Numbers, Sequences and Series

Lecture Notes

Dr. Silvio Fanzon

8 Nov 2023

Academic Year 2023/24

Department of Mathematics

University of Hull

Table of contents

Welcome

These are the Lecture Notes of **Numbers, Sequences and Series 400297** for T1 2023/24 at the University of Hull. I will follow these lecture notes during the course. If you have any question or find any typo, please email me at

S.Fanzon@hull.ac.uk

Up to date information about the course, Tutorials and Homework will be published on the University of Hull **Canvas Website**

canvas.hull.ac.uk/courses/67551

and on the **Course Webpage** hosted on my website

silviofanzon.com/blog/2023/NSS

Digital Notes

Digital version of these notes available at

silviofanzon.com/2023-NSS-Notes

Readings

We will study the set of real numbers $\mathbb{R}$, and then sequences and series in $\mathbb{R}$. I will follow mainly the textbook by Bartle and Sherbert [2]. Another good reading is the book by Abbott [1]. I also point out the classic book by Rudin [3], although this is more difficult to understand.

> **!** You are not expected to purchase any of the above books. These lecture notes will cover 100% of the topics you are expected to known in order to excel in the final exam.

1 Introduction

The first aim of this lecture notes is to rigorously introduce the set of **real numbers**, which is denoted by $\mathbb{R}$. But what do we mean by real numbers? To start our discussion, introduce the set of natural numbers (or non-negative integers)

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \dots\}$$

On this set we have a notion of **sum** of two numbers, denoted as usual by

$$n + m$$

for $n, m \in \mathbb{N}$. Here the symbol $\in$ denotes that m and n belong to $\mathbb{N}$. For example $3 + 7$ results in 10.

Question 1.1

Can the sum be inverted? That is, given any $n, m \in \mathbb{N}$, can you always find $x \in \mathbb{N}$ such that

$$n + x = m\,? \tag{1.1}$$

Of course to invert (1.1) we can just perform a **subtraction**, implying that

$$x = m - n\,.$$

But there is a catch. In general x does not need to be in $\mathbb{N}$. For example, take $n = 10$ and $m = 1$. Then $x = -9$, which does not belong to $\mathbb{N}$. Therefore the answer to Question 1.1 is **NO**.

To make sure that we can always invert the sum, we need to **extend** the set $\mathbb{N}$. This is done simply by introducing the set of **integers**

$$\mathbb{Z} := \{-n, n \,:\, n \in \mathbb{N}\}\,,$$

that is, the set

$$\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}\,.$$

The sum can be extended to $\mathbb{Z}$, by defining

$$(-n) + (-m) := -(m + n) \tag{1.2}$$

for all $m, n \in \mathbb{N}$. Now every element of $\mathbb{Z}$ possesses an **inverse**, that is, for each $n \in \mathbb{Z}$, there exists $m \in \mathbb{Z}$, such that

$$n + m = 0\,.$$

Can we characterize m explicitly? Of course! Seeing the definition at (1.2), we simply have

$$m = -n\,.$$

On the set $\mathbb{Z}$ we can also define the operation of **multiplication**, in the usual way we learnt in school. For $n, m \in \mathbb{Z}$, we denote the multiplication by nm or $n \cdot m$. For example $7 \cdot 2 = 14$ and $1 \cdot (-1) = -1$.

Question 1.2

Can the multiplication in $\mathbb{Z}$ be inverted? That is, given any $n, m \in \mathbb{Z}$, can you always find $x \in \mathbb{Z}$ such that

$$nx = m\,? \tag{1.3}$$

To invert (1.3) if $n \neq 0$, we can just perform a **division**, to obtain

$$x = \frac{m}{n}\,.$$

But again there is a catch. Indeed taking $n = 2$ and $m = 1$ yields $x = 1/2$, which does not belong to $\mathbb{Z}$. The answer to Question 1.2 is therefore **NO**.

Thus, in order to invert the multiplication, we need to **extend** the set of integers $\mathbb{Z}$. This extension is called the set of **rational numbers**, defined by

$$\mathbb{Q} := \left\{ \frac{m}{n} \;:\; m, n \in \mathbb{Z},\ n \neq 0 \right\}.$$

We then extend the operations of sum and multiplication to $\mathbb{Q}$ by defining

$$\frac{m}{n} + \frac{p}{q} := \frac{mq + np}{nq}$$

and

$$\frac{m}{n} \cdot \frac{p}{q} := \frac{mp}{nq}$$

Now the multiplication is invertible in $\mathbb{Q}$. Specifically, each non-zero element has an inverse: the inverse of m/n is given by n/m.

To summarize, we have extended $\mathbb{N}$ to $\mathbb{Z}$, and $\mathbb{Z}$ to $\mathbb{Q}$. By construction we have

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}\,.$$

Moreover **sum** and **product** are **invertible** in $\mathbb{Q}$. Now we are happy right? So and so.

Question 1.3

Can we draw the set $\mathbb{Q}$?

It is clear how to draw $\mathbb{Z}$, as seen below.

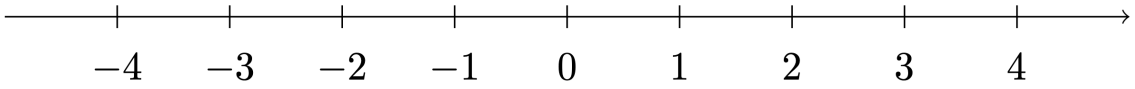

Figure 1.1: Representation of integers $\mathbb{Z}$

However $\mathbb{Q}$ is much **larger** than the set $\mathbb{Z}$ represented by the ticks in Figure 1.1. What do we mean by **larger**? For example, consider $0 \in \mathbb{Q}$.

Question 1.4

What is the number $x \in \mathbb{Q}$ which is closest to 0?

There is no right answer to the above question, since whichever rational number m/n you consider, you can always squeeze the rational number $m/(2n)$ in between:

$$0 < \frac{m}{2n} < \frac{m}{n}\,.$$

For example think about the case of the numbers

$$\frac{1}{n} \text{ for } n \in \mathbb{N},\, n \neq 0\,.$$

Such numbers get arbitrarily close to 0, as depicted below.

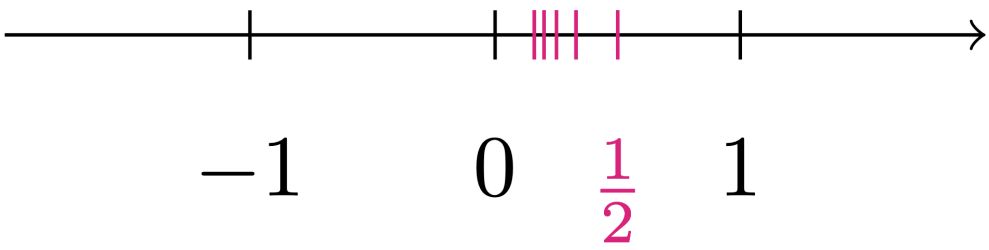

Figure 1.2: Fractions $\frac{1}{n}$ can get arbitrarily close to 0

Maybe if we do the same reasoning with other progressively smaller rational numbers, we manage to fill out the interval $[0, 1]$. In other words, we might conjecture the following.

Conjecture 1.5

Maybe $\mathbb{Q}$ can be represented by a continuous line.

Do you think the above conjecture is true? If it was, mathematics would be quite boring. Indeed Conjecture 1.5 is **false**, as shown by the Theorem below.

Theorem 1.6

The number $\sqrt{2}$ does not belong to $\mathbb{Q}$.

Theorem 1.6 is the reason why $\sqrt{2}$ is called an **irrational number**. For reference, a few digits of $\sqrt{2}$ are given by

$$\sqrt{2} = 1.414213562373095048\ldots$$

and the situation is as in the picture below.

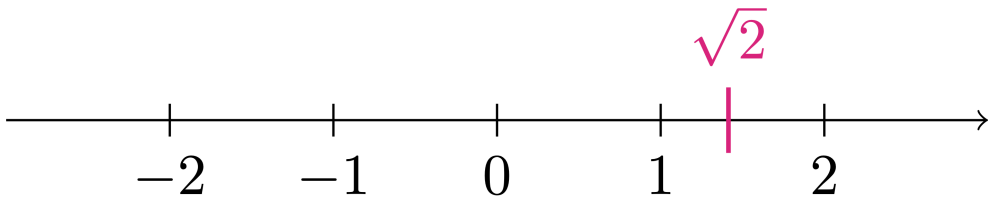

Figure 1.3: Representing $\sqrt{2}$ on the numbers line.

We can therefore see that Conjecture 1.5 is **false**, and $\mathbb{Q}$ is not a line: indeed $\mathbb{Q}$ has a **gap** at $\sqrt{2}$. Let us see why Theorem 1.6 is true.

Proof: Proof of Theorem 1.6

We prove that

$$\sqrt{2} \notin \mathbb{Q}$$

by **contradiction**.
Wait, what does this mean? Proving the claim by contradiction means assuming that the claim is **false**. This means we **assume** that

$$\sqrt{2} \in \mathbb{Q}\,. \tag{1.4}$$

From this assumption we then start deducing other statements, hoping to encounter a statement which is **FALSE**. But if (1.4) leads to a false statement, then it must be that (1.4) is **FALSE**. Thus the contrary of (1.4) must hold, meaning that

$$\sqrt{2} \notin \mathbb{Q}$$

as we wanted to show. This would conclude the proof.
Now we need to actually show that (1.4) will lead to a contradiction. Since this is our first proof, let us take it slowly, step-by-step.

1. Assuming (1.4) just means that there exists $q \in \mathbb{Q}$ such that
$$q = \sqrt{2}\,. \tag{1.5}$$

2. Since $q \in \mathbb{Q}$, by definition we have
$$q = \frac{m}{n}$$
for some $m, n \in \mathbb{N}$ with $n \neq 0$.

3. Recalling (1.5), we then have
$$\frac{m}{n} = \sqrt{2}\,.$$

4. We can square the above equation to get
$$\frac{m^2}{n^2} = 2\,. \tag{1.6}$$

5. **Withouth loss of generality**, we can **assume** that m and n have no common factors.

   Wait. What does Step 5 mean? You will encounter the sentence *withouth loss of generality* many times in mathematics. It is often abbreviated in **WLOG**. WLOG means that the assumption that follows is chosen arbitrarily, but does not affect the validity of the proof in general.
   For example in our case we can assume that m and n have no common factor. This is because if m and n had common factors, then it would mean
   $$m = a\tilde{m}\,, \quad n = a\tilde{n}$$
   for some $a \in \mathbb{N}$ with $a \neq 0$. Then
   $$\frac{m}{n} = \frac{a\tilde{m}}{a\tilde{n}} = \frac{\tilde{m}}{\tilde{n}}\,.$$
   Therefore by (1.6)
   $$\frac{\tilde{m}^2}{\tilde{n}^2} = 2\,.$$
   The proof can now proceed in the same way we would have proceeded from Step 4, but in addition we have the hypothesis that $\tilde{m}$ and $\tilde{n}$ have no common factors.

6. Equation (1.6) implies
$$m^2 = 2n^2\,. \tag{1.7}$$
Therefore the integer m^2 is an even number.

Why is m^2 even? As you already know, **even** numbers are

$$0, 2, 4, 6, 8, 10, 12, \ldots$$

All these numbers have in common that they can be divided by 2, and so they can be written as

$$2p$$

for some $p \in \mathbb{N}$. For example 52 is even, because

$$52 = 2 \cdot 26 .$$

Instead, **odd** numbers are

$$1, 3, 5, 7, 8, 9, 11, \ldots$$

These can be all written as

$$2p + 1$$

for some $p \in \mathbb{N}$. For example 53 is odd, because

$$52 = 2 \cdot 26 + 1 .$$

7. Thus m is an even number, and so there exists $p \in \mathbb{N}$ such that

$$m = 2p . \tag{1.8}$$

Why is (1.8) true? Let us see what happens if we take the square of an even number $m = 2p$

$$m^2 = (2p)^2 = 4p^2 = 2(2p^2) = 2q .$$

Thus $m^2 = 2q$ for some $q \in \mathbb{N}$, and so m^2 is an even number. If instead m is odd, then $m = 2p + 1$ and

$$m^2 = (2p + 1)^2 = 4p^2 + 4p + 1 = 2(2p^2 + 2p) + 1$$

showing that also m^2 is odd.
This justifies Step 7: Indeed we know that m^2 is an even number from Step 6. If m was odd, then m^2 would be odd. Hence m must be even as well.

8. If we substitute (1.8) in (1.7) we get

$$m^2 = 2n^2 \implies (2p)^2 = 2n^2 \implies 4p^2 = 2n^2$$

Dividing both terms by 2, we obtain

$$n^2 = 2p^2 . \tag{1.9}$$

9. We now make a series of observations:

- Equation (1.9) says that n^2 is even.
- Step 6 says that m^2 is even.
- Therefore n and m are also even.

- Hence n and m have 2 as common factor.
- But Step 5 says that n and m have no common factors.
- `CONTRADICTION`

10. Our reasoning has run into a **contradiction**, starting from assumption (1.4), which says that

$$\sqrt{2} \in \mathbb{Q}\,.$$

Hence the above must be **FALSE**, and so

$$\sqrt{2} \notin \mathbb{Q}$$

ending the proof.

Seeing that $\sqrt{2} \notin \mathbb{Q}$, we might be tempted to just fill in the gap by adding $\sqrt{2}$ to $\mathbb{Q}$. However, with analogous proof to Theorem 1.6, we can prove that

$$\sqrt{p} \notin \mathbb{Q}$$

for each prime number p. As there are infinite prime numbers, this means that $\mathbb{Q}$ has infinite gaps. Then we might attempt to fill in these gaps via the extension

$$\tilde{\mathbb{Q}} := \mathbb{Q} \cup \{\sqrt{p} : \ p \text{ prime}\}\,.$$

However even this is not enough, as we would still have numbers which are not contained in $\tilde{Q}$, for example

$$\sqrt{2}+\sqrt{3},\ \pi,\ \pi+\sqrt{2} \notin \tilde{\mathbb{Q}}\,.$$

Remark 1.7

Proving that

$$\sqrt{2}+\sqrt{3} \notin \mathbb{Q}$$

is relatively easy, and will be left as an **exercise**. Instead, proving that

$$\pi \notin \mathbb{Q}$$

is way more complicated. There are several proof of the fact, all requiring mathematics which is more advanced of the one presented in this course. For some proofs, see this Wikipedia page.

The reality of things is that to **complete** $\mathbb{Q}$ and make it into a **continuous line** we have to add a lot of points. Indeed, we need to add way more points than the ones already contained in $\mathbb{Q}$. Such extension of $\mathbb{Q}$ will be called $\mathbb{R}$, the set of **real numbers**. The inclusions will therefore be

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}\,.$$

The set $\mathbb{R}$ is not at all trivial to construct. In fact, at first we will not construct it, but just do the following:

- We will assume that $\mathbb{R}$ **exists** and satisfies some basic **axioms**.
- One of the axioms is that $\mathbb{R}$ fills **all** the **gaps** that $\mathbb{Q}$ has. Therefore $\mathbb{R}$ can be thought as a **continuous** line.
- We will study the **properties** of $\mathbb{R}$ which descend from such **axioms**.

For example one of the properties of $\mathbb{R}$ will be the following:

Theorem 1.8: We will prove this in the future

$\mathbb{R}$ contains all the square roots. This means that for every $x \in \mathbb{R}$ with $x \geq 0$, we have

$$\sqrt{x} \in \mathbb{R}\,.$$

At the end of this chapter we will provide a concrete **model** for the real numbers $\mathbb{R}$, to prove once and for all that such set indeed exists.

Theorem 1.9: We will prove this in the future

There exists a set $\mathbb{R}$, called the set of real numbers, which has the following properties:

- $\mathbb{R}$ extends $\mathbb{Q}$, that is,
$$\mathbb{Q} \subset \mathbb{R}\,.$$
- $\mathbb{R}$ satisfies certain **axioms**.
- $\mathbb{R}$ fills **all** the **gaps** that $\mathbb{Q}$ has. In particular $\mathbb{R}$ can be represented by a **continuous** line.

2 Preliminaries

Before introducing $\mathbb{R}$ we want to make sure that we cover all the basics needed for the task.

2.1 Sets

A sets is a **collection** of objects. These objects are called **elements** of the set. For example in the previous section we mentioned the following sets:

- $\mathbb{N}$ the set of natural numbers
- $\mathbb{Z}$ the set of integers
- $\mathbb{Q}$ the set of rational numbers
- $\mathbb{R}$ the set of real numbers

Given an arbitrary set A, we write

$$x \in A$$

if the element x belongs to the set A. If an element x is not contained in A, we say that

$$x \notin A\,.$$

Remark 2.1

A set can contain all sorts of elements. For example the students in a classroom can be modelled by a set S. The elements of the set are the students. For example

$$S = \{\text{Alice, Olivia, Jake, Sahab}\}$$

In this case we have

$$\text{Alice} \in S$$

but instead

$$\text{Silvio} \notin S\,.$$

2.2 Logic

In this section we introduce some basic logic symbols. Suppose that you are given two statements, say α and β. The formula

$$\alpha \implies \beta$$

means that α **implies** β. In other words, if α is true then also β is true.
The formula

$$\alpha \impliedby \beta$$

means that α is implied by β: if β is true then also α is true.
When we write

$$\alpha \iff \beta \tag{2.1}$$

we mean that α and β are **equivalent**. Note that (2.1) is equivalent to

$$\alpha \implies \beta \text{ and } \beta \implies \alpha\,.$$

Such equivalence is very useful in proofs.

Example 2.2

We have that

$$x > 0 \implies x > -100\,,$$

and

$$\text{contradiction} \impliedby \sqrt{2} \in \mathbb{Q}\,.$$

Concerning $\iff$ we have

$$x^2 < 2 \iff -\sqrt{2} < x < \sqrt{2}\,.$$

We now introduce logic **quantifiers**. These are

- $\forall$ which reads **for all**
- $\exists$ which reads **exists**
- $\exists!$ which reads **exists unique**
- $\nexists$ which reads **does not exists**

These work in the following way. Suppose that you are given a statement $\alpha(x)$ which depends on the point $x \in \mathbb{R}$. Then we say

- $\alpha(x)$ is satisfied for all $x \in A$ with A some collection of numbers. This translates to the symbols

$$\alpha(x) \text{ is true } \forall\, x \in A\,,$$

- There exists some x in $\mathbb{R}$ such that $\alpha(x)$ is satisfied: in symbols

$$\exists\, x \in \mathbb{R} \text{ such that } \alpha(x) \text{ is true},$$

- There exists a unique x_0 in $\mathbb{R}$ such that $\alpha(x)$ is satisfied: in symbols

$$\exists!\, x_0 \in \mathbb{R} \text{ such that } \alpha(x_0) \text{ is true},$$

- $\alpha(x)$ is never satisfied:

$$\nexists\, x \in \mathbb{R} \text{ such that } \alpha(x) \text{ is true}.$$

Example 2.3

Let us make concrete examples:

- The expression x^2 is always non-negative. Thus we can say

$$x^2 \geq 0 \quad \text{for all} \quad x \in \mathbb{R}\,.$$

- The equation $x^2 = 1$ has two solutions $x = 1$ and $x = -1$. Therefore we can say

$$\exists\, x \in \mathbb{R} \text{ such that } x^2 = 1\,.$$

- The equation $x^3 = 1$ has a unique solution $x = 1$. Thus

$$\exists!\, x \in \mathbb{R} \text{ such that } x^3 = 1\,.$$

- We know that the equation $x^2 = 2$ has no solutions in $\mathbb{Q}$. Then

$$\nexists\, x \in \mathbb{Q} \text{ such that } x^2 = 2\,.$$

2.3 Operations on sets

2.3.1 Union and intersection

For two sets A and B we define their **union** as the set

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

The **intersection** of A and B is defined by

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

We denote the **empty set** by the symbol $\emptyset$. Two sets are **disjoint** if

$$A \cap B = \emptyset\,.$$

Example 2.4

Define the subset of rational numbers

$$S := \left\{ x \in \mathbb{Q} \,:\, 0 < x < \frac{5}{2} \right\}.$$

Then we have

$$\mathbb{N} \cap S = \{1, 2\}.$$

We can also define the sets of **even** and **odd** numbers by

$$E := \{2n \,:\, n \in \mathbb{N}\}, \tag{2.2}$$
$$O := \{2n + 1 \,:\, n \in \mathbb{N}\}. \tag{2.3}$$

Then we have

$$\mathbb{N} \cap E = E, \ \mathbb{N} \cap O = O, \tag{2.4}$$
$$O \cup E = \mathbb{N}, \ O \cap D = \emptyset. \tag{2.5}$$

2.3.2 Inclusion and equality

Given two sets A and B, we say that A is **contained** in B if all the elements of A are also contained in B. This will be denoted with the **inclusion** symbol $\subseteq$, that is,

$$A \subseteq B.$$

In this case we say that

- A is a **subset** of B,
- B is a **superset** of A.

The inclusion $A \subseteq B$ is equivalent to the implication:

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

for all $x \in A$. The symbol $\implies$ reads **implies**, and denotes the fact that the first condition implies the second.

Example 2.5

Given two sets A and B we always have

$$(A \cap B) \subseteq A\,,\ (A \cap B) \subseteq B\,, \tag{2.6}$$
$$A \subseteq (A \cup B)\,,\ B \subseteq (A \cup B)\,. \tag{2.7}$$

We say that two sets A and B are equal if they contain the **same** elements. We denote equality by the symbol

$$A = B\,.$$

If $A \subseteq B$ and $A \neq B$, we write

$$A \subset B \quad \text{or} \quad A \subsetneq B\,.$$

Example 2.6

1. The sets
$$A = \{1, 2, 3\}\,, \quad B = \{3, 1, 2\}$$
are equal, that is $A = B$. This is because they contain exactly the same elements: **order** does not matter when talking about sets.

2. Consider the sets
$$A = \{1, 2\}\,, \quad B = \{1, 2, 5\}\,.$$
Then A is contained in B, but A is not equal to B. Therefore we write $A \subset B$ or $A \subsetneq B$.

Proposition 2.7

Let A and B be sets. Then

$$A = B$$

if and only if

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

Proof

The proof is almost trivial. However it is a good exercise in basic logic, so let us do it.

1. First implication $\Longrightarrow$:
Suppose that $A = B$. Let us show that $A \subseteq B$. Since $A = B$, this means that all the elements of A are also contained in B. Therefore if we take $x \in A$ we have
$$x \in A \implies x \in B\,.$$
This shows $A \subseteq B$. The proof of $B \subseteq A$ is similar.

2. Second implication $\Longleftarrow$:
   Suppose that $A \subseteq B$ and $B \subseteq A$. We need to show $A = B$, that is, A and B have the same elements. To this end let $x \in A$. Since $A \subseteq B$ then we have $x \in B$. Thus B contains all the elements of A. Since we are also assuming $B \subseteq A$, this means that A contains all the elements of B. Hence A and B contain the same elements, and $A = B$.

The above proposition is very useful when we need to **prove** that two sets are equal: rather than showing directly that $A = B$, we can prove that $A \subseteq B$ and $B \subseteq A$.

2.3.3 Infinite unions and intersections

Suppose given a set Ω, and a family of sets $A_n \subseteq \Omega$, where $n \in \mathbb{N}$. Then we can define the **infinte union**

$$\bigcup_{n\in\mathbb{N}} A_n := \{x \in \Omega : \ x \in A_n \ \text{ for at least one } \ n \in \mathbb{N}\}.$$

The **infinte intersection** is defined as

$$\bigcap_{n\in\mathbb{N}} A_n := \{x \in \Omega : \ x \in A_n \ \text{ for all } \ n \in \mathbb{N}\}.$$

Example 2.8

Let the ambient set be $\Omega := \mathbb{N}$ and define the family A_n by

$$A_1 := \{1, 2, 3, 4, ...\} \tag{2.8}$$
$$A_2 := \{2, 3, 4, 5, ...\} \tag{2.9}$$
$$A_3 := \{3, 4, 5, 6, ...\} \tag{2.10}$$
$$\ldots\ldots \tag{2.11}$$
$$A_n := \{n, n+1, n+2, n+3, ...\}, \tag{2.12}$$

for arbitrary $n \in \mathbb{N}$. Then

$$\bigcup_{n\in\mathbb{N}} A_n = \mathbb{N}. \tag{2.13}$$

The above equality can be easily proven using Proposition 2.7. Indeed, assume that $m \in \cup_n A_n$. Then $m \in A_n$ for at least one $n \in \mathbb{N}$. Since $A_n \subseteq \mathbb{N}$, we conclude that $m \in \mathbb{N}$. This shows

$$\bigcup_{n\in\mathbb{N}} A_n \subseteq \mathbb{N}.$$

Conversely, suppose that $m \in \mathbb{N}$. By definition $m \in A_m$. Hence there exists at least one index n, $n = m$ in this case, such that $m \in A_n$. Then by definition $m \in \cup_{n\in\mathbb{N}} A_n$, showing that

$$\mathbb{N} \subseteq \bigcup_{n\in\mathbb{N}} A_n.$$

Hence we conclude (2.13) by Proposition 2.7.
We also have that

$$\bigcap_{n\in\mathbb{N}} A_n = \emptyset\,. \tag{2.14}$$

We prove the above by **contradiction**. Indeed, suppose that (2.14) is false, i.e.,

$$\bigcap_{n\in\mathbb{N}} A_n \neq \emptyset\,.$$

This means there exists some $m \in \mathbb{N}$ such that $m \in \cap_{n\in\mathbb{N}} A_n$. Hence, by definition, $m \in A_n$ for all $n \in \mathbb{N}$. However $m \notin A_{m+1}$, yielding a contradiction. Thus (2.14) holds.

2.3.4 Complement

Suppose that A and B are subsets of a larger set Ω. The **complement** of A with respect to B is the set of elements of B which do not belong to A, that is

$$B \setminus A := \{x \in \Omega : \ x \in B \text{ and } x \notin A\}\,.$$

In particular, the complement of A with respect to Ω is denoted by

$$A^c := \Omega \setminus A := \{x \in \Omega : \ x \notin A\}\,.$$

Remark 2.9

Suppose that $A \subseteq \Omega$. Then A and A^c form a **partition** of Ω, in the sense that

$$A \cup A^c = \Omega \ \text{ and } \ A \cap A^c = \emptyset\,.$$

Example 2.10

Suppose $A, B \subseteq \Omega$. Then

$$A \subseteq B \iff B^c \subseteq A^c\,.$$

Let us prove the above claim:

- First implication $\implies$:
  Suppose that $A \subseteq B$. We need to show that $B^c \subseteq A^c$. Hence, assume $x \in B^c$. By definition this means that $x \notin B$. Now notice that we cannot have that $x \in A$. Indeed, assume $x \in A$. By assumption we have $A \subseteq B$, hence $x \in B$. But we had assumed $x \in B$, contradiction. Therefore it must be that $x \notin A$. Thus $B^c \subseteq A^c$.

- Second implication $\Longleftarrow$:
  Essentially the same proof, hence we omit it.

We conclude by stating the De Morgan's Laws. The proof will be left as an exercise.

Proposition 2.11: De Morgan's Laws

Suppose $A, B \subseteq \Omega$. Then

$$(A \cap B)^c = A^c \cup B^c$$

and

$$(A \cup B)^c = A^c \cap B^c \,.$$

2.3.5 Power set

Let Ω be an arbitray set. We define the **power set** of Ω as

$$\mathscr{P}(\Omega) := \{A \,:\, A \subseteq \Omega\},$$

that is, the power set of Ω is the set of all subsets of Ω.

Remark 2.12

It holds that:

1. $\mathscr{P}(\Omega)$ is always non-empty, since we have that

   $$\emptyset \in \mathscr{P}(\Omega), \quad \Omega \in \mathscr{P}(\Omega).$$

2. Given $A, B \in \mathscr{P}(\Omega)$, then the sets

   $$A \cup B, \quad A \cap B, \quad A^c, \quad B \setminus A$$

   are all elements of $\mathscr{P}(\Omega)$.

3. Suppose Ω is **discrete** and **finite**, that is,

   $$\Omega = \{x_1, \ldots, x_m\}$$

   for some $m \in \mathbb{N}$. Then $\mathscr{P}(\Omega)$ contains 2^m elements.

   This is because for each $x_i \in \Omega$ we have just two choices: either include x_i in a subset, or do not include x_i in a subset.

Example 2.13

Define the set

$$\Omega = \{x, y, z\}.$$

Then $\mathscr{P}(\Omega)$ has $2^3 = 8$ elements. These are

- $\emptyset$
- $\{x\}$
- $\{y\}$
- $\{z\}$
- $\{x, y\}$
- $\{x, z\}$
- $\{y, z\}$
- $\{x, y, z\}$

We therefore write

$$\mathscr{P}(\Omega) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\} \tag{2.15}$$
$$\{x, z\}, \{y, z\}, \{x, y, z\}\}. \tag{2.16}$$

2.3.6 Product of sets

Suppose A and B are two sets. The **product** of A and B is the set of pairs

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

By definition two elements in $A \times B$ are the same, in symbols

$$(a, b) = (\tilde{a}, \tilde{b})$$

if and only if they are equal component-by-componenent, that is

$$a = \tilde{a}, \qquad b = \tilde{b}.$$

2.4 Equivalence relation

Suppose A is a set. A **binary relation** R on A is a subset

$$R \subseteq A \times A.$$

Definition 2.14: Equivalence relation

A binary relation R is called an **equivalence relation** if it satisfies the following properties:

1. **Reflexive**: For each $x \in A$ one has
$$(x, x) \in R,$$
This is saying that all the elements in A must be related to themselves
2. **Symmetric**: We have
$$(x, y) \in R \implies (y, x) \in R$$
If x is related to y, then y is related to x
3. **Transitive**: We have
$$(x, y) \in R,\ (y, z) \in R \implies (x, z) \in R$$
If x is related to y, and y is related to z, then x must be related to z

If $(x, y) \in R$ we write
$$x \sim y$$
and we say that x and y are **equivalent**.

Definition 2.15: Equivalence classes

Suppose R is an **equivalence relation** on A. The **equivalence class** of an element $x \in A$ is the set
$$[x] := \{y \in A : \ y \sim x\}.$$
The set of equivalence classes of elements of A with respect to the equivalence relation R is denoted by
$$A/R := \{[x] : \ x \in A\}.$$

Let us immediately clarify the above definitions by considering the prototypical example of equivalence relation: the **equality**.

Example 2.16: Equality is an equivalence relation

Consider the set of natural numbers $\mathbb{N}$. The equality defines a **binary relation** on $\mathbb{N} \times \mathbb{N}$, via
$$R := \{(x, y) \in \mathbb{N} \times \mathbb{N} : \ x = y\}.$$
Let us check that R is an **equivalence relation**:

1. Reflexive: It holds, since $x = x$ for all $x \in \mathbb{N}$,

2. Symmetric: Again $x = y$ if and only if $y = x$,
3. Transitive: If $x = y$ and $y = z$ then $x = z$.

The class of equivalence of $x \in \mathbb{N}$ is given by

$$[x] = \{x\},$$

that is, this relation is quite trivial, given that each element of $\mathbb{N}$ can only be related to itself. The quotient space is then

$$\mathbb{N}/R = \{[x] \,:\, x \in \mathbb{N}\} = \{\{x\} \,:\, x \in \mathbb{N}\}.$$

Example 2.17

Suppose that R is a binary relation on the set $\mathbb{Q}$ of rational numbers defined by

$$x \sim y \iff x - y \in \mathbb{Z}.$$

Then R is an equivalence relation on $\mathbb{Q}$. Indeed:

1. Reflexive: Let $x \in \mathbb{Q}$. Then $x - x = 0$ and $0 \in \mathbb{Z}$. Thus $x \sim x$.
2. Symmetric: If $x \sim y$ then $x - y \in \mathbb{Z}$. But then also

   $$-(x - y) = y - x \in \mathbb{Z}$$

   and so $y \sim x$.
3. Transitive: Suppose $x \sim y$ and $y \sim z$. Then

   $$x - y \in \mathbb{Z} \text{ and } y - z \in \mathbb{Z}.$$

   Thus we have

   $$x - z = (x - y) + (y - z) \in \mathbb{Z}$$

   showing that $x \sim z$. This shows that R is an equivalence relation on $\mathbb{Q}$.

Now note that

$$y \sim x \iff y - x \in \mathbb{Z}$$

and the above is equivalent to

$$\exists n \in \mathbb{Z} \text{ s.t. } y - x = n$$

which again is equivalent to

$$\exists n \in \mathbb{Z} \text{ s.t. } y = x + n.$$

Therefore all the elements of $\mathbb{Q}$ related to x by R are of the form

$$x + n, \forall n \in \mathbb{Z}.$$

The equivalence classes with respect to R are then

$$[x] = \{x + n \ : \ n \in \mathbb{Z}\}.$$

Each equivalence class has exactly one element in $[0, 1) \cap \mathbb{Q}$, meaning that:

$$\forall x \in \mathbb{Q}\,, \ \exists!\, q \in \mathbb{Q} \text{ s.t. } 0 \leq q < 1 \text{ and } q \in [x]\,.$$

Therefore

$$\mathbb{Q}/R = \{[x] \ : \ x \in \mathbb{Q}\} = \{q \in \mathbb{Q} \ : \ 0 \leq q < 1\}.$$

2.5 Order relation

Similarly, we define **order relations**.

Definition 2.18: Partial order

A binary relation R on A is called a **partial order** if it satisfies the following properties:

1. **Reflexive**: For each $x \in A$ one has
$$(x, x) \in R\,,$$
2. **Transitive**: We have
$$(x, y) \in R\,, \ (y, z) \in R \implies (x, z) \in R$$
3. **Antisymmetric**: We have
$$(x, y) \in R \text{ and } (y, x) \in R \implies x = y$$
This is the only new condition with respect to the definition of equivalence relation, and it replaces symmetry.

