Department of Logic FFUK

Introduction to mathematics

Radek Honzík

University text for a one-semester course in Introduction to mathematics at Department of Logic, Faculty of Arts, Charles University in Prague.

Version: March 22, 2018

Contents

1 Natural numbers ℕ

Based on the previous section concerning Euclid's geometry – see a separate file *euclid.pdf* available on my web page –, we now know that we had better be careful with other "obvious" concepts, such as a natural, rational or real number.

Natural numbers are the basic units for counting. Together with the basic operation on natural numbers, such as $+$ and $\times$, we can rigorously define them in several "intuitive ways".

1.1 A set-theoretical approach

In this approach, we define natural numbers as certain *sets*. To be able to define natural numbers in this way, we need some preliminary information about sets. A set is a definite collection of objects. The important property is that we considered two sets as identical if and only if they have the same elements (this property is known as *extensionality*). In other words, a set is determined by its elements, not by its definitions: for instance $\{2,3,5\}$ and $\{p \mid p \text{ is a prime } < 6\}$ is the same set.

We need to introduce some notation concerning sets which we shall need for the definition of natural numbers. We will not try to describe sets as entities, we take this concept to be a primitive notion (similarly as a line was for Euclid). Indirectly, sets will be determined by the properties we postulate about them.

(i) $x \in y$, a binary relation of membership: if a set x is in the relation "to be an element of" with a set y, we write it symbolically as $x \in y$.

(ii) $x \subseteq y \leftrightarrow (\forall q)\ q \in x \to q \in y$, we say that x is a *subset* of y. This relation is determined by the propositional connective "if, then", $\to$.

Exercise: Show that for every x, y it holds that $x = y \leftrightarrow x \subseteq y \wedge y \subseteq x$.

Notice that $\subseteq$ is a *partial order, partial ordering,* or just *ordering*: it is a binary relation which is

- *reflexive*: $x \subseteq x$ for every set x.
- *transitive*: $x \subseteq y$ and $y \subseteq z$ implies $x \subseteq z$ for all sets x, y, z.
- *weakly antisymmetrical*: $x \subseteq y$ and $y \subseteq x$ implies $x = y$ for all x, y.

Exercise. Verify that $\subseteq$ is indeed a partial ordering.

Exercise. Notice that these three properties are satisfied by the usual partial orderings you know: $\leq$ on natural numbers, $\leq$ on rational numbers etc. Notice however that there are properties which are true of $\leq$ on natural numbers, for instance, but are not included in the three properties above. For instance the partial order $\subseteq$ is not *linear* – while for all natural numbers m, n it holds that either $m \leq n$ or $n \leq m$, it is not true that $x \subseteq y$ or $y \subseteq x$ for all sets x, y (find two sets x, y such that neither $x \subseteq y$, nor $y \subseteq x$, as an exercise). An example of an ordering on numbers which is *not* linear is the relation $m|n$, "m divides n"; verify that $|$ is a partial order according to the definition above.

(iii) $x \cap y = \{q \mid q \in x \wedge q \in y\}$, the operation of *intersection.* This operation is determined by the propositional connective *and*, $\wedge$.

(iv) $x \cup y = \{q \mid q \in x \vee q \in y\}$, the operation of *union*. This operation is determined by the propositional connective *or*, $\vee$.

(v) $x - y = \{q \mid q \in x \wedge q \notin y\}$, the operation of *subtraction*. This operation is determined by the propositional connective *not*, $\neg$.

(vi) $\mathscr{P}(x) = \{q \mid q \subseteq x\}$, a powerful axiom which says that the collection of all subsets of any set is also a set. The set $\mathscr{P}(x)$ is called the *powerset* of x.

(vii) $\{x, y\}$ is a set which contains exactly x, y as elements. Note that it works for a single set x as well: $\{x, x\} = \{x\}$; this set is called the *singleton* (singleton) of x.

(viii) Comprehension. Given a property φ and a set y, there is a set x of all q which are in y and satisfy φ: $x = \{q \mid q \in y \wedge \varphi(q)\}$. I.e. for all q, $q \in x$ if and only if $q \in y \wedge \varphi(q)$.

Notation. Sometimes we write $\{q \in y \mid \varphi(q)\}$ instead of $\{q \mid q \in y \wedge \varphi(q)\}$. This is just a matter of notation. In any case, these two expressions denote the same set. (We prefer the notation $\{q \in y \mid \varphi(q)\}$ because it is shorter.)

(ix) Assume there is at least one set x. Then there is an *empty set*, denoted by $\emptyset$, where $\emptyset = \{q \mid q \in x \wedge q \neq q\}$.

Exercise. Verify that there is only one emptyset; i.e. the definition of the emptyset does not depend on the initial set x: if x_1 and x_2 are two sets, then $\{q \mid q \in x_1 \wedge q \neq q\} = \{q \mid q \in x_2 \wedge q \neq q\}$. [Hint. Use extensionality of sets.]

Exercise. Verify that the emptyset $\emptyset$ is a subset of every set, i.e. if x is a set, then $\emptyset \subseteq x$. However, notice that it is *not* true that $\emptyset$ is an element of every set. Give an example of a set x such that $\emptyset \notin x$.

Exercise. Use the previous exercise to conclude that $\mathscr{P}(x)$, the powerset of x, is always non-empty, even if $x = \emptyset$.

(x) * The set y above in the Comprehension axiom (viii) is necessary to avoid inconsistency right from the start: consider an object defined by $x = \{q \mid q \notin q\}$. It is easy to show that if x were a set, then its existence would lead to contradiction: assuming $x \in x$, we can derive $x \notin x$, and assuming $x \notin x$, we can derive $x \in x$. This is a contradiction since either $x \in x$ or $x \notin x$ must be true.

(xi) We say that a structure $\langle B, \wedge, \vee, -, 0, 1\rangle$ is a Boolean algebra if B is a set, $\wedge$ and $\vee$ are binary operations[1] on B, i.e. for every $a, b \in B$, $a \wedge b$ and $a \vee b$ are elements of B, $-$ is an unary operation on B, i.e. for every $b \in B$, $-b$ is an element of B, and $0, 1$ are distinct (i.e. $0 \neq 1$) special elements of B (called constants). And moreover the operations satisfy the following axioms for all $a, b, c \in B$:

(1) Associativity of $\wedge, \vee$:
$a \wedge (b \wedge c) = (a \wedge b) \wedge c$ and $a \vee (b \vee c) = (a \vee b) \vee c$.

[1] Although $\wedge$ and $\vee$ are the same symbols as the ones used for the propositional connectives *and* and *or*, here they are taken as new symbols with different meaning. It might be clearer to use different symbols, but we should get used to the fact that there is only limited number of typographically acceptable symbols, and potentially infinitely many mathematical concepts. Therefore, the same symbol may be used in different meanings, depending on the context.

(2) Commutativity of $\wedge, \vee$:
$a \wedge b = b \wedge a$ and $a \vee b = b \vee a$.
(3) Absorption:
$a \wedge (a \vee b) = a$ and $a \vee (a \wedge b) = a$.
(4) Distributivity:
$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
(5) Axioms of constants:
$a \vee -a = 1$ and $a \wedge -a = 0$.

Exercise: Basic operations on sets.
Verify that if x is a nonempty set, then $\langle \mathscr{P}(x), \cap, \cup, -, \emptyset, x \rangle$ is a Bolean algebra, called the *powerset algebra*, when we identify $\wedge$ with intersection, $\vee$ with union, $-a$ with the operation of subtraction $x - a$, 0 with the emptyset and 1 with the set x. Show also that the de Morgan's law holds:

$$-(a \cup b) = -a \cap -b \text{ and } -(a \cap b) = -a \cup -b.$$

[Hint: Use the fact that the propositional connectives form a Boolean algebra: i.e. they satisfy the axioms (1)–(5) above when instead of B we have the two-element set $\{0, 1\}$ (where 0 stands for "false" and 1 for "true"), and we identify $\vee$ with disjunction, $\wedge$ with conjunction, $-$ with negation. For instance the operation $\cap$ is commutative because $\wedge$ is commutative: $(\forall q)[(q \in x \wedge q \in y) \leftrightarrow (q \in y \wedge q \in x)]$.]

(xii) Generalisation of $\cup$ and $\cap$ for any set x:

$$\bigcup x = \{q \mid (\exists y)(y \in x \wedge q \in y)\} \text{ and } \bigcap x = \{q \mid (\forall y)(y \in x \to q \in y)\}.$$

Exercise. $\bigcup\{x, y\} = x \cup y$, $\bigcap\{x, y\} = x \cap y$. $\bigcap \emptyset = V$ (all sets), $\bigcup \emptyset = \emptyset$.

Notation. To shorten our expressions, we will write $\forall x \in y \varphi(x)$ instead of $(\forall x) x \in y \to \varphi(x)$ and $\exists x \in y \varphi(x)$ instead of $(\exists x) x \in y \wedge \varphi(x)$.

We further assume there exists one infinite set. We capture the intuitive notion of infinity by the following definition (we view every inductive set as infinite):

Definition 1.1 *A set x is called* inductive *if it contains $\emptyset$ and with every element y in x, x also contains the set $y \cup \{y\}$.*

Axiom of Infinity. There exists an inductive set.

Remark 1.2 Intuitively, Axiom of Infinity states that "the collection of all natural numbers forms a set". We use the more abstract statement featuring inductive sets because we have not yet defined what a natural number is (so morally speaking, our Axiom of Infinity states that there exists a set which contains the set of natural numbers).

Comment: $y \cup \{y\}$ is the set-theoretical "translation" of the concept $+1$ from the natural numbers. The reason is that there are good reasons to prohibit existence of sets x such that $x \in x$, therefore $y \cup \{y\}$ contains exactly one new set with respect to y, namely the set y: $y \notin y$, while $y \in y \cup \{y\}$. It should seem reasonable that if a collection of objects is closed under the operation "+1", it can never be finite. Hence, our notion of "inductiveness" is a reasonable formalisation of the notion of "infinity".

It looks like we could define that the set of natural numbers, which we want to denote as $\mathbb{N}$, is an inductive set whose existence is postulated in the Axiom of infinity. However, there are more inductive sets, and we definitely want to have "unique" natural numbers.

We therefore choose to define $\mathbb{N}$ as the *smallest* inductive set, in set-theoretical language it means the following:

Definition 1.3 (Natural numbers) $\mathbb{N}$*, the set of natural numbers, is defined as*

$$\mathbb{N} = \bigcap \{x \mid x \text{ is an inductive set}\}, \tag{1.1}$$

in other words $\mathbb{N}$ *is defined to be the intersection of all inductive sets.*

As a corollary, we can conclude that we have managed to define a *unique* set which will represent for us the natural numbers.[2]

We identify: $\emptyset$ with 0, $\emptyset \cup \{\emptyset\} = \{\emptyset\}$ with 1, $\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$ with 2, etc. In general the number $n \in \mathbb{N}$ is identified with the set $\{0, \ldots, n-1\}$.

Claim 1.4 *If* A *is any inductive set, then* $\mathbb{N} \subseteq A$.

Proof. Let x be an arbitrary element of $\mathbb{N}$, we need to show that x is also in A. Since $x \in \mathbb{N}$, then it is by definition of $\mathbb{N}$ an element of every inductive set. In particular, it is an element of A which is by assumption inductive. □

Now we show that $\mathbb{N}$ is still big (notice that Claim 1.4 would still be true if $\mathbb{N}$ were equal to $\emptyset$, which would disqualify $\mathbb{N}$ as the set of natural numbers).

Claim 1.5 $\mathbb{N}$ *is inductive. It follows that* $\mathbb{N}$ *is the smallest inductive set with respect to inclusion.*

Proof. $\emptyset$ must be in $\mathbb{N}$ because it is in every inductive set. If $x \in \mathbb{N}$, then x is in every inductive set, and hence also $x \cup \{x\}$ is in every inductive set. It follows that $x \cup \{x\}$ is in $\mathbb{N}$, and so $\mathbb{N}$ is inductive. By Claim 1.4, $\mathbb{N}$ is the least inductive set. □

The following important Induction theorem holds about $\mathbb{N}$:

Theorem 1.6 *Assume* A *is a subset of* $\mathbb{N}$ *such that* $\emptyset \in A$ *and for every* $n \in A$ *also* $n \cup \{n\} \in A$. *Then* $A = \mathbb{N}$.

Proof. Our assumption about A means that A is an inductive set. Since $\mathbb{N}$ is the least inductive set, we get $\mathbb{N} \subseteq A$. By the assumption of theorem, we also know that $A \subseteq \mathbb{N}$, which implies $\mathbb{N} = A$ as required. □

In addition to defining $\mathbb{N}$, we should also define the operations which we use with natural numbers: plus and times. We discuss this topic in more detail in Set Theory I. Just for illustration: we know that $n + 1$ is identified with set-theoretical operation $n \cup \{n\}$. What about $n \times m$? Intuitively, it will be the set of all pair $\langle a, b \rangle$ such that a comes from n and b comes from m. The notion of the ordered-pair is introduced properly in the next section.

[2] We have been a bit sloppy in Definition 1.3 in the interest of simplicity. Notice that the operation of intersection $\bigcap$ has been defined above only for sets: however the collection $\{x \mid x \text{ is an inductive set}\}$ in (1.1) is not a set! We will learn how to make this correct in Set Theory I.

1.1.1 Some more set theory

For the further sections, we need to introduce some more basic concepts from set theory.

We start by providing basic information concerning relations and functions.

If a, b are sets, then we know that $\{a, b\}$ is a set which contains exactly the sets a, b. This set is un-ordered: $\{a, b\} = \{b, a\}$ by extensionality. To be able to distinguish the order, we define an ordered pair $\langle a, b\rangle$ as follows:

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}.$$

This (rather awkward-looking) definition has the following property: if $a \neq b$, then $\langle a, b\rangle \neq \langle b, a\rangle$.

If x, y are sets, then the *Cartesian product* $x \times y$ of x, y is defined as follows:

$$x \times y = \{\langle a, b\rangle \mid a \in x \wedge b \in y\}.$$

A *binary relation* r on sets x, y is a subset of $x \times y$, i.e.

$$r \subseteq x \times y.$$

If r is a relation on x, y, we define the *domain* of r as

$$\mathrm{dom}(r) = \{q \mid (\exists q' \in y)\langle q, q'\rangle \in r\}. \tag{1.2}$$

and similarly we define *range* of r as

$$\mathrm{rng}(r) = \{q \mid (\exists q' \in x)\langle q', q\rangle \in r\}. \tag{1.3}$$

We also define the *inverse relation*

$$r^{-1} = \{\langle q, q'\rangle \mid \langle q', q\rangle \in r\}. \tag{1.4}$$

and if $a \subseteq x$ we define the *image of* r *on* a:

$$r''a = \{q \mid (\exists q' \in a)\langle q', q\rangle \in r\}. \tag{1.5}$$

If $a \subseteq x$ then we say that $r \restriction a$ is the *restriction* of r to a, where

$$r \restriction a = \{\langle q, q'\rangle \mid \langle q, q'\rangle \in r \wedge q \in a\}. \tag{1.6}$$

Exercise.

1. Check the following for binary relations x, w and sets y, z:
   (a) $x \cup w, x \cap w, x - w$ are binary relations,
   (b) $x''(y \cup z) = x''y \cup x''z$,
   (c)

   $$x''(y \cap z) \subseteq x''y \cap x''z \text{ and } x''y - x''z \subseteq x''(y - z). \tag{1.7}$$

   Give an example where the converse inclusion $\supseteq$ does not hold in (1.7). Compare with (1.11).

Composition of relations. If r, s are binary relations then the composition $r \circ s$ is defined as

$$r \circ s = \{\langle x, z\rangle \mid (\exists y)\langle x, y\rangle \in r \wedge \langle y, z\rangle \in s\}. \tag{1.8}$$

Exercise. Check the following for all binary relations r, s, t:
1. $\mathrm{dom}(r^{-1}) = \mathrm{rng}(r)$, $\mathrm{rng}(r^{-1}) = \mathrm{dom}(r)$, $(r^{-1})^{-1} = r$, $\mathrm{dom}(r \circ s) \subseteq \mathrm{dom}(r)$, $\mathrm{rng}(r \circ s) \subseteq \mathrm{rng}(s)$. When the identity holds in the last two formulas?
2. $(r \circ s)^{-1} = s^{-1} \circ r^{-1}$.
3. $r \circ (s \circ t) = (r \circ s) \circ t$.

A binary relation r is called a *function* if it satisfies the following:

$$(\forall x, y_1, y_2)(\langle x, y_1\rangle \in r \wedge \langle x, y_2\rangle \in r \to y_1 = y_2). \tag{1.9}$$

Since every function f is a relation, we can use for f the notation defined above for relations: Let f be a function.

- If $x \in \mathrm{dom}(f)$ we write $f(x)$ for the unique y such that $\langle x, y\rangle \in f$.
- If $a \subseteq \mathrm{dom}(f)$ we write $f[a]$ for $\{y \mid (\exists x \in a) f(x) = y\}$.

  Note that as f is a relation, it holds that $f[a] = f''a$ by the notation for relations; when dealing with functions however, we often (not always) prefer to use the notation $f[a]$.
- If $b \subseteq \mathrm{rng}(f)$ we write $f^{-1}[b]$ for $\{x \mid (\exists y \in b) f(x) = y\}$. Note again that this can be written as ${f^{-1}}''b$. Which notation is used depends on the context.

  Notation. Let $f : x \to y$ and $g : y \to z$ be two functions. This notation means that $\mathrm{dom}(f) = x$, $\mathrm{dom}(g) = y$ and $\mathrm{rng}(f) \subseteq y$ and $\mathrm{rng}(g) \subseteq z$. We will denote as $g \circ f$ the function $h : x \to z$ defined by $h(q) = g(f(q))$ for every $q \in x$. Note that this deviates from the notation used for composition of relations. The reason is that if we write $(g \circ f)(q) = g(f(q))$, it suggests that f is the first function which we apply.
- A function f is called *injective*, or 1-1, if it satisfies:

  $$(\forall x_0, x_1 \in \mathrm{dom}(f))\ x_0 \neq x_1 \to f(x_0) \neq f(x_1).$$

  Exercise. Verify that f is 1-1 if and only if f^{-1} is a function.
- f is *onto* y if $\mathrm{rng}(f) = y$.

Exercises.

1. Let $f : x \to y$ and $g : y \to z$ be 1-1 functions, then:
   (a) $g \circ f$ is 1-1.
   (b) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

2. Let x, y be any sets and f a function:[3]

$$(1.10)\quad (f^{-1})''(x \cap y) = (f^{-1})''x \cap (f^{-1})''y \qquad \text{and } (f^{-1})''(x - y) = (f^{-1})''x - (f^{-1})''y.$$

If f is moreover 1-1, then it also holds:

$$(1.11)\qquad f''(x \cap y) = f''x \cap f''x \text{ and } f''(x - y) = f''x - f''y.$$

Definition 1.7 *We say that $f : x \to y$ is a* bijection *if it is 1-1 and onto.*

Exercise. Verify that if f is a bijection from x onto y, then f^{-1} is a bijection from y onto x.

The notion of a bijection can be used to define the notion of a *finite set*:

Definition 1.8 *We say that x is* finite *if there is a bijection between x and some $n \in \mathbb{N}$. Otherwise we say that x is* infinite.

Finally, we define the notion of set exponentiation:

Definition 1.9 *If x and y are non-empty sets, we can consider the set of all functions $f : x \to y$:*

$$^{x}y = \{f \mid f : x \to y\}.$$

Examples

- Let set a contain 3 elements $a = \{1, 2, 3\}$, and set b four elements $b = \{a, b, c, d\}$. Decide which of the following is true:
  - There exists a 1-1 function from a to b.
  - There exists a 1-1 function from b to a.
  - There exists a function from a which is onto b.
  - Every function f from b to a is such that some element in a has two preimages under f in b, i.e. for some $x \in a$, there are at least two elements $y, z \in b$ such that $f(y) = f(z) = x$.
- Let set a be equal to all odd numbers and let b denote the natural numbers $\mathbb{N}$. Again decide which of the following is true:
  - There exists a 1-1 function from a to b.
  - There exists a 1-1 function from b to a.
  - There exists a function from a which is onto b.
  - Every function f from b to a is such that some element in a has two preimages under f in b, i.e. for some $x \in a$, there are at least two elements $y, z \in b$ such that $f(y) = f(z) = x$.

