Topic 1: Set Theory and Mathematical Proofwriting

Seppe Staelens

July 18, 2024

Introduction

We will start the course by introducing the basics of set theory, a branch of mathematics that lies at the foundation of all other mathematical concepts. We will discuss basic set operations, concepts like cardinality and the power set, and study maps and functions between sets. With this very basic setup, we will then explore the basis of proofwriting by discussing some of the most commonly used methods to prove mathematical theorems - a skill that any good mathematician needs to master.

We finish this topic by making sense of the statement that "there are as many natural numbers as there are rational numbers" in the context of cardinality of infinite sets, and then proceed to show that there really are more real numbers than rational numbers.

1 Lecture 1: Set Theory

A **set** is one of the most basic, yet abstract concepts in mathematics. A set is a *collection of objects* - summarized in the most non-mathematical way. A set consists of different elements, and this can really be anything, from integers to real numbers, or even matrices, functions and more abstract objects.

Other mathematical structures are obtained from equipping sets with more properties and relations between them, and we will encounter many throughout the course.

1.1 Basic definitions

For now, we aim to denote sets with capital letters and their elements with small letters. We say that

- x is an **element** of A if x is contained in the set A. This is denoted as $x \in A$.
- x is not an element of A otherwise. This is denoted as $x \notin A$.
- the set A is a **subset** of the set B if every element of A is in B as well. This is denoted as $A \subset B$.
- the set A and B are equal if they contain the same elements. Equality of sets is denoted as $A = B$. Given the above definition, this is equivalent to $A \subset B$ and $B \subset A$ holding at the same time.

Sets can be denoted in different ways. The most common way is to list the elements of the set between curly brackets, separated by commas. For example, the set of the first three natural numbers[1] can be written as

$$A = \{0, 1, 2\}. \tag{1}$$

Another way to denote sets is by specifying a **set condition**. For example, the set of all even natural numbers can be written as

$$B = \{x \in \mathbb{N} \mid x \text{ is even}\}. \tag{2}$$

The vertical line precedes the condition(s) that the elements of the set must satisfy. We can use similar notation to specify a set by means of a formula. For example, the set of all perfect squares can be written as

$$C = \{n^2 \mid n \in \mathbb{N}\}. \tag{3}$$

The size of a set, also known as **the cardinality** of the set, is denoted as $\#A$. For finite sets, i.e. sets with a finite number of elements, this is simply the number of elements. A set with cardinality 1, i.e. a set with only one element, is called a **singleton (set)**. The (unique) set with no elements, i.e. cardinality 0, is called the **empty set**, and is denoted as $\emptyset$. For sets with an infinite amount of elements, like the integers, this is a bit more subtle. We will come back to this in Sec. 2.5.

1.2 Operations on sets

Given two sets A, B, we can define the following operations:

- The **union** of A and B, denoted as $A \cup B$, is the set of all elements that are in A or in B. In mathematical notation, this is
$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}. \tag{4}$$
- The **intersection** of A and B, denoted as $A \cap B$, is the set of all elements that are in both A and B. In mathematical notation, this is
$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}. \tag{5}$$
If two sets have an empty intersection, i.e. $A \cap B = \emptyset$, we say that the sets are **disjoint**.
- The **set difference** of A and B, denoted as $A \setminus B$, is the set of all elements that are in A but not in B. In mathematical notation, this is
$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}. \tag{6}$$
Note that this is not symmetric, i.e. $A \setminus B \neq B \setminus A$ (much like $a - b$ is in general not equal to $b - a$, for real numbers a, b).
- The **Cartesian product** of A and B, denoted as $A \times B$, is the set of all pairs (a, b) with $a \in A$ and $b \in B$. In mathematical notation, this is
$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}. \tag{7}$$
- If we consider some *Universe* U, a 'large' set containing all elements that could potentially be relevant for our problem, and a subset $A \subset U$, we can define the **complement** of A in U as
$$A^c = U \setminus A. \tag{8}$$
- The **power set** of A, denoted as $\mathcal{P}(A)$, is the set of all subsets of A. In mathematical notation, this is
$$\mathcal{P}(A) = \{B \mid B \subset A\}. \tag{9}$$
Note that this is *set of sets*, meaning that every element of $\mathcal{P}(A)$ is a set itself.

The first five of these operations are rather straightforward, and we discuss some examples in class. The power set, however, deserves a bit more attention.

