

Definition 4.3.2 (Norm). A norm on a vector space \( V \) over \( \mathbb{R} \) is a map

\[
\| \| : V \to \mathbb{R}
\]

such that for all \( \mathbf{u}, \mathbf{v} \in V \) and \( \lambda \in \mathbb{R} \), we have:

Non-degeneracy: \( \| \mathbf{v} \| = 0 \) if and only if \( \mathbf{v} = \mathbf{0} \) (the zero vector).

Positive homogeneity: \( \| \lambda \mathbf{v} \| = |\lambda| \cdot \| \mathbf{v} \| \).

Triangle inequality: \( \| \mathbf{u} + \mathbf{v} \| \leq \| \mathbf{u} \| + \| \mathbf{v} \| \).
In particular, these axioms imply that $\|v\|$ is always non-negative.  
So the Hamming weight is not a norm, since it doesn’t satisfy “Positive homogeneity”. A normed vector space is simply a vector space with a norm on it, and we will write it as a pair $[V, \|\cdot\|]$. 

**Example 4.3.3.** Consider the $n$-dimensional vector space $\mathbb{R}^n$ over $\mathbb{R}$. We have already see the Euclidean norm as a way of measuring distance and magnitude on $\mathbb{R}^n$, but there is another useful norm: 

$\|v\|_\infty := \max\{|v_1|, |v_2|, \ldots, |v_n|\}$ 

where we write $v$ as $(v_1, v_2, \ldots, v_n)$. We leave it as an exercise at the end of the chapter that $\|\cdot\|_\infty$ does indeed define a norm on $\mathbb{R}^n$ (Exercise 4.8.8. So if $n = 2$, we see that $\|3, 4\|_\infty = 4$ whereas for the Euclidean norm, we have $\|3, 4\| = \sqrt{3^2 + 4^2} = 5$. 

**Example 4.3.4.** Consider the vector space $V$ of all polynomials in $\mathbb{R}[x]$ with degree at most $n$. The following defines a norm on $V$: 

$\|a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0\| := (n+1)|a_n| + n|a_{n-1}| + \cdots + 2|a_1| + |a_0|$. 

(See Exercise 4.8.7). 

### 4.4 Boundedness 

We say that $u \in \mathbb{R}$ of $S$ is an **upper bound** if for all $s \in S$ we have $s \leq u$. 

**Definition 4.4.1** (Least upper bound (supremum)). Let $S \subset \mathbb{R}$. An upper bound $\ell$ of $S$ is a least upper bound if for every other upper bound $u$ of $S$, we have $\ell \leq u$. 

Equivalently, we can use the following definition of least upper bound which is perhaps more amenable in giving proofs: 

An upper bound $\ell$ of $S$ is a least upper bound if it satisfies: 

- $(\forall s \in S) \quad s \leq \ell$, 
- $(\forall \epsilon > 0) (\exists s \in S) \quad \ell - \epsilon < s$. 

---

**Example 4.4.2.** Let $S := \{2 - 1/n : n \in \mathbb{N}\}$. **There is no ‘maximum’ of this set $S$, but 2 is a least upper bound for $S$.** 

**Proof.** We need to prove that 2 is an upper bound of $S$, and then that it is the smallest of the upper bounds of $S$. 

**Upper bound:** Let $s \in S$. So there exists $n \in \mathbb{N}$ such that $s = 2 - 1/n$. 

Now $1/n > 0$ and hence $-1/n < 0$. Then $2 - 1/n < 2$, and so $s < 2$. Therefore, 2 is an upper bound for $S$. 

---
**Least upper bound**: Let $\epsilon > 0$. We need to find a suitable $s \in S$ such that $\ell - \epsilon < s$. Let $n$ be the next largest integer after $1/\epsilon$ and let $s = 2 - 1/n$. Then $n > 1/\epsilon$ and so $\epsilon > 1/n$. Thus $2 - \epsilon < 2 - 1/n$ and hence $2 - \epsilon < s$. Since $s \in S$, we have found an element of $S$ that is greater than $2 - \epsilon$ and so $2$ is the least upper bound of $S$.

\[ \Box \]

**Theorem 4.4.3** (The Least Upper Bound Property of $\mathbb{R}$). *Every nonempty subset $S$ of $\mathbb{R}$ which has an upper bound, has a least upper bound.*

We will come back to the proof of this result once we properly define what $\mathbb{R}$ is!

The generalisation of an open interval in higher dimensions is a sphere, or ball, of $\mathbb{R}^n$. We will go one step further and define balls for normed vector spaces.

**Definition 4.4.4** (Ball). *Let $x$ be an element of a normed vector space $[V, \|\cdot\|]$. Then the (open) ball of radius $r \in \mathbb{R}^+$ about the element $x$ is the set $B_r(x) := \{ v \in V : \|v - x\| < r \}.**

In the mathematical discipline of topology, a ball is the canonical example of an open set. Below we give some examples of what these balls look like for the various norms we’ve seen so far.

**Example 4.4.5** (Balls in $\mathbb{R}^2$ with the Euclidean norm). *In $\mathbb{R}^2$ with the Euclidean norm, balls are just discs.*

**Example 4.4.6** (Balls in $\mathbb{R}^2$ with the max-norm). *If we take the norm $\|\cdot\|_\infty$ from Example 4.3.3, the balls look like squares! For example, take the ball of radius 1 about the origin:* $B_1((0,0)) = \{(x, y) \in \mathbb{R}^2 : \|(x, y)\|_\infty < 1\} = \{(x, y) \in \mathbb{R}^2 : \max\{|x|, |y|\} < 1\} = \{(x, y) \in \mathbb{R}^2 : |x| < 1 \text{ and } |y| < 1\}.
Example 4.4.7 (Balls in $\mathbb{R}[x]$ (bounded degree)). Let $R = \mathbb{C}$ and consider the polynomials in $\mathbb{R}[x]$ that have degree at most 2. We will use the norm that was defined in Example 4.3.4. Consider the ball of radius 1 about the polynomial $x + i$:

$$B_1(x + i) = \{a_2x^2 + a_1x + a_0 \in \mathbb{C}[x] : \| (a_2x^2 + a_1x + a_0) - (x + i) \| < 1 \}$$

$$= \{a_2x^2 + a_1x + a_0 \in \mathbb{C}[x] : 3|a_2| + 2|a_1 - 1| + |a_0 - i| < 1 \}$$

So for example, $\frac{1}{5}x^2 + x + \frac{3}{4}i \in B_1(x + i)$.

4.5 Epsilon versus delta

The definition of a limit has two quantifiers: $\forall$ followed by $\exists$. It is very important that they are in this order\(^\text{11}\). We have seen this already in the definitions of onto and of the least upper bound of a set:

$f : A \rightarrow B$ is onto: \( (\forall b \in B) (\exists a \in A) \quad f(a) = b \)

$\ell$ is a least upper bound of $S \subseteq \mathbb{R}$: \( (\forall \epsilon > 0) (\exists s \in S) \quad \ell - \epsilon < s \)

I like to think of such mathematical statements as games. For example, with the definition of onto, I give you $b \in B$, and then it is up to you to present me with $a \in A$ such that $f(a) = b$. I then choose another $b \in B$, and so-on and so-on. A proof that $f$ is onto requires you coming up with a winning strategy for this game. This is the same for proving that a function or sequence converges. I give you $\epsilon$ and you must come up with a systematic way to provide a $\delta$. For sequences, you are asked to provide a threshold value $N \in \mathbb{N}$.

Example 4.5.1 (Old chestnut: $1/n$). Let us consider the sequence $s_n := 1/n$. If I give you a window around 0 in the y-axis (the codomain) with a particular size $\epsilon$, can you find a cut-off point $N$ so that the sequence beyond $s_N$ is contained in this window?

Below we look at the case that $\epsilon = 0.18$.

By the picture above, if we only regard the sequence after $n = 5$ onwards, we can be sure that the sequence lies in the orange-strip. How

\(^{11}\) Note the difference between the sentences (i) “everybody loves somebody” and (ii) “there is somebody who loves everyone”!

Figure 4.1: $1/n$ drawn as ‘$n$ versus $s_n$’
would we prove this? Well . . .

\[ n \geq 6 \implies \frac{1}{n} \leq \frac{1}{6} \]
\[ \implies \frac{1}{n} < 0.18 = \epsilon. \]

In general, we have a winning strategy for this game.

You give me \( \epsilon \), and I declare that \( N = \frac{1}{\epsilon} \).

So with this strategy, I can show:

\[ n > N \implies n > \frac{1}{\epsilon} \]
\[ \implies \frac{1}{n} < \epsilon. \]

### 4.6 Continuity for normed vector spaces

One of the main successes of the theory of normed vector spaces is in the generalisation of continuity from Euclidean spaces (over \( \mathbb{R} \) or \( \mathbb{C} \)) to arbitrary vector spaces. We are then able to study functions or sequences of polynomials, of matrices and sequences of continuous functions themselves! Continuity then gains a deeper meaning when we look for solutions of differential equations, where the differentiable functions are the elements of our vector space and the integration and differentiation operators are the continuous maps!

**Definition 4.6.1** (Continuous maps between normed vector spaces). A map \( f : V \to W \) between normed vector spaces \( (V, \| \cdot \|_V) \) and \( (W, \| \cdot \|_W) \) is continuous at \( a \in V \) if for every ball \( B_\epsilon(f(a)) \) of \( W \) with centre \( f(a) \), there exists a ball \( B_\delta(a) \) of \( V \) about \( a \), such that

\[ f(B_\delta(a)) \subset B_\epsilon(f(a)). \]

A map is continuous if it is continuous at each point in its domain.

**Example 4.6.2** (Constant functions are continuous). Suppose we have two normed vector spaces \( (V, \| \cdot \|_V) \) and \( (W, \| \cdot \|_W) \) and consider a constant function \( f : V \to W \) that is defined by \( f(v) = w \) where \( v \in V \) and \( w \) is a fixed element of \( W \). We will show that \( f \) is continuous (everywhere).

**Proof.** Let \( \epsilon > 0 \) and let \( v \in V \). We want to find \( \delta > 0 \) so that

\[ f(B_\delta(v)) \subset B_\epsilon(f(v)). \]

This can be greatly simplified when we apply the definition of \( f \):

\[ \{w\} \subset B_\epsilon(w). \]
In fact, we can choose $\delta$ to be anything we like, since

$$B_\epsilon(w) = \{w' \in W : \|w' - w\|_W < \epsilon\}$$

and clearly $w \in B_\epsilon(w)$ as $\|w - w\|_W = \|0\|_W = 0$. So $f$ is continuous at every point of $V$. \qed

**Example 4.6.3** (Dirichlet’s characteristic function of the rationals). Let $\chi_Q$ be the function on $\mathbb{R}$ defined by

$$\chi_Q(x) := \begin{cases} 1 & \text{if } x \in \mathbb{Q} \\ 0 & \text{if } x \notin \mathbb{Q}. \end{cases}$$

Here our normed vector space is just $[\mathbb{R}, |\cdot|]$. We will show that $\chi_Q$ is not continuous at any point $a$ of $\mathbb{R}$. To do this, we must take the negation of the definition of continuous:

<table>
<thead>
<tr>
<th>$f$ is not continuous at $a$ if</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(\exists \epsilon \in \mathbb{R}^+) (\forall \delta \in \mathbb{R}^+) \ f(B_\delta(a)) \notin B_\epsilon(f(a))$</td>
</tr>
</tbody>
</table>

Choose $\epsilon = \frac{1}{2}$ and let $\delta \in \mathbb{R}^+$. We will show that $\chi_Q(B_\delta(a))$ is not a subset$^{12}$ of $B_\epsilon(\chi_Q(a))$. If $a \in \mathbb{Q}$, choose $x \in \mathbb{R} \setminus \mathbb{Q} \cap B_\delta(a)$. If $a \notin \mathbb{Q}$, choose $x \in \mathbb{Q} \cap B_\delta(a)$. This is possible because of the Archimedean property of the real numbers: every open interval in $\mathbb{R}$ contains a rational number and an irrational number. So in both cases we will have $|\chi_Q(a) - \chi_Q(x)| = 1 > \frac{1}{2}$ and hence $\chi_Q(x) \notin B_\epsilon(\chi_Q(a))$. Therefore, $\chi_Q$ is not continuous at any point of $\mathbb{R}$.

**Example 4.6.4** (A fully worked out, difficult, example). Let $V$ and $W$ both be $\mathbb{R}^2$, but equip $V$ with the Euclidean norm and $W$ with the norm $\|\cdot\|_\infty$ from Example 4.3.3. Then the map $f : V \to W$ defined by

$$f((x, y)) := (x - y, xy)$$

is continuous at $(1, 1)$. How would we devise a proof of this?

Let $\epsilon > 0$. We want to find $\delta > 0$ so that

$$f(B_\delta((1, 1))) \subset B_\epsilon(f((1, 1))) = B_\epsilon((0, 1)).$$

We should figure out first what these two entities are and what they look like.

- The set $f(B_\delta((1, 1)))$ is just the set of elements $(x - y, xy)$ such that

$$\|(x, y) - (1, 1)\| = \sqrt{(x - 1)^2 + (y - 1)^2} < \delta.$$

- The set $B_\epsilon((0, 1))$ is just the set of elements $(u, v)$ such that

$$\|(u, v) - (0, 1)\|_\infty = \max\{|u|, |v - 1|\} < \epsilon.$$

What would the proof look like?

---

$^{12}$ To show that a subset $X$ is not a subset of a set $Y$, we only need to find an element $x \in X$ that is not in $Y$. 

![Diagram](image.png)
Choose $\delta$ to be something depending on $\varepsilon$? and let $(x, y) \in B_\delta((1, 1))$. We want to show that $f((x, y)) \in B_\varepsilon((0, 1))$. Now
\[
\|(x, y) - (1, 1)\| < \delta \implies \sqrt{(x - 1)^2 + (y - 1)^2} < \delta
\]
\[
\implies \ldots
\]
\[
\implies \max\{|x - y|, |xy - 1|\} < \varepsilon
\]
\[
\implies \|f((x, y)) - (0, 1)\|_\infty < \varepsilon
\]
\[
\implies f((x, y)) \in B_\varepsilon((0, 1))
\]

The ‘$\varepsilon$’ was given to us, and we must find the $\delta$ which makes this work. The picture in the margin shows that if $\varepsilon = 5$, then $\delta = 2$ is a suitable choice. How do we find $\delta$ in general, in terms of $\varepsilon$? We basically do reverse-engineering to find a $\delta$ which will do the job. It doesn’t need to be the best $\delta$; any suitable $\delta$ will do!

\[
\max\{|x - y|, |xy - 1|\} < \varepsilon \iff |x - y| < \varepsilon \quad \text{and} \quad |xy - 1| < \varepsilon
\]
\[
\iff |(x - 1) - (y - 1)| < \varepsilon \quad \text{and} \quad |xy - y + y - 1| < \varepsilon
\]
\[
\iff |x - 1| + |y - 1| < \varepsilon \quad \text{and} \quad |xy - y| + |y - 1| < \varepsilon
\]
\[
\iff |x - 1| + |y - 1| < \varepsilon \quad \text{and} \quad |y||x - 1| + |y - 1| < \varepsilon
\]

Choosing $\delta = \min\{1, \varepsilon/2\}$ will do the job, as we will see.