[3] Notice that if f is a function, then f^{-1} is a relation which is 1-1: $\langle x_1, y\rangle \in f^{-1}$ and $\langle x_2, y\rangle \in f^{-1}$ implies $x_1 = x_2$. This is actually the key property required to prove (1.10).

- Let x be a non-empty set. There is a bijection between the Cartesian product $x^2 = x \times x$, and the set ${}^2x$.

  Define a function $g : x^2 \to {}^2x$ as follows: to each pair $\langle a, b\rangle$ in x^2 assign the function $f : 2 \to x$ which to 0 assigns a and to 1 assigns b. Formally:

  $$g(\langle a, b\rangle) = \{\langle 0, a\rangle, \langle 1, b\rangle\} \text{ for every pair } \langle a, b\rangle \text{ in } x^2.$$

  Verify that g is really a bijection.

- Let x be a non-empty set. There is a bijection between the set of all subsets of x, $\mathscr{P}(x) = \{y \mid y \subseteq x\}$ and the set ${}^x2$.

  Let a be a subset of x. We say that χ_a is the *characteristic function* of a if $\chi_a : x \to 2$ such that

  $$\chi_a(q) = 1 \leftrightarrow q \in a.$$

  Thus χ_a says which elements are in a (they have value 1), and also which elements are not in a (they have value 0). Argue that a function g which assigns to each subset $a \subseteq x$ the characteristic function χ_a is the desired bijection.

1.1.2 The notions of size in set theory

If a, b are two finite sets, we say that a is bigger than b if there are more elements in a than in b. This seems to depend on our ability to measure the size of a and b by natural numbers: if the size of a is m and the size of b is n, then a is bigger than b if $m \geq n$. However, we can compare a, b without assigning them natural numbers: if there is an injective function from b into a, then a is clearly bigger. This definition can be generalised to infinite sets as well:

Definition 1.10 *A set a has the same size as a set b if there is a bijection f from a onto b, and we denote this by $a \approx b$. We say that a is smaller than b if there is a 1-1 function f from a into b, and we denote this by $a \preceq b$. We say that a is strictly smaller if $a \preceq b$ but $a \not\approx b$, and we denote this by $a \prec b$.*

If $a \approx \mathbb{N}$, then we say that a is countable. *If $\mathbb{N} \prec a$, we say that a is* uncountable.

**Exercise.*

– Let a denote the even natural numbers: $a \approx \mathbb{N} \approx \mathbb{N} \setminus a$.
– $\{0\} \times \mathbb{N} \approx \{1\} \times \mathbb{N}$.
– $\mathbb{N}^2 \approx \mathbb{N}$.

What about $\mathbb{N} \approx \mathscr{P}(\mathbb{N})$? Actually, this is false, as the following theorem shows:

Theorem 1.11 (Cantor) *For every set X it holds*

$$X \prec \mathscr{P}(X).$$

In particular, the set $\mathscr{P}(\mathbb{N})$ is uncountable.

PROOF. A function $h : X \to \mathscr{P}(X)$ defined by $h(x) = \{x\}$ for each $x \in X$ is clearly 1-1 from X to $\mathscr{P}(X)$. This means that X is smaller than $\mathscr{P}(X)$: $X \preceq \mathscr{P}(X)$.

Now we show that there is no bijection between X and $\mathscr{P}(X)$, which will imply $X \prec \mathscr{P}(X)$. Suppose for contradiction that there exists a bijection f from X onto $\mathscr{P}(X)$. Define

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

Note that $A \subseteq X$. Since $A \subseteq X$ (i.e. $A \in \mathscr{P}(X)$), there is $a \in X$ such that $f(a) = A$ because f is onto. It must be the case that either $a \in A$ or $a \notin A$: If $a \in A$, then $a \notin f(a) = A$, contradiction. If $a \notin A$, then $a \notin f(a)$ and so $a \in A$, contradiction. It follows that there cannot be a bijection between X and $\mathscr{P}(X)$. □

1.2 An axiomatic approach: Peano and Dedekind

The set-theoretical definition looks impressive, but one may wonder whether we have not reduced the problem of defining a natural number to something infinitely more complicated than the notion we have wanted to define. Indeed, if anything, sets look like more complicated things than natural numbers, and how are we supposed to define sets?

Here is another approach which avoids this problem by not saying *what* numbers are, but rather postulates which *properties* are true about them. These are the original five postulates of Guiseppe Peano (1858–1932):[4]

(1.12)

(P1) 0 is a natural number.
(P2) The successor of a natural number is a natural number.
(P3) 0 is not the successor of a natural number.
(P4) If two natural numbers have the same successor, then they are equal.
(P5) Any property which holds for 0, and which holds for the successor of any number for which it holds, is true for every natural number.

We will write $S(n)$ to denote the successor of a natural number.

Strangely enough, it is again the fifth postulate P5 which is problematic, although not in the way as the E5 of Euclid. The problem is with the word "property". Indeed, the reason for this axiomatic approach was (among other things) to avoid using the unrestricted (and possibly complicated) notion of a set. However, by our definition in item (viii) on page 5, a set is determined by a property. Hence P5 above can be rephrased as "Any set which contains 0 and which contains with each number also its successor, contains all natural numbers." This problem, which we will refer to as the problem of the postulate P5, is a difficult one, and it cannot be solved to satisfy all which one can desire for.

[4] We wish to mention here also the name of J. W. R. Dedekind, a German mathematician 1831–1916, who was interested in axiomatic approach to numbers, in particular to real numbers. The most common way to define real numbers was formulated by him, and is called *Dedekind completion of rational numbers*. For more information see Section 6.

1.2.1 The second-order solution to postulate P5

The second-order solution basically comes down to leaving the notion of set in place. Technically, we use the term *second-order* for expressions which refer not just to elements of the structure in question, but also to its *subsets*. In contrast, *first-order*, see next section, will be used for expressions which refer just to the elements of the domain in question.

(1.13) **Second-order axiomatisation of arithmetics.**

(P1–P4) from (1.12) plus,
(P5) $(\forall X)[(X(0) \wedge (\forall x)(X(x) \to X(S(x))) \to (\forall x)X(x)]$,
where $\forall X$ is the second-order quantifier ranging over subsets of the desired domain, and the expression $X(x)$ means that x is an element of the subset X.

With this second-order interpretation of P5, we are able to determine $\mathbb{N}$ uniquely in the sense that (morally speaking) there is exactly one structure which satisfies the axioms P1–P5.

This seems to be an excellent result, and one might conclude that the axiomatisation based on the second-order quantifiers is the intuitively most correct approach to axiomatisation of natural numbers. However, there are deep structural reasons which in practice lead to rejection of second-order logic, and hence of this axiomatisation. The main problem is that the logic built with second-order quantifiers has certain unpleasant properties (you will learn more in further logical lectures).

1.2.2 The first-order solution to postulate P5

The problem with the second order formulation of P5 is that it says something about all "properties" of natural numbers, or equivalently about all subsets of natural numbers. With the second order definition we manage to characterise the natural numbers, but at the expense of implicitly using set theory in the process. However, if we are allowed to use a set theory, then we can use the set-theoretical approach and do not need to bother with axiomatisation.

The true power of axiomatisation transpires when we restrict P5 to first-order formulas. The first-order logic has many mathematically nice properties (such as completeness), which make it in practice a preferred choice.

A first-order language permits the quantification of just the elements of the desired domain, not its subsets. So we can say "for every natural number $x \ldots$", but not "for every subset X of natural numbers $\ldots$".

How can one expresses P5 using a first-order language? The key is to realize that if $\varphi(x)$ is a first-order formula in the language of arithmetics, then it determines some property of natural numbers. For instance if $\varphi(x)$ is equal to the formula $\exists y\, x = S(y)$, then $\varphi(x)$ determines the property "to be a successor of a natural number". Thus, instead of quantifying over properties, we will just list all conceivable properties in a long (infinite) list. This is how it is done:

(1.14) **First-order axiomatisation of arithmetics (denoted PA).**

(Q1) $(\forall x, y)(S(x) = S(y) \to x = y)$,
(Q2) $(\forall x)(S(x) \neq 0)$,
(Q3) $(\forall x)(x \neq 0 \to (\exists y)x = S(y))$,
(Q4) $(\forall x)(x + 0 = x)$
(Q5) $(\forall x, y)(x + S(y) = S(x + y))$
(Q6) $(\forall x)(x \cdot 0 = 0)$
(Q7) $(\forall x, y)(x \cdot S(y) = x \cdot y + x)$
(P5*) For every formula $\varphi(x)$ in the language $\{0, S, +, \cdot\}$ (including parameters) the following is an axiom:

$$[\varphi(0) \wedge (\forall x)\,(\varphi(x) \to \varphi(S(x)))] \to (\forall x)\,\varphi(x).$$

Instead of having a single axiom P5 we have an Axiom scheme (P5*). However, this is not all, we also need to add to our language the symbols for addition and multiplication (and for ordering $\leq$, if we wish to have it). In the first-order axiomatisation, it is no longer true that addition and multiplication can be uniquely defined just from 0 and S (and from induction). Also, the axioms (P1,P2) are not needed because the presence of 0 as a constant already postulates that 0 is a "natural number", and the presence of S postulates that $S(x)$ is a "natural number". However, we explicitly include (Q3), which can be proved for the second-order axiomatisation. This axiomatisation is given in [1], where an interested student can find more information.

Still, naively, we could hope that by using the formulas we will somehow capture all the important properties of $\mathbb{N}$. However, this is not the case: in a strong way (which we will discuss in further lectures), the first-order axiomatisation allows the existence of structures which do not resemble $\mathbb{N}$: they are called *non-standard models of arithmetics*.

Remark 1.12 Note that we cannot solve the problem of how to refer to subsets of the universe by allowing quantification over formulas themselves: consider changing (P5) above to a single axiom which starts by "$(\forall\varphi)\ldots$. However, this is an invalid move because referring to all expressions inside language by an expression in that language immediately leads to severe problems. Consider the **Berry's paradox**: Since there are infinitely many natural numbers, there are certainly some such numbers which cannot be defined by any combination of 100 letters in English or less. Define n to be "the least number not definable in 100 letters or less." Then n *is* definable using 100 letters or less, which is a contradiction.

1.3 Finite combinatorics

The natural numbers are a complicated structure with a lot of difficult problems. Probably the oldest unsolved problem concerning prime numbers is as follows:

Goldbach's conjecture. Every even number greater than 2 is a sum of two primes.

Goldbach's conjecture seems too difficult for our current mathematical techniques; computers have verified that it is true up to $4 \cdot 10^{14}$. However, it does not mean that it is really true for *every* even number greater than 2. This shows the limits of computer-aided verifications of conjectures such as Goldbach's: in principle, the testing by a computer can answer the conjecture only if it is false (because than it suffices to run the testing up

to the first counterexample); if the conjecture is true, than no amount of testing will help (there is no counterexample we can possibly find). This is often referred to as *asymmetry* of the positive and negative solutions. Note however that even if the conjecture is false, the least counterexample n, i.e. the first even number > 2 which cannot be written as the sum of two primes, can be very big – so big that no conceivable testing can get that far.[5]

Thus if the Goldbach's conjecture is true, we can only verify it by finding a proof – no computation can help.

Goldbach's conjecture is too hard, but there are many other problems which we can solve. An example of such a problem is in Section 1.3.1

1.3.1 Ramsey theorem for graphs

In this section we will prove a famous theorem which concerns the degree of uniformity vs. chaos in finite structures. It is instructive to see how abstraction and mathematisation help us to extract mathematical meaning from a real-life problem.

The problem. Suppose there are n people at the party. What is the biggest group of people such that either everyone knows everyone in that group, or nobody knows anybody in that group (we call such a group *homogeneous*)? In particular is there a number n such that in every party with n people one can find a homogeneous group with 5 people (or any other number you wish)?

Intuitively, the bigger the homogeneous set, the more *order* we have in the group of people (or equivalently, less chaos).

Examples. From popular mathematics, one perhaps knows that in any party with at least 6 people there is a homogeneous group with 3 people. In a party with at least 18 people, there is a homogeneous group with size 4. What about a homogeneous group of size 5? Currently, it is known that it suffices to have a party of 46, but it is currently unknown whether 45, 44 or 43 is not enough. How do we get these numbers? And how is it possible that we do not know the exact number for a homogeneous group of size 5? After all 43 is a very small number, so perhaps computers could help us here?

To formulate this problem in the mathematical language, first notice that it is irrelevant what the people in the party are – it is enough to know their number. Thus n people in a party can be represented by natural numbers $\{1, \dots, n\}$. The fact that two people m, k know each other can be represented by considering the set $\{m, k\}$. Thus we can represent the situation by fixing a set E of two-element subsets of $\{1, \dots, n\}$ such that for any pair of people k, m, k knows m if and only if $\{k, m\} \in E$.[6]

The pair $\langle \{1, \dots, m\}, E \rangle$ is an example of a symmetric graph:

Definition 1.13 *Let V be a non-empty set and E a subset of $[V]^2$, where $[V]^2$ is the set of all two-element subsets of V, i.e.*

$$[V]^2 = \{\{v_1, v_2\} \mid v_1 \neq v_2 \ \& \ v_1, v_2 \in V\}.$$

[5] The estimate on the number of atoms in the whole known universe is $\leq 10^{100}$; so it seems that a number such as $10^{10^{10000}}$ is literally too big for any conceivable testing. There are examples of conjectures with the counterexamples very big.

[6] Notice that we need to make some extra assumptions in formalising the problem: we have decided that the relation of knowing one another is symmetric: k knows m if and only if m knows k.

We call elements in V vertices*, and elements in E* edges*. The pair $\langle V, E\rangle$ is called a* symmetric graph*.*

If we changed the definition by writing $E \subseteq V^2$, then we get the notion of a *directed* graph – in a directed graph, one considers also the order of the elements in the edges: $\langle v_1, v_2\rangle$ may be in E, but $\langle v_2, v_1\rangle$ not (and $v_1 = v_2$ is allowed).

What is the number of symmetric graphs on n vertices?

Lemma 1.14 *For $n > 1$, there are 2^l many symmetric graphs on n vertices, where $l = \frac{1}{2}n(n-1)$. This means that the number of graphs grows roughly exponentially with the number of vertices.*

Proof. There are n^2 ordered pairs in the set V^2, where V is the set of vertices and $|V| = n$. Notice there are n many pairs $\langle v, v\rangle$ in V^2, and for any two $v_1 \neq v_2$ elements in V, $\langle v_1, v_2\rangle$ and $\langle v_2, v_1\rangle$ are both in V^2. Thus we can write $n^2 = 2l + n$, where the number n counts the pairs $\langle v, v\rangle$, and l counts half of the pairs $\langle v_1, v_2\rangle$ and $\langle v_2, v_1\rangle$ for $v_1 \neq v_2$. It is easy to see that the size of $[V]^2$ is l when we identify $\{v_1, v_2\}$ with $\langle v_1, v_2\rangle$ (and do not count $\langle v_2, v_1\rangle$). By manipulating the equation $n^2 = 2l + n$, we get $l = \frac{1}{2}n(n-1)$.

Notice that the number of graphs is equal to the number of subsets of $[V]^2$ because for fixed V, a graph is determined by the set of edges E and $E \subseteq [V]^2$. Since for every m, the number of subsets in a set of size m is 2^m, we get that the number of graphs is 2^l for $l = \frac{1}{2}n(n-1)$. □

Example. We have discussed above that it is currently unknown what is the least number n such that every symmetric graph on n vertices has a homogeneous set of size 5 (we only know that n is in the set $\{43, 44, 45, 46\}$). To answer this question, it is enough to check all symmetric graphs on 43 vertices (and possibly on 44 or 45 if we find a counterexample with 43 vertices). This seems feasible until we calculate the number of such graphs: $2^{\frac{1}{2}43\cdot 42}$ which is extremely big. Of course, finding the exact number for a homogeneous set of size 6, 7, 101, etc. is even more difficult. The crude force will not going to help us here.

Definition 1.15 *Let $\langle V, E\rangle$ be a symmetric graph. We say that $H \subseteq V$ is a homogenous set of vertices if either all vertices in H are connected by edges with every other element in H (i.e. $[H]^2 \subseteq E$), or no elements in H are connected with edges (i.e. $[H]^2 \cap E = \emptyset$).*

We now have everything set up to formulate a mathematical theorem corresponding to the above problem.

Theorem 1.16 (Finite Ramsey theorem) *Let k be a natural number, $k > 1$. Then there exists a number n such that every symmetric graph $\langle V, E\rangle$ on n vertices has a homogeneous subset of size at least k.*

Proof. Our strategy is to find in every graph on $n > 1$ vertices a homogenous set of size at least $\frac{1}{2}\log_2 n$. For a given k, it therefore suffices to take n equal to 2^{2k} because then

$$\frac{1}{2}\log_2 n = k.$$

Without loss of generality $V = \{1, \ldots, n\}$ (we know that it does not matter what the elements in V are). To simplify our exposition, note that we can represent unordered pairs in E by ordered pairs $\langle k, m\rangle$ with the condition that $k < m$. We say that a pair $\langle k, l\rangle$ has color c_1 if k and m are connected by an edge, and color c_0 otherwise. Denote $X_0 = V$. Fix the vertex 1, denote it v_0, and consider all pairs $\langle v_0, k\rangle$ for $1 < k \leq n$ and look at the color of the pairs. There must be one prevailing color; in other words there are at least $\frac{1}{2}(n-1)$-many pairs $\langle v_0, k\rangle$ which have all either color c_1 or color c_0. Choose this prevailing color, and consider the set $X_1 = \{v_0, v_1, \ldots\}$ of the vertices such that for every element $x > 1$ in X_1, $\langle v_0, x\rangle$ has the prevailing color. Now start with v_1 and consider the prevailing color for pairs $\langle v_1, x\rangle$ for $x \in X_1$, $x > v_1$, and define the set $X_2 = \{v_0, v_1, v_2, \ldots\}$ similarly as X_1. Repeat this argument several times till you have no more vertices to consider (i.e. till $X_r = \{v_0, \ldots, v_r\}$). Denote the resulting set of vertices $A = \{v_0, v_1, \ldots, v_r\}$. Now, for every $0 \leq i < r$, we do not lose more than one half of the elements in X_i when defining X_{i+1}. It follows that that we can carry out this construction at least $\log_2 n$-many times, and each time we repeat the step from X_i to X_{i+1} we fix one more element v_i which stays in A. Thus the size of A is at least $\log_2 n$.

A may not be homogenous but has the nice property that the color of any pair $\langle x, y\rangle$ in A, where $x < y$, depends only on the color of the first element. Choose a color which prevails and select those elements in A with this color. Denote the resulting set H. H is homogeneous and has size at least $\frac{1}{2}|A|$.

As we argued at the beginning, in order to prove the theorem, it suffices to take $n = 2^{2k}$. □

We have proved above that for any k there is some n such that all symmetric graphs with at least n vertices have a homogeneous set of size k. We even have an estimate on the number n: by the proof, if we choose n to be 2^{2k}, then we do find a homogeneous set of size k in any symmetric graph of size n. However, is n the *least* number which works? The least such n is called the *Ramsey* number of k, and is denoted $R(k)$. One can thus write up the examples above as: $R(3) = 6$, $R(4) = 18$, and $R(5) \in \{43, 44, 45, 46\}$. Notice that our bound 2^{2k} is not optimal for either of these cases. This means that a more complicated argument must be found. This is beyond the limits of our lecture...

Remark 1.17 Frank P. Ramsey (1903–1930) was a British mathematician and philosopher, and proved the theorem above.

Exercises.