[1] Note that we treat 0 as belonging to the natural numbers $\mathbb{N}$, which is not always the case. The set of natural numbers *without* 0 is denoted as $\mathbb{N}_0$ in our convention.

1.2.1 Power set

The powerset of a set A is the set of all subsets of A. Intuitively, the power set must be larger than the original set. Indeed, for every element in the set A, call it x, the singleton $\{x\}$ is a subset of A, and thus an element of the power set. This means that the power set contains at least as many elements as there are in A. But, do we know whether the power set is always larger than A?

Lemma 1. *(Binomial Theorem) For any natural number $n \in \mathbb{N}$ and any real numbers $a, b \in \mathbb{R}$, we have*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k. \tag{10}$$

This is a very useful formula, which can be proven in many ways (as we will see in the next lecture). The coefficient $\binom{n}{k}$ is called a **binomial coefficient**, and is defined as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \tag{11}$$

where $n! = n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1$ is the **factorial** of n. The binomial coefficient counts the number of ways to choose k elements from a set of n elements, and is a very important concept in *combinatorics*.

Theorem 1. *Given a finite set A with $\#A = N$, the power set of A, $\mathcal{P}(A)$, has 2^N elements.*

Proof. We will count the subsets of A by considering subsets of size $k = 0, 1, \ldots, N$.

For $k = 0$, there is only one subset of A with no elements, namely the empty set $\emptyset$. For $k = 1$, there are N subsets of A with one element, namely the singletons $\{x\}$ for $x \in A$. For $k = 2$, we need to find the number of subsets with 2 elements. Clearly, any subset with two elements is obtained by *choosing* two elements from A. We have seen right before that the number of ways this can be done is $\binom{N}{2}$, and therefore there are $\binom{N}{2}$ subsets of A with two elements.

Similarly, for $k = 3$, there are $\binom{N}{3}$ subsets of A with three elements, and so on. Finally, for $k = N$, there is only one subset of A with N elements, namely A itself.

Therefore, adding up all these numbers, we find that the total number of subsets of A is

$$\begin{aligned}
\#\mathcal{P}(A) &= 1 + N + \binom{N}{2} + \binom{N}{3} + \cdots + \binom{N}{N-1} + 1 \\
&= \binom{N}{0} + \binom{N}{1} + \binom{N}{2} + \binom{N}{3} + \cdots + \binom{N}{N-1} + \binom{N}{N} \\
&= \sum_{k=0}^{N} \binom{N}{k} \\
&= (1+1)^N \qquad \text{by the binomial theorem} \\
&= 2^N.
\end{aligned}$$

□

1.3 Functions

You have normally already seen functions in high school, in the context of functions of real numbers. For example, you probably have seen something like a linear function $f(x) = ax + b$, where x is a real number, and studied its graph - which is a straight line. Functions, however, are a much more general concept, and can be defined between any two sets.

A **function (map)** from a set X to a set Y is a map that assigns to each element $x \in X$ exactly one element $y \in Y$. This is denoted as $f : X \to Y$. This clearly encompasses the concept of a function that you are more familiar with, which is a function from $\mathbb{R}$ to $\mathbb{R}$. We discuss more general examples in class.

Usually we describe a function by specifying its **image**, i.e. given $x \in X$ we specify the element $f(x) \in Y$. A more extensive notation for the function would then be

$$f : X \to Y : x \mapsto f(x). \tag{12}$$

Note the different arrows in the expression above: they are not the same. Usually the set X is called the **domain** of the function, and the set Y is called the **codomain** of the function.

Given two functions $f : X \to Y$ and $g : Y \to Z$, we can define the **composition** of these functions as

$$g \circ f : X \to Z : x \mapsto g(f(x)). \tag{13}$$

This is a new function, which maps elements of X to elements of Z by first applying f and then g.

Given subsets $A \subset X$ and $B \subset Y$ and a function $f : X \to Y$, we can define the **image** of A under f as

$$f(A) = \{f(x) \mid x \in A\}. \tag{14}$$

Similarly, we can define the **preimage** of B under f as

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}. \tag{15}$$

Note that this is not the same as the inverse of the function f, which is a different concept.