Suppose $\|(x, y) - (1, 1)\| < \delta$. Then $\sqrt{(x - 1)^2 + (y - 1)^2} < \delta$
Then $|x - 1| + |y - 1| < \delta$
Then $|x - 1 - (y - 1)| < \delta$ and $2|x - 1| + |y - 1| < 2\delta$

Now by the triangle inequality, and what we’ve deduced so far:
\[
|y| = |1 + y - 1| < 1 + |y - 1| < 1 + \delta < 2.
\]

Then $|x - y| < \delta$ and $|y||x - 1| + |y - 1| < 2\delta$
Then $|x - y| < \delta$ and $|xy - y| + |y - 1| < 2\delta$
Then $|x - y| < \delta$ and $|xy - y + y - 1| < 2\delta$
Then $|x - y| < \varepsilon$ and $|xy - 1| < \varepsilon$
Then $\max\{|x - y|, |xy - 1|\} < \varepsilon$
Then $\|f((x, y)) - (0, 1)\|_\infty < \varepsilon$
Then $f((x, y)) \in B_\varepsilon((0, 1))$.

Therefore, there exists $\delta$ such that $f(B_\delta((1, 1))) \subset B_\varepsilon(f((1, 1)))$ and hence $f$ is continuous at $(1, 1)$.

We have given the most general topological definition of continuity\(^\text{13}\). As we shall see below, this definition radically reduces when the map $f$ is a linear operator.

---

\(^\text{13}\) Except that ‘open sets’ take the place of ‘open balls’.
Definition 4.6.5 (Linear operator). A map \( f : V \to W \) between normed vector spaces \( (V, \| \cdot \|_V) \) and \( (W, \| \cdot \|_W) \) (defined over a field \( F \)) is called a linear operator if for all \( v_1, v_2 \in V \) and \( \lambda_1, \lambda_2 \in F \), we have

\[
f(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 f(v_1) + \lambda_2 f(v_2).
\]

The proof of the following result is an excellent example of an ‘analysis’-style proof.

Theorem 4.6.6. Let \( f : V \to W \) be a linear operator between normed vector spaces \( (V, \| \cdot \|_V) \) and \( (W, \| \cdot \|_W) \). Then \( f \) is continuous (everywhere) if and only if \( f \) is continuous at 0.

\[\star \text{ Proof (mostly restricted syntax):} \quad \text{Clearly the ”} \implies \text{” direction holds, so suppose } f \text{ is continuous at } 0. \text{ Let } a \in V \text{ with } a \neq 0. \text{ We will show that } f \text{ is continuous at } a \in V.\]

Suppose \( \epsilon \in \mathbb{R}^+ \).

Then there exists \( \delta \in \mathbb{R}^+ \) such that \( f(\mathcal{B}_\delta(0)) \subset \mathcal{B}_\epsilon(f(0)) \)

Then \( f(\mathcal{B}_\delta(0)) \subset \mathcal{B}_\epsilon(0) \)

(We will show that \( f(\mathcal{B}_\delta(a)) \subset \mathcal{B}_\epsilon(f(a)) \)).

Suppose \( x \in \mathcal{B}_\delta(a) \).

Then \( \|x - a\|_V < \delta \)

Then \( x - a \in \mathcal{B}_\delta(0) \)

Then \( f(x - a) \in f(\mathcal{B}_\delta(0)) \)

Then \( f(x - a) \in \mathcal{B}_\epsilon(0) \)

Then \( \|f(x - a)\|_W < \epsilon \)

Then \( \|f(x) - f(a)\|_W < \epsilon \)

Then \( f(x) \in \mathcal{B}_\epsilon(f(a)) \)

Then \( f(\mathcal{B}_\delta(a)) \subset \mathcal{B}_\epsilon(f(a)) \)

Therefore, \( f \) is continuous at \( a \).

\[\square\]

Example 4.6.7. If \( f : V \to W \) is a linear operator between normed vector spaces \( (V, \| \cdot \|_V) \) and \( (W, \| \cdot \|_W) \), and \( V \) has finite dimension \( d \in \mathbb{N} \), then \( f \) is continuous.

4.7 Function spaces

Let \( X \) be a set and let \( V \) be a vector space over a field \( F \). As we saw in Example 4.1.3, the set \( F(X, V) \) of all functions from \( X \) to \( V \) forms a vector space under the operations of point-wise addition and scalar multiplication.

It forms a normed vector space if we consider just the bounded functions \( \mathcal{B}(X, V) \) in \( F(X, V) \). We can also consider subspaces of this normed vector space to give us other interesting normed vectors spaces.

Suppose \( X \) is a normed vector space. Then we have:

\( C(X, V) \): The continuous bounded functions from \( X \) to \( V \).

\( D(X, V) \): The differentiable bounded functions from \( X \) to \( V \).

\( L(X, V) \): The linear operators from \( X \) to \( V \).

These subspaces will recur in later sections.
In some sense, the opposite of infinite ought to be bounded. We lose too much of the interesting mathematics and its applications if we only study the finite structures. We will see in a later section that boundedness is a key concept that guarantees that certain functions and sequences have limits or fixed points.

**Definition 4.7.1 (Bounded set).** A subset $S$ of a normed vector space $[V, \| \cdot \|]$ is bounded if it is contained in some ball. That is, there exists $x \in V$ and $r \in \mathbb{R}^+$ such that $S \subseteq B_r(x)$.

**Definition 4.7.2 (Bounded function).** A function $f$ from a set $X$ to a normed vector space $[V, \| \cdot \|]$ is bounded if its image is a bounded set of $[V, \| \cdot \|]$. That is, there exists $x \in V$ and $r \in \mathbb{R}^+$ such that $f(X) \subseteq B_r(x)$.

The set of all bounded functions $\mathcal{B}(X, V)$ is a vector subspace of the set $F(X, V)$ of all functions from $X$ to $V$\(^{14}\). So now we will turn $\mathcal{B}(X, V)$ into a normed vector space by equipping it with an appropriate norm. In the example below, we will look at the case where $V = \mathbb{R}$, but it can be done in general if $V$ itself is a normed vector space.

**Example 4.7.3 (The ‘sup’ norm).** Let $X$ be a set and let $f : X \to \mathbb{R}$ be a bounded function. An equivalent definition\(^{15}\) that $f$ be bounded is that there exists a positive constant $C$ such that for all $x \in X$, we have

$$|f(x)| < C.$$  

By the Least Upper Bound Property of $\mathbb{R}$ (Theorem 4.4.3), there exists a least upper bound for $f(X)$. So we can define

$$\|f\| := \sup\{|f(x)| : x \in X\}.$$  

Let’s check now that it is a norm on bounded functions from $X$ to $\mathbb{R}$:

**Non-degeneracy:** If $f$ is the zero function 0, then clearly $\|f\| = 0$. Now suppose we have a bounded function $g : X \to \mathbb{R}$ such that $\|g\| = 0$. Then $|g(x)| \leq 0$ for all $x \in X$, and so we must have $g(x) = 0$ for all $x \in X$; that is, $g$ is the zero function.

**Positive homogeneity:** Let $\lambda \in \mathbb{R}$ and $f \in \mathcal{B}(X, \mathbb{R})$. Then $|\lambda f(x)| = |\lambda||f(x)|$ for all $x \in X$. So it is not difficult to see that $\sup\{|\lambda f(x)| : x \in X\} = |\lambda|\sup\{|f(x)| : x \in X\}$ and hence $\|\lambda f\| = |\lambda||f||$.

**Triangle inequality:** Let $f, g \in \mathcal{B}(X, \mathbb{R})$ and let $u := \|f\| + \|g\|$. Now for a given element $x \in X$, we have from the triangle inequality for the absolute value norm, the following:

$$|(f + g)(x)| = |f(x) + g(x)| \leq |f(x)| + |g(x)|.$$  

By definition, $|f(x)| \leq \|f\|$ and $|g(x)| \leq \|g\|$ and so

$$|(f + g)(x)| \leq u.$$  

Since $\|f + g\|$ is the least upper bound of $\{|(f + g)(x)| : x \in X\}$, we must have

$$\|f + g\| \leq u.$$  

\(^{14}\) This will be left as an exercise for those interested in vector spaces.

\(^{15}\) Prove this!
Example 4.7.4. What is the ‘distance’ (with respect to the sup norm) between the functions $f(x) := x$ and $g(x) := x^2$ on the closed interval $[0, 1]$?

$$\|g - f\| = \sup\{|x^2 - x| : x \in [0, 1]\}$$

$$= \sup\{|x - x^2| : x \in [0, 1]\}$$

$$= \frac{1}{4}.$$  

This is because $x - x^2$ is symmetric about $\frac{1}{2}$, and so attains its maximum for $x = \frac{1}{2}$.

Now we show that if a linear map $f$ is continuous if it preserves bounded sets.

**Theorem 4.7.5.** Let $f : V \to W$ be a linear operator between normed vector spaces $[V, \|\cdot\|_V]$ and $[W, \|\cdot\|_W]$. Then $f$ is continuous if and only if there is a constant $C > 0$ such that for all $v \in V$

$$\|f(v)\|_W \leq C \cdot \|v\|_V.$$  

★ Proof: To be done in lectures. □

### 4.7.1 Aside: Fourier series

One of the most important concepts in applied mathematics and harmonic analysis is the decomposition of a periodic function into trigonometric functions. Here, the function space are the set of all functions $f : \mathbb{R} \to \mathbb{R}$ which are integrable on $[-\pi, \pi]$ and a periodic:

$$f(x + 2\pi) = f(x), \quad \text{for all } x \in \mathbb{R}.$$  

Such functions with only finitely many discontinuities are *square integrable* and so the following defines a norm on this function space, and it is called the $L^2$-norm.

$$\|f\| := \sqrt{\frac{1}{2\pi} \int_{-\pi}^{\pi} |f(\theta)|^2 \, d\theta}.$$  

It turns out that the cosine and sine functions form a basis for this function space, and the decomposition of $f$ into this basis is known as a *Fourier series*.

### 4.8 Exercises

**Exercise 4.8.1.** Show that $f$ in Example 4.1.8 is well-defined.

**Exercise 4.8.2.** Let $[V, \|\cdot\|]$ be a normed vector space, and consider $\mathbb{R}$ equipped with the Euclidean norm. Show that the function $f : V \to \mathbb{R}$ defined by $f(x) := \|x\|$ is continuous.

**Exercise 4.8.3.** Let $[V, \|\cdot\|]$ be a normed vector space and let $V^*$ be the set of all continuous linear functions from $V$ to $\mathbb{R}$.

(a) Define addition and scalar multiplication on $V^*$ as we have done for function spaces and verify that $V^*$ is a vector space.
Now we show that $V^*$ has a natural norm on it. Show that

$$\|f\| := \sup\{|f(x)| : \|x\| \leq 1\}$$

is a norm on $V^*$.

**Exercise 4.8.4.** Consider the following function $M$ from $\mathbb{R}^n$ to $\mathbb{R}$:

$$M((x_1, x_2, \ldots, x_n)) := \sum_{i=1}^{n} |x_i|.$$

(a) Show that $M$ defines a norm on $\mathbb{R}^n$.

(b) For $n = 2$, draw a picture of the ball $B_1((0, 0))$.

**Exercise 4.8.5.** Show that the continuous bounded functions from $X$ to $V$ form a subspace of $B(X, V)$.

**Exercise 4.8.6.** Let $g : \mathbb{R}^2 \to \mathbb{R}$ be the function defined by

$$g((x, y)) := x - y.$$

It turns out that $g$ is continuous (everywhere). Let $\epsilon = 7$. Find the best possible $\delta \in \mathbb{R}^+$ such that

$$g(B_\delta((2, 1))) \subseteq B_\epsilon(g(2, 1)).$$

**Exercise 4.8.7.** Prove that the $\|\cdot\|$ in Example 4.3.4 defines a norm.

**Exercise 4.8.8.** Prove that the $\|\cdot\|_\infty$ in Example 4.3.3 defines a norm.

**Exercise 4.8.9.** Let $S$ be the set $\{1 + \frac{1}{n} : n \in \mathbb{N}\}$. Guess a least upper bound $\ell$ for $S$ and prove that it is indeed the supremum of $S$.

**Exercise 4.8.10.** Let $f : [1, 2] \to \mathbb{R}$ be the function with

$$f(x) = \begin{cases} 
  x & \text{if } 1 \leq x < 2 \\
  1 & \text{if } x = 2.
\end{cases}$$

Show that $\|f\| = 2$.

**Exercise 4.8.11.** Consider sin and cos restricted to the interval $[0, \pi]$ (so they are elements of $B([0, \pi])$) Show that $\|\sin - \cos\| = \sqrt{2}$. 
5

**Metric Spaces**

For the notions of continuity and limit in \( \mathbb{R} \) or \( \mathbb{C} \), it is not the fact that these structures are ordered that makes it all work, rather it is the notion of distance that prevails. In this chapter, we go beyond normed vector spaces to the realm of ‘metric spaces’. These are one of the most widely available sources of interesting spaces and shapes that we can study limits and continuity on.

5.1 Limit of a function and limit of a sequence are really the same thing

In calculus we meet the definition of a limit of a function on the real numbers.

\[
\lim_{x \to a} f(x) = \ell \text{ means } \ldots
\]

\[
(\forall \epsilon > 0) (\exists \delta > 0) (\forall x \in \mathbb{R}) \quad 0 < |x - a| < \delta \implies |f(x) - \ell| < \epsilon.
\]

Then perhaps we learn about sequences of real numbers and what it means for \( \{s_n\} \) to converge to a real number \( \ell \).

\[
\lim_{n \to \infty} s_n = \ell \text{ means } \ldots
\]

\[
(\forall \epsilon > 0) (\exists N \in \mathbb{N}) (\forall n \in \mathbb{N}) \quad n > N \implies |s_n - \ell| < \epsilon.
\]

Are these notions of limit different? One of these definitions of a limit applies to a function \( f : \mathbb{R} \to \mathbb{R} \), and the other applies to a sequence of real numbers. The problem lies in understanding what a sequence is.