1. In Lemma 1.14, we calculated the number of two-element subsets of a given set V. Generalise this result as follows: assume n is a natural number larger than 0, and k is in $\{1, \ldots, n\}$; let $\binom{n}{k}$ denote the number of all k-element subsets of a set with n elements. By Lemma 1.14, $\binom{n}{2} = \frac{n(n-1)}{2}$. Give an argument for computation of $\binom{n}{k}$. [Hint. When choosing the first element of a set with k elements, we can choose any element (so we have n options); once we choose the first one, we only have $n-1$ left to choose from, etc. The number $n(n-1)\cdots(n-(k-1))$ counts all ordered k-tuples of elements if we do not allow repetition of its elements; to get the number of subsets with k elements, we need to calculate the number of possible re-arrangement of a set with k elements, which equals to $k!$, and divide with $k!$ the number $n(n-1)\cdots(n-(k-1))$. Thus $\binom{n}{k} = \frac{n(n-1)\cdots(n-(k-1))}{k!} = \frac{n!}{(n-k)!k!}$.]

2. Using the previous exercise, and the fact that the number of all subsets of a set with n elements is 2^n, verify for every natural number n:

$$2^n = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}.$$

2 Integers $\mathbb{Z}$ as a group with respect to addition

Integers $\mathbb{Z}$ extend the natural numbers $\mathbb{N}$ and have the property that for every $n \in \mathbb{Z}$, there is an inverse element $-n \in \mathbb{Z}$ such that $n + (-n) = 0$. Integers $\mathbb{Z}$, together with the operations $+$ and $-$, are an example of a *group*.

2.1 Definition of a group

Definition 2.1 *We say that a set G together with the constant $e \in G$, binary operation $\circ : G^2 \to G$ and unary operation $' : G \to G$ is a* group *(grupa) if the following identities are true in G:*

(G1) Associativity. For all $x, y, z \in G$,
$(x \circ y) \circ z = x \circ (y \circ z)$,
(G2) Neutral element. For every $x \in G$,
$x = x \circ e = e \circ x$,
(G3) Inverse element. For every $x \in G$,
$x \circ x' = x' \circ x = e$.

If the operation $\circ$ is commutative, i.e.
(G4) For every $x, y \in G$, $x \circ y = y \circ x$,
we say that the group G is *abelian*, or commutative group.

Examples:

1. The structure $\langle \mathbb{Z}, +, -, 0 \rangle$, i.e. integers with addition $+$, inverse element $-$, and the constant 0, is a commutative group.

2. *Permutation groups.*
Sym($\mathbb{N}$), the permutation group on $\mathbb{N}$ is defined as follows: a function $p : \mathbb{N} \to \mathbb{N}$ is in Sym($\mathbb{N}$) if it is a permutation, i.e. a bijection between $\mathbb{N}$ and $\mathbb{N}$. The neutral element is the identity function id defined by $\mathrm{id}(n) = n$ for every n. The inverse to p is p^{-1}, the inverse function. The binary operation is the composition of functions.
Exercise. Show that Sym($\mathbb{N}$) is an example of a group which is not abelian.

   A group of permutations on a set X is also called the *symmetric group on X*. *Cayley's Theorem* states that every group is isomorphic to a subgroup of some symmetric group, in simple words, every group is included in some symmetric group. This means that symmetric groups of permutations are very general. See Section 2.2 for more information about subgroups.

One can show that every group satisfies some basic properties:

Lemma 2.2 *Let G be a group, then:*

(i) *The neutral element is unique. I.e. if f is an element in G such that $x \circ f = f \circ x = x$ for every x, then $f = e$. Also $e = e'$.*
(ii) *The inverse element is unique. I.e. given y in G, if z is an element in G such that $z \circ y = y \circ z = e$, then $z = y'$.*
(iii) *For every x, y in G:*
$(x \circ y)' = y' \circ x'$.
(iv) *For every x in G:*
$x'' = x$.
(v) *(The function $'$ is a 1-1 function.) For every $x, y \in G$:*
if $x \neq y$ then $x' \neq y'$.
(vi) *(Cancelation). For every $x, y, z \in G$:*
if $x \circ y = x \circ z$, then $y = z$, and if $y \circ x = z \circ x$, then $y = z$.

Proof. Ad (i). $f = e \circ f$ because e is the neutral element but also $e \circ f = e$ by our assumption about f. The second part follows easily by arguing as follows: $e = e \circ e'$ because e' is the inverse of e, but also $e \circ e' = e'$ because e is the neutral element.

Ad (ii) $z = z \circ e = z \circ (y \circ y') = (z \circ y) \circ y' = e \circ y' = y'$.

Ad (iii) Because the complement is unique by (ii), it suffices to show that $(y' \circ x') \circ (x \circ y) = (x \circ y) \circ (y' \circ x') = e$, however this is obvious: by associativity $(y' \circ x') \circ (x \circ y)$ is equal to $y' \circ (x' \circ x) \circ y = y' \circ e \circ y = y' \circ y = e$. Analogously for $(x \circ y) \circ (y' \circ x') = e$.

Ad (iv). By (ii) it suffices to show that x behaves as the inverse of x', i.e. that $x \circ x' = e$, but this is obvious from G3.

Ad (v). This is equivalent to the fact that $x' = y'$ implies $x = y$. However this is obvious: $x' = y'$ implies $x'' = y''$, which is by (iv) equivalent to $x = y$.

Ad (vi). Add to both sides of the equation x' from the left in the first case, and from the right in the second case: $x' \circ x \circ y = x' \circ x \circ z \leftrightarrow y = z$. □

2.2 Subgroups and Lagrange's theorem

In this section, we will study the general notion of a group and introduce some more set-theoretical notions (equivalences and congruences).

For simplicity, we will work in this section with commutative groups. Analogous results work for general groups as well.

2.2.1 Subgroups

Definition 2.3 *Let G be a commutative group with operations $\circ, ', e$ and H be a subset of G. We say that H is a* subgroup *of G, and write this as $H \leq G$, if:*
(i) *$e \in H$,*
(ii) *For every $x \in H$, $x' \in H$,*
(iii) *For every $x, y \in H$, $x \circ y \in H$.*
We express the conditions (i)–(iii) by saying that H is closed under the group operations.

Exercise. Convince yourself that every group G has at least two subgroups: one contains just the neutral element, and the second one is the whole group G (a group G is its own subgroup by the definition). There are groups, such as $\mathbb{Z}(p)$ for a prime number p (see below), which have just these two subgroups.

The conditions (i)–(iii) are equivalent to a single condition over any commutative group:

Lemma 2.4 *Let $H \subseteq G$ and $H \neq \emptyset$. Then the following holds: H is a subgroup of G if and only if for every $x, y \in H$, $x \circ y' \in H$.*

Proof. Exercise. □

Example. Consider the integers $\mathbb{Z}$ with the operations $+, -$ and the neutral element 0. Then for instance the set of all even numbers, with 0, and their inverses is a subgroup: $\mathbb{Z}_2 = \{k \mid \exists m \in \mathbb{Z}, k = 2m\}$. Note that $\mathbb{Z}_2$ contains no odd numbers, so it is a proper subgroup of $\mathbb{Z}$. In fact for every natural number $l > 1$, the set of all multiples of l, $\mathbb{Z}_l = \{k \mid \exists m \in \mathbb{Z}, k = lm\}$ is a proper subgroup of $\mathbb{Z}$. Fix now some such $l > 1$, say $l = 4$, and work with $\mathbb{Z}_4$. Notice now that by "shifting" the subgroup $\mathbb{Z}_4$ we can cover the whole set of integers in the following sense: for every integer q, consider the set $\mathbb{Z}_4 + q = \{k + q \mid k \in \mathbb{Z}_4\}$. Then by choosing $q = 0$, $q = 1$, $q = 2$, and $q = 3$ we get

$$\mathbb{Z} = \mathbb{Z}_4 \cup (\mathbb{Z}_4 + 1) \cup (\mathbb{Z}_4 + 2) \cup (\mathbb{Z}_4 + 3). \tag{2.15}$$

Exercise. Show that if $q_1 - q_2$ is divisible by 4, then $\mathbb{Z}_4 + q_1 = \mathbb{Z}_4 + q_2$.
Also note that for each $q, q' \in \{0, 1, 2, 3\}$ such that $q \neq q'$, $(\mathbb{Z}_4 + q) \cap (\mathbb{Z}_4 + q') = \emptyset$.
Systems like $\{(\mathbb{Z}_4 + q) \mid q \in \mathbb{Z}\}$ are called *partitions*. See Definition 2.6 in Section 2.2.2 for more detailed treatment of this notion.

2.2.2 Some more of set theory – equivalencies and partitions

Definition 2.5 *A binary relation R on a set A is called an* equivalence *if it satisfies for all $x, y, z \in A$:*

(i) $\langle x, x\rangle \in R$.
(ii) $\langle x, y\rangle \in R$ implies $\langle y, x\rangle \in R$.
(iii) $\langle x, y\rangle \in R$ and $\langle y, z\rangle \in R$ implies $\langle x, z\rangle \in R$.

If R is an equivalence relation on A and $a \in A$, let us define

$$[a]_R = \{b \in A \mid \langle a, b\rangle \in R\}. \tag{2.16}$$

$[a]_R$ is called the *equivalence class* of a. We also define the *quotient* of A by R, denoted by A/R:

$$A/R = \{[a]_R \mid a \in A\}.^{7} \tag{2.17}$$

Definition 2.6 *Let A be a set. A family $\mathscr{A} \subseteq \mathscr{P}(A)$ is called* a partition of A *if the following holds:*

(i) $\emptyset \notin \mathscr{A}$.
(ii) $\bigcup \mathscr{A} = A$.
(iii) For all $x \neq y$ in $\mathscr{A}$, $x \cap y = \emptyset$.

[7] If the relation R is obvious from the context, we will often just write $[a]$ instead of $[a]_R$.

Lemma 2.7 *Equivalences and partitions are equivalent in the following sense:*
(i) If R is an equivalence on a set A, then the quotient A/R is a partition of A.
(ii) If $\mathscr{A}$ is a partition of a set A, then there exists an equivalence relation R such that $A/R = \mathscr{A}$.

Proof. Ad (i). Since $a \in [a]_R$ for every $a \in A$, all classes $[a]_R$ in A/R are nonempty, and moreover $\bigcup A/R = A$. It remains to verify that if $[a]_R \neq [b]_R$, then $[a]_R \cap [b]_R = \emptyset$. We will show the converse: if there is y such that $y \in [a]_R \cap [b]_R$, then $[a]_R = [b]_R$. Let q be in $[a]_R$; then $\langle a, y\rangle \in R \wedge \langle q, a\rangle \in R$ and by transitivity (and symmetry) $\langle q, y\rangle \in R$. Because $y \in [b]_R$ we also obtain $\langle q, y\rangle \in R \wedge \langle b, y\rangle \in R$ which again implies $\langle q, b\rangle \in R$, and hence $q \in [b]_R$. If q is in $[b]_R$, just follow the previous argument backwards.

Ad (ii). Given a partition $\mathscr{A}$, define the relation R by

$$\langle x, y\rangle \in R \text{ iff } (\exists a \in \mathscr{A})\, x \in a \wedge y \in a \tag{2.18}$$

R is clearly reflexive and symmetric. If $\langle x, y\rangle \in R$ and $\langle y, z\rangle \in R$ and $x, y \in a$ and $y, z \in a'$ then $a \cap a'$ contains y is thus nonempty; by the definition of a partition this means that $a = a'$ and so $\langle x, z\rangle \in R$.

One can also show (*Exercise**) that this correspondence between partitions and equivalences on a set A is 1-1: i.e. given an equivalence R there is exactly one partition $\mathscr{A}$ such that $A/R = \mathscr{A}$, and given a partition $\mathscr{A}$, there is exactly one equivalence R such that $A/R = \mathscr{A}$. □

Notation. If R is an equivalence, we often write aRb instead of $\langle a, b\rangle \in R$. We often denote an equivalence by a symbol such as $\equiv$ or $\approx$ and write $a \equiv b$.

Exercise. Recall the construction of the partition in (2.15) and notice that it can be generalised to any number n (example (2.15) has $n = 4$) (see the next Exercise). Show that the equivalence relation associated to this partition in the sense of Lemma 2.7(ii) is defined by

$$k \equiv m \bmod n \leftrightarrow k - m \in \mathbb{Z}_n, \text{ for } k, m \in \mathbb{Z}.$$

We read the notation $k \equiv m \bmod n$ as "k is equivalent to m mod n".

Exercise. For any natural number $n > 1$, the system $\mathscr{A} = \{\mathbb{Z}_n + q \,|\, q \in \mathbb{Z}\}$ is a partition of $\mathbb{Z}$ into n many pieces.

2.2.3 Back to subgroups

The above construction with $\mathbb{Z}_n$ is just an example of a more general phenomenon. It holds that any subgroup of a group generates a partition. Here are details.

If H is a subgroup of G, and $x \in G$, let us call the set $H \circ x = \{h \circ x \,|\, h \in H\}$ a *coset of H*.[8]

Lemma 2.8 *Let G be a commutative group and H its subgroup. Then collection of all cosets of H forms a partition of G.*

[8] If G is not commutative, then we need to distinguish the left cosets $x \circ H$ and the right cosets $H \circ x$; of course if G is commutative then $x \circ H = H \circ x$ for every x, and so we do not need to make this distinction.

PROOF. Let us denote $G/H = \{H \circ x \,|\, x \in G\}$. We need to show that G/H is a partition.

Clearly, for any $x \in G$, the coset $H \circ x$ contains x because $e \in H$, and $e \circ x = x$. It follows that $\bigcup G/H = G$.

Lastly we need to show that if two cosets $H \circ x$ and $H \circ y$ are not identical, then they are disjoint. We will show the converse: $H \circ x \cap H \circ y \neq \emptyset \to H \circ x = H \circ y$. So assume $H \circ x \cap H \circ y \neq \emptyset$ and fix a in $H \circ x \cap H \circ y$. This means that

$$a = h_1 \circ x = h_2 \circ y \text{ for some } h_1, h_2 \in H.$$

From this we obtain by applying h_1' to both sides of the identity $h_1 \circ x = h_2 \circ y$:

$$x = h_2 \circ h_1' \circ y,$$

and similarly by applying h_2':

$$y = h_1 \circ h_2' \circ x.$$

Now let $z \in H \circ x$ be arbitrary, then $z = h \circ x$ for some $h \in H$; by substituting for x, we obtain $z = h \circ x = h \circ h_2 \circ h_1' \circ y$. Since $\bar{h} = h \circ h_2 \circ h_1'$ is in H, $z = \bar{h} \circ y$ is in $H \circ y$. Conversely, when $z \in H \circ y$, we substitute for y and show that $z \in H \circ x$. It follows $H \circ x = H \circ y$ as required. □

2.2.4 Lagrange's theorem on subgroups

If G is a finite commutative group, and H is its subgroup, then we can easily calculate the number of partition classes in G/H. Note that this does not hold for infinite G (for each $n > 1$, the subgroup $\mathbb{Z}_n$ is infinite, but the number of classes changes with n).

Theorem 2.9 (Lagrange) *Let G be a finite commutative[9] group and H its subgroup. Then the size of H divides the size of G, i.e. $\frac{|G|}{|H|} = n$ for some $n \in \mathbb{N}$.*

PROOF. By Lemma 2.8, the collection of cosets G/H forms a partition of G. We now show that each coset in G/H has the same size, and this size is equal to the size $|H|$ of H: for every $q \in G$:

$$|H \circ q| = |H|.$$

In order to see this, define a function $i : H \to H \circ q$ by $i(h) = h \circ q$ for each $h \in H$. i is by definition onto, and it is also 1-1, and hence a bijection, which implies $|H| = |H \circ q|$: i is 1-1 because if $h_1 \circ q = h_2 \circ q$, for some $h_1, h_2 \in H$, then $h_1 \circ q \circ q' = h_2 \circ q \circ q'$, and so $h_1 = h_2$.

It follows that the number of elements in G is equal to $n \cdot |H|$, where n is the number of classes in the partition G/H. □

The Lagrange's theorem provides information about possible subgroups of a group G. If for instance G has 21 elements, then any subgroup of G has size either 1 (the trivial group with just the neutral element), 3, 7 or 21.

[9] We assume commutativity only for convenience. The word "commutative" can be erased without affecting the truth of the theorem.

2.3 Finite groups $\mathbb{Z}(n)$

2.3.1 Congruences

In order to define $\mathbb{Z}(n)$, we need to introduce the notion of a congruence – a strengthening of the notion of an equivalence.

If the set A is the domain of some structure with operations defined on A, and $\equiv$ is an equivalence on A, there is a canonical way how to extend these operations to $A/\equiv$. Assume that $\oplus$ is a binary operation on A, that is a function from A^2 to A. We wish to extend $\oplus$ to some $\oplus^*$ defined on $A/\equiv$. If $[a]$ and $[b]$ are equivalence classes in $A/\equiv$, we define

$$[a] \oplus^* [b] = [a \oplus b]. \tag{2.19}$$

Thus the value of $\oplus^*$ when applied to $[a]$ and $[b]$ is calculated by first computing $a \oplus b$, and then taking the equivalence class which contains $a \oplus b$. However, some caution is due here: $\oplus^*$ may not be a correctly defined operation: assume that for some $a \equiv a'$ and $b \equiv b'$ it holds that $a \oplus b \not\equiv a' \oplus b'$. Then the definition of $\oplus^*$ is not correct because it is not a function: By our assumption about a, a', b, b', $[a] = [a']$ and $[b] = [b']$, but $[a] \oplus^* [b] \neq [a'] \oplus^* [b']$. If there are no such a, a', b, b', we say that R is *congruent* with respect to $\oplus$. We also express this fact by saying that the definition in (2.19) does not depend on the representatives of the equivalence classes.

In general we define:

Definition 2.10 *We say that an n-ary function $F : A^n \to A$ is* congruent *with respect to an equivalence $\equiv$ on A if for every two n-tuples $(a_0, \ldots, a_{n-1})$ and $(b_0, \ldots, b_{n-1})$ of elements in A^n it holds that*

$$\text{if } a_0 \equiv b_0 \wedge \ldots \wedge a_{n-1} \equiv b_{n-1}, \text{ then } F(a_0, \ldots, a_{n-1}) \equiv F(b_0, \ldots, b_{n-1}).$$

Note. We sometimes say that an equivalence $\equiv$ on A is a *congruence* if it is congruent with respect to all operations on A which we care about.

If F is congruent, then we can extend F to F^* by defining for every n-tuple of equivalence classes $([a_0], \ldots, [a_{n-1}])$:

$$F^*([a_0], \ldots, [a_{n-1}]) = [F(a_0, \ldots, a_{n-1})].$$

2.3.2 From partitions to groups

Continuing with our Example from the previous section, look at the partition $\mathbb{Z}/\mathbb{Z}_4$, which we will denote as $\mathbb{Z}(4)$. As it turns out the partition $\mathbb{Z}(4)$ itself can become a group which is in a precise sense determined by the original group $\mathbb{Z}$, and its subgroup $\mathbb{Z}_4$.

Define on $\mathbb{Z}(4)$ operations $\oplus$, *, and the constant $\mathbf{0}$:

$$\begin{aligned} \mathbf{0} &= \mathbb{Z}_4, \\ (\mathbb{Z}_4 + q)^* &= (\mathbb{Z}_4 + (-q)), \text{ where } q \in \mathbb{Z} \\ (\mathbb{Z}_4 + q_1) \oplus (\mathbb{Z}_4 + q_2) &= \mathbb{Z}_4 + (q_1 + q_2), \text{ where } q_1, q_2 \in \mathbb{Z}. \end{aligned} \tag{2.20}$$

We call $\mathbb{Z}(4)$ the *quotient group of $\mathbb{Z}$ by $\mathbb{Z}_4$*.

