Delft University of Technology
Faculty Electrical Engineering, Mathematics and Computer Science
Delft Institute of Applied Mathematics

Zermelo–Fraenkel Set Theory and the Construction of the Real Numbers

Report for the benefit of the
Delft Institute of Applied Mathematics
as part of obtaining

the degree of

BACHELOR OF SCIENCE
in
APPLIED MATHEMATICS

by

F.M.H. van der Els

Delft, The Netherlands
August 13, 2024

BSc thesis APPLIED MATHEMATICS

"Zermelo–Fraenkel Set Theory and the Construction of the Real Numbers"

F.M.H. van der Els

Supervisor:

Dr. K.P. Hart

Committee members:

Dr. K.P. Hart

Dr. C. Kraaikamp

Mathematics is the language with which God has written the universe.

– Galileo Galilei

Preface

I would like to open by saying how thankful I am for having the opportunity to be able to express my interest in foundational mathematics by formal means of writing a thesis. This is perhaps the best excuse for spending as much time as I have exploring this field of mathematics. Writing this thesis has been an extremely fun journey. I would like to thank Dr. K.P. Hart in particular for allowing me to diverge from the available list of projects for this thesis and venture into my own. His assistance has been very helpful throughout the development of this thesis. My ideas for the project started off way too broad, which was a direct consequence of my enthusiasm to delve into as much as possible in the field. As the project progressed the scope became more narrow. It is now what I believe to be a great midway between coverage and detail. With that, I wish you much pleasure in reading this thesis.

Layman summary

In this thesis we will construct the real numbers. For doing so we will define the necessary mathematical objects using a foundation of mathematics called Zermelo-Fraenkel set theory. We will use these sets to construct first the natural numbers, integers and rational numbers. We will show how these constructed number systems align with our intuition mathematically by proving the properties they are expected to enjoy, as well as by showing how these number systems are mathematically deemed unique. Finally we will construct the real numbers in three ways. The first two constructions are the most common, whereas the third is nonstandard. We will show each construction in essence achieves the same real numbers. The real numbers are lastly characterised in terms of the properties that naturally arose from the first two constructions.

Summary

In this thesis models of the real numbers will be constructed using a set-theoretic approach. The mathematical foundation we will assume is the first-order theory with equality known as Zermelo-Fraenkel set theory (**ZF**). From the axioms of **ZF**, the necessary notions for the construction will be introduced as definitional extensions to the language of **ZF**. We will show how functions can be defined as relations, which in turn are defined as subsets of Cartesian products. Using this preliminary work we will first construct the natural numbers. We will see how our intuition of using the natural numbers for counting gives rise to the Dedekind-Peano axioms (**PA**). Defining the natural numbers $\mathbb{N}$ as the smallest set satisfying the requirement in the statement of the Axiom of Infinity, we find that they are indeed a model of **PA**. By using our knowledge of what properties operations relating to the natural numbers should satisfy, we induce algebraic structures, the most basal of which being the ordered semiring. We will see how the successor function and induction are intimately tied to the predecessor function and well-ordering. This structure will be used to prove the uniqueness of $\mathbb{N}$; it is the unique well-ordered commutative semiring in which every nonzero element has a predecessor. Next the integers $\mathbb{Z}$ are defined as equivalence classes of pairs of the natural numbers. We observe how the integers have additive inverses, which allows for a simple characterisation of them as the unique ordered commutative ring whose positive elements are well-ordered. Using the integers, we will define the rational numbers $\mathbb{Q}$ as fractions represented by equivalence classes of pairs of integers. An important result will be that the rational numbers are the smallest ordered field, in that every ordered field has a subfield isomorphic to $\mathbb{Q}$. After this, we will turn to constructing the real numbers. Three models will be constructed: the Dedekind reals $\mathbb{R}_D$, the Cantor reals $\mathbb{R}_C$ and the Schanuel reals $\mathbb{R}_S$. The first two constructions both induce a fundamental property of the real numbers: completeness. The third construction is a lesser known construction. We will compare the three constructions and prove they are indeed equivalent. That is, we will prove that any ordered field is Dedekind-complete if and only if it is Archimedean and Cauchy-complete. This property of the real numbers will be used to prove that they are the unique ordered Dedekind-complete field. Lastly some directions for further research will be discussed.

Introduction

In *Analysis with an Introduction to Proof* the following is said [19]:

> We begin by assuming the existence of a set $\mathbb{R}$, called the set of real numbers, and two operations $+$ and $\cdot$, called addition and multiplication, such that the following apply: [...]

after which a list of requirements (axioms) in terms of $+$, $\cdot$ and elements of the set $\mathbb{R}$ is given. Further on a relation "$<$" is introduced, and axioms are imposed on it. This construction is called an axiomatic (or synthetic) construction of the real numbers, because it defines the real numbers as a set in which certain axioms apply. Using these axioms, one can then prove more statements about the real numbers, use those to prove even more, and so on.

Crucially, one may wonder why the following was not said instead: "The set of real numbers $\mathbb{R}$ is the set that satisfies the following axioms: [...].". Well, what if no such set exists in the first place? Then the definition of $\mathbb{R}$ would not even make sense. Secondly, what if many such sets exist? Then it would not be clear which one of those would be the set $\mathbb{R}$, given that the definite article "the" imposes the existence of only a single one.

Both these objections are at the heart of this thesis. To resolve them, we will explicitly construct a suitable set for the real numbers. Then, instead of assuming, we will be proving that the constructed set satisfies the axioms, whereby we resolve the existence objection. Next, we will show that the resulting set is, in a way, unique. That is, any set satisfying the axioms is in essence the same set. This resolves the uniqueness objection.

It might seem strange to ponder the existence and uniqueness of the real numbers at all. After all, the calculations one performs in their daily lives all involve the real numbers. Measurements of quantities like weight, length and velocity all have their values in the real numbers. It would seem almost nonsensical to question their existence or uniqueness. What would it even mean if the real numbers were not unique? Yet an important branch of mathematics concerns these and similar questions; foundational mathematics. This thesis aspires to be an accessible introduction to this field. As the name suggests, this type of mathematics is about the objects at the foundation of various other branches of mathematics. The dependency of other fields of mathematics on foundational mathematics is what makes it inherently vital to all of mathematics. It is for this reason that the real numbers are well worth to study thoroughly. We want

to formally assure that the real numbers we think exist also exist mathematically, and have the properties we are used to.

To construct the real numbers, one must start somewhere. This starting point will be Zermelo-Fraenkel set theory. This will be Chapter 1. Zermelo-Fraenkel set theory centres around one object; the set. Every mathematical object can then be described in terms of sets. To match our intuitive idea of a set as a collection of things to the mathematical object, we impose a list of axioms on them. This will not only help with our intuition, but it will also formally guide us on how one can and cannot operate with sets. Notably, Zermelo-Fraenkel set theory is a framework built on top of a foundation laid by mathematical logic. As such, we will assume knowledge of some definitions and results from mathematical logic. These will be mostly self-explanatory, but for reference one may consult Appendix A.

To construct the real numbers we will in Chapter 2 first construct simpler number systems. These are the natural numbers, integers and rational numbers. These are not only convenient for the construction of the real numbers, but also of great individual significance. As for the real numbers, specifically the natural numbers, integers and rational numbers appear on a daily basis in ones life. These number systems therefore also warrant a mathematical formalisation.

In Chapter 3 we will construct the real numbers. Actually, we will do it three ways. There is in fact no single way to construct the real numbers, or any number system for that matter. While the natural numbers, integers and rational numbers have a mostly standard construction, the real numbers show much diversity. This is also what makes the construction of the real numbers particularly interesting. The third construction will be a nonstandard construction of the real numbers. After the three constructions, we will prove their equivalence.

The characterisations of number systems throughout this thesis will be stated in terms of three notions. Addition, multiplication and order. These are the central operations with which the results will be formulated. The most basic sets in which these operations behave nicely with each other yield an important algebraic structure; the ordered semiring. The ordered semiring is the most fundamental structure that unifies all three operations. The sets we will construct can then be characterised in terms of ordered semiring structures with additional properties. Further structure, like exponentiation, can be added but are not strictly necessary. The precise definitions of the algebraic structures we will use will be stated as we need them.

This thesis will be written from a perspective that is familiar with how the numbers and operations behave. That is, we intuitively know what numbers are, and subject to what rules we can perform operations on them. Using these intuitions, we will both define and characterise these operations mathematically. This perspective will help to remove the potential arbitrariness that may arise when presented with the constructions without further comment on the "why" aspect. Moreover, we will sometimes write things in quotes. All mathematics in quotes is to be read solely for instructional purposes. It appeals to the intuition of the reader, but is not always mathematically sound.

We will distinguish the following types of results:

Proposition. A minor result of independent interest.

Lemma. A minor result for use in the proof of a more major result.

Theorem. A major result.

Most results in this thesis will be propositions. This is due to the nature of foundational mathematics. Each step of the construction establishes results that are useful throughout all of mathematics and are therefore assigned propositions.