1.4 Injection, surjection, bijection

To properly define some of the concepts in this section, we first briefly discuss quantifiers:

- The **existential quantifier** $\exists$ is used to denote that there exists at least one element in a set that satisfies a certain property. For example, with $X \subset \mathbb{R}$, the expression $\exists x \in X : x > 2$ means that there is at least one element x in X that is larger than 2.
- The **universal quantifier** $\forall$ is used to denote that all elements in a set satisfy a certain property. For example, with $X \subset \mathbb{R}$, the expression $\forall x \in X : x > 2$ means that all elements x in X are larger than 2.
- The **unique quantifier** $\exists!$ is used to denote that there exists exactly one element in a set that satisfies a certain property. For example, with $X \subset \mathbb{R}$, the expression $\exists! x \in X : x > 2$ means that there is exactly one element x in X that is larger than 2.

We use these quantifiers in the following defintions. Given a function $f : X \to Y$, we can give the following definitions:

- The function f is called an **injection** if for every $y \in Y$, there is at most one $x \in X$ such that $f(x) = y$. In mathematical notation, this can be expressed as[2]

$$\forall x_1, x_2 \in X : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2). \tag{16}$$

- The function f is called a **surjection** if for every $y \in Y$, there is at least one $x \in X$ such that $f(x) = y$. In mathematical notation, this can be expressed as

$$\forall y \in Y, \exists x \in X : f(x) = y. \tag{17}$$

[2]Note the use of the "⇒" symbol, to which we come back in Lecture 2.

- The function f is called a **bijection** if it is both an injection and a surjection. In mathematical notation, this can be expressed as

$$\forall y \in Y, \exists! x \in X : f(x) = y. \tag{18}$$

Using these concepts, we can revisit our definition of cardinality. For any strictly positive natural number $n \in \mathbb{N}_0$ we define the set E_n as

$$E_n = \{k \in \mathbb{N} \mid 1 \leq k \leq n\}. \tag{19}$$

Furthermore, we define $E_0 = \emptyset$. Clearly, the set E_n has n elements, and therefore has cardinality n.

Definition 1. *A set A is said to be **finite** if there exists a bijection between A and E_n for some $n \in \mathbb{N}$. The number n is then called the **cardinality** of A, and is denoted as $\#A = n$.*

2 Lecture 2: Mathematical Proofwriting

With basic arsenal of set theory concepts at our disposal, we can now start to explore the basics of mathematical proofwriting. This is an essential skill of any mathematician, and is used to show that a certain statement is objectively true, given some assumptions.

We have already seen a proof, namely the one of Theorem 1, though this was not the most elegant one. In general, any theorem, proposition, lemma ... should be accompanied by a proof, which is a logical argument that shows that the statement is true. Proofs also often use the symbols $\Rightarrow, \Leftrightarrow$, which are used to denote logical implications. We already saw this in the definition of an injection in the previous lecture, in the statement

$$\forall x_1, x_2 \in X : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2).$$

In words, this expression means that, given any elements x_1, x_2 in the domain X of the function f, if x_1 and x_2 are different, then their images under f are also different. The symbol $\Rightarrow$ translates to "then" in this case, and it requires some practice to be able to translate these mathematical statements to English, and the other way around.

In the following subsections, we will discuss some of the most commonly used methods to prove mathematical statements.

2.1 Direct proof

A direct proof simply means that, starting from the assumptions, we directly follow a series of logical implications that lead to the conclusion. As an example, we consider the following theorem:

Lemma 2. *Given three sets A, B, C, we have*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \tag{20}$$

To prove the equality of these two sets, we will show that each set is a subset of the other. Indeed, as we saw in the first lecture, $(A \subset B \wedge B \subset A) \Rightarrow A = B$. The symbol $\wedge$ is used to denote a logical "and", and is used to combine multiple logical statements.

Proof. We start by showing that $A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C)$. Choose $x \in A \cap (B \cup C)$ randomly. This means that $x \in A$ and $x \in B \cup C$. Therefore, $x \in B$ or $x \in C$. Without loss of generality[3], we assume that $x \in B$. Since both $x \in A$ and $x \in B$, we have $x \in A \cap B$. This means that $x \in (A \cap B) \cup (A \cap C)$ as well. Since x is chosen randomly, this proves the statement.