In order to verify that $\mathbb{Z}(4)$ is really a group with the operations as defined above, we need to check several points. First we need to address the question whether the operations above are correctly defined. By this we mean the following:

(*) The definition of the inverse * does not depend on the particular q we choose in the following sense: if

$$(\mathbb{Z}_4 + q_1) = (\mathbb{Z}_4 + q_2) \text{ for some } q_1, q_2,$$

then we need to have that

$$(\mathbb{Z}_4 + q_1)^* = (\mathbb{Z}_4 + q_2)^*.$$

(**) Similarly, the operation $\oplus$ does not depend on the particular q's: if

$$(\mathbb{Z}_4 + q_1) = (\mathbb{Z}_4 + q_2) \text{ and } (\mathbb{Z}_4 + q_3) = (\mathbb{Z}_4 + q_4), \text{ for some } q_1, \ldots, q_4,$$

then we need to have that

$$(\mathbb{Z}_4 + q_1) \oplus (\mathbb{Z}_4 + q_3) = (\mathbb{Z}_4 + q_2) \oplus (\mathbb{Z}_4 + q_4).$$

If the properties (*) and (**) hold, we say that the partition $\mathbb{Z}/\mathbb{Z}_4$ is *congruent* with respect to the operations $+$ and $-$ on $\mathbb{Z}$. A general discussion of this topic is included in Section 2.3.1 above.

Verification of (*) and (**) is not difficult, and we leave it as an *Exercise**.

Once the conditions (*) and (**) are verified, it remains to check that the structure $\langle \mathbb{Z}(4), \oplus, ^*, \mathbf{0} \rangle$ satisfies the axioms (G1)–(G4) of groups. This is again easy. We will just show (G3): we need to show that for any $q \in \mathbb{Z}$,

$$(\mathbb{Z}_4 + q) \oplus (\mathbb{Z}_4 + q)^* = \mathbf{0}.$$

The left-hand side of this identity is equal to $(\mathbb{Z}_4+q)\oplus(\mathbb{Z}_4+(-q)) = (\mathbb{Z}_4+(q+(-q)) = \mathbb{Z}_4$, using the definition of * and $\oplus$. However $\mathbb{Z}_4 = \mathbf{0}$, and we are finished. The rest of the axioms (G1),(G2), (G4) is left as an *Exercise**.

The construction of $\mathbb{Z}(4)$ can be generalised to any natural number n.

Definition 2.11 *For any natural number $n > 1$, we denote $\mathbb{Z}(n)$ the quotient group $\mathbb{Z}/\mathbb{Z}_n$, with the constant $\mathbf{0}$, inverse $*$ and addition $\oplus$, defined as in (2.20):*

$$\begin{aligned} \mathbf{0} &= \mathbb{Z}_n, \\ (\mathbb{Z}_n + q)^* &= (\mathbb{Z}_n + (-q)), \text{ where } q \in \mathbb{Z} \\ (\mathbb{Z}_n + q_1) \oplus (\mathbb{Z}_n + q_2) &= \mathbb{Z}_n + (q_1 + q_2), \text{ where } q_1, q_2 \in \mathbb{Z}. \end{aligned}$$

There is another, but equivalent description, of the group $\mathbb{Z}(n)$. In order to formulate this precisely, we will define the notion of an isomorphism for groups:

Definition 2.12 *Let $G = \langle G, \circ_1, ', e \rangle$ and $F = \langle F, \circ_2, ^*, f \rangle$ be two groups. We say that G and F are isomorphic, and write this as $G \cong F$, if there there is a bijection $i : G \to F$ such that:*

(i) $i(e) = f$ (i preserves the neutral element),

(ii) For every $x \in G$, $i(x') = (i(x))^*$ (i preserves the inverse),
(iii) For every $x, y \in G$, $i(x \circ_1 y) = i(x) \circ_2 i(y)$ (i preserves the binary operation).

Exercise. If $i : G \to F$ is an isomorphism, then $i^{-1} : F \to G$ is also an isomorphism.

An equivalent definition of $\mathbb{Z}(n)$. Set $G(n) = \{0, \ldots, n-1\}$ and define the following operations on $G(n)$:

Neutral element. The neutral element is 0.

Addition $\boxplus$. We define for every k, l in $G(n)$: $k \boxplus l = l \boxplus k = z$, where z is the unique number in the set $\{0, \ldots, n-1\}$ such that $k + l - z$ is the multiple of n (in other words z is the remainder after the division of $k + l$ by n: $k + l = pn + z$ for some $p \geq 0$). [The operation $+$ is the usual operation of addition on $\mathbb{N}$, and $-$ is the usual subtraction.]

Inverse element $'$. For $k \in G(n)$, $k > 0$, we define $k' \in G(n)$ to be the unique $k' \in G(n)$ such that $k + k' = n$. If $k = 0$, then $0' = 0$. [The operation $+$ is the usual operation of addition on $\mathbb{N}$.]

Lemma 2.13 *The group*

$$\langle G(n), \boxplus, ', 0 \rangle$$

is isomorphic to the group

$$\langle \mathbb{Z}(n), \oplus, ^*, \mathbf{0} \rangle.$$

Proof. (Exercise*). Define a function $i : \mathbb{Z}(n) \to G(n)$ by assigning to each coset $\mathbb{Z}_n + q$, $q \in \mathbb{Z}_n$, the number $r \in G(n)$ such that r is the remainder after dividing q by n, i.e.

$$q = kn + r, \text{ for some } k \in \mathbb{Z}_n.$$

In other words, given a coset $\mathbb{Z} + q$,

$$i(\mathbb{Z}_n + q) \text{ is the unique } r \in \{0, \ldots, n-1\} \text{ such that } (\mathbb{Z}_n + q) = (\mathbb{Z}_n + r).$$

□

The representation $\mathbb{Z}(n)$ using the partition $\mathbb{Z}/\mathbb{Z}_n$ is preferable to the direct description as given for $G(n)$ because it provides a more structural understanding of $\mathbb{Z}(n)$. Or to put it differently, the route from the group $\mathbb{Z}$ and its subgroup $\mathbb{Z}_n$ to the group $\mathbb{Z}(n)$ is an instance of a general technique which works even in cases where a "simple description" such as $G(n)$ is not available.

There is a connection between the group $\mathbb{Z}(n)$ and the group $\mathbb{Z}$. If we define a function $j : \mathbb{Z} \to \mathbb{Z}(n)$ which assigns to each $k \in \mathbb{Z}$ the unique coset $(\mathbb{Z}_n + q)$ such that $k \in (\mathbb{Z}_n + q)$, then this j has some nice properties. We call j the *quotient morphism generated by the subgroup* $\mathbb{Z}_n$. In fact j satisfies all the properties (i)–(iii) in Definition 2.12, except that j is not a bijection (it is not 1-1).

Remark 2.14 We say that a group G is *cyclic* if it is generated by a single element, i.e. there is some $g \in G$ such that the least subgroup in G which contains g is G. For instance $\mathbb{Z}$ is generated by 1. Similarly, for every $n > 0$, $\mathbb{Z}(n)$ is generated by 1. Let us note that any two cyclic groups of the same finite size, or two countable cyclic groups (there are no other), are isomorphic. Hence $\mathbb{Z}(n)$ for $n > 0$, and $\mathbb{Z}$ are the only cyclic groups up to isomorphism.

3 Integers $\mathbb{Z}$ as a ring

3.1 Definition of a ring

In $\mathbb{Z}$, in addition to the operation $+$, we can consider also the operation of multiplication $\cdot$. Integers $\mathbb{Z}$ with the operations of $+$ and $\cdot$ are an example of a *ring*.

We say that a structure $\langle R, +, -, 0, \cdot, 1\rangle$ is a *ring* if $1 \neq 0$, and the following properties hold for all $x, y, z \in R$:

(R1) Associativity for $+, \cdot$.

(R2) Commutativity for $+$.

(R3) Neutral element for $+$.
$0 + x = x + 0 = x$.

(R4) Inverse element for $+$.
$x + (-x) = (-x) + x = 0$.

(R5) Neutral element for $\cdot$.
$1x = x1 = x$.

(R6) Distributivity.
$x(y + z) = xy + xz$, $(y + z)x = yx + zx$.

Note that if R is a ring, we require that $\langle R, +, -, 0\rangle$ is an abelian group. This is a natural condition; in fact in the presence of the distributivity axiom (R6), if $\langle R, +, -0, \rangle$ is a group it *must* be abelian (i.e. commutative): let x, y be elements of R, then

$$(1 + 1)(x + y) = 1(x + y) + 1(x + y) = x + y + x + y, \tag{3.21}$$

using distributivity from the right

and

$$(1 + 1)(x + y) = (1 + 1)x + (1 + 1)y = x + x + y + y, \tag{3.22}$$

using distributivity from the left.

It follows that $x + y + x + y = x + x + y + y$. By adding $-x$ from the left, and then $-y$ from the right, we obtain $y + x = x + y$.

If the operation of $\cdot$ is commutative, i.e.

(R7) Commutativity for '$\cdot$': $xy = yx$,

we call R a *commutative ring*.

If moreover a commutative ring R has no zero-divisor, i.e.

(R8) $xy = 0$ implies $x = 0$ or $y = 0$,

we call R an *integral domain*.[10]

If moreover R carries a binary relation $\leq$ such that:

(R9) $\leq$ is a linear ordering,

(R10) Monotonicity with respect to $+$.
$x \leq y$ implies $x + z \leq y + z$,

[10] The existence of zero-divisors is not desirable if we want to have multiplicative inverses: assume $xy = 0$ and x and y are not 0, then neither x or y can have the inverse: assume x^{-1} is the inverse to x, then if we multiply $xy = 0$ by x^{-1}, we obtain $x^{-1}xy = x^{-1}0$, and so $y = 0$, which contradicts our initial assumption that both x and y are non-zero.

(R11) Monotonicity with respect to $\cdot$.
$x \leq y$ and $0 \leq z$ implies $xz \leq yz$,
we call R an *ordered ring*.

Fact 3.1 *The integers $\mathbb{Z} = \langle \mathbb{Z}, +, -, 0, \cdot, 1, \leq \rangle$ are an ordered commutative ring which is an integral domain.*

Lemma 3.2 *If R is a ring, then for all $x, y \in R$:*
(i) $0x = x0 = 0$.
(ii) $x(-y) = (-x)y = -(xy)$,
(iii) $-x(-y) = xy$,
(iv) $-x = (-1)x$,
If R is moreover an integral domain, then:
(v) $xy = xz$ *and* $x \neq 0$, *then* $y = z$ *(Cancellation law).*

Proof. Ad (i). Since 0 is the neutral element for $+$, it holds $x + 0 = x$. If we multiply both sides by x, we obtain $x(x + 0) = xx$. By distributivity, $xx + x0 = xx$. Now add to each side $-(xx)$, and obtain $x0 = 0$. And analogously for $0x = 0$.

Ad (ii).

$$\begin{aligned} x(-y) &= [-(xy) + xy] + x(-y) \\ &= -(xy) + [xy + x(-y)] \\ &= -(xy) + x(y + (-y)) \\ &= -(xy) + x0 \\ &= -(xy) + 0 \\ &= -(xy). \end{aligned}$$

And analogously for $(-x)y = -(xy)$.

Ad (iii).

$$\begin{aligned} (-x)(-y) &= -((-x)y) \\ &= -(-(xy)) \\ &= xy; \quad \text{by Lemma 2.2(iv).} \end{aligned}$$

Ad (iv). $(-1)x = -(1x) = -x$.

Ad (v).

$$\begin{aligned} 0 &= xy + (-(xz)) \\ &= xy + (x(-z)) \\ &= x(y + (-z)); \end{aligned}$$

since R has no zero-divisors and $x \neq 0$, it must be the case that $y + (-z) = 0$. This implies that y is inverse of $(-z)$ and so $y = -(-z) = z$. □

Corollary 3.3 *If R is a ring, then 0 cannot have an inverse element with respect to $\cdot$ and 1.*

Proof. Assume for contradiction that there is x in R such that $x \cdot 0 = 0 \cdot x = 1$. Since $0 \neq 1$, this contradicts (i) in Lemma 3.2. □

3.2 An example: $\mathbb{Z}(n)$ as a ring

Consider the group $\mathbb{Z}(n)$ defined above for $n > 1$. We know that $\mathbb{Z}(n)$ is isomorphic to the group $G(n)$ with domain $\{0, \ldots, n-1\}$ (see Lemma 2.13). It is this representation which we use here. We can turn $G(n)$ into a ring by defining the operation of multiplication as follows:

Multiplication $\otimes$. $l \otimes k = k \otimes l = z$, where z is the unique number in the set $\{0, \ldots, n-1\}$ such that $kl - z$ is the multiple of n (in other words z is the remainder after the division of kl by n: $kl = pn + z$ for some $p \geq 0$). [The operations $+$ and $\cdot$ are the usual operations of addition and multiplication on $\mathbb{N}$, and $-$ is the usual subtraction.]

Exercise. Verify that for $n > 1$, $\langle G(n), \boxplus, ', 0, \otimes, 1\rangle$ is a commutative ring. Notice however that $G(n)$ is not generally an integral domain (for instance in $G(4)$, $2 \otimes 2 = 0$).

One can show that $G(n)$ is an integral domain if and only if n is a prime number.

Remark 3.4 We could define the ring on $G(n)$ using a quotient construction similar to the one we used to obtain the group $\mathbb{Z}(n)$. We do not do it here for the lack of time.

3.3 The existence and uniqueness of the integers

We will construct the integers $\mathbb{Z}$ as the smallest extension of the natural numbers $\mathbb{N}$ which has the inverse element with respect to $+$ for every element in $\mathbb{Z}$. We will also want that $\mathbb{Z}$ becomes an integral domain: this is well motivated by the fact that $\mathbb{N}$ is itself "almost" an integral domain. One can check that the structure $\mathbb{N}$ with the operations $+, \cdot$ and constants $0, 1$ satisfies axioms R1–R3, R5–R8; that is all axioms of an integral domain except for the existence of the inverse for $+$. We want definitely to preserve these properties when extending to $\mathbb{Z}$. In fact $\mathbb{Z}$ will be an ordered integral domain.

In particular notice that $\mathbb{Z}$ will satisfy the properties in Lemma 3.2 because these are true for every integral domain. For instance, we view the otherwise "not-so-much-motivated" fact that the multiplication of two negative numbers should be a positive number as a necessary consequence of other properties which we hold as true about integers.[11]

Notation. As is customary in algebra, we will write (m, n) to denote an ordered pair $\langle m, n\rangle$. This is just a matter of notation, the meaning is the same.

Define a binary relation $\equiv$ on $\mathbb{N}^2$ by

$$(m, n) \equiv (k, l) \text{ iff } m + l = n + k.$$

Lemma 3.5 *$\equiv$ is an equivalence relation on $\mathbb{N}^2$.*

Proof. The relation $\equiv$ is clearly reflexive and symmetric. We verify transitivity: Assume $(m_1, n_1) \equiv (m_2, n_2) \equiv (m_3, n_3)$. By definition of $\equiv$, $m_1 + n_2 = n_1 + m_2$ and $m_2 + n_3 = n_2 + m_3$. If we add the left-hand sides and the right-hand sides, we obtain $m_1 + n_2 + m_2 + n_3 = n_1 + m_2 + n_2 + m_3$. By cancellation law for natural numbers, we obtain $m_1 + n_3 = n_1 + m_3$ as required. □

[11] The fact that $n(-m) = -(nm)$ can be motivated by viewing negative numbers as "quantities which measure a debt". In this framework, if we multiply our debt $-m$ by a number n, then we definitely have a bigger debt. This argument however does not seem to extend to multiplication of two debts.

Definition 3.6 *Let us define $\mathbb{Z} = \mathbb{N}^2/\equiv$. We call elements of $\mathbb{Z}$ integers.*

We wish to extend the operations $+$ and $\cdot$ to $\mathbb{Z}$. In fact, it will become obvious (see Theorem 3.9) that it suffices to show how to extend $+$ because this operation (together with the inverse) fully characterises the structure of integers. The operation of multiplication can be easily defined once we have this characterisation.

First notice that we can naturally extend $+$ to $\mathbb{N}^2$ by adding coordinate-wise: if (a, b) and (c, d) are pairs of natural numbers, we define

$$(a, b) \oplus (c, d) = (a + c, b + d),$$

where $\oplus$ is the extended operation of addition. By the discussion in the previous section, we need to verify that $\equiv$ is congruent with respect to $\oplus$ to extend $\oplus$ further to $\mathbb{Z}$.

Lemma 3.7 *The relation $\equiv$ is congruent with respect to operation addition $\oplus$ on $\mathbb{N}^2$.*

Proof. Assume that $(a, b) \equiv (k, l)$ and $(c, d) \equiv (m, n)$, i.e. $a+l = b+k$ and $c+n = d+m$. We want to show that $(a, b)\oplus(c, d) \equiv (k, l)\oplus(m, n)$, i.e. $(a+c)+(l+n) = (b+d)+(k+m)$.

$$\begin{aligned} (a + c) + (l + n) &= (a + l) + (c + n) \\ &\text{; by commutativity and associativity} \\ &= (b + k) + (d + m) \\ &\text{; by our assumption;} \\ &= (b + d) + (k + m) \\ &\text{; by commutativity and associativity.} \end{aligned}$$

□

Definition of operations on $\mathbb{Z}$.

(i) By results in Subsection 2.3.1, we can extend the operation $\oplus$ to an operation $\oplus^*$ on $\mathbb{Z}$ as follows: for all $m, n, k, l \in \mathbb{N}$:

$$[(m, n)] \oplus^* [(k, l)] = [(m, n) \oplus (k, l)].$$

(ii) If $[(m, n)]$ is an element of $\mathbb{Z}$, we define the inverse $-[(m, n)]$ as $[(n, m)]$.

(iii) The neutral element is defined to be $[(0, 0)]$.

Lemma 3.8 *$\mathbb{Z}$ together with the operation $\oplus^*$, the inverse element $-$, and the neutral element $[(0, 0)]$ is an abelian group.*

The proof is omitted. We just show that we now have inverse elements with respect to $+$:

The inverse element. Evidently, $[(m, n)] \oplus^* -[(m, n)] = [(m, n)] \oplus^* [(n, m)] = [(m + n, n + m)]$. Noticing, that for every $k \in \mathbb{N}$, $(k, k) \equiv (0, 0)$, it holds that $[(m + n, n + m)] = [(0, 0)]$, as required.

The following theorem claims that the smallest extension of $\mathbb{N}$ which is an abelian group is determined uniquely. The meaning of Theorem 3.9 in simple words is as follows: $\mathbb{Z}$ constructed above is up to isomorphism the unique integral domain which contains just natural numbers and their inverses.

Theorem 3.9 *Let $\langle \mathbb{Z}, \oplus, -, e\rangle$ and $\langle \mathbb{Z}^*, \oplus^*, *, e^*\rangle$ be two abelian groups which both contain an isomorphic copy of the structure $\langle \mathbb{N}, +, 0\rangle$, i.e. there are 1-1 functions $i : \mathbb{N} \to \mathbb{Z}$ and $i^* : \mathbb{N} \to \mathbb{Z}^*$ such that $i(0) = e$ and $i^*(0) = e^*$, and moreover for every $n, m \in \mathbb{N}$,*

$$i(n + m) = i(n) \oplus i(m) \text{ and } i^*(n + m) = i^*(n) \oplus^* i^*(m).$$

Assume further that every element of $\mathbb{Z}$ is either an element of $i[\mathbb{N}] = \{i(n) \mid n \in \mathbb{N}\}$, or an inverse of an element in $i[\mathbb{N}]$, and similarly every element of $\mathbb{Z}^*$ is either an element in $i^*[\mathbb{N}] = \{i^*(n) \mid n \in \mathbb{N}\}$, or an inverse of an element of $i^*[\mathbb{N}]$.
Then $\langle \mathbb{Z}, +, -, 0\rangle$ and $\langle \mathbb{Z}^*, +^*, *, 0\rangle$ are isomorphic via a function f which "fixes $\mathbb{N}$ pointwise", i.e. $f(i(n)) = i^*(n)$ for every $n \in \mathbb{N}$.

The proof is omitted.