Final note from the author: I intend to continue developing this work in the future. I will make the project files open source for the mathematical community to view and contribute to. As of its initial publication, the source code can be found in the repository xpple/ConstructionOfMathematics on GitHub.

Contents

Chapter 1

Zermelo–Fraenkel set theory

Introduction

In the beginning of the 20th century, there was a lot of research devoted towards the development of a contradiction-free set theory, and even contradiction-free mathematics in general. This was in part due to the discovery of a mathematical paradox by Russell. We will state the precise paradox later; he himself also considered a hairy variant of it [27]:

> You can define the barber as "one who shaves all those, and those only, who do not shave themselves". The question is, does the barber shave himself?

If the barber shaves himself, then the barber must not shave himself. If the barber does not shave himself, then the barber must shave himself. Hence the barber shaves himself if and only if he does not shave himself, a contradiction. The paradox is an example of self-referential statement. There are resolutions to this variant of the paradox, but at the time there were no resolutions to the formal statement of his paradox. Any contradictory statement is disastrous for mathematics as a whole. This is no overexaggeration; due to the principle of explosion, once a contradiction exists, any statement at all can be proven both true and false.

After a lot of unsatisfactory attempts, finally through the combined work of mostly Zermelo, Fraenkel and Skolem a formalisation of mathematics in terms of axioms was established that satisfied all the requirements the set theorists of that time had. It is for example, free of Russell's paradox. This set theory is now known as Zermelo-Fraenkel set theory, and is abbreviated to **ZF**. To this day, this set of axioms forms the most common foundation of mathematics.

First in Section 1.1 we will introduce some preliminary definitions that will help to state the axioms in Section 1.2. With these axioms we will first define relations in Section 1.3 and lastly functions in Section 1.4. For a comprehensive overview of basic set theory see [20] and also [16].

1.1 Preliminaries

To abbreviate and increase the readability of the axiom statements, it is useful to define a few shorthands. To do this we will use concepts from mathematical logic. If not explained, these notions will be understandable from the context. Additionally one may consult Appendix A for a brief overview of **ZF** as a first-order theory with equality. See also this appendix for justifying adding new symbols to the theory of **ZF**, without actually changing it.

Definition 1.1.1 (Unique existential quantifier)**.** Let φ be a formula with free variables among which x. We write $\exists! x(\varphi(x))$ to mean

$$\exists x(\varphi(x) \wedge \forall y(\varphi(y) \implies x = y)).$$

Definition 1.1.2 (Shorthand for quantifiers)**.** Let φ be a formula with free variables among which x. We write $\forall x \in X(\varphi(x))$ and $\exists x \in X(\varphi(x))$ to mean

$$\forall x(x \in X \implies \varphi(x)) \quad \text{and} \quad \exists x(x \in X \wedge \varphi(x))$$

respectively. Variants of this notation will be used later and are to be interpreted similarly.

Definition 1.1.3 (Set nonmembership.)**.** Define the binary relation symbol $\notin$ by $x \notin X$ when $\neg(x \in X)$.

Definition 1.1.4 ((Improper) subset)**.** Define the binary relation symbol $\subseteq$ by $X \subseteq Y$ when $\forall x \in X(x \in Y)$.

Definition 1.1.5 (Unequality[1].)**.** Define the binary relation symbol $\neq$ by $x \neq y$ when $\neg(x = y)$.

One could also define proper subsets, (im)proper supersets and negations thereof, but we will not need those.

1.2 Axioms of ZF

As mentioned in the introduction, **ZF** consists of a set of axioms; colloquially these are starting points that are assumed to be true. These axioms were given names to reflect their purpose. Below is an overview of these axioms written purely in the language of **ZF** along with the notational extensions from the previous section. We will use that any interpretation (model) of the theory **ZF** is required to be nonempty. This stems from the semantics of **ZF** being a first-order theory [10]. In other words, we may use that a set exists without needing any axiom[2].

Note that some of the axioms depend on each other. That is, some cannot be stated without assuming others. This imposes a certain partial order in which they are stated. This order is unimportant however. This is because we are interested in the statements that **ZF** can prove after all the axioms are stated, after which the order no longer matters.

[1] "Unequality" is used as opposed to "inequality" because the latter is usually reserved for relations of the type "$\leq$".

[2] In *Set Theory: An Introduction to Independence Proofs* Kunen acknowledges this too, but includes a zeroth axiom that stipulates the existence of a set for emphasis [16].

Axiom of Extensionality

We want sets to be equal when they consist of the same elements. This axiom assures that two sets having the same elements make them actually equal as prescribed by the primitive logical symbol "=".

$$\forall x \forall y (x \subseteq y \wedge y \subseteq x \implies x = y).$$

The converse of this statement follows immediately by the substitution axiom of equality. For reference, the axioms of equality are stated in Appendix A.

Axiom Schema of Specification

This axioms allows for (restricted) set-builder notation. It also known as the Axiom Schema of Separation and the Axiom Schema of Comprehension. These names all reflect that one may construct a set by specifying a domain set and a statement every member of the domain must satisfy. Let φ be a formula with free variables among which x and D and nonfree variable A. Then

$$\forall D \exists A \forall x (x \in A \iff (x \in D \wedge \varphi(x, D))).$$

The set A is unique by the Axiom of Extensionality. Because of this, we can define a function symbol to denote this set.

Definition 1.2.1 (Set-builder notation)**.** We add the unary function symbol

$$\{x \in D \mid \varphi(x, D)\} := A.$$

This function symbol is called set-builder notation, because it allows one to build a set of elements that satisfy a given constraint.

An example set that is not allowed to be created is $R = \{a \mid a \notin a\}$. One quickly realises why this set is disallowed. Suppose $R \in R$, well then $R \notin R$. So $R \notin R$? Well, then $R \in R$. In other words, $R \in R \iff R \notin R$, a contradiction. This is Russell's paradox. As was alluded to in the introduction, this paradox was a serious concern for mathematicians in the beginning of the 20th century. Luckily it is prevented in **ZF** because restricted specification requires a domain to be specified, the set D. This was not done for R, and so the construction of R was invalid.

Moreover, because a set is known to exist, using this axiom we can construct a set that contains no elements. This set is then unique by the Axiom of Extensionality. We will introduce a new function symbol to denote this set.

Definition 1.2.2 (Empty set)**.** Let x be any set. Define the nullary function symbol $\varnothing := \{y \in x \mid y \neq y\}$.

The empty set is convenient to have, and it allows some of the remaining axioms to be formulated more concisely. In fact, we will put it to use in the next axiom.

Axiom of Regularity

The axiom of regularity aims to regularise the theory by disallowing certain sets. It is also known as the Axiom of Foundation. In words, every nonempty set should contain an element that has no elements in common with the set.

$$\forall x \neq \varnothing \exists y \in x(\neg \exists z(z \in x \wedge z \in y)).$$

Alone this axiom does not achieve much regularisation, but in combination with other axioms it will for example prohibit self-referential sets.

Axiom of Pairing

For every two sets, there is a set that contains both of them.

$$\forall x \forall y \exists z(x \in z \wedge y \in z).$$

By the Axiom Schema of Specification there exists a unique set only containing the elements x and y. We capture this in a definition.

Definition 1.2.3 (Two element roster notation)**.** We introduce a new binary function symbol denoted by $\{x, y\}$ to mean the set only containing x and y. This notation is called roster (or enumeration) notation. When $x = y$, the set $\{x, y\}$ has one element by the Axiom of Extensionality, in which case we denote it by the unary function symbol $\{x\}$.

Using this axiom and the Axiom of Regularity we can prove no set can be an element of itself. Let x be a set. Then $\{x\}$ is a set. Invoking the Axiom of Regularity on $\{x\}$ we find that there is a $y \in \{x\}$ such that there does not exist a z for which $z \in \{x\}$ and $z \in y$. We must have $y = x$, so there does not exist a z such that $z = x$ and $z \in x$. Hence $x \notin x$. In a similar way it follows by invoking the Axiom of Regularity on $\{x, y\}$ for arbitrary sets x and y that only one of x and y can be an element of the other. From now on we will use these facts without comment.

An immediate consequence of the first fact is that the set of all sets does not exist. Formally put: $\neg(\exists x \forall y(y \in x))$. If we assume the contrary, that is assume such a set x exists, then $x \in x$, a contradiction. Hence there exists no such set. Looking at Russell's paradox, we see that R would have to be the set of all sets, also disproving its existence.

Axiom of Union

We would also like to combine sets. That is, given a set, there should exist a set that comprises the elements of the elements of that set.

$$\forall \mathcal{F} \exists A \forall Y \forall x((Y \in \mathcal{F} \wedge x \in Y) \implies x \in A).$$

For any $\mathcal{F}$, take an A which exists by this axiom. Then A contains the elements of the subsets of $\mathcal{F}$, but may also contain other elements. To capture the set only containing the subsets of $\mathcal{F}$ we introduce a new function symbol.