Next, we show that $(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C)$. Choose $x \in (A \cap B) \cup (A \cap C)$ randomly. This means that $x \in A \cap B$ or $x \in A \cap C$. Without loss of generality, we assume that $x \in A \cap B$. This means that $x \in A$ and $x \in B$. Since $x \in B$, we have $x \in B \cup C$, and therefore $x \in A \cap (B \cup C)$. Since x is chosen randomly, this proves the statement.

We have proven that both sets are contained in each other, and must therefore be equal. □

Note

- that the proof is written in a very structured way, with clear indications of what is being proven and how. A proof does not only contain equations and logical implications, but also a lot of text to explain the reasoning.

[3]This is a common phrase in mathematics, and indicates that the argument can be made irrespective of the specific choice that follows. In this case, it means that we might as well have had $x \in C$ instead of $x \in B$. However, by simply renaming the sets B and C, we would again have $x \in B$. This is sometimes abbreviated to WLOG.

- that at the end of the proof the symbol □ is used. This is a common symbol to signal the end of the proof, other alternatives being ■ or the letters QED[4].
- that the proof ensures that the reasoning is fully general, making sure to exhaust all possible options - or indicating generality by means of phrases like "without loss of generality".

Direct proofs are straightforward in reasoning and clear. However, they are not always the most elegant way to prove a statement, and sometimes not even possible.

2.2 Proof by contradiction

Another very popular method to prove a statement is by contradiction. This method usually assumes that the statement is false, and then uses the assumptions to derive a contradiction. This means that the original assumption - the statement being false - must be incorrect, and therefore the statement must be true.

A famous example is the proof that $\sqrt{2}$ is irrational.

Theorem 2. *The number $\sqrt{2}$ is irrational, i.e. cannot be written as a fraction of two integers.*

Proof. Suppose that $\sqrt{2}$ is rational. This means that there exist two integers a, b without a common divisor such that $\sqrt{2} = \frac{a}{b}$ (otherwise we could simply divide both a and b by this common divisor). Squaring both sides of this equation gives $2 = \frac{a^2}{b^2}$, or $a^2 = 2b^2$. This means that a^2 is even, and therefore a is even as well[5]. Since a is even, it can be written as $a = 2k$ for some integer k. Substituting this back into the equation gives $4k^2 = 2b^2$, such that b^2 - and therefore b - is even as well. This means that both a and b are even, and are therefore both divisible by 2. This is in contradiction with the assumption that a and b have no common divisor, and therefore our assumption that $\sqrt{2}$ is rational must be incorrect. □

A proof by contradiction can be very elegant, like above, and often provides a good alternative to a direct proof. The downside is that it may sometimes be less obvious.

2.3 Proof by induction

Proof by induction is a very powerful method to prove statements that depend on a natural number n. The idea is to first prove the statement for a *base case*, usually $n = 0$ or $n = 1$, and then show that if the statement holds for some $n = k$, it also holds for $n = k + 1$. The principle of induction is then that, starting from this base case, the statement must be true for all natural numbers by the recursive application of the second step.

A standard example is the proof of the following formula:

Proposition 1. *For any natural number $n \in \mathbb{N}_0$, the sum of the first n natural numbers is given by*

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \tag{21}$$

Proof. We start by proving the formula for the base case $n = 1$. This gives

$$\sum_{i=1}^{1} i = 1 = \frac{1 \cdot 2}{2}, \tag{22}$$

[4]From the latin *quod erat demonstrandum*, meaning "that which was to be demonstrated".
[5]Another fun proposition to prove by contradiction - you can try this yourself!

and it is clear that the formula holds for $n = 1$. Assume now that the formula holds for some $n = k$. This means that

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}. \tag{23}$$

We now show that the formula also holds for $n = k + 1$. Note that

$$\begin{aligned}\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

We have shown that, assuming the formula holds for $n = k$, it also holds for $n = k + 1$. By the principle of induction, the formula must hold for all natural numbers n. □

Exercise 1. *Prove the Binomial Theorem in Lemma 1 by induction. You will probably need some properties of the binomial coefficients, like* $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

2.4 To be "well-defined"

An important part of mathematical definitions and formulas is that they are "well-defined". In the most basic sense, this means that the definition or formula is clear and unambiguous, and does not suffer any problems. As this explanation is *extremely vague*, it is easier to illustrate this by means of several examples. Ensuring that something is well-defined requires one or more checks, which vary depending on the context.