4 Rational numbers $\mathbb{Q}$ as a field

4.1 Definition of a field

We wish to extend the integers $\mathbb{Z}$ to a field, i.e. preserve all good properties which are true of $\mathbb{Z}$, and add multiplicative inverses to all elements except 0. Note that we also have to make sure that not only the former elements of $\mathbb{Z}$ have inverses, also the new elements we add must have them.

Definition 4.1 *A ring R is called a* division ring *if every non-zero element x has a multiplicative inverse, i.e. there exists y such that $xy = yx = 1$. A commutative division ring is called a* field.

By the same argument as in Lemma 2.2(ii), the inverse to multiplication is unique. We will write x^{-1} to denote the unique inverse of x.

We now provide a different characterisation of a field:

Lemma 4.2 *$F = \langle F, +, -, 0, \cdot, ^{-1}, 1\rangle$ is a field according to Definition 4.1 if and only if $\langle F, +, -, 0\rangle$ is an abelian group, $\langle F - \{0\}, \cdot, ^{-1}, 1\rangle$ is an abelian group and distributivity connects the two binary operations, i.e. $x(y + z) = xy + xz$.*

Proof. Exercise. □

The notion of a field can be applied also to finite structures, but it is trivialised in the following sense for finite structures:

Lemma 4.3 *Any finite integral domain R is already a field. For instance if p is a prime number, then the ring $\mathbb{Z}(p)$ is a field.*

Proof. Consider a map $x \mapsto ax$ where a is some fixed $a \in R$ not equal to 0. Then this map is 1-1 from R to R by the cancellation law, and since R if finite, $\mathrm{rng}(f) = R$. It follows that there is some x such that $ax = 1$, and this x is the inverse of a. Since a is arbitrary non-zero, this shows that every element has a multiplicative inverse. □

Remark 4.4 A remarkable (and more complex than the above lemma) result of Wedderburn shows that any finite division ring is necessarily commutative, i.e. is a field.

Recall that the extension from $\mathbb{N}$ to $\mathbb{Z}$ can be viewed as a way of making the operation of subtraction total (i.e. everywhere defined). Similarly, the extension from $\mathbb{Z}$ to $\mathbb{Q}$ is a way of making the operation of *division* total. I.e. rational numbers should be the least extension of $\mathbb{Z}$ where for any $a, b \in \mathbb{Q}, b \neq 0$, there is unique c such that $a = bc = cb$, this c is written as $\frac{a}{b}$.

Lemma 4.5 *If R is a ring, then the following are equivalent:*
(i) Every element except 0 has an inverse with respect to multiplication.
(ii) The operation of division is correctly defined.

Proof. (i)→(ii). Given a, b as above, set $c = ab^{-1}$, then $a = bab^{-1} = bb^{-1}a$.
(ii)→(i). For a, set a^{-1} to be $\frac{1}{a}$. Then $1 = a\frac{1}{a} = aa^{-1}$. □

Recall that we have shown that 0 cannot have an inverse, because every ring satisfies $0 = x0$ for any x. In view of the Lemma above, this translates into the claim that division by 0 cannot be correctly defined: $\frac{1}{0}$ would be the inverse of 0.

Note. The only case when division by 0 could in principle be considered is $\frac{0}{0}$, however the value of this expression is not uniquely defined: indeed for any x, $x0 = 0$, and so $\frac{0}{0} = x$ for every x. We therefore decide that division by 0 is not defined for any $x \in R$.

4.2 Size of $\mathbb{Q}$

Although we are adding new elements to $\mathbb{N}$ to obtain $\mathbb{Z}$, and we add still more elements to $\mathbb{Z}$ to obtain $\mathbb{Q}$, one can show that if we measure "size" by bijection, all these number domains have the same number of elements (see Definition 1.10, where the relations $X \prec Y, X \preceq Y$, and $X \approx Y$ are introduced).

Lemma 4.6 *The size of $\mathbb{N}$ is the same as the size of $\mathbb{Z}$, i.e. $\mathbb{N} \approx \mathbb{Z}$.*

Proof. It suffices to construct a bijection $f : \mathbb{N} \to \mathbb{Z}$. There are many options, but consider for instance the following function:

$$\begin{aligned} f(0) &= 0, \\ f(2n) &= n, \text{ for } n > 0, \\ f(2n-1) &= -n \text{ for } n > 0. \end{aligned}$$

It is easy to check that f is 1-1 and onto. □

Before we show that $\mathbb{Q}$ has also the same size as $\mathbb{Z}$ and $\mathbb{N}$, we state some basic facts about sizes.

Lemma 4.7 *(i) If $X \approx Y$ and $Y \approx Z$, then also $X \approx Z$. And similarly, if $X \preceq Y$ and $Y \approx Z$, then $X \preceq Z$.*
(ii) If X, Y are two non-empty sets and $X \approx Y$, then also $X^2 \approx Y^2$. In particular $\mathbb{N}^2 \approx \mathbb{Z}^2$.

(iii) ***(Cantor-Bernstein)*** *If $X \preceq Y$ and $Y \preceq X$, then $X \approx Y$.*
(iv) $\mathbb{N} \approx \mathbb{N}^2$.

Proof. Ad (i). If $f : X \to Y$ and $g : Y \to Z$ are bijections, then it is easy to show that the composition $g \circ f : X \to Z$ is also a bijection. $g \circ f$ is 1-1 because if $x \neq y$ are two elements in X, then $f(x) \neq f(y)$ are two elements in Y (because f is 1-1) and so $g \circ f(x) = g(f(x)) \neq g(f(y)) = g \circ f(y)$ (because g is 1-1). $g \circ f$ is onto because if $z \in Z$ is an element in Z, then $f^{-1}((g^{-1})(z))$ is its preimage.

Ad (ii). Let $f : X \to Y$ be a bijection. We want to find a bijection $g : X^2 \to Y^2$. Define

$$g(\langle x, x' \rangle) = \langle f(x), f(x') \rangle, \text{ where } x, x' \in X.$$

It is easy to check that g is a bijection (*Exercise.*).

Ad (iii). This claim seems perfectly obvious (and is some sense it is), but its proof is not completely trivial. We will prove this theorem in Set Theory I.

Ad (iv). We will prove this theorem in Set Theory I. □

Theorem 4.8 *$\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are all countable sets, i.e.*

$$\mathbb{N} \approx \mathbb{Z} \approx \mathbb{Q}.$$

Proof. By the construction of the numbers, we trivially have:

$$\mathbb{N} \preceq \mathbb{Z} \preceq \mathbb{Q} \preceq \mathbb{Z}^2. \tag{4.23}$$

To verify (4.23), we need to find 1-1 functions witnessing the relation $\preceq$. Clearly $\mathbb{N} \preceq \mathbb{Z}$ because the identity function $\mathrm{id}_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}$ defined by $\mathrm{id}_{\mathbb{N}}(n) = n$ for each $n \in \mathbb{N}$ is a 1-1 function from $\mathbb{N}$ to $\mathbb{Z}$. Similarly, the identity function $\mathrm{id}_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q}$ shows that $\mathbb{Z} \preceq \mathbb{Q}$.

To see that $\mathbb{Q} \preceq \mathbb{Z}^2$, notice that each element of $\mathbb{Q}$ can be uniquely expressed by a pair of integers (a, b), and thus corresponds to an element in $\mathbb{Z}^2$, where $a \in \mathbb{Z}$ and $b > 0$ (see discussion in Remark 4.12). This correspondence is the required 1-1 function which witnesses $\mathbb{Q} \preceq \mathbb{Z}^2$.

Since $\mathbb{N} \approx \mathbb{Z}$ by Lemma 4.6, and $\mathbb{N} \approx \mathbb{N}^2$ by Lemma 4.7(iv), we obtain by Lemma 4.7(i)(ii) that $\mathbb{N} \approx \mathbb{Z}^2$. Thus we obtain:

$$\mathbb{N} \preceq \mathbb{Z} \preceq \mathbb{Q} \preceq \mathbb{Z}^2 \approx \mathbb{N}. \tag{4.24}$$

By Cantor-Bernstein theorem 4.7(iii), we can conclude that all these sets have the same size as $\mathbb{N}$, i.e.

$$\mathbb{N} \approx \mathbb{Z} \approx \mathbb{Q} \approx \mathbb{Z}^2 \approx \mathbb{N}. \tag{4.25}$$

□

4.3 The linear ordering on $\mathbb{Q}$

The ordering on $\mathbb{Q}$ has some special properties.

We can order $\mathbb{Q}$ as in (4.29) as follows (this gives the standard intuitive order):

$$\frac{m}{n} \leq \frac{k}{l} \Leftrightarrow ml \leq nk \text{ and } n, l > 0, \tag{4.26}$$

where $m, n, k, l \in \mathbb{Z}$.

We say that the ordering $\leq$ on a set A is *dense* if for every $a < b$ in A, there is $c \in A$ such that $a < c < b$. We say that a linear ordering $\leq$ on A is without *end points* if it has no least and no greatest element, i.e. there is no a_0 and a_1 such that $a_0 \leq x$ for every x and $x \leq a_1$ for every x.

Lemma 4.9 *The ordering $\langle \mathbb{Q}, \leq \rangle$ is a linear dense order without end points.*

Proof is omitted (though not difficult, as you may check for yourself).

4.4 Uniqueness of the ordering on $\mathbb{Q}$

The ordering on $\mathbb{Q}$ is unique in the following sense:

Theorem 4.10 *Let A be a countable set and $\preceq$ an ordering of A which is linear, dense and without end points. Then $\langle A, \preceq \rangle$ and $\langle \mathbb{Q}, \leq \rangle$ are isomorphic. It follows that up to isomorphism the ordering of $\mathbb{Q}$ is unique.*

Proof. Let us recall that $\langle A, \preceq \rangle$ and $\langle \mathbb{Q}, \leq \rangle$ are isomorphic if

(i) There is a bijection i from $\mathbb{Q}$ to A, and

(ii) For every q, q' in $\mathbb{Q}$:

$$q \leq q' \leftrightarrow i(q) \preceq i(q').$$

In the rest of the proof, we will construct such a function i.

Let $A = \{a_0, a_1, \dots\}$ and $\mathbb{Q} = \{q_0, q_1, \dots\}$ be some enumerations of A and $\mathbb{Q}$ (this is possible because by assumption A and $\mathbb{Q}$ are countable). We will define a sequence $\langle i_n \mid n < \omega \rangle$ of partial isomorphisms from $\mathbb{Q}$ to A. The final isomorphism between $\langle \mathbb{Q}, \leq \rangle$ and $\langle A, \preceq \rangle$ will be the union $\bigcup \{i_n \mid n < \omega\}$. The isomorphisms i_n's will satisfy the following:

(i) Domain of i_n will be a subset of $\mathbb{Q}$ of size $2n$, and moreover the domain of i_n will contain first n elements in the enumeration of $\mathbb{Q}$;

(ii) Range of i_n will be a subset of A of size $2n$, and moreover the range of i_n will contain first n elements of the enumeration of A;

(iii) i_n will be a partial isomorphism: it will be 1-1 and for all $q, q' \in \mathrm{dom}(i_n)$ $q \leq q' \leftrightarrow i_n(q) \preceq i_n(q')$;

(iv) Whenever $m \leq n$, then $i_m \subseteq i_n$.

The sequence $\langle i_n \mid n < \omega \rangle$ will be constructed by induction. Set $i_0 = \emptyset$. If i_n is already constructed, we construct i_{n+1} as follows. Consider the set $\mathbb{Q} \setminus \mathrm{dom}(i_n)$; let q be the unique rational number which is in this set and has the least index in the enumeration fixed above – that is, if $q = q_k$ for some $k < \omega$, then $q_k \in \mathbb{Q} \setminus \mathrm{dom}(i_n)$ and for all $k' < k$, $q_{k'} \in \mathrm{dom}(i_n)$. Choose a in $A \setminus \mathrm{rng}(i_n)$ so that $i_n \cup \{\langle q, a \rangle\}$ is a partial isomorphism.

This is possible because the ordering on A is without end-points and dense: for instance, if q is between some elements r and s in $\mathrm{dom}(i_n)$, one can choose a between $i_n(r)$ and $i_n(s)$. Repeat the previous construction on the A side: let b be the unique element of A with the least index of an element in $A \setminus \mathrm{rng}(i_n) \cup \{a\}$ and choose some p in $\mathbb{Q}$ so that $i_n \cup \{\langle q, a\rangle, \langle p, b\rangle\} = i_{n+1}$ is a partial isomorphism. Again, this can be done by density and lack of end-points of $\mathbb{Q}$.

Set $i = \bigcup\{i_n \mid n < \omega\}$. Since i_n's are increasing under inclusion, i is a function. Since i_n's were 1-1, so is i. The domain of i is equal to $\mathbb{Q}$ and the range to A. Similarly, since i is a union of isomorphisms, it is itself an isomorphism. In some detail, if $q \leq q'$ are in $\mathbb{Q}$, then q, q' appear in the enumeration of $\mathbb{Q}$, say $q = q_k$ and $q' = q_{k'}$, for $k, k' < \omega$. If $l = \max(k, k')$, then $q, q' \in \mathrm{dom}(i_{l+1})$, and so $q \leq q' \leftrightarrow i_{l+1}(q) \leq i_{l+1}(q')$, where $i_{l+1}(q) = i(q)$ and $i_{l+1}(q') = i(q')$. □

The construction in the previous theorem is called a *back-and-forth construction*: this is because we change sides from $\mathbb{Q}$ to A and back. This changing of sides is used to ensure $\mathrm{dom}(i) = \mathbb{Q}$ and $\mathrm{rng}(i) = A$.

Remark 4.11 The ordering $\leq$ on $\mathbb{Q}$ has the *Archimedean property*: for every $x \in \mathbb{Q}$ there is $n \in \mathbb{N}$ such that $x \leq n$. Indeed given $x > 0$, there are $m, n \in \mathbb{N}$ such that $x = \frac{m}{n}$. Clearly $\frac{m}{n} \leq \frac{m}{1} = m$.

4.5 Construction of $\mathbb{Q}$

We provide only hints, details can be found in [2].

The construction of $\mathbb{Q}$ is similar to that of $\mathbb{Z}$: we define a certain congruence on $\mathbb{Z}^2$. For (m, n) and (k, l) in $\mathbb{Z}^2$, where $n \neq 0$ and $l \neq 0$, define:

$$(m, n) \equiv (k, l) \;\Leftrightarrow\; ml = nk. \tag{4.27}$$

Intuitively, think of (m, n) as $\frac{m}{n}$. Then we say that two such fractions $\frac{m}{n}$ and $\frac{k}{l}$ are equivalent if the result of dividing m by n should be the same as the result of dividing k by l: this happens when $ml = nk$.

We define $\mathbb{Q}$ to be the set of all equivalence classes with respect to $\equiv$:

$$\mathbb{Q} = \{[(m, n)] \mid m, n \in \mathbb{Z}\}. \tag{4.28}$$

Exercise.* Show that $\equiv$ is an equivalence relation on $\mathbb{Z}^2$.

Exercise.* Show that $\equiv$ is a congruence with respect to operation $\odot$ of multiplication on pairs of integers defined coordinatewise:[12] i.e. if $(a, b) \equiv (k, l)$ and $(c, d) \equiv (m, n)$, then

$$(a, b) \odot (c, d) \equiv (k, l) \odot (m, n).$$

It follows that multiplication of the $\equiv$-equivalence classes can be defined by

$$[(m, n)] \odot^* [(k, l)] = [(mk, nl)].$$

[12] That is $(m, n) \odot (k, l) = (mk, nl)$.

Note that since R has no zero divisors, the value of nl is non-zero, and so the "fraction" $\frac{mk}{nl}$ is correctly defined.

The inverse $^{-1}$ to $[(m,n)]$, where $m,n \neq 0$, is defined as

$$[(m,n)]^{-1} = [(n,m)].$$

This definition really gives the inverse since $[(m,n)] \odot^* [(n,m)] = [(1,1)]$ for every $[(m,n)]$ (where $n,m \neq 0$), as can be easily checked (Exercise*).

Remark 4.12 We can uniformly choose a *representative* from each equivalence class $[(m,n)] \in \mathbb{Q}$. This representative is defined to be the unique pair $(a,b) \in [(m,n)]$ such that $a,b \in \mathbb{Z}$ have no common divisor other than 1. We may further require that this representative (a,b) has the special form that either both a,b are ≥ 0 (with $b \neq 0$), or $b > 0$ and $a < 0$. We can then define

$$\mathbb{Q} = \{(a,b) \mid (\exists [(m,n)] \text{ such that } (a,b) \text{ represents } [(m,n)]\},$$

or in the more usual transcription

$$\mathbb{Q} = \{\frac{a}{b} \mid b > 0, a \in \mathbb{Z}, a, b \text{ have no common divisor other than } 1\}. \tag{4.29}$$

Note. The two definitions (4.28) and (4.29) are just two ways of writing down the same concept: (4.28) uses equivalence classes, (4.29) uses uniquely chosen representatives of the very same classes.

5 Analytic properties of $\mathbb{Q}$

5.1 Sequences and their limits

In preparation for extension of $\mathbb{Q}$ to $\mathbb{R}$, the real numbers, we will define the notion of a limit and show some basic properties.

We first define the *absolute value* of elements in $\mathbb{Q}$:

$$|q| = q \text{ if } q \geq 0, |q| = -q \text{ if } q < 0.$$

We look at $|q|$ as the size or length of q.

Lemma 5.1 *For all q,r,y and z in $\mathbb{Q}$:*
(i) $|q| \geq 0$ *for all* $q \in \mathbb{Q}$, *and* $|q| = 0 \Leftrightarrow q = 0$.
(ii) $|qr| = |q| \cdot |r|$, *and so in particular* $|q| = |-q|$ *for* $r = -1$.
(iii) $|q - r| = |r - q|$, *the distance between two rational numbers.*
(iv) $|q + r| \leq |q| + |r|$, $|q - z| \leq |q - y| + |y - z|$ *the triangle inequality.*

Proof. *Exercise.* □

We say that $(a_i)_{i \in \mathbb{N}}$ is a sequence of rational numbers if there is a function $f : \mathbb{N} \to \mathbb{Q}$ such that $f(i) = a_i$ for each $i \in \mathbb{N}$. To save some notation, we write just (a_i) instead of $(a_i)_{i \in \mathbb{N}}$.

Definition 5.2 *We say that* (a_i) converges *to a rational number* a*, and write this as* $\lim_{n\to\infty} a_n = a$*, or just* $\lim(a_n) = a$*, if for any rational number* $\varepsilon > 0$ *there is* $n_0 \in \mathbb{N}$ *such that for every* $n \geq n_0$*,* $|a_n - a| < \varepsilon$*.*

If (a_i) does not converge, we say that it *diverges*.

Here are some basic properties of limits.

Lemma 5.3 *(i) A limit, if it exists, is unique. That is if* $\lim(a_n) = a$ *and* $\lim(a_n) = b$*, then* $a = b$*.*

(ii) If (a_n) *and* (b_n) *differ at finitely many points, then either both have limits and they are the same, or they both diverge.*

(iii) If (a_n) *converges and* $q \in \mathbb{Q}$*, then* (qa_n) *converges and* $q\lim(a_n) = \lim(qa_n)$*.*

(iv) If (a_n) *and* (b_n) *converge, then* $(a_n + b_n)$ *converges and* $\lim(a_n) + \lim(b_n) = \lim(a_n + b_n)$*.*

(v) If (a_n) *and* (b_n) *converge , then* $(a_n b_n)$ *converges and* $\lim(a_n)\lim(b_n) = \lim(a_n b_n)$*.*

(vi) If (a_n) *converges and its limit is non-zero, and* $a_n \neq 0$ *for all* n*, then* $(\frac{1}{a_n})$ *converges and* $\lim(\frac{1}{a_n}) = \frac{1}{\lim(a_n)}$*.*

Proof. Ad (i). Assume for contradiction, that $a \neq b$ are two limits of (a_n). Choose $\varepsilon < |a - b|/2$. Then there must be some n_0 such that for every $n \geq n_0$, $|a - a_n| < \varepsilon$ and $|b - a_n| < \varepsilon$. But this is impossible by our choice of ε.