Definition 2.19: Total order

A binary relation R on A is called a **total order relation** if it satisfies the following properties:

1. **Partial order**: R is a partial order on A.
2. **Total**: For each $x, y \in A$ we have
$$(x, y) \in R \ \text{ or } \ (y, x) \in R\,.$$
This is saying that all elements in A are related.

An example of partial order is the operation of **set inclusion**.

Example 2.20: Set inclusion is a partial order

Consider an arbitrary non-empty set Ω and consider its **power set**

$$\mathscr{P}(\Omega) = \{A \ : \ A \subseteq \Omega\}.$$

The inclusion defines **binary relation** on $\mathscr{P}(\Omega) \times \mathscr{P}(\Omega)$, via

$$R := \{(A, B) \in \mathscr{P}(\Omega) \times \mathscr{P}(\Omega) \ : \ A \subseteq B\}.$$

Let us check that R is an **order relation**:

1. Reflexive: It holds, since $A \subseteq A$ for all $A \in \mathscr{P}(\Omega)$,
2. Transitive: If $A \subseteq B$ and $B \subseteq C$, then by definition of inclusion $A \subseteq C$.
3. Antisymmetric: If $A \subseteq B$ and $B \subseteq A$, then $A = B$ by Proposition 2.7.

Therefore R is a **partial order** on $\mathscr{P}(\Omega)$. Note that in general R is **not** a total order. For example if we consider

$$\Omega = \{x, y\}.$$

Thus

$$\mathscr{P}(\Omega) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}.$$

If we pick $A = \{x\}$ and $B = \{y\}$ then $A \cap B = \emptyset$, meaning that

$$A \nsubseteq B, \quad B \nsubseteq A,$$

showing that R is not a total order.

A very important example of total order is the **inequality** on $\mathbb{Q}$.

Example 2.21: Inequality is a total order

Consider the set of rationals $\mathbb{Q}$. The usual inequality defines a **binary relation** on $\mathbb{Q} \times \mathbb{Q}$, via

$$R := \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \ : \ x \leq y\}.$$

Let us check that R is an **order relation**:

1. Reflexive: It holds, since $x \leq x$ for all $x \in \mathbb{Q}$,
2. Transitive: If $x \leq y$ and $y \leq z$ then $x \leq z$.

3. Antisymmetric: If $x \leq y$ and $y \leq x$ then $x = y$.

Finally, we halso have that R is a **total order** on $\mathbb{Q}$, since for all $x, y \in \mathbb{Q}$ we have

$$x \leq y \quad \text{or} \quad y \leq x\,.$$

Notation 2.22

If Ω is a set and R is a total order on Ω, we write

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

Therefore the symbol $\leq$ will always denote a total order relation.

2.6 Intervals

In this section we assume to have available the set $\mathbb{R}$ of **real numbers**, which we recall is an extension of $\mathbb{Q}$. We now introduce the concept of **interval**.

Definition 2.23

Let $a, b \in \mathbb{R}$ with $a < b$. We define the **open interval** (a, b) as the set

$$(a, b) := \{x \in \mathbb{R} : \ a < x < b\}\,.$$

We define the **close interval** $[a, b]$ as the set

$$[a, b] := \{x \in \mathbb{R} : \ a \leq x \leq b\}\,.$$

In general we also define the intervals

$$[a, b) := \{x \in \mathbb{R} : \ a \leq x < b\}\,, \tag{2.17}$$
$$(a, b] := \{x \in \mathbb{R} : \ a \leq x \leq b\}\,, \tag{2.18}$$
$$(a, \infty) := \{x \in \mathbb{R} : \ x > a\}\,, \tag{2.19}$$
$$[a, \infty) := \{x \in \mathbb{R} : \ x \geq a\}\,, \tag{2.20}$$
$$(-\infty, b) := \{x \in \mathbb{R} : \ x < b\}\,, \tag{2.21}$$
$$(-\infty, b] := \{x \in \mathbb{R} : \ x \leq b\}\,. \tag{2.22}$$

Some of the above intervals are depicted in Figure 2.1, Figure 2.2, Figure 2.3, Figure 2.4 below.

Figure 2.1: Interval (a, b)

Figure 2.2: Interval $[a, b]$

2.7 Functions

Definition 2.24: Functions

Let A and B be sets. A **function** from A to B is a rule which associates **at each** element $x \in A$ a **single** element $y \in B$. Notations:

- We write
$$f : A \to B$$
to indicate such rule,
- For $x \in A$, we denote by
$$y := f(x) \in B$$
the element associated with x by f.
- We will often denote the map f also by
$$x \mapsto f(x).$$

In addition:

- The set A is called the **domain** of f,
- The **range** of f is the set
$$\{y \in B : \ y = f(x) \text{ for some } x \in A\} \subseteq B.$$

Warning

We want to stress the importance of the first two sentences in Definition 2.24. Assume that $f : A \to B$ is a function. Then:

Figure 2.3: Interval (a, ∞)

Figure 2.4: Interval $(-\infty, b]$

- To each element $x \in A$ we can **only** associate **one** element $f(x) \in B$,
- Every element $x \in A$ has to be associated to an element $f(x) \in B$.

Example 2.25

Assume given the two sets

$$A = \{a_1, a_2\}, \quad B = \{b_1, b_2, b_3\}.$$

Let us see a few examples:

- Define $f : A \to B$ by setting
$$f(a_1) = b_1, \quad f(a_2) = b_1.$$
In this way f is a function, with domain A and range
$$f(A) = \{b_1\} \subseteq B.$$
- Define $g : A \to B$ by setting
$$g(a_1) = b_2, \quad g(a_1) = b_3, \quad g(a_2) = b_3$$
Then g is **NOT** a function, since the element a_1 has two elements associated.
- Define $h : A \to B$ by setting
$$h(a_1) = b_1.$$
Then g is **NOT** a function, since the element a_2 has no element associated.

Example 2.26

Let us make two examples of functions on $\mathbb{R}$:

- Define $f : \mathbb{R} \to \mathbb{R}$ by
$$f(x) = x^2.$$
Note that the domain of f is given by $\mathbb{R}$, while the range is
$$f(\mathbb{R}) = [0, \infty).$$
- Define $g : \mathbb{R} \to \mathbb{R}$ as the logarithm:
$$g(x) = \log(x).$$
This time the domain is $(0, \infty)$, while the range is $g(\mathbb{R}) = \mathbb{R}$.

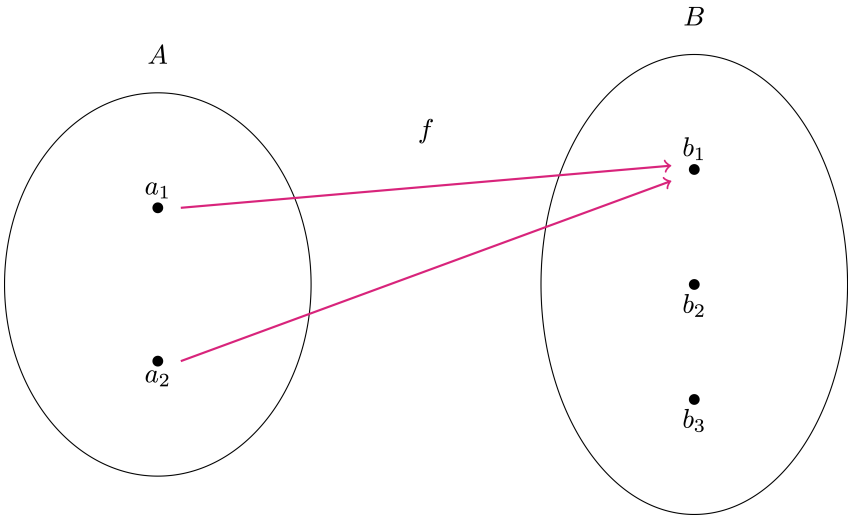

Figure 2.5: Schematic picture of the function f

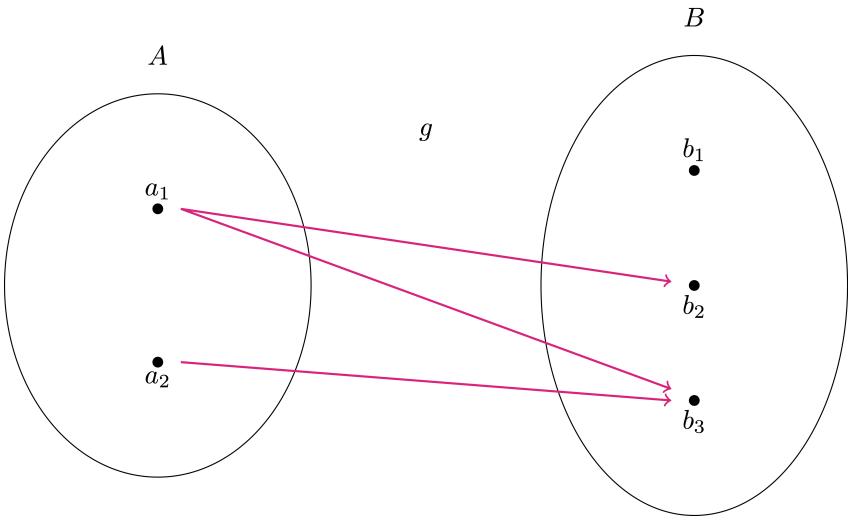

Figure 2.6: Schematic picture of the function g

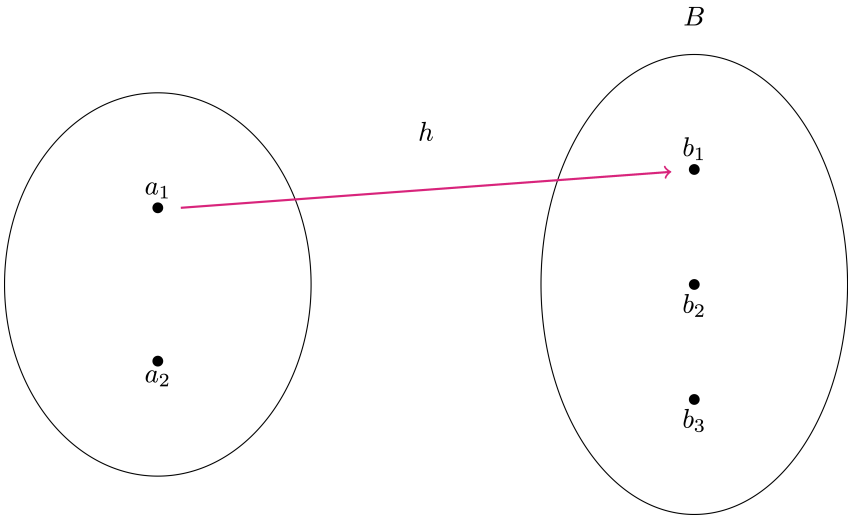

Figure 2.7: Schematic picture of the function h

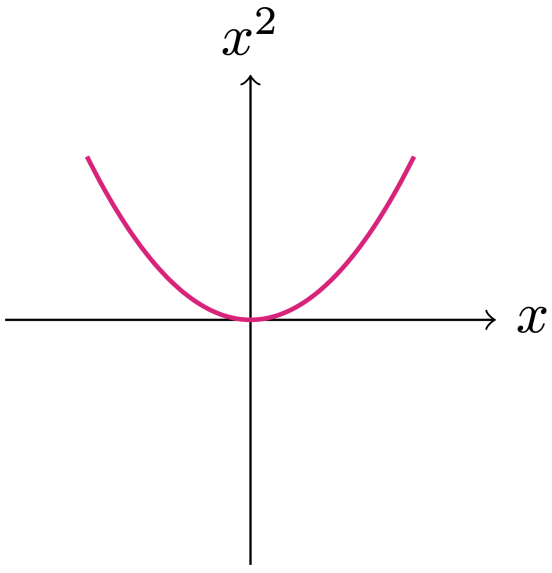

Figure 2.8: Plot of function $f(x) = x^2$

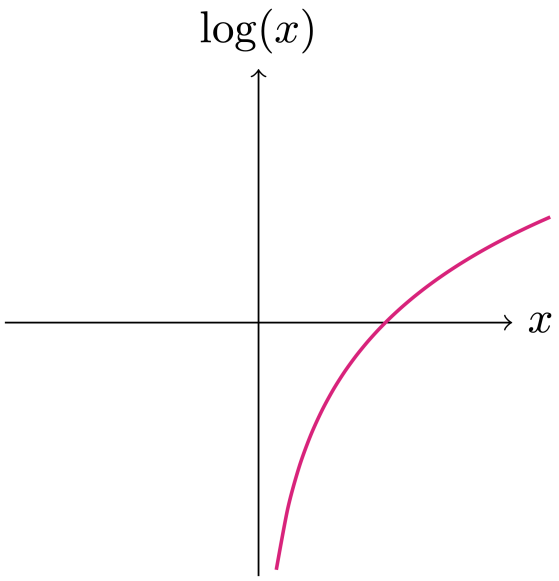

Figure 2.9: Plot of function $g(x) = \log(x)$

2.8 Absolute value or Modulus

In this section we assume to have available the set $\mathbb{R}$ of **real numbers**, which we recall is an extension of $\mathbb{Q}$.

Definition 2.27: Absolute value

For $x \in \mathbb{R}$ we define its **absolute value** as the quantity

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

Example 2.28

By definition one has $|x| = x$ if $x \geq 0$. For example

$$|\pi| = \pi\,, \quad \left|\sqrt{2}\right| = \sqrt{2}\,, \quad |0| = 0\,.$$

Instead $|x| = -x$ if $x < 0$. For example

$$|-\pi| = \pi\,, \quad \left|-\sqrt{2}\right| = \sqrt{2}\,, \quad |-10| = 10\,.$$

Let us also make the following basic remark, whose proof will be left as an exercise.

Remark 2.29

For all $x \in \mathbb{R}$ one has

$$|x| \geq 0\,.$$

Moreover

$$|x| = 0 \iff x = 0\,.$$

Another basic remark (proof by exercise).

Remark 2.30

For all $x \in \mathbb{R}$ one has

$$|x| = |-x|\,.$$

We can use the definition of absolute value to define the **absolute value function**. This is the function

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) := |x|\,.$$

You might be familiar with the graph associated to f, as seen below.

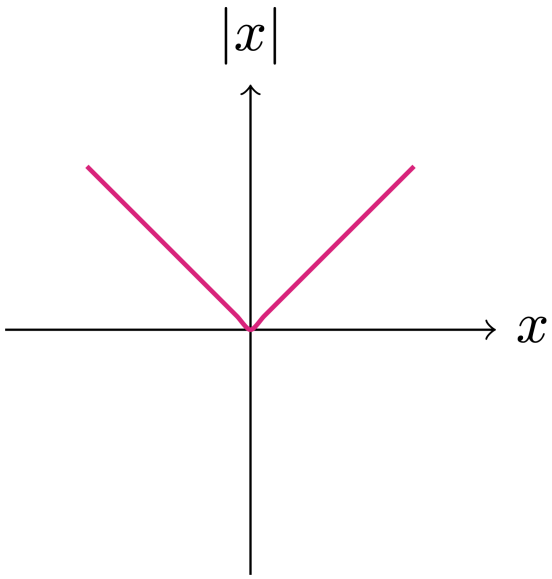

Figure 2.10: Plot of the absolute value function $f(x) = |x|$

It is also useful to understand the absolute value in a geometric way.

Remark 2.31: Geometric interpretation of $|x|$

A number $x \in \mathbb{R}$ can be represented with a point on the real line $\mathbb{R}$.The non-negative number $|x|$ represents the **distance** of x from the origin 0. Notice that this works for both positive and negative numbers x_1 and x_2 respectively, as shown in Figure 2.11 below.

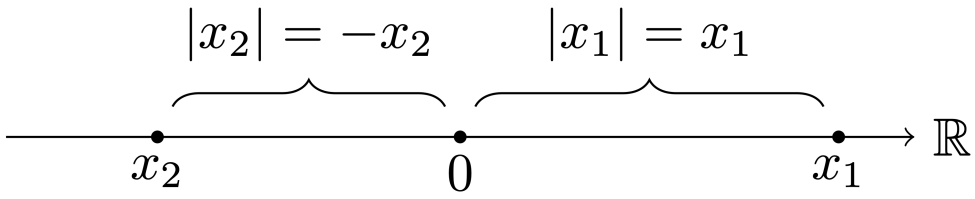

Figure 2.11: Geometric interpretation of $|x|$

Remark 2.32: Geometric interpretation of $|x - y|$

If $x, y \in \mathbb{R}$ then the number $|x - y|$ represents the distance between x and y on the real line, as shown in Figure 2.12 below. Note that by Remark 2.30 we have

$$|x - y| = |y - x| .$$

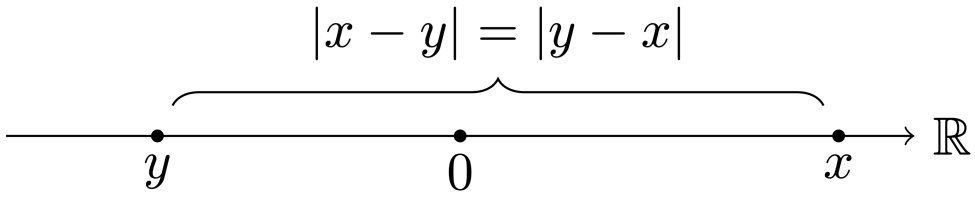

Figure 2.12: Geometric interpretation of $|x - y|$

In the next Lemma we show a fundamental equivalence regarding the absolute value.

Lemma 2.33

Let $x, y \in \mathbb{R}$. Then

$$|x| \leq y \iff -y \leq x \leq y .$$

The geometric meaning of the above statement is clear: the distance of x from the origin is less than y, in formulae

$$|x| \leq y ,$$

if and only if x belongs to the interval $[-y, y]$, in formulae

$$-y \leq x \leq y .$$

A sketch of this explanation is seen in Figure 2.13 below.

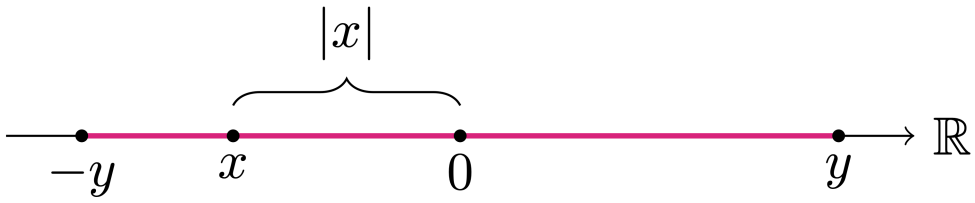

Figure 2.13: Geometric meaning of Lemma 2.33

Proof: Proof of Lemma 2.33

Step 1: First implication.
Suppose first that

$$|x| \leq y\,. \tag{2.23}$$

Recalling that the absolute value is non-negative, from (2.23) we deduce that $0 \leq |x| \leq y$. In particular it holds

$$y \geq 0\,. \tag{2.24}$$

We make separate arguments for the cases $x \geq 0$ and $x < 0$:

- Case 1: $x \geq 0$. From (2.23), (2.24) and from $x \geq 0$ we have

  $$-y \leq 0 \leq x = |x| \leq y$$

  which shows

  $$-y \leq x \leq y\,.$$

- Case 2: $x < 0$. From (2.23), (2.24) and from $x < 0$ we have

  $$-y \leq 0 < -x = |x| \leq y$$

  which shows

  $$-y \leq -x \leq y\,.$$

  Multiplying the above inequalities by -1 yields

  $$-y \leq x \leq y\,.$$

Step 2: Second implication.
Suppose now that

$$-y \leq x \leq y\,. \tag{2.25}$$

We make separate arguments for the cases $x \geq 0$ and $x < 0$:

- Case 1: $x \geq 0$. Since $x \geq 0$, from (2.25) we get

$$|x| = x \leq y$$

  showing that

$$|x| \leq y\,.$$

- Case 2: $x < 0$. Since $x < 0$, from (2.25) we have

$$-y \leq x = -|x|\,.$$

  Multiplying the above inequality by -1 yields

$$|x| \leq y\,.$$

With the same arguments, just replacing $\leq$ with $<$, one can also show the following.

Lemma 2.34

Let $x, y \in \mathbb{R}$. Then

$$|x| < y \iff -y < x < y\,.$$

2.9 Triangle inequality

The triangle inequality relates the absolute value to the sum operation. It is a very important inequality, which we will use a lot in the future.

Theorem 2.35: Triangle inequality

For every $x, y \in \mathbb{R}$ we have

$$||x| - |y|| \leq |x + y| \leq |x| + |y|\,. \tag{2.26}$$

Before proceeding with the proof, let us discuss the geometric meaning of the triangle inequality.

Remark 2.36: Geometric meaning of triangle inequality

The notion of absolute value can be extended also to vectors in the plane. Suppose that x and y are two vectors in the plane, as in Figure 2.14 below. Then $|x|$ and $|y|$ can be interpreted as the **lengths** of these

vectors.
Using the rule of sum of vectors, we can draw $x + y$, as shown in Figure 2.15 below. From the picture it is evident that

$$|x + y| \leq |x| + |y|\,, \tag{2.27}$$

that is, *the length of each side of a triangle does not exceed the sum of the lengths of the two remaining sides.* Note that (2.27) is exactly the second inequality in (2.26). This is why (2.26) is called triangle inequality.

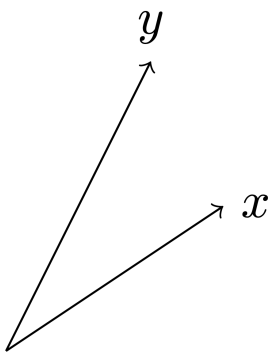

Figure 2.14: Vectors x and y

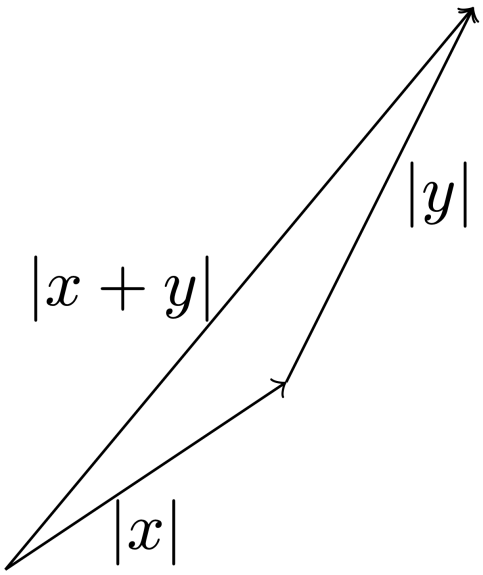

Figure 2.15: Summing the vectors x and y. The triangle inequality relates the length of $x + y$ to the length of x and y

Proof: Proof of Theorem 2.32

Assume that $x, y \in \mathbb{R}$. We prove the two inequalities in (2.26) individually.
Step 1. Proof of the second inequality in (2.26).
Trivially we have

$$|x| \leq |x| .$$

Therefore we can apply Lemma 2.33 and infer

$$-|x| \leq x \leq |x| . \tag{2.28}$$

Similarly we have that $|y| \leq |y|$, and so Lemma 2.33 implies

$$-|y| \leq y \leq |y| . \tag{2.29}$$

Summing (2.28) and (2.29) we get

$$-(|x| + |y|) \leq x + y \leq |x| + |y| .$$

We can now again apply Lemma 2.33 to get

$$|x + y| \leq |x| + |y| , \tag{2.30}$$

which is the second inequality in (2.26).
Step 2. Proof of the first inequality in (2.26).
Note that the trivial identity

$$x = x + y - y$$

always holds. We then have

$$\begin{aligned} |x| &= |x + y - y| && (2.31)\\ &= |(x + y) + (-y)| && (2.32)\\ &= |a + b| && (2.33) \end{aligned}$$

with $a = x + y$ and $b = -y$. We can now apply (2.30) to a and b to obtain

$$\begin{aligned} |x| &= |a + b| && (2.34)\\ &\leq |a| + |b| && (2.35)\\ &= |x + y| + |-y| && (2.36)\\ &= |x + y| + |y| && (2.37) \end{aligned}$$

Therefore

$$|x| - |y| \leq |x + y| . \tag{2.38}$$

We can now swap x and y in (2.38) to get

$$|y| - |x| \leq |x + y| .$$

By rearranging the above inequality we obtain

$$-|x+y| \leq |x| - |y| \,. \tag{2.39}$$

Putting together (2.38) and (2.39) yields

$$-|x+y| \leq |x| - |y| \leq |x+y| \,.$$

By Lemma 2.33 the above is equivalent to

$$||x| - |y|| \leq |x+y| \,,$$

which is the first inequality in (2.26).

An immediate consequence of the triangle inequality are the following inequalities, which are left as an exercise.

Remark 2.37

For any $x, y \in \mathbb{R}$ it holds

$$||x| - |y|| \leq |x-y| \leq |x| + |y| \,.$$

Moreover for any $x, y, z \in \mathbb{R}$ it holds

$$|x-y| \leq |x-z| + |z-y| \,.$$

2.10 Proofs in Mathematics

In a mathematical proof one needs to show that

$$\alpha \implies \beta \tag{2.40}$$

where

- α is a given set of assumptions, or **Hypothesis**
- β is a conclusion, or **Thesis**

Proving (2.40) means convincing ourselves that β follows from α. Common strategies to prove (2.40) are:

1. **Contradiction**: Assume that the thesis is **false**, and hope to reach a contradiction: that is, prove that

   $$\neg\beta \implies \text{contradiction}$$

   where $\neg\beta$ is the **negation** of β.

For example we already proved by contradiction that

$$\text{Definition of } \mathbb{Q} \implies \sqrt{2} \notin \mathbb{Q}\,,$$

In the above statement

$$\alpha = (\text{Definition of } \mathbb{Q})\ .$$
$$\beta = \left(\sqrt{2} \notin \mathbb{Q}\right)\ .$$

Therefore

$$\neg\beta = \left(\sqrt{2} \in \mathbb{Q}\right)\ .$$

2. **Direct**: Sometimes proofs will also need **direct** arguments, meaning that one need to show directly that (2.40) holds.
3. **Contrapositive**: The statement (2.40) is equivalent to

$$\neg\beta \implies \neg\alpha\,. \tag{2.41}$$

Thus, instead of proving (2.40), one could show (2.41). The statement (2.41) is called the **contrapositive** of (2.40).

Let us make an example.

Proposition 2.38

Two real numbers a, b are equal if and only if for every real number $\varepsilon > 0$ it follows that $|a - b| < \varepsilon$.

Before proceeding with the proof, note that the above stetement is just saying that:

Two numbers are equal if and only if they are **arbitrarily** close

By *arbitrarily close* we mean that they are *as close as you want the to be.*

Proof: of Proposition 2.38

Let us first rephrase the statement using mathematical symbols:

Let $a, b \in \mathbb{R}$. Then it holds:

$$a = b \iff |a - b| < \varepsilon\,,\ \forall\, \varepsilon > 0\,.$$

Setting

$$\alpha = (a = b) \tag{2.42}$$
$$\beta = (|a - b| < \varepsilon\,,\ \forall\, \varepsilon > 0) \tag{2.43}$$

the statement is equivalent to

$$\alpha \iff \beta\,.$$

To show the above, it is sufficient to show that

$$\alpha \implies \beta \quad \text{and} \quad \beta \implies \alpha\,.$$

Step 1. Proof that $\alpha \implies \beta$.
This proof can be carried out by a **direct** argument. Since we are assuming α, this means

$$a = b\,.$$

We want to see that β holds. Therefore fix an arbitrary $\varepsilon > 0$. This means that ε can be **any** positive number, as long as you fix it. Clearly

$$|a-b| = |0| = 0 < \varepsilon$$

since $a = b$, $|0| = 0$, and $\varepsilon > 0$. The above shows that

$$|a-b| < \varepsilon\,.$$

As $\varepsilon > 0$ was arbitrary, we have just proven that

$$|a-b| < \varepsilon\,,\ \forall\, \varepsilon > 0\,,$$

meaning that β holds and the proof is concluded.
Step 2. Proof that $\beta \implies \alpha$.
Let us prove this implication by showing the **contrapositive**

$$\neg\alpha \implies \neg\beta\,.$$

So let us assume $\neg\alpha$ is true. This means that

$$a \neq b\,.$$

We have to see that $\neg\beta$ holds. But $\neg\beta$ means that

$$\exists\, \varepsilon_0 > 0 \ \text{ s.t. } \ |a-b| \geq \varepsilon_0\,.$$

The above is satisfied by choosing

$$\varepsilon_0 := |a-b|\,,$$

since $\varepsilon_0 > 0$ given that $a \neq b$.

2.11 Induction

Another technique for carrying out proofs is **induction**, which we take as an axiom.

Axiom 2.39: Principle of Induction

Let $S \subseteq \mathbb{N}$. Suppose that

1. We have $1 \in S$, and
2. Whenever $n \in S$, then $(n+1) \in S$.

Then we have

$$S = \mathbb{N}.$$

Important

The above is an **axiom**, meaning that we do not prove it, but rather we just **assume it holds**.

Remark 2.40

It would be possible to prove the Principle of Induction starting from elementary axioms for $\mathbb{N}$, called the **Peano Axioms**, see the Wikipedia page.
However, in justifying basic principles of mathematics, one at some point needs to draw a line. This means that something which looks elementary needs to be assumed to hold, in order to have a starting point for proving deeper statements.
In the case of the Principle of Induction, the intuition is clear:

> The Principle of Induction is just describing the **domino effect**: *If one tile falls, then the next one will fall as well.* Therefore if the *first tile falls, all the tiles will fall.*

It seems reasonable to assume such evident principle.

The Principle of Induction can be used to prove statements which depend on some index $n \in \mathbb{N}$. Precisely, the following statement holds.

Corollary 2.41: Principle of Inducion - Alternative formulation

Let $\alpha(n)$ be a statement which depends on $n \in \mathbb{N}$. Suppose that

1. $\alpha(1)$ is true, and

2. Whenever $\alpha(n)$ is true, then $\alpha(n+1)$ is true.

Then $\alpha(n)$ is true for all $n \in \mathbb{N}$.

Proof

Define the set

$$S := \{n \in \mathbb{N} \text{ s.t. } \alpha(n) \text{ is true}\}.$$

Then

1. We have $1 \in S$, since $\alpha(1)$ is true.
2. If $n \in S$ then $\alpha(n)$ is true. By assumption this implies that $\alpha(n+1)$ is true. Therefore $(n+1) \in S$.

Therefore S satisfies the assumptions of the Induction Principle and we conclude that

$$S = \mathbb{N}.$$

By definition this means that $\alpha(n)$ is true for all $n \in \mathbb{N}$.

Example 2.42: Formula for summing first n natural numbers

Using the Principle of Induction we can prove that

$$1 + 2 + 3 + \ldots + (n-1) + n = \frac{n(n+1)}{2} \tag{2.44}$$

holds for all $n \in \mathbb{N}$.
Proof. To be really precise, consider the statement

$$\alpha(n) := \text{ the above formula is true for } n.$$

In order to apply induction, we need to show that

1. $\alpha(1)$ is true,
2. If $\alpha(n)$ is true then $\alpha(n+1)$ is true.

Let us proceed:

1. It is immediate to check that (2.44) holds for $n = 1$.

2. Suppose (2.44) holds for n. Then

$$1 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) \tag{2.45}$$

$$= \frac{n(n+1) + 2(n+1)}{2} \tag{2.46}$$

$$= \frac{(n+1)(n+2)}{n} \tag{2.47}$$

where in the first equality we used that (2.44) holds for n. We then have

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

which shows that (2.44) holds for $n+1$.

By the Principle of Induction we then conclude that $\alpha(n)$ is true for all $n \in \mathbb{N}$, which means that (2.44) holds for all $n \in \mathbb{N}$.

Example 2.43: Statements about sequences of numbers

Suppose you are given a collection of numbers

$$\{x_n \text{ s.t. } n \in \mathbb{N}\}.$$

Such collection of numbers is called **sequence**. Assume that

$$x_1 := 1 \tag{2.48}$$

$$x_{n+1} := \frac{x_n}{2} + 1. \tag{2.49}$$

A sequence defined as above is called **recurrence sequence**. Using the above rule we can compute all the terms of x_n.

For example

$$x_2 = \frac{x_1}{2} + 1 = \frac{1}{2} + 1 = \frac{3}{2} \tag{2.50}$$

$$x_3 = \frac{x_2}{2} + 1 = \frac{3}{4} + 1 = \frac{7}{4}. \tag{2.51}$$

By computing these terms, we suspect that the sequence might be increasing, meaning that

$$x_{n+1} \geq x_n \tag{2.52}$$

for all $n \in \mathbb{N}$.
Claim. *(2.52) holds for all $n \in \mathbb{N}$.*
Proof of Claim.
We argue by induction:

1. We have seen that $x_1 = 1$ and $x_2 = 3/2$. Thus
$$x_2 \geq x_1 .$$
2. Suppose now that
$$x_{n+1} \geq x_n . \tag{2.53}$$
We need to prove that
$$x_{n+2} \geq x_{n+1} . \tag{2.54}$$
Indeed, we can multiply the inequality (2.53) by $1/2$ and add 1 to get
$$\frac{x_{n+1}}{2} + 1 \geq \frac{x_n}{2} + 1 .$$
The above is equivalent, by definition, to (2.54).

Therefore the assumptions of the Induction Principle are satisfied, and (2.52) follows.

3 Real Numbers

In this chapter we introduce the system of Real Numbers $\mathbb{R}$ and study some of its properties.

3.1 Fields

In order to introduce $\mathbb{R}$, we need the concepts of **binary operation** and **field**. We proceed in a general setting, starting from a set K.

Definition 3.1: Binary operation

A binary operation on a set K is a function

$$\circ : K \times K \to K$$

which maps the ordered pair (x, y) into $x \circ y$.