**Definition 5.1.1 (Sequence).** A sequence of elements of a set \( X \) is a function \( s : \mathbb{N} \to X \).

We often write \( s(n) \) simply as \( s_n \). We now use the idea of a ball from the previous section to recast the two definitions above. Here, the normed vector space we are contending with is simply the real numbers equipped with the absolute value norm.

**Definition of limit of \( f \) using balls:**

\[
(\forall B_\epsilon(\ell)) (\exists B_\delta(a) \setminus \{a\}) \quad f(B_\delta(a) \setminus \{a\}) \subseteq B_\epsilon(\ell).
\]
Definition of limit of $s$ using balls:

$$(\forall B_{\varepsilon}(\ell))(\exists (N, \infty) \cap \mathbb{N}) \ s((N, \infty) \cap \mathbb{N}) \subseteq B_{\varepsilon}(\ell).$$

What we will see later is that both of these definitions are of the form

$$(\forall B)(\exists A) \ f(A) \subseteq B$$

where $A$ and $B$ are suitably defined sets (like a punctured open set).

Using the ball-definition allows us to be flexible with the space we are working in, and what notion of distance or closeness that we can choose to adopt.

5.2 A good definition?

In the last chapter, we explored continuity of functions on normed vector spaces and gave the “ball”-definition there. The definition of continuity comes about from thinking of drawing the function without lifting your pen. And lifting your pen and moving to another spot would violate continuity.

If the function was ‘broken’ as we see in the figure, then we could find an interval of $\mathbb{R}$ for which there is an unresolvable gap in the image of $f$. So a function is NOT continuous, if there is some $a \in \mathbb{R}$ and some width $\varepsilon \in \mathbb{R}^+$ such that $f(B_\delta(a)) \not\subseteq B_\varepsilon(f(a))$

for every $\delta \in \mathbb{R}^+$. We saw this in Example 4.6.3. What about the definition of a limit?

Many mathematicians of the late 18th century toiled hard to find a definition for the limit of a function. They wanted to delineate the ‘good functions’ in calculus from the ‘bad ones’. The notion of a limit is critical in distilling the infinitesimal approximation of a rate of change; the derivative of a function\(^1\). It is also vital in a water-tight theory of integration and in order to have a Fundamental Theorem of Calculus (i.e., a way to invert differentiation).

Example 5.2.1. The series

$$1 + \frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \frac{1}{3 \times 4} + \cdots$$

does have a finite sum, namely the number 2. Do you see why? (Hint: Take the difference of this series with a similar one that starts at the second term).

Now the popular Harmonic series $1 + 1/4 + 1/9 + 1/16 + 1/25 + \cdots$ was shown to have a finite sum by Euler. This is because this series is bounded term for term by the one we have above. It turns out that the value of it is $\pi^2 / 6$, but to show this rigorously requires a precise definition of a limit.

It was Bernhard Bolzano (1817), Augustin-Louis Cauchy (1821), and Karl Weierstrass (1859/60) who made precise the definition of a limit as we know it today.

---

\(^1\) Indeed, Newton and Leibniz did not have a precise definition of a limit and thought that you could get by without having one! The ensuing 150 years of mathematical development proved them wrong.

When the values successively attributed to a particular variable approach indefinitely a fixed value so as to differ from it by as little as one wishes, this latter value is called the limit of the others.”

–Augustin-Louis Cauchy.
Example 5.2.2 (A sequence in \(\mathbb{R}^3\)). Define a sequence in \(\mathbb{R}^2\) by
\[
x_n := \left( \frac{n}{n+1}, \frac{1}{n} \right).
\]

Does this sequence converge to something?

By the graph, it seems that the sequence gets closer and closer to the point \((1, 0)\). Let’s try and prove this. Suppose \(\epsilon > 0\). On the back of an envelope, I worked out that choosing \(N > \sqrt{2}/\epsilon\) will do the job, as you will now see.

Proof. Suppose \(\epsilon > 0\). Choose \(N\) to be an integer greater than \(\sqrt{2}/\epsilon\), and suppose \(n\) is an integer such that \(n > N\).

Then \(n > \sqrt{2}/\epsilon\)
Then \(\frac{2}{n} < \epsilon^2\)
Then \(\frac{1}{n+1} + \frac{1}{n} < \epsilon^2\)
Then \(\frac{\sqrt{n+1} + 1}{n} < \epsilon\)
Then \(\|\left( \frac{1}{n+1}, \frac{1}{n} \right)\| < \epsilon\)
Then \(\|x_n - (1, 0)\| < \epsilon\)
Therefore, there exists an integer \(N\) such that if \(n > N\), then \(\|x_n - (1, 0)\| < \epsilon\). Therefore, \(\{x_n\}\) converges to \((1, 0)\).

Now we will look at generalising the notion of distance one step further than norms on vector spaces. We will throw away the linear structure so that we are left with a metric on a set.

5.3 Metrics

A norm \(\|\cdot\|\) can be used to find the distance between two elements \(x\) and \(y\) of a vector space \(V\) by simply computing \(\|x - y\|\). This gives us a function that takes pairs from \(V \times V\) and gives them a non-negative value in \(\mathbb{R}\). We will see that this idea of measuring distance can be extended beyond norms on vector spaces; we just need a similar type of function on a set \(X\) which has the same properties as the example arising from a norm.

Definition 5.3.1 (Metric). Given a nonempty set \(X\), a function \(d : X \times X \to \mathbb{R}\) is a metric if it satisfies the following axioms:

(i) \(d(x, y) \geq 0\) for all \(x, y \in X\),

(ii) \(d(x, y) = 0\) if and only if \(x = y\),

(iii) \(d(x, y) = d(y, x)\) for all \(x, y \in X\),

(iv) \(d(x, y) \leq d(x, z) + d(z, y)\) for all \(x, y, z \in X\).

We say that \([X, d]\) is a metric space.

Notice that the function defined by \(d(x, y) := \|x - y\|\) arising from a normed vector space \([V, \|\cdot\|]\) satisfies these properties directly from the definition of a norm.

The great analyst Maurice Fréchet (1878 – 1973) introduced the idea of a metric on a set in his doctoral dissertation (Sur quelques points du calcul fonctionnel): “On some points of functional calculus”), though the term metric was first coined by Hausdorff.
Example 5.3.2 (A metric not arising from a norm; the discrete metric). Let $X$ be a set and define $d : X \times X \to \mathbb{R}$ by

$$d(x,y) := \begin{cases} 1 & \text{if } x \neq y \\ 0 & \text{if } x = y. \end{cases}$$

Clearly $d$ satisfies (i), (ii) and (iii) of Definition 5.3.1. For the triangle inequality, part (iv), let us consider $x, y, z \in X$. If $x = y$, then clearly $d(x,y) = 0$ and $d(x,z) + d(z,y) = 1 = d(x,y)$. Hence in all cases, we have $d(x,y) \leq d(x,z) + d(z,y)$.

Therefore, $d(z,y) = 0$ and $d(x,z) = 1$, giving us $d(x,z) + d(z,y) = 1 = d(x,y)$. Hence in all cases, we have $d(x,y) \leq d(x,z) + d(z,y)$.

Almost everything that works for normed vector spaces can be extended to metric spaces. The canonical open sets, the balls of normed vector spaces, have a direct analogue in the theory of metric spaces.

Definition 5.3.3 (Balls of metric spaces). Let $x$ be an element of a metric space $[X,d]$. Then the (open) ball of radius $r \in \mathbb{R}^+$ about the element $x$ is the set

$$B_r(x) := \{ y \in X : d(x,y) < r \}.$$

Example 5.3.4 (Manhattan metric). The Manhattan metric $d_M$ on $\mathbb{R}^2$ is defined by

$$d_M((x_1,x_2),(y_1,y_2)) := |x_1 - y_1| + |x_2 - y_2|$$

where $|\cdot|$ is the absolute value norm on $\mathbb{R}$.

What does a ball look like?

So we can extend the notion of a limit in a normed vector space to the context of metric spaces.

Definition 5.3.5 (Limit of a sequence in a metric space). Let $[X,d]$ be a metric space, let $(s_n)$ be a sequence in $X$, and let $x \in X$. We say that $x$ is the limit of $(s_n)$ or that $(s_n)$ converges to $x$ if for every $\varepsilon \in \mathbb{R}^+$, there exists $N \in \mathbb{N}$ such that

$$n > N \implies s_n \in B_\varepsilon(x).$$

Example 5.3.6 (Post-Office metric). The Post-Office metric $d_P$ on $\mathbb{R}^2$ is defined by

$$d_P(x,y) := \begin{cases} ||x|| + ||y|| & \text{if } x \neq y \\ 0 & \text{if } x = y \end{cases}$$

where $||\cdot||$ is the Euclidean norm. What does a ball look like here?

$$B_r(x) = \{ y \in \mathbb{R}^2 : d_P(x,y) < r \} = \{ y \in \mathbb{R}^2 : ||y|| < r - ||x|| \text{ or } x = y \} = \{ y \in \mathbb{R}^2 : ||y|| < r - ||x|| \} \cup \{ x \}$$

In particular, the sequence from Example 5.2.2 does not converge to $(1,0)$. It turns out (see Exercise 5.6.1) that this metric does not arise from a norm!
Example 5.3.7 (Radar-screen metric). Let \([V, \| \cdot \|]\) be a normed vector space. The radar-screen metric \(d_r\) for \([V, \| \cdot \|]\) is defined by
\[
d_r(x, y) = \min\{1, \|x - y\|\}.
\]

What does a ball look like? Does the sequence from Example 5.2.2 converge? Does this metric arise from a norm?

Example 5.3.8 (Induced metric). Let \(S\) be a subset of a metric space \([X, d]\). Then \(d\) induces a metric \(d_{\mid S}\) on \(S\), where we define \(d_{\mid S}\) to be identical to \(d\) on \(S\).

5.4 Boundedness

Just as we did for normed vector spaces, we can readily extend the notion of a bounded set, a bounded function or a bounded sequence to metric spaces. A subset \(W\) of a metric space \([X, d]\) is bounded if it is contained in some ball:
\[
W \subseteq B_r(a), \quad \exists a \in X, r \in \mathbb{R}^+.
\]

Likewise, a sequence is bounded if the whole sequence is contained in some ball. Finally, a function whose codomain is a metric space is bounded if its image is contained in a ball.

Example 5.4.1. Every nonempty subset \(S\) of a discrete metric space \([X, d]\) is bounded. Just take an element \(s \in S\) and the ball \(B_2(s)\). Then every element of \(X\) is contained in \(B_2(s)\).

Example 5.4.2. The set of natural numbers \(\mathbb{N}\) is unbounded in \(\mathbb{R}\) with respect to the Euclidean metric. There is no open interval big enough that contains \(\mathbb{N}\).

The brilliant insight of Fréchet and Hausdorff was that the theory of metric spaces has many of the properties as functions on Euclidean space have. For example, there are unique limits of convergent sequences and such sequences do not ramble off too infinity. In the generality of topological spaces, this is not true!

Theorem 5.4.3. In a metric space \([X, d]\), a convergent sequence has a unique limit.

\[ \star \text{ Proof: To be done in lectures.} \]

Theorem 5.4.4. In a metric space \([X, d]\), a convergent sequence is bounded.

\[ \star \text{ Proof: To be done in lectures.} \]

5.5 Cauchy sequences

The Babylonians (1800–1600BC) had a sophisticated method for finding \(\sqrt{2}\). First, it was known that \(\sqrt{2}\) is the length of the side of a rectangle that has area 2, and their idea was to approximate such a square with rational rectangles. Start with a \(2 \times 1\) rectangle\(^2\) and draw the line \(\text{‘}y = x\text{’}\). This line meets the other side of the rectangle with \(x\)-coordinate 1, and so we take the

\[ \text{\textsuperscript{2} it has an area of } 2 \]
average of this \( x \)-coordinate with the width of the rectangle: \( \frac{3}{2} \). The next rectangle we draw has width \( \frac{1}{2} \) and height \( \frac{2}{3} \). This time, the diagonal meets the top-side of the rectangle in a point with \( x \)-coordinate equal to \( \frac{4}{3} \), and so take the average of this \( x \)-coordinate with the width of the rectangle: \( \frac{4}{3} + \frac{1}{2} \). Continuing in this way, the rectangle quickly converges to a square with side lengths equal to \( \sqrt{2} \).

If we look at the height of this rectangle, we obtain a sequence:

\[
x_{n+1} := \frac{x_n}{2} + \frac{1}{x_n}, \quad x_1 = 1.
\]

If we are living in a world only of rational numbers (such as the Babylonians did), then we would not know what this sequence is converging to. But we do know that what ever it is, its square is equal to 2. Notice that if it happened that \( x_2^2 = 2 \), then we would have

\[
x_2^2 = (x_1/2 + 1/x_1)^2 = x_1^2/4 + 1 + 1/x_1^2 = \frac{1}{2} + 1 + \frac{1}{2} = 2.
\]

That is, the sequence would be a constant sequence where every element would have square equal to 2. This is an example of a Cauchy sequence, or if you like, convergence of a sequence without a designated limit. The sequence gets closer and closer to itself! More mathematically, no matter what window we allow, at some point, the envelope of the sequence has a width less than that of the window.

**Definition 5.5.1** (Cauchy sequence). Let \([X, d]\) be a metric space and let \( \{x_n\} \) be a sequence in this metric space. We say that \( \{x_n\} \) is a Cauchy sequence, if for every \( \epsilon \in \mathbb{R}^+ \), there is a number \( N \in \mathbb{N} \) such that for all \( n, m, \)

\[
n, m > N \implies d(x_n, x_m) < \epsilon.
\]

**Example 5.5.2.** Consider the metric space on the open unit interval \((0, 1)\) with the Euclidean metric \( d \). We will show that the following sequence is a Cauchy sequence, but it has no limit in \((0, 1)\):

\[
x_n := 1 - \frac{1}{10^n}.
\]

Let \( \epsilon \in \mathbb{R}^+ \). Choose \( N \) to be an integer greater than \( \log_{10}(\frac{1}{\epsilon}) \) and suppose \( n \geq m > N \).

Then \( m > \log_{10}(\frac{1}{\epsilon}) \).

Then \( \frac{1}{10^m} < \epsilon \).

Then \( \frac{1}{10^m} = \frac{1}{10^m} < \epsilon \).

Then \( (1 - \frac{1}{10^m}) - (1 - \frac{1}{10^n}) < \epsilon \).

Then \( |x_n - x_m| < \epsilon \).

Then \( d(x_n, x_m) < \epsilon \).

Therefore, \( \{x_n\} \) is a Cauchy sequence.
Example 5.5.3. Back to our original example. The metric space is \([\mathbb{Q}, d]\) where \(d\) is the Euclidean metric, and the sequence is

\[x_{n+1} := x_n / 2 + 1 / x_n, \quad x_1 = 1.\]

Let \(\epsilon \in \mathbb{R}^+\). What should we choose for \(N\) so that \(n, m > N \implies d(x_n, x_m) < \epsilon\)?