- As a first example, suppose we are given two real numbers a, b and want to define their quotient $q = a/b$. This is not well defined, as we can have $b = 0$ - and you should be aware that we can't divide by zero. Therefore, we can only define the quotient of two real numbers a, b if b is non-zero.
- Consider the function $f : \mathbb{N} \to \mathbb{N} : n \mapsto n/2$. This is not well-defined, as $n/2$ is not always a natural number (e.g. $n = 3$) and we defined the codomain of f to be $\mathbb{N}$. To make f well-defined, we could for example restrict the domain to even numbers (denoted as $2\mathbb{N}$), or extend the codomain to the rational numbers $\mathbb{Q}$.
- Say we are writing some proof related to set theory, involving two sets A, B. Suppose we have found an ingenious way to prove the statement using an element in the intersection of A and B, i.e. we write in our proof "take $x \in A \cap B$". This may not be well-defined, as $A \cap B$ could be empty. In this case, we should first argue why $A \cap B$ is non-empty, or consider the case where $A \cap B = \emptyset$ separately.

Many more examples can be given, but the main takeaway is that checking whether something is well-defined comes down to checking what could possibly go wrong, and showing that it doesn't.

2.5 Cardinality of infinite sets

We have already defined the concept of cardinality, the "size" of a set, for finite sets (see Definition 1). The question is now how to extend this to infinite sets. Are they all just "infinitely large"? Or are some of the sets *actually larger* than others?

An obvious point of reference that we have is the set of natural numbers $\mathbb{N}$. This set is infinite, as you should be well aware, and provides us with a good point of reference. A nice thing about $\mathbb{N}$ is that we can list them (of course, going $0, 1, 2, 3 \dots$): we call this property **countability**. We say that the natural numbers are

countably infinite. Of course, there is no way to *actually count* the natural numbers, but this property means that we can list them in a way that we will at some point[6] reach any given number $n \in \mathbb{N}$.

In the spirit of Definition 1, the following definition now makes sense:

Definition 2. *A set A is said to be **countably infinite** if there exists a bijection between A and $\mathbb{N}$. A countably infinite set is said to have cardinality $\aleph_0$ (pronounced aleph zero).*

Essentially, this definition gives meaning to the size of a whole bunch of inifinite sets: if we can *count* them, i.e. list them in a way akin to the natural numbers, we say that the set is "as large" as $\mathbb{N}$. The following examples show that this definition is not always intuitive though:

- Consider the set $\mathbb{Z}$ of all integers. Obviously, $\mathbb{N}$ is a strict subset of the latter, and therefore we would expect the latter to be "larger". However, consider the following mapping between the integers and natural numbers:
$$f : \mathbb{Z} \to \mathbb{N} : z \mapsto \begin{cases} 2z & \text{if } z \geq 0, \\ 2(-z) - 1 & \text{if } z < 0. \end{cases} \tag{24}$$
This mapping maps the positive integers to the even natural numbers, and the negative integers to the odd natural numbers. It is easy to see that this mapping is a bijection, and therefore the set of integers is countably infinite as well.
- Consider the set $\mathbb{Q}$ of all rational numbers. This set seems to be *much larger* than the natural numbers, containing all fractions. However, it is possible to construct a bijection between $\mathbb{Q}$ and $\mathbb{N}$, as explained below, and therefore the set of rational numbers is also countably infinite.
- We can think of $\mathbb{Q}$ as being equivalent to the set $\mathbb{Z} \times \mathbb{N}_0$, i.e. the set of all pairs (z, n) where z is the denominator, being any integer, and n is the numerator, being any non-zero natural number. It can therefore be proven that the Cartesian product of two countably infinite sets is again countably infinite. By inductive reasoning any finite Cartesian product of countably infinite sets is countably infinite.

The question now of course is whether there are sets that are *not* countably infinite, i.e. sets that really are "larger" than the natural numbers. The answer is yes, which becomes clear from the following definition and theorem.

Definition 3. *Let X, Y be two sets. We say that X and Y have the same cardinality if there exists a bijection between X and Y, and denote $|X| = |Y|$. We say that the cardinality of X is smaller than the cardinality of Y if there exists an injection $f : X \to Y$, and denote $|X| \leq |Y|$ (with equality only holding if the injection is a bijection[a]).*

[a] If we have two sets X, Y, as well as injections $f : X \to Y$ and $g : Y \to X$ and therefore $|X| \leq |Y|$ and $|Y| \leq |X|$, we would like to conclude that $|X| = |Y|$. This is indeed the case, as the *Cantor-Bernstein-Schröder theorem* guarantees the existence of a bijection $h : X \to Y$ given the existence of the two injections.