Notation 3.2

There are two main binary operations we are interested in:

- **Addition**: denoted by $+$. The addition, or **sum** of $x, y \in K$ is denoted by

$$x + y .$$

- **Multiplication**: denoted by $\cdot$. The multiplication, or **product** of $x, y \in K$ is denoted by

$$x \cdot y \quad \text{or} \quad xy .$$

Example 3.3: of binary operation

Let $K = \{0, 1\}$. We can for example define operations of sum and product on K according to the tables

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

The above mean that

$$0 + 0 = 1 + 1 = 0\,, \quad 0 + 1 = 1 + 0 = 1\,,$$

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0\,, \quad 1 \cdot 1 = 1\,.$$

This is just one option. Note that we could not have defined

$$1 + 1 = 2\,,$$

since $2 \notin K$.

Binary operations take ordered pairs of elements of K as input. Therefore the operation

$$x \circ y \circ z$$

does not make sense, since we do not know which one between

$$x \circ y \quad \text{or} \quad y \circ z$$

has to be performed first. Moreover the outcome of an operation depends on order:

$$x \circ y \neq y \circ x\,.$$

This motivates the following definition.

Definition 3.4

Let K be a set and $\circ : K \times K \to K$ be a binary operation on K. We say that:

1. $\circ$ is **commutative** if
$$x \circ y = y \circ x\,, \quad \forall\, x, y \in K$$
2. $\circ$ is **associative** if
$$(x \circ y) \circ z = x \circ (y \circ z)\,, \quad \forall\, x, y, z \in K$$
3. An element $e \in K$ is called **neutral element** of $\circ$ if
$$x \circ e = e \circ x = x\,, \quad \forall\, x \in K$$
4. Let e be a neutral element of $\circ$ and let $x \in K$. An element $y \in K$ is called an **inverse** of x with respect to $\circ$ if
$$x \circ y = y \circ x = e\,.$$

Example 3.5

Let K with $+$ and $\cdot$ be as in Example 3.1. The sum satisfies:

- $+$ is commutative, since
$$0 + 1 = 1 + 0 = 0\,.$$
- $+$ is associative, since for example
$$(0 + 1) + 1 = 1 + 1 = 0\,, \quad 0 + (1 + 1) = 0 + 0 = 0\,,$$
and therefore
$$(0 + 1) + 1 = 0 + (1 + 1)\,.$$
In general one can show that $+$ is associative by checking all the other permutations.
- The neutral element of $+$ is 0, since
$$0 + 0 = 0\,, \quad 1 + 0 = 0 + 1 = 1\,.$$
- Every element has an inverse. Indeed, the inverse of 0 is 0, since
$$0 + 0 = 0\,,$$
while the inverse of 1 is 1, since
$$1 + 1 = 1 + 1 = 0\,.$$

The multiplication satisfies:

- $\cdot$ is commutative, since
$$1 \cdot 0 = 0 \cdot 1 = 0\,.$$
- $\cdot$ is associative, since for example
$$(0 \cdot 1) \cdot 1 = 0 \cdot 1 = 0\,, \quad 0 \cdot (1 \cdot 1) = 0 \cdot 1 = 0\,,$$
and therefore
$$(0 \cdot 1) \cdot 1 = 0 \cdot (1 \cdot 1)\,.$$
By checking all the other permutations one can show that $\cdot$ is associative.
- The neutral element of $\cdot$ is 1, since
$$0 \cdot 1 = 1 \cdot 0 = 0\,, \quad 1 \cdot 1 = 1\,.$$
- The element 0 has no inverse, since
$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0\,,$$
and thus we never obtain the neutral element 1. The inverse of 1 is given by 1, since
$$1 \cdot 1 = 1\,.$$

Example 3.6

Let $K = \{0, 1\}$ be a set with binary relation $\circ$ defined by the table

$\circ$	0	1
0	1	1
1	0	0

In this case $\circ$ is not commutative since

$$0 \circ 1 = 1\,, \quad 1 \circ 0 = 0$$

and therefore

$$0 \circ 1 \neq 1 \circ 0\,.$$

Moreover $\circ$ is not associative, since

$$(0 \circ 1) \circ 1 = 1 \circ 1 = 0\,,$$

while

$$0 \circ (1 \circ 1) = 0 \circ 0 = 1\,,$$

so that

$$(0 \circ 1) \circ 1 \neq 0 \circ (1 \circ 1)\,.$$

We are ready to define fields.

Definition 3.7: Field

Let K be a set with binary operations of **addition**

$$+ \,:\, K \times K \to K\,, \quad (x, y) \mapsto x + y$$

and **multiplication**

$$\cdot \,:\, K \times K \to K\,, \quad (x, y) \mapsto x \cdot y = xy\,.$$

We call the triple $(K, +, \cdot)$ a **field** if:

1. The addition $+$ satisfies: $\forall\, x, y, z \in K$
   - (A1) **Commutativity and Associativity**:

$$x + y = y + x$$

$$(x + y) + z = x + (y + z)$$

   - (A2) **Additive Identity**: There exists a **neutral element** in K for $+$, which we call 0. It holds:

$$x + 0 = 0 + x = x$$

- (A3) **Additive Inverse**: There exists an **inverse** of x with respect to $+$. We call this element the **additive inverse** of x and denote it by $-x$. It holds

$$x + (-x) = (-x) + x = 0$$

2. The multiplication $\cdot$ satisifes: $\forall\, x, y, z \in K$

- (M1) **Commutativity and Associativity**:

$$x \cdot y = y \cdot x$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

- (M2) **Multiplicative Identity**: There exists a **neutral element** in K for $\cdot$, which we call 1. It holds:

$$x \cdot 1 = 1 \cdot x = x$$

- (M3) **Multiplicative Inverse**: If $x \neq 0$ there exists an **inverse** of x with respect to $\cdot$. We call this element the **multiplicative inverse** of x and denote it by x^{-1}. It holds

$$x \cdot x^{-1} = x^{-1} \cdot x = 1$$

3. The operations $+$ and $\cdot$ are related by

- (AM) **Distributive Property**: $\forall\, x, y, z \in K$

$$x \cdot (y + z) = (x \cdot y) + (y \cdot z)\,.$$

Example 3.8

Let K with $+$ and $\cdot$ be as in Example 3.1. We can show that $(K, +, \cdot)$ is a field. Indeed we have already shown in Example 3.5 that:

- (A1) and (M1) hold,
- (A2) holds with neutral element 0,
- (M2) holds with neutral element 1,
- (A3) every element has an additive inverse, with

$$-0 = 0\,, \quad -1 = 1\,,$$

- (M3) every element which is not 0 a multiplicative inverse, with

$$1^{-1} = 1\,.$$

We are left to show the Distributive Property (AM). Indeed:

- (AM) For all $y, z \in K$ we have

$$0 \cdot (y+z) = 0\,, \quad (0 \cdot y) + (0 \cdot z) = 0 + 0 = 0\,,$$

and also

$$1 \cdot (y+z) = y+z\,, \quad (1 \cdot y) + (1 \cdot z) = y+z\,.$$

Thus (AM) holds.

Definition 3.9: Subtraction and division

Let $(K, +, \cdot)$ be a field. We define:

- **Subtraction** as the operation $-$ defined by

$$x - y := x + (-y)\,, \quad \forall\, x, y \in K\,,$$

where $-y$ is the additive inverse of y.
- **Division** as the operation $/$ defined by

$$x/y := x \cdot y^{-1}\,, \quad \forall\, x, y \in K\,,\ y \neq 0\,,$$

where y^{-1} is the multiplicative inverse of y.

Proposition 3.10: Uniqueness of neutral elements and inverses

Let $(K, +, \cdot)$ be a field. Then

1. There is a unique element in K with the property of 0,
2. There is a unique element in K with the property of 1,
3. For all $x \in K$ there is a unique additive inverse $-x$,
4. For all $x \in K$, $x \neq 0$, there is a unique multiplicative inverse x^{-1}.

Proof

1. Suppose that $0 \in K$ and $\tilde{0} \in K$ are both neutral element of $+$, that is, they both satisfy (A2). Then

$$0 + \tilde{0} = 0$$

since $\tilde{0}$ is a neutral element for $+$. Moreover

$$\tilde{0} + 0 = \tilde{0}$$

since 0 is a neutral element for $+$. By commutativity of $+$, see property (A1), we have

$$0 = 0 + \tilde{0} = \tilde{0} + 0 = \tilde{0}\,,$$

showing that $0 = \tilde{0}$. Hence the neutral element for $+$ is unique.

2. Exercise.
3. Let $x \in K$ and suppose that $y, \tilde{y} \in K$ are both additive inverses of x, that is, they both satisfy (A3). Therefore
$$x + y = 0$$
since y is an additive inverse of x and
$$x + \tilde{y} = 0$$
since $\tilde{y}$ is an additive inverse of x. Therefore we can use commutativity and associativity and of $+$, see property (A1), and the fact that 0 is the neutral element of $+$, to infer
$$\begin{aligned} y &= y + 0 = y + (x + \tilde{y}) \\ &= (y + x) + \tilde{y} = (x + y) + \tilde{y} \\ &= 0 + \tilde{y} = \tilde{y}\,, \end{aligned}$$
concluding that $y = \tilde{y}$. Thus there is a unique additive inverse of x, and
$$y = \tilde{y} = -x\,,$$
with $-x$ the element from property (A3).
4. Exercise.

Using the properties of field we can also show that the usual properties of sum, subtraction, multiplication and division still hold in any field. We list such properties in the following proposition.

Proposition 3.11: Properties of field operations

Let $(K, +, \cdot)$ be a field. Then for all $x, y, z \in K$,

- $x + y = x + z \implies y = z$
- $x \cdot y = x \cdot z$ and $x \neq 0 \implies y = z$
- $-0 = 0$
- $1^{-1} = 1$
- $x \cdot 0 = 0$
- $-1 \cdot x = -x$
- $-(-x) = x$
- $(x^{-1})^{-1} = x$ if $x \neq 0$
- $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$

The above properties can be all proven with elementary use of the field properties (A1)-(A3), (M1)-(M3) and (AM). This is an exercise in patience, and is left to the reader.

Let us conclude with examining the sets of numbers introduced in Chapter 1.

Theorem 3.12

Consider the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ with the usual operations $+$ and $\cdot$. We have:

- $(\mathbb{N}, +, \cdot)$ is **not a field**:
  It satisfies properties (A1), (A2), (M1), (M2), (AM) of fields. It is missing properties (A3) and (M3), the additive and multiplicative inverse properties, respectively.
- $(\mathbb{Z}, +, \cdot)$ is **not a field**:
  It satisfies properties (A1), (A2), (A3), (M1), (M2), (AM) of fields. Thus it is only missing (M3), the multiplicative inverse property.
- $(\mathbb{Q}, +, \cdot)$ **is a field**.

The proof is omitted.

3.2 Ordered fields

Definition 3.13

Let K be a set with binary operations $+$ and $\cdot$, and with an order relation $\leq$. We call $(K, +, \cdot, \leq)$ an **ordered field** if:

1. $(K, +, \cdot)$ is a field
2. There $\leq$ is of **total order** on K: $\forall\, x, y, z \in K$
   - (O1) **Reflexivity**:
   $$x \leq x$$
   - (O2) **Antisymmetry**:
   $$x \leq y \text{ and } y \leq x \implies x = y$$
   - (O3) **Transitivity**:
   $$x \leq y \text{ and } y \leq z \implies x = z$$
   - (O4) **Total order**:
   $$x \leq y \text{ or } y \leq x$$
3. The operations $+$ and $\cdot$, and the total order $\leq$, are related by the following properties: $\forall x, y, z \in K$
   - (AM) **Distributive**: Relates addition and multiplication via
   $$x \cdot (y + z) = x \cdot y + x \cdot z$$
   - (AO) Relates addition and order with the requirement:
   $$x \leq y \implies x + z \leq y + z$$
   - (MO) Relates multiplication and order with the requirement:
   $$x \geq 0,\ y \geq 0 \implies x \cdot y \geq 0$$

Example 3.14

$(\mathbb{Q}, +, \cdot, \leq)$ is an **ordered field**.

3.3 Cut Property

We have just introduced the notion of **field**, and noted that the set of rational numbers with the usual operations

$$(\mathbb{Q}, +, \cdot)$$

is a **field**.

We now need to address the key issue we proved in Chapter 1, that is, that

$$\sqrt{2} \notin \mathbb{Q}\,.$$

This means that $\mathbb{Q}$ has **gaps**, and cannot be represented as a **continuous** line. The rigorous definition of **lack of gaps** needs the concept of **cut** of a set.

Definition 3.15: Partition of a set

Let S be a non-empty set. The pair (A, B) is a **partition** of S if

$$A, B \subseteq S, \quad A \neq \emptyset, \quad B \neq \emptyset,$$

and

$$S = A \cup B, \quad A \cap B = \emptyset.$$

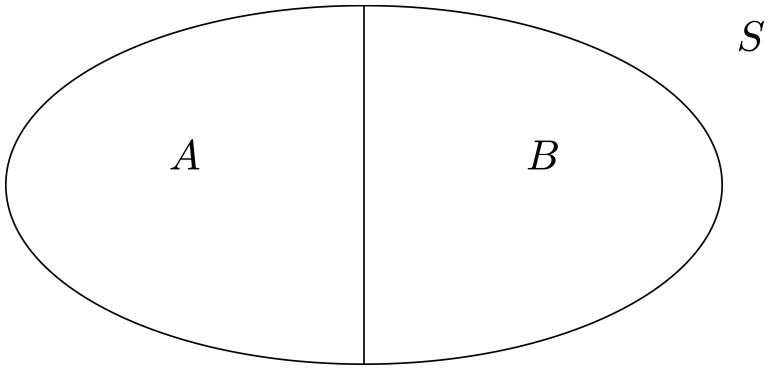

Figure 3.1: Schematic picture of a partition (A, B) of the set K.

Definition 3.16: Cut of a set

Let S be a non-empty set with a total order relation $\leq$. The pair (A, B) is a **cut** of S if

1. (A, B) is a **partition** of S,
2. We have
$$a \leq b, \quad \forall a \in A, \ \forall b \in B.$$

The **cut** of a set is often called **Dedekind cut**, named after **Richard Dedekind**, who used cuts to give an explicit construction of the real numbers $\mathbb{R}$, see Wikipedia page.

Definition 3.17: Cut property

Let S be a non-empty set with a total order relation $\leq$. We say that S has the **cut property** if for every cut (A, B) of S there exists some $s \in S$ such that

$$a \leq s \leq b, \quad \forall a \in A, \ \forall b \in B.$$

We call s the **separator** of the cut (A, B).

Example 3.18

Let $S = \mathbb{Q}$ and consider the sets

$$A = (-\infty, s] \cap \mathbb{Q}\,, \quad B = (s, \infty) \cap \mathbb{Q}\,.$$

for some $s \in \mathbb{Q}$. Then the pair (A, B) is a cut of $\mathbb{Q}$, and s is the separator.

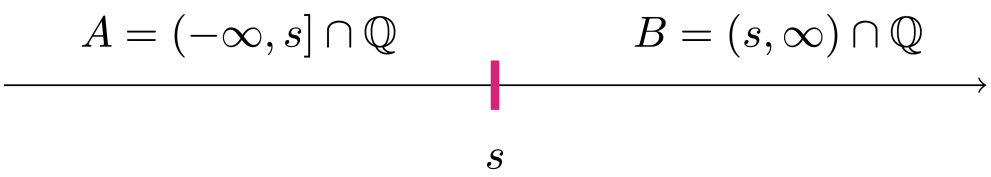

Figure 3.2: (A, B) is a cut of $\mathbb{Q}$ with separator s.

Question 3.19

Do all ordered fields have the Cut Property? Does $\mathbb{Q}$ have the Cut Property?

The answer to the above question is **NO**. For example the pair

$$A = (-\infty, \sqrt{2}) \cap \mathbb{Q}\,, \quad B = (\sqrt{2}, \infty) \cap \mathbb{Q}\,. \tag{3.1}$$

is a cut of $\mathbb{Q}$, since $\sqrt{2} \notin \mathbb{Q}$. However what is the separator? It should be $s = \sqrt{2}$, given that clearly

$$a \leq \sqrt{2} \leq b\,, \quad \forall\, a \in A\,,\ \forall\, b \in B\,.$$

However $\sqrt{2} \notin \mathbb{Q}$, so we are **NOT ALLOWED** to take it as separator. Indeed, we can show that (A, B) defined as in (3.1) has no separator.

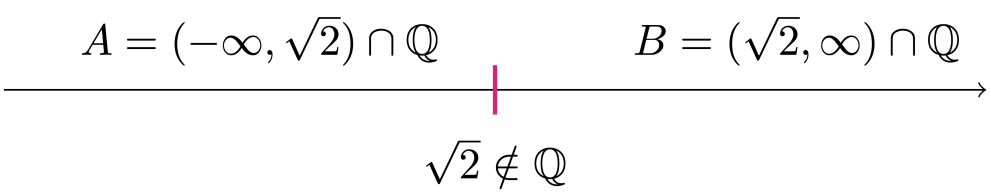

Figure 3.3: (A, B) is a cut of $\mathbb{Q}$ which has no separator

Theorem 3.20: $\mathbb{Q}$ does not have the cut property.

$\mathbb{Q}$ does not have the cut property. More explicitly, there exist a cut (A, B) of $\mathbb{Q}$ which has no separator.

Remark 3.21: Ideas for the proof of Theorem 3.20

Before proceeding with the proof, let us summarize the ideas behind it:
We will consider the cut (A, B) in (3.1). We then assume by contradiction that (A, B) admits a separator $L \in \mathbb{Q}$, so that

$$a \leq L \leq b\,, \quad \forall\, a \in A\,,\ \forall\, b \in B\,. \tag{3.2}$$

Since (A, B) is a partition of $\mathbb{Q}$, then either $L \in A$ or $L \in B$. These will both lead to a contradiction:

- If $L \in A$, by definition of A we have
$$L < \sqrt{2}\,.$$
We want to contradict the fact that L is a separator for the cut (A, B). The idea is that $\sqrt{2} \notin \mathbb{Q}$, and therefore it is possible to find a rational number $\tilde{L}$ such that
$$L < \tilde{L} < \sqrt{2}\,.$$
How do we find such $\tilde{L}$ in practice? We look for a number $\tilde{L}_n$ of the form
$$\tilde{L}_n = 1 + \frac{1}{n}$$
for some $n \in \mathbb{N}$ to be suitably chosen later. Clearly $\tilde{L}_n \in \mathbb{Q}$ and
$$L < \tilde{L}_n$$
for all $n \in \mathbb{N}$. We need to prove that we can find $n_0 \in \mathbb{N}$ such that
$$L < \tilde{L}_{n_0} < \sqrt{2}\,. \tag{3.3}$$
This is indeed possible: There exists $n_0 \in \mathbb{N}$ such that (3.3) holds. From (3.3) we see that $\tilde{L}_{n_0} \in A$. Since L is a separator, from (3.2) we obtain
$$\tilde{L}_{n_0} \leq L\,,$$
which contradicts (3.3).
- If $L \in B$, by definition of B we have
$$\sqrt{2} < L\,.$$
The idea is the same as above: Since $\sqrt{2} \notin \mathbb{Q}$, we can find $\tilde{L} \in \mathbb{Q}$ such that
$$\sqrt{2} < \tilde{L} < L\,.$$

Since we want $\tilde{L}$ to be a rational number smaller than L, we look for $\tilde{L}$ of the form

$$\tilde{L}_n := L - \frac{1}{n},$$

for a suitable $n \in \mathbb{N}$. This satisfies $\tilde{L}_n \in \mathbb{Q}$ and

$$\tilde{L}_n < L,$$

for all $n \in \mathbb{N}$. We then find $n_0 \in \mathbb{N}$ such that

$$\sqrt{2} < \tilde{L}_{n_0} < L. \tag{3.4}$$

The above shows that $\tilde{L}_{n_0} \in B$. As L is a separator, we find that

$$L \leq \tilde{L}_{n_0},$$

which contradicts (3.4).

Therefore, both cases $L \in A$ or $L \in B$ lead to a contradiction. Since these are all the possibilities, we conclude that the cut (A, B) has no separator in $\mathbb{Q}$.

Time to make the ideas in the above remark rigorous.

Proof: Proof of Theorem 3.20

Let A and B be the sets defined in (3.1). It is useful to rewrite A and B in the form

$$A = A_1 \cup A_2,$$

where

$$A_1 = \{q \in \mathbb{Q} : \ q < 0\},$$
$$A_2 = \{q \in \mathbb{Q} : \ q \geq 0, \ q^2 < 2\},$$

and

$$B = \{q \in \mathbb{Q} : \ q > 0, \ q^2 > 2\}.$$

Step 1. (A, B) *is a cut of* $\mathbb{Q}$:
We need to prove the following:

1. (A, B) is a partition of $\mathbb{Q}$. This is because $A, B \subseteq \mathbb{Q}$ with $A \neq \emptyset$ and $B \neq \emptyset$. Moreover $A \cap B = \emptyset$ and

   $$A \cup B = \mathbb{Q},$$

   given that $\sqrt{2} \notin \mathbb{Q}$, and so there is no element $q \in \mathbb{Q}$ such that $q^2 = 2$.

2. It holds
$$a \leq b\,, \quad \forall a \in A\,,\ \forall b \in B\,.$$
Indeed, suppose that $a \in A$ and $b \in B$. We have two cases:
   - $a \in A_1$: Therefore $a < 0$. In particular
   $$a < 0 < b\,,$$
   given that $b > 0$ for all $b \in B$. Thus $a < b$.
   - $a \in A_2$: Therefore $a \geq 0$ and $a^2 < 2$. In particular
   $$a^2 < 2 < b^2\,,$$
   since $b^2 > 2$ for all $b \in B$. In particular
   $$a^2 < b^2\,.$$
   Since $b > 0$ for all $b \in B$, from the above inequality we infer $a < b$, concluding.

Step 2. (A, B) *has no separator*:
Suppose by contradiction that (A, B) admits a separator
$$L \in \mathbb{Q}\,.$$
By definition this means
$$a \leq L \leq b\,, \quad \forall a \in A\,,\ \forall b \in B\,. \tag{3.5}$$
Since
$$L \in \mathbb{Q}\,, \quad \mathbb{Q} = A \cup B\,, \quad A \cap B = \emptyset\,,$$
then either $L \in A$ or $L \in B$. We will see that both these possibilities lead to a contradiction:
Case 1: $L \in A$.
By (3.5) we know that
$$a \leq L\,, \quad \forall\, a \in A\,. \tag{3.6}$$
In particular the above implies
$$L \geq 0 \tag{3.7}$$
since $0 \in A$. Therefore we must have $L \in A_2$, that is,
$$L \geq 0 \ \text{ and } \ L^2 < 2\,. \tag{3.8}$$
Set
$$\tilde{L} := L + \frac{1}{n}$$
for $n \in \mathbb{N}$, $n \neq 0$ to be chosen later. Clearly we have
$$\tilde{L} \in \mathbb{Q} \ \text{ and } \ L < \tilde{L}\,. \tag{3.9}$$

From (3.7) and (3.9) we have also

$$\tilde{L} > 0\,. \tag{3.10}$$

We now want to show that there is a choice of n such that $\tilde{L}^2 < 2$, which will lead to a contradiction. Indeed, we can estimate

$$\begin{aligned}\tilde{L}^2 &= \left(L + \frac{1}{n}\right)^2 \\ &= L^2 + \frac{1}{n^2} + 2\frac{L}{n} \\ &< L^2 + \frac{1}{n} + 2\frac{L}{n} \qquad \left(\text{using } \frac{1}{n} < \frac{1}{n^2}\right) \\ &= L^2 + \frac{2L+1}{n}\,.\end{aligned}$$

If we now impose that

$$L^2 + \frac{2L+1}{n} < 2\,,$$

we can rearrange the above and obtain

$$n(2 - L^2) > 2L + 1\,.$$

Now note that $L^2 < 2$ by assumption (3.8). Thus we can divived by $(2 - L^2)$ and obtain

$$n > \frac{2L+1}{2-L^2}\,.$$

Therefore we have just shown that

$$n > \frac{2L+1}{2-L^2} \implies \tilde{L}^2 < 2\,.$$

Together with (3.10) this implies $\tilde{L} \in A$. Therefore we have

$$\tilde{L} \leq L$$

by (3.6). On the other hand it also holds

$$\tilde{L} > L$$

by (3.9), and therefore we have a contradiction. Thus $L \notin A$.
Case 2: $L \in B$.
As $L \in B$, we have by definition

$$L > 0\,, \quad L^2 > 2\,. \tag{3.11}$$

Moreover since L is a separator, see (3.5), in particular

$$L \leq b\,,\ \forall\, b \in B\,. \tag{3.12}$$

Define now

$$\tilde{L} := L - \frac{1}{n}$$

with $n \in \mathbb{N}$, $n \neq 0$ to be chosen later. Clearly we have

$$\tilde{L} \in \mathbb{Q}\,, \quad \tilde{L} < L\,. \tag{3.13}$$

We now show that n can be chosen so that $\tilde{L} \in B$. Indeed

$$\begin{aligned}
\tilde{L}^2 &= \left(L - \frac{1}{n}\right)^2 \\
&= L^2 + \frac{1}{n^2} - 2\frac{L}{n} \\
&> L^2 - \frac{1}{n^2} - 2\frac{L}{n} \qquad \left(\text{using } \frac{1}{n^2} > -\frac{1}{n^2}\right) \\
&> L^2 - \frac{1}{n} - 2\frac{L}{n} \qquad \left(\text{using } -\frac{1}{n^2} > -\frac{1}{n}\right) \\
&= L^2 - \frac{1+2L}{n}\,.
\end{aligned}$$

Now we impose

$$L^2 - \frac{1+2L}{n} > 2$$

which is equivalent to

$$n(L^2 - 2) > 1 + 2L\,.$$

Since we are assuming $L \in B$, then $L^2 > 2$, see (3.11). Therefore we can divide by $(L^2 - 2)$ and get

$$n > \frac{1+2L}{L^2-2}\,.$$

In total, we have just shown that

$$n > \frac{1+2L}{L^2-2} \quad \Longrightarrow \quad \tilde{L}^2 > 2\,,$$

proving that $\tilde{L} \in B$. Therefore by (3.12) we get

$$L \leq \tilde{L}\,.$$

This contradicts (3.13).
Conclusion:
We have seen that assuming that (A, B) has a separator $L \in \mathbb{Q}$ leads to a contradiction. Thus the cut (A, B) has no separator.

Remark 3.22

The above proof can be summarized by saying that the set

$$A = (-\infty, \sqrt{2}) \cap \mathbb{Q}$$

does not admit a **largest** element in $\mathbb{Q}$, and that the set

$$B = (\sqrt{2}, \infty) \cap \mathbb{Q}$$

does not admit a **lowest element** in $\mathbb{Q}$. We will clarify this remark in the next section.

3.4 Supremum and infimum

A crucial definition in Analysis is the one of supremum or infimum of a set. This is also another way of studying the **gaps** of $\mathbb{Q}$.

Example 3.23: Intuition about supremum and infimum

Consider the set

$$A = [0, 1) \cap \mathbb{Q}\,.$$

Intuitively, we understand that A is bounded, i.e. not infinite. We also see that

- 0 is the lowest element of A
- 1 is the highest element of A

However we see that $0 \in A$ while $1 \notin A$. We will see that

- 0 can be defined as the **infimum** and **minimum** of A.
- 1 can be defined as the **supremum**, but not **maximum**, of A.

3.4.1 Upper bound, supremum, maximum

We start by defining the supremum. First we need the notion of upper bound of a set.

Definition 3.24: Upper bound and bounded above

Let $(K, +, \cdot, \leq)$ be an ordered field and $A \subseteq K$:

1. We say that $b \in K$ is an **upper bound** for A if
$$a \leq b\,, \quad \forall\, a \in A\,.$$
2. We say that A is **bounded above** if there exists and upper bound $b \in K$ for A.

Definition 3.25: Supremum

Let $(K, +, \cdot, \leq)$ be an ordered field and $A \subseteq K$. A number $s \in K$ is called **least upper bound** or **supremum** of A if:

i. s is an upper bound for A,
ii. s is the smallest upper bound of A, that is,

$$\text{If } b \in K \text{ is upper bound for } A \text{ then } s \leq b\,.$$

Notation 3.26

We will almost always prefer the name supremum to least upper bound. For $A \subseteq K$ the supremum is denoted by

$$s := \sup A\,.$$

Remark 3.27

Note that if a set $A \subseteq K$ in **NOT** bounded above, then the supremum does not exist, as there are no upper bounds of A.

Proposition 3.28

Let $(K, +, \cdot, \leq)$ be an ordered field and $A \subseteq K$. If

$$\sup A$$

exists, then it is unique.

Proof

Suppose there exist $s_1, s_2 \in K$ such that

$$s_1 = \sup A,\ \ s_2 = \sup A\,.$$

Then:

- Since $s_2 = \sup A$, in particular s_2 is an upper bound for A. Since $s_1 = \sup A$ then s_1 is the lowest upper bound. Thus we get

$$s_1 \leq s_2\,.$$

- Exchanging the roles s_1 and s_2 in the above reasoning we also get

$$s_2 \leq s_1 .$$

This shows $s_1 = s_2$.

Warning

In general:

- A set can have infinite upper bounds,
- The supremum does not belong to the set.

For example

$$A = [0, 1) \cap \mathbb{Q}$$

has for upper bounds all the numbers $b \in \mathbb{Q}$ with $b > 1$. Moreover one can show that

$$\sup A = 1 ,$$

and so

$$\sup A \notin A .$$

Warning

The supremum does not exist in general. For example let

$$A = [0, \sqrt{2}) \cap \mathbb{Q} .$$

We will show that $\sup A$ does not exist in $\mathbb{Q}$. Indeed we will have that

$$\sup A = \sqrt{2} \in \mathbb{R} .$$

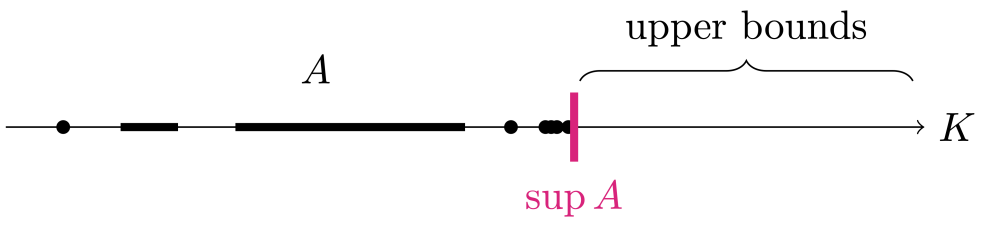

Figure 3.4: Supremum and upper bounds of a set A in the field K

Definition 3.29: Maximum

Let $(K, +, \cdot, \leq)$ be an ordered field and $A \subseteq K$. A number $M \in K$ is called the **maximum** of A if:

$$M \in A \quad \text{and} \quad a \leq M\,, \forall a \in A\,.$$

We denote the maximum by

$$M = \max A\,.$$

Proposition 3.30

Let $(K, +, \cdot, \leq)$ be an ordered field and $A \subseteq K$. If the maximum of A exists, then also the supremum exists, and

$$\sup A = \max A\,.$$

Proof

Let

$$M = \max A\,.$$

Then:

- By definition we have $M \in A$ and
$$a \leq M\,, \quad \forall\, a \in A\,.$$
In particular the above tells us that M is an upper bound of A.
- We claim that M is the least upper bound. Indeed, suppose b is an upper bound of A, that is,
$$a \leq b\,, \quad \forall\, a \in A\,.$$
In particular, since $M \in A$, by the above condition we have
$$M \leq b\,.$$

Therefore M is the least upper bound of A, meaning that $M = \sup A$.

Warning

The converse of the above statement is not true: In general the sup might exist while the max does not.

For example

$$A = [0, 1) \cap \mathbb{Q}$$

is such that

$$\sup A = 1$$

but $\max A$ does not exist. Instead for the set

$$B = [0, 1] \cap \mathbb{Q}$$

we have that

$$\max A = \sup A = 1\,.$$

3.4.2 Lower bound, infimum, minimum

We now introduce the definitions of lower bound, infimum, minimum. These are the counterpart of upper bound, supremum and maximum, respectively.

Definition 3.31: Upper bound, bounded below, infimum, minimum

Let $(K, +, \cdot, \leq)$ be an ordered field and $A \subseteq K$:

1. We say that $l \in K$ is a **lower bound** for A if

$$l \leq a\,, \quad \forall\, a \in A\,.$$

2. We say that A is **bounded below** if there exists a lower bound $l \in K$ for A.

3. We say that $i \in K$ is the **greatest lower bound** or **infimum** of A if:

   - i is a lower bound for A,
   - i is the largest lower bound of A, that is,

   $$\text{If } l \in K \text{ is a lower bound for } A \text{ then } l \leq i\,.$$

   If it exists, the infimum is denoted by

   $$i = \inf A\,.$$

4. We say that $m \in K$ is the **minimum** of A if:

   $$m \in A \text{ and } m \leq a\,,\ \forall a \in A\,.$$

   If it exists, we denote the minimum by

   $$m = \min A\,.$$

Figure 3.5: Infimum and lower bounds of a set A in the field K

Proposition 3.32

Let $(K, +, \cdot, \leq)$ be an ordered field and $A \subseteq K$:

1. If $\inf A$ exists, then it is unique.
2. If the minimum of A exists, then also the infimum exists, and

$$\inf A = \min A\,.$$

The proof uses similar arguments to the one employed in the previous section, and is left to the reader as an exercise.

Warning

We have

- A set can have infinite lower bounds,
- The infimum does not belong to the set.