Theorem 5.5.4 (Convergent implies Cauchy implies bounded). Let \(\{s_n\}\) be a sequence in a metric space \([X, d]\).

(i) If \(\{s_n\}\) is convergent, then it is also a Cauchy sequence.

(ii) If \(\{s_n\}\) is a Cauchy sequence, then it is bounded.

⋆ Proof: To be done in lectures. □

5.6 Exercises

Exercise 5.6.1. Show (by proof by contradiction) that the Post-Office metric (Example 5.3.6) does not arise from a norm.

Exercise 5.6.2. Here we explore the Manhattan metric on \(\mathbb{R}^n\):

\[d(x, y) := \sum |x_i - y_i|\]

where \(x_i\) is the \(i\)-th component of \(x\), and similarly for \(y\).

(i) Prove that \(d\) defines a metric\(^3\) on \(\mathbb{R}^n\).

(ii) Assume now that \(n = 2\). Draw the unit ball \(B_1(0)\) around the origin, with respect to \(d\).

(iii) Consider the sequence

\[s_n := \left(1 + \frac{(-1)^n}{n}, (-1)^n + 1/n\right), \quad n = 1, 2, 3, \ldots\]

(a) Plot the first ten points of the sequence.

(b) Let \(\ell := (1, 0)\). Find a positive number \(\epsilon\) so that for every \(n, d(s_n, \ell) > \epsilon\).

What have we shown?

Exercise 5.6.3. Consider the following sequence

\[x_n := -\sum_{i=1}^n (-1)^i \frac{4}{2i - 1}.

(a) Compute \(x_1, x_2, x_3, x_4\) and \(x_5\).

(b) It looks like this sequence is convergent. What do you think this sequence is convergent to?

(c) Simplify

\[|x_{m+1} - x_m|\].

\(^3\) You may assume that the Euclidean norm on \(\mathbb{R}\) is a metric.
(d) Let \( m, n \in \mathbb{N} \) and suppose \( n > m \). Show that 
\[
|x_n - x_m| \leq |x_{m+1} - x_m|.
\]

(e) Suppose \( \epsilon = 0.1 \). Find \( N \in \mathbb{N} \) such that for all \( n, m > N \),
\[
|x_n - x_m| < \epsilon.
\]

Exercise 5.6.4. In this exercise, we will show that the sequence \( \{1/n\} \) is a Cauchy sequence in the open interval \((0, 2)\) (w.r.t., the Euclidean metric).

(i) Write the start of the proof.

(ii) Suppose, without loss of generality, that \( n \geq m > N \). Show that
\[
\left| \frac{1}{m} - \frac{1}{n} \right| \leq \frac{1}{m}
\]
and hence make a suitable, and simple, choice for \( N \) in terms of \( \epsilon \).

(iii) Write the remainder of your proof, starting with “Choose \( N = \ldots \) and suppose \( m, n \in \mathbb{N} \) such that \( m, n > N \). Then ...”.

Exercise 5.6.5. Give an example of a sequence \( \{x_n\} \) of real numbers (w.r.t., the Euclidean metric) such that
\[
(\forall \epsilon \in \mathbb{Q}^+)(\exists N \in \mathbb{N})(\forall n \in \mathbb{N}) \quad n > N \implies |x_{n+1} - x_n| < \epsilon
\]
but is NOT a Cauchy sequence.

5.7 Complete metric spaces

Normed vector spaces are an important framework for the applications of mathematics in science and engineering, and in order to have ‘calculus’ work on normed vector spaces, we need the notion of a complete normed vector space. These are also known as Banach spaces after the great polish mathematician Stefan Banach (1892 – 1945). The Fréchet derivative on a normed vector space is then defined as a generalisation of the usual derivative that one encounters with real-valued functions. In particle physics and quantum mechanics, the notion of a Hilbert space is vitally important: it is just a complex Banach space equipped with an inner product.

Suppose we want to find a solution to the following differential equation:
\[
f'(x) = \frac{1}{4}(f(x)^2 + x^2), \quad f(0) = 0,
\]
where \( f \) is a function from the closed interval \([-\frac{1}{2}, \frac{1}{2}]\) to \( \mathbb{R} \).

• How do we know that this differential equation has a solution?

• Can the solution be written out nicely in terms of functions we already know?

By the end of this chapter, we will have a solution to this question that uses the theory of complete metric spaces and contraction maps.
Definition 5.7.1 (Complete metric space). A metric space \([X, d]\) is complete if every Cauchy sequence in \([X, d]\) converges (to an element of \([X, d]\)).

If \(X\) is a normed vector space and is complete, then we call it a Banach space. Throughout, we will denote the Euclidean metric by \(d_E\).

Example 5.7.2. \([\mathbb{Q}, d_E]\) is not complete. Consider the sequence in Example 5.5.3:
\[
x_{n+1} := x_n/2 + 1/x_n, \quad x_1 = 1.
\]
This is a Cauchy sequence and it gives rational approximations to the real number \(\sqrt{2}\). However, \(\sqrt{2}\) is irrational and so this Cauchy sequence does not converge in \([\mathbb{Q}, d_E]\).

Example 5.7.3. \([\mathbb{R}^n, d_E]\) is complete, but we will postpone a proof of this until later. In fact, every finite dimensional vector space is complete.

Example 5.7.4. \([[(0, 2), d_E]\) is not complete. Consider the following Cauchy sequence:
\[
x_n := 2 - 1/n.
\]
The sequence is increasing but has no limit in \((0, 2)\).

Example 5.7.5. A discrete metric space is always complete. Let \([X, d]\) be a discrete metric space and let \(\{x_n\}\) be a Cauchy sequence in \([X, d]\). Then there exists \(N \in \mathbb{N}\) such that
\[d(x_n, x_m) < 1\]
for all \(m, n > N\). Moreover,
\[d(x_n, x_{N+1}) < 1\]
for all \(n > N\) which means that \(x_n = x_{N+1}\) (for all \(n > N\)) by definition of the discrete metric. So we see that \(\{x_n\}\) converges to \(x_{N+1}\).

5.8 The ring of Cauchy sequences

We have already seen the vector space of all functions \(F(X, V)\) from a set \(X\) to a vector space \(V\), and that a sequence in a metric space \([X, d]\) is just a function \(\mathbb{N} \to X\). Let us consider just the metric space \([\mathbb{Q}, d_E]\) and the set of all Cauchy sequences \(R\) in \([\mathbb{Q}, d_E]\). We will show that \(R\) is a ring under suitably defined operations of addition and multiplication.

Addition of Cauchy sequences: Given two Cauchy sequences \(\{x_n\}\) and \(\{y_n\}\) in \([\mathbb{Q}, d_E]\), define a new sequence \(\{z_n\}\) by the term-by-term sum:
\[z_n := x_n + y_n.\]

Multiplication of Cauchy sequences: Given two Cauchy sequences \(\{x_n\}\) and \(\{y_n\}\) in \([\mathbb{Q}, d_E]\), define a new sequence \(\{z_n\}\) by the term-by-term product:
\[z_n := x_n \cdot y_n.\]

The two constructions above yield Cauchy sequences.

Lemma 5.8.1. The term-by-term sum and product of two Cauchy sequences of \([\mathbb{Q}, d_E]\) are also Cauchy sequences.
The zero-Cauchy sequence is just the constant sequence $0$ and the unit-Cauchy sequence is just the constant sequence $1$. We leave it as an exercise to verify that these two sequences serve as additive and multiplicative identities for $R$ (respectively).

**Definition 5.8.2 (Null sequence).** A sequence $\{x_n\}$ in $[\mathbb{Q}, d_E]$ is null if it converges to $0$.

By Theorem 5.5.4, a null sequence is a Cauchy sequence. In fact, the set of all null sequences not only forms a subring of $R$, but it is an ideal.

**Theorem 5.8.3.** The set of all null sequences of $[\mathbb{Q}, d_E]$ forms an ideal of $R$.

**Proof:** To be done in lectures.

This means that we can take a quotient of $R$ by the null sequences. In this course, this means that there is a nice equivalence relation on $R$, which we will use to define the real numbers.

### 5.9 Construction of the real numbers

**Definition 5.9.1 (Equivalence of rational Cauchy sequences).** For two Cauchy sequences $\{x_n\}$ and $\{y_n\}$ in $[\mathbb{Q}, d_E]$, we say that they are equivalent and write $\{x_n\} \sim \{y_n\}$ if and only if the term-by-term difference $\{x_n\} - \{y_n\}$ is a null sequence.

**Example 5.9.2.** The sequence $\{1/n\}$ is equivalent to $\{-1/n\}$, which is in turn equivalent to the zero-sequence!

**Lemma 5.9.3.** The relation $\sim$ on $R$ is an equivalence relation.

**Proof:** To be done in lectures.

Now for the construction of the real numbers:

The real numbers are defined to be the equivalence classes of $\sim$.

So what is $\mathbb{Q}$ as a subset of $\mathbb{R}$?

**Lemma 5.9.4.** The function $x \rightarrow \overline{x}$, where $\overline{x}$ is the constant sequence $x, x, x, \ldots$ is a one-to-one function from $\mathbb{Q}$ to $\mathbb{R}$. Moreover, if $x, y \in \mathbb{Q}$, then $\overline{x} \sim \overline{y}$ if and only if $x = y$.

**Example 5.9.5.** The only real numbers representable by Cauchy sequences of integers are the integers! Let’s see why this is true. Suppose we have a Cauchy sequence $\{x_n\}$ of integers. Then the difference of any two unequal members of the sequence is at least 1. So let $\epsilon = 1/2$. Since $\{x_n\}$ is a Cauchy sequence, there is some $N \in \mathbb{N}$ such that for every $n, m > N$ we have $|x_n - x_m| < \epsilon = 1/2$. This condition forces $x_n = x_m$ (as they are integers) which in turn implies that the subsequence $\{x_n : n > N\}$ is the constant sequence $\{x_{N+1}\}$. 

That is, 0 is the sequence $0, 0, 0, \ldots$, and 1 is the sequence $1, 1, 1, \ldots$. 

![Figure 5.4: A Cauchy sequence of integers will eventually become a constant sequence.](image-url)
5.10 Arithmetic on \( \mathbb{R} \)

Now that we have finally defined the real numbers by simpler things (i.e., rational numbers), we can review how addition and multiplication are defined on real numbers in the way we have defined them. In fact, we have essentially already seen our arithmetic works on \( \mathbb{R} \) when we defined the term-by-term sums and products of Cauchy sequences.

**Addition on \( \mathbb{R} \):** Given two real numbers \([x_n]\) and \([y_n]\), define
\[
[x_n] + [y_n] := [x_n + y_n].
\]

**Multiplication on \( \mathbb{R} \):** Given two real numbers \([x_n]\) and \([y_n]\), define
\[
[x_n] \cdot [y_n] := [x_n y_n].
\]

Are these operations well-defined? Let us look at addition and leave multiplication as an exercise. Suppose we have \([x_n] = [x'_n]\) and \([y_n] = [y'_n]\). Then \([x_n]\) and \([x'_n]\), and \([y_n]\) and \([y'_n]\), differ by null sequences:

- \([x'_n] = [x_n] + [u_n]\), where \([u_n]\) converges to 0;
- \([y'_n] = [y_n] + [v_n]\), where \([v_n]\) converges to 0.

So
\[
[x'_n] + [y'_n] = [x_n] + [u_n] + [y_n] + [v_n]
\]
and \([u_n] + [v_n]\) is also a null sequence as the set of null sequences is a subring of the Cauchy sequences. Therefore,
\[
[x'_n] + [y'_n] \sim [x_n] + [y_n]
\]
and hence
\[
[x'_n] + [y'_n] = [x_n] + [y_n].
\]

So addition is well-defined.

In fact, it would then be not difficult to show (though tedious) that \( \mathbb{R} \) forms a ring under these operations, as we would hope it would! To show that \( \mathbb{R} \) is a field requires showing that every nonzero element has an inverse, which we have left as Exercise 5.18.4.

5.11 What does 0.99999 \ldots mean?

A decimal expansion such as 0.717171717 \ldots can be realised from a sequence of rational numbers:
\[
0.71, 0.7171, 0.717171, 0.71717171, \ldots.
\]

In other words, the real number we have written above is the equivalence class of the sequence
\[
\{\frac{71}{10^{2n}}\}.
\]

It turns out that this sequence is actually a rational number since
\[
\{\frac{71}{10^{2n}}\} \sim \{\frac{71}{99}\}.
\]
What about 0.999999...? This is really the real number whose Cauchy sequence of rationals is
\[\{1 - 1/10^n\}\].
Consider the unit-sequence \(\frac{1}{n}\) = \(\{1\}\). If we look at the term-by-term difference of these two sequences, we obtain
\[\{1/10^n\}\]
which converges to 0; it is a null-sequence! So we formally consider the two sequences \(\{1 - 1/10^n\}\) and \(\{1\}\) to be the same: they are equivalent Cauchy sequences of rational numbers and so represent the same real number. That is,
\[1 = 0.99999 \cdots\].

5.12 Aside: other ways to construct \(\mathbb{R}\)

There are two other mainstream ways of defining the real numbers in mathematics. One is the famous ‘Dedekind cuts’ method, the other is more abstract and arises in the theory of field extensions. The latter can be found in a book on ring theory and you would find it under the topic of transcendental extensions of the rational numbers. We will explain here the former and easier notion of Dedekind cuts (see also page 194 of Liebeck’s book).

A nonempty subset \(X\) of the rational numbers \(\mathbb{Q}\) is called a Dedekind cut if it satisfies the following conditions:

- for any \(x \in X\), we have that \(X\) contains all the rationals less than \(x\);
- \(X\) has no maximum.

For example, \(X := \{x \in \mathbb{Q} : x < \frac{2}{5}\}\) is a Dedekind cut.

Now for the construction of the real numbers:

\[
\mathbb{R}
\]

The real numbers are the set of all Dedekind cuts of \(\mathbb{Q}\).

So what is \(\mathbb{Q}\) as a subset of \(\mathbb{R}\)? Well, for \(q \in \mathbb{Q}\), the Dedekind cut \(X_q := \{x \in \mathbb{Q} : x < q\}\) represents \(q\). We can make this notion stronger by noting that the map \(q \mapsto X_q\) is a one-to-one function. Moreover, real numbers like \(\sqrt{2}\) are defined as
\[\{q \in \mathbb{Q} : q^2 < 2 \text{ or } q \leq 0\}\].
We can also define addition and multiplication on \(\mathbb{R}\).

\[\text{Addition on } \mathbb{R}: \text{ Given two real numbers }^5 X \text{ and } Y, \text{ define } X + Y := \{x + y : x \in X, y \in Y\}.\]

One can show that this operation gives us a Dedekind cut.

\[^5\text{ Remember, a real number in this small section is a Dedekind cut of rationals.}\]
Multiplication on \( \mathbb{R} \): This one is more complicated. Given two positive real numbers \( X \) and \( Y \), define
\[
X \cdot Y := \mathbb{Q}^{-} \cup [0] \cup \{xy : x \in X \cap \mathbb{Q}^+, y \in Y \cap \mathbb{Q}^+\}.
\]
Something similar can be done for non-positive real numbers. Again, it is not difficult to see that this operation gives us a Dedekind cut.