Ad (ii). If (a_n) and (b_n) differ at finitely many points, then for some n^*, every $n \geq n^*$ satisfies that $a_n = b_n$. We show that if (a_n) converges to a, then so does (b_n). Let $\varepsilon > 0$ be given. We need to find n_0 such that for every $n \geq n_0$, $|a - b_n| < \varepsilon$. Since (a_n) converges to a, there must be some m_0 such that for every $n \geq m_0$, $|a - a_n| < \varepsilon$. Choose $n_0 = \max(n^*, m_0)$. The argument when (a_n) diverges is similar.

Ad (iii). For $\varepsilon > 0$, we need to find n_0 such that for all $n \geq n_0$, $|qa - qa_n| < \varepsilon$, where a is the limit of (a_n). Assume $q \neq 0$ (otherwise (iii) holds trivially). We use the identity

$$qa - qa_n = q(a - a_n) \tag{5.30}$$

and the identity

$$|q(a - a_n)| = |q||a - a_n|. \tag{5.31}$$

If we choose n_0 such that for all $n \geq n_0$, $|a - a_n| < \varepsilon/|q|$, then by the above identities $|qa - qa_n| = |q||a - a_n| < \varepsilon$.

Ad (iv). For $\varepsilon > 0$, we need to find n_0 such that for all $n \geq n_0$, $|(a+b)-(a_n+b_n)| < \varepsilon$, where a is the limit of (a_n) and b the limit of (b_n). We use the identity

$$(a + b) - (a_n + b_n) = (a - a_n) + (b - b_n), \tag{5.32}$$

and the inequality

$$|(a + b) - (a_n + b_n)| \leq |a - a_n| + |b - b_n|. \tag{5.33}$$

If we choose $n_0 = \max(n_1, n_2)$, where n_1 satisfies that for all $n \geq n_1$, $|a - a_n| < \varepsilon/2$, and n_1 satisfies that for all $n \geq n_2$, $|b - b_n| < \varepsilon/2$, then by the above identity and inequality $|(a + b) - (a_n + b_n)| < \epsilon$.

Ad (v). This time we will proceed less directly and show that $\lim(a_nb_n - ab) = 0$. This will achieve our goal because by (iii) and (iv) above, this limit is equal to $\lim(a_nb_n) - ab$, and this implies that $\lim(a_nb_n - ab) = 0$ if and only if $\lim(a_nb_n) = ab$. We use the identity

$$a_nb_n - ab = (a_n - a)(b_n - b) + a(b_n - b) + b(a_n - a). \tag{5.34}$$

Again by (iii) and (iv), it suffices to show that $\lim((a-a_n)(b-b_n)) = 0$, $\lim(a(b_n-b)) = 0$, and $\lim(b(a_n - a)) = 0$. By (iii) and (iv), $\lim(a(b_n - b)) = 0$ whenever $a \lim(b - b_n) = 0$, whenever $\lim(b_n) = b$. The same holds for $\lim(b(a_n - a)) = 0$. It remains to show that $\lim((a - a_n)(b - b_n)) = 0$. Given $\varepsilon > 0$, we need to find n_0 such that for all $n \geq n_0$, $|(a - a_n)(b - b_n) - 0| < \varepsilon$. Choose $n_0 = \max(n_1, n_2)$, where for all $n \geq n_1$, $|a - a_n| < \sqrt{\varepsilon}$, and for all $n \geq n_2$, $|b - b_n| < \sqrt{\varepsilon}$.

Ad (vi). First choose n_0 such that for all $n \geq n_0$,

$$|a_n - a| < |a|/2, \text{ which implies } |a_n| > |a|/2. \tag{5.35}$$

Now, let $\varepsilon > 0$ be given. Choose $n_1 > n_0$ such that for all $n \geq n_1$,

$$|a_n - a| < \frac{1}{2}|a|^2\varepsilon. \tag{5.36}$$

Now for all $n \geq n_1$,

$$\Big|\frac{1}{a_n} - \frac{1}{a}\Big| = \Big|\frac{a_n - a}{a_na}\Big| = \frac{|a_n - a|}{|a_na|} < \frac{|a_n - a|}{|a|^2} < \frac{\frac{1}{2}|a|^2\varepsilon}{|a|^2} = \frac{1}{2}\varepsilon < \varepsilon. \tag{5.37}$$

□

5.2 An example: geometrical progressions

We say that a sequence (a_i) is geometrical if there are $b \neq 0$ and $q > 0$ in $\mathbb{Q}$ such that $a_i = bq^i$ for every $i \in \mathbb{N}$. For instance when $b = 1$ and $q = \frac{1}{2}$, we obtain:

$$1, \frac{1}{2}, \frac{1}{4}, \ldots.$$

We are interested in the "infinite sum" of the sequence (a_i):

$$a_0 + a_1 + a_2 \ldots.$$

We define this sum as follows: for each n let s_n be the sum of the first n-many elements of (a_i):

$$s_n = a_0 + \ldots + a_{n-1}.$$

If the sequence of partial sums (s_n) converges, we define the sum $\sum_{i\in\mathbb{N}} a_i$ of the whole sequence (a_i) as the limit of the partial sums:

$$\sum_{i\in\mathbb{N}} a_i = \lim(s_n).$$

We can easily give an equation for the value of s_n if (a_i) is a geometrical sequence. First note that $s_n = b + bq + \ldots + bq^{n-1} = b(1 + q + \ldots + q^{n-1})$, so we can without loss of

generality study just the geometrical sequences with $b = 1$. So let (a_i) be a geometrical sequence with $b = 1$, then for every $n \in \mathbb{N}$,

$$s_n + q^n = 1 + q + \ldots + q^n,$$

where the rigth-hand side is equal to $1+q(1+\ldots+q^{n-1}) = 1+qs_n$, and so $s_n+q^n = 1+qs_n$, and so

$$s_n - qs_n = 1 - q^n$$

and

$$s_n = \frac{1-q^n}{1-q}.$$

Let us apply this to the geometrical sequence with $q = \frac{1}{2}$. Then $s_n = 2-\frac{2}{2^n} = 2-\frac{1}{2^{n-1}}$, and so

$$\lim(s_n) = 2 - \lim(\frac{1}{2^{n-1}}).$$

Applying the definition on convergence, one can check (Exercise) that $\lim(\frac{1}{2^{n-1}}) = 0$, and so

$$1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots = \textstyle\sum_{i\in\mathbb{N}}(a_i) = \lim(s_n) = 2 - 0 = 2.$$

Remark 5.4 If (a_i) is a geometrical sequence, we call the sequence $a_0 + a_1 + \ldots$ a geometrical progression.

*Exercise**. For each $0 < q < 1$ (and $b = 1$ for simplicity), the geometrical progression with q converges.[13]

5.3 Cauchy sequences

We have shown above, in Section 5.2 devoted to geometrical progressions, that one can reasonably define the infinite sum

$$\textstyle\sum_{i\in\mathbb{N}} a_i = a_0 + a_1 + \cdots$$

for a sequence (a_i). We say that the infinite sum $\sum_{i\in\mathbb{N}} a_i$ exists and is equal to a if the sequence of partial sums (s_n), where $s_n = a_0 + \ldots + a_{n-1}$, converges to a. We have shown in Section 5.2 that if (a_i) is a geometrical sequence and $q < 1$, then the sum of the whole sequence exists (and can be easily calculated).

However, if (a_i) is not geometrical, then what is the condition on the existence of $\sum_{i\in\mathbb{N}} a_i$? Consider the following three examples:

E1 $1 + 2 + 3 + \cdots$,

E2 $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots$, so called "harmonic progression",

E3 $1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots$ (the Euler constant, e).

[13] When we say that a geometrical progression converges we mean that the sequence of the partial sums converges.

The sequence E1 does not converge because it gets bigger and bigger (see Lemma 5.8, where it is shown that every convergent sequence must be bounded). The case of E2 is not immediately obvious; however, one can show that also E2 gets bigger and bigger, and so it does not converge [Hint. Argue that the sum of the harmonic series is $\geq$ than the sum of the series $1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}\cdots$, which is clearly unbounded, and hence divergent.]. The sequence E3 however does not get bigger and bigger, so perhaps it should converge. The problem with E3 is that although the sequence of partial sums gets closer and closer to some number, this number does not exist in $\mathbb{Q}$! But for certain reasons, mathematicians would like to have this number. This motivates us to say that we would like to extend $\mathbb{Q}$ to $\mathbb{R}$ by adding the limits of all sequences, which "should converge". The correct formalisation of the vague notion "should converge" is attributed to A. L. Cauchy, French mathematician 1789–1857. He formulated the following definition:

Definition 5.5 *A sequence (a_n) of rational numbers is a* Cauchy sequence *if for every $\varepsilon > 0$ there exists n_0 such that for every $m, n \geq n_0$ it holds that $|a_m - a_n| < \varepsilon$.*

Thus the extension of $\mathbb{Q}$ to $\mathbb{R}$ is obtained by adding the limits of all Cauchy sequences. Here are some basic properties of Cauchy sequences.

Lemma 5.6 *Every convergent sequence is a Cauchy sequence.*

Proof. Let (a_n) be a sequence with $\lim(a_n) = a$ a let $\varepsilon > 0$ be given. We wish to find n_0 such that for every $m, n \geq n_0$, $|a_m - a_n| < \varepsilon$. By definition of a limit, there is some n_0 such that $|a - a_m| < \varepsilon$ and $|a - a_n| < \varepsilon$ for every $m, n \geq n_0$. By the triangle inequality in Lemma 5.1(iii),(iv), we have $|a_m - a_n| \leq |a - a_m| + |a - a_n| < 2\varepsilon$. This is apparently not sufficient because we wish to show $|a_m - a_n| < \varepsilon$. However, by a standard move in analysis, the argument is essentially the right one because we can start with $\frac{\varepsilon}{2}$, find n_0 as above to satisfy $|a - a_m| < \frac{\varepsilon}{2}$ and $|a - a_n| < \frac{\varepsilon}{2}$, so that finally $|a_m - a_n| \leq |a - a_m| + |a - a_n| = 2\frac{\varepsilon}{2} = \varepsilon$. □

Remark 5.7 Notice that it does not make sense to try to prove the converse to Lemma 5.6: i.e. that every Cauchy sequence converges. For instance the sequence E3 is a Cauchy sequence, but it does not converge in $\mathbb{Q}$ (because the number e is not rational). However, in $\mathbb{R}$, it will be true that a sequence of real number (a_n) converges if and only if (a_n) is Cauchy. Thus in $\mathbb{R}$, the Cauchy condition is sometimes called the *Cauchy's convergence criterion.*

Lemma 5.8 *Every Cauchy sequence is bounded.*

Proof. Let (a_n) be a Cauchy sequence. Apply the definition of being Cauchy with $\varepsilon = 1$: then there is some n_0 such that for all $m, n \geq n_0$, $|a_m - a_n| < 1$. In particular $|a_m - a_{n_0}| < 1$ for every $m \geq n_0$. It follows that for every $m \geq n_0$, $|a_m| \leq |a_{n_0}| + 1$. The bound k is defined to be the maximum of the elements $\{|a_0|, \ldots, |a_{n_0-1}|, |a_{n_0}| + 1\}$. □

Note that by combining Lemma 5.6 and Lemma 5.8, we get that every convergent sequence is bounded.

It turns out that the property of being a Cauchy sequence is the right condition which formalises the idea of a sequence which "should converge". Note that we now have a criterion for a sequence to converge without ever mentioning its limit! We will see in Section 6 that $\mathbb{R}$ can be defined as the smallest and unique (up to isomorphism) extension of $\mathbb{Q}$ where all Cauchy sequences converge.

6 Real numbers $\mathbb{R}$ as a completion of $\mathbb{Q}$

More details about the properties and the construction of $\mathbb{R}$ will be given in the optional lecture Introduction to mathematics II.

6.1 Achilles and Tortoise: Zenon's paradox

Why have not the ancient Greeks discovered real numbers? To simplify a little, one of the reasons is the proverbial Greek horror of infinity. It is best illustrated in the following notorious paradox.

In a simple setting, it runs as follows. Assume Achilles runs at the velocity $v_A = 1$ m/s and the Tortoise at the velocity $v_T = 1/2$ m/s. To offset the difference in velocities, the Tortoise has a head start of $1m$. The question is when does Achilles catch the Tortoise if they both start running at the same moment?

Solution 1; known to Greeks. Recall the following basic formula for calculation of distance s:

$$s = vt,$$

where v is the velocity and t the time. Since Achilles catches the tortoise at the moment when both have run the same distance, we look for t such that

$$s_A = v_A t \text{ is equal to } s_T = 1 + v_T t,$$

that is

$$t = 1 + 1/2t, \text{ which gives } t = 2.$$

This shows that Achilles catches the Tortoise after 2 seconds, that is after he has run 2 meters.

Solution 2; the paradox. However, the same task can be possibly solved as follows: The distance of Achilles from the start is $1m$ when the distance of Tortoise is $1 + 1/2$ m from the start; when Achilles runs $1 + 1/2$ m, the Tortoise runs $1 + 1/2 + 1/4$ m, and so on. It seems that Achilles can never catch the Tortoise because it will always be a little in front of Achilles. In fact the distance when Achilles catches the Tortoise is strangely enough given by the infinite sum

$$1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots . \tag{6.38}$$

Here is the paradox: Greeks knew that Achilles catches the Tortoise after $2m$, but they also knew that the distance is given by the infinite sum in (6.38). How is it possible that it should be equal to 2 when the sum is infinite and increasing? Or more generally, what is the meaning of an infinite sum?

The formalisation of infinite sums is a bold new concept discovered in the 16th century.

Recall that in Section 5.2 we have defined all notions necessary to give a correct meaning to infinite sums such as (6.38), and we have in fact calculated that the sum of (6.38) is 2.

It follows that with the notion of convergence and limit, there is nothing paradoxical in the Solution 2.

Remark 6.1 The number 2 is still a rational number, indeed a natural number. So what new numbers can we introduce with the use of infinite sums? The answer is that once we can deal with infinite sums, we can consider *arbitrary Cauchy sequences*, not only the simple sequences such as (6.38), and these will give numbers which are not rational. The example is the number e below. The use of arbitrary infinite sums is essential for the development of mathematical analysis, and thus the "horror of infinity" prevented the Greeks from developing mathematical analysis beyond rudimentary results.

6.2 What numbers are missing in $\mathbb{Q}$?

Already in ancient Greece, philosophers realised that there are some quantities which are not expressible as a ratio of two natural numbers (i.e. in our terminology, they are not equal to any rational number). The motivation for these quantities is *geometrical*, in contrast to the *algebraical* motivation used to extend $\mathbb{N}$ to $\mathbb{Z}$, and then $\mathbb{Z}$ to $\mathbb{Q}$. The geometrical motivation is based on the notion of a *continuous line without gaps*. The detailed study of continuous lines and related concepts (such as derivation and integration) is called *mathematical analysis*; that is why we sometimes say that the motivation for extension of $\mathbb{Q}$ to $\mathbb{R}$ is analytical. The mathematical analysis is strongly connected with the study of nature and real phenomena (physics).

Consider the following examples of quantities which are not present in $\mathbb{Q}$:

(A) Consider a parabole given by the formula $x^2 - 2 = 0$. The intuition based on the notion of "continuity" says that there must be some number r such that the parabole meets the line x in the point r, in other words that

$$r^2 - 2 = 0.$$

In fact, the same number can be described as the length of the hypotenuse of the right-angled triangle with sides 1.

Here is a simple argument, known already to ancients, that this r (if it exists) cannot be rational: Assume for contradiction that $r = \frac{p}{q}$ for some natural numbers p, q greater than 0 which have no common divisor. Then $(\frac{p}{q})^2 = 2$, and $\frac{p^2}{q^2} = 2$, and so $p^2 = 2q^2$. This means that p^2 is an even number, and so also p must be an even number (Exercise: check for yourself that if s is an odd number, then s^2 is also an odd number). Let us write $p = 2p_0$, then $p^2 = 4p_0^2 = 2q^2$; it follows that q^2 and so q is also even. This is a contradiction because we assumed that p and q have no common divisor greater than 1. It follows that r such that $r^2 - 2 = 0$ is not a rational number.

(B) Let r be the quantity which gives the ratio of the perimeter of a circle to its diameter. This r is a the well-known π: perimeter $= d\pi$, where d is the diameter of the circle.

One can show that π is not a rational number (it is not easy, and was first shown by Legendre in 1794).

π can be defined by means of a progression[14] as follows: For $x \in \mathbb{R}$, one can show that

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots , \tag{6.39}$$

and also

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots . \tag{6.40}$$

Then we can define that π is the least $x > 0$ such that $\sin x = 0$, or equivalently, the $2x$, where $x > 0$ is the least such that $\cos x = 0$.

One can still ask if there is some polynomial equation $p(n) = 0$ with rational coefficients such that π is the solution of this equation. A difficult result by Lindenmann (1882) shows that this is not the case. Thus π is even more complicated than $\sqrt{2}$: it is irrational but not a solution of any polynomial equation.

(C) Let r be the limit of the progression[15]

$$1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots .$$

This is the famous number e, the Euler constant. It is not difficult to prove that e is irrational (see Introduction to mathematics II). But more is true: just as π, e is not a solution of any polynomial equation with rational coefficients (this was first shown by Hermite in 1873).

The series defining e is an instance of the more general fact that there exists f with domain $\mathbb{R}$ as follows:

$$f(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots . \tag{6.41}$$

Note that $f(1) = e$. Thus we can write e^x instead of $f(x)$.

(D) Consider the parabole given by the equation $x^2 + 1 = 0$. Although in form similar to case (A), there seems to be no solid reason for introducing a "real number" r such that $r^2 + 1 = 0$. Indeed, there is no such real number.

However, for reasons not so easily motivated (note that there is no immediate *geometrical* reason for adding such a number), we still wish to have this number. It is denoted as i (the *imaginary* number to distinguish it from *real* numbers). By adjoining i to $\mathbb{R}$ we obtain the *complex numbers* $\mathbb{C}$.

The numbers such as $\sqrt{2}$ (case (A)) are called *algebraic irrational*. The word "algebraic" means that such numbers are obtained as solutions of polynomial equations with rational coefficients. For instance $\sqrt{3}$ and $\sqrt{5}$ are algebraic irrational numbers.

The numbers π and e are called *transcendental irrational numbers* because they cannot be obtained as solutions of polynomial equations with rational coefficients.

[14] One can check that the sequence of partial sums of this progression is a Cauchy sequence.
[15] One can check that the sequence of partial sums of this progression is a Cauchy sequence.

Remark 6.2 The definition of functions $\sin x, \cos x$, and e^x by means of the power series in (6.39), (6.40), and (6.41) has got the added benefit that it can be used to extend the operations sin, cos, and e^x to complex numbers $\mathbb{C}$. One can show the following fundamental formula:

$$e^{ix} = \cos x + i \sin x. \tag{6.42}$$

Another famous formula connecting the numbers $e, \pi, i, 1, 0$ is this one:

$$e^{\pi i} + 1 = 0. \tag{6.43}$$

6.3 Some facts about $\mathbb{R}$

6.3.1 Limits of Cauchy sequences of $\mathbb{R}$

Theorem 6.3 *The real numbers $\mathbb{R}$ are up to isomorphism the unique extension of $\mathbb{Q}$ such that:*

(i) $\mathbb{Q}$ is dense in $\mathbb{R}$ in the sense that for every pair $r_1 < r_2$ of real numbers there exists $q \in \mathbb{Q}$ such that $r_1 < q < r_2$,

(ii) Every Cauchy sequence of rational numbers converges.