For example

$$A = (0, 1) \cap \mathbb{Q}$$

has for lower bounds all the numbers $b \in \mathbb{Q}$ with $b < 1$. Moreover we will show that

$$\inf A = 0\,,$$

and so

$$\inf A \notin A\,.$$

Warning

The infimum does not exist in general. For example let

$$A = (\sqrt{2}, 5] \cap \mathbb{Q}\,.$$

We will show that $\inf A$ does not exist in $\mathbb{Q}$. Indeed we will have that

$$\inf A = \sqrt{2} \in \mathbb{R}\,.$$

Warning

In general the inf might exist while the min does not. For example

$$A = (0,1) \cap \mathbb{Q}$$

is such that

$$\inf A = 0$$

but $\min A$ does not exist. Instead for the set

$$B = [0,1] \cap \mathbb{Q}$$

we have that

$$\inf A = \min A = 0\,.$$

Proposition 3.33

Let $(K, +, \cdot, \leq)$ be an ordered field and $A \subseteq K$. If $\inf A$ and $\sup A$ exist, then

$$\inf A \leq a \leq \sup A\,, \quad \forall a \in A\,.$$

The proof is simple, and is left as an exercise. We now have a complete picture about supremum and infimum, see figure below.

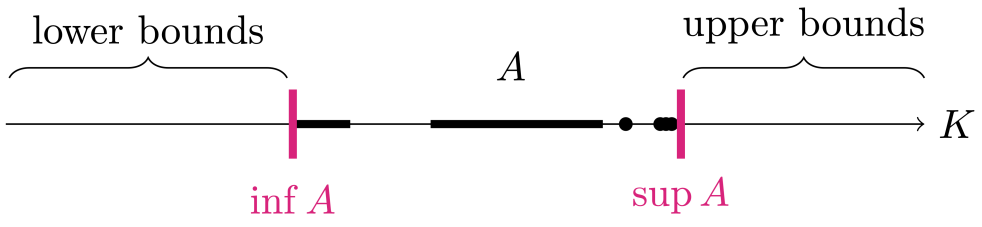

Figure 3.6: Supremum, upper bounds, infimum and lower bounds of a set A in K

We conclude with another simple proposition. The proof is again left to the reader.

Proposition 3.34: Relationship between sup and inf

Let $(K, +, \cdot, \leq)$ be an ordered field and $A \subseteq K$. Define

$$-A := \{-a : a \in A\}.$$

It holds:

- If $\sup A$ exists, then $\inf A$ exists and
$$\inf(-A) = -\sup A.$$
- If $\inf A$ exists, then $\sup A$ exists and
$$\sup(-A) = -\inf A.$$

3.5 Completeness

We have introduced the concepts of supremum and infimum on an ordered field K.

Question 3.35

Suppose $(K, +, \cdot, \leq)$ is an ordered field, and that $A \subseteq K$ is non-empty and bounded above. Does

$$\sup A$$

always exist?

The answer to the above question is **NO**. Like we did with the Cut Property, the counterexample can be found in the set of rational numbers $\mathbb{Q}$. A set bounded above for which the supremum does nor exist is, for example,

$$A = [0, \sqrt{2}) \cap \mathbb{Q}. \tag{3.14}$$

Theorem 3.36

There exists a set $A \subseteq \mathbb{Q}$ such that

- A is non-empty,
- A is bounded above,
- $\sup A$ does not exist in $\mathbb{Q}$.

The proof uses the same ideas we used for showing that $\mathbb{Q}$ does not have the Cut Property.

Proof

Define the set A as in (3.14). Equivalently, this can be written as

$$A = \{q \in \mathbb{Q} : \ q \geq 0\,,\ q^2 < 2\}\,.$$

Step 1. A is bounded above.
Take $b := 9$. Then b is an upper bound for A. Indeed by definition

$$q^2 < 2\,,\ q \geq 0\,,\ \ \forall q \in A\,.$$

Therefore

$$q^2 < 2 < 9 \implies q^2 < 9 \implies q < 3 = b\,.$$

Step 2. $\sup A$ *does not exist.*
Assume by contradiction that

$$s = \sup A \in \mathbb{Q}$$

exists. By definition it holds

$$s \geq q\,, \quad \forall\, q \in A \tag{3.15}$$

$$b \geq q\,, \forall\, q \in A \implies s \leq b \tag{3.16}$$

There are two possibilities: $s \in A$ or $s \notin A$:

- *Case 1.* $s \in A$.
  If $s \in A$ by definition

  $$s \geq 0\,, \quad s^2 < 2\,. \tag{3.17}$$

  Define

  $$\tilde{s} := s + \frac{1}{n}$$

  with $n \in \mathbb{N}$, $n \neq 0$ to be chosen later. Then

  $$\begin{aligned}\tilde{s}^2 &= \left(s + \frac{1}{n}\right)^2 \\ &= s^2 + \frac{1}{n^2} + 2\frac{s}{n} \\ &< s^2 + \frac{1}{n} + 2\frac{s}{n} \qquad \left(\text{using } \frac{1}{n} < \frac{1}{n^2}\right) \\ &= s^2 + \frac{2s+1}{n}\,.\end{aligned}$$

  If we now impose that

  $$s^2 + \frac{2s+1}{n} < 2\,,$$

  we can rearrange the above and obtain

  $$n(2 - s^2) > 2s + 1\,.$$

Now note that $s^2 < 2$ by assumption (3.17). Thus we can divide by $(2 - s^2)$ and obtain

$$n > \frac{2s+1}{2-s^2}\,.$$

To summarize, we have just shown that

$$n > \frac{2s+1}{2-s^2} \implies \tilde{s}^2 < 2\,.$$

Moreover $\tilde{s} := (s + 1/n) \in \mathbb{Q}$. Therefore

$$\tilde{s} \in A\,.$$

Since $s = \sup A$, we then have

$$\tilde{s} \leq s\,.$$

However

$$\tilde{s} := s + \frac{1}{n} > s\,,$$

yielding a contradiction. Thus $s \in A$ is not possible.

- *Case 2.* $s \notin A$.
  If $s \notin A$, by the fact that $s = \sup A$ and by definition of A we get

$$s > 0\,, \quad s^2 > 2\,. \tag{3.18}$$

Define

$$\tilde{s} := s - \frac{1}{n}\,.$$

We have

$$\begin{aligned}
\tilde{s}^2 &= \left(s - \frac{1}{n}\right)^2 \\
&= s^2 + \frac{1}{n^2} - 2\frac{s}{n} \\
&> s^2 - \frac{1}{n^2} - 2\frac{s}{n} \qquad \left(\text{using } \frac{1}{n^2} > -\frac{1}{n^2}\right) \\
&> s^2 - \frac{1}{n} - 2\frac{s}{n} \qquad \left(\text{using } -\frac{1}{n^2} > -\frac{1}{n}\right) \\
&= s^2 - \frac{1+2s}{n}\,.
\end{aligned}$$

Now we impose

$$s^2 - \frac{1+2s}{n} > 2$$

which is equivalent to

$$n(s^2 - 2) > 1 + 2s\,.$$

By (3.18) we have $s^2 > 2$. Therefore we can divide by $(s^2 - 2)$ and get

$$n > \frac{1 + 2s}{s^2 - 2}\,.$$

In total, we have just shown that

$$n > \frac{1 + 2s}{s^2 - 2} \quad \Longrightarrow \quad \tilde{s}^2 > 2\,.$$

Therefore $\tilde{s} \notin A$, and by definition of A we have

$$\tilde{s} \geq q\,, \quad \forall q \in A\,.$$

Moreover $\tilde{s} := (s - 1/n) \in \mathbb{Q}$. Therefore $\tilde{s}$ is an upper bound of A in $\mathbb{Q}$. Since $s = \sup A$ is the smallest upper bound, see (3.16), it follows

$$s \leq \tilde{s}\,.$$

However

$$\tilde{s} := s - \frac{1}{n} < s\,,$$

obtaining a contradiction. Then $s \notin A$.

Conclusion.
We have assumed by contradiction that $s = \sup A$ exists in $\mathbb{Q}$. In this case either $s \in A$ or $s \notin A$. In both cases we found a contradiction. Therefore $\sup A$ does not exist.

The above theorem shows that the supremum does not necessarily exist. What about the infimum?

Question 3.37

Suppose $(K, +, \cdot, \leq)$ is an ordered field, and that $A \subseteq K$ is non-empty and bounded below. Does

$$\inf A$$

always exist?

The answer to the above question is again **NO**. A set bounded below for which the infimum does nor exist is, for example,

$$A = (\sqrt{2}, 10] \cap \mathbb{Q}\,.$$

The proof of this fact is, of course, very similar to the one of Theorem 3.36, and is therefore omitted.

Thus infimum and supremum do not exist in general. The fields for which all the bounded sets admit supremum or infimum are called **complete**.

Definition 3.38: Completeness

Let $(K, +, \cdot, \leq)$ be an ordered field. We say that K is **complete** if it holds the property:

- (AC) For every $A \subseteq K$ non-empty and bounded above

$$\sup A \in K\,.$$

Notation 3.39

We have that:

- Property (AC) is called **Axiom of Completeness**
- If K is an ordered field in which (AC) holds, then K is called a **complete ordered field**

Notice that if the **Axiom of Completeness** holds, then also the infimum exists. This is shown in the following proposition.

Proposition 3.40

Let $(K, +, \cdot, \leq)$ be a complete ordered field. Suppose that $A \subseteq K$ is non-empty and bounded below. Then

$$\inf A \in K\,.$$

Proof

Suppose that $A \subseteq K$ is non-empty and bounded below. Then

$$-A := \{-a : \ a \in A\}$$

is non-empty and bounded above. By completeness we have that $\sup(-A)$ exists in K. But then Proposition 3.34 implies that $\inf A$ exists in K, with

$$\inf A = -\sup(-A)\,.$$

3.6 Equivalence of Completeness and Cut Property

We can show that **Completeness** is equivalent to the **Cut Property**. Such result is not essential, but its proof is very instructive.

Theorem 3.41: Equivalence of Cut Property and Completeness

Let $(K, +, \cdot, \leq)$ be an ordered field. Then they are equivalent:

1. K has the **Cut Property**
2. K is **Complete**

Remark 3.42: Ideas for proving Theorem 3.41

The proof of Theorem 3.41 is rather long, but the ideas are simple:
Step 1. Cut Property $\implies$ *Completeness.* Suppose K has the Cut Property. To prove that K is Complete, we need to:

- Consider an arbitrary set $A \subseteq K$ such that $A \neq \emptyset$ and A is bounded above.
- Show that A has a supremum.

To achieve this, consider the set

$$B := \{b \in K \,:\, b \geq a\,,\ \forall a \in A\}\,,$$

which is the set of Upper Bounds of A. We can show that the pair

$$(B^c, B)$$

is a Cut of K. As K has the Cut Property, then there exists $s \in K$ separator of (B^c, B). We will show that the separator s is the supremum of A

$$s = \sup A\,.$$

Thus K is complete. See Figure 3.7 for a schematic picture of the above construction.
Step 2. Completeness $\implies$ *Cut Property.* Conversely, suppose that K is Complete. To prove that K has the Cut Property, we need to:

- Consider a cut (A, B) of K.
- Show that (A, B) has a separator $s \in K$.

This implication is easier. Indeed, since A is non-empty and bounded above, by Completeness there exists

$$\sup A \in K\,.$$

We will show that

$$s := \sup A$$

is a separator for the cut (A, B). See Figure 3.8 for a schematic picture of the above construction.

Keeping the above ideas in mind, let us proceed with the proof.

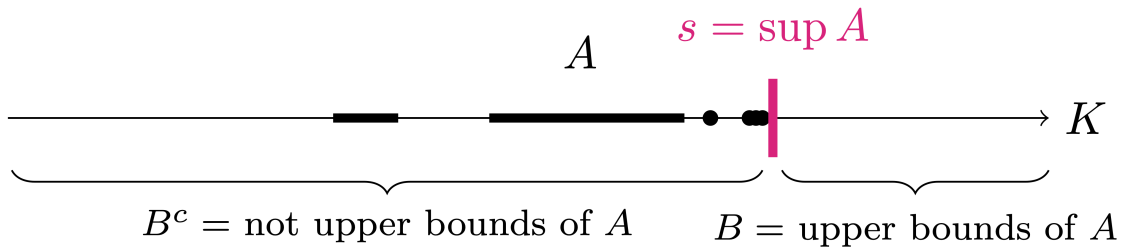

Figure 3.7: Let s be the separator of the cut (B^c, B), with B the set of upper bounds of A. Then $s = \sup A$.

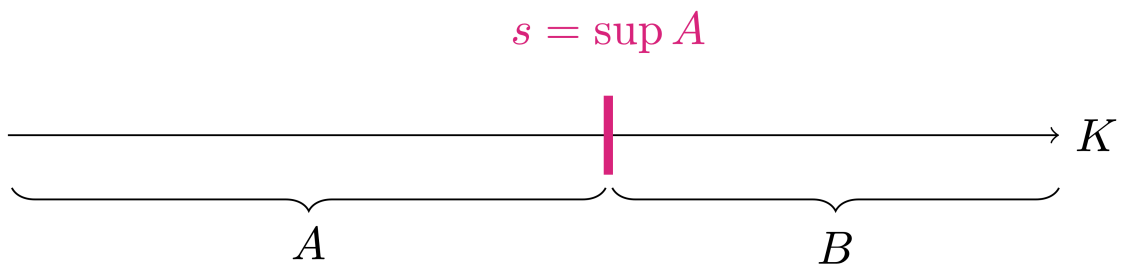

Figure 3.8: Let (A, B) be a cut of K and let $s = \sup A$. Then s is the separator of the cut (A, B).

Proof: Proof of Theorem 3.41

Step 1. Cut Property $\Longrightarrow$ Completeness.
We need to prove that K is complete. To this end, consider $A \subseteq K$ non-empty and bounded above. Define the set of upper bounds of A:

$$B := \{b \in K \,:\, b \geq a\,,\ \forall a \in A\}\,.$$

Claim. The pair (B^c, B) is a cut of K.
Proof of Claim. We have to prove two points:

- (B^c, B) forms a partition of K.

  Indeed, we have $B \neq \emptyset$, since A is bounded above. Further, we have $B^c \neq \emptyset$, since A is non-empty. Thus

  $$K = B^c \cup B\,, \quad B^c \cap B = \emptyset\,.$$

  Then (B^c, B) is a partition of K.

- We have

  $$x \leq y\,, \quad \forall\, x \in B^c\,, \forall\, y \in B\,. \tag{3.19}$$

  To show the above, let $x \in B^c$ and $y \in B$. By definition of B we have that elements of B^c are not upper bounds of A. Therefore x is not an upper bound. This means there exists $\tilde{a} \in A$ which is larger than x, that is,

  $$x \leq \tilde{a}\,.$$

Since $y \in B$, then y is an upper bound for A, so that

$$a \leq y\,,\ \forall a \in A\,.$$

Therefore

$$x \leq \tilde{a} \leq y\,,$$

concluding (3.19).

Thus (B^c, B) is a cut of K and the claim is proven.
Since (B^c, B) is a cut of K, by the Cut Property there exists a separator $s \in K$ such that

$$x \leq s \leq y\,, \quad \forall\, x \in B^c\,, \forall\, y \in B\,. \tag{3.20}$$

Claim. s is an upper bound for A.
Proof of Claim.
Suppose by contradiction that s is not an upper bound for A. Therefore by definition of upper bound, there exists $\tilde{a} \in A$ such that

$$s < \tilde{a}\,.$$

Consider the mid-point between s and $\tilde{a}$, that is,

$$m := \frac{s+\tilde{a}}{2} \in K\,.$$

Since m is the mid-point between s and $\tilde{a}$, and $s < \tilde{a}$, it holds

$$s < m < \tilde{a}\,.$$

Indeed, since $s < \tilde{a}$ then

$$s = \frac{2s}{2} < \frac{s+\tilde{a}}{2} < \frac{2\tilde{a}}{2} = \tilde{a}\,.$$

In particular the above tells us that m is not an upper bound for A, given that $\tilde{a} \in A$ and $m < \tilde{a}$. Therefore $m \in B^c$, by definition of B^c. Therefore(3.20) implies

$$m \leq s\,,$$

which contradicts $s < m$. Hence s is an upper bound of A, concluding the proof of Claim.
Conclusion. We have shown that s is an upper bound of A. Condition
(3.20) tells us that

$$s \leq y\,,\ \forall y \in B\,.$$

Recalling that B is the set of upper bounds of A, this means that s is the smallest upper bound of A, that is,

$$s = \sup A \in K\,.$$

Step 2. Completeness $\implies$ Cut Property.
Suppose K is complete. We need to show that K has the Cut Property. Therefore assume (A, B) is a cut of K, that is,

$$\begin{aligned} A \neq \emptyset, \quad & B \neq \emptyset, \\ K = A \cup B, \quad & A \cap B = \emptyset, \\ a \leq b, \quad & \forall a \in A, \ \forall b \in B. \end{aligned} \tag{3.21}$$

Since $B \neq \emptyset$, from (3.21) it follows that A is bounded above: indeed, every element of B is an upper bound for A, thanks to (3.21). Since $A \neq \emptyset$, by the Axiom of Completeness we have

$$s = \sup A \in K.$$

In particular, by definition of supremum, we have

$$a \leq s, \ \forall a \in A.$$

Let now $b \in B$ be arbitrary. From (3.21) we have that

$$a \leq b, \ \forall a \in A. \tag{3.22}$$

Therefore b is an upper bound of A. Since $s = \sup A$, we have that s is the smallest upper bound, and so

$$s \leq b.$$

Given that $b \in B$ was arbitrary, it actually holds

$$s \leq b, \ \forall b \in B. \tag{3.23}$$

From (3.22) and (3.23) we therefore have

$$a \leq s \leq b, \ \forall a \in A, \forall b \in B,$$

showing that s is a separator of (A, B). Thus K has the Cut Property.

3.7 Axioms of Real Numbers

We now have all the key elements to introduce the Real Numbers $\mathbb{R}$. These ingredients are:

- Definition of **ordered field**,
- The **Cut Property** or **Axiom of Completeness**.

The definition of $\mathbb{R}$ is given in an axiomatic way.

Definition 3.43: System of Real Numbers $\mathbb{R}$

A system of Real Numbers is a set $\mathbb{R}$ satisfying the following properties:

1. There is an operation $+$ of **addition** on $\mathbb{R}$

$$+ : \mathbb{R}\times\mathbb{R}\to\mathbb{R}, \quad (x,y)\mapsto x+y$$

The addition satisifes: $\forall\, x,y,z\in\mathbb{R}$

- (A1) **Commutativity and Associativity**:

$$x+y=y+x$$

$$(x+y)+z=x+(y+z)$$

- (A2) **Additive Identity**: $\exists\, 0\in\mathbb{R}$ s.t.

$$x+0=0+x=x$$

- (A3) **Additive Inverse**: $\exists\,(-x)\in\mathbb{R}$ s.t.

$$x+(-x)=(-x)+x=0$$

2. There is an operation $\cdot$ of **multiplication** on $\mathbb{R}$

$$\cdot : \mathbb{R}\times\mathbb{R}\to\mathbb{R}, \quad (x,y)\mapsto x\cdot y=xy$$

The multiplication satisifes: $\forall\, x,y,z\in\mathbb{R}$

- (M1) **Commutativity and Associativity**:

$$x\cdot y=y\cdot x$$

$$(x\cdot y)\cdot z=x\cdot(y\cdot z)$$

- (M2) **Multiplicative Identity**: $\exists\, 1\in\mathbb{R}$ s.t.

$$x\cdot 1=1\cdot x=x$$

- (M3) **Multiplicative Inverse**: If $x\neq 0$, $\exists\, x^{-1}\in\mathbb{R}$ s.t.

$$x\cdot x^{-1}=x^{-1}\cdot x=1$$

3. There is a relation $\leq$ of **total order** on $\mathbb{R}$. The order satisfies: $\forall\, x,y,z\in\mathbb{R}$

- (O1) **Reflexivity**:

$$x\leq x$$

- (O2) **Antisymmetry**:

$$x\leq y \text{ and } y\leq x \implies x=y$$

- (O_3) **Transitivity**:
$$x \leq y \text{ and } y \leq z \implies x = z$$
- (O_4) **Total order**:
$$x \leq y \text{ or } y \leq x$$

4. The operations $+$ and $\cdot$, and the total order $\leq$, are related by the following properties: $\forall x, y, z \in \mathbb{R}$
   - (AM) **Distributive**: Relates addition and multiplication via
   $$x \cdot (y + z) = x \cdot y + x \cdot z$$
   - (AO) Relates addition and order with the requirement:
   $$x \leq y \implies x + z \leq y + z$$
   - (MO) Relates multiplication and order with the requirement:
   $$x \geq 0,\ y \geq 0 \implies x \cdot y \geq 0$$
5. **Cut Property** holds:
   - (CP) Every cut (A, B) of $\mathbb{R}$ admits a **separator** $s \in \mathbb{R}$ s.t.
   $$a \leq s \leq b, \quad \forall a \in A, \forall b \in B$$

Remark 3.44

Since **Cut Property** and **Axiom of Completeness** are equivalent by Theorem 3.41, one can replace the Cut Property in Definition 3.43 Point 5 with:

5. **Axiom of Completeness** holds:
   - (AC) For every $A \subseteq \mathbb{R}$ non-empty and bounded above
   $$\sup A \in \mathbb{R}$$

Notation 3.45

For $x \in \mathbb{R}$, $x \neq 0$, the multiplicative inverse is also denoted by
$$x^{-1} = \frac{1}{x}.$$

Remark 3.46

Recall that

- $(K, +, \cdot)$ satisfying
$$\text{(A1)-(A3), (M1)-(M3), (AM)}$$
is a **field**
- $(K, +, \cdot, \geq)$ satisfying
$$\text{(A1)-(A3), (M1)-(M3), (O1)-(O4) ,(AM), (AO), (MO)}$$
is an **ordered field**

In particular we have that
$$(\mathbb{R}, +, \cdot, \leq)$$
is a **complete ordered field**: that is, an ordered field in which the **Cut Property** (CP) or **Axiom of Completeness** (AC) hold

Important

It can be shown that $(\mathbb{R}, +, \cdot, \leq)$ is the **only** complete ordered field.

> The above has to be intended in the following sense: if $(K, +, \cdot, \geq)$ is another complete ordered field, then K *looks like* $\mathbb{R}$. Mathematically this means that there exists an invertible map $\Psi : \mathbb{R} \to K$, called isomorphism of fields, which preserves the operations $+, \cdot$ and the order $\leq$.

Question 3.47

We have only postulated the existence of $\mathbb{R}$. Does such complete ordered field actually exist?

The answer is **YES**. There are several equivalent models for the system $\mathbb{R}$. If time allows, we will look into one of these models at the end of the module.

3.8 Special subsets of $\mathbb{R}$

In Definition 3.43 we have introduced $\mathbb{R}$ as a complete ordered field. This was done axiomatically and in a non constructive way. What happens now to the sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$? Are they well defined? Does it still hold that
$$\mathbb{N}, \mathbb{Z}, \mathbb{Q} \subseteq \mathbb{R}?$$

The definitions that we gave in Chapter 1 for $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ are not related to the system of real numbers $\mathbb{R}$ we just introduced. To overcome this problem, we will have to define new sets

$$\mathbb{N}_{\mathbb{R}},\ \mathbb{Z}_{\mathbb{R}},\ \mathbb{Q}_{\mathbb{R}}$$

from scracth, starting from the axioms of $\mathbb{R}$. Note that we are using the subscript $\mathbb{R}$ to distinguish these new sets from the old ones.

3.8.1 Natural numbers

Let us start with the definition of $\mathbb{N}_{\mathbb{R}}$. We would like $\mathbb{N}_{\mathbb{R}}$ to be

$$\mathbb{N}_{\mathbb{R}} = \{\mathbf{1}, \mathbf{2}, \mathbf{3}, ...\}.$$

Note that we are denoting the above numbers with bold symbols in order to distinguish them from the elements of $\mathbb{R}$. The key property that we would like $\mathbb{N}_{\mathbb{R}}$ to have is the following:

$$\text{Every } \mathbf{n} \in \mathbb{N}_{\mathbb{R}} \text{ has a successor } (\mathbf{n} + \mathbf{1}) \in \mathbb{N}_{\mathbb{R}}.$$

How do we ensure this property? We could start by defining

$$\mathbf{1} := 1,$$

with 1 the neutral element of the multiplication in $\mathbb{R}$, which exists by the field axiom (M2) in Defintion 3.43. We could then define $\mathbf{2}$ by setting

$$\mathbf{2} := 1 + 1.$$

We need a formal definition to capture this idea. This is the concept of **inductive set**.

Definition 3.48: Inductive set

Let $S \subseteq \mathbb{R}$. We say that S is an inductive set if they are satisfied:

- $1 \in S$,
- If $x \in S$, then $(x + 1) \in S$.

Note that in the above definition we just used:

- The existence of the neutral element 1, given by axiom (M2).
- The operation of sum in $\mathbb{R}$, which is again given as an axiom.

Example 3.49

We have that

- $\mathbb{R}$ is an inductive set.

  Indeed we have $1 \in \mathbb{R}$ by axiom (M2). Moreover $(x + 1) \in \mathbb{R}$ for every $x \in \mathbb{R}$, by definition of

sum $+$.

- The set $A = \{0, 1\}$ is not an inductive set.

  This is because $1 \in A$, but $(1 + 1) \notin A$, since $1 + 1 \neq 0$.

Therefore $\mathbb{R}$ is an inductive set, showing that the definition of inductive set is not sufficient to fully describe our intuitive idea of $\mathbb{N}_{\mathbb{R}}$. The right way to define $\mathbb{N}_{\mathbb{R}}$ is as follows:

$$\mathbb{N}_{\mathbb{R}} \text{ is the smallest inductive subset of } \mathbb{R}.$$

To make the above definition formal we need a few observations.

Proposition 3.50

Let $\mathscr{M}$ be a collection of inductive subsets of $\mathbb{R}$. Then

$$S := \bigcap_{M \in \mathscr{M}} M$$

is an inductive subset of $\mathbb{R}$.

Proof

We have to show that the two properties of inductive sets hold for S:

- We have $1 \in M$ for every $M \in \mathscr{M}$, since these are inductive sets. Thus

$$1 \in \bigcap_{M \in \mathscr{M}} M = S.$$

- Suppose that $x \in S$. By definition of S this implies that $x \in M$ for all $M \in \mathscr{M}$. Since M is an inductive set, then $(x + 1) \in M$. Therefore $(x + 1) \in M$ for all $M \in \mathscr{M}$, showing that $(x + 1) \in S$.

Therefore S is an inductive set.

We are now ready to define the natural numbers $\mathbb{N}_{\mathbb{R}}$.

Definition 3.51: Set of Natural Numbers

Let $\mathscr{M}$ be the collection of **all** inductive subsets of $\mathbb{R}$. We define the set of natural numbers in $\mathbb{R}$ as

$$\mathbb{N}_{\mathbb{R}} := \bigcap_{M \in \mathscr{M}} M .$$

Therefore $\mathbb{N}_{\mathbb{R}}$ is the intersection of all the inductive subsets of $\mathbb{R}$. From this definition it follows that $\mathbb{N}_{\mathbb{R}}$ is the smallest inductive subset of $\mathbb{R}$, as shown in the following proposition.

Proposition 3.52: $\mathbb{N}_{\mathbb{R}}$ is the smallest inductive subset of $\mathbb{R}$

Let $C \subseteq \mathbb{R}$ be an inductive subset. Then

$$\mathbb{N}_{\mathbb{R}} \subseteq C .$$

In other words, $\mathbb{N}_{\mathbb{R}}$ is the smallest inductive set in $\mathbb{R}$.

Proof

Let $\mathscr{M}$ be the collection of **all** inductive subsets of $\mathbb{R}$. By definition

$$\mathbb{N}_{\mathbb{R}} = \bigcap_{M \in \mathscr{M}} M .$$

Let $x \in \mathbb{N}_{\mathbb{R}}$, then $x \in M$ for all $M \in \mathscr{M}$. Since $C \in \mathscr{M}$ then $x \in C$. This shows $\mathbb{N}_{\mathbb{R}} \subseteq C$.

The definition of $\mathbb{N}_{\mathbb{R}}$ guarantees that all numbers in $\mathbb{N}_{\mathbb{R}}$ are larger than 1.

Theorem 3.53

Let $x \in \mathbb{N}_{\mathbb{R}}$. Then

$$x \geq 1 .$$

Proof

Define the set

$$C := \{x \in \mathbb{R} : \ x \geq 1\} .$$

We have that C is an inductive subset of $\mathbb{R}$.

By definition $1 \in C$. Suppose now that $x \in C$, so that $x \geq 1$. Since $1 \geq 0$ as a consequence of

the field axioms, we deduce that

$$x + 1 \geq x + 0 = x \geq 1\,,$$

showing that $x + 1 \geq 1$. Thus $(x + 1) \in C$.

By Proposition 3.52 we conclude that

$$\mathbb{N}_{\mathbb{R}} \subseteq C\,,$$

showing that $x \geq 1$ for all $x \in \mathbb{N}_{\mathbb{R}}$.

Notation 3.54

We have just shown that all the numebers $x \in \mathbb{N}_{\mathbb{R}}$ satisfy

$$x \geq 1\,.$$

Moreover by the fact that $\mathbb{N}_{\mathbb{R}}$ is an inductive set, we know that

$$1 + 1 \in \mathbb{N}_{\mathbb{R}}\,,$$

since $1 \in \mathbb{N}_{\mathbb{R}}$. We denote

$$2 := 1 + 1\,.$$

Similarly, we will have that

$$2 + 1 \in \mathbb{N}_{\mathbb{R}}\,,$$

since $2 \in \mathbb{N}_{\mathbb{R}}$. We denote

$$3 := 2 + 1\,.$$

In this way we give a name to all the numbers in $\mathbb{N}_{\mathbb{R}}$.

3.8.2 Principle of induction

The Principle of Induction is a consequence of the definition of $\mathbb{N}_{\mathbb{R}}$, see Definition 3.51, and of the field axioms of $\mathbb{R}$ in Definition 3.43.

Theorem 3.55: Principle of Induction

Let $\alpha(n)$ be a statement depending on $n \in \mathbb{N}_{\mathbb{R}}$. Assume that

1. $\alpha(1)$ is true.

2. If $\alpha(n)$ is true then also $\alpha(n+1)$ is true.

Then $\alpha(n)$ is true for all $n \in \mathbb{N}_{\mathbb{R}}$.

Proof

Define the set

$$C := \{x \in \mathbb{N}_{\mathbb{R}} : \ \alpha(n) \text{ is true}\}.$$

We have that C is an inductive subset of $\mathbb{R}$.

Indeed:

- $1 \in C$ since $\alpha(1)$ is true by assumption.
- If $n \in C$ then $\alpha(n)$ is true. By assumption $\alpha(n+1)$ is true. Therefore $(n+1) \in C$.

By Proposition 3.52 we conclude that

$$\mathbb{N}_{\mathbb{R}} \subseteq C\,.$$

As by definition $C \subseteq \mathbb{N}_{\mathbb{R}}$, we have proven that

$$\mathbb{N}_{\mathbb{R}} = C\,,$$

showing that $\alpha(n)$ is true for all $n \in \mathbb{N}_{\mathbb{R}}$.

As a consequence of the principle of induction, we can prove that $\mathbb{N}_{\mathbb{R}}$ is closed under the field operations of sum and multiplication.

Theorem 3.56

For all $n, m \in \mathbb{N}_{\mathbb{R}}$ we have:

1. $\mathbb{N}_{\mathbb{R}}$ is closed under addition, that is,
$$m + n \in \mathbb{N}_{\mathbb{R}}\,.$$
2. $\mathbb{N}_{\mathbb{R}}$ is closed under multiplication, that is,
$$m \cdot n \in \mathbb{N}_{\mathbb{R}}\,,$$
3. If $m > n$ there exists $k \in \mathbb{N}_{\mathbb{R}}$ such that
$$m = n + k\,.$$

Proof

We only prove the first point, the other statements are left as an exercise. Fix $m \in \mathbb{N}_{\mathbb{R}}$. We prove that

$$m + n \in \mathbb{N}_{\mathbb{R}}\,, \quad \forall\, n \in \mathbb{N}_{\mathbb{R}}\,, \tag{3.24}$$

by using induction.

- Induction base: We have $m + 1 \in \mathbb{N}_{\mathbb{R}}$, since $m \in \mathbb{N}_{\mathbb{R}}$ and $\mathbb{N}_{\mathbb{R}}$ is an inductive set.
- Inductive hypothesis: Suppose $m+n \in \mathbb{N}_{\mathbb{R}}$. Since $\mathbb{N}_{\mathbb{R}}$ is an inductive set, we have $(m+n)+1 \in \mathbb{N}_{\mathbb{R}}$. By associativity of the sum, see axiom (A1), we get

  $$m + (n + 1) = (m + n) + 1 \in \mathbb{N}_{\mathbb{R}}\,,$$

  which is the desired theis.

By the Induction Principle of Theorem 3.55 we conclude (3.24).

As a consequence of the above theorem, we see that the restriction of the operations of sum and multiplication to $\mathbb{N}_{\mathbb{R}}$ are still binary operations:

$$+ : \mathbb{N}_{\mathbb{R}} \times \mathbb{N}_{\mathbb{R}} \to \mathbb{N}_{\mathbb{R}}\,, \quad \cdot : \mathbb{N}_{\mathbb{R}} \times \mathbb{N}_{\mathbb{R}} \to \mathbb{N}_{\mathbb{R}}\,.$$

Equipped with the above operations, $\mathbb{N}_{\mathbb{R}}$ satisfies the following properties.

Theorem 3.57

$(\mathbb{N}_{\mathbb{R}}, +, \cdot, \leq)$ satisfies the following axioms from Definition 3.43:

- (A1).
- (M1), (M2).
- (O1)-(O4).
- (AM), (AO), (MO).

The proof is trivial, as it follows immediately from the inclusion of $\mathbb{N}_{\mathbb{R}}$ in $\mathbb{R}$.