So why does it give us a structure that it the same as the set of equivalence classes of Cauchy sequences? This question does not have a short answer, though the interested reader may want to delve deeper to find out why these two definitions are equivalent ways to construct \( \mathbb{R} \).

5.13 The topology of metric spaces

In the study of topology which you will see more of in 3rd year, the key notion is that of an open set. This is yet another level of abstraction of “closeness” and allows one to analyse interesting spaces that are not metric spaces. We will see how this works in metric spaces as preparation for a course in point-set topology.

Definition 5.13.1 (Open set). A subset \( S \) of a metric space \([X,d]\) is open if and only if \( S \) is a union of open balls.

In other words, every point \( x \in S \) lies inside a ball \( B_r(x) \subseteq S \).

Example 5.13.2. The trivial examples of open sets are the empty set \( \emptyset \) and the whole metric space \( X \) itself. An open ball itself is open.

Example 5.13.3. Subspaces of metric spaces can offer counter-intuitive ways to create open sets. Take for instance closed interval \([0,1]\) equipped with the Euclidean metric. Then the subset \([0,\frac{1}{2}]\) is an open set! To see this, suppose we have an element \( x \in [0,\frac{1}{2}] \). Then either \( x \in (0,\frac{1}{2}) \), and we can easily find an open ball centered at \( x \) contained in \([0,\frac{1}{2}]\), or \( x = 0 \). If \( x = 0 \), then we take \( B_{\frac{1}{2}}(x) \), which is just \([0,\frac{1}{2}]\) and is contained in \([0,\frac{1}{2}]\).

Example 5.13.4. In a discrete metric space, every singleton subset is open. Take a singleton subset \( \{x\} \). Then the only element of this set is \( x \) and the ball \( B_{\frac{1}{2}}(x) \) is just \( \{x\} \).

The next lemma tells us that in a discrete metric space, every subset is open. The two properties outlined in the lemma essentially give us the axioms of a topological space, which you will see more of in 3rd year mathematics.

Lemma 5.13.5. Let \([X,d]\) be a metric space.

(a) An intersection of finitely many open sets of \([X,d]\) is an open set.

(b) Any union of open sets of \([X,d]\) is an open set.

\( \diamond \) Proof:

(a) Let \( \{O_1, O_2, \ldots, O_n\} \) be a finite collection of open sets in \([X,d]\). Let \( x \in \bigcap_{i=1}^{n} O_i \). So \( x \in O_i \) for every \( i \). Then for each \( i \), there is a ball \( B_{\epsilon_i}(x) \) contained in \( O_i \). Now \( \{\epsilon_i : i = 1, 2, \ldots, n\} \) is a finite set of real numbers.

From a Dedekind cut \( X \), select an element \( x_1 \in X \) and an element \( y_1 \in Q/X \). Now define for each \( n \geq 2 \) the following two coupled sequences where we take averages at each step:

\[
x_n := \begin{cases} \frac{x_{n-1} + y_{n-1}}{2} & \text{if } \frac{x_{n-1} + y_{n-1}}{2} \in Q \\ y_{n-1} & \text{otherwise.} \end{cases}
\]

\[
y_n := \begin{cases} \frac{x_{n-1} + y_{n-1}}{2} & \text{if } \frac{x_{n-1} + y_{n-1}}{2} \in Q \\ y_{n-1} & \text{otherwise.} \end{cases}
\]

It turns out that \( \{x_n\} \) is a Cauchy sequence of rational numbers.
and so there exists a minimum value, say \( \epsilon_{\min} \) of this set. Then \( B_{\epsilon_{\min}}(x) \) is contained in each \( O_i \), and therefore, is contained in \( \bigcap_{i=1}^{n} O_i \). Thus, \( \bigcap_{i=1}^{n} O_i \) is open.

(b) Let \( \{O_i : i \in I\} \) be a collection of open sets of \( [X,d] \), where \( I \) is just an index set. Let \( x \in \bigcup_{i \in I} O_i \). So there exists \( i \in I \) such that \( x \in O_i \). Since \( O_i \) is open, there exists a ball \( B_\epsilon(x) \) contained in \( O_i \). This ball is certainly contained in \( \bigcup_{i \in I} O_i \), and so we have shown that \( \bigcup_{i \in I} O_i \) is open.

\[ \square \]

A closed set is something like a closed interval, such as \([0,1]\). One of the most common mistakes of students is that they think that the opposite of open is closed, as we would in normal everyday language. However, in mathematics, this is not true! We will see examples of sets which are neither open or closed, and examples which are both open and closed.

**Definition 5.13.6** (Closed set). A subset \( C \) of a metric space \([X,d]\) is **closed** if and only if its complement \( X \setminus C \) is open.

**Example 5.13.7.** A set which is both closed and open is said to be clopen. For example, the subset

\[ \{x \in \mathbb{Q} : x^2 > 2\} \]

of \([\mathbb{Q},d_E]\) is clopen. We will leave the proof of this to Exercise 5.18.6.

One of the most useful results in the theory of metric spaces is the characterisation of closed subsets by convergent sequences.

**Lemma 5.13.8.** Let \( C \) be a closed subset of a metric space \([X,d]\). Then every convergent sequence \( \{x_n\} \) of elements of \( C \) has its limit in \( C \).

\[ \diamond \text{ Proof: } \] To be done in lectures. \[ \square \]

And conversely …

**Lemma 5.13.9.** Let \( Y \) be a subset of a metric space \([X,d]\) such that every convergent sequence \( \{y_n\} \) of elements of \( Y \) has its limit in \( Y \). Then \( Y \) closed.

\[ \diamond \text{ Proof: } \] To be done in lectures. \[ \square \]

The next result will be important when we look at sequences of functions, and is the one of the first key results in the theory of Hilbert spaces.

**Theorem 5.13.10.** Let \([X,d]\) be a metric space and let \( Y \) be a subset of \( X \).

(i) If \([X,d]\) is complete and \( Y \) is closed then \([Y,d \upharpoonright_Y]\) is complete.

(ii) If \([Y,d \upharpoonright_Y]\) is complete, then \( Y \) is closed.

\[ \diamond \text{ Proof: } \] To be done in lectures. \[ \square \]
5.14 Continuity revisited

Recall from Definition 1.7.15 that if \( f : X \to Y \) is a function, and \( S \subseteq Y \), then the preimage of \( S \) under \( f \) is the subset of \( X \) defined by

\[
\begin{align*}
\{ x \in X : f(x) \in S \}.
\end{align*}
\]

The topological definition of continuity does not need \( \epsilon \) or \( \delta \), and is a beautiful and succinct way to define a continuous function on metric spaces: the preimage of any open set is open. We prove now that the topological definition fits with our usual notion of continuity.

**Theorem 5.14.1.** Let \([X, d]\) and \([Y, e]\) be two metric spaces and let \( f : X \to Y \) be a function. Then \( f \) is continuous if and only if the preimage of any open set of \( Y \) is an open set of \( X \).

\[ \Box \]

**Proof:** To be done in lectures.

5.15 Function spaces as metric spaces

Consider the following functions on the closed interval \([0, 1]\):

\[ f_n(x) := x^n, \quad n \in \mathbb{N}. \]

The functions seem to converge to another function:

\[
\begin{align*}
f(x) := \begin{cases} 
1 & \text{if } x = 1 \\
0 & \text{otherwise.}
\end{cases}
\end{align*}
\]

But what does convergence of functions mean? The problem is that we have drawn the function, so what we are seeing is that the graph of \( f_n \) converges to the graph of \( f \). In other words

for every \( x \), the limit of \( f_n(x) \) as \( n \to \infty \) is \( f(x) \).

This is what we call \textit{point-wise convergence}. We see here that with this notion of convergence, the limit of a sequence of continuous functions is a discontinuous function!

We shall explore now the notion of \textit{uniform-convergence} of functions which preserves continuity. The difference between the two forms of convergence is that instead of thinking about the values of \( f_n \) and what they tend to, we just look at the \textbf{functions themselves}.

**Example 5.15.1.** Consider the set of bounded functions \( \mathcal{B}([0, 1], \mathbb{R}) \) on the closed interval \([0, 1]\). We have seen in Section 4.7 that \( \mathcal{B}([0, 1], \mathbb{R}) \) is a normed vector space when equipped with the \textquote{sup}-norm (see Example 4.7.3). This norm gives us the sup-metric so that \( \mathcal{B}([0, 1], \mathbb{R}) \) can be viewed as a metric space:

\[
d_{\infty}(f, g) := \|f - g\| = \sup\{|f(x) - g(x)| : x \in [0, 1]|.
\]

This is given us a notion of the distance between two functions. So let us look at the previous example, where we had a sequence of functions \( \{f_n\} \)
that point-wise converge to a discontinuous function \( f \). Then for each \( n \in \mathbb{N} \), we have

\[
d_{\infty}(f_n, f) = \sup \{|f_n(x) - f(x)| : x \in [0, 1]\}
= \sup \{|x^n - 0| : x \in [0, 1]\}
= 1.
\]

So with respect to the sup-metric, the sequence \( \{f_n\} \) does not converge!

**Example 5.15.2.** Now we look at a different sequence of functions, this time on the closed interval \([-\pi, \pi] \):

\[ g_n(x) := \frac{1}{n} \cos(nx), \quad n \in \mathbb{N} \]

This time, it seems the drawing of \( g_n \) converges to the x-axis, that is, the zero function \( 0 \). We will see in this example that it also converges in \( \mathcal{B}([-\pi, \pi], \mathbb{R}), d_{\infty} \) to the same function (which is continuous (by the way). Now

\[
d_{\infty}(g_n, 0) = \sup \{|g_n(x) - 0| : x \in [-\pi, \pi]\}
= \sup \{|\frac{1}{n}\cos(nx)| : x \in [-\pi, \pi]\}
= \frac{1}{n} \sup \{ |\cos(nx)| : x \in [-\pi, \pi]\}
= \frac{1}{n}.
\]

So here we see that \( d(g_n, 0) \) tends to 0 as \( n \) tends to infinity, and therefore, \( g_n \), as a function, tends to 0.

These two examples are interesting from another perspective. The first sequence of functions (Example 5.15.1) was not convergent in \( \mathcal{B}([0, 1], \mathbb{R}), d_{\infty} \), and nor was it a Cauchy sequence (see Exercise 5.18.9). The second example (Example 5.15.2) is a convergent sequence in \( \mathcal{B}([-\pi, \pi], \mathbb{R}), d_{\infty} \), and so by Theorem 5.5.4, it is also a Cauchy sequence. In fact, we will prove now and important result about bounded functions; they form a complete metric space.

**Theorem 5.15.3.** For any nonempty set \( X \), we have that \( \mathcal{B}(X, \mathbb{R}), d_{\infty} \) is complete.

\[ \star \text{ Proof: } \] To be done in lectures.

**Theorem 5.15.4.** For any nonempty set \( X \), the subspace of bounded continuous functions \( C(X, \mathbb{R}), d_{\infty} \) is closed and hence complete.

\[ \diamond \text{ Proof: } \] To be done in lectures.

5.16 Contraction maps

**Definition 5.16.1** (Lipschitz function). Suppose \( [X, d] \) and \( [Y, e] \) are metric spaces. A function \( f : X \to Y \) is Lipschitz if there is a constant \( c \in \mathbb{R}^+ \) such that for every \( x_1, x_2 \in X \) we have

\[ e(f(x_1), f(x_2)) \leq c \cdot d(x_1, x_2). \]

We call the smallest possible value of \( c \) the Lipschitz constant of \( f \).
Example 5.16.2.

(a) The function
\[ f : \mathbb{R} \to \mathbb{R} : x \mapsto c|x| \]
is Lipschitz with Lipschitz constant \( c \).

(b) \( g : \mathbb{R} \to \mathbb{R} : x \mapsto x^2 \) is not Lipschitz.

(c) \( h : [-1, 1] \to \mathbb{R} : x \mapsto x^2 \) is Lipschitz with Lipschitz constant 2.

Lemma 5.16.3. Lipschitz functions are continuous.

\[ \diamond \text{ Proof: Suppose } [X, d] \text{ and } [Y, e] \text{ are metric spaces and suppose } f : X \to Y \text{ is Lipschitz with Lipschitz constant } c \in \mathbb{R}^+. \text{ Suppose } \epsilon > 0 \text{ and let } x \in X. \text{ Choose } \delta = \epsilon / c. \text{ Now if } y \in B_\delta(x), \text{ then } f(y) \text{ would lie inside the closed ball } B_{c \cdot d(x,y)}(f(x)) \text{ which in turn is a subset of } B_\epsilon(f(x)), \text{ and hence, } f \text{ is continuous at every point.} \]

In fact, the set of bounded Lipschitz functions in \( B(X, \mathbb{R}) \) form a closed subset of \( C(X, \mathbb{R}) \), and hence they are complete.

Definition 5.16.4 (Contraction map). Suppose \([X, d]\) and \([Y, e]\) are metric spaces. A Lipschitz function \( f : X \to Y \) is a contraction map if its Lipschitz constant is less than 1.

A fixed point of a function \( f : X \to X \) is an element \( x \in X \) such that \( f(x) = x \).

Example 5.16.5.

(a) The map \((x, y) \mapsto (x^2 + x - 1, y)\) on \( \mathbb{R}^2 \) has two fixed points: \((0, 0)\) and \((-1, 0)\). We will see from the theorem below that it is not a contraction map.

(b) The map \((x, y) \mapsto (x, y \begin{bmatrix} 0.4 & -0.5 \\ 0.5 & 0.5 \end{bmatrix} + (1, 0))\) is a contraction map.\(^6\) Why?

Now it fixes the point \((x, y)\) if and only if \((0.4x + 0.5y + 1, -0.5x + 0.5y) = (x, y)\). So we see that this contraction map has a unique fixed point, namely \((10/11, -10/11)\).

Theorem 5.16.6 (Banach’s Contraction Mapping Theorem). Suppose \([X, d]\) is a nonempty complete metric space, and we have a contraction map \( f : X \to X \). Then there exists a unique point \( x \in X \) such that \( f(x) = x \).

\[ \star \text{ Proof: To be done in lectures.} \]

Example 5.16.7. Now we return to our original example. Suppose we want to find a solution to the following differential equation:

\[ f'(x) = \frac{1}{4}(f(x)^2 + x^2), \quad f(0) = 0, \]

where \( f \) is a function from the closed interval \([-\frac{1}{2}, \frac{3}{2}]\) to \( \mathbb{R} \).