Definition 1.2.4 (Arbitrary set union)**.** We introduce the new unary function symbol $\bigcup \mathcal{F}$ by

$$\bigcup \mathcal{F} := \{x \in A \mid \exists Y \in \mathcal{F}(x \in Y)\}$$

called the union of $\mathcal{F}$.

One can imagine it would also be useful to talk about the union of two sets: the set containing the elements of both sets. This can defined in terms of an arbitrary set union.

Definition 1.2.5 (Set union)**.** For two sets X and Y we introduce the binary function symbol $X \cup Y := \bigcup\{X, Y\}$. This set is called the union of X and Y.

Using set unions, we can extend Definition 1.2.3 to arbitrarily many elements.

Definition 1.2.6 (Roster notation)**.** For $n > 2$ we introduce the n-ary function symbol $\{x_1, \ldots, x_n\} := \{x_1\} \cup \cdots \cup \{x_n\}$.

Note that we can omit brackets because $\cup$ is associative, which boils down to the fact $\vee$ is associative. Similar to set unions, we wish to consider the set of common elements of subsets.

Definition 1.2.7 (Arbitrary set intersection)**.** We introduce the unary function symbol $\bigcap \mathcal{F}$ by

$$\bigcap \mathcal{F} := \{x \in \bigcup \mathcal{F} \mid \forall Y \in \mathcal{F}(x \in Y)\}$$

called the intersection of $\mathcal{F}$.

Similar to the union, it is useful to talk about the intersection of two sets. This can be defined in terms of an arbitrary set intersection.

Definition 1.2.8 (Set intersection)**.** We define the binary function symbol $X \cap Y := \bigcap\{X, Y\}$. This set is called the intersection of X and Y.

Lastly we will define the difference between two sets.

Definition 1.2.9 (Set difference)**.** We define the binary function symbol denoted $X \setminus Y$ by

$$X \setminus Y := \{x \in X \mid x \notin Y\}.$$

Similar to the definition of the difference of two sets, one could have chosen to define the intersection of two sets as $X \cap Y = \{x \in X \mid x \in Y\}$.

Axiom of Infinity

We saw that the existence of a set was a consequence of **ZF** being first-order theory. This axiom additionally assures a set exist, and even an "infinite" one. Define the unary function symbol $S(x) = x \cup \{x\}$.

$$\exists X(\varnothing \in X \wedge \forall x \in X(S(x) \in X)).$$

In Section 2.1 we will re-encounter the function symbol S, where it will play an important role in defining the natural numbers.

Axiom Schema of Replacement

The axiom schema of replacement asserts that the "range" of a "function" is again a set. Even though we have not defined what those words mean, we can write it down formally in terms of formulas. Let φ be a formula with free variables among which x, y, A and nonfree variable B.

$$\forall A(\forall x \in A \exists! y(\varphi(x, y, A)) \implies \exists B \forall y(y \in B \iff \exists x \in A(\varphi(x, y, A)))).$$

That is, if for all $x \in A$ there exists a unique y satisfying $\varphi(x, y, A)$, then there exists a set B such that $y \in B$ precisely when there is an $x \in A$ for which $\varphi(x, y, A)$ is satisfied. When $\varphi(x, y, A)$ holds, we write this as $F_\varphi(x) = y$, where F_φ is the "function" described by φ. This is closely related to a different notion of functions we will define in Section 1.4, where the functions are actual sets and not just notation. To denote the set B, which is unique by the Axiom of Extensionality, we will introduce the following function symbol.

Definition 1.2.10 (Image under a "function")**.** Introduce the unary function symbol $F_\varphi(A)$ by

$$F_\varphi(A) := B.$$

Axiom of Power Set

In words, the power set of a set is the set of all subsets of that set. This axiom asserts this set exists.

$$\forall X \exists A \forall z(z \subseteq X \implies z \in A).$$

Similar to the Axiom of Union asserting the existence of a set without further restriction, this axiom does too. That means that the set A achieved by applying this axiom to any set X may contain more elements than just the subsets of the set. To capture the set only containing the subsets, we introduce a new function symbol.

Definition 1.2.11 (Power set)**.** We introduce the unary function symbol $\mathcal{P}(X)$ by

$$\mathcal{P}(X) := \{x \in A \mid x \subseteq X\}$$

called the power set of X.

These axioms conclude the eight axioms of **ZF**. Perhaps unexpectedly however, not all axioms are strictly necessary. One may remove the Axiom Schema of Specification and the Axiom of Pairing without weakening the theory. That is, **ZF** with these axioms included cannot prove any more statements than **ZF** without these axioms. This is because both axioms follow from the Axiom Schema of Replacement along with the existence of the empty set and any set with two (or more) elements. It is for historical and instructional reasons that they are included in most formulations of the theory.

However, it will turn out that we will not need the Axiom Schema of Replacement for the purposes of this thesis. Hence in the case this axiom is not assumed, both the Axiom of Pairing and the Axiom Schema of Specification become necessary. The Axiom Schema of Replacement becomes relevant for more advanced set theory. The same is true for an axiom that is often assumed

along with the axioms of **ZF**: the Axiom of Choice[3]. Roughly put, the axiom states that one can manifest a set that, given a possibly infinite collection of sets, contains one element of each set of this collection. This axiom is independent of **ZF**, which means that it cannot be proven or disproven from **ZF**. We will also not need this axiom.

1.3 Relations

Using these axioms, we can start to define new mathematical objects. To start, we define the ordered pair. We will first define it, and afterwards justify its definition.

Definition 1.3.1 (Ordered pair)**.** Define the ordered pair as the binary function symbol (x, y) denoting the set $\{\{x\}, \{x, y\}\}$.

We can use the ordered pair to define ordered triples, quadruples, etc. For the ordered triple, one can choose between $(x, (y, z))$ or $((x, y), z)$. It does not matter for the purposes of the ordered triple, so we will arbitrarily choose the latter. This can then be generalised into a definition for ordered n-tuples.

Definition 1.3.2 (Ordered n-tuples)**.** For $n > 2$ we define the n-ary function symbol $(x_1, \ldots, x_n)$ by $((x_1, \ldots, x_{n-1}), x_n)$ called the ordered n-tuple.

Ordered tuples, and specifically ordered pairs, are ordered in the sense that generally $(x, y) \neq (y, x)$. In particular, this definition of ordered tuples satisfies the defining property for an ordered tuple.

Proposition 1.3.3 (Ordered tuples are ordered)**.** *Two ordered tuples are equal if and only if their components are equal. That is,*

$$(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$$

if and only if $x_i = y_i$ *for all* $1 \leq i \leq n$*.*

Proof. The if direction follows from the substitution axiom of equality. We will prove the only if direction by induction on n. Consider the base case $n = 2$. Suppose $\{\{x_1\}, \{x_1, x_2\}\} = \{\{y_1\}, \{y_1, y_2\}\}$. Since equal sets have the same members, we have that $\{x_1\} \in \{\{y_1\}, \{y_1, y_2\}\}$ and $\{x_1, x_2\} \in \{\{y_1\}, \{y_1, y_2\}\}$. From the first it follows that $x_1 = y_1$. From the second it follows using $x_1 = y_1$ that $x_1 = x_2 = y_1$ or $x_2 = y_2$. By symmetry, we also have $y_1 = y_2 = x_1$ or $x_2 = y_2$. These statements combined yield $x_2 = y_2$. For the induction step, suppose the statement holds for some $n = k$. Then,

$$\begin{aligned}(x_1, \ldots, x_{k+1}) &= (y_1, \ldots, y_{k+1}) \\ ((x_1, \ldots, x_k), x_{k+1}) &= ((y_1, \ldots, y_k), y_{k+1})\end{aligned}$$

so by the base case $x_{k+1} = y_{k+1}$ and $(x_1, \ldots, x_k) = (y_1, \ldots, y_k)$ after which it follows that $x_i = y_i$ for all $1 \leq i \leq k + 1$ by the induction hypothesis. □

[3]Zermelo included the Axiom of Choice from the beginning, others later removed it to distinguish the two theories [32].

We have now shown that the definition of ordered pairs as given in Definition 1.3.1 yields a pair that is actually ordered. Notably, there are many more definitions possible that would satisfy this property. A reason for accepting this definition is that it "just works" and is quite simple[4].

Given an ordered pair $z = (x, y)$, one can extract x and y as follows.

$$\begin{aligned}\pi_1(z) &:= \bigcup\bigcap z = \bigcup\bigcap\{\{x\},\{x,y\}\} = \bigcup\{x\} = x,\\ \pi_2(z) &:= \bigcup\left\{a \in \bigcup z \;\middle|\; \bigcup z \neq \bigcap z \implies a \notin \bigcap z\right\}\\ &= \bigcup\{a \in \{x,y\} \mid \{x,y\} \neq \{x\} \implies a \notin \{x\}\} = \bigcup\{y\} = y.\end{aligned}$$

Because we can extract the components of a pair, we may let (x, y) be an arbitrary pair, instead of letting z be a pair and defining $x = \pi_1(z)$ and $y = \pi_2(z)$. Henceforth, we will not bother using π_1 or π_2.