3.8.3 Integers

We have seen in Theorem 3.56 that $\mathbb{N}_{\mathbb{R}}$ is closed under addition. However $\mathbb{N}_{\mathbb{R}}$ is not closed under subtraction. We therefore define the set of **integers** $\mathbb{Z}_{\mathbb{R}}$ in a way that we can perform subtraction of any two natural numbers.

Definition 3.58: Set of Integers

The set of integers in $\mathbb{R}$ is defined by

$$\mathbb{Z}_{\mathbb{R}} := \{m - n : \ n, m \in \mathbb{N}_{\mathbb{R}}\}.$$

In the definition of $\mathbb{Z}_{\mathbb{R}}$ we denote by $-n$ the inverse of n in $\mathbb{R}$, which exists by the field axiom (A3) in Definition 3.43. The following characterization explains the relationship between $\mathbb{Z}_{\mathbb{R}}$ and $\mathbb{N}_{\mathbb{R}}$.

Theorem 3.59

It holds

$$\mathbb{Z}_{\mathbb{R}} = \{-n : \ n \in \mathbb{N}_{\mathbb{R}}\} \cup \{0\} \cup \mathbb{N}_{\mathbb{R}}.$$

Proof

Define the set

$$M := \{-n : \ n \in \mathbb{N}_{\mathbb{R}}\} \cup \{0\} \cup \mathbb{N}_{\mathbb{R}}.$$

- $M \subseteq \mathbb{Z}_{\mathbb{R}}$: Suppose $m \in M$. We have 3 cases:
  - If $m \in \{-n : \ n \in \mathbb{N}_{\mathbb{R}}\}$ then there exists $n \in \mathbb{N}_{\mathbb{R}}$ such that $m = -n$. Thus
  $$m = -n = 1 - (n + 1) \in \mathbb{Z}_{\mathbb{R}},$$
  since $1 \in \mathbb{N}_{\mathbb{R}}$ and $n + 1 \in \mathbb{N}_{\mathbb{R}}$ because $n \in \mathbb{N}_{\mathbb{R}}$.
  - If $m = 0$ then
  $$m = 0 = 1 - 1 \in \mathbb{Z}_{\mathbb{R}},$$
  as $1 \in \mathbb{N}_{\mathbb{R}}$.
  - If $m \in \mathbb{N}_{\mathbb{R}}$ then
  $$m = (m + 1) - 1 \in \mathbb{Z}_{\mathbb{R}},$$
  since $1 \in \mathbb{N}_{\mathbb{R}}$ and $m + 1 \in \mathbb{N}_{\mathbb{R}}$, given that $m \in \mathbb{N}_{\mathbb{R}}$.

  In all 3 cases we have shown that $m \in \mathbb{Z}_{\mathbb{R}}$, proving that $M \subseteq \mathbb{Z}_{\mathbb{R}}$.
- $\mathbb{Z}_{\mathbb{R}} \subseteq M$: Let $z \in \mathbb{Z}_{\mathbb{R}}$. Then $z = m - n$ for some $n, m \in \mathbb{N}_{\mathbb{R}}$. We have 3 cases:
  - If $m = n$ then
  $$z = m - n = m - m \overset{(A3)}{=} 0 \in M.$$
  - If $m > n$, by Theorem 3.56 there exists $k \in \mathbb{N}_{\mathbb{R}}$ such that $m = k + n$. Therefore
  $$\begin{aligned} z = m - n &= (k + n) - n \\ &\overset{(A1)}{=} k + (n - n) \overset{(A3)}{=} k + 0 \\ &\overset{(A2)}{=} k \in M, \end{aligned}$$

since $k \in \mathbb{N}_{\mathbb{R}}$.

– If $m < n$, by Theorem 3.56 there exists $k \in \mathbb{N}_{\mathbb{R}}$ such that $n = k + m$. Therefore

$$z = m - n = -k \in M\,,$$

since $k \in \mathbb{N}_{\mathbb{R}}$, where again we have used (implicitly) the field axioms (A1), (A2) and (A3).

Therefore $\mathbb{Z}_{\mathbb{R}} = M$.

Like we did with $\mathbb{N}_{\mathbb{R}}$, we can also show that $\mathbb{Z}_{\mathbb{R}}$ is closed under the operations of sum and multiplication.

Theorem 3.60

For all $n, m \in \mathbb{Z}_{\mathbb{R}}$ we have:

1. $\mathbb{Z}_{\mathbb{R}}$ is closed under addition, that is,
$$m + n \in \mathbb{Z}_{\mathbb{R}}\,.$$
2. $\mathbb{Z}_{\mathbb{R}}$ is closed under multiplication, that is,
$$m \cdot n \in \mathbb{Z}_{\mathbb{R}}\,,$$

The proof is left as an exercise. As a consequence of Theorem 3.60 we have that the restriction of the operations of sum and multiplication to $\mathbb{Z}_{\mathbb{R}}$ are still binary operations:

$$+ : \mathbb{Z}_{\mathbb{R}} \times \mathbb{Z}_{\mathbb{R}} \to \mathbb{Z}_{\mathbb{R}}\,, \quad \cdot : \mathbb{Z}_{\mathbb{R}} \times \mathbb{Z}_{\mathbb{R}} \to \mathbb{Z}_{\mathbb{R}}\,.$$

Equipped with the above operations, $\mathbb{Z}_{\mathbb{R}}$ satisfies the following properties.

Theorem 3.61

$(\mathbb{Z}_{\mathbb{R}}, +, \cdot, \leq)$ satisfies the following axioms from Definition 3.43:

- (A1), (A2), (A3).
- (M1), (M2).
- (O1)-(O4).
- (AM), (AO), (MO).

Proof

The fact that

$$\text{(A1), (A2), (M1), (M2), (O1)-(O4), (AM), (AO), (MO)}$$

are satisfied descends immediately from the inclusion

$$\mathbb{Z}_{\mathbb{R}} \subseteq \mathbb{R}\,.$$

We are left to prove (A3). This is non-trivial because a priori the additive inverse $-z$ of some $z \in \mathbb{Z}_{\mathbb{R}}$ belongs to $\mathbb{R}$. We need to check that $-z \in \mathbb{Z}_{\mathbb{R}}$. Indeed, since $z \in \mathbb{Z}_{\mathbb{R}}$, there exist $n, m \in \mathbb{N}_{\mathbb{R}}$ such that $z = m - n$. Define $y := n - m$. We have that $y \in \mathbb{Z}_{\mathbb{R}}$ and

$$z + y = (m - n) + (n - m) = (m - m) + (n - n) = 0\,.$$

Therefore y is the inverse of z and $y \in \mathbb{Z}_{\mathbb{R}}$, proving that the sum in $\mathbb{Z}_{\mathbb{R}}$ satisfies (A3).

Remark 3.62

$\mathbb{Z}_{\mathbb{R}}$ does not satisfy (M3).

For example, let us show that $2 \in \mathbb{Z}_{\mathbb{R}}$ has no inverse in $\mathbb{Z}_{\mathbb{R}}$. Indeed, let $m \in \mathbb{Z}_{\mathbb{R}}$. By Theorem 3.59 we have 3 cases:

- $m \in \mathbb{N}_{\mathbb{R}}$: Since $2 > 1$ we have
$$2 \cdot m > 1 \cdot m \geq 1$$
where in the last inequality we used that $m \geq 1$ for all $m \in \mathbb{N}_{\mathbb{R}}$, as shown in Theorem 3.53. The above shows that
$$2 \cdot m > 1\,,$$
and therefore m cannot be the inverse of 2.
- $m = 0$: Then $2 \cdot m = 0$, so that m cannot be the inverse of 2.
- $m = -n$ with $n \in \mathbb{N}_{\mathbb{R}}$. Then
$$2 \cdot m = 2 \cdot (-n) < 0\,,$$
so that m cannot be the inverse of 2.

As we have exhausted all the possibilities, we conclude that 2 does not have a multiplicative inverse in $\mathbb{N}_{\mathbb{R}}$.

3.8.4 Rational numbers

In Theorem 3.61 and 3.62 we have seen that $\mathbb{Z}_{\mathbb{R}}$ satisfy all the field axiom, except for (M3). We therefore extend $\mathbb{Z}_{\mathbb{R}}$ in a way that the extension contains multiplicative inverses. The extension is the set of rational numbers $\mathbb{Q}_{\mathbb{R}}$.

Definition 3.63: Set of Rational Numbers

The set of rational numbers in $\mathbb{R}$ is

$$\mathbb{Q}_{\mathbb{R}} := \left\{ \frac{m}{n} \ : \ m \in \mathbb{Z}_{\mathbb{R}} \, , \ n \in \mathbb{N}_{\mathbb{R}} \right\} .$$

Notice that in the above definition we are just using the field axiom (M3), with

$$\frac{m}{n} := m \cdot n^{-1} .$$

The inverse of n exists because we are assuming $n \in \mathbb{N}_{\mathbb{R}}$, and therefore n cannot be 0, as a consequence of Theorem 3.53.

The set $\mathbb{Q}_{\mathbb{R}}$ is closed under addition and multiplication (exercise). Therefore they are well defined the operations:

$$+ \ : \ \mathbb{Q}_{\mathbb{R}} \times \mathbb{Q}_{\mathbb{R}} \to \mathbb{Q}_{\mathbb{R}} \, , \quad \cdot \ : \ \mathbb{Q}_{\mathbb{R}} \times \mathbb{Q}_{\mathbb{R}} \to \mathbb{Q}_{\mathbb{R}} \, .$$

Theorem 3.64

$(\mathbb{Q}_{\mathbb{R}}, +, \cdot, \leq)$ is an ordered field.

Proof

All the field properties, except for (M3), follow from the inclusion

$$\mathbb{Q}_{\mathbb{R}} \subseteq \mathbb{R}$$

and from the field properties of $\mathbb{R}$. To check (M3), let $q \in \mathbb{Q}_{\mathbb{R}}$ with $q \neq 0$. Therefore $q = m/n$ for $m \in \mathbb{Z}_{\mathbb{R}}$, $n \in \mathbb{N}_{\mathbb{R}}$. As $q \neq 0$ and $n \neq 0$, see Theorem 3.53, we deduce that $m \neq 0$. We have two cases:

- $m > 0$: In this case $m \in \mathbb{N}_{\mathbb{R}}$ by Theorem 3.59. Therefore

  $$p = \frac{n}{m} \in \mathbb{Q}_{\mathbb{R}}$$

  by definition, since $n, m \in \mathbb{N}_{\mathbb{R}}$. By commutativity we have

  $$q \cdot p = \frac{m}{n} \cdot \frac{n}{m} = 1 \, .$$

- $m < 0$: Then $m = -x$ with $x \in \mathbb{N}_{\mathbb{R}}$ by Theorem 3.59. Therefore

  $$p = \frac{-n}{x} \in \mathbb{Q}_{\mathbb{R}}$$

  by definition, since $-n \in \mathbb{Z}_{\mathbb{R}}$ and $x \in \mathbb{N}_{\mathbb{R}}$. By commutativity we have

  $$q \cdot p = \frac{m}{n} \cdot \frac{-n}{x} = \frac{m}{n} \cdot \frac{-n}{-m} = 1 \, .$$

Therefore q always admits a multiplicative inverse q^{-1} belonging to $\mathbb{Q}_{\mathbb{R}}$, proving (M3).

The set $\mathbb{Q}_{\mathbb{R}}$ does not have the Cut Property or the Axiom of Completeness.

Theorem 3.65

$\mathbb{Q}_{\mathbb{R}}$ is not complete.

The proof of the above Theorem is a one to one copy of the proof of Theorem 3.36: indeed the proof of Theorem 3.36 only makes use of field axioms, and thus it applies to $\mathbb{Q}_{\mathbb{R}}$.

Notation 3.66

From now on we denote

$$\mathbb{N} := \mathbb{N}_{\mathbb{R}}, \quad \mathbb{Z} := \mathbb{Z}_{\mathbb{R}}, \quad \mathbb{Q} := \mathbb{Q}_{\mathbb{R}},$$

dropping the subscript $\mathbb{R}$.

4 Properties of $\mathbb{R}$

Now that we established the axiomatic definition of the Real Numbers $\mathbb{R}$ as a **complete ordered field**, let us investigate some of the properties of $\mathbb{R}$. These will be consequence of the axioms of the real numbers, particulaly of the **Axiom of Completeness**.

4.1 Archimedean Property

The Archimedean property is one of the most useful properties of $\mathbb{R}$, and it essentially states that the set of natural numbers $\mathbb{N}$ is not bounded above in $\mathbb{R}$.

More precisley, the Archimedean Property says two things:

1. For any $x \in \mathbb{R}$ we can always find a natural number $n \in \mathbb{N}$ such that
$$n > x\,.$$
2. For any $x \in \mathbb{R}$ with $x > 0$, we can always find a natural number $m \in \mathbb{N}$ such that
$$0 < \frac{1}{m} < x\,.$$

The situation is depicted in Figure 4.2.

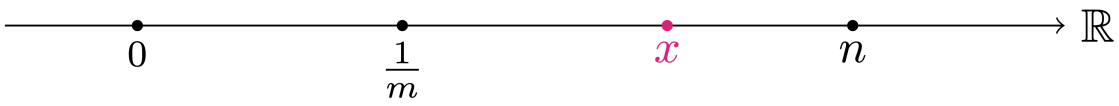

Figure 4.1: For any $x > 0$ we can find $n, m \in \mathbb{N}$ such that $1/m < x < n$.

Remark 4.1

The Archimedean property might sound trivial. However there are examples of ordered fields K that satisfy:

1. $\mathbb{N} \subseteq K$.
2. K does not have the Archimedean property.
3. In particular, $\mathbb{N}$ is bounded above in K.

Of course such fields K cannot be complete.

If K is complete, then K is essentially $\mathbb{R}$, and we are going to prove the Archimedean Property holds in $\mathbb{R}$.

Let us proceed with the precise statement of the Archimedean property in $\mathbb{R}$.

Theorem 4.2: Archimedean Property

Let $x \in \mathbb{R}$ be given. Then:

1. There exists $n \in \mathbb{N}$ such that
$$n > x\,.$$
2. Suppose in addition that $x > 0$. There exists $n \in \mathbb{N}$ such that
$$\frac{1}{n} < x\,.$$

Proof

Part 1. Let $x \in \mathbb{R}$. Suppose by contradiction that there is no $n \in \mathbb{N}$ such that
$$n > x\,.$$
This means that
$$n \leq x \quad \forall n \in \mathbb{N}\,. \tag{4.1}$$
The above is saying that the set $\mathbb{N}$ is bounded above. Since $\mathbb{N}$ is not empty, by the Axiom of Completeness there exists
$$\alpha = \sup \mathbb{N}\,.$$
Claim: $(\alpha - 1)$ *is not an upper bound for* $\mathbb{N}$.
Proof of Claim. Indeed, we have
$$(\alpha - 1) < \alpha\,. \tag{4.2}$$
Therefore $\alpha - 1$ cannot be an upper bound for $\mathbb{N}$. Indeed, if by contradiction $\alpha - 1$ was an upper bound for $\mathbb{N}$, then we would have
$$\alpha \leq (\alpha - 1)\,,$$
since α is the smallest upper bound for $\mathbb{N}$. This contradicts (4.2). Therefore $\alpha - 1$ is not an upper bound for $\mathbb{N}$.
Conclusion. Since $\alpha - 1$ is not an upper bound for $\mathbb{N}$, there exists $n_0 \in \mathbb{N}$ such that
$$\alpha - 1 < n_0\,.$$
The above implies
$$\alpha < n_0 + 1\,.$$

Since

$$(n_0 + 1) \in \mathbb{N},$$

we have obtained a contradiction, given that α was the supremum of $\mathbb{N}$. Thus (4.1) is false, meaning that there exists $n \in \mathbb{N}$ such that

$$n > x.$$

Part 2. Suppose $x \in \mathbb{R}$ with $x > 0$. We can define

$$y := \frac{1}{x}.$$

By Part 1 there exists $n \in \mathbb{N}$ such that

$$n > y = \frac{1}{x}.$$

Using that $x > 0$, we can rearrange the above inequlaity to obtain

$$\frac{1}{n} < x,$$

which is the desired thesis.

There is another formulation of the Archimedean Property which, depending on the situation, might be more useful. This formulation says the following: If $x, y \in \mathbb{R}$ are such that

$$0 < x < y,$$

then there exists $n \in \mathbb{N}$ such that

$$nx > y.$$

In other words, if one does n steps of size x in the positive numbers direction, then the resulting number nx will be larger than y. The situation is depicted in Figure 4.2.

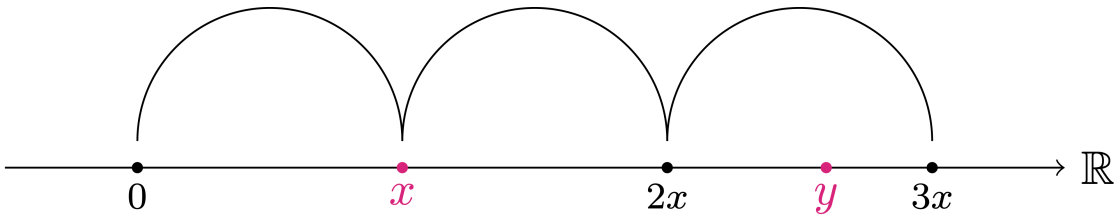

Figure 4.2: For $0 < x < y$ there exists $n \in \mathbb{N}$ such that that $nx > y$. In the picture $n = 3$.

Theorem 4.3: Archimedean Property (Alternative formulation)

Let $x, y \in \mathbb{R}$, with $0 < x < y$. There exists $n \in \mathbb{N}$ such that

$$nx > y.$$

Proof

Suppose by contradiction that there does not exist some $n \in \mathbb{N}$ such that

$$nx > y\,.$$

This means that

$$nx \leq y\,, \quad \forall\, n \in \mathbb{N}\,. \tag{4.3}$$

Define the set

$$A := \{nx \,:\, n \in \mathbb{N}\}\,.$$

Condition (4.3) is saying that A is bounded above by y. Morever A is trivially non-empty. By the Axiom of Completeness there exists

$$\alpha = \sup A\,.$$

Since α is the supremum of A, by definition of supremum and of the set A, we have

$$nx \leq \alpha\,, \quad \forall\, n \in \mathbb{N}\,. \tag{4.4}$$

As (4.4) holds for every $n \in \mathbb{N}$, then it also holds for $(n+1)$, meaning that

$$(n+1)x \leq \alpha\,.$$

The above implies

$$nx \leq \alpha - x\,.$$

As n was arbitrary, we conclude that

$$nx \leq \alpha - x\,, \quad \forall\, n \in \mathbb{N}\,.$$

The above is saying that $(\alpha - x)$ is an upper bound for A. Since α is the supremum of A, in particular α is the smallest upper bound. Thus it must hold

$$\alpha \leq \alpha - x\,.$$

The above is equivalent to

$$x \leq 0\,,$$

which contradicts our assumption of $x > 0$. Therefore (4.3) is false, and there exists $n \in \mathbb{N}$ such that

$$nx > y\,,$$

concluding the proof.

4.2 Nested Interval Property

Another consequence of the axiom of completeness is the **Nested Interval Property**. This is yet another way of saying the same thing: $\mathbb{R}$ does not have **gaps**.

Let us look at a construction. Suppose given some closed intervals

$$I_n := [a_n, b_n] = \{x \in \mathbb{R} : \ a_n \leq x \leq b_n\},$$

where the end points are ordered in the following way:

$$a_1 \leq a_2 \leq \ldots \leq a_n \leq \cdots \leq b_n \leq \ldots b_n \leq b_1\,,$$

as shown in Figure 4.3.

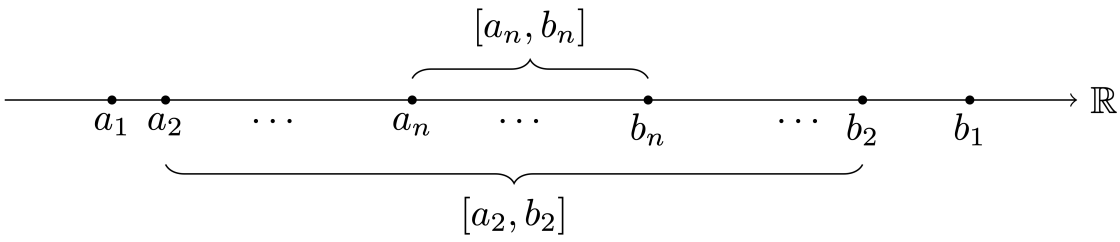

Figure 4.3: Nested intervals $I_n = [a_n, b_n]$.

The intervals I_n are **nested**, meaning that

$$I_1 \supset I_2 \supset I_3 \supset \ldots I_n \supset \ldots$$

For finite intersections we clearly have

$$\bigcap_{n=1}^{k} I_n = I_k\,,$$

that is, intersecting the first k intervals yields I_k, the smallest interval in the sequence.

Question 4.4

Consider the infinite intersection

$$\bigcap_{n=1}^{\infty} I_n := \{x \in \mathbb{R} : \ x \in I_n\,, \forall\, n \in \mathbb{N}\}\,.$$

What can we say about it? Is it empty? Is it not empty?

The answer is that the infinite intersection is not empty, because $\mathbb{R}$ was constructed in a way that it does not have gaps.

Theorem 4.5: Nested Interval Property

For each $n \in \mathbb{N}$ assume given a closed interval

$$I_n := [a_n, b_n] = \{x \in \mathbb{R} : \ a_n \leq x \leq b_n\}.$$

Suppose that the intervals are nested, that is,

$$I_n \supset I_{n+1}, \quad \forall n \in \mathbb{N}.$$

Then

$$\bigcap_{n=1}^{\infty} I_n \neq \emptyset. \tag{4.5}$$

Proof

By definition we have

$$\bigcap_{n=1}^{\infty} I_n := \{x \in \mathbb{R} : \ x \in I_n, \forall n \in \mathbb{N}\}.$$

We want to prove (4.5). This means we need to find a real number x such that

$$x \in I_n, \quad \forall n \in \mathbb{N}. \tag{4.6}$$

Idea of the Proof: Condition (4.6) is saying that it should hold

$$x \geq a_n, \quad \forall n \in \mathbb{N}.$$

We might be tempted to choose x to be any of the b_n. This choice would indeed satisy the above. However (4.6) also implies that

$$x \leq b_n, \quad \forall n \in \mathbb{N}.$$

Therefore x has to be larger than all the a_n, but not too large. This suggests that x should be defined as a supremum.

Define the set

$$A := \{a_n : \ n \in \mathbb{N}\}.$$

The set A is non-empty and is bounded above by any of the b_n. Therefore there exists

$$x = \sup A.$$

By definition of supremum and definition of the set A, we have

$$a_n \leq x, \quad \forall n \in \mathbb{N}.$$

On the other hand, consider an arbitrary number b_n. By construction we have

$$a_i \leq b_n\,, \quad \forall\, i \in \mathbb{N}\,.$$

Therefore b_n is an upper bound for A. Since the supremum is the smallest upper bound, we conclude that

$$x \leq b_n\,.$$

The index n was chosen arbitrarily, and therefore

$$x \leq b_n\,, \quad \forall\, n \in \mathbb{N}\,.$$

In total we have

$$a_n \leq x \leq b_n\,, \quad \forall\, n \in \mathbb{N}\,,$$

showing that x satisfies (4.6). Therefore (4.5) holds and the proof is concluded.

Important

The assumption that I_n is **closed** is crucial in Theorem 4.14. Without such assumption the thesis of Theorem 4.14 does not hold in general, as seen in Example 4.6 below.

Example 4.6

Consider the **open** intervals

$$I_n := \left(0, \frac{1}{n}\right)\,.$$

These are clearly nested

$$I_n \supset I_{n+1}\,, \quad \forall\, n \in \mathbb{N}\,.$$

For this choice of I_n we have

$$\bigcap_{n=1}^{\infty} I_n = \emptyset\,. \tag{4.7}$$

Indeed, suppose by contradiction that the intersection is non-empty. Then there exists $x \in \mathbb{N}$ such that

$$x \in I_n\,, \quad \forall\, n \in \mathbb{N}\,.$$

By definition of I_n the above reads

$$0 < x < \frac{1}{n}\,, \quad \forall\, n \in \mathbb{N}\,. \tag{4.8}$$

Since $x > 0$, by the Archimedean Property in Theorem 4.11 Point 2, there exists $n_0 \in \mathbb{N}$ such that

$$0 < \frac{1}{n_0} < x\,.$$

The above contradicts (4.8). Therefore (4.7) holds.

4.3 Revisiting Sup and inf

We now investigate some of the properties of supremum and infimum in $\mathbb{R}$. The first property is an alternative characterization of the supremum, which we will often use. A sketch of such characterization is in Figure 4.4 below.

Proposition 4.7: Characterization of Supremum

Let $A \subseteq \mathbb{R}$ be a non-empty set. Suppose that $s \in \mathbb{R}$ is an upper bound for A. They are equivalent:

1. $s = \sup A$
2. For every $\varepsilon > 0$ there exists $x \in A$ such that

$$s - \varepsilon < x\,.$$

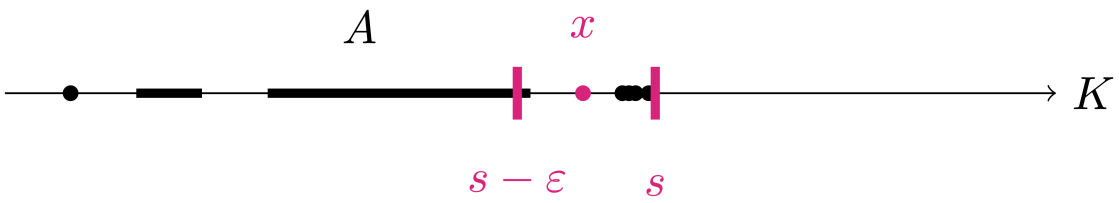

Figure 4.4: Let $s = \sup A$. Then for every $\varepsilon > 0$ there exist $x \in A$ such that $s - \varepsilon < x$.

Proof: Proof of Proposition 4.16

Step 1. Assume that

$$s = \sup A\,.$$

Let $\varepsilon > 0$ be arbitrary. We clearly have that

$$s - \varepsilon < s\,. \tag{4.9}$$

Therefore $(s - \varepsilon)$ cannot be an upper bound of A. Indeed, if by contradiction $(s - \varepsilon)$ was an upper bound, then we would have

$$s \leq (s - \varepsilon)\,,$$

since s is the smallest upper bound. The above contradicts (4.9), and therefore $(s-\varepsilon)$ is not an upper bound for A. Hence there exists some $x \in A$ such that

$$s - \varepsilon < x\,,$$

concluding.
Step 2. Assume that Point 2 in the statement of Proposition 4.16 holds. By assumption we have that s is an upper bound for A. Suppose by contradiction that

$$s \neq \sup A\,.$$

This is equivalent to the statement

$$s \text{ is not the smallest upper bound of } A. \tag{4.10}$$

Hence there exists an upper bound b of A such that

$$b < s\,.$$

Let

$$\varepsilon := s - b\,.$$

By assumption there exists $x \in A$ such that

$$s - \varepsilon < x\,.$$

Substituting the definition of ε we get

$$s - s + b < x \quad \Longrightarrow \quad b < x\,.$$

Since b is an upper bound for A and $x \in A$, the above is a contradiction. Therefore (4.10) is false, and s is the smallest upper bound of A. Thus $s = \sup A$.

The analogue of Proposition 4.16 is as follows. The proof is left as an exercise.

Proposition 4.8: Characterization of Infimum

Let $A \subseteq \mathbb{R}$ be a non-empty set. Suppose that $i \in \mathbb{R}$ is a lower bound for A. They are equivalent:

1. $i = \inf A$
2. For every $\varepsilon \in \mathbb{R}$, with $\varepsilon > 0$, there exists $x \in A$ such that

$$x < i + \varepsilon\,.$$

A sketch of the characterization in Proposition 4.17 can be found in Figure 4.5 below.

With the above characterizations of supremum and infimum, it is now easier to prove that some candidate

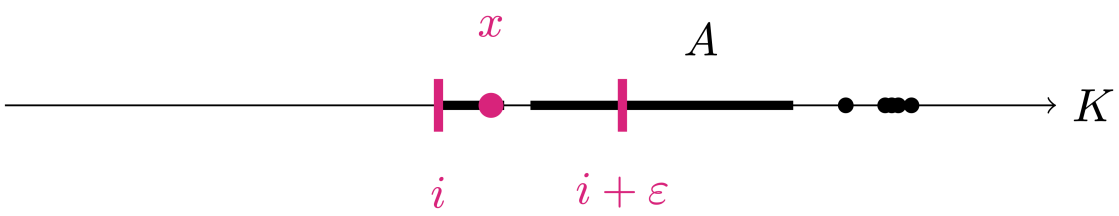

Figure 4.5: Let $i = \inf A$. Then for every $\varepsilon > 0$ there exist $x \in A$ such that $x < i + \varepsilon$.

number is the supremum or infimum of some set. As an example, let us characterize supremum and infimum of an open interval of $\mathbb{R}$.

Proposition 4.9

Let $a, b \in \mathbb{R}$ with $a < b$. Let

$$A := (a, b) = \{x \in \mathbb{R} : \ a < x < b\}.$$

Then

$$\inf A = a\,, \quad \sup A = b\,.$$

Proof

We will only prove that

$$\inf A = a\,,$$

since the proof of

$$\sup A = b$$

is similar.
By definition of A, we have that

$$a < x\,, \quad \forall\, x \in A\,.$$

The above says that a is a lower bound for A.
Claim. a is the largest lower bound of A.
Proof of Claim. Let L be a lower bound for A, that is,

$$L \leq x\,, \quad \forall\, x \in A\,.$$

We have to prove that

$$L \leq a\,. \tag{4.11}$$

Indeed suppose by contradiction that (4.11) does not hold, namely that

$$a < L\,.$$

Since $a < b$ we have

$$a = \frac{2a}{2} < \frac{a+b}{2} < \frac{2b}{b} = b\,,$$

showing that the midpoint between a and b satisfies

$$\frac{a+b}{2} \in A\,.$$

Since L is a lower bound for A we have

$$L \leq \frac{a+b}{2} < b\,. \tag{4.12}$$

Consider the midpoint

$$M := \frac{a+L}{2}\,.$$

We have that

$$M \in A\,.$$

Indeed, recalling that $a < L$, we have

$$a = \frac{2a}{2} < \frac{a+L}{2} = M\,.$$

Moreover by (4.12) we have $L < b$. Thus

$$M = \frac{a+L}{2} \leq \frac{a+b}{2} < b\,.$$

This shows $M \in A$.

Moreover

$$M < L\,.$$

This is because $a < L$, and therefore

$$M = \frac{a+L}{2} < \frac{2L}{2} = L\,.$$

This is a contradiction, since by assumption L is a lower bound for A, and thus we should have

$$L \leq M\,.$$

Therefore (4.11) holds, showing that a is the largest lower bound of A. Thus $a = \inf A$.

As a corollary of the above we have that the maximum and minimum of an open interval do not exist.

Corollary 4.10

Let $a, b \in \mathbb{R}$ with $a < b$. Let

$$A := (a, b) = \{x \in \mathbb{R} : \ a < x < b\}.$$

Then $\min A$ and $\max A$ do not exist.

Proof

Suppose by contradiction that $\min A$ exists. We have shown that if the minimum of a set exists, then it must be

$$\min A = \inf A.$$

Since

$$\inf A = a,$$

by Proposition 4.9, we would obtain that

$$\min A = a.$$

By definition $\min A \in A$, so that $a \in A$. This is contradiction. Then $\min A$ does not exist.
The proof that $\max A$ does not exist is similar, and is left as an exercise.

We can also consider intervals for which one or both of the sides are closed.

Corollary 4.11

Let $a, b \in \mathbb{R}$ with $a < b$. Let

$$A := [a, b) = \{x \in \mathbb{R} : \ a \leq x < b\}.$$

Then

$$\min A = \inf A = a, \quad \sup A = b,$$

$\max A$ does not exist.

The proof is very similar to the ones above, and is left to the reader for exercise. Let us now compute supremum and infimum of a set which is not an interval.

Proposition 4.12

Define the set

$$A := \left\{\frac{1}{n} : \ n \in \mathbb{N}\right\}.$$

Then

$$\inf A = 0, \quad \sup A = \max A = 1.$$

Proof

Part 1. We have

$$\frac{1}{n} \leq 1\,, \quad \forall\, n \in \mathbb{N}\,.$$

Therefore 1 is an upper bound for A. Let us prove it is the least upper bound: let b be an upper bound for A. Since $1 \in A$ and b is an upper bound, we have $1 \leq b$. Hence 1 is the least upper bound, and

$$\sup A = \max A = 1\,.$$

Part 2. We have

$$\frac{1}{n} > 0\,, \quad \forall\, n \in \mathbb{N}\,,$$

showing that 0 is a lower bound for A. Suppose by contradiction that 0 is not the infimum. Therefore 0 is not the largest lower bound. Then there exists $\varepsilon \in \mathbb{R}$ such that:

- ε is a lower bound for A, that is,
$$\varepsilon \leq \frac{1}{n}\,, \quad \forall\, n \in \mathbb{N}\,, \tag{4.13}$$
- ε is larger than 0:
$$0 < \varepsilon\,.$$

As $\varepsilon > 0$, by the Archimedean Property there exists $n_0 \in \mathbb{N}$ such that

$$0 < \frac{1}{n_0} < \varepsilon\,.$$

This contradicts (4.13). Thus 0 is the largest lower bound of A, that is, $0 = \inf A$.
Part 3. We have that $\min A$ does not exist. Indeed suppose by contradiction that $\min A$ exists. Then

$$\min A = \inf A\,.$$

As $\inf A = 0$ by Part 2, we conclude $\min A = 0$. As $\min A \in A$, we obtain $0 \in A$, which is a contradiction.