Note that (ii) can be reformulated as follows: we say that $X \subseteq \mathbb{R}$ has the supremum in $\mathbb{R}$ if there is some r such that for all $x \in X$, $x \leq r$, and moreover whenever r' such that for all $x \in X$, $x \leq r'$, then $r \leq r'$ ($r \in \mathbb{R}$ satisfying this condition is called the supremum of X). We say that $X \subseteq \mathbb{R}$ is bounded from above if there is some $s \in \mathbb{R}$ such that for all $x \in X$, $x \leq s$.

Then we can prove:

Theorem 6.4 *The real numbers $\mathbb{R}$ are up to isomorphism the unique extension of $\mathbb{Q}$ such that:*

(i) $\mathbb{Q}$ is dense in $\mathbb{R}$ in the sense that for every pair $r_1 < r_2$ of real numbers there exists $q \in \mathbb{Q}$ such that $r_1 < q < r_2$,

(ii) Every subset $X \subseteq \mathbb{R}$ bounded from above has the supremum.

The construction of $\mathbb{R}$ using the suprema is attributed to Dedekind (the so called *Dedekind cuts* – see Section 6.3.3).

6.3.2 Size of $\mathbb{R}$

There are more real numbers than natural numbers. This is a consequence of Cantor's theorem because one can show (see Set Theory I) that there is a bijection between real numbers and the powerset of $\mathbb{N}$:

Fact 6.5 $\mathbb{R} \approx \mathscr{P}(\mathbb{N})$.

It follows by Cantor's theorem 1.11 that the set of real numbers is uncountable: $\mathbb{N} \prec \mathscr{P}(\mathbb{N}) \approx \mathbb{R}$.

In fact one can show the following:

(i) The number of all irrational numbers is the same as of all real numbers.

(ii) The number of algebraic irrational numbers is small: the set of algebraic irrational numbers is just countable (has the size of $\mathbb{N}$).
(iii) It follows that the majority of real numbers is transcendental: the set of all transcendental irrational numbers has the same size as the set of all real numbers.

6.3.3 $\mathbb{R}$ as a complete ordering

Definition 6.6 *Let $\langle X, \leq \rangle$ be a partially ordered set, not necessarily linearly ordered. We say $A \subseteq X$ has an* upper bound *if there is some $q \in X$ such that $a \leq q$ for all $a \in A$; similarly $A \subseteq X$ has a* lower bound *if there is some $q \in X$ such that $q \leq a$ for all $a \in A$. We say that x is the* supremum *of A if x is the least upper bound of A. We say that x is the* infimum *of A if x is the greatest lower bound of A.*

In general, a supremum, or an infimum, for $A \subseteq X$ may or may not exist, depending on $\langle X, \leq \rangle$ and A.

Definition 6.7 *We say that a linearly ordered set $\langle X, \leq \rangle$ is* order-complete *if every non-empty bounded set $A \subseteq X$ has the supremum and the infimum.*

The order-completeness can be formulated in an apparently weaker form, which however turns out to be equivalent.

Lemma 6.8 *Let $\langle X, \leq \rangle$ be an infinite linearly ordered set without end points.*[16] *The following are equivalent.*
(i) $\langle X, \leq \rangle$ is order-complete.
(ii) Every non-empty A bounded below has the infimum.
(iii) Every non-empty A bounded above has the supremum.

Proof. (i)→(ii). Choose any $x \in A$, such that $A_x = A \cap \{y \in A \mid y < x\}$ is non-empty (such x always exists if A has more than one element; if is has just one element, then this element is both the supremum and the infimum of A). Then A_x is bounded and so has the infimum, which is also the infimum of A, which can be easily verified.

(ii)→(iii). Define B to be the set of all upper bounds of A. Since A is bounded above, B is non-empty and bounded below. By (ii), it has the infimum b. We will show that in fact b is the supremum of A. To show that b is the supremum, we need to check two things:

(1) b is the upper bound of A.
(2) b is the least upper bound of A.

(1). Given $a \in A$, we want to show $a \leq b$: notice that a is a lower bound of B and because b is the greatest lower bound of B, this implies $a \leq b$ as required.

(2). Let b' be another upper bound of A, we want to show $b \leq b'$. Since b' is an upper bound of A, $b' \in B$. Since b is a lower bound of B, it satisfies $b \leq b'$ as required.

Since also (iii)→(ii) by an analogous argument, we can conclude that (iii) implies (i). □

[16] More general formulations are possible. We will use this one because it is of the main interest.

Theorem 6.9 *There is a unique ordered field $\mathbb{R}$ such that the ordering $\leq$ on $\mathbb{R}$ is order-complete, and such that $\mathbb{Q}$ is included in $\mathbb{R}$ as a subfield.*

The proof of the theorem proceeds by directly constructing $\mathbb{R}$. Two most known constructions – Dedekind's and Cantor's – are shortly introduced in the next sections.

6.4 Constructions of $\mathbb{R}$

6.4.1 Dedekind's construction of $\mathbb{R}$

Theorem 6.10 *There is a unique ordered field $\mathbb{R}$ such that the ordering $\leq$ on $\mathbb{R}$ is order-complete, and such that $\mathbb{Q}$ is included in $\mathbb{R}$ as a subfield.*

Note that when we say that $\mathbb{Q}$ is a subfield of $\mathbb{R}$ we mean that the operations of addition and multiplication in $\mathbb{R}$ when applied to members in $\mathbb{Q}$ coincide with the usual operations on $\mathbb{Q}$; moreover, the ordering coincides as well, and all the positive elements in $\mathbb{Q}$ are also positive in $\mathbb{R}$.

Exercise. Show that if $+$ coincides in $\mathbb{R}$ and $\mathbb{Q}$, then also the inverse element of some $q \in \mathbb{Q}$ in $\mathbb{R}$ is the inverse element of q in $\mathbb{Q}$. [Hint: The inverse element in $\mathbb{R}$ to q is the unique $q' \in \mathbb{R}$ such that $q + q' = 0$; since q is in $\mathbb{Q}$ there is some $q'' \in \mathbb{Q}$ which is the inverse element of q: $q + q'' = 0$; since $+$ coincides between $\mathbb{Q}$ and $\mathbb{R}$, we obtain in $\mathbb{R}$ that $q + q'' = q + q' = 0$; since the inverse element is unique in every group, we obtain $q' = q''$].

Exercise. Argue similarly for the inverse element with respect to multiplication.

Dedekind published in 1872 a construction of $\mathbb{R}$ which proves the above theorem 6.9. We shall briefly review how Dedekind's construction works. The construction essentially uses some fact about sets – the first evidence for the usefulness of the notion of a set in mathematics.

Elements of $\mathbb{R}$ will be certain subset of $\mathbb{Q}$ which we will call the *Dedekind's cuts*. We say that $\alpha \subseteq \mathbb{Q}$ is a cut if:

(i) α is not empty and $\alpha \neq \mathbb{Q}$,
(ii) α is an initial segment in the sense that if $q \in \alpha$ and $p < q$, then also $p \in \alpha$,
(iii) α has no greatest element.

We define $\alpha < \beta$ if α is a proper subset of β. And we define

$$\mathbb{R} = \{\alpha \mid \alpha \text{ is a cut in } \mathbb{Q}\}.$$

Note that we can identify a rational number q with the cut $\alpha_q = \{q' \in \mathbb{Q} \mid q' < q\}$, and so rational numbers are included in $\mathbb{R}$ as the cuts α_q for $q \in \mathbb{Q}$. However, $\mathbb{R}$ contains much more cuts, for instance the set $A = \{q \in \mathbb{Q} \mid q^2 < 2\}$ is a cut, and not of the form α_q for some rational number q (because $\sqrt{2}$ is irrational).

Now we can show:

Lemma 6.11 *The following holds of $\langle \mathbb{R}, \leq \rangle$:*
(i) $\leq$ is really a linear ordering on $\mathbb{R}$,
(ii) $\langle \mathbb{R}, \leq \rangle$ is order-complete.

PROOF. First notice the following simple consequences of the definition of $\leq$ on $\mathbb{R}$. Let α be a cut, then

$$\begin{aligned} &\text{If } p \in \alpha \text{ and } q \notin \alpha, \text{ then } p < q, \\ &\text{If } r \notin \alpha \text{ and } r < s, \text{ then } s \notin \alpha. \end{aligned} \tag{6.44}$$

Ad (i). Since $<$ on $\mathbb{R}$ is the relation of proper inclusion by our definition, we need to show that if α, β are two cuts, then

$$\alpha \subsetneq \beta \text{ or } \beta \subsetneq \alpha \text{ or } \alpha = \beta.$$

Suppose $\alpha \neq \beta$, and α is not a proper subset of β. We will show that β is a proper subset of α. If α is not a proper subset of β, and $\alpha \neq \beta$, there is some $q_0 \in \alpha$ such that $q_0 \notin \beta$. In order to show that $\beta \subsetneq \alpha$, consider an arbitrary element $p \in \beta$. By (6.44), it must be the case that $p < q_0$ because otherwise we would have that q_0 is in β. But since q_0 is in α, so is p.

Ad (ii). By Lemma 6.8, it suffices to show that if a nonempty $A \subseteq \mathbb{R}$ is bounded above, then it has the supremum. We will first argue that $\bigcup A$ is a cut. Then it follows by a general argument that $\bigcup A$ is the supremum.

The verification that $\bigcup A$ satisfies the conditions (i)–(iii) for a cut is straightforward: since A is bounded above, there is some q not in A, and so (i) holds. Conditions (ii) and (iii) follow from the definition of $\bigcup$. □

We further define the addition as follows:

$$\alpha + \beta = \{r + s \,|\, r \in \alpha, s \in \alpha\}.$$

And we also define the neutral element with respect to $+$ on $\mathbb{R}$:

$$0* = \text{ the set of all negative rational numbers.}$$

Then we show that for each α there exists β such that

$$\alpha + \beta = 0*,$$

this β will of course be the inverse element $-\alpha$.

With some more effort we can also define the multiplication of cuts.

6.4.2 Cantor's construction of $\mathbb{R}$

Theorem 6.12 *There is a unique ordered field $\mathbb{R}$ such that the ordering $<$ on $\mathbb{R}$ is oder-complete, and such that $\mathbb{Q}$ is included in $\mathbb{R}$ as a subfield.*

It is not a mistake we state the same Theorem again. Cantor provided another construction of $\mathbb{R}$ using the Cauchy sequences.

Here, we will give still less details than for the Dedekind construction. Naively, we take the elements of $\mathbb{R}$ to be the Cauchy sequences (q_n) in $\mathbb{Q}$. A Cauchy sequence (q_n) represents in $\mathbb{R}$ the limit to which (q_n) should converge. However, there is a little problem here: there may be more sequences converging to the same "number". We deal with this issue by defining an equivalence relation on all Cauchy sequences in $\mathbb{Q}$, identifying two sequences if they "should converge to the same number". The real numbers $\mathbb{R}$ are then defined as the set of all equivalence classes on the set of all Cauchy sequences.

6.5 Topological concepts and the notion of continuity

6.5.1 System of open sets

If $r_1 < r_2$ are two real numbers, we call the set $(r_1, r_2) = \{r \in \mathbb{R} \mid r_1 < r < r_2\}$ an *open interval*. For technical reasons, we also call $\emptyset$ and $\mathbb{R}$ open intervals. In general, we say that a subset $O \subseteq \mathbb{R}$ is *open* if for every $r \in O$ there exists an open interval (r_1, r_2) containing r such that $(r_1, r_2) \subseteq O$.

The collection of open sets of $\mathbb{R}$ satisfies the following properties:

Lemma 6.13 *(i) $\emptyset$ and $\mathbb{R}$ are open.*
(ii) If O_1 and O_2 are open, so is $O_1 \cap O_2$.
(iii) If $\{O_j \mid j \in J\}$ are open, where J is a non-empty set, then $\bigcup_{j\in J} O_j$ is open.

Proof. (i) is immediate.

Ad (ii). We first show that if $I = (r_1, r_2)$ and $I' = (s_1, s_2)$ are open intervals, then $I \cap I'$ is an open interval. If $I \cap I'$ is empty, then it is the open interval by definition. So assume the intersection is non-empty. Let us fix $r_1 < r_2$ and consider the relation of s_1 and s_2 to r_1 and r_2. If $s_1 \leq r_1$, then because $I \cap I'$ is non-empty, $s_2 > r_1$, and so $(r_1, \min(s_2, r_2)) = I \cap I'$ is an open interval. If $r_1 < s_1$, then because $I \cap I'$ is non-empty, it must actually be true that $r_1 < s_1 < r_2$. Then $(s_1, \min(s_2, r_2)) = I \cap I'$ is an open interval.

If $O_1 \cap O_2$ is empty, then it is open. So assume that the intersection is non-empty, and let $r \in O_1 \cap O_2$ be given. Let $I \subseteq O_1$ and $I' \subseteq O_2$ be two intervals containing r. By the above paragraph, the intersection $I \cap I' \subseteq O_1 \cap O_2$ is an open interval containing r.

Ad (iii). Let $r \in \bigcup_{j\in J} O_j$ be given. Then there is some $j_0 \in J$ such that $r \in O_{j_0}$. It follows that there is an open interval $I \subseteq O_{j_0}$ containing r, and clearly also $I \subseteq \bigcup_{j\in J} O_j$. □

Definition 6.14 *The set of all open subsets of $\mathbb{R}$ is called the natural* topology on $\mathbb{R}$ *and denoted as $\tau_{\mathbb{R}}$.*

In fact, the open intervals in a precise sense generate $\tau_{\mathbb{R}}$: We say that a subset $\mathscr{B} \subseteq \tau_{\mathbb{R}}$ is a *base* if every open set O is the union of some of the elements in $\mathscr{B}$.

Lemma 6.15 *Open intervals form a base for the open sets on $\mathbb{R}$.*

Proof. If O is open and non-empty, then by definition there is for each $r \in O$ and open interval I_r containing r such that $I_r \subseteq O$. Then $O = \bigcup_{r\in O} I_r$.[17] □

Recall that rational numbers, $\mathbb{Q}$, are dense in $\mathbb{R}$. This leads to the following lemma. Let us say that (r_1, r_2) is an open interval with rational end-points if $r_1, r_2 \in \mathbb{Q}$.

Lemma 6.16 *Open intervals with rational end-points form a base for the open sets on $\mathbb{R}$. It follows that $\tau_{\mathbb{R}}$ has a countable base.*

[17] A little more complicated argument shows that every open subset of $\mathbb{R}$ is a disjoint union of open intervals.

PROOF. By Lemma 6.15, it suffices to show that every open interval is a union of open intervals with rational end-points. So assume (r_1, r_2) with $r_1 < r_2 \in \mathbb{R}$ is given. Then by the density of $\mathbb{Q}$ in $\mathbb{R}$, the union of all open intervals (q_1, q_2) with rational end-points such that $r_1 \leq q_1 < q_2 \leq r_2$ is equal to (r_1, r_2):

$$(r_1, r_2) = \bigcup \{(q_1, q_2) \mid q_1, q_2 \in \mathbb{Q}, r_1 \leq q_1 < q_2 \leq r_2\}.$$

Since the size of $\mathbb{Q} \times \mathbb{Q}$ is just countable, there are just countably many intervals with rational end-points, and this finishes the proof. □

Intuitively, the collection of open sets singles out those subsets of $\mathbb{R}$ which are important for mathematical analysis, the study of well-behaved functions. The basic notion here is the notion of *continuity* (see Section 6.5.3 below).

By generalising the properties of open intervals on $\mathbb{R}$, we can talk about open sets on any set X, not just on $\mathbb{R}$:

Definition 6.17 *We say that the pair (X, τ) is a* topological space *if $\tau \subseteq \mathscr{P}(X)$ and:*

(i) $\emptyset$ and X in τ.
(ii) If O and O' are in τ, then so is $O \cap O'$.
(iii) If $\{O_j \mid j \in J\}$ is a set of elements of τ for some non-empty J, then $\bigcup_{j \in J} O_j$ is in τ.

Note that the above notion of a base is still applicable to (X, τ). Similarly, once we have a topological space (X, τ) and a function $f : X \to X$ we may define when it is continuous by Definition 6.27 and (6.47).

Remark 6.18 The dual notion to open is *closed*. We say that $A \subseteq X$ is closed if $X \setminus A$ is open. Using this duality, all topological concepts can be equivalently formulated starting with the notion of a closed set (a closed interval in the sense of $\mathbb{R}$). The strength of topological notions is among other things in the interaction between open and closed sets.

The topological space $(\mathbb{R}, \tau_{\mathbb{R}})$ has some nice properties, such as a countable base, which are not shared by other topological spaces. Another important property which $(\mathbb{R}, \tau_{\mathbb{R}})$ satisfies is *separability*. We say that a topological space (X, τ) is *separable* if it contains countable dense subset (where D is dense if it has non-empty intersection with every open set; it follows that $\mathbb{Q}$ is dense in $\tau_{\mathbb{R}}$). We will not prove this, but let us just say that the notion of "topological density" is a generalisation of the notion of one ordering being dense in another ordering (such as $(\mathbb{Q}, <)$ is dense in $(\mathbb{R}, <)$). So the fact that $\mathbb{Q}$ is dense in $\mathbb{R}$ in $<$ implies that $\mathbb{Q}$ is a dense subset of $\mathbb{R}$ in the topological sense.

Another nice property of $(\mathbb{R}, \tau_{\mathbb{R}})$ is that it has no "gaps", which is topologically expressible as follows: a topological space is *connected* if it not a union of two disjoint non-empty open subsets (which are then also closed). A set which is both open and close is called *clopen*.

Lemma 6.19 *In $(\mathbb{R}, \tau_{\mathbb{R}})$ there exactly two clopen sets: $\emptyset$ and $\mathbb{R}$. It follows that $\mathbb{R}$ is connected.*

PROOF. Exercise. □

The mathematical brach called *general topology* studies the general properties of arbitrary topological spaces.

Nice as the topology $(\mathbb{R}, \tau_{\mathbb{R}})$ is, it does have some drawbacks for certain applications. For instance it is not invariant under dimension. By this we mean the following. We say that (X, τ_X) and (Y, τ_Y) are *homeomorphic*, if there is bijection $f : X \to Y$ such that for any $A \subseteq X$, $A \in \tau_X \leftrightarrow f[A] \in \tau_Y$, and so the two topologies are not distinguishable.[18] We may define a general topology $\tau_{\mathbb{R}\times\mathbb{R}}$ on $\mathbb{R} \times \mathbb{R}$ similarly as in the case of $\mathbb{R}$. Now the following holds:

Fact 6.20 *$(\mathbb{R}, \tau_{\mathbb{R}})$ and $(\mathbb{R} \times \mathbb{R}, \tau_{\mathbb{R}\times\mathbb{R}})$ are not homeomorphic.*

The reason for the is that $\mathbb{R}$ has *dimension* 1, whereas $\mathbb{R} \times \mathbb{R}$ has dimension 2, and every homeomorphism must respect dimension because it is a topological notion.[19] There are spaces which share many nice properties of $(\mathbb{R}, \tau_{\mathbb{R}})$ but in addition do not have the problem with dimension. We introduce one such example, the Cantor space 2^ω, in the next Section 6.5.2.

6.5.2 Cantor space

An important property of topological spaces is *compactness*. Let (X, τ) be a topological space. We say that $\mathscr{C} \subseteq \mathscr{P}(X)$ is an *open cover* if $\bigcup \mathscr{C} = X$ and all elements in $\mathscr{C}$ are open.

Definition 6.21 *We say that (X, τ) is* compact *if every open cover of X has a finite subcover, i.e. if $\mathscr{C}$ is an open cover of X, then there exists finite $\mathscr{C}^* \subseteq \mathscr{C}$ such that $\bigcup \mathscr{C}^* = X$.*

Notice that $(\mathbb{R}, \tau_{\mathbb{R}})$ is not compact: for instance no cover formed by open intervals of finite length has a finite subcover.