Next, we would like to define a certain notion of a product of two sets. One such notion is the Cartesian product. The Cartesian product of sets X and Y is the set of all pairs (x, y) where x is a member of X and y is a member of Y. To define this Cartesian product, we must figure out what set the set (x, y) is a member of to use the Axiom Schema of Specification. Since $\{x\} \in \mathcal{P}(X)$ and $\{x, y\} \in \mathcal{P}(X \cup Y)$, we have that $(x, y) \in \mathcal{P}(\mathcal{P}(X \cup Y))$.

Definition 1.3.4 (Cartesian product)**.** We introduce the binary function symbol $X \times Y$ by

$$X \times Y := \{z \in \mathcal{P}(\mathcal{P}(X \cup Y)) \mid \exists x \in X \exists y \in Y(z = (x, y))\}$$

called the Cartesian product.

We can use this to define a relation; a way of relating two sets. The following definition defines a relation in its most general form.

Definition 1.3.5 (Relation)**.** Let R be any subset of $X \times Y$. Define a relation over X and Y as the ordered triple (X, Y, R).

Two elements x and y are related if $(x, y) \in R$. Note that usually one also refers to just the set R as a relation. In this case the sets X and Y should be clear from the context.

The elements of the set X are to be related with the elements of the set Y. For this reason, it is useful to define some notions involving X and Y for a relation R.

Definition 1.3.6 (Domain, corange, codomain and range)**.** We introduce the unary function symbols dom, corange, codom and range by

$$\begin{aligned}\mathrm{dom}(R) &:= X,\\ \mathrm{corange}(R) &:= \{x \in X \mid \exists y \in Y((x, y) \in R)\},\\ \mathrm{codom}(R) &:= Y,\\ \mathrm{range}(R) &:= \{y \in Y \mid \exists x \in X((x, y) \in R)\}.\end{aligned}$$

[4]One may seek a more technical justification. In the words of Kuratowski, after whom this definition is due, a simple way to create a structure that encodes ordering is by considering the set of all elements that precede an element. To encode that a comes before b, these would be $\varnothing$, $\{a\}$ and $\{a, b\}$. Since $\varnothing$ would always be present, one can dismiss it. Thus one obtains the list $\{\{a\}, \{a, b\}\}$ [17].

For brevity, we introduce the ternary relation symbol $x\ R\ y$ to mean $(x, y) \in R$. A relation on a set X is a relation where $\text{dom}(R) = \text{codom}(R) = X$. For a given relation, it will be useful to group the elements that are related to each other. This group will later be called an equivalence class of an equivalence relation. Using these groups we will induce a definition for what an equivalence relation should be.

Definition 1.3.7. We introduce the following binary function symbol to denote the set of elements that are related to a given representative x.

$$[x]_R := \{y \in X \mid x\ R\ y\}.$$

When the context is clear, the subscript R is often omitted. Since each member of $[x]$ is related, we will want to regard each one of them as the same. It will be the different sets $[x]$ that we are interested in; we wish to consider each $[x]$ as a single object in of itself. That is, for all $x \in X$ and $y \in X$ the following statements should be equivalent.

- $x\ R\ y$
- $[x] = [y]$ (1.1)
- $[x] \cap [y] \neq \varnothing$

This yields the following definition for an equivalence relation.

Definition 1.3.8 (Equivalence relation)**.** A relation (X, X, R) is an equivalence relation if the statements in Equation (1.1) are equivalent, in which case the set $[x]$ from Definition 1.3.7 will be called an equivalence class of R.

While this definition is sufficient, it will often be easier to prove an equivalent definition. This new definition is more practical.

Proposition 1.3.9. *Let (X, X, R) be a relation. Then R is an equivalence relation if and only if the following properties apply.*

Reflexive. $\forall x \in X(x\ R\ x)$.

Symmetric. $\forall x \in X \forall y \in X(x\ R\ y \iff y\ R\ x)$.

Transitive. $\forall x \in X \forall y \in X \forall z \in X(x\ R\ y \wedge y\ R\ z \implies x\ R\ z)$.

Proof. The forward direction follows directly from the axioms of equality. For the converse, suppose R is reflexive, symmetric and transitive. We will reason as follows.

1. $x\ R\ y \implies [x] = [y]$,
2. $[x] = [y] \implies [x] \cap [y] \neq \varnothing$,
3. $[x] \cap [y] \neq \varnothing \implies x\ R\ y$.

1. Suppose $x\ R\ y$, hence also $y\ R\ x$ by symmetry. Let $z \in [x]$ be arbitrary, so $x\ R\ z$. By transitivity we find $y\ R\ z$ and therefore $z \in [y]$. By a similar argument $[y] \subseteq [x]$. 2. Now suppose $[x] = [y]$. By reflexivity we have $x \in [x]$, so $[x]$ is nonempty and $[x] \cap [y] \neq \varnothing$. 3. Lastly if $[x] \cap [y] \neq \varnothing$, then there exists $z \in X$ such that both $z \in [x]$ and $z \in [y]$. Hence $x\ R\ z$ and $y\ R\ z$. By symmetry $z\ R\ y$ and then by transitivity $x\ R\ y$. □

To actually consider the equivalence classes as single objects, we introduce a new function symbol. The members of this set are precisely the equivalence classes.

Definition 1.3.10 (Quotient set)**.** Introduce the binary function symbol X/R by

$$X/R := \{[x] \in \mathcal{P}(X) \mid x \in X\}$$

called the quotient set.

1.4 Functions

One of the most important objects in mathematics are functions. Functions produce an output given an input in a prescribed way. We can use relations to define a function; two elements are related when one is the input and the other is the output. For this, we will introduce the following concepts.

Definition 1.4.1 (Total relation)**.** A relation (X, Y, R) is called total if $\mathrm{dom}(R) = \mathrm{corange}(R)$. That is $\mathrm{corange}(R) = X$.

Definition 1.4.2 (Univalent relation)**.** A relation (X, Y, R) is called univalent if

$$\forall x \in X \forall y_1 \in Y \forall y_2 \in Y (x \; R \; y_1 \wedge x \; R \; y_2 \implies y_1 = y_2)$$

A function is then a relation that satisfies both these conditions.

Definition 1.4.3 (Function)**.** A function is a relation (X, Y, f) that is both total and univalent.

For functions, Definition 1.4.1 states that every $x \in X$ is a valid input to the function; there exists a $y \in Y$ such that x is mapped to y. Definition 1.4.2 ensures that this y is unique; the same input to the function should return the same output. For functions, we introduce the ternary relation symbol $f(x) = y$ to mean $(x, y) \in f$. To further emphasise that a function transforms elements of a set X into elements of a set Y, we write $f : X \to Y$ for (X, Y, f). Sometimes one defines a function before it is verified that it is total and univalent. Once this is done, we call the function well-defined. Using functions we will now extend the set-builder notation.

Definition 1.4.4 (Extended set-builder notation)**.** Let φ be a formula with free variables among which X, y, Y. Define the ternary function symbol

$$\{f(x) \in Y \mid \varphi(X, y, Y)\} := \{y \in Y \mid \exists x \in X (f(x) = y \wedge \varphi(X, y, Y))\}.$$

With this, we can define the set of all function values.

Definition 1.4.5 (Image of set)**.** We introduce the binary function symbol $f(A)$ by

$$f(A) := \{f(x) \in Y \mid x \in A\}$$

called the image of A under f.

It follows that $f(X) = \mathrm{range}(f)$. This notation is often used because it is shorter.

The dual definitions of Definition 1.4.1 and 1.4.2 and will also be useful.

Definition 1.4.6 (Surjective relation)**.** A relation (X, Y, R) is surjective if $\text{codom}(R) = \text{range}(R)$. That is $\text{range}(R) = Y$.

Definition 1.4.7 (Injective relation)**.** A relation (X, Y, R) is injective if

$$\forall x_1 \in X \forall x_2 \in X \forall y \in Y (x_1 R y \wedge x_2 R y \implies x_1 = x_2).$$

Definition 1.4.6 states that every $y \in Y$ is attained; there exists an $x \in X$ such that $f(x) = y$. Definition 1.4.6 states that this x is unique. A function that satisfies these properties establishes a two-way correspondence between X and Y.

Definition 1.4.8 (Bijective function)**.** A function is bijective if it is both surjective and injective.

Being bijective means that every element of the domain can be associated with a unique element of the codomain, and the other way around. When this is the case, one can consider a new function where the output is the input and the input is the output. To rigorise this notion, we introduce a new function symbol.

Definition 1.4.9 (Inverse relation)**.** Let (X, Y, R) be a relation. We introduce the unary function symbol R^{-1} by

$$R^{-1} := \{(y, x) \in Y \times X \mid (x, y) \in R\}$$

called the inverse relation.

See Figure 1.1 for an example. The following proposition will be useful.