4.4 Density of $\mathbb{Q}$ in $\mathbb{R}$

A set S is dense in $\mathbb{R}$ if the elements of S are arbitrarily close to the elements of $\mathbb{R}$.

Definition 4.13: Dense set

Let $S \subseteq \mathbb{R}$. We say that S is dense in $\mathbb{R}$ if for every $x \in \mathbb{R}$ and $\varepsilon \in \mathbb{R}$ with $\varepsilon > 0$, there exist $q \in \mathbb{Q}$ such that

$$|x - q| < \varepsilon .$$

In other words, the above definition is saying that S and $\mathbb{R}$ are tightly knitted together. An equivalent definition of dense set is given below.

Remark 4.14

Let $S \subseteq \mathbb{R}$. They are equivalent:

- S is dense in $\mathbb{R}$.
- For every pair of numbers $x, y \in \mathbb{R}$ with $x < y$, there exists $s \in S$ such that

$$x < s < y .$$

We now prove that $\mathbb{Q}$ is dense in $\mathbb{R}$.

Theorem 4.15: Density of $\mathbb{Q}$ in $\mathbb{R}$

Let $x, y \in \mathbb{R}$, with $x < y$. There exists $q \in \mathbb{Q}$ such that

$$x < q < y .$$

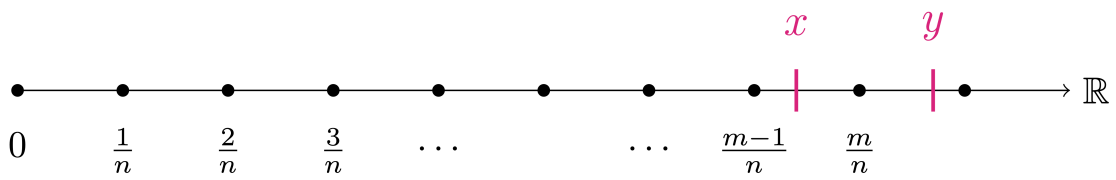

Figure 4.6: Let $n \in \mathbb{N}$ be such that $1/n < y - x$. Then take m so that $m/n \in (x, y)$.

Proof

We need to find $q \in \mathbb{Q}$ such that

$$x < q < y . \tag{4.14}$$

By definition of $\mathbb{Q}$, we have that q has to be $q = m/n$ for $m \in \mathbb{Z}$ and $n \in \mathbb{N}$. Therefore (4.14) is equivalent to finding $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that

$$x < \frac{m}{n} < y . \tag{4.15}$$

The idea is to proceed as in Figure 4.6: We take n such that $1/n$ is small enough so that we can make m

jumps of size $1/n$ and end up between x and y.
To this end, let $n \in \mathbb{N}$ be such that

$$\frac{1}{n} < y - x\,. \tag{4.16}$$

Such n exists thanks to the Archimedean Property in Theorem 4.11 Point 2. Inequality (4.15) is equivalent to

$$nx < m < ny\,.$$

Take $m \in \mathbb{Z}$ such that

$$m - 1 \leq nx < m\,. \tag{4.17}$$

> Why does such m exist? Because by Archimedean Property in Theorem 4.11 Point 1, there exists $m' \in \mathbb{Z}$ such that
>
> $$m' > nx$$
>
> We can then choose m to be the smallest element in $\mathbb{Z}$ such that $m > nx$. Such m satisfies (4.17).

The second inequality in (4.17) implies

$$x < \frac{m}{n}\,,$$

which is the first inequality in (4.15). Now note that (4.16) is equivalent to $x < y - 1/n$. We can use the latter and the first inequality in (4.17) to estimate

$$\begin{aligned} m &\leq 1 + nx \\ &< 1 + n\left(y - \frac{1}{n}\right) \\ &= ny\,, \end{aligned}$$

which yields

$$\frac{m}{n} < y\,.$$

Therefore the second inequality in (4.15) is proven, concluding the proof.

We have constructed the real numbers $\mathbb{R}$ so that they would fill the **gaps** of $\mathbb{Q}$. Formally, these gaps are the numbers in $\mathbb{R} \setminus \mathbb{Q}$. Let us give a name to this set.

Definition 4.16: Irrational numbers

The set of irrational numbers in $\mathbb{R}$ is

$$\mathcal{I} := \mathbb{R} \setminus \mathbb{Q}\,.$$

Question 4.17

How many gaps does $\mathbb{Q}$ have? In other words, how many irrational numbers are out there?

The answer is quite surprising, and is a corollary of the density result of Theorem 4.15: The irrational numbers are dense in $\mathbb{R}$.

Corollary 4.18

Let $x, y \in \mathbb{R}$, with $x < y$. There exists $t \in \mathscr{I}$ such that

$$x < t < y\,.$$

Proof

Consider

$$\tilde{x} := x - \sqrt{2}\,, \quad \tilde{y} := y - \sqrt{2}\,.$$

Since $x < y$, we have

$$\tilde{x} < \tilde{y}\,.$$

By Theorem 4.15 there exists $q \in \mathbb{Q}$ such that

$$\tilde{x} < q < \tilde{y}\,.$$

Adding $\sqrt{2}$ to the above inequalities we get

$$x < t < y\,, \quad t := q + \sqrt{2}\,. \tag{4.18}$$

We claim that $t \in \mathscr{I}$. Indeed, suppose by contradiction $t \in \mathbb{Q}$. Then

$$\sqrt{2} = t - q \in \mathbb{Q}\,,$$

since $t, q \in \mathbb{Q}$, and $\mathbb{Q}$ is closed under summation. Since $\sqrt{2} \in \mathscr{I}$, we obtain a contradiction. Thus $t \in \mathscr{I}$ and (4.18) is our thesis.

4.5 Existence of k-th Roots

We have started our discussion by proving that

$$\sqrt{2} \notin \mathbb{Q}\,. \tag{4.19}$$

We have shown that (4.19) implies that the set

$$A := \{q \in \mathbb{Q} : \ q^2 < 2\}$$

does not have a supremum in $\mathbb{Q}$. We then introduced the Real Numbers $\mathbb{R}$ so that each non-empty and bounded above set would have a supremum. As the set A is non-empty and bounded above, there exists $\alpha \in \mathbb{R}$ such that

$$\alpha = \sup A\,.$$

We are going to prove that

$$\alpha^2 = 2\,,$$

which means that in $\mathbb{R}$ we can take the square root of 2. More in general, with the same fudamental idea, we can prove that for each $x \in \mathbb{R}$ with $x \geq 0$ and $k \in \mathbb{N}$, there exists $\alpha \in \mathbb{R}$ such that

$$\alpha^k = x\,.$$

Theorem 4.19: Existence of k-th roots

Let $x \in \mathbb{R}$ with $x \geq 0$ and $k \in \mathbb{N}$. There exists a unique $\alpha \in \mathbb{R}$ such that

$$\alpha^k = x\,.$$

The proof of Theorem 4.19 rests on similar ideas to the ones used to prove that $\mathbb{Q}$ does not have the cut property.

Proof: Proof of Theorem 4.19

Part 1: Uniqueness.
Suppose $\alpha_1, \alpha_2 \in \mathbb{R}$ are such that

$$\alpha_1^k = \alpha_2^k = x\,.$$

If $\alpha_1 \neq \alpha_2$, then

$$\alpha_1^k \neq \alpha_2^k\,,$$

obtaining a contradiction. Therefore $\alpha_1 = \alpha_2$.
Part 2: Existence.
Let $x \in \mathbb{R}$ with $x \geq 0$. If $x = 0$ there is nothing to prove, as

$$0^k = 0\,,$$

so that $\alpha = 0$. Therefore we can assume $x > 0$. Define the subset of $\mathbb{R}$

$$A := \{t \in \mathbb{R} : \ t^k < x\}\,.$$

Clearly A is non-empty and bounded above.

An upper bound is given, for example, by $b := x + 1$. Indeed, since we are assuming $x \geq 0$, then $x + 1 \geq 1$. In particular we have

$$(x + 1)^k \geq x + 1 .$$

Let $t \in A$. Then

$$t^k < x < x + 1 < (x + 1)^k,$$

showing that $t < x + 1$.

By the Axiom of Completeness of $\mathbb{R}$, there exists $\alpha \in \mathbb{R}$ such that

$$\alpha = \sup A .$$

We claim that

$$\alpha^k = x . \tag{4.20}$$

Suppose by contradiction that (4.20) does not hold. We will need the formula: For all $a, b \in \mathbb{R}$ it holds

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^k + \ldots + ab^{k-2} + b^{k-1}) . \tag{4.21}$$

Formula (4.21) can be easily proven by induction on k. Since we are assuming that (4.20) does not hold, we have two cases:

- $\alpha^k < x$: We know that α is the supremum of A. We would like to violate this, by finding a number L which is larger than α, but still belongs to A. This means L has to satisfy

  $$\alpha < L , \quad L^k < x .$$

  We look for L of the form

  $$L_n := \alpha + \frac{1}{n}$$

  for $n \in \mathbb{N}$ to be chosen later. Clearly

  $$\alpha < L_n , \tag{4.22}$$

  for all $n \in \mathbb{N}$. We now search for $n_0 \in \mathbb{N}$ such that

  $$L_{n_0}^k < x .$$

  Using formula (4.21) with $a = \alpha$ and $b = L_{n_0}$ we obtain

  $$L_{n_0}^k - \alpha^k = \frac{1}{n_0}\left(L_{n_0}^{k-1} + L_{n_0}^{k-2}\alpha + \ldots + L_{n_0}\alpha^{k-2} + \alpha^{k-1}\right) . \tag{4.23}$$

  Now notice that (4.22) implies

  $$\alpha^j < L_{n_0}^j$$

for all $j \in \mathbb{N}$. Using this estimate on all the terms α^j appearing in the RHS of (4.23) we obtain

$$\begin{aligned} L_{n_0}^k - \alpha^k &= \frac{1}{n_0}\left(L_{n_0}^{k-1} + L_{n_0}^{k-2}\alpha + \ldots + L_{n_0}\alpha^{k-2} + \alpha^{k-1}\right) \\ &< \frac{1}{n_0}\left(L_{n_0}^{k-1} + L_{n_0}^{k-2}L_{n_0} + \ldots + L_{n_0}L_{n_0}^{k-2} + L_{n_0}^{k-1}\right) \\ &= \frac{k}{n_0}\, L_{n_0}^{k-1} \end{aligned}$$

Rearranging the above we get

$$L_{n_0}^k < \frac{k}{n_0}\, L_{n_0}^{k-1} + \alpha^k \,. \tag{4.24}$$

Now note that

$$L_{n_0} = \alpha + \frac{1}{n_0} < \alpha + 1 \,.$$

Therefore

$$L_{n_0}^{k-1} < (\alpha + 1)^{k-1} \,,$$

and from (4.24) we obtain

$$L_{n_0}^k < \frac{k}{n_0}\,(\alpha + 1)^{k-1} + \alpha^k \,.$$

We wanted to find $n_0 \in \mathbb{N}$ so that $L_{n_0}^k < x$. Therefore we impose

$$\frac{k}{n_0}\,(\alpha + 1)^{k-1} + \alpha^k < x \,,$$

and find that the above is satisfied for

$$n_0 > \frac{k(\alpha + 1)^{k-1}}{x - \alpha^k} \,. \tag{4.25}$$

Notice that the RHS in (4.25) is a positive real number, since $\alpha^k < x$ by assumption. Therefore, by the Archimedean Property of Theorem 4.11 Point 1, there exists $n_0 \in \mathbb{N}$ satisfying (4.25).
We have therefore shown the existence of $n_0 \in \mathbb{N}$ such that

$$\alpha < L_{n_0} \,, \quad L_{n_0}^k < x \,.$$

The above says that $L_{n_0} \in A$ and that

$$L_{n_0} > \alpha = \sup A \,,$$

which is a contradiction, as $\sup A$ is an upper bound for A.

- $\alpha^k > x$: We know that α is the supremum of A. We would like to find a contradiction, by finding an upper bound L for A which is smaller than α. This means L has to satisfy

$$L < \alpha \,, \quad L^k > x \,.$$

Such L is an upper bound for A: If $t \in A$ then

$$t^k < x < L^k \quad \Longrightarrow \quad t < L\,.$$

We therefore look for L of the form

$$L_n := \alpha - \frac{1}{n}$$

for $n \in \mathbb{N}$ to be chosen later. In this way

$$L_n < \alpha\,, \tag{4.26}$$

for all $n \in \mathbb{N}$. We now search for $n_0 \in \mathbb{N}$ such that

$$L_{n_0}^k > x\,.$$

Using formula (4.21) with $a = L_{n_0}$ and $b = \alpha$ we obtain

$$\alpha^k - L_{n_0}^k = \frac{1}{n_0}\left(\alpha^{k-1} + \alpha^{k-2}L_{n_0} + \ldots + \alpha L_{n_0}^{k-2} + L_{n_0}^{k-1}\right)\,. \tag{4.27}$$

Now notice that (4.26) implies

$$L_{n_0}^j < \alpha^j$$

for all $j \in \mathbb{N}$. Using this estimate on all the terms $L_{n_0}^j$ appearing in the RHS of (4.27) we obtain

$$\begin{aligned}\alpha^k - L_{n_0}^k &= \frac{1}{n_0}\left(\alpha^{k-1} + \alpha^{k-2}L_{n_0} + \ldots + \alpha L_{n_0}^{k-2} + L_{n_0}^{k-1}\right)\\ &< \frac{1}{n_0}\left(\alpha^{k-1} + \alpha^{k-2}\alpha + \ldots + \alpha\alpha^{k-2} + \alpha^{k-1}\right)\\ &= \frac{k}{n_0}\,\alpha^{k-1}\end{aligned}$$

Rearranging the above we get

$$L_{n_0}^k > \alpha^k - \frac{k}{n_0}\,\alpha^{k-1}\,.$$

We wanted to find $n_0 \in \mathbb{N}$ so that $L_{n_0}^k > x$. Therefore we impose

$$\alpha^k - \frac{k}{n_0}\,\alpha^{k-1} > x\,,$$

and find that the above is satisfied for

$$n_0 > \frac{k\alpha^{k-1}}{\alpha^k - x}\,. \tag{4.28}$$

Notice that the RHS in (4.28) is a positive real number, since $\alpha^k > x$ by assumption. Therefore, by the Archimedean Property of Theorem 4.11 Point 1, there exists $n_0 \in \mathbb{N}$ satisfying (4.28).
We have therefore shown the existence of $n_0 \in \mathbb{N}$ such that

$$L_{n_0} < \alpha\,, \quad L_{n_0}^k > x\,.$$

Condition $L_{n_0}^k > x$ says that L_{n_0} is an upper bound for A. At the same time it holds

$$L_{n_0} < \alpha = \sup A\,,$$

which is a contradiction, as $\sup A$ is the smallest upper bound for A.

Therefore, both cases $\alpha^k > x$ and $\alpha^k < x$ lead to a contradiction. Hence $\alpha^k = x$, concluding.

Definition 4.20: k-th root of a number

Let $x \in \mathbb{R}$ with $x \geq 0$ and $k \in \mathbb{N}$. The real number α such that

$$\alpha^k = x$$

is called the k-**th root** of x, and is denoted by

$$\sqrt[k]{x} := \alpha\,.$$

4.6 Cardinality

We have proven that the sets or rational numbers $\mathbb{Q}$ and irrational numbers $\mathcal{I}$ are both dense in $\mathbb{R}$, with

$$\mathbb{R} = \mathbb{Q} \cup \mathcal{I}\,.$$

From this result we might think that $\mathbb{R}$ is obtained by mixing $\mathbb{Q}$ and $\mathcal{I}$ in equal proportions. This is however false. We will see that $\mathbb{R}$ has much more elements than $\mathbb{Q}$. Therefore also the set of irrational numbers $\mathcal{I}$ is much larger than $\mathbb{Q}$.

To make the above discussion precise, we need to define what we mean by size of a set. For this, we need the concept of bijective function.

Definition 4.21: Bijective function

Let X, Y be sets and $f : X \to Y$ be a function. We say that:

- f is **injective** if it holds:
$$f(x) = f(y) \quad \Longrightarrow \quad x = y\,.$$
- f is **surjective** if it holds:
$$\forall y \in Y\,,\ \exists x \in X \ \text{ s.t. } \ f(x) = y\,.$$
- f is **bijective** if it is both **injective** and **surjective**.

In other words: A function $f:\ X \to Y$ is

- injective if any two different elements in X are mapped into two different elements in Y.
- surjective if every element in Y has at least one element in X associated via f.
- bijective if to each element in X we associate one and only one element in Y via f.

Example 4.22: Injectivity

Consider the sets
$$X = \{1, 2, 3\}\,, \quad Y = \{a, b, c, d, e\}\,.$$

- The function $f:\ X \to Y$ defined by
$$f(1) = c\,, \quad f(2) = a\,, \quad f(3) = e\,,$$
is injective.
- The function $g:\ X \to Y$ defined by
$$g(1) = c\,, \quad g(2) = a\,, \quad g(3) = c\,,$$
is not injective, since
$$g(1) = g(3) = c\,, \quad 1 \neq 3\,.$$
- The function $h:\ \mathbb{R} \to \mathbb{R}$ defined by
$$h(x) = x^2$$
is not injective, since
$$h(1) = h(-1) = 1\,, \quad 1 \neq -1\,.$$
- The function $l:\ \mathbb{R} \to \mathbb{R}$ defined by
$$l(x) = 2x$$
is injective, since
$$l(x) = l(y) \quad \Longrightarrow \quad 2x = 2y \quad \Longrightarrow \quad x = y\,.$$

Example 4.23: Surjectivity

Consider the sets

$$X = \{1, 2, 3, 4\}, \quad Y = \{a, b, c\}.$$

- The function $f : X \to Y$ defined by

  $$f(1) = c, \quad f(2) = a, \quad f(3) = a, \quad f(4) = b,$$

  is surjective.

- The function $g : X \to Y$ defined by

  $$g(1) = a, \quad g(2) = a, \quad g(3) = c, \quad g(4) = a,$$

  is not surjective, since there is no element $x \in X$ such that

  $$g(x) = b.$$

- The function $h : \mathbb{R} \to \mathbb{R}$ defined by

  $$h(x) = x^2$$

  is not surjective, since there is no $x \in \mathbb{R}$ such that

  $$h(x) = x^2 = -1.$$

- The function $l : \mathbb{R} \to [0, \infty)$ defined by

  $$l(x) = x^2$$

  is surjective, since for every $y \geq 0$ there exists $x \in \mathbb{R}$ such that

  $$l(x) = x^2 = y.$$

  This is true by Theorem 4.19.

Example 4.24: Bijectivity

- Let $X = \{1, 2, 3\}, Y = \{a, b, c\}$. The function $f : X \to Y$ defined by

  $$f(1) = c, \quad f(2) = a, \quad f(3) = b,$$

  is bijective, since it is both injective and surjective.

- Let $X = \{1, 2, 3\}, Y = \{a, b\}$. The function $g : X \to Y$ defined by

  $$g(1) = a, \quad g(2) = b, \quad g(3) = b,$$

  is not bijective, since it is not injective: we have

  $$g(2) = g(3) = b \quad 2 \neq 3.$$

- Let $X = \{1, 2\}, Y = \{a, b, c\}$. The function $h : \mathbb{R} \to \mathbb{R}$ defined by

$$h(1) = a\,, \quad h(2) = c\,,$$

is not bijective, since it is not surjective: there is no $x \in X$ such that

$$h(x) = b\,.$$

- Let $X = \{1, 2, 3\}, Y = \{a, b, c\}$. The function $l : \mathbb{R} \to [0, \infty)$ defined by

$$l(1) = a\,, \quad l(2) = a\,, \quad l(3) = b\,,$$

is not bijective, as it is neither injective nor surjective.

We are ready to define the size of a set.

Definition 4.25: Cardinality, finite, countable, uncountable

Let X be a set. The **cardinality** of X is the number of elements in X. We denote the cardinality of X by

$$|X| := \#\text{ of elements in }X\,.$$

Further, we say that:

- X is **finite** if there exists a natural number $n \in \mathbb{N}$ and a bijection

$$f : X \to \{1, 2, \dots, n\}\,.$$

In particular

$$|X| = n\,.$$

- X is **countable** if there exists a bijection

$$f : X \to \mathbb{N}\,.$$

In this case we denote the cardinality of X by

$$|X| = |\mathbb{N}|\,.$$

- X is **uncountable** if X is neither finite, nor countable.

In other words: A set X is

- finite, if X can be listed as

$$X = \{x_1, \dots, x_n\}$$

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

- countable, if X can be listed as
$$X = \{x_n \ : \ n \in \mathbb{N}\}.$$
- uncountable, if X cannot be listed.

Question 4.26

Is there an intermediate cardinality between finite and countable?

The answer is no, as shown in the next proposition.

Proposition 4.27

Let X be a countable set and $A \subseteq X$. Then either A is finite or countable.

Proof

If A is finite we are done. Therefore suppose A is not finite. Since X is countable there exists a bijection $f : \mathbb{N} \to X$. Let $n_1 \in \mathbb{N}$ be such that

$$n_1 = \min\{n \in \mathbb{N} \text{ s.t. } f(n) \in A\}.$$

Note that n_1 exists since f is surjective. Define

$$g(1) := f(n_1).$$

Now let

$$n_2 = \min\{n \in \mathbb{N} \text{ s.t. } n > n_1, \ f(n) \in A\}.$$

Notice that n_2 exists, since f is surjective and A is not finite. Set

$$g(2) := f(n_2).$$

Iterating, we define

$$n_k = \min\{n \in \mathbb{N} \text{ s.t. } n > n_{k-1}, \ f(n) \in A\}$$

and

$$g(k) := f(n_k).$$

In this way we have defined a function $g : \mathbb{N} \to A$. We have:

- g is injective: This is because g was defined thourgh f, and f is injective.

- g is surjective: If $x \in A$, by surjectivity of f there exists $\tilde{n} \in \mathbb{N}$ such that $f(\tilde{n}) = x$. Therefore

$$\tilde{n} \in \{n \in \mathbb{N} \text{ s.t. } f(n) \in A\},$$

so that $n_k = \tilde{n}$, for some $k \geq \tilde{n} - 1$.

Hence g is bijective, showing that A is countable.

Example 4.28

1. Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3\}$. The function $f : X \to Y$ defined by

$$f(1) = a, \quad f(2) = b, \quad f(3) = c,$$

is bijective. Therefore X is finite, with $|X| = 3$.

2. Let $X = \mathbb{N}$. The function $f : X \to \mathbb{N}$ defined by

$$f(n) := n,$$

is bijective. Therefore $X = \mathbb{N}$ is countable.

3. Let X be the set of even numbers

$$X = \{2n : n \in \mathbb{N}\}.$$

Define the map $f : X \to \mathbb{N}$ by

$$f(m) := \frac{m}{2}.$$

We have that:

- f is injective: $f(m) = f(k)$ implies that $m/2 = k/2$ which implies $m = k$.
- f is surjective: If $n \in \mathbb{N}$, then $f(2n) = n$.

Therefore f is bijective, showing that X is countable and $|X| = |\mathbb{N}|$.

4. Let $X = \mathbb{Z}$ the set of integers. Define $f : \mathbb{N} \to \mathbb{Z}$ by

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

For example

$$f(0) = 0, \quad f(1) = -1, \quad f(2) = 1, \quad f(3) = -2,$$
$$f(4) = 2, \quad f(5) = -3, \quad f(6) = 3, \quad f(7) = -4.$$

We have:

- f is injective: Indeed, suppose that $m \neq n$. If n and m are both even or both odd we have, respectively

$$f(m) = \frac{m}{2} \neq \frac{n}{2} = f(n)$$
$$f(m) = -\frac{m+1}{2} \neq -\frac{n+1}{2} = f(n)\,.$$

  If instead m is even and n is odd, we get

$$f(m) = \frac{m}{2} \neq -\frac{n+1}{2} = f(n)\,,$$

  since the LHS is positive and the RHS is negative. The case when m is odd and n even is similar.

- f is surjective: Let $z \in \mathbb{Z}$. If $z \geq 0$, then $m := 2z$ belongs to $\mathbb{N}$, is even, and

$$f(m) = f(2z) = z\,.$$

  If instead $z < 0$, then $m := -2z - 1$ belongs to $\mathbb{N}$, is odd, and

$$f(m) = f(-2z-1) = z\,.$$

Therefore f is bijective, showing that $\mathbb{Z}$ is countable and

$$|\mathbb{Z}| = |\mathbb{N}|\,.$$

We have seen that the sets $\mathbb{N}$ and $\mathbb{Z}$ are countable. What about $\mathbb{Q}$? To study this case, we need the following result.

Proposition 4.29

Let the set A_n be countable for all $n \in \mathbb{N}$. Define

$$A = \bigcup_{n\in\mathbb{N}} A_n\,.$$

Then A is countable.

Proof

Since each A_i is countable, we can list their elements as

$$A_i = \{a_k^i \ : \ k \in \mathbb{N}\} = \{a_1^i, \, a_2^i, \, a_3^i, \, a_4^i, \, ...\}\,.$$

The proof that A is countable is based on a diagonal argument by Georg Cantor, see Wikipedia page. The idea of th is that we can list the elements of the sets A_i in an infinite square: In the first row we put the elements of A_1, in the second row the elements of A_2, and so on. Therefore the i-th row contains the elements of A_i. This procedure is illustrated in Figure 4.7. Therefore this infinite square contains all the elements of A. We then list all the elements of the square by looking at the diagonals, as shown in Figure 4.7. This procedure defines a function $f : \mathbb{N} \to A$. For example the first few terms of f are

$$f(1) = a_1^1\,, \quad f(2) = a_2^1\,, \quad f(3) = a_1^2\,, \quad f(4) = a_1^3\,.$$

Since f is injective and surjective, we have that A is countable.

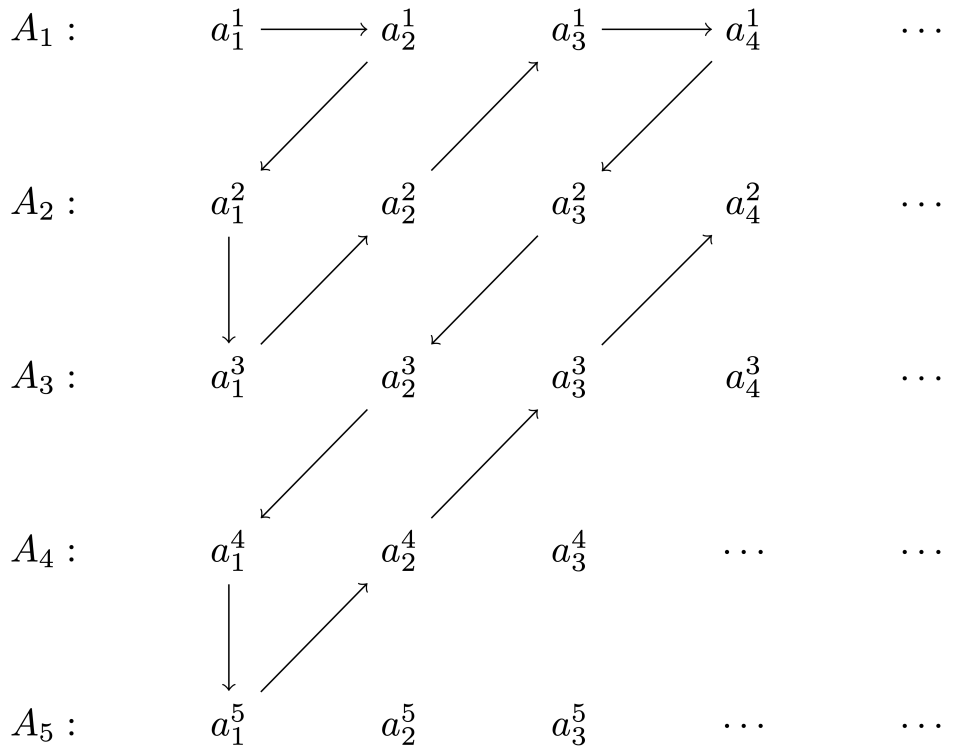

Figure 4.7: The i-th row contains all the elements $a_1^i, a_2^i, a_3^i, ...$ of the countable set A_i. We define the function $f : \mathbb{N} \to A$ by going throgh the square diagonally.

Theorem 4.30: $\mathbb{Q}$ is countable

The set of rational numbers $\mathbb{Q}$ is countable.

Proof

For $i \in \mathbb{N}$ define the sets

$$L_i := \left\{ \frac{m}{i} \ : \ m \in \mathbb{Z} \right\}.$$

We have that $f : L_i \to \mathbb{Z}$ defined by

$$f\left(\frac{m}{i}\right) := m$$

is a bijection. As $\mathbb{Z}$ is countable, we deduce that L_i is countable. Therefore the set L defined by

$$L := \bigcup_{i \in \mathbb{N}} L_i$$

is countable by Proposition 4.29. Clearly we have

$$\mathbb{Q} \subseteq L.$$

Since $\mathbb{Q}$ is not finite, by Proposition 4.27 we conclude that $\mathbb{Q}$ is countable.

We have proven that the sets

$$\mathbb{N}, \quad \mathbb{Z}, \quad \mathbb{Q},$$

are all countable. What about $\mathbb{R}$?

Theorem 4.31: $\mathbb{R}$ is uncountable

The set of Real Numbers $\mathbb{R}$ is **uncountable**.

Proof

Suppose by contradiction $\mathbb{R}$ is countable. Then there exists a bijection $f : \mathbb{N} \to \mathbb{R}$, meaning that we can list the elements of $\mathbb{R}$ as

$$\mathbb{R} = \{x_1, x_2, x_3, x_4, x_5, \ldots\}.$$

Let I_1 be a closed interval such that

$$x_1 \notin I_1.$$

Let I_2 be another closed interval, contained in I_1, and such that $x_2 \notin I_2$. Such interval exists, because I_1 contains two disjoint closed intervals: hence x_2 can be at most in one of these two intervals. To

summarize, we have

$$x_1 \notin I_1\,, \quad x_2 \notin I_2\,, \quad I_2 \subseteq I_1\,.$$

We can iterate this procedure, and construct a sequence of nested intervals I_n such that

$$I_{n+1} \subseteq I_n\,, \quad x_n \notin I_n\,,$$

for all $n \in \mathbb{N}$, see Figure 4.8. Since $x_k \notin I_k$, we conclude that

$$x_k \notin \bigcap_{n=1}^{\infty} I_n\,, \quad \forall\, k \in \mathbb{N}\,.$$

As the points x_k are all the elements of $\mathbb{R}$, we conclude that

$$\bigcap_{n=1}^{\infty} I_n = \emptyset\,.$$

However the Nested Interval Property of Theorem 4.14 implies that

$$\bigcap_{n=1}^{\infty} I_n \neq \emptyset\,,$$

yielding a contradiction. Therefore $\mathbb{R}$ is uncountable.

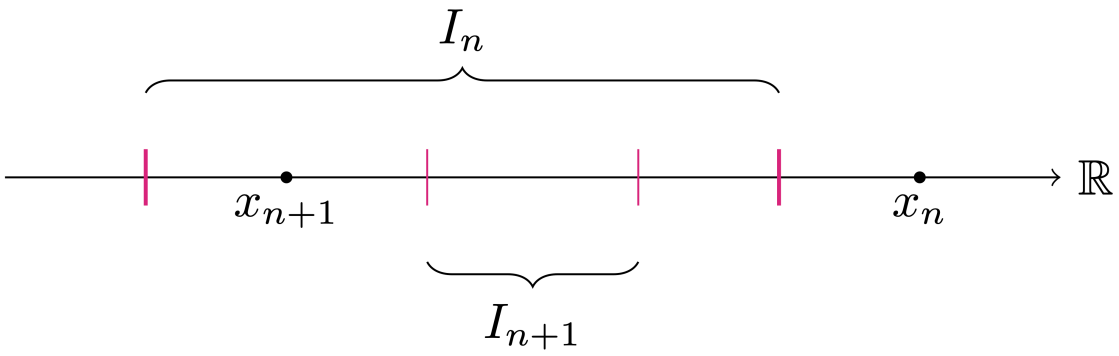

Figure 4.8: The intervals I_n are nested, and can be chosen so that $x_n \notin I_n$.

As a corollary we obtain that also the irrational numbers are uncountable.

Theorem 4.32

The set of irrational numbers

$$\mathcal{I} := \mathbb{R} \setminus \mathbb{Q}$$

is uncountable.

Proof

In Theorems 4.30, 4.31 we have shown that $\mathbb{R}$ in uncountable and $\mathbb{Q}$ is countable. Suppose by contradiction that $\mathcal{I}$ is countable. Then

$$\mathbb{Q} \cup \mathcal{I}$$

is countable by Proposition 4.29, being union of countable sets. Since by definition

$$\mathbb{R} = \mathbb{Q} \cup \mathcal{I},$$

we conclude that $\mathbb{R}$ is countable. Contradiction.

5 Complex Numbers

We have seen that $\sqrt{x}$ exists in $\mathbb{R}$ for all for $x \geq 0$. We defined

$$\sqrt{x} := \alpha\,, \quad \alpha := \sup\{t \in \mathbb{R} : \ t^2 < x\}\,,$$

and proved that

$$\alpha^2 = x\,.$$

This procedure was possible for $x \geq 0$.

Question 5.1

Is there a number $\alpha \in \mathbb{R}$ such that

$$\alpha^2 = -1 \ ? \tag{5.1}$$

The answer to the above question is no. This is because $\mathbb{R}$ is an ordered field, and from axiom (MO) it follows that:

$$x^2 \geq 0\,, \quad \forall\, x \in \mathbb{R}\,.$$

However we would still like to solve equation (5.1) somehow. To do this, we introduce the **imaginary numbers** or **complex numbers**. We define i to be that *number* such that

$$i^2 = -1\,.$$

Formally, we can also think of $i = \sqrt{-1}$. We can use this speacial number to define the square root of a negative number $x < 0$:

$$\sqrt{x} := i\sqrt{-x}\,.$$

Note that $\sqrt{-x}$ is properly defined in $\mathbb{R}$, because $-x > 0$ if $x < 0$.