- How do we know that this differential equation has a solution?
Can the solution be written out nicely in terms of functions we already know?

First we use the Fundamental Theorem of Calculus to see this differential equation as an integral equation:

\[ f(x) - f(0) = \int_0^x \frac{1}{4} (f(x)^2 + x^2) \, dx \]

and hence

\[ f(x) = \int_0^x \frac{1}{4} (f(x)^2 + x^2) \, dx. \]

To make things more difficult, we will define a function \( \Phi \) on the metric space of continuous functions \( C([-\frac{1}{2}, \frac{1}{2}], \mathbb{R}) \). For such a function \( f \), define \( \Phi(f) \) to be the function that maps \( x \) to \( \int_0^x \frac{1}{4} (f(x)^2 + x^2) \, dx \). It is not difficult to see that

\[ \Phi(B_{1/2}(0)) \subset B_{1/2}(0), \]

that is, if we look at the space of functions that are distance at most \( \frac{1}{4} \) from the zero function \( 0 \) with respect to the sup-metric, then \( \Phi \) maps this set into itself. It turns out that \( \Phi \) is a contraction map on \( B_{1/2}(0) \) as we will now see.

Let \( f_1, f_2 \in B_{1/2}(0) \). Then

\[ \| \Phi(f_1) - \Phi(f_2) \|_\infty = \| \frac{1}{4} \int_0^x (f_1^2 - f_2^2) \|_\infty \]

where \( \int_0^x (f_1^2 - f_2^2) \) is the map that takes \( x \) to the definite integral \( \int_0^x (f_1^2 - f_2^2) \, dx \). Now we will use a fact from calculus that if \( f \) is continuous on the interval \([a, b]\) and \( c \in [a, b] \), then \( \| \int_a^b f \| \leq (b - a) \| f \| \). So

\[ \| \Phi(f_1) - \Phi(f_2) \|_\infty \leq \frac{1}{4} \left( \frac{1}{2} - \frac{-1}{2} \right) \| f_1^2 - f_2^2 \|_\infty \]

\[ \leq \frac{1}{4} \| f_1 - f_2 \|_\infty \| f_1 + f_2 \|_\infty \]

\[ \leq \frac{1}{4} \| f_1 - f_2 \|_\infty (\| f_1 \|_\infty + \| f_2 \|_\infty) \]

\[ \leq \frac{1}{4} \| f_1 - f_2 \|_\infty \left( \frac{1}{2} + \frac{1}{2} \right) \]

and so

\[ \| \Phi(f_1) - \Phi(f_2) \|_\infty \leq \frac{1}{4} \| f_1 - f_2 \|_\infty. \]

Therefore, \( \Phi \) is a contraction map on \( B_{1/2}(0) \) with Lipschitz constant at most \( \frac{1}{4} \). Now \( B_{1/2}(0) \) is a closed subset of a complete metric space, and so must also be complete. Therefore, by Banach’s Contraction Mapping Theorem 5.16.6, there exists a unique fixed-point of \( \Phi \).

That is, there is a continuous function \( f \in B_{1/2}(0) \) such that

\[ \Phi(f) = f, \]

which means, that \( f \) is a solution to our original differential equation.

According to mathematica, there is no nice way to write this function \( f \) in terms of functions we know!
5.17 Aside: Iteration Function System

An Iteration Function System (IFS) in \( \mathbb{R}^m \) (or a complete metric space, if you prefer) is a finite set of contraction maps \( \{ w_1, \ldots, w_m \} \) and they are used to generate interesting fractals and dynamical systems. Let \( \mathcal{H}(\mathbb{R}^m) \) be the set of all closed and bounded subsets of \( \mathbb{R}^m \). We can define a metric on this space known as the Hausdorff distance:

\[
h(A, B) := \max \{ \min \{ d_E(a, b) : b \in B \} : a \in A \}.
\]

So the Hausdorff distance is the greatest of all the distances from a point in one set to the closest point in the other set. It turns out that \( [\mathcal{H}(\mathbb{R}^m), h] \) is a complete metric space.

Now we define a function \( G \) on \( \mathcal{H}(\mathbb{R}^m) \), known as the Hutchison operator:

\[
H(B) := w_1(B) \cup w_2(B) \cup \cdots \cup w_m(B).
\]

This gives us a contraction map on \( \mathcal{H}(\mathbb{R}^m) \). So by Banach’s Contraction Mapping Theorem 5.16.6, there exists a unique closed and bounded set \( B \) that is a fixed-point of \( H \). This set \( B \) is the fractal we want to generate.

Example 5.17.1 (Barnsley’s Fern). Consider the following four functions

\[
f_i(x, y) := (x, y) \begin{bmatrix} a & b \\ c & d \end{bmatrix} + (e, f), \quad i = 1, 2, 3, 4
\]

where we extract the parameters from the following table:

<table>
<thead>
<tr>
<th>i</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0.16</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0.85</td>
<td>-0.04</td>
<td>0.04</td>
<td>0.85</td>
<td>1.6</td>
<td>0.85</td>
</tr>
<tr>
<td>3</td>
<td>0.2</td>
<td>0.23</td>
<td>0.26</td>
<td>0.22</td>
<td>1.6</td>
<td>0.07</td>
</tr>
<tr>
<td>4</td>
<td>-0.15</td>
<td>0.26</td>
<td>0.28</td>
<td>0.24</td>
<td>0.44</td>
<td>0.07</td>
</tr>
</tbody>
</table>

The mathematica code to generate the fractal is:

```mathematica
Needs["ProgrammingInMathematica'IFS'"]
Needs["ProgrammingInMathematica'ChaosGame'"]
f1 = AffineMap[{{0, 0, 0}, {0, 0.16, 0}}];
f2 = AffineMap[{{0.85, 0.04, 0}, {-0.04, 0.85, 1.6}}];
f3 = AffineMap[{{0.2, 0.23, 0}, {0.26, 0.22, 1.6}}];
f4 = AffineMap[{{-0.15, 0.28, 0}, {0.26, 0.24, 0.44}}];
fern = IFS[{f1, f2, f3, f4}];
ChaosGame[fern, 50000, Coloring -> Automatic]
```

5.18 Exercises

Exercise 5.18.1. Define \( d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R} \) by \( d(x, y) = |x - y| \) for all \( x, y \in \mathbb{Q} \). Show that the metric space \( (\mathbb{Q}, d) \) is not complete.

Exercise 5.18.2. Let \( \mathcal{D}([-1, 1], \mathbb{R}) \) be the set of differentiable functions from \([-1, 1]\) to \( \mathbb{R} \).

(a) For each \( n \in \mathbb{N} \), define the following function \( f_n : [-1, 1] \to \mathbb{R} \):

\[
f_n(x) = \sqrt{x^2 + 1/n^2}.
\]

Draw \( f_1, f_2 \) and \( f_3 \).
(b) Is \( f_n \) differentiable for every \( n \)?

(c) Which function \( f \) do you think the sequence \( \{ f_n \} \) converges to in \( \mathcal{B}([-1,1], \| \cdot \|_{\infty}) \)? **Give a proof.** (Hint: You may use the fact that the maximum of \( f_n(x) - f(x) \) is attained at \( x = 0 \).)

**Proof.** Let \( \epsilon > 0 \). We want to find \( N \in \mathbb{N} \) such that if \( n > N \), then
\[
\| f_n - f \|_{\infty} < \epsilon.
\]

\[\ldots\]

\[\square\]

(d) So what can you say about \( D([-1,1], \mathbb{R}) \)?

**Exercise 5.18.3.** For each \( i \in \mathbb{N} \), let \( m_i \) be the set of Cauchy sequences on \( \mathbb{Q}, d_E \) whose \( i \)-th element is zero. Show that \( m_i \) is an ideal of the ring of all Cauchy sequences on \( \mathbb{Q}, d_E \).

**Exercise 5.18.4.** Let \( \{ x_n \} \) be a Cauchy sequence of rationals, and suppose it is not equivalent to the zero-sequence. Show that the real number \( [x_n] \) has a multiplicative inverse.

**Exercise 5.18.5.** Here we show that metric spaces are Hausdorff; a set of spaces in topology which are key to generalising calculus to nice shapes and geometries. Let \( [X, d] \) be a metric space and suppose \( x, y \in X \) with \( x \neq y \). Find two disjoint open balls \( B_{\epsilon_x}(x) \) and \( B_{\epsilon_y}(y) \).

**Hausdorff Property for \([X, d]\):** For every pair of distinct points \( x, y \in X \), there exist disjoint open sets \( U_x \) and \( U_y \) containing \( x \) and \( y \) respectively.

**Exercise 5.18.6.** Show that the the subset \( \{ x \in \mathbb{Q} : x^2 > 2 \} \) of \( \mathbb{Q}, d_E \) is clopen.

**Exercise 5.18.7.** Prove that all functions from a discrete metric space to any given topological space are continuous.

**Exercise 5.18.8.** Let \([X, d] \) and \([Y, e] \) be metric spaces and suppose \( f : X \rightarrow Y \) is continuous. Prove that if \( C \subseteq Y \) is closed, then \( f^{-1}(C) \) is closed in \( X \).

**Exercise 5.18.9.** Show that the sequence of functions defined in Example 5.15.1 is not a Cauchy sequence.

**Exercise 5.18.10.** Let \( \mu \in \mathbb{R}^+ \) and let \( T : \mathbb{R} \rightarrow \mathbb{R} \) be the function defined by \( T(x) := 4\mu x(1 - x) \). This is the famous logistic map from the theory of dynamical systems. For what values of \( \mu \) is \( T \) a contraction map? (The metric on \( \mathbb{R} \) is the usual Euclidean one).

**Exercise 5.18.11.** Consider the differential equation over \( \mathbb{R} \)
\[
f'(x) = f(x)
\]
where \( f(0) = C \). Use Banach’s Contraction Mapping Theorem 5.16.6 to show that this differential equation has a unique solution.
6
Compactness

In this chapter we explore the generalisation of finite sets to compact spaces, which turn out to be the right kind of definition for nice functions to behave as they ought to. Continuous functions are bounded and have maxima and minima, and closed sets really look like closed sets as we intuitively think of them.

6.1 From finiteness to compactness

Calculus and analysis on a finite set $X$ is very straight-forward:

The finite world

<table>
<thead>
<tr>
<th>The finite world</th>
</tr>
</thead>
<tbody>
<tr>
<td>All functions $f : X \rightarrow \mathbb{R}$ are bounded.</td>
</tr>
<tr>
<td>All functions $f : X \rightarrow \mathbb{R}$ attain a maximum.</td>
</tr>
<tr>
<td>All sequences of elements of $X$ have constant subsequences.</td>
</tr>
<tr>
<td>All covers have finite subcovers.</td>
</tr>
</tbody>
</table>

The latter property does not make much sense for the moment, so we will explore a particular example. My topology teacher at La Trobe University, John Banks, described a compact set as something where you can measure temperature. That is, there is a continuous function to the reals whose image is bounded and attains a maximum. For example, the sphere is such a set; on the planet earth we can measure the temperature sensibly at each point of its surface. There is a maximum temperature, and it is a continuous function.

Example 6.1.1 (Aside: Motivating the definition of compact). Suppose we have a metric space $[X, d]$. Let $K \subseteq X$ and we will see what happens to $K$ if we stipulate certain conditions on its image under an arbitrary continuous function $f$. We would like the first property to hold above, so we will suppose $f(K)$ is bounded, that is, there is a constant $C_f$ such that $|f(k)| < C_f$ for all $k \in K$. Alternatively, we can think of boundedness in a finer sense. Instead of bounding $f(K)$ with one large open ball, we can cover $f(K)$ with a collection of open balls. Let’s see why this would give us a bounded set. Suppose we have a collection $\{U_i : i \in I\}$ of bounded open sets that cover up $f(K)$, where $I \subseteq \mathbb{N}$. So $f(K) \subseteq \bigcup_{i \in I} U_i$. 

“We have already pointed out and will recognize throughout this book the importance of compact sets. All those concerned with general analysis have seen that it is impossible to do without them”

– Maurice Fréchet
Then the preimages \( \{ f^{-1}(U_i) : i \in I \} \) form a covering of \( K \) by open sets, since \( f \) is continuous. Moreover, each \( f(f^{-1}(U_i)) \) is bounded since \( f(f^{-1}(U_i)) \subseteq U_i \).

Now suppose we can reduce this cover of \( K \) to just a finite collection of bounded open sets. That is, we have a finite subset \( J \) of \( I \) such that \( K \) is contained in the union of \( \{ f^{-1}(U_j) : j \in J \} \). Then after a small calculation, we would have

\[
f(K) \subseteq \bigcup_{j \in J} U_j.
\]

Now a union of finitely many bounded sets is a bounded set, and so \( \bigcup_{j \in J} U_j \) is bounded. So what we have done is shown that if we can reduce any cover of \( K \) by open sets to a finite one, then it ensures that \( f(K) \) is bounded. This is the first thing we need in order for a maximum and minimum of \( f(K) \) to exist. We also would like \( f(K) \) to closed, and this will also be guaranteed.

6.2 Covers and the definition of compact sets

**Definition 6.2.1 (Cover).** Let \( K \) be a subset of \( X \), \( I \subseteq \mathbb{N} \), and suppose \( \{ U_i : i \in I \} \) is a set of subsets of \( X \) such that \( K \subseteq \bigcup_{i \in I} U_i \).

We say that \( \{ U_i : i \in I \} \) is a cover for \( K \).

If \( [X, d] \) is a metric space and \( K \subseteq X \), then an open cover of \( K \) is a cover consisting only of open subsets of \( X \). Similarly, a cover \( \{ U_i : i \in I \} \) is finite if \( I \) is finite. A subcover of a cover \( \{ U_i : i \in I \} \) for \( K \) is another cover \( \{ U_i : i \in J \} \) for \( K \) where \( J \subseteq I \).

**Example 6.2.2.** Let \( K \) the set of positive reals \( \mathbb{R}^+ \), and let \( U_i \) be the open interval \((0, i), \) for each \( i \in \mathbb{N} \). Then \( \{ U_i : i \in \mathbb{N} \} \) is an open cover for \( K \).

However, no matter what you do, you cannot find a finite subset of these open intervals which will cover all of \( K \).

Mathematicians liken compactness to “almost finiteness”. In generalising the finite world to the infinite world, one way is to see whether the property preserved will work in the compact world.

**Definition 6.2.3 (Compact).** A subset \( K \) of a metric space \( [X, d] \) is compact if every open cover of \( K \) contains a finite subcover.