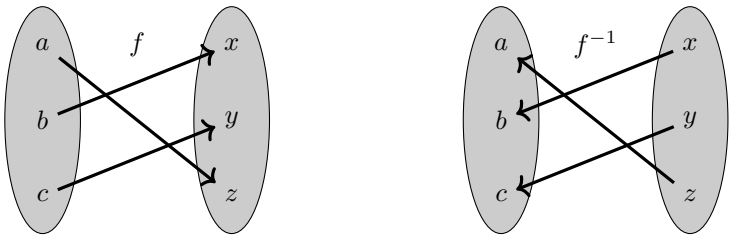

Figure 1.1: A bijective function and its inverse function

Proposition 1.4.10. *A function is bijective if and only if its inverse is a function as well.*

Proof. We will only need to prove one direction of the equivalence because of the total-surjective and univalent-injective dualities. Suppose f is bijective. The domain of f^{-1} is Y. By surjectivity of f, for any $y \in Y$ there exists an $x \in X$ such that $f(x) = y$, so $(y, x) \in f^{-1}$ and hence f^{-1} is total. Furthermore, this x is unique by injectivity of f, and hence f^{-1} is univalent. □

It is often useful to apply one function after the other, so that the output of one function becomes the input of another. We can define this as follows.

Definition 1.4.11 (Function composition)**.** Let $f : X \to Y$ and $g : Y \to Z$ be functions. Introduce the binary function symbol $g \circ f$ by

$$g \circ f := \{(x, z) \in X \times Z \mid \exists y \in Y((x, y) \in f \wedge (y, z) \in g)\}$$

called the composition of g and f.

Lastly we will introduce another useful function symbol. This will allow us to quickly write down the set of functions between any two sets.

Definition 1.4.12 (Set exponentiation)**.** We introduce the binary function symbol Y^X by

$$Y^X = \{f \in \mathcal{P}(X \times Y) \mid f : X \to Y\}.$$

Chapter 2

The natural numbers, integers and rational numbers

Introduction

Before constructing the real numbers, we will construct the intermediate number systems. Their constructions will be based on properties that should intuitively be true. For every number system we will both prove what properties they satisfy and in what way these properties make them unique.

First in Section 2.1 the natural numbers will be constructed. It will be in this section that we start defining algebraic structures with which the uniqueness of all number systems will be formulated. These structures are induced by the respective properties of the number system we are working in. The integers are then constructed in Section 2.2. The algebraic structures are expanded upon based on the new property the integers enjoy which the natural numbers do not. Lastly the rational numbers are constructed in Section 2.3, where also the most rich algebraic structure is defined.

2.1 The natural numbers

In his work *Was sind und was sollen die Zahlen* [8] Dedekind asked the right questions. Before defining what the natural numbers are, we should think about what they should be. One thing that we use the natural numbers for is counting things. Three apples, two books, etc. The gerund (a noun formed from a verb by adding "-ing") "counting" suggests this is a process. We do not instantly count three apples. Instead, we start with a count of zero, and for each apple we increment the count by one[1]. This intuition of counting apples in succession will form the foundation of the natural numbers.

[1]There are all kinds of psychological exceptions to this, where we do instantly count three objects by the shape they are arranged in! This is called "subitising", but is beyond the scope of this thesis.

With this in mind, mathematicians have attempted to characterise the natural numbers. The very first characterisation was given in the aforementioned work by Dedekind. He stated a list of properties that the natural numbers should satisfy. Today, these are known as the Dedekind-Peano axioms (**PA**). Dedekind initially stated these axioms in [8] and Peano later formalised these statements into a larger theory of sets in [25]. The axioms are stated in terms of a nullary function symbol 0 ("zero") and unary function symbol S. The function symbol S is called the successor function. Notably, in the formulations of both Dedekind and Peano the first axiom was that 1 ("one") is a natural number. Today it is more common to start counting from 0 ("zero"), in accordance with the intuition of starting with a count of zero. Below is an overview of the axioms. Even though these axioms are stated using sets, it should be noted that they are logically separate from **ZF**.

PA1 $0 \in \mathbb{N}$.

PA2 $\forall x \in \mathbb{N}(x = x)$.

PA3 $\forall x \in \mathbb{N} \forall y \in \mathbb{N}(x = y \implies y = x)$.

PA4 $\forall x \in \mathbb{N} \forall y \in \mathbb{N} \forall z \in \mathbb{N}(x = y \wedge y = z \implies x = z)$.

PA5 $\forall x \forall y \in \mathbb{N}(x = y \implies x \in \mathbb{N})$.

PA6 $\forall x \in \mathbb{N}(S(x) \in \mathbb{N})$.

PA7 $\forall x \in \mathbb{N} \forall y \in \mathbb{N}(S(x) = S(y) \implies x = y)$.

PA8 $\forall x \in \mathbb{N}(S(x) \neq 0)$.

PA9 $\forall N((0 \in N \wedge \forall x \in N(S(x) \in N)) \implies N = \mathbb{N})$.

These axioms capture the intuition related to counting we alluded to above. Axiom PA1 asserts that there is a count of zero. Axiom PA6 asserts that we can increment this count by one. That is, we can continue counting. Axiom PA9 makes sure that if another set behaves exactly like the natural numbers in the sense of Axiom PA1 and Axiom PA6, then this set is the set of natural numbers. Axiom PA8 says that a count of zero cannot be achieved by incrementing another count, and so on. When these axioms are stated in terms of sets within **ZF**, as we did here, the Axioms PA2-PA5 are trivially logically valid since **ZF** is a first-order theory with equality.

To construct the natural numbers, we will give an explicit definition of a suitable set of natural numbers along with a successor function and prove that they satisfy the Peano-Dedekind axioms. This characterises the natural numbers by their intuition of counting things. Afterwards, we will introduce algebraic operations that one can perform on the natural numbers. We will show these operations also satisfy the properties we expect them to satisfy. We will then give a characterisation of the natural numbers in terms of these operations and their properties.

Now, **ZF** comes with the Axiom of Infinity. Notice the similarity of this axiom with the Axioms PA1 and PA6. We will use the Axiom of Infinity to construct the natural numbers. Note that the it does not produce a unique set however, nor a set that only contains the natural numbers; we will have to

extract them. Intuitively, we will define the natural numbers as the smallest set satisfying the requirement in the statement of the Axiom of Infinity.

Definition 2.1.1 (Natural numbers)**.** Let S be the unary function symbol defined by $S(x) = x \cup \{x\}$. Let $\varphi(X)$ mean $\varnothing \in X \wedge \forall x \in X(S(x) \in X)$. Define the set $\mathbb{N}$ of natural numbers as the unique set satisfying the below formula with free variable N.

$$\forall n(n \in N \iff \forall X(\varphi(X) \implies n \in X)).$$

If $\mathbb{N}$ exists, it is clear it is unique. We will have to prove that $\mathbb{N}$ exists.

Proof. Let N be a set that exists by the Axiom of Infinity. Take $\mathbb{N} = \{n \in N \mid \forall X(\varphi(X) \implies n \in X)\}$. Then if $n \in \mathbb{N}$ we clearly have $\forall X(\varphi(X) \implies n \in X)$. On the other hand, if $\forall X(\varphi(X) \implies n \in X)$, we may choose $X = N$ so that we find $n \in N$ and hence $n \in \mathbb{N}$. □

It is easy to see that $\mathbb{N}$ satisfies φ as well. In particular $\varnothing \in \mathbb{N}$, and if $n \in \mathbb{N}$ then also $S(n) \in \mathbb{N}$ because $n \in N$. This allows us to transform the successor function symbol to an actual function on $\mathbb{N}$.

Definition 2.1.2 (Successor function)**.** We define $0 := \varnothing$. Define the successor function $S : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ by $S(n) = n \cup \{n\}$, and also define

$$\begin{aligned} 1 &:= S(0), & 4 &:= S(3), & 7 &:= S(6), \\ 2 &:= S(1), & 5 &:= S(4), & 8 &:= S(7), \\ 3 &:= S(2), & 6 &:= S(5), & 9 &:= S(8). \end{aligned}$$

Notice that $0 \notin \text{range}(S)$ because $S(n)$ is nonempty for all $n \in \mathbb{N}$. We continue counting according to any positional number system.

Notice that each natural number contains all "previous" natural numbers as elements. For example, $4 = \{0, 1, 2, 3\}$. Previous is in quotes, because we have not technically defined yet what it means for two natural numbers to be less than each other. This definition yields a straightforward way to do so, as we will see later.

As the name suggests, the successor function resembles the successor function symbol from the Dedekind-Peano axioms. It differs in a key aspect, though. Its codomain by definition does not include 0, making Axiom PA8 satisfied by definition. This is by design, and will prove useful.

Integrally tied to the successor function is the principle of mathematical induction. For this reason Axiom PA9 is sometimes also called the "axiom of induction". It states that if a statement is true for 0, and its truth for any $n \in \mathbb{N}$ implies the truth of the statement for $S(n)$, then the statement is true for all $n \in \mathbb{N}$. Figure 2.1 illustrates how this idea of induction forces $\mathbb{N}$ to exclude any unreachable numbers.