5.1 The field $\mathbb{C}$

We would like to be able to do calculations with the newly introduced complex numbers, and investigate their properties. We can introduce them rigorously as a field, as we did for $\mathbb{R}$.

Definition 5.2: Complex Numbers

The set of complex numbers $\mathbb{C}$ is defined as

$$\mathbb{C} := \mathbb{R} \oplus i\mathbb{R} := \{x \oplus iy : \ x, y \in \mathbb{R}\}.$$

In the above the symbol $\oplus$ is used to denote the pair

$$x \oplus iy = (x, y)$$

with $x, y \in \mathbb{R}$. This means that x and y play different *roles*.

Definition 5.3

For a complex number

$$z = x \oplus iy \in \mathbb{C}$$

we say that

- x is the **real part** of z, and denote it by

$$x = \mathrm{Re}(z)$$

- y is the **imaginary part** of z, and denote it by

$$y = \mathrm{Im}(z)$$

We say that

- If $\mathrm{Re}\, z = 0$ then z is a **purely imaginary** number.
- If $\mathrm{Im}\, z = 0$ then z is a **real** number.

In order to make the set $\mathbb{C}$ into a field, we first have to define the two binary operations of addition $+$ and multiplication $\cdot$,

$$+, \cdot \ : \ \mathbb{C} \times \mathbb{C} \to \mathbb{C}\,.$$

Then we need to prove that these operations satisfy all the field axioms.

Definition 5.4: Addition in $\mathbb{C}$

Let $z_1, z_2 \in \mathbb{C}$, so that

$$z_1 = x_1 \oplus iy_1\ , \quad z_2 = x_2 \oplus iy_2\ ,$$

for some $x_1, x_2, y_1, y_2 \in \mathbb{R}$. We define the sum of z_1 and z_2 as

$$z_1 + z_2 = (x_1 \oplus iy_1) + (x_2 \oplus iy_2) := (x_1 + x_2) \oplus i\,(y_1 + y_2)$$

where the $+$ symbol on the right hand side is the addition operator in $\mathbb{R}$.

Clearly, $z_1 + z_2$ as defined above is an element of $\mathbb{C}$. Therefore $+$ defines a binary operation over $\mathbb{C}$.

Notation 5.5

From the above definition, we have that, for all $x, y \in \mathbb{R}$,

$$(x \oplus i0) + (0 \oplus iy) = x \oplus iy.$$

To simplify notation, we will write

$$x \oplus i0 = x\,, \qquad 0 \oplus iy = iy$$

and

$$x \oplus iy = x + iy\,.$$

We will also often swap i and y, writing equivalently

$$x + iy = x + yi\,.$$

We now want to define multiplication between complex numbers.

Remark 5.6: Formal calculation for multiplication in $\mathbb{C}$

How to define multiplication in $\mathbb{C}$? Whatever the definition may be, at least it has to give that that

$$i^2 = i \cdot i = -1\,.$$

Keeping the above in mind, let us do some formal calculations: For $z_1 = x_1 + iy_1, z_2 = x_2 + iy_2$ we have

$$\begin{aligned} z_1 \cdot z_2 &= (x_1 + iy_1) \cdot (x_2 + iy_2) \\ &= x_1 \cdot x_2 + x_1 \cdot iy_2 + x_2 \cdot iy_1 + y_1 \cdot i^2 y_2 \\ &= (x_1 \cdot x_2 - y_1 \cdot y_2) + i\,(x_1 \cdot y_2 + x_2 \cdot y_1) \end{aligned}$$

Remark 5.6 motivates the following definition of multiplication.

Definition 5.7: Multiplication in $\mathbb{C}$

Let $z_1, z_2 \in \mathbb{C}$, so that

$$z_1 = x_1 \oplus iy_1\,, \qquad z_2 = x_2 \oplus iy_2\,,$$

for some $x_1, x_2, y_1, y_2 \in \mathbb{R}$. We define the multiplication of z_1 and z_2 as

$$z_1 \cdot z_2 = (x_1 + iy_1) \cdot (x_2 + iy_2) := (x_1 \cdot x_2 - y_1 \cdot y_2) + i\,(x_1 \cdot y_2 + x_2 \cdot y_1)\,,$$

where the operations + and · on the right hand side are the operations in $\mathbb{R}$.

Clearly, $z_1 \cdot z_2$ as defined above is an element of $\mathbb{C}$. Therefore · defines a binary operation over $\mathbb{C}$.

Remark 5.8

To check that we have given a good definition of product, we should have that

$$i^2 = -1\,,$$

as expected. Indeed:

$$\begin{aligned} i^2 &= (0+1i)\cdot(0+1i) \\ &= (0\cdot 0 - 1\cdot 1) + (0\cdot 1 + 0\cdot 1)i = -1\,. \end{aligned}$$

Important

In view of Remark 5.8, we see that he formal calculations in Remark 5.6 are compatible with the definition of multiplication of complex numbers. Therefore, it is not necessary to memorize the multiplication formula, but it suffices to carry out calculations as usual, and replace i^2 by -1.

Example 5.9

Suppose we want to multiply the complex numbers

$$z = -2+3i\,, \quad w = 1-i\,.$$

Using the definition we compute

$$\begin{aligned} z\cdot w &= (-2+3i)\cdot(1-i) \\ &= (-2-(-3)) + (2+3)i \\ &= 1+5i\,. \end{aligned}$$

Alternatively, we can proceed formally as in Remark 5.6. We just need to recall that i^2 has to be replaced

with -1:

$$\begin{aligned} z \cdot w &= (-2+3i)\cdot(1-i) \\ &= -2+2i+3i-3i^2 \\ &= (-2+3)+(2+3)i \\ &= 1+5i\,. \end{aligned}$$

We now want to check that

$$(\mathbb{C}, +, \cdot)$$

is a field. All the field axioms are trivial to check, except for the existence of additive and multiplicative inverses.

Proposition 5.10: Additive inverse in $\mathbb{C}$

The neutral element of addition in $\mathbb{C}$ is the number

$$0 := 0 + 0i\,.$$

For any $z = x + iy \in \mathbb{C}$, the unique additive inverse is given by

$$-z := -x - iy\,.$$

The proof is immediate and is left as an exercise. The multiplication requires more care.

Remark 5.11: Formal calculation for multiplicative inverse

Let us first carry our some formal calculations. Let

$$z = x + iy \in \mathbb{C}\,, \quad z \neq 0\,.$$

First, note that

$$z \cdot 1 = (x+iy)\cdot(1+0i) = x+iy = z\,,$$

and therefore 1 is the neutral element of multiplication. Thus, the inverse of z should be a complex number $z^{-1} \in \mathbb{C}$ such that

$$z \cdot z^{-1} = 1\,.$$

We would like to define

$$z^{-1} = \frac{1}{x+iy}\,.$$

Such number does not belong to $\mathbb{C}$, as it is not of the form $a + ib$ for some $a, b \in \mathbb{R}$. However it is what the inverse should look like. Proceeding formally:

$$\begin{aligned}\frac{1}{x+iy} &= \frac{1}{x+iy} \cdot 1 \\ &= \frac{1}{x+iy} \cdot \frac{x-iy}{x-iy} \\ &= \frac{x-iy}{x^2-(iy)^2} \\ &= \frac{x-iy}{x^2+y^2} \\ &= \frac{x}{x^2+y^2} + i\,\frac{-y}{x^2+y^2}\,.\end{aligned}$$

The right hand side is an element of $\mathbb{C}$, and looks like a good candidate for z^{-1}.

Motivated by the above remark, we define inverses in $\mathbb{C}$ in the following way.

Proposition 5.12: Multiplicative inverse in $\mathbb{C}$

The neutral element of multiplication in $\mathbb{C}$ is the number

$$1 := 1 + 0i\,.$$

For any $z = x + iy \in \mathbb{C}$, the unique multiplicative inverse is given by

$$z^{-1} := \frac{x}{x^2+y^2} + i\,\frac{-y}{x^2+y^2}\,.$$

Proof

It is immediate to check that 1 is the neutral element of multiplication in $\mathbb{C}$. For the remaining part of the statement, set

$$w := \frac{x}{x^2+y^2} + i\,\frac{-y}{x^2+y^2}\,.$$

We need to check that $z \cdot w = 1$

$$\begin{aligned} z \cdot w &= (x+iy) \cdot \left(\frac{x}{x^2+y^2} + i \frac{-y}{x^2+y^2} \right) \\ &= \left(\frac{x^2}{x^2+y^2} - \frac{y \cdot (-y)}{x^2+y^2} \right) + i \left(\frac{x \cdot (-y)}{x^2+y^2} + \frac{xy}{x^2+y^2} \right) \\ &= 1 \,, \end{aligned}$$

so indeed $z^{-1} = w$.

Important

It is not necessary to memorize the formula for z^{-1}. Indeed one can just remember the trick of multiplying by

$$1 = \frac{x-iy}{x-iy} \,,$$

and proceed formally, as done in Remark 5.11.

Example 5.13

Let $z = 3 + 2i$. We want to compute z^{-1}. By the formula in Propostion 5.12 we immediately get

$$z^{-1} = \frac{3}{3^2+2^2} + \frac{-2}{3^2+2^2} i = \frac{3}{13} - \frac{2}{13} i \,.$$

Alternatively, we can proceed formally as in Remark 5.11

$$\begin{aligned} (3+2i)^{-1} &= \frac{1}{3+2i} \\ &= \frac{1}{3+2i} \frac{3-2i}{3-2i} \\ &= \frac{3-2i}{3^2+2^2} \\ &= \frac{3}{13} - \frac{2}{13} i \,, \end{aligned}$$

and obtain the same result.

We can now prove that $\mathbb{C}$ is a field.

Theorem 5.14

$(\mathbb{C}, +, \cdot)$ is a field.

Proof

We need to check that all field axioms hold. For the addition we have

- (A1) To show that $+$ is commutative, note that

$$\begin{aligned}(x+iy)+(a+ib) &= (x+a)+i(y+b)\\ &= (a+x)+i(b+y)\\ &= (a+ib)+(x+iy)\,,\end{aligned}$$

  where we used Definition 5.4 in the first and last equality, and the commutative property of the real numbers (which holds since by definition $\mathbb{R}$ is a field) in the second equality. Associativity can be checked in the same way.

- (A2) The neutral element of addition is 0, as stated in Proposition 5.10.

- (A3) Existence of additive inverses is given by Proposition 5.10.

For multiplication we have:

- (M1) Commutativity and associativity of product in $\mathbb{C}$ can be checked using Definition 5.7 and commutativity and associativity of sum and multiplication in $\mathbb{R}$.

- (M2) The neutral element of multiplication is 1, as stated in Propostion 5.12.

- (M3) Existence of multiplicative inverses is guaranteed by Proposition 5.12.

Finally one should check the associative property (AM). This is left as an exercise.

5.1.1 Division in $\mathbb{C}$

Suppose we want to divide two complex numbers $w, z \in \mathbb{C}, z \neq 0$, with

$$z = x + iy\,, \quad w = a + ib\,.$$

We have two options:

1. Use the formula for the inverse from Proposition 5.12 and compute

$$z^{-1} := \frac{x}{x^2+y^2} + i\,\frac{-y}{x^2+y^2}\,.$$

Then we use the multiplication formula of Definition 5.7 to compute

$$\begin{aligned}\frac{w}{z} &= w \cdot z^{-1} \\ &= (a+ib) \cdot \left(\frac{x}{x^2+y^2} + i \frac{-y}{x^2+y^2} \right) \\ &= \frac{(ax+by)+i(bx-ay)}{x^2+y^2}\end{aligned}$$

2. Proceed formally as in Remark 5.11, using the multiplication by 1 trick. We would have

$$\begin{aligned}\frac{w}{z} &= \frac{a+ib}{x+iy} \\ &= \frac{a+ib}{x+iy}\frac{x-iy}{x-iy} \\ &= \frac{(ax+by)+i(bx-ay)}{x^2+y^2}\end{aligned}$$

Example 5.15

Let $w = 1+i$ and $z = 3-i$. We compute $\frac{w}{z}$ using the two options we have:

1. Using the formula for the inverse from Proposition 5.12 we compute

$$\begin{aligned}z^{-1} &= \frac{x}{x^2+y^2} + i\frac{-y}{x^2+y^2} \\ &= \frac{3}{3^2+1^2} - i\frac{-1}{3^2+1^2} \\ &= \frac{3}{10} + \frac{1}{10}i\end{aligned}$$

and therefore

$$\begin{aligned}\frac{w}{z} &= w \cdot z^{-1} \\ &= (1+i)\left(\frac{3}{10} + \frac{1}{10}i\right) \\ &= \left(\frac{3}{10} - \frac{1}{10}\right) + \left(\frac{1}{10} + \frac{3}{10}\right)i \\ &= \frac{2}{10} + \frac{4}{10}i \\ &= \frac{1}{5} + \frac{2}{5}i\end{aligned}$$

2. We proceed formally, using the multiplication by 1 trick. We have

$$\begin{aligned}\frac{w}{z} &= \frac{1+i}{3-i} \\ &= \frac{1+i}{3-i}\frac{3+i}{3+i} \\ &= \frac{3-1+(3+1)i}{3^2+1^2} \\ &= \frac{2}{10}+\frac{4}{10}i \\ &= \frac{1}{5}+\frac{2}{5}i\end{aligned}$$

5.1.2 $\mathbb{C}$ is not ordered

We have seen that $(\mathbb{C}, +, \cdot)$ is a field. One might wonder whether $\mathbb{C}$ is also an ordered field. It turns out that this is not the case.

Theorem 5.16

The field $(\mathbb{C}, +, \cdot)$ is not ordered.

Proof

Suppose that $\mathbb{C}$ is an ordered field, that is, there exists an order relation $\leq$ on $\mathbb{C}$ compatible with the operations $+$ and $\cdot$. By axiom (MO) it follows that for all elements $z \in \mathbb{C}, z \neq 0$, we have that $z^2 > 0$. But since $i^2 = -1 < 0$, we get a contradiction.

Hence, it is not possible to compare two complex numbers.

5.1.3 Completeness of $\mathbb{C}$

One might also wonder whether $\mathbb{C}$ is complete. Our definition of completeness uses the notion of supremum, which only makes sense if the field is ordered. This is not the case for $\mathbb{C}$ as we have seen in Theorem 5.16.

Still, it is possible to give a different definition of completeness using the notion of Cauchy sequence. In ordered fields, this new definition of completeness is equivalent to the definition which uses the supremum.

The new definition of completeness with Cauchy sequences also makes sense in non-ordered fields. We will see that $\mathbb{C}$ is a complete field, according to this new definition.

5.2 Complex conjugates

When computing inverses, we used the trick to multiply by 1:

$$z^{-1} = \frac{1}{z} \cdot 1 = \frac{1}{x+iy} \cdot \frac{x-iy}{x-iy}.$$

The complex number $x - iy$ is obtained by changing the sign to the imaginary part of $z = x + iy$. We give a name to this operation.

Definition 5.17: Complex conjugate

Let $z = x + iy$. We call the **complex conjugate** of z, denoted by $\bar{z}$, the complex number

$$\bar{z} = x - iy\,.$$

Example 5.18

We have the following conjugates:

$$\overline{3+4i} = 3-4i\,, \qquad \overline{3-4i} = 3+4i\,,$$
$$\overline{-3+4i} = -3-4i\,, \qquad \overline{-3-4i} = -3+4i\,,$$
$$\overline{3} = 3\,, \qquad \overline{4i} = -4i\,.$$

Complex conjugates have the following properties:

Theorem 5.19

For all $z_1, z_2 \in \mathbb{C}$ it holds:

- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
- $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$

Proof

Let $z_1, z_2 \in \mathbb{C}$. Then

$$z_1 = x_1 + iy_1\,, \quad z_2 = x_2 + iy_2\,,$$

for some $x_1, y_1, x_2, y_2 \in \mathbb{R}$.

- Using the definition of addition in $\mathbb{C}$ and of conjugate,

$$\begin{aligned}\overline{z_1+z_2} &= \overline{(x_1+iy_1)+(x_2+iy_2)}\\ &= \overline{(x_1+x_2)+i(y_1+y_2)}\\ &= (x_1+x_2)-i(y_1+y_2)\\ &= (x_1-iy_1)+(x_2-iy_2)\\ &= \overline{x_1+iy_1}+\overline{x_2+iy_2}\\ &= \overline{z_1}+\overline{z_2}\,.\end{aligned}$$

- Using the definition of multiplication in $\mathbb{C}$ and of conjugate,

$$\begin{aligned}\overline{z_1\cdot z_2} &= \overline{(x_1+iy_1)\cdot(x_2+iy_2)}\\ &= \overline{(x_1x_2-y_1y_2)+i(x_1y_2+x_2y_1)}\\ &= (x_1x_2-y_1y_2)-i(x_1y_2+x_2y_1)\\ &= (x_1-iy_1)\cdot(x_2-iy_2)\\ &= \overline{z_1}\cdot\overline{z_2}\end{aligned}$$

Example 5.20

Let $z_1 = 3-4i$ and $z_2 = -2+5i$. Then

- Let us check that

$$\overline{z_1+z_2} = \overline{z_1}+\overline{z_2}$$

Indeed, we have

$$z_1+z_2 = 1+i \quad\Longrightarrow\quad \overline{z_1+z_2} = 1-i\,.$$

On the other hand

$$\overline{z_1} = 3+4i\,,\quad \overline{z_2} = -2-5i \quad\Longrightarrow\quad \overline{z_1}+\overline{z_2} = 1-i\,.$$

- Let us check that

$$\overline{z_1\cdot z_2} = \overline{z_1}\cdot\overline{z_2}$$

Indeed,

$$\begin{aligned}z_1\cdot z_2 &= (3+4i)\cdot(-2+5i)\\ &= (-6+20)+(8+15)i\\ &= 14+23i\end{aligned}$$

so that

$$\overline{z_1 \cdot z_2} = 14 - 23i$$

On the other hand:

$$\begin{aligned}\overline{z_1} \cdot \overline{z_2} &= (3 + 4i) \cdot (-2 - 5i) \\ &= (-6 + 20) + (-15 - 8)i \\ &= 14 - 23i\end{aligned}$$

5.3 The complex plane

We can depict a real number x as a point on the one-dimensional real line $\mathbb{R}$. The distance between two real numbers $x, y \in \mathbb{R}$ on the real line is given by $|x - y|$, see Figure 5.1.

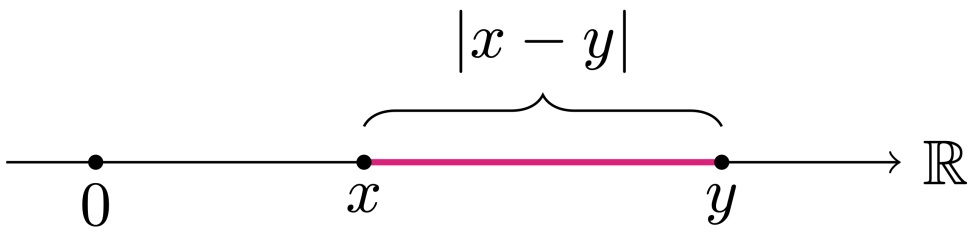

Figure 5.1: Two points x and y on the real line $\mathbb{R}$. Their distance is $|x - y|$.

We would like to do something similar for the complex numbers, but the point

$$z = x + iy\,, \quad x,\, y \in \mathbb{R}\,.$$

We therefore depict $z = z + iy$ in the two-dimensional plane at the point with (Cartesian) coordinates (x, y). This two-dimensional plane in which we can depict all complex numbers is called the **complex plane**. The origin of such plane, with coordinates $(0, 0)$, corresponds to the complex number

$$0 + 0i = 0\,,$$

see Figure 5.2.

5.3.1 Distance on $\mathbb{C}$

The Cartesian representation allows us to introduce a distance between two complex numbers. Let us start with the distance between a complex number $z = x + iy$ and 0. By Pythagoras Theorem this distance is given by

$$\sqrt{x^2 + y^2}\,,$$

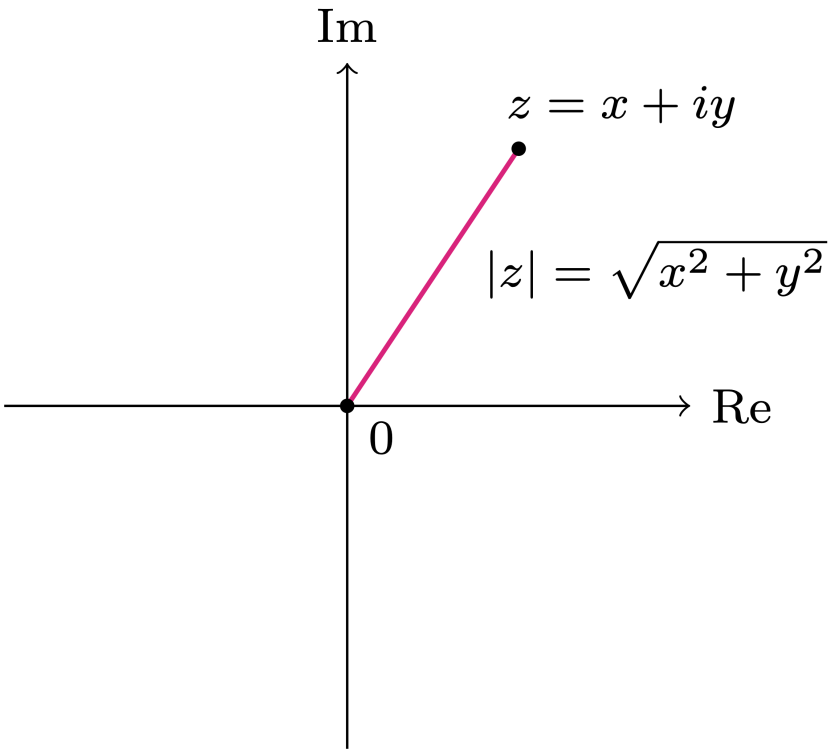

Figure 5.2: A point $z = x + iy \in \mathbb{C}$ can be represented on the complex plane by the point of coordinates (x, y). The distance between z and 0 is given by $|z| = \sqrt{z^2 + y^2}$.

see Figure 5.2. We give a name to this quantity.

Definition 5.21: Modulus

The **modulus** of a complex number $z = x + iy$ is defined by

$$|z| := \sqrt{x^2 + y^2}\,.$$

Note that the distance between z and 0 is always a non-negative number.

Remark 5.22: Modulus of Real numbers

A real number $x \in \mathbb{R}$ can be written as

$$x = x + 0i \in \mathbb{C}\,.$$

Hence the modulus of x is given by

$$|x| = \sqrt{x^2 + 0^2} = \sqrt{x^2}\,.$$

The above coincides with the absolute value of x. This explains why the notation for modulus in $\mathbb{C}$ is the same as the one for absolute value in $\mathbb{R}$.

We can now define the distance between two complex numbers.

Definition 5.23: Distance in $\mathbb{C}$

Given $z_1, z_2 \in \mathbb{C}$, we define the **distance** between z_1 and z_2 as the quantity

$$|z_1 - z_2|\,.$$

The geometric intuition of why the quantity $|z_1 - z_2|$ is defined as the distance between z_1 and z_2 is given in Figure 5.3.

Theorem 5.24

Given $z_1, z_2 \in \mathbb{C}$, we have

$$|z_1 - z_2| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}\,.$$

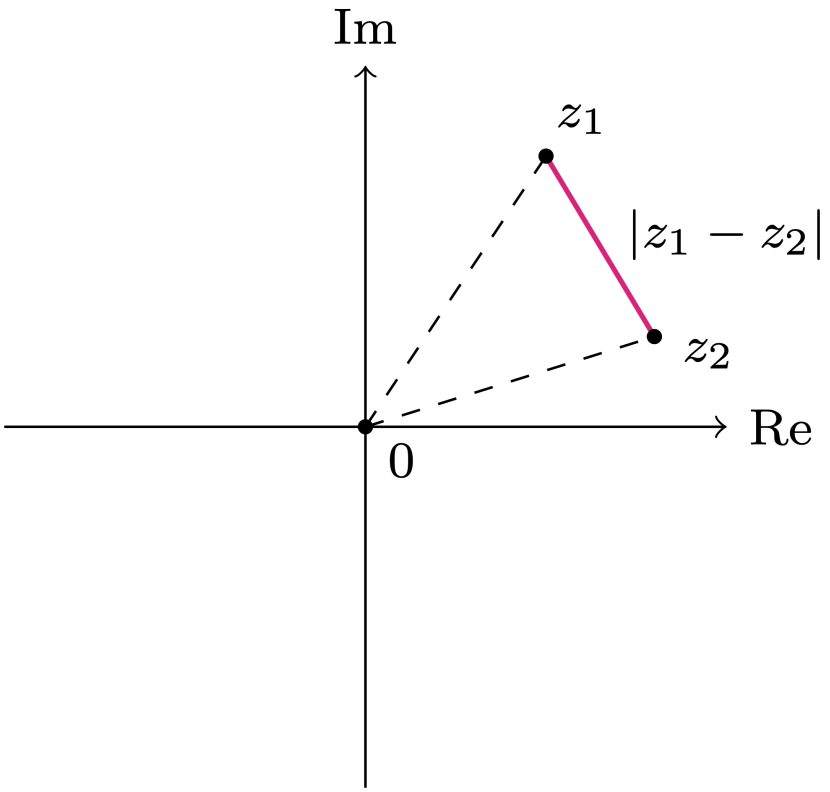

Figure 5.3: The difference $z_1 - z_2$ of the two points $z_1, z_2 \in \mathbb{C}$ is given by the magenta vector. We define $|z_1 - z_2|$ as the distance between z_1 and z_2.

Proof

We have

$$z_1 - z_2 = (x_1 - x_2) + i(y_1 - y_2)\,.$$

Therefore, by definition of modulus,

$$|z_1 - z_2| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}\,.$$

Example 5.25

The distance between

$$z = 2 - 4i\,, \quad w = -5 + i$$

is given by

$$\begin{aligned} |z - w| &= |(2 - 4i) - (-5 + i)| \\ &= |7 - 5i| \\ &= \sqrt{7^2 + (-5)^2} \\ &= \sqrt{74} \end{aligned}$$

5.3.2 Properties of modulus

The modulus has the following properties.

Theorem 5.26

Let $z, z_1, z_2 \in \mathbb{C}$. Then

1. $|z_1 \cdot z_2| = |z_1|\,|z_2|$
2. $|z^n| = |z|^n$ for all $n \in \mathbb{N}$
3. $z \cdot \bar{z} = |z|^2$

Proof

Part 1. We have

$$\begin{aligned} z_1 \cdot z_2 &= (x_1 + iy_1) \cdot (x_2 + iy_2) \\ &= (x_1 x_2 - y_1 y_2) + i(x_2 y_1 + x_1 y_2) \end{aligned}$$

and therefore

$$\begin{aligned}|z_1 \cdot z_2| &= \sqrt{(x_1x_2 - y_1y_2)^2 + (x_2y_1 + x_1y_2)^2} \\ &= \sqrt{x_1^2x_2^2 + y_1^2y_2^2 + x_2^2y_1^2 + x_1^2y_2^2}\,.\end{aligned}$$

On the other hand,

$$|z_1| = \sqrt{x_1^2 + y_1^2}\,, \quad |z_2| = \sqrt{x_2^2 + y_2^2}$$

so that

$$\begin{aligned}|z_1||z_2| &= \sqrt{x_1^2 + y_1^2}\sqrt{x_2^2 + y_2^2} \\ &= \sqrt{x_1^2x_2^2 + y_1^2y_2^2 + x_2^2y_1^2 + x_1^2y_2^2}\end{aligned}$$

proving that $|z_1 \cdot z_2| = |z_1||z_2|$.
Part 2. Exercise. It easily follows from Point 1 and induction.
Part 3. Let $z = x + iy$ for some $x, y \in \mathbb{R}$. Then,

$$\begin{aligned}z \cdot \bar{z} &= (x + iy)(x - iy) \\ &= x^2 - (iy)^2 \\ &= x^2 + y^2 \\ &= |z|^2\end{aligned}$$

The modulus in $\mathbb{C}$ satisfies the triangle inequality.

Theorem 5.27: Triangle inequality in $\mathbb{C}$

For all $x, y, z \in \mathbb{C}$,

1. $|x + y| \leq |x| + |y|$
2. $|x - z| \leq |x - y| + |y - z|$

Proof

Part 1. Suppose that $x = a + ib$ and $y = c + id$ for $a, b, c, d \in \mathbb{R}$. Then,

$$|x + y| = |(a + c) + i(b + d)| = \sqrt{(a + c)^2 + (b + d)^2}\,.$$

Therefore the inequality

$$|x + y| \leq |x| + |y| \tag{5.2}$$

is equivalent to

$$\sqrt{(a+c)^2+(b+d)^2} \leq \sqrt{a^2+b^2}+\sqrt{c^2+d^2}\,. \tag{5.3}$$

Now note that, for $A, B \in \mathbb{R}$, we have that

$$A^2 \leq B^2 \quad \Longrightarrow \quad |A| \leq |B|\,. \tag{5.4}$$

In the two reverse implications $\Longleftarrow$ below we will use (5.4):

$$\begin{aligned}
&\sqrt{(a+c)^2+(b+d)^2} \leq \sqrt{a^2+b^2}+\sqrt{c^2+d^2}\\
\Longleftarrow\ &(a+c)^2+(b+d)^2 \leq \left(\sqrt{a^2+b^2}+\sqrt{c^2+d^2}\right)^2\\
\Longleftrightarrow\ &a^2+2ac+c^2+b^2+2bd+d^2 \leq a^2+b^2+2\sqrt{a^2+b^2}\sqrt{c^2+d^2}+c^2+d^2\\
\Longleftrightarrow\ &ac+bd \leq \sqrt{a^2+b^2}\sqrt{c^2+d^2}\\
\Longleftarrow\ &(ac+bd)^2 \leq \left(a^2+b^2\right)\left(c^2+d^2\right)\\
\Longleftrightarrow\ &a^2c^2+2abcd+b^2d^2 \leq a^2c^2+a^2d^2+b^2c^2+b^2d^2\\
\Longleftrightarrow\ &a^2d^2+b^2c^2-2abcd \geq 0\\
\Longleftrightarrow\ &(ad-bc)^2 \geq 0.
\end{aligned}$$

This last statement is clearly true, since $ad-bc \in \mathbb{R}$. Therefore (5.3) holds, and so (5.2) follows.
Part 2. Using (5.2) we estimate

$$|x-z| = |x-y+y-z| \leq |x-y|+|y-z|.$$

Remark 5.28: Geometric interpretation of triangle inequality

We finally have a justification of why the inequality

$$|x-z| \leq |x-y|+|y-z|$$

is called **triangle inequality**: By drawing three points $x, y, z \in \mathbb{C}$ in the complex plane, the distance between x and z is shorter than the distance to go from x to z via the point y, see Figure 5.4.

5.4 Polar coordinates

We have seen that we can identify a complex number $z = x+iy$ by a point in the complex plane with Cartesian coordinates (x, y). We can also specify the point (x, y) by using the so-called polar coordinates (ρ, θ), where

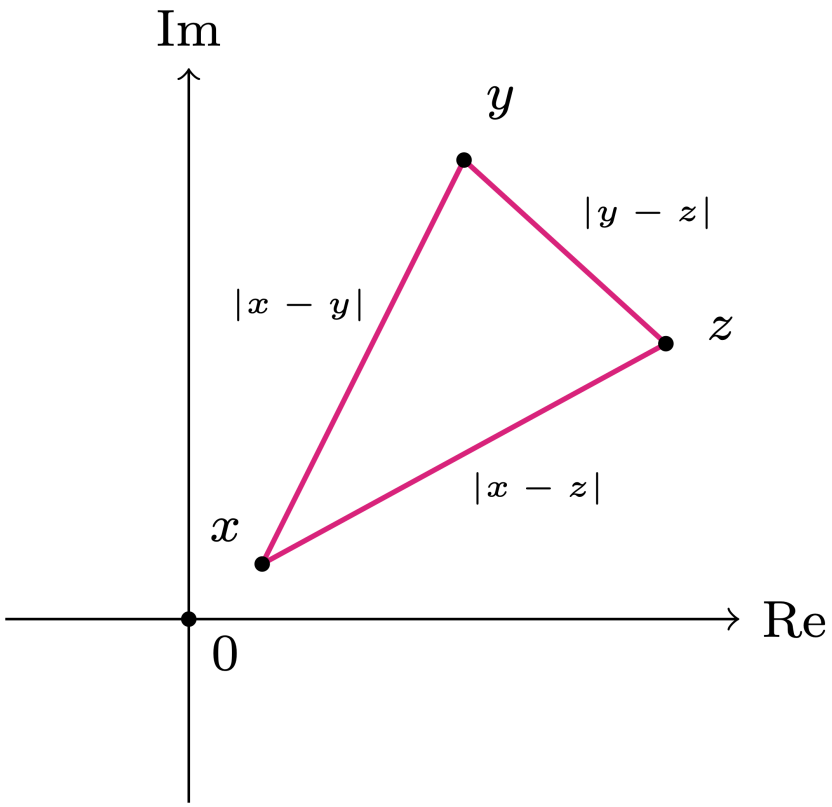

Figure 5.4: Let $x, y, z \in \mathbb{C}$. The distance between x and z is shorter than the distance to go from x to z via the point y.

- ρ is the distance between z and the origin

$$\rho = |z| = \sqrt{x^2 + y^2}$$

- θ is the angle between the line connecting the origin and z and the positive real axis, see Figure 5.5.