So the example above shows that \( \mathbb{R}^+ \) is not compact: there exists an open cover which does not have a finite subcover. We will see later that the closed intervals of \( \mathbb{R} \) are compact, and that many of the nice bounded sets that naturally occur in nature are examples of compact sets. Notice that it depends on what an open set is, and so what the metric is. We will also

The notion of compactness arose out of the notion of a uniformly continuous function. It was shown by Heine that a continuous map on a closed and bounded subset of a metric space is uniformly continuous. Let \( [X, d] \) and \( [Y, e] \) be two metric spaces, and let \( f : X \rightarrow Y \) be a function. We say that \( f \) is uniformly continuous if \( \forall \epsilon \in \mathbb{R}^+ \) \( \exists \delta \in \mathbb{R}^+ \) \( \forall x, x' \in X \)

\[
d(x, x') < \delta \implies e(f(x), f(x')) < \epsilon.
\]

Notice that uniform continuity is a global property of functions, whereas continuity at a point is a local property.
see some strange compact sets from considering counter-intuitive metric spaces.

We should also comment now on our motivating example above; the converse turns out to also be true. By Exercise 6.5.5, if every continuous function \( f : K \to \mathbb{R} \) is bounded, then \( K \) is compact.

The compact world

<table>
<thead>
<tr>
<th>The compact world</th>
</tr>
</thead>
<tbody>
<tr>
<td>All continuous functions ( f : X \to \mathbb{R} ) are bounded.</td>
</tr>
<tr>
<td>All continuous functions ( f : X \to \mathbb{R} ) attain a maximum.</td>
</tr>
<tr>
<td>All sequences of elements of ( X ) have convergent subsequences.</td>
</tr>
<tr>
<td>All open covers have finite subcovers.</td>
</tr>
</tbody>
</table>

**Lemma 6.2.4.** If \([X, d]\) is a metric space and \( K \) is a finite subset of \( X \), then \( K \) is compact.

\( \diamond \) **Proof:** Suppose \( \{U_i : i \in I\} \) is an open cover for \( K \). By definition of union, for each \( k \in K \), there exists \( i_k \in I \) such that \( k \in U_{i_k} \). Since \( K \) is finite, \( \{U_{i_k} : k \in K\} \) is finite and we also have automatically that \( K \subseteq \bigcup_{k \in K} U_{i_k} \). Therefore, we have a finite subcover of \( \{U_i : i \in I\} \), and so \( K \) is compact. \( \Box \)

**Lemma 6.2.5.** The closed interval \([0, 1]\) is compact.

\( \ast \) **Proof:** To see this, suppose \( \{U_i : i \in I\} \) is an open cover for \([0, 1]\). Now consider the following set \( A \):

\[ A := \{x \in [0, 1] : [0, x) \text{ can be covered by finitely many } U_i's\}. \]

Notice that \( A \) is nonempty since \( 0 \in A \) (as \([0, 0] = \{0\}\) and we can find one element of \( \{U_i : i \in I\} \) containing 0). Moreover, 1 is an upper bound for \( A \), and so by the least upper bound property for \( \mathbb{R} \), we see that a least upper bound \( \alpha \) for \( A \) exists.

Suppose \( \alpha < 1 \). By definition of union, there exists \( j \in I \) such that \( \alpha \in U_j \). Now by definition of an open set, there exists \( \epsilon \in \mathbb{R}^+ \) such that \( B_\epsilon(\alpha) \subseteq U_j \). On the other hand, \( \alpha - \frac{\epsilon}{2} < \alpha \) and so

\[ [0, \alpha - \frac{\epsilon}{2}] \]

is covered by finitely many \( U'_i \)'s, since \( \alpha - \frac{\epsilon}{2} \in A \). Let this set of \( U'_i \)'s be indexed by \( J \subseteq I \) where \( J \) is finite. Therefore

\[ \{U_j\} \cup \{U_i : i \in J\} \]

is a finite cover of \([0, \alpha - \frac{\epsilon}{2}]\); which is a contradiction as \( \alpha + \frac{\epsilon}{2} > \alpha \) and \( \alpha + \frac{\epsilon}{2} \in [0, 1] \).

Therefore, \( \alpha = 1 \) and hence \([0, 1] = A \). It follows then that \([0, 1]\) is compact. \( \Box \)

### 6.3 Closed, bounded and compact

**Theorem 6.3.1.** Every compact subset of a metric spaces \([X, d]\) is closed and bounded.
\* Proof: To be done in lectures. \hfill \Box

We will see later that the converse holds for Euclidean spaces, though there are examples of metric spaces that are non-compact but closed and bounded.

**Example 6.3.2.** Suppose we have a discrete metric space \([X, d]\). Then the collection 
\[
\{B_\frac{1}{2}(x) : x \in X\}
\]
is an open cover of \(X\), and in fact, it is just 
\[
\{\{x\} : x \in X\}.
\]

If \(X\) is infinite, then this open cover has no finite subcover. So \(X\) is not compact, but it is closed and bounded.

---

**Revision on images mixed with preimages.** Each of these statements can be proved easily from the definitions of image and preimage, and we saw some of these properties in the exercises in Chapter 1. Let \(f : A \to B\) be a function. Then

(i) \(U \subseteq f^{-1}(f(U))\) for all \(U \subseteq A\).

(ii) \(U \subseteq V \subseteq A \implies f(U) \subseteq f(V)\).

(iii) \(X \subseteq Y \subseteq B \implies f^{-1}(X) \subseteq f^{-1}(Y)\).

(iv) \(f^{-1}(\bigcup_{i \in I} X_i) = \bigcup_{i \in I} f^{-1}(X_i)\), where \(X_i \subseteq B\) for each \(i \in I\).

(v) \(f(\bigcup_{i \in I} U_i) = \bigcup_{i \in I} f(U_i)\), where \(U_i \subseteq A\) for each \(i \in I\).

We will be using the above properties in the proof of the next result.

**Lemma 6.3.3.** Let \([X, d]\) and \([Y, e]\) be metric spaces and suppose \(f : X \to Y\) is continuous. If \(K \subseteq X\) is compact, then \(f(K)\) is compact in \([Y, e]\).

\* Proof: \label{proof: compactness} Let \(\mathcal{U}\) be an open cover for \(f(K)\). Then 
\[
K \subseteq f^{-1}(f(K)) \subseteq f^{-1}(\bigcup_{U \in \mathcal{U}} U) = \bigcup_{U \in \mathcal{U}} f^{-1}(U).
\]
Since \(f\) is continuous, \(f^{-1}(U) : U \in \mathcal{U}\) is an open cover for \(K\). Since \(K\) is compact, there is a subcover \(\{f^{-1}(U) : U \in \mathcal{V}\}\), where \(\mathcal{V}\) is a finite subset of \(\mathcal{U}\). Now 
\[
f(K) \subseteq f\left(\bigcup_{U \in \mathcal{V}} f^{-1}(U)\right) \subseteq \bigcup_{U \in \mathcal{V}} U
\]
and hence \(\mathcal{V}\) is a finite subcover of \(\mathcal{U}\). Therefore, \(f(K)\) is compact. \hfill \Box

**Theorem 6.3.4** (Heine-Borel-Dirichlet Theorem). A nonempty subset \(K\) of \(\mathbb{R}^n\) is compact if and only if \(K\) is closed and bounded.

\* Proof: Beyond the scope of this course. \hfill \Box
For example, the $n$-sphere is compact as it is a closed and bounded subset of $\mathbb{R}^n$. Also, every closed interval of $\mathbb{R}$ is compact, the torus is compact in $\mathbb{R}^3$, and the Klein bottle is compact in $\mathbb{R}^4$.

For metric spaces, we have the following generalisation of Heine-Borel, whose proof is also beyond the scope of this course. We say that a subset $K$ is totally bounded if it can be covered with finitely many balls of equal radius $r$.

**Theorem 6.3.5** (Generalised Heine-Borel-Dirichlet Theorem). A nonempty subset $K$ of a metric space $[X,d]$ is compact if and only if $K$ is complete and totally bounded.

### 6.4 Aside: Brouwer’s fixed-point theorem

One of the successes of abstracting to the compact world is a truly beautiful theorem due to Brouwer, known universally as Brouwer’s fixed-point theorem. It is perhaps better known as the device upon which Nash’s Equilibrium Theorem in game theory is based, along with its far sweeping consequences in analysis and topology: the Jordan Curve Theorem, The Hairy Ball Theorem and the Borsak-Ulam Theorem.\footnote{Luitzen E. J. Brouwer (1881 – 1966) was one of the best dutch mathematicians of all time, and he’s work transformed the disciplines of topology, measure theory and analysis. He is also famous for his contributions to the philosophy of mathematics, founding the intuitionist movement.}

**Theorem 6.4.1** (Brouwer’s fixed-point theorem). Every continuous function $f$ from a convex compact subset $K$ of a Euclidean space to $K$ itself has a fixed point.

There are many interesting consequences of this theorem where $f$ is thought of as a deformation of a geometric object:

1. No matter how much you stir a jar of honey, some point in the liquid will end up in exactly the same place in the glass as before.

2. Take a map of Perth, and suppose that that map is laid out on a table inside Perth. There will always be a point on the map which represents that same point as its own position in Perth.

3. The game Hex cannot end in a draw.

4. If you want to go to sleep while standing up in a train that travels along a perfectly straight track, there is some starting angle that will cause you not to fall over.

### 6.5 Exercises

**Exercise 6.5.1.** Wherever possible, give a proper subcover of the following covers of $\mathbb{R}$. Justify your answer.

(a) $\{(-n,n) : n \in \mathbb{N}\}$

(b) $\{(x-2,x+2) : x \in \mathbb{Z}\}$

(c) $\{(x-1,x+1) : x \in \mathbb{Z}\}$

**Exercise 6.5.2.** Which of the following subsets of $\mathbb{R}^2$ are compact, under the usual topology?
(a) \{ (x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1 \} \\
(b) \{ (x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1 \} \\
(c) \{ (x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1 \} \\
(d) \{ (x, y) \in \mathbb{R}^2 : x^2 + y^2 \geq 1 \} \\
(e) \{ (x, y) \in \mathbb{R}^2 : x^2 - y^2 \leq 1 \}

Exercise 6.5.3. Let \( A \) have the discrete topology. Which subsets of \( A \) are compact? Give a proof.

Exercise 6.5.4. Below, we look at an example in the metric space on the closed interval \([0, 1]\).

(a) Show that the sets 
\[ U_i := \left[ 0, \frac{1}{\pi} - \frac{1}{i} \right] \cup \left[ \frac{1}{\pi} + \frac{1}{i}, 1 \right], \quad i = 4, 5, \ldots, \]
form an open cover of \( \mathbb{Q} \cap [0, 1] \).

(b) Does \( \{ U_i \} \) have a finite subcover of \( \mathbb{Q} \cap [0, 1] \)?

Exercise 6.5.5. Let \( [X, d] \) be a metric space and let \( K \) be a subset of \( X \). Show that if every continuous function \( f : K \to \mathbb{R} \) is bounded, then \( K \) is compact.
7

The twain shall meet

One of the most important constructs in mathematics are the so-called \( p \)-adic numbers, which find themselves in all sorts of areas of mathematics from algebraic number theory to finite combinatorics. It takes a course such as this to understand what the \( p \)-adic numbers are. They are a combination of algebraic concepts and analytic ones, needing the notion of a completion of a metric space and yields a fundamental example of a ‘local field’ in abstract algebra.

7.1 \( p \)-adic metric and the \( p \)-adic numbers

For \( \frac{x}{y} \in \mathbb{Q} \), suppose we have integers \( a, b, n \) so that
\[
\frac{x}{y} = p^n \frac{a}{b}
\]
so that neither \( a \) nor \( b \) are divisible by \( p \). Then the \( p \)-adic valuation of \( \frac{x}{y} \), written \( |\frac{x}{y}|_p \) is defined to be
\[
|\frac{x}{y}|_p := p^{-n}.
\]
By convention, \( |0|_p = 0 \). Another way to see the \( p \)-adic valuation is to look at integers first. If \( z \in \mathbb{Z} \), then \( |z|_p \) is \( p^{-n} \) where \( n \) is the largest power of \( p \) so that \( p^n \) divides \( z \). Then for a rational number, \( \frac{x}{y} \) we need not worry about reducing its expression and simply define \( |\frac{x}{y}|_p := |x|_p / |y|_p \).

Example 7.1.1.
- \( |5|_5 = \frac{1}{5} \) whereas \( |50|_5 = \frac{1}{25} \).
- \( |1/2|_5 = 1 \) and note that \( |20/40|_5 = |20|_5 / |40|_5 = \frac{1/5}{1/5} = 1 \).

When we defined a norm in Chapter 4, the positive homogeneity condition was respect to the absolute value norm on \( \mathbb{R} \). A more general definition of norm is over a normed field where there is a more general definition of ‘absolute value’. Here, we replace the absolute value with the \( p \)-adic valuation, and we end up with a more general norm on \( \mathbb{Q} \).

Lemma 7.1.2. The \( p \)-adic valuation defines a norm on the rational numbers.

Proof (sketch):
(a) **Non-degeneracy:** By convention, $|0|_p = 0$, and we cannot have $|v|_p = 0$ when $v \neq 0$.

(b) **Pos. homogeneity:** For all $v \in \mathbb{Q}$, we have $|\lambda v|_p = |\lambda|_p \cdot |v|_p$.

(c) **Triangle inequality:** To show that for all $u, v \in \mathbb{Q}$, we have $\left| u + v \right|_p \leq |u|_p + |v|_p$. It suffices to show something stronger: $|p^n(a/b) + p^n'(a'/b')|_p \leq \max\{1/p^n, 1/p^n'\}$.

We then define the $p$-adic metric $d_p$ on $\mathbb{Q}$ by $d_p(u, u') := |u - u'|_p$.

**Example 7.1.3.** Notice that $d_7(8, 1) = 7/7 = 1$ whereas $d_7(100, 1) = 99/7 = 1$. But then $d_7(99, 1) = 1/7$.

**Example 7.1.4.** We will show that the harmonic series

$$1 + p + p^2 + p^3 + \ldots$$

converges in $[\mathbb{Q}, |\cdot|_p]$. Let $x_n$ be the partial sum $\sum_{i=0}^{n} p^i$ for each integer $n \geq 0$. Using the formula of a geometric series we see that $x_n - (-1) = p^{n+1}$.

and so $|x_n - (-1)|_p = p^{-(n+1)}$.

Let $\epsilon > 0$. Choose $N$ to be the next integer larger than $-\log_p(\epsilon) - 1$ and suppose $n > N$. Then $n + 1 > -\log_p(\epsilon)$

and thus $p^{-(n+1)} < \epsilon$. Therefore, $p^{-(n+1)} < \epsilon$ and $|x_n - (-1)|_p < \epsilon$.