Theorem 2.1.3 (Mathematical induction)**.** *Let φ be a formula with free variables among which n. Then*

$$(\varphi(0) \wedge \forall n \in \mathbb{N}(\varphi(n) \implies \varphi(S(n)))) \implies \forall n \in \mathbb{N}(\varphi(n)).$$

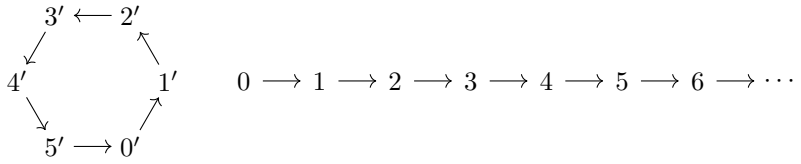

Figure 2.1: The accented natural numbers along with the regular natural numbers together satisfy Axioms PA1-PA8, but not Axiom PA9.

Proof. To prove induction holds, we will prove Axiom PA9 holds in $\mathbb{N}$ first. Let N be a set such that $0 \in N$ and for all $x \in N$ we have $S(x) \in N$. It is clear that $N \subseteq \mathbb{N}$. Also, N witnesses the Axiom of Infinity. Since we defined $\mathbb{N}$ as the smallest set satisfying this axiom, we must have $\mathbb{N} \subseteq N$, completing the proof of Axiom PA9. Now define $N = \{n \in \mathbb{N} \mid \varphi(n)\}$. Clearly $0 \in N$. Suppose $n \in N$ for some $n \in \mathbb{N}$. Then $\varphi(S(n))$ holds, so $S(n) \in N$. By Axiom PA9 we have $N = \mathbb{N}$. □

Notably, the proof of such a strong mathematical rule of inference is this short because it was essentially assumed as axiom. The Axiom of Infinity and Axiom PA9 are at the heart of the statement of mathematical induction; Theorem 2.1.3 only rephrases them as mathematical induction explicitly.

We have now shown that all but one of the Dedekind-Peano axioms apply in $\mathbb{N}$. We will capture the final result in a proposition.

Proposition 2.1.4 ($(\mathbb{N}, S)$ is a model of **PA**)**.** *The set* $\mathbb{N}$ *along with the function* S *satisfies the Dedekind-Peano axioms.*

Proof. All axioms but Axiom PA7 have been shown to apply. This last axiom corresponds to showing injectivity of S. Since its codomain excludes 0, we can make a stronger claim; S is bijective.

Injective. Suppose $S(m) = S(n)$. We will show $m = n$. By definition $m \cup \{m\} = n \cup \{n\}$, so $m \in n \cup \{n\}$ and $n \in m \cup \{m\}$. If $m \in n$, then we must have $n \notin m$. Hence $n \in \{m\}$ and so $m = n$. But then $m \notin n$, a contradiction. Thus $m \in \{n\}$, so $m = n$.

Surjective. Both induction and surjectivity pertain to the successor function reaching all natural numbers. Induction is a much stronger property though, and surjectivity follows from it. Since the codomain of S excludes 0, we will have to rephrase surjectivity of S in the following way to be able to use induction.

$$\forall m \in \mathbb{N}(m \neq 0 \implies \exists n \in \mathbb{N}(S(n) = m)).$$

The base case follows vacuously. For the induction step, suppose $m \neq 0$ implies the existence of an $n \in \mathbb{N}$ such that $S(n) = m$. Suppose $S(m) \neq 0$. If $m = 0$ then we can take $n = 0$ so that $S(n) = S(m)$. Else by the induction hypothesis there exists an $n_1 \in \mathbb{N}$ such that $S(n_1) = m$. Hence for $n_2 = S(n_1)$ we find $S(n_2) = S(m)$.

□

With the definition of the natural numbers out of the way, we can start to define the basic operations on them. To characterise these operations, we will use some algebraic structures. We will state their definitions as we will need them.

A consequence of the fact that S is is bijective, is that we can define its inverse function.

Definition 2.1.5 (Predecessor function)**.** We define the predecessor function $P : \mathbb{N} \setminus \{0\} \to \mathbb{N}$ to be the inverse of S. That is $P = S^{-1}$.

The predecessor function is not part of the language of **PA**, but the notion is convenient to have. We did not make the distinction here, but the predecessor is the algebraic predecessor. Order predecessors of a natural number also exist, which are natural numbers that precede that number. It is not always clear from the context which of the two is meant. In this thesis we will only consider the algebraic predecessor.

To define addition, one may think of it as repeated succession. The following definition captures this intuition.

Definition 2.1.6 (Addition of natural numbers)**.** We define addition as the map $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$\begin{aligned} m + 0 &= m, \\ m + S(n) &= S(m + n). \end{aligned}$$

This definition indeed boils down to repeatedly applying the successor function. This is illustrated by the following example.

Example. To evaluate $2 + 2$ we will simply follow the recursion.

$$\begin{aligned} 2 + 2 &= 2 + S(1) = S(2 + 1) \\ &= S(2 + S(0)) = S(S(2 + 0)) \\ &= S(S(2)) = S(3) = 4. \end{aligned}$$

One could use the predecessor function to find a direct expression for $m+n$. Namely for $n \neq 0$ we have $m + n = S(m + P(n))$. It is however more common to adhere to the language of **PA**, only using the successor function.

The first step into characterising the natural numbers is to show some properties of addition we expect addition to have. That is, if we add zero to something it remains unchanged, the grouping with which we evaluate a sum like "1+2+3" (either as "(1 + 2) + 3" or as "1 + (2 + 3)") should not matter and the order should not matter. Structures where these rules apply, are called commutative monoids.

Definition 2.1.7 (Commutative monoid)**.** Let $+$ be a binary operation on X. Then $(X, +)$ is a commutative monoid if the following properties apply.

Identity. $\exists 0 \in X \forall x \in X(0 + x = x + 0 = x)$.

Associative. $\forall x \in X \forall y \in X \forall z \in X(x + (y + z) = (x + y) + z)$.

Commutative. $\forall x \in X \forall y \in X(x + y = y + x)$.

Proposition 2.1.8. $(\mathbb{N}, +)$ *is a commutative monoid.*

Proof. Note that $x + 1 = x + S(0) = S(x + 0) = S(x)$.

Identity. Take the identity to be $0 \in \mathbb{N}$. We will argue by induction. The base case is trivially satisfied. Suppose $x+0 = 0+x = x$ for some $x \in \mathbb{N}$. Then $0 + S(x) = S(0 + x) = S(x) = S(x) + 0$.

Associative. We will argue by induction on z. The base case holds as $(x + y) + 0 = x + y = x + (y + 0)$. Now suppose $(x + y) + z = x + (y + z)$ for some $z \in \mathbb{N}$. Then

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

Commutative. We will argue by induction on x. The base case is satisfied by the existence of an identity element. As an intermediary result we will prove $x + 1 = 1 + x$, also by induction. The base case is again already satisfied. Suppose $x + 1 = 1 + x$ for some $x \in \mathbb{N}$. Then

$$S(x) + 1 = (x + 1) + 1 = (1 + x) + 1 = 1 + (x + 1) = 1 + S(x).$$

To complete the proof, suppose $x + y = y + x$ for some $x \in \mathbb{N}$. Then

$$\begin{aligned} y + S(x) &= y + (x + 1) = (y + x) + 1 = (x + y) + 1 \\ &= x + (y + 1) = x + (1 + y) = (x + 1) + y = S(x) + y. \end{aligned}$$

□

Similar to how we defined addition as repeated succession, we can define multiplication as repeated addition. The following definition does exactly that.

Definition 2.1.9 (Multiplication of natural numbers)**.** We define multiplication as the map $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by

$$\begin{aligned} m \cdot 0 &= 0, \\ m \cdot S(n) &= (m \cdot n) + m. \end{aligned}$$

The reader is invited to evaluate $2 \cdot 2$ using this definition to see that this definition of multiplication indeed captures the notion of repeated addition. Like with addition, one can use the predecessor function to write $m \cdot n = (m \cdot P(n)) + m$ for $n \neq 0$.

By convention, we will assume that multiplication has a higher precedence than addition. That is, we will read $x + y \cdot z$ as $x + (y \cdot z)$ and $x \cdot y + z$ as $(x \cdot y) + z$. Now that we have defined multiplication, we will show that it satisfies all the properties we want it to have. Along with the properties we saw addition had that multiplication should have too, we want addition and multiplication to interact as expected. That means that multiplication distributes over addition; "$1 \cdot (1 + 2)$" should equal "$1 \cdot 1 + 1 \cdot 2$". This yields the definition for the following important structure.

Definition 2.1.10 (Commutative semiring)**.** Let $+$ and $\cdot$ be binary operations on X. Then $(X, +, \cdot)$ is a commutative semiring if $(X, +)$ and $(X \setminus \{0\}, \cdot)$ are commutative monoids, $0 \neq 1$ and the distributive property applies.