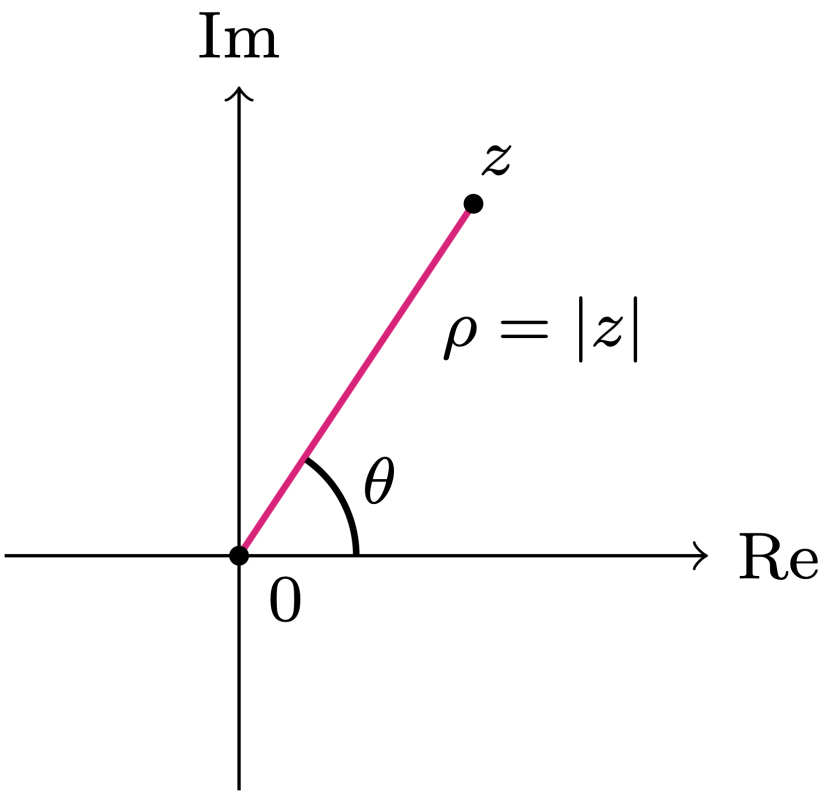

Figure 5.5: Polar coordinates (ρ, θ) for the complex number $z \in \mathbb{C}$.

We give such angle a name.

Definition 5.29: Argument

Let $z \in \mathbb{C}$. The angle θ between the line connecting the origin and z and the positive real axis is called the **argument** of z, and is denoted by

$$\theta := \arg(z)\,.$$

Warning

We always use angles in radians, not degrees. Make sure your calculator is set to radians if you want to use it to compute angles.

Remark 5.30: Principal Value

The argument of a complex number is not uniquely defined. We can always add an integer number of times 2π to the argument to specify the same point. We usually use the convention to choose the argument in the interval $(-\pi, \pi]$. This is called the **principal value** of the argument function. Therefore the complex numbers in the upper half plane have a positive argument, and in the lower half plane have a negative argument.

Example 5.31

We have the following arguments:

$$\arg(1) = 0 \qquad \arg(i) = \frac{\pi}{2}$$
$$\arg(-1) = \pi \qquad \arg(-i) = -\frac{\pi}{2}$$
$$\arg(1+i) = \frac{1}{4}\pi \qquad \arg(-1-i) = -\frac{3}{4}\pi$$

We can represent non-zero complex numbers in polar coordinates.

Theorem 5.32: Polar coordinates

Let $z \in \mathbb{C}$ with $z = x + iy$ and $z \neq 0$. Then

$$x = \rho\cos(\theta), \quad y = \rho\sin(\theta),$$

where

$$\rho = \sqrt{x^2 + y^2}, \quad \theta = \arg(z).$$

The proof of Theorem 5.32 is trivial, and is based on basic trigonometry and definition of $\arg(z)$. Complex numbers in polar form can be useful. We give a name to such polar form.

Definition 5.33: Trigonometric form

Let $z \in \mathbb{C}$. The trigonometric form of z is

$$z = |z|\left[\cos(\theta) + i\sin(\theta)\right],$$

where $\theta = \arg(z)$.

Let us make an example.

Example 5.34

Suppose that we have polar coordinates

$$\rho = \sqrt{8}\,, \quad \theta = \frac{3}{4}\pi$$

We compute

$$x = \rho\cos(\theta) = \sqrt{8}\cos\left(\frac{3}{4}\pi\right) = -\frac{\sqrt{8}\sqrt{2}}{2} = -2$$
$$y = \rho\sin(\theta) = \sqrt{8}\sin\left(\frac{3}{4}\pi\right) = \frac{\sqrt{8}\sqrt{2}}{2} = 2\,.$$

The complex number z corresponding to the polar coordinates (ρ, θ) is

$$z = x + iy = -2 + 2i\,.$$

The trigonometric form of z is

$$z = \sqrt{8}\left[\cos\left(\frac{3}{4}\pi\right) + i\sin\left(\frac{3}{4}\pi\right)\right].$$

As a consequence of Theorem 5.32 we obtain a formula for computing the argument.

Corollary 5.35: Computing $\arg(z)$

Let $z \in \mathbb{C}$ with $z = x + iy$ and $z \neq 0$. Then

$$\arg(z) = \begin{cases} \arctan\left(\dfrac{y}{x}\right) & \text{if } x > 0 \\ \arctan\left(\dfrac{y}{x}\right) + \pi & \text{if } x < 0 \text{ and } y \geq 0 \\ \arctan\left(\dfrac{y}{x}\right) - \pi & \text{if } x < 0 \text{ and } y < 0 \\ \dfrac{\pi}{2} & \text{if } x = 0 \text{ and } y > 0 \\ -\dfrac{\pi}{2} & \text{if } x = 0 \text{ and } y < 0 \end{cases}$$

where arctan is the inverse of tan.

Proof

Using the polar coordinates formulas from Theorem 5.32 we have

$$\frac{y}{x} = \frac{\rho \sin(\theta)}{\rho \cos(\theta)} = \tan(\theta)\,.$$

The thesis can be obtained by carefully inverting the tangent.

Example 5.36

We want to compute the arguments of the complex numbers

$$3+4i\,, \quad 3-4i\,, \quad -3+4i\,, \quad -3-4i\,.$$

Using the formula for arg in Corollary 5.35 we have

$$\begin{aligned}
\arg(3+4i) &= \arctan\left(\frac{4}{3}\right) \\
\arg(3-4i) &= \arctan\left(-\frac{4}{3}\right) = -\arctan\left(\frac{4}{3}\right) \\
\arg(-3+4i) &= \arctan\left(-\frac{4}{3}\right) + \pi = -\arctan\left(\frac{4}{3}\right) + \pi \\
\arg(-3-4i) &= \arctan\left(\frac{4}{3}\right) - \pi
\end{aligned}$$

5.5 Exponential form

We have seen that we can represent complex numbers in

- Cartesian form
- Trigonometric form

We now introduce a third way of representing complex numbers: the exponential form. For this, we need Euler's identity:

Theorem 5.37: Euler's identity

For all $\theta \in \mathbb{R}$ it holds

$$e^{i\theta} = \cos(\theta) + i\sin(\theta)\,.$$

Proof

The proof of this theorem uses Taylor power series. Note that we have not introduced what series are, yet, so we just assume that everything below makes sense and actually exists. We have the following Taylor series at $x_0 = 0$ that you might know from calculus:

$$\begin{aligned} e^x &= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \frac{x^6}{6!} + \frac{x^7}{7!} + \dots \\ \sin(x) &= \frac{x}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots \\ \cos(x) &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \dots \end{aligned}$$

The above identities also holds for $x \in \mathbb{C}$. Hence we can substitute $x = i\theta$ in the series for e^x to obtain

$$\begin{aligned} e^{i\theta} &= 1 + i\theta + \frac{(i\theta)^2}{2!} + \frac{(i\theta)^3}{3!} + \frac{(i\theta)^4}{4!} + \frac{(i\theta)^5}{5!} + \frac{(i\theta)^6}{6!} + \frac{(i\theta)^7}{7!} \dots \\ &= 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + i\frac{\theta^5}{5!} - \frac{\theta^6}{6!} - i\frac{\theta^7}{7!} + \dots \\ &= \cos(\theta) + i\sin(\theta), \end{aligned}$$

where we used that $i^2 = -1$ in the second equality, and the third equality follows by observing that all terms with an even power of θ are exactly the terms in the expansion of $\cos(\theta)$ and all terms with an odd power of θ are exactly the terms in the expansion of $\sin(\theta)$ multiplied by i.

Theorem 5.38

For all $\theta \in \mathbb{R}$ it holds

$$\left|e^{i\theta}\right| = 1\,.$$

Proof

From Euler's identity in Theorem 5.37 we get

$$\left|e^{i\theta}\right| = |\cos(\theta) + i\sin(\theta)| = \sqrt{\cos^2(\theta) + \sin^2(\theta)} = 1\,.$$

Theorem 5.39

Let $z \in \mathbb{C}$ with $z = x + iy$ and $z \neq 0$. Then

$$z = \rho e^{i\theta}\,,$$

where

$$\rho = \sqrt{x^2 + y^2} = |z|\,, \quad \theta = \arg(z)\,.$$

Proof

By Theorem 5.32 we have

$$x = \rho\cos(\theta)\,, \quad y = \rho\sin(\theta)\,.$$

Hence

$$\begin{aligned} z &= x + iy \\ &= \rho\cos(\theta) + i\rho\sin(\theta) \\ &= \rho e^{i\theta}\,, \end{aligned}$$

where in the last line we used Euler's identity in Theorem 5.37.

Definition 5.40: Exponential form

A complex number $z \in \mathbb{C}$ is in **exponential form** if

$$z = \rho e^{i\theta} = |z|\, e^{i\arg(z)}\,.$$

Example 5.41

From Example 5.34 we know that

$$z = -2 + 2i$$

can be written in trigonometric form as

$$z = \sqrt{8}\left[\cos\left(\frac{3}{4}\pi\right) + i\sin\left(\frac{3}{4}\pi\right)\right].$$

By Euler's identity we hence obtain the exponential form

$$z = \sqrt{8}e^{i\frac{3}{4}\pi}\,.$$

Remark 5.42: Periodicity of exponential

For all $k \in \mathbb{Z}$ we have

$$e^{i\theta} = e^{i(\theta+2\pi k)}\,. \tag{5.5}$$

As we did for the principal value of the argument, also for the exponential form we select $\theta \in (-\pi, \pi]$. In particular equation (5.5) is saying that the complex exponential is 2π-periodic.

Equation (5.5) follows immediately by Euler's identity and periodicity of cos and sin, since

$$\begin{aligned} e^{i(\theta+2\pi k)} &= \cos(\theta + 2\pi k) + i\sin(\theta + 2\pi k) \\ &= \cos(\theta) + i\sin(\theta) = e^{i\theta}\,. \end{aligned}$$

The exponential for is very useful for computing products and powers of complex numbers.

Proposition 5.43

Let $z, z_1, z_2 \in \mathbb{C}$ and suppose that

$$z = \rho e^{i\theta}\,, \quad z_1 = \rho_1 e^{i\theta_1}\,, \quad z_2 = \rho_2 e^{i\theta_2}\,.$$

We have

$$z_1 \cdot z_2 = \rho_1\rho_2 e^{i(\theta_1+\theta_2)}\,, \quad z^n = \rho^n e^{in\theta}\,,$$

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

The proof follows immediately by the properties of the exponential. Let us see some applications of Propostion 5.43.

Example 5.44

Suppose we want to compute $(-2+2i)^4$. We could do this by means of the binomial theorem:

$$\begin{aligned} (-2+2i)^4 &= (-2)^4 + \binom{4}{1}(-2)^3\cdot 2i + \binom{4}{2}(-2)^2\cdot(2i)^2 + \binom{4}{3}(-2)\cdot(2i)^3 + (2i)^4 \\ &= 16 - 4\cdot 8\cdot 2i - 6\cdot 4\cdot 4 + 4\cdot 2\cdot 8i + 16 \\ &= 16 - 64i - 96 + 64i + 16 = -64\,. \end{aligned}$$

Using the exponential form simplifies this calculation. Indeed, we know that

$$-2+2i = \sqrt{8}e^{i\frac{3}{4}\pi}$$

by Example 5.41. Hence

$$(-2+2i)^4 = \left(\sqrt{8}e^{i\frac{3}{4}\pi}\right)^4 = 8^2 e^{i3\pi} = -64\,,$$

where we used that

$$e^{i3\pi} = e^{i\pi} = \cos(\pi) + i\sin(\pi) = -1$$

by 2π periodicity of e^z and Euler's identity.

Example 5.45

Suppose we want to compute

$$i^i\,.$$

It is not even clear how to do this calculation in Cartesian form. However, we know that

$$|i| = 1\,, \quad \arg(i) = \frac{\pi}{2}\,.$$

Hence we can write i in exponential form

$$i = |i|e^{i\arg(i)} = e^{i\frac{\pi}{2}}\,.$$

Therefore

$$i^i = \left(e^{i\frac{\pi}{2}}\right)^i = e^{i^2\frac{\pi}{2}} = e^{-\frac{\pi}{2}}\,.$$

5.6 Fundamental Theorem of Algebra

We started the introduction to complex numbers with the following question:

Question 5.46

Is there a number $x \in \mathbb{R}$ such that

$$x^2 = -1\ ? \tag{5.6}$$

The answer is no. For this reason we introduced the complex number i, which satisfies

$$i^2 = -1\,.$$

Therefore (5.6) has solution in $\mathbb{C}$, with $x = i$. We also have that

$$(-i)^2 = (-1)^2 i^2 = -1\,.$$

Hence (5.6) has two solutions in $\mathbb{C}$, given by

$$x_1 = i\,, \quad x_2 = -i\,.$$

It turns out that the set $\mathbb{C}$ is so large that we are not only able to solve (5.6), but in fact any polynomial equation.

Theorem 5.47: Fundamental theorem of algebra

Let $p_n(x)$ be a polynomial of degree n with complex coefficients, i.e.,

$$p_n(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

for some coefficients $a_n, \ldots, a_0 \in \mathbb{C}$ with $a_n \neq 0$. Then there exist $z_1, \ldots, z_n \in \mathbb{C}$ such that

$$p_n(x) = a_n (x - z_1)(x - z_2) \cdots (x - z_n) \,. \tag{5.7}$$

Hence, the polynomial equation

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 \tag{5.8}$$

has solutions $z_1, \ldots, z_n$.

Theorem 5.47 says that every polynomial of degree n has n zeros, sometimes also called roots, i.e., n solutions to (5.8). We call the expression (5.7) a factorization of the polynomial p_n.

Several proofs of Theorem 5.47 exist in the literature, but they all use mathematical tools which are out of reach for now. Therefore we will not show a proof. For example one can prove Theorem 5.47 by

- Liouville's theorem (complex analysis)
- Homotopy arguments (general topology)
- Fundamental Theorem of Galois Theory (algebra)

Example 5.48

The equation

$$x^2 = -1 \tag{5.9}$$

is equivalent to

$$p(x) = 0\,, \quad p(x) := x^2 + 1\,.$$

Since p has degree $n = 2$, the Fundamental Theorem of Algebra tells us that there are two solutions to (5.9). We have already seen that these two solutions are $x = i$ and $x = -i$. Then

$$p(x) = x^2 + 1 = (x - i)(x + i)\,.$$

Example 5.49

Suppose we want to solve

$$x^4 - 1 = 0\,. \tag{5.10}$$

The associated polynomial equation is

$$p(x) = 0\,, \quad p(x) := x^4 + 1\,.$$

Since p has degree $n = 4$, the Fundamental Theorem of Algebra tells us that there are 4 solutions to (5.10). Let us find such solutions. We have

$$x^4 - 1 = 0 \iff \left(x^2\right)^2 = 1 \iff x^2 = \pm 1\,.$$

This means that we can have

$$x^2 = 1\,,$$

in which case $x = 1$ or $x = -1$, or we can have

$$x^2 = -1\,,$$

in which case $x = i$ or $x = -i$. Hence, the four solutions of (5.10) are given by $x = 1, -1, i, -i$ and

$$p(x) = x^4 + 1 = (x-1)(x+1)(x-i)(x+i)\,.$$

Definition 5.50

If a complex number z shows up k times on the right hand side of (5.7) for some $k \in \mathbb{N}$, then we say that z is a solution to (5.8) with multiplicity k.

Example 5.51

The equation

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

has 6 solutions:

- $x = 1$ with multiplicity 1
- $x = 2$ with multiplicity 2
- $x = -i$ with multiplicity 3

5.7 Solving polynomial equations

The non-factorized version of the polynomial

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

from Example 5.51 is

$$\begin{aligned} p(x) =& x^6 - (5-3i)x^5 + (5-15i)x^4 \\ &+ (11+23i)x^3 - (24+7i)x^2 + (12-8i)x + 4i \end{aligned}$$

We therefore have the following natural question.

Question 5.52

The Fundamental Theorem of Algebra states that

$$p_n(x) = 0 \tag{5.11}$$

has n complex solutions. How do we find such solutions?

The answer is that there is no general way to solve (5.11) when $n \geq 5$. This is the content of the Abel-Ruffini Theorem.

Theorem 5.53: Abel-Ruffini

There is no elementary solution formula to the polynomial equation

$$p_n(x) = 0$$

with p_n polynomial of degree n, with $n \geq 5$.

Similarly to the Fundamental Theorem of Algebra, the proof of the Abel-Ruffini Theorem is out of reach for our current mathematical knowledge. A proof can be carried out, for example, using Galois Theory.

There are however explicit formulas for solving (5.11) when p_n has degree $n = 2, 3, 4$. For $n = 2$ we can use the well-known quadratic formula.

Proposition 5.54: Quadratic formula

Let $a, b, c \in \mathbb{R}, a \neq 0$ and consider the equation

$$ax^2 + bx + c = 0\,. \tag{5.12}$$

Define

$$\Delta := b^2 - 4ac\,.$$

The following hold:

- If $\Delta > 0$ then (5.12) has two distinct real solutions given by

$$x_1 = \frac{-b - \sqrt{\Delta}}{2a}\,, \quad x_2 = \frac{-b + \sqrt{\Delta}}{2a}\,.$$

- If $\Delta = 0$ then (5.12) has one solution with multiplicity 2. Such solution is given by

$$x_1 = \frac{-b}{2a}\,.$$

- If $\Delta < 0$ then (5.12) has two distinct complex solutions given by

$$x_1 = \frac{-b - i\sqrt{-\Delta}}{2a}\,, \quad x_2 = \frac{-b + i\sqrt{-\Delta}}{2a}\,,$$

  where $\sqrt{-\Delta}$ is a real number, since $-\Delta > 0$.

Moreover, if $\Delta \neq 0$ we have

$$ax^2 + bx + c = a(x - x_1)(x - x_2)\,,$$

while if $\Delta = 0$ then

$$ax^2 + bx + c = a(x - x_1)^2\,.$$

Example 5.55

Suppose we want to solve

$$3x^2 - 6x + 2 = 0\,.$$

We have that

$$\Delta = (-6)^2 - 4 \cdot 3 \cdot 2 = 12 > 0$$

Therefore the equation has two distinct real solutions, given by

$$x = \frac{-(-6) \pm \sqrt{12}}{2 \cdot 3} = \frac{6 \pm \sqrt{12}}{6} = 1 \pm \frac{\sqrt{3}}{3}$$

In particular we have the factorization

$$3x^2 - 6x + 2 = 3\left(x - 1 - \frac{\sqrt{3}}{3}\right)\left(x - 1 + \frac{\sqrt{3}}{3}\right)\,.$$

Example 5.56

Suppose we want to solve

$$4x^2 - 8x + 4 = 0\,.$$

We have that

$$\Delta = (-8)^2 - 4 \cdot 4 \cdot 4 = 0\,.$$

Therefore there exists one solution with multiplicity 2. This is given by

$$x = \frac{-(-8)}{2 \cdot 4} = 1\,.$$

In particular we have the factorization

$$4x^2 - 8x + 4 = 4(x-1)^2\,.$$

Example 5.57

Consider

$$x^2 + 2x + 3 = 0\,.$$

We have

$$\Delta = 2^2 - 4 \cdot 1 \cdot 3 = -8 < 0\,.$$

Therefore there are two complex solutions given by

$$x = \frac{-2 \pm i\sqrt{8}}{2 \cdot 1} = -1 \pm i\sqrt{2}\,.$$

In particular we have the factorization

$$x^2 + 2x + 3 = (x + 1 - i\sqrt{2})(x + 1 + i\sqrt{2})\,.$$

So far we have considered the polynomial equation

$$ax^2 + bx + c = 0\,,$$

for $a, b, c \in \mathbb{R}$ and $a \neq 0$.

Question 5.58

What if $a, b, c \in \mathbb{C}$?

If $a, b, c \in \mathbb{C}$ then we might have

$$\Delta := b^2 - 4ac \in \mathbb{C}\,.$$

Therefore it is not clear how to compute

$$\sqrt{\Delta}\,.$$

However, we can still use the quadratic equation.

Proposition 5.59: Generalization of quadratci formula

Let $a, b, c \in \mathbb{C}, a \neq 0$. The two solutions to

$$ax^2 + bx + c = 0$$

are given by

$$x_1 = \frac{-b + S_1}{2a}\,, \quad x_2 = \frac{-b + S_2}{2a}\,,$$

where S_1 and S_2 are the two solutions to

$$z^2 = \Delta\,, \quad \Delta := b^2 - 4ac\,.$$

Remark 5.60

Suppose that $\Delta \in \mathbb{R}$. The equation

$$z^2 = \Delta$$

has the following solutions:

- If $\Delta > 0$ there are two real solutions

$$S_1 = -\sqrt{\Delta}\,, \quad S_2 = \sqrt{\Delta}$$

- If $\Delta = 0$ then 0 is the only solution with multiplicity 2. Hence

$$S_1 = S_2 = 0$$

- If $\Delta < 0$ there are two complex solutions

$$S_1 = -i\sqrt{-\Delta}\,, \quad S_2 = i\sqrt{-\Delta}$$

Therefore the solutions

$$x_1 = \frac{-b + S_1}{2a}\,, \quad x_2 = \frac{-b + S_2}{2a}\,,$$

given in Proposition 5.54 coincide with the ones given in Proposition 5.59.

Example 5.61

Let us see an application of Proposition 5.59. Consider the equation

$$\frac{1}{2}x^2 - (3+i)x + (4-i) = 0\,. \tag{5.13}$$

We have

$$\begin{aligned}\Delta &= (-(3+i))^2 - 4\cdot\frac{1}{2}\cdot(4-i)\\ &= 8 + 6i - 8 + 2i\\ &= 8i\,.\end{aligned}$$

Therefore $\Delta \in \mathbb{C}$. We have to find solutions S_1 and S_2 to the equation

$$z^2 = \Delta = 8i\,. \tag{5.14}$$

We look for solutions of the form $z = x + iy$. Then we must have that

$$z^2 = (a+ib)^2 = a^2 - b^2 + 2abi = 8i\,.$$

Thus

$$a^2 - b^2 = 0\,, \quad 2ab = 8\,.$$

From the first equation we conclude that $|a| = |b|$. From the second equation we have that $ab = 4$, and therefore a and b must have the same sign. Hence $a = b$, and

$$2ab = 8 \quad \Longrightarrow \quad a = b = \pm 2\,.$$

From this we conclude that the solutions to (5.14) are

$$S_1 = 2 + 2i\,, \quad S_2 = -2 - 2i\,.$$

Hence the solutions to (5.13) are

$$\begin{aligned}x_1 &= \frac{3 + i + S_1}{2\cdot\frac{1}{2}} = 3 + i + S_1\\ &= 3 + i + 2 + 2i = 5 + 3i\,,\end{aligned}$$

and

$$\begin{aligned}x_2 &= \frac{3 + i + S_2}{2\cdot\frac{1}{2}} = 3 + i + S_2\\ &= 3 + i - 2 - 2i = 1 - i\,.\end{aligned}$$

In the above example it was a bit laborious to compute S_1 and S_2. In the next section we will see an easier way to solve problems of the form $z^2 = \Delta$.

Remark 5.62: Polynomial equations of order $n = 3, 4$

For polynomial equations

$$p_n(x) = 0$$

with p_n of degree $n = 3, 4$ similar methods exist. However the solution formulas for such equations are really complicated, and we do not cover them here.
Still, it is sometimes possible to solve equations of degree higher than 2, in case it is obvious from inspection that a certain number is a solution, e.g., when $x = -1, 0, 1$ is a solution.

Example 5.63

Consider the equation

$$x^3 - 7x^2 + 6x = 0\,.$$

It is clear that $x = 0$ is a solution and that we can write

$$x^3 - 7x^2 + 6x = x\left(x^2 - 7x + 6\right)\,.$$

We could now use the quadratic formula to find the remaining two roots, but we can also directly observe that also $x = 1$ is a solution, so that $x - 1$ divides $x^2 - 7x + 6$. Using polynomial long division, we find that

$$\frac{x^2 - 7x + 6}{x - 1} = x - 6\,,$$

see Figure 5.6. Therefore the last solution is $x = 6$, and

$$x^3 - 7x^2 + 6x = x(x - 1)(x - 6)\,.$$

Example 5.64

Suppose we want to solve

$$x^3 - 7x + 6 = 0\,.$$

It is easy to see $x = 1$ is a solution. This means that $x - 1$ divides $x^3 - 7x + 6$, so we can compute by using polynomial long division,

$$\frac{x^3 - 7x + 6}{x - 1} = x^2 + x - 6\,,$$

see Figure 5.8. For the remaining two solutions, we can use the quadratic formula to obtain that also $x = 2$ and $x = -3$ are solutions. Thus

$$x^3 - 7x + 6 = (x - 1)(x - 2)(x + 3)\,.$$

$$
\begin{array}{r}
x-6 \\
\hline
x-1 \,\big)\; x^2-7x+6 \\
\underline{-x^2+x} \\
-6x+6 \\
\underline{6x-6} \\
0
\end{array}
$$

Figure 5.6: Polynomial long division between x^2-7x+6 and $x-1$.

$$
\begin{array}{r}
2x+3 \\
\hline
3x^2-2x-1 \,\big)\; 6x^3+5x^2-7 \\
\underline{-6x^3+4x^2+2x} \\
9x^2+2x-7 \\
\underline{-9x^2+6x+3} \\
8x-4
\end{array}
$$

Figure 5.7: Example of polynomial long division between $6x^3+5x^2-7$ and $3x^2-2x-1$.

$$
\begin{array}{r}
x^2 + x - 6 \\
\hline
x - 1 \,\big)\; x^3 - 7x + 6 \\
\underline{-x^3 + x^2} \\
x^2 - 7x \\
\underline{-x^2 + x} \\
-6x + 6 \\
\underline{6x - 6} \\
0
\end{array}
$$

Figure 5.8: Polynomial long division between $x^3 - 7x + 6$ and $x - 1$.

5.8 Roots of unity

Problem

Let $n \in \mathbb{N}$. We want to find all complex solutions to

$$z^n = 1\,. \tag{5.15}$$

Note that $z = 1$ is always a solution to (5.15) if n is even. In such case also $z = -1$ is a solution. If we were only looking for solutions in $\mathbb{R}$, these two would be the only solutions.

However, the Fundamental Theorem of Algebra, see Theorem 5.47, tells us that there are n complex solutions to (5.15).

Question 5.65

Is there a way to find all n solutions?

Example 5.66

We have seen in Example 5.49 that the solutions to

$$x^4 = 1$$

are $x = -1, 1, i, -i$. However we deduced this with a procedure which does not seem to generalize well to other exponents.

The trick to find all n solutions to (5.15) is to use the exponential form.

Theorem 5.67

Let $n \in \mathbb{N}$ and consider the equation

$$z^n = 1\,. \tag{5.16}$$

All the n solutions to (5.16) are given by

$$z_k = \exp\left(i\frac{2\pi k}{n}\right), \quad k = 0, \dots, n-1\,,$$

where $\exp(x)$ denotes e^x.

Proof

Rewrite 1 in exponential form:

$$1 = |1|e^{i\arg(1)} = e^{i2\pi k}, \quad k \in \mathbb{Z}\,.$$

Therefore (5.16) is equivalent to

$$z^n = e^{i2\pi k}\,.$$

By the properties of the exponential, we see that the above is solved by

$$z_k = \exp\left(i\frac{2\pi k}{n}\right), \quad k \in \mathbb{Z}\,.$$

By choosing $k = 0, \dots, n-1$ we obtain n different solutions.

Definition 5.68

The solutions to

$$z^n = 1$$

are called the **roots of unity**.

Example 5.69

The solutions to

$$z^4 = 1$$

are given by

$$z_k = \exp\left(i\frac{2\pi k}{4}\right) = \exp\left(i\frac{\pi k}{2}\right).$$

By taking $k = 0, 1, 2, 3$, we obtain the four solutions

$$z_0 = e^{i0} = 1, \qquad z_1 = e^{i\frac{\pi}{2}} = i,$$
$$z_2 = e^{i\pi} = -1, \qquad z_3 = e^{i\frac{3\pi}{2}} = -i.$$

Note that for $k = 4$ we would again get the solution $z = e^{i2\pi} = 1$.

Example 5.70

The solutions to

$$z^3 = 1$$

are given by

$$z_k = \exp\left(i\frac{2\pi k}{3}\right).$$

By taking $k = 0, 1, 2$, we obtain the three solutions

$$z_0 = e^{i0} = 1, \quad z_1 = e^{i\frac{2\pi}{3}}, \quad z_2 = e^{i\frac{4\pi}{3}}.$$

We can also convert z_1 and z_2 to trigonometric form:

$$z_1 = e^{i\frac{2\pi}{3}} = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$$

and

$$z_2 = e^{i\frac{4\pi}{3}} = \cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$$

5.9 Roots in $\mathbb{C}$

Problem

Let $n \in \mathbb{N}$ and $c \in \mathbb{C}$. We want to find the n-th roots of c. This means we want to find all complex solutions to

$$z^n = c\,.$$

The Fundamental Theorem of Algebra ensures that the above has n complex solutions. To find these solutions, we pass to the exponential form.

Theorem 5.71

Let $n \in \mathbb{N}$, $c \in \mathbb{C}$ and consider the equation

$$z^n = c\,. \tag{5.17}$$

All the n solutions to (5.17) are given by

$$z_k = \sqrt[n]{|c|}\,\exp\left(i\,\frac{\theta + 2\pi k}{n}\right), \quad k = 0, \dots, n-1\,,$$

where $\sqrt[n]{|c|}$ is the n-th root of the real number $|c|$, and $\theta = \arg(c)$.

Proof

Write c in exponential form:

$$c = |c|e^{i\theta} = |c|e^{i(\theta+2\pi k)}\,, \quad k \in \mathbb{Z}\,,$$

where $\theta = \arg(c)$. Therefore (5.17) is equivalent to

$$z^n = |c|e^{i(\theta+2\pi k)}\,.$$

By the properties of the exponential, we see that the above is solved by

$$z_k = \sqrt[n]{|c|}\,\exp\left(i\,\frac{\theta + 2\pi k}{n}\right), \quad k \in \mathbb{Z}\,.$$

By choosing $k = 0, \dots, n-1$ we obtain n different solutions.

Example 5.72

We want to find all the $z \in \mathbb{C}$ such that

$$z^5 = -32\,.$$

Let $c = -32$. We have

$$|c| = |-32| = 32 = 2^5\,, \quad \theta = \arg(-32) = \pi\,.$$

Hence, the solutions are given by

$$z_k = \left(2^5\right)^{\frac{1}{5}} \exp\left(i\pi \frac{1+2k}{5}\right), \quad k \in \mathbb{Z}.$$

By taking $k = 0, 1, 2, 3, 4$ we get the solutions

$$z_0 = 2e^{i\frac{\pi}{5}} \qquad z_1 = 2e^{i\frac{3\pi}{5}}$$
$$z_2 = 2e^{i\pi} = -2 \qquad z_3 = 2e^{i\frac{7\pi}{5}}$$
$$z_4 = 2e^{i\frac{9\pi}{5}}$$

Example 5.73

We want to find all the $z \in \mathbb{C}$ such that

$$z^4 = 9\left(\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right)\right).$$

Set

$$c := 9\left(\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right)\right).$$

The complex number c is already in the trigonometric form, so that we can immediately obtain

$$|c| = 9, \quad \theta = \arg(c) = \frac{\pi}{3}.$$

Hence the solutions are given by

$$z_k = \sqrt[4]{9}\, \exp\left(i\,\frac{\pi/3 + 2\pi k}{4}\right)$$
$$= \sqrt{3}\exp\left(i\pi\,\frac{1+6k}{12}\right)$$

for $k \in \mathbb{Z}$. Choosing $k = 0, 1, 2, 3$ gives the 4 solutions

$$z_0 = \sqrt{3}e^{i\pi\frac{1}{12}} \qquad z_1 = \sqrt{3}e^{i\pi\frac{7}{12}}$$
$$z_2 = \sqrt{3}e^{i\pi\frac{13}{12}} \qquad z_3 = \sqrt{3}e^{i\pi\frac{19}{12}}$$

License

Reuse

Citation

For attribution, please cite this work as:

> Fanzon, Silvio. (2023). *Lecture Notes on Numbers, Sequences and Series.* https://www.silviofanzon.com/2023-NSS-Notes/

BibTex citation:

```
@electronic{Fanzon-NSS-2023,
    author = {Fanzon, Silvio},
    title = {Lecture Notes on Numbers, Sequences and Series},
    url = {https://www.silviofanzon.com/2023-NSS-Notes/},
    year = {2023}}
```

References

[1] S. Abbott. *Understanding Analysis*. Second Edition. Springer, 2015.

[2] Bartle, Robert G. and Sherbert, Donald R. *Introduction to Real Analysis*. Fourth Edition. Wiley, 2011.

[3] W. Rudin. *Principles of Mathematical Analysis*. Third Edition. McGraw Hill, 1976.