We will define a certain topology τ on 2^ω (the set of all infinite sequence of 0 and 1) which will be compact. We proceed by defining a base for τ (because a topology is determined by its base): we say that a set $O \subseteq 2^\omega$ is *a basic open set in τ* whenever there exists $n = \{0, \ldots, n-1\}$ and $\sigma : n \to 2$ such that

$$O = O_\sigma = \{f \in 2^\omega \mid \sigma \subseteq f\}, \tag{6.45}$$

i.e. O contains all sequences of $0, 1$ which on the first n arguments agree with σ. The topology is defined from these basic sets as follows:

$$\tau = \{X \subseteq 2^\omega \mid X \text{ is a union of a collection of basic open sets}\}.$$

It is easy to check that the collection of basic open sets is closed under intersection (if we add $\emptyset$ to it), and is therefore a base of the topology τ. The topology τ is called the *product topology* on 2^ω.[20]

[18] *Homeomorphism* is the topological equivalent of the notion of *isomorphism* for structures.

[19] It is not so easy to define dimension, so let us leave it this intuitive level.

[20] 2^ω can be viewed as a topological product of ω-many copies of 2 equipped with the *discrete topology*, i.e. topology where all subsets of 2 are open.

Definition 6.22 *The topological space $(2^\omega, \tau)$ is called the* Cantor space.

Fact 6.23 *The Cantor space is compact.*

Proof. We will not give a proof of the theorem. It follows from the product characterisation of 2^ω (see Footnote 20) using the Tichonoff theorem which says that a topological product of compact spaces is compact (and 2 with discrete topology is certainly compact). □

The space $(2^\omega, \tau)$ is similar to the space $(\mathbb{R}, \tau_\mathbb{R})$ – it has the same size as $\mathbb{R}$, the respective topologies have the same size, it has a countable base and it is separable – but also some important differences, one of them being:

Lemma 6.24 *Every basic open set in 2^ω is* clopen.

Proof. Let O be a basic open set determined by some $\sigma : n \to 2$. We need to show that it is also closed, or equivalently that $2^\omega - O$ is open. Clearly,

$$2^\omega - O = \bigcup \{O_{\sigma'} \mid \sigma' : n \to 2, \sigma \neq \sigma'\}.$$

Hence $2^\omega - O$ is a union of open sets, and is therefore open. It follows that O is closed. □

In the lecture *Boolean algebras* we will learn that the compactness of $(2^\omega, \tau)$ implies that there are only countably many clopen sets, and that they form a countable atomless Boolean algebra (which is unique up to isomorphism).

Remark 6.25 The Cantor space can also be described as follows. Consider the closed interval $[0, 1]$ on $\mathbb{R}$. Define a sequence $\langle C_i \mid i \in \omega \rangle$ of closed subsets of $[0, 1]$ as follows: $C_0 = [0, 1]$, $C_1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1]$, $C_2 = [0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{7}{9}] \cup [\frac{8}{9}, 1]$, etc. (in the next step divide each segment into three equal pieces and remove the open middle interval). Denote

$$\mathbb{K} = \bigcap_{n \in \omega} C_n.$$

It can be shown that $\mathbb{K}$ has size 2^ω and it is a compact subset of $[0, 1]$ in the topology $\tau_\mathbb{R}$ restricted to $\mathbb{K}$. It can also be shown that $\mathbb{K}$ (with the topology $\tau_\mathbb{R}$) is *homeomorphic* to the Cantor space $(2^\omega, \tau)$.

6.5.3 Continuity

For simplicity, we will assume that the functions f used below are defined on all of $\mathbb{R}$. Where appropriate, we will point out additional information relevant when f is not defined on all of $\mathbb{R}$.

Definition 6.26 (ϵ-δ-definition) *We say that a function $f : \mathbb{R} \to \mathbb{R}$ is* continuous *at r if for every $\epsilon > 0$ there exists $\delta > 0$ such that if $|x - r| < \delta$, then $|f(x) - f(r)| < \epsilon$.*

Note. If f is not defined everywhere, the definition of continuity reads as follows: let $f : E \to \mathbb{R}$, $E \subseteq \mathbb{R}$, and $p \in E$. Then f is continous at p if for every $\epsilon > 0$ exists $\delta > 0$ such that whenever $x \in E$ and $|x - p| < \delta$, then $|f(x) - f(p)| < \epsilon$. Note that f is required to be defined at p.

Definition 6.26 is the usual ϵ-δ definition. We can easily rephrase it using the notion of an open interval (see Theorem 6.28 for proof of the equivalence of these Definitions):

Definition 6.27 (topological definition) *We say that a function $f : \mathbb{R} \to \mathbb{R}$ is* continuous *at r if for every open set O containing $f(r)$ there exists an open set O' containing r such that*

$$f[O'] \subseteq O. \tag{6.46}$$

Exercise. Show that (6.46) is equivalent to $O' \subseteq f^{-1}[O]$. [Hint. This just a simple argument, not using the openness properties of O,O'. In fact if $f : X \to Y$ is function, where X, Y are non-empty sets, $A \subseteq X$ and $B \subseteq Y$, then $f[A] \subseteq B \leftrightarrow A \subseteq f^{-1}[B]$.]

We say that $f : \mathbb{R} \to \mathbb{R}$ is *continuous* if it is continuous on every element of its domain (for simplicity, we assume here that the domain of f is $\mathbb{R}$). An equivalent definition of continuity is the following (see Theorem 6.28 below):

(6.47) $f : \mathbb{R} \to \mathbb{R}$ is continuous if $f^{-1}[O]$ is open for every open set O.

and the following:

(6.48) $f : \mathbb{R} \to \mathbb{R}$ is continuous if $f^{-1}[C]$ is closed for every closed set C.

Theorem 6.28 *Let $f : \mathbb{R} \to \mathbb{R}$ be a function, then the following are equivalent:*
(i) f is continuous at every $r \in \mathbb{R}$ according to Definition 6.26,
(ii) f is continuous at every $r \in \mathbb{R}$ according to Definition 6.27,
(iii) (6.47) holds,
(iv) (6.48) holds.

Proof. (i)→(ii). Let an open set O containing $f(r)$ be given. Since O is open, there is some $\epsilon > 0$ such that $(f(r) - \epsilon, f(r) + \epsilon)$ is included in O. Applying (i), there is some $\delta > 0$ such that if x in $(r - \delta, r + \delta)$ then $f(x) \in (f(r) - \epsilon, f(r) + \epsilon)$. It suffices to set $O' = (r - \delta, r + \delta)$.

(ii)→(i). Similarly, Exercise.

(i)→(iii). Let O be an open set. Fix $x \in f^{-1}[O]$. We will find an open interval I containing x such that $I \subseteq f^{-1}[O]$, thus showing that $f^{-1}[O]$ is open because x is chosen arbitrarily. Since $x \in f^{-1}[O]$, there is some $x' \in O$ such that $f(x) = x'$. O is open, and so there is some $\epsilon > 0$ such that $(x' - \epsilon, x' + \epsilon)$ is included in O. It follows from (i) that there is some $\delta > 0$ such that for every $y \in (x - \delta, x + \delta)$, $f(x) \in (x' - \epsilon, x' + \epsilon) \subseteq O$. Thus $f[(x - \delta, x + \delta)] \subseteq O$ which is equivalent to $(x - \delta, x + \delta) \subseteq f^{-1}[O]$, which we needed to prove.

(iii)→(i). Similarly, Exercise.

(iii)→(iv). First notice that $f^{-1}[\mathbb{R}]$ is equal to the whole domain of f, that is $\mathbb{R}$. Let C be a closed set. Then $O = \mathbb{R} \setminus C$ is open, and by (iii), $f^{-1}[O]$ is open. Now, it is simple to check that for every function f,

$$f^{-1}[O] = f^{-1}[\mathbb{R} \setminus C] = f^{-1}[\mathbb{R}] \setminus f^{-1}[C] = \mathbb{R} \setminus f^{-1}[C]. \tag{6.49}$$

It follows that the complement of $f^{-1}[C]$ in $\mathbb{R}$ is open, and hence $f^{-1}[C]$ is closed.

(iv)→(iii). Similarly, Exercise. □

Note. We demand that $f^{-1}[O]$ is open for an open O, and not that

$$f[O] \text{ is open for an open } O. \tag{6.50}$$

Convince yourself that (6.50) is not an equivalent definition of continuity. The property (6.50) is also important, although not for continuity. We say that a function f is *open* if it satisfies (6.50).

The topological definition as in Definition 6.27 has the advantage that it is more general: the ϵ-δ definition uses the notion of *distance*, or *metric* ($|x - r| < \delta$ reads as "if the distance between x and r is less than δ"). In the case of our topology $\tau_{\mathbb{R}}$ we have defined the topology from the metric $|\cdot|$, but in general, the notion of an open set is more general than that of a metric.

Remark 6.29 The usefulness of taking the inverse image under $f^{-1}[X]$ of some sets $X \subseteq \mathbb{R}$, rather than using $f[X]$, is partly due to the fact that if $f : \mathbb{R} \to \mathbb{R}$ is a function which is not necessarily 1-1, then f^{-1} interacts better with the Boolean operations $\cap, \cup, \setminus$ than f does:

$$f^{-1}[X \cup Y] = f^{-1}[X] \cup f^{-1}[Y], f^{-1}[X \cap Y] = f^{-1}[X] \cap f^{-1}[Y], \\ f^{-1}[X \setminus Y] = f^{-1}[X] \setminus f^{-1}[Y]. \tag{6.51}$$

While we only have:

$$f[X \cup Y] = f[X] \cup f[Y], f[X \cap Y] \subseteq f[X] \cap f[Y], f[X \setminus Y] \supseteq f[X] \setminus f[Y]. \tag{6.52}$$

Notice that (6.51) holds for any function f, not necessarily from $\mathbb{R}$ to $\mathbb{R}$.

6.5.4 Characterization of continuity by limits of sequences

Our goal in this section is to show that for instance all polynomial functions are continuous. In the progress, we introduce one more useful characterization of continuity – by means of limits of sequences.

We first define a notion of a limit of a function at some point p:

Definition 6.30 *Let $f : \mathbb{R} \to \mathbb{R}$ be a function. We write*

$$\lim_{x \to p} f(x) = q$$

to denote the fact that f converges at p to q as x tends to p, more precisely: $\lim_{x \to p} f(x) = q$ *if and only if for every $\epsilon > 0$ there is some $\delta > 0$ such that for every x such that*

$$0 < |x - p| < \delta$$

it holds that

$$|f(x) - q| < \epsilon.$$

Note that we demand that $|x - p| > 0$ in the condition above because we wish to ignore the value $f(p)$. In fact f need not be defined at p at all.

Note. If f is not defined everywhere, then we must assume in Definition 6.30 that the point p is not isolated in the domain of f (i.e. f is defined at some point in every open set containing p).

Exercise. Assume that $f : \mathbb{R} \to \mathbb{R}$ is defined by $f(x) = 1$ for all $x \neq 0$ and $f(0) = 0$. Show that $\lim_{x\to 0} f(x) = 1$, even though $f(0) = 0$.

However, if f is continuous at p, then the limit tends to $f(p)$:

Theorem 6.31 *Let $f : \mathbb{R} \to \mathbb{R}$ be given. Then the following are equivalent for every real p:*

(i) f is continuous at p according to Definition 6.26,

(ii) $\lim_{x\to p} f(x) = f(p)$.

Proof. Obvious from the definitions. □

We now show that the limit of a function at p can be equivalently expressed as a limit a countable sequence of elements (this of course uses the fact that the topology of the real line is separable).

Theorem 6.32 *Let $f : \mathbb{R} \to \mathbb{R}$ be given, and let p be an arbitrary real number, then the following are equivalent:*

(i) $\lim_{x\to p} f(x) = q$,

(ii) For every sequence of real numbers $(p_n)_{n\in\omega}$ such that for every $n \in \omega$, $p_n \neq p$, and $\lim_{n\to\infty}(p_n) = p$, it holds that

$$\lim_{n\to\infty}(f(p_n)) = q.$$

Proof. (i)→(ii). Let (p_n) be a sequence satisfying the assumptions in (ii). We need to show that for every $\epsilon > 0$ there is some $n_0 \in \omega$ such that $\forall n \geq n_0$ it holds that $|f(p_n) - q| < \epsilon$. So let $\epsilon > 0$ be given. By (i), there is some $\delta > 0$ such that whenever $0 < |x - p| < \delta$, then $|f(x) - q| < \epsilon$. Since $\lim_{n\to\infty}(p_n) = p$, there is some $n_0 \in \omega$ such that $\forall n \geq n_0$, $0 < |p_n - p| < \delta$. It follows that for every $n \geq n_0$, $|f(p_n) - q| < \epsilon$.

(ii)→(i). We will show that the negation of (i) implies the negation of (ii). So assume $\lim_{x\to p} f(x) \neq q$. This means that there is some $\epsilon > 0$ such that for every $\delta > 0$ there is some x such that

$$0 < |x - p| < \delta \text{ and } |f(x) - q| \geq \epsilon.$$

Let us denote $\delta_n = \frac{1}{n}$. Choose for each δ_n some p_n such that $0 < |p_n - p| < \delta_n$ and $|f(p_n) - q| \geq \epsilon$. Then the sequence (p_n) satisfies that $p_n \neq p$ for every n, and $\lim_{n\to\infty} p_n = p$. However, it also holds that for every $n \in \omega$, $|f(p_n) - q| \geq \epsilon$, or equivalently $\lim_{n\to\infty} f(p_n) \neq q$. □

Remark 6.33 The proof of (ii)→(i) made an essential use of AC (Axiom of Choice). In fact, only a weak version, the so called countable axiom of choice (AC_ω), suffices for the proof of (ii)→(i). AC_ω says that for every countable family of sets, there exits a choice function. AC_ω is known to be consistent (modulo some extra set-theoretical

assumptions) for instance with the fact that all subsets of $\mathbb{R}$ are Lebesgue measurable, which is not possible with the full AC (in fact AC_{2^ω} is enough for the construction of a non-measurable subset of the reals).

Theorem 6.32 allows us to use some already known fact about the limits of sequence in the context of limits of functions. If f, g are functions and c is a real number, let us write cf to denote the function defined by $cf(x) = c(f(x))$, $f + g$ to denote the function defined by $f + g(x) = f(x) + g(x)$, and similarly $fg(x) = f(x)g(x)$, and $\frac{f}{g}(x) = \frac{f(x)}{g(x)}$, for $g(x) \neq 0$.

Theorem 6.34 *Let $f, g : \mathbb{R} \to \mathbb{R}$ be functions and let p be a real. Assume further that*

$$\lim_{x\to p} f(x) = A, \text{ and } \lim_{x\to p} g(x) = B.$$

Then the following hold:
(i) If c is a real number, then $\lim_{x\to p} cf(x) = cA$,
(ii) $\lim_{x\to p} f + g(x) = A + B$,
(iii) $\lim_{x\to p} fg(x) = AB$,
(iv) $\lim_{x\to p} \frac{f}{g}(x) = \frac{A}{B}$, if $B \neq 0$, and $g(x) \neq 0$ for every x.

Proof. By invoking Theorem 6.32, it suffices to show the analogous statements for limits of sequences: Let (p_n) converge to p, and $p_n \neq p$ for every $n \in \omega$, then
(i) $\lim_{n\to\infty}(cf(p_n)) = c \lim_{n\to\infty}(f(p_n))$,
(ii) (similarly for other items (ii)–(iv))
(i) and (ii) are easy, and were in fact shown above. (iii) and (iv) are a bit more difficult, *Exercise. □

Theorem 6.35 *Let f and g be continuous functions from $\mathbb{R}$ to $\mathbb{R}$, then cf (for c a real), $f + g$, fg and $\frac{f}{g}$ (provided that $g(x) \neq 0$ for every x) are continuous on $\mathbb{R}$.*

Proof. By Theorem 6.34. □

Corollary 6.36 *All polynomial functions are continuous.*

Proof. Recall that $p(x)$ is a polynomial function (with real coefficients) if is of the form $c_n x^n + c_{n-1}x^{n-1} \ldots + c_0$, where c_i are real numbers for $i \in \{0, \ldots, n\}$.

The proof follows from Theorem 6.35.

In some detail, the fact that $p(x)$ is continuous at every point of its domain is shown by the induction on the complexity of $p(x)$. If $p(x)$ is just the constant function c_0, then it is clearly continuous. If $p(x) = x$, then it is again continuous. In general, every function of the form x^n is continous (by induction) because $x^n = x^{n-1}x$. Also, cx^n is continous. It follows that the whole polynom is continuous because if f are continuous so is $f + g$. □

The continuous functions are also closed under compositions of functions:

Theorem 6.37 *Let f be a function from $E \to \mathbb{R}$ continuous at every element of $E \subseteq \mathbb{R}$ and assume that g is defined at every element of* $\mathrm{rng}(f)$ *and is continuous here. Then $g \circ f : E \to \mathbb{R}$ is continuous at every element of E, where $g \circ f(x) = g(f(x))$ for every $x \in E$.*

Proof. Let $p \in E$ be given. Fix $\epsilon > 0$. By assumption, g is continous at $f(p)$; this means that there is some $\delta > 0$ such that for all $x \in \mathrm{rng}(f)$, if $|x - f(p)| < \delta$, then $|g(x) - g(f(p))| < \epsilon$. Since f is continuous at p, there is some δ_1 such that for all $x \in E$, if $|x - p| < \delta_1$, then $|f(x) - f(p)| < \delta$. This means that for every $x \in E$ such that $|x - p| < \delta_1$ it holds that $|g(f(x)) - g(f(p))| < \epsilon$, which shows that $g \circ f$ is continous at p. □

6.5.5 Some examples

Exercises

(1) Show that if f and g are continous functions from $\mathbb{R}$ to $\mathbb{R}$ which agree on $\mathbb{Q}$, i.e. $f(x) = g(x)$ for every $x \in \mathbb{Q}$, then already $f = g$. This means that there are only 2^ω continous functions from $\mathbb{R}$ to $\mathbb{R}$ (although there are $2^{(2^\omega)}$ functions from $\mathbb{R}$ to $\mathbb{R}$).

(2) The Dirichlet function $d(x) : \mathbb{R} \to \mathbb{R}$ is defined as follows:

$$d(x) = \begin{cases} 1 & \text{for } x \in \mathbb{Q}, \\ 0 & \text{for } x \in \mathbb{R} \setminus \mathbb{Q}. \end{cases}$$

Show that $d(x)$ is discontinuous (i.e. not continuous) at every $x \in \mathbb{R}$.

(3) *The Riemann function $r(x) : \mathbb{R} \to \mathbb{R}$ is defined as follows:

$$r(x) = \begin{cases} \frac{1}{n} & \text{for } x \in \mathbb{Q}, \\ & \text{where } x = \frac{m}{n} \text{ with } m, n \text{ having no common divisor,} \\ & \text{and } n > 0, m \in \mathbb{Z}, \\ 0 & \text{for } x \in \mathbb{R} \setminus \mathbb{Q}. \end{cases}$$

In addition define $r(0) = 1$.

Show that $r(x)$ is continous at every irrational number (i.e. a number in $\mathbb{R} \setminus \mathbb{Q}$), and is discontinuous at every rational number.

7 Further reading

Introduction to mathematics:

- J.K.Truss, *Foundation of Mathematical Analysis.* Clarendon Press, Oxford. 1997.
- Jiří Matoušek a Jaroslav Nešetřil, *Kapitoly z diskrétní matematiky.* Karolinum, Praha. 2002.
- Milan Mareš, *Příběhy matematiky.* Pistorius a Olšanská, Přibram 2008.

Walter Rudin, *Principles of Mathematical Analysis.* McGraw-Hill, 3rd edition.

Philosophical aspects:

- Vojtěch Kolman, *Filosofie čísla.* Filosofia, 2008.

Mathematical Logic and Set theory:

- Antonín Sochor, *Klasická matematická logika*, Karolinum 2001.
- Vítězslav Švejdar, *Logika: neúplnost, složitost a nutnost*, Academia 2002.
- Bohuslav Balcar a Petr Štěpánek, *Teorie množin*, Academia 2000.

References

[1] Vítězslav Švejdar. *Neúplnost, složitost, nutnost.* Academia, 2002.

[2] J. K Truss. *Foundations of mathematical analysis.* Oxford University Press, 1997.