Note that this definition seems trivial in the context of the finite sets we encountered before. However, this definition applies to inifinite sets as well.

Lemma 3. *For non-empty sets X, Y, we have $|X| \leq |Y|$ if and only if there exists a surjection $f : Y \to X$.*

Proof. The proof is left as en exercise to the reader.[7] □

[6] Note that this assumes the existence of a person with a lot of patience and spare time.
[7] This is also a very common phrase in mathematics textbooks - though one that is usually not appreciated by students.

Theorem 3. *For any set X, we have $|X| < |\mathcal{P}(X)|$, i.e. the power set of X has a larger cardinality than X.*

Proof. First, notice that the function $f : X \to \mathcal{P}(X) : x \mapsto \{x\}$ is an injection, and therefore $|X| \leq |\mathcal{P}(X)|$.

We now show that there exists no surjection $f : X \to \mathcal{P}(X)$, by proving that the set

$$A = \{x \in X \mid x \notin f(x)\}.$$

is not contained in the image of any function f. We do this by contradiction. Suppose $f(a) = A$ for some $a \in X$. There are now two possibilities, either $a \in A$ or $a \notin A$. If $a \in A$, then by definition of A we have $a \notin f(a) = A$, which is a contradiction. If $a \notin A$, then by definition of A we have $a \in f(a) = A$, which is again a contradiction.

Therefore, we find a contradiction and A cannot be in the image of f. This means that there is no surjection $f : X \to \mathcal{P}(X)$, and therefore $|X| < |\mathcal{P}(X)|$. □

This theorem shows that the power set of a set is always "larger" than the set itself, and therefore there are sets that are not countably infinite. Furthermore, this means that there is no such thing as "the largest set", as we can always construct a larger set by taking the power set of a given set.

2.5.1 $\mathbb{Q}$ is countably infinite

As mentioned above, the collection of rational numbers, $\mathbb{Q}$, is countably infinite. To prove this, we first show two other propositions.

Proposition 2. *The set $X_0 := \mathbb{Q} \cap [0, 1[$ is countably infinite.*

Proof. The rational numbers in $[0, 1[$ can be counted as follows:

$$0, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{1}{6}, \frac{5}{6}, \frac{1}{7}, \dots$$

This is best illustrated by use of a diagram:

	2	3	4	5	…
1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	…
2	-	$\frac{2}{3}$	-	$\frac{2}{5}$	…
3	-	-	$\frac{3}{4}$	$\frac{3}{5}$	…
4	-	-	-	$\frac{4}{5}$	…
	⋮	⋮	⋮	⋮	⋱

We go over the columns, from left to right, and for every column we start at the top and go until the diagonal. If we encounter a fraction we have encountered before, we simply skip it. This gives us a well-defined order to go over the set X_0. □

Theorem 4. *Let X_n be a countable set for every $n \in \mathbb{N}$. Then*

$$X = \bigcup_{n \in \mathbb{N}} X_n$$

is also countable.

Proof. We assume that the sets X_n are countably infinite. The proof can be adapted easily if some of the sets are finite. Because every X_n is countably infinite, we can list the elements of X_n as $x_{n,0}, x_{n,1}, x_{n,2}, \dots$. We can display all of these elements in an infinite matrix

$$\begin{pmatrix} x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} & \dots \\ x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} & \dots \\ x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} & \dots \\ x_{3,0} & x_{3,1} & x_{3,2} & x_{3,3} & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \tag{25}$$

We can now list all elements of X by going over the matrix along the antidiagonals, which gives us an ordering

$$x_{0,0}, x_{1,0}, x_{0,1}, x_{2,0}, x_{1,1}, x_{0,2}, x_{3,0}, x_{2,1}, x_{1,2}, x_{0,3}, \dots$$

If all sets X_n are disjoint, this gives us a well-defined way to list all elements of X, and therefore X is countably infinite. If the sets are not all disjoint, we can simply skip over the elements we have already encountered. □

We can now prove the following theorem.