Hence, $\{x_n\}$ converges to $-1$!

### 7.2 A bit more than what you know

Recall that we can write an integer in base 2 by listing 0’s and 1’s. So for example, the number 22 can be written in base 2 as $10110_2$ because $20 = 16 + 4 + 2$ and we put zeros for where 8 and 1 appear. In base 3, we write 22 as $211_3$ since $22 = 2 \cdot 3^2 + 1 \cdot 3^1 + 1 \cdot 3^0$. So we have used a finite series to represent integers.

Any positive integer can be written in base $p$ as

$$\sum_{i=0}^{n} a_i p^i$$
where each \( a_i \in \mathbb{Z}_p \). Can we do the same for positive rationals? Let us consider the fraction \( \frac{3}{13} \). We can use negative powers of 3 to give a base 3 expansion of this rational number:

\[
0 \cdot \frac{1}{3} + 2 \cdot \frac{1}{9} + 0 \cdot \frac{1}{81} + 0 \cdot \frac{1}{243} + 2 \cdot \frac{1}{729} + \cdots
\]

which we can write as

\[
0.02002002002 \ldots_3
\]

Notice that the base 3 expansion here does not terminate, but it is periodic.

Now \( [\mathbb{Q}, | \cdot |] \) is not complete, but often the partial sums \( \sum_{i=-n}^{\infty} a_i p^{-i} \) (where \( a_i \in \mathbb{Z}_p \)) converge to a rational number.

**Lemma 7.2.1.** Let \( p \) be a prime number. Any positive rational number can be written in the form

\[
\sum_{i=n}^{\infty} a_i p^{-i}, \quad a_i \in \mathbb{Z}_p
\]

where convergence of the series above is given by the Euclidean metric.

Except for the expressions where \( a_i = p - 1 \) for all \( i \) beyond a certain point, the base \( p \) expansion of a rational number is unique.

Notice that the series expansion of a rational number in terms of powers of \( p \) is valid since we have been careful to prove that the result is something that converges with respect to the absolute value metric. We will see now, that if we use a different metric, something similar but “upside-down” happens. For the so-called \( p \)-adic expansion of a rational number, we use the \( p \)-adic metric, which in some sense inverts the distances given by the absolute value metric. So instead of summing from negative infinity, we need to begin our summation at a determinate value, and continue to positive infinity.

**Lemma 7.2.2.** Let \( p \) be a prime number. Any positive rational number can be written uniquely in the form

\[
\sum_{i=n}^{\infty} a_i p^i
\]

where each \( a_i \in \mathbb{Z}_p \), and convergence of the series above is given by the \( p \)-adic metric.

### 7.3 Completing the rationals

With respect to the \( p \)-adic metric, the rational numbers are not complete, and we will see this by exhibiting a particular example. Consider the following sequence:

\[
p, \quad p + p^2, \quad p + p^2 + p^3, \ldots \quad x_n := \sum_{i=1}^{n} p^i.
\]

Then \( \{x_n\} \) is a Cauchy sequence but it does not converge.

**Proof.** Let \( \epsilon > 0 \). We want to find an \( N \in \mathbb{N} \) such that if \( n > m > N \), then \( d(x_m, x_n) < \epsilon \). Choose \( N \) to be the next largest integer after \( \log_p(1/\epsilon) - 1 \).
It turns out that if \( n > m > N \), then \( \frac{1}{p^{m+1}} < \epsilon \). Now \( \sum_{i=0}^{n-m-1} p^i \) is coprime to \( p \) and so it has \( p \)-adic valuation 1. Therefore,

\[
\frac{1}{p^{m+1}} = \left| \frac{p^{m+1}}{p} \cdot \sum_{i=0}^{n-m-1} p^i \right|_p = \left| \sum_{i=m+1}^{n} p^i \right|_p
\]

\[
= \left| \sum_{i=1}^{n} p^i - \sum_{i=1}^{m} p^i \right|_p = |x_n - x_m|_p.
\]

Hence \( d_p(x_n, x_m) < \epsilon \) and \( \{x_n\} \) is a Cauchy sequence.

However, this sequence does not converge in \( [\mathbb{Q}, d_p] \). For a proof by contradiction, suppose \( \{x_n\} \) converges to \( q \), and write \( q = \frac{a}{b} \) where \( a, b \) are coprime to \( p \) (we won’t need to consider the case that \( q = 0 \), because it is clear that the sequence does not converge to \( 0 \)). Let \( \epsilon = \frac{1}{p^t} \). Then there exists \( N \in \mathbb{N} \) such that for all \( n > N \), we have \( |x_n - q|_p < \frac{1}{p^t} \). If \( t > 1 \), then \( p^2 \) divides \( x_nb - p^t a \), which is a contradiction as \( x_n \) is divisible by \( p \), and the difference between \( \frac{1}{p} x_nb \) and \( p^{t-1} a \) is coprime to \( p \). Similarly, if \( t < 0 \), then \( p^2 \) divides \( x_nb p^{t-1} - a \). So consider the remaining case \( t = 1 \). Then

\[
|x_n - q|_p = |x_nb - p^t a|_p = \frac{1}{p} \left| (1 + p + \ldots + p^{n-1})b - a \right|_p
\]

\( \square \)

Now we come to the culmination of this set of notes; the definition of the \( p \)-adic numbers.

**Definition 7.3.1** (\( p \)-adic numbers). The equivalence classes of Cauchy sequences in \( [\mathbb{Q}, d_p] \) is the set of \( p \)-adic numbers and we denote it by \( \mathbb{Q}_p \). The closed ball of radius 1 about 0 is the set of \( p \)-adic integers, which we denote by \( \mathbb{Z}_p \).

We can add and multiply \( p \)-adic numbers just as we did when we constructed the real numbers as Cauchy sequences of rationals.

**Lemma 7.3.2.** The \( p \)-adic numbers form a ring, and the \( p \)-adic integers are a subring of \( \mathbb{Q}_p \).

**Theorem 7.3.3.** The set of \( p \)-adic numbers are uncountable.
In this course you will see proofs of statements which have layers of difficulty. Most of the proofs you’ve seen so far have been of statements such as the sum of two odd numbers is an even number or for every $x \geq 4$, we have $2^x \geq x^2$. Now you will statements such as

$$\text{for every } b \in B, \text{ there exists an element } a \in A, \text{ such that } f(a) = b.$$  

You might recognise the above as being the definition of an onto function. A similar type of statement was encountered in first year when we saw the definition of limit. If you break down the statement into its fundamental pieces, that is, into its quantifiers and clauses, you will see how to do the proof.

**Proving “$(\forall b \in B)(\exists a \in A) \text{ Property}(a, b)$”:**

This type of proof is used to prove that a function is onto or that a function is continuous at a point.

**Proof.** Suppose $b \in B$. We want to find an element $a \in A$ such that $\text{Property}(a, b)$.

Do some work somewhere else to figure out what $a$ should be.

Choose $a \in A$. Then ...

\[ \vdots \]

Therefore, $\text{Property}(a, b)$. \hfill \Box

**Converting “$P \implies Q$” to a “for all” statement**

A handy thing to remember when proving statements like $P \implies Q$ is that logically, this is equivalent to proving

$$\text{for all instances when } P \text{ holds, we also have } Q.$$
Proving "\((\forall x, y \in A)\ P(x, y) \implies Q(x, y)\)":

Here we have statements \(P(x, y)\) and \(Q(x, y)\) depending on \(x\) and \(y\). The definition of a one-to-one function is an example of a statement with this shape, and we can convert it to the following:

\[\left(\forall x, y \in A; \text{ satisfying } P(x, y)\right) Q(x, y)\]

So this is how we write the proof.

\[
\text{Proof. Suppose } x, y \in A \text{ and suppose } P(x, y) \text{ holds. Then ...} \\
\quad \vdots \\
\text{Therefore } Q(x, y) \text{ holds. } \square
\]

Set equality

Two sets \(A\) and \(B\) are equal if they have the same elements. That is,

\[A = B \iff A \subseteq B \text{ and } B \subseteq A.\]

Proving containment

To prove \(A \subseteq B\), we show that

\[\text{if } a \in A, \text{ then } a \in B.\]

Example: Let \(A\) be the set of positive integers which are divisible by 4, and let \(B\) be the set of integers which are greater than or equal to \(-10\). We will show that \(A \subseteq B\).

\[
\text{Proof. Let } a \in A. \text{ Then } 4 \text{ divides } a \text{ and hence } 4 \leq a. \text{ So } -10 \leq a \text{ and hence } a \in B. \text{ Therefore } A \subseteq B. \quad \square
\]

Some set constructions

The union of two subsets \(A\) and \(B\) of a set \(X\), is the set

\[A \cup B = \{x \in X : x \in A \text{ or } x \in B\}.\]

The intersection of two subsets \(A\) and \(B\) of a set \(X\), is the set

\[A \cap B = \{x \in X : x \in A \text{ and } x \in B\}.\]

The complement of a subset \(A\) of a set \(X\), is the set

\[X \setminus A = \{x \in X : x \notin A\}.\]

The power set of a set \(X\), is the set of all subsets of \(X\), and we denote it \(\mathcal{P}(X)\). The Cartesian product of two sets \(A\) and \(B\), is the set of all ordered pairs \((a, b)\) of elements \(a \in A\) and \(b \in B\), and we write this set as

\[A \times B = \{(a, b) : a \in A \text{ and } b \in B\}.\]
De Morgan’s Laws for sets:

Let $A$ and $B$ be subsets of a set $X$. Then

- $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$,
- $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B)$,
- $A \subseteq B \iff X \setminus B \subseteq X \setminus A$. 
addition modulo \(n\), 42
algebraic integer, 72
algebraic number, 71
arithmetic progression, 37
associative, 19
Bézout’s identity, 32
Bézout’s identity for polynomials, 65
ball
of a metric space, 98
of a normed vector space, 85
Banach space, 103
bounded
function, 91
set, 91
canonical factorisation, 36
cardinality, 18
cartesian product, 12
Cauchy sequence, 100
addition of, 103
equivalence, 104
null, 104
unit, 104
zero, 104
Cauchy sequence multiplication of, 103
cells, 56
characteristic function, 23
closed set, 108
closed under an operation, 30
codomain, 15
commutative, 19
compact, 116
complete metric space, 103
composition, 18
congruence
modulo \(n\), 41
modulo a polynomial, 67
congruence class, 43
congruence classes, 58
continuous maps
between normed vector spaces, 87
contraction map, 111
coprime, 34
countable, 20
cover, 116
Dedekind cuts, 106
degree of a polynomial, 62
divides relation
for integers, 29
for polynomials, 63
domain, 15
equinumerous, 18
equivalence classes, 57
Euclidean Algorithm, 32
for polynomials, 64
even number, 14
field, 54
field of fractions, 60
fixed point, 111
function, 12, 15
bijection, 17
invertible, 19
one-to-one, 15
onto, 16
Gauss’s Lemma, 66
greatest common divisor, 31
for polynomials, 64
ideal
principal, 71
image, 15, 19
infix notation, 12
integers modulo \(n\), 42
kidney diagram, 15
least common multiple, 34
least upper bound, 84
least upper bound, 84
lemma: Euclid’s Lemma for polynomials, 65
limit of a sequence
in a metric space, 98
linear diophantine equation, 43
linear operator, 90
Mersenne prime, 38
metric, 97
\(p\)-adic, 122
discrete metric, 98
induced on a subset, 99
Post-Office metric, 98
metric space, 97
minimal polynomial, 72
multiplication modulo \(n\), 42
naïve set theory, 13
norm, 83
Euclidean, 83
sup norm, 91
odd number, 14
open set, 107
partition, 56
parts, 56
polynomial, 61
content of, 66
irreducible, 65
monic, 64
polynomial ring, 62
power set, 23
preimage, 19
proofs
restricted syntax, 14
quotient, 59
ring, 53
Russell’s paradox, 13
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>sequence</td>
<td>95</td>
</tr>
<tr>
<td>subfield</td>
<td>81</td>
</tr>
<tr>
<td>sum-of-divisors function</td>
<td>39</td>
</tr>
<tr>
<td>theorem</td>
<td></td>
</tr>
<tr>
<td>Banach’s Contraction Mapping Theorem</td>
<td>111</td>
</tr>
<tr>
<td>Bertrand’s Postulate</td>
<td>36</td>
</tr>
<tr>
<td>Brouwer’s fixed-point theorem</td>
<td>119</td>
</tr>
<tr>
<td>Chinese Remainder Theorem</td>
<td>44</td>
</tr>
<tr>
<td>Content Theorem</td>
<td>66</td>
</tr>
<tr>
<td>Dirichlet’s Theorem</td>
<td>38</td>
</tr>
<tr>
<td>Division Rule</td>
<td>31</td>
</tr>
<tr>
<td>Division Rule for polynomials</td>
<td>63</td>
</tr>
<tr>
<td>Eisenstein’s Irreducibility Criterion</td>
<td>67</td>
</tr>
<tr>
<td>Equivalence Relation Theorem</td>
<td>58</td>
</tr>
<tr>
<td>Euclid</td>
<td>39</td>
</tr>
<tr>
<td>Euler</td>
<td>40</td>
</tr>
<tr>
<td>Factor Theorem</td>
<td>65</td>
</tr>
<tr>
<td>Fermat’s Little Theorem</td>
<td>45</td>
</tr>
<tr>
<td>Fundamental Theorem of Arithmetic</td>
<td>35</td>
</tr>
<tr>
<td>Generalised Heine-Borel-Dirichlet</td>
<td>119</td>
</tr>
<tr>
<td>Green-Tao Theorem</td>
<td>38</td>
</tr>
<tr>
<td>Heine-Borel-Dirichlet</td>
<td>118</td>
</tr>
<tr>
<td>infinitude of primes</td>
<td>35</td>
</tr>
<tr>
<td>LDE Theorem</td>
<td>43</td>
</tr>
<tr>
<td>Prime Number Theorem</td>
<td>37</td>
</tr>
<tr>
<td>theorem:Fundamental Theorem of Polynomial Arithmetic</td>
<td>65</td>
</tr>
<tr>
<td>theorem:Least Upper Bound Property</td>
<td>85</td>
</tr>
<tr>
<td>totally bounded</td>
<td>119</td>
</tr>
<tr>
<td>unit interval</td>
<td>61</td>
</tr>
<tr>
<td>units</td>
<td>55</td>
</tr>
<tr>
<td>upper bound</td>
<td>84</td>
</tr>
<tr>
<td>vector space</td>
<td>80</td>
</tr>
<tr>
<td>well-ordering principle</td>
<td>26</td>
</tr>
</tbody>
</table>