Distributive. $\forall x \in X \forall y \in X \forall z \in X (x \cdot (y + z) = x \cdot y + x \cdot z)$.

Proposition 2.1.11. $(\mathbb{N}, +, \cdot)$ *is a commutative semiring.*

Proof. By Proposition 2.1.8 we have that $(\mathbb{N}, +)$ is a commutative monoid. It remains to show that $(\mathbb{N} \setminus \{0\}, \cdot)$ is a commutative monoid too and that multiplication distributes over addition.

Identity. Take $1 \in \mathbb{N}$ to be the identity. We will argue by induction. The base case holds because $0 \cdot 1 = (0 \cdot 0) + 0 = 0 = 1 \cdot 0$. Suppose $x \cdot 1 = 1 \cdot x = x$ for some $x \in \mathbb{N}$. Then $1 \cdot S(x) = 1 \cdot x + 1 = x + 1 = S(x) = S(x) \cdot 1$.

Distributive. We will argue by induction on z. The base case holds because $x \cdot (y + 0) = x \cdot y = x \cdot y + x \cdot 0$. Suppose $x \cdot (y + z) = x \cdot y + x \cdot z$ for some $z \in \mathbb{N}$. Then

$$\begin{aligned} x \cdot (y + S(z)) &= x \cdot S(y + z) = x \cdot (y + z) + x \\ &= x \cdot y + x \cdot z + x = x \cdot y + x \cdot S(z). \end{aligned}$$

Associative. We will argue by induction on z. The base case holds because $x \cdot (y \cdot 0) = x \cdot 0 = 0 = (x \cdot y) \cdot 0$. Suppose $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for some $z \in \mathbb{N}$. Then

$$\begin{aligned} (x \cdot y) \cdot S(z) &= (x \cdot y) \cdot z + x \cdot y = x \cdot (y \cdot z) + x \cdot y \\ &= x \cdot (y \cdot z + y) = x \cdot (y \cdot S(z)). \end{aligned}$$

Commutative. We will argue by induction on y. We will prove the base case by induction as well. The base case for this inner induction is trivially satisfied. Suppose $x \cdot 0 = 0 \cdot x$ for some $x \in \mathbb{N}$. Then

$$\begin{aligned} 0 \cdot S(x) &= 0 \cdot x + 0 = 0 \cdot x \\ &= x \cdot 0 = 0 = S(x) \cdot 0. \end{aligned}$$

Now suppose $x \cdot y = y \cdot x$ for some $y \in \mathbb{N}$. Then

$$\begin{aligned} x \cdot S(y) &= x \cdot y + x = x + y \cdot x \\ &= 1 \cdot x + y \cdot x = (1 + y) \cdot x = S(y) \cdot x. \end{aligned}$$

□

Lastly we will define the order on $\mathbb{N}$. The fact that each natural number contains every "previous" natural number will allow for a very simple definition.

Definition 2.1.12 (Order on natural numbers)**.** For two natural numbers m and n define the relation $\leq$ on $\mathbb{N}$ by $m \leq n$ if $m \in n \vee m = n$.

Orders can also be generalised to other sets. Thinking about how the order on natural numbers should work, the following definition should be reasonable.

Definition 2.1.13 (Total order)**.** Let $\leq$ be a relation on X. Then $(X, \leq)$ is a total order if the following properties apply.

Reflexive. $\forall x \in X (x \leq x)$.

Transitive. $\forall x \in X \forall y \in X \forall z \in X (x \leq y \wedge y \leq z \implies x \leq z)$.

Antisymmetric. $\forall x \in X \forall y \in X (x \leq y \wedge y \leq x \implies x = y)$.

Strongly connected. $\forall x \in X \forall y \in X (x \leq y \vee y \leq x)$.

Note that reflexivity follows from strongly connectedness. It is included for emphasis. We write $x < y$ to mean $x \leq y \wedge x \neq y$. Moreover $x > y$ and $x \geq y$ are to be interpreted as $y < x$ and $y \leq x$ respectively.

Like with multiplication interacting nicely with addition, the order should interact nicely with both these operations. This yields the important fundamental structure that was alluded to in the introduction; the ordered (commutative) semiring. The precise definition of this varies throughout the literature, though. For our purposes we will use the following definition.

Definition 2.1.14 (Ordered commutative semiring)**.** Let $+$ and $\cdot$ be binary operations on X and let $\leq$ be a relation on X. Then $(X, +, \cdot, \leq)$ is an ordered semiring if $(X, +, \cdot)$ is a commutative semiring, $(X, \leq)$ is a total order and the following properties apply.

OR1. $\forall x \in X \forall y \in X \forall z \in X (x \leq y \iff x + z \leq y + z)$.

OR2. $\forall x \in X \forall y \in X \forall z \in X (x \leq y \wedge z \geq 0 \implies x \cdot z \leq y \cdot z)$.

The backward implication of the first property is known as the cancellation law of the order. We will call an element $x \in X$ positive if $x > 0$, negative if $x < 0$ and nonnegative if $x \geq 0$.

There is an additional property that the order of the natural numbers has. This property is called well-ordering principle. It states that every nonempty subset of the natural numbers has a least element. For general orders this property is called well-foundedness and gives rise to the following definition.

Definition 2.1.15 (Well-order)**.** Let $\leq$ be a relation on X. Then $(X, \leq)$ is a well-order if it is a total order and it satisfies well-foundedness.

Well-founded. $\forall A \subseteq X (A \neq \varnothing \implies \exists x \in A \forall y \in A (x \leq y))$.

The importance of the well-ordering principle for the natural numbers is because of its relation to mathematical induction. In fact, it is equivalent to mathematical induction on the natural numbers. We will prove it implies induction first. We will show the converse in the proof of $(\mathbb{N}, \leq)$ being a well-order.

Proposition 2.1.16. *If $(\mathbb{N}, \leq)$ with $\leq$ from Definition 2.1.12 is a well-order, then the principle of mathematical induction holds.*

Proof. Suppose $(\mathbb{N}, \leq)$ is a well-order. Let φ be a formula with free variables among which n. By way of contradiction, suppose induction does not apply. Then there must be a set of counterexamples to $\varphi(n)$, so define $A = \{n \in \mathbb{N} \mid \neg\varphi(n)\}$. By the well-ordering principle we have that A has a least element n. Note that by assumption $\varphi(0)$ holds, so $n \neq 0$. But then for the predecessor $P(n)$ of n we must have that $\varphi(P(n))$ is true. However that implies $\varphi(n)$ is true, a contradiction. □

Note that this proof is technically superfluous because we already established that mathematical induction for the natural numbers holds in Theorem 2.1.3. The proof itself is very instructive, though. The interaction between the well-ordering principle and the predecessor function actually give rise to way we will characterise the natural numbers. First though, we will verify that the operations on the natural numbers indeed satisfy all the properties of a well-ordered commutative semiring.

Proposition 2.1.17. $(\mathbb{N}, +, \cdot, \leq)$ *is a well-ordered commutative semiring.*

Proof. By Proposition 2.1.11 we know that $(\mathbb{N}, +, \cdot)$ is a commutative semiring. It remains to show that $(\mathbb{N}, \leq)$ is a well-order and that addition and multiplication preserve the order. First we show that for all $x \in \mathbb{N}$ and $y \in \mathbb{N}$ we have that $x \in y$ implies $S(x) \in S(y)$. We will prove this by induction on y. The base case follows vacuously. For the induction step, suppose $x \in y$ implies $S(x) \in S(y)$ and take $x \in S(y)$. If $x \in y$ we find $S(x) \in S(y)$. Because $S(y) \subseteq S(S(y))$ we find $S(x) \in S(S(y))$. Else suppose $x \in \{y\}$, so $x = y$. Hence $S(x) = S(y)$, after which it follows that $S(x) \in S(S(y))$.

Transitive. We need to show that $x \leq y$ and $y \leq z$ implies $x \leq z$. When $x = y$ or $y = z$ the statement is trivially true. The same applies to when $y = 0$ or $z = 0$. It therefore remains to show that $x \in y$ and $y \in z$ implies $x \in z$ when $x \neq y$, $y \neq z$, $y \neq 0$ and $z \neq 0$. We will argue by induction on z. The base case follows by vacuous truth. For the induction step suppose $x \in y$ and $y \in z$ implies $x \in z$ under the conditions above. Take $x \neq y$, $y \neq S(z)$, $y \neq 0$ and $S(z) \neq 0$ and suppose $x \in y$ and $y \in S(z)$. If $y \in z$ we find $x \in z$ by the induction hypothesis, so also $x \in S(z)$. Else $y \in \{z\}$, so $y = z$. Hence $x \in z$ and again $x \in S(z)$.

Antisymmetric. Suppose $x \leq y$ and $y \leq x$. We have $x \in y \vee x = y$ and $y \in x \vee y = x$. If $x = y$ we are done. If not, we have $x \in y$ and $y \in x$, which is impossible.