Theorem 5. *The set of rational numbers $\mathbb{Q}$ is countably infinite.*

Proof. Define for every $n \in \mathbb{N}$ the set $X_n = \mathbb{Q} \cap [n, n+1[$. All of these sets are countably infinite, which can be shown analogously to the proof of Prop. 2. By Thm. 4, the union of all these sets is also countably infinite. The union of these sets is exactly the set $\mathbb{Q}^+$ of positive rational numbers. In the exact same way, it can be shown that $\mathbb{Q}^-$ is countably infinite. Therefore, $\mathbb{Q} = \mathbb{Q}^+ \cup \mathbb{Q}^-$ is countably infinite as well. □

2.5.2 $\mathbb{R}$ is not countably infinite

We are now ready to discuss why $\mathbb{R}$ is not countably infinite. The proof of this statement is a classic example of a proof by contradiction, and is known as Cantor's diagonal argument.

Theorem 6. *The set $\mathbb{R}$ of real numbers is not countably infinite.*

Proof. We prove the statement by contradiction. Suppose $\mathbb{R}$ is countably infinite. Then $[0, 1[$ must be countable as well, as it is a subset of $\mathbb{R}$. This set is clearly infinite, and therefore we must have a bijection $f : \mathbb{N} \to [0, 1[$. Every number in $[0, 1[$ can be written as a decimal expansion, e.g. $0.123456\dots$ This can be schematically represented as

$$x = 0, x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \dots$$

where $x_1, x_2, x_3, \dots$ are the digits of the decimal expansion. Note that this representation is not unique, as $0.9999\dots = 1$. However, we choose the representation such that the decimal expansion does not end in an infinite string of 9's, which makes each of these expansions unique. Every number $f(j) \in [0, 1[$ has such a decimal expansion, which we list for all $j \in \mathbb{N}$ as

$$\begin{array}{llllll}
f(1) = 0, & x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} & x_{1,5} \dots \\
f(2) = 0, & x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} & x_{2,5} \dots \\
f(3) = 0, & x_{3,1} & x_{3,2} & x_{3,3} & x_{3,4} & x_{3,5} \dots \\
f(4) = 0, & x_{4,1} & x_{4,2} & x_{4,3} & x_{4,4} & x_{4,5} \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}$$

We now construct a number $y \in [0, 1[$ that is not in the list. We define y as

$$y = 0, y_1 \quad y_2 \quad y_3 \quad y_4 \quad y_5 \dots$$

where

$$y_n = \begin{cases} 1 & \text{if } x_{n,n} \neq 1, \\ 2 & \text{if } x_{n,n} = 1. \end{cases}.$$

This number y is not in the list, as it differs from every number in the list in at least one digit. Note that the digits we used to construct y are the ones on the diagonal $(x_{n,n})$, which is why this proof is called Cantor's diagonal argument. This is a contradiction, as we assumed that the list contained all numbers in $[0, 1[$. Therefore, $f : \mathbb{N} \to [0, 1[$ cannot be surjective, and therefore not a bijection. This means that $[0, 1[$ is not countably infinite, and therefore $\mathbb{R}$ is not countably infinite. □

2.5.3 The Continuum Hypothesis

The proof above shows that the set of real numbers is not countably infinite, and therefore there are sets that are "larger" than the natural numbers. Furthermore, due to Thm. 3, we know that $\mathcal{P}(\mathbb{N})$ is larger than $\mathbb{N}$. This raises the question of whether $\mathbb{R}$ and $\mathcal{P}(\mathbb{N})$ have the same cardinality. This turns out to be the case, and we have that $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| \equiv 2^{\aleph_0}$.

The **Continuum Hypothesis** states that there is no set whose cardinality is strictly between that of the natural numbers and the real numbers, i.e. there is no set X such that $\aleph_0 < |X| < 2^{\aleph_0}$. This turns out to be a very complicated problem, and it has been shown that the Continuum Hypothesis cannot be proven or disproven using the standard axioms of set theory. Delving into the details would take us too far, but it is one of the suggested projects for the summer school.

3 References

These notes are based on my own knowledge of these basic mathematical concepts, and the writing has been accelerated by the use of *Github copilot* and its implementation in VSCode. Inspiration (and most of Section 2.5) has been taken from the course notes for *"Bewijzen en Redeneren"* (Proving and Reasoning), used in the first year of the Bachelor of Mathematics at the KU Leuven, at the time taught by Prof. Arno Kuijlaars - also the author of the lecture notes.