Strongly connected. We need to show that for all $x \in \mathbb{N}$ and $y \in \mathbb{N}$ we have either $x \leq y$ or $y \leq x$. This is equivalent to showing that $x \neq y$ implies $x \in y$ or $y \in x$. We will argue by induction on x. The base case follows trivially. For the induction step suppose $x \neq y$ implies $x \in y$ or $y \in x$. Take $x \in \mathbb{N}$ with $S(x) \neq y$. If $x = y$ we immediately find $y \in S(x)$. Else $x \neq y$, so by the induction hypothesis we find $x \in y$ or $y \in x$. If $y \in x$ then clearly $y \in S(x)$. If $x \in y$ then $S(x) \in S(y)$. We cannot have $S(x) \in \{y\}$ since that would imply $S(x) = y$. Hence $S(x) \in y$.

OR1. Suppose $x \leq y$. We need to show that for all $z \in \mathbb{N}$ we have $x+z \leq y+z$. We will argue by induction on z. The base case trivially holds. Suppose $x+z \leq y+z$ for some $z \in \mathbb{N}$. If $x+z = y+z$ then we are done. If not, then $x + z \in y + z$. We then have $S(x + z) \in S(y + z)$, so $x + S(z) \in y + S(z)$.

Now suppose $x+z \leq y+z$. If $x = y$ then we are done. Else suppose $y \in x$, so $y + z \in x + z$. Regardless of whether $x + z = y + z$ or $x + z \in y + z$ we find $x + z \in x + z$, a contradiction. Therefore by strongly connectedness the only remaining possibility is $x \in y$.

Well-founded. Let $A \subseteq \mathbb{N}$ with $A \neq \varnothing$ be arbitrary. We need to show there exists an $x \in A$ such that for all $y \in A$ we have $x \leq y$. Take $x = \bigcap A$. We will show $x \in A$ by showing that for $s \in \mathbb{N}$ and $t \in \mathbb{N}$ we have $s \cap t = s$ or $s \cap t = t$. By strongly connectedness it suffices to show that $s \in t$ implies $s \cap t = s$. We will argue by induction on s. The base case follows trivially. For the induction step, suppose $s \in t$ implies $s \cap t = s$ for some $s \in \mathbb{N}$. Take $S(s) \in t$. That is $s + 1 < t$, so $s < t$. Hence by the induction hypothesis we find $S(s) \cap t = (s \cup \{s\}) \cap t = (s \cap t) \cup (\{s\} \cap t) = s \cup (\{s\} \cap t)$. Notice that $\{s\} \cap t = \{s\}$ since $s \in t$ implies $s \in \{s\} \cap t$. We conclude $S(s) \cap t = s \cup \{s\} = S(s)$. To show that x is indeed the minimum of A, let $y \in A$ be arbitrary. Then if $x = y$ we are done. If not, we have that $x \in y$, completing the proof.

OR2. Suppose $x \leq y$. We need to show that for all $z \in \mathbb{N}$ we have $x \cdot z \leq y \cdot z$. We will argue by induction on z. Suppose $x \leq y$. The base case trivially holds. Suppose $x \cdot z \leq y \cdot z$ for some $z \in \mathbb{N}$ with $z \geq 0$. Then $x \cdot S(z) = x \cdot (z + 1) = x \cdot z + x \leq y \cdot z + x \leq y \cdot z + y = y \cdot S(z)$.

□

We have now shown various properties of $\mathbb{N}$ along with its operations $+$, $\cdot$ and $\leq$. These properties, along with the fact that every nonzero natural number has a predecessor, yield a characterisation in terms of a well-ordered semiring structure that uniquely pinpoints the natural numbers. Here unique means "unique up to isomorphism". That is, if two sets satisfy these requirements, there exists an isomorphism between them. An isomorphism is a correspondence between two sets that preserves the operations in that set. We will only give the relevant precise definitions for ordered semiring structures; variants are easily derivable.

Definition 2.1.18 (Ordered semiring homomorphism)**.** Let $(X, +, \cdot, \leq)$ and $(Y, \oplus, \odot, \preceq)$ be ordered semirings. Then a function $f : X \to Y$ is an ordered semiring homomorphism if $f(0_X) = 0_Y$, $f(1_X) = 1_Y$ and $\forall x \in X \forall y \in X$

$$\begin{aligned} f(x + y) = f(x) \oplus f(y) \quad &\wedge \\ f(x \cdot y) = f(x) \odot f(y) \quad &\wedge \\ x \leq y \implies f(x) \preceq f(y), & \end{aligned}$$

in which case we say f preserves the structure of X and Y.

Definition 2.1.19 (Ordered semiring isomorphism)**.** Let $(X, +, \cdot, \leq)$ and $(Y, \oplus, \odot, \preceq)$ be ordered semirings. Then a function $f : X \to Y$ is an ordered semiring isomorphism if it is an ordered semiring homomorphism as well as bijective. We regard sets to be the same if there exists an isomorphism between them.

One can verify that the relation "unique op to isomorphism" satisfies the properties of an equivalence relation, which allows us to regard the structure as unique[2]. With that, the uniqueness of $\mathbb{N}$ is expressed in the following theorem.

[2]It is not a relation in the sense of Definition 1.3.5 because it would have to be a relation on the set of all sets, which as we have shown does not exist.

Theorem 2.1.20 (Uniqueness of $\mathbb{N}$)**.** *$(\mathbb{N}, +, \cdot, \leq)$ is the unique well-ordered commutative semiring in which every nonzero element has a predecessor.*

Proof. By Proposition 2.1.17 our set $\mathbb{N}$ is a well-ordered commutative semiring. It follows from Definition 2.1.5 that every nonzero element has a predecessor. Let N also satisfy these requirements. Define $\varphi : \mathbb{N} \to N$ by $\varphi(0_\mathbb{N}) = 0_N$ and $\varphi(n + 1_\mathbb{N}) = \varphi(n) + 1_N$. It will be useful to know that $0_N < 1_N$. Since $0_N \neq 1_N$ we either have $0_N < 1_N$ or $0_N > 1_N$. By way of contradiction, suppose $0_N > 1_N$. We then have $\varphi(n) > \varphi(n) + 1_N = \varphi(n + 1_\mathbb{N})$. That is, φ is a strictly decreasing sequence. Then $\varphi(\mathbb{N})$ is a subset of N that has no least element, violating well-foundedness of N. We conclude $0_N < 1_N$. This also means that the predecessors of N are unique, so that the predecessor function $P : N \setminus \{0_N\} \to N$ is well-defined. We will now show φ is an ordered semiring isomorphism.

Order homomorphism. We need to show that for all $m \in \mathbb{N}$ and $n \in \mathbb{N}$ with $m \leq n$ we have $\varphi(m) \leq \varphi(n)$. We will argue by induction on n. The base case $n = 0_\mathbb{N}$ follows because $m \leq n$ implies $m = 0_\mathbb{N}$. For the induction step, suppose $m \leq n$ implies $\varphi(m) \leq \varphi(n)$ for some $n \in \mathbb{N}$. Suppose $m \leq n + 1_\mathbb{N}$. If $m = n + 1_\mathbb{N}$, then clearly $\varphi(m) \leq \varphi(n + 1_\mathbb{N})$. Else $m < n + 1_\mathbb{N}$, so $m \leq n$. By the induction hypothesis we find $\varphi(m) \leq \varphi(n) \leq \varphi(n) + 1_N = \varphi(n + 1_\mathbb{N})$.

Injective. We will prove the contrapositive. Suppose $m < n$, so $m + 1_\mathbb{N} \leq n$. Since φ preserves the order we have $\varphi(m) + 1_N = \varphi(m + 1_\mathbb{N}) \leq \varphi(n)$. Hence $\varphi(m) < \varphi(n)$.

Surjective. By way of contradiction, suppose there exists an $m \in N$ such that for all $n \in \mathbb{N}$ we have $\varphi(n) \neq m$. Because N is well-ordered, we can take a minimal such m. Note that $m \neq 0_N$ because $\varphi(0_\mathbb{N}) = 0_N$. So m has a predecessor $P(s)$ for which there exists an $n \in \mathbb{N}$ such that $\varphi(n) = P(m)$. But then $m = P(m) + 1_N = \varphi(n) + 1_N = \varphi(n + 1_\mathbb{N})$, a contradiction.

Semiring homomorphism. Clearly $\varphi(0_\mathbb{N}) = 0_N$ and $\varphi(1_\mathbb{N}) = 1_N$. To prove that for all $m \in \mathbb{N}$ and $n \in \mathbb{N}$ we have $\varphi(m + n) = \varphi(m) + \varphi(n)$ we will use induction on m. The base case follows trivially. Suppose $\varphi(m + n) = \varphi(m) + \varphi(n)$ for some $m \in \mathbb{N}$. Then

$$\begin{aligned}\varphi(m + 1_N + n) &= \varphi(m + n + 1_N)\\ &= \varphi(m + n) + 1_N\\ &= \varphi(m) + \varphi(n) + 1_N\\ &= \varphi(m) + 1_N + \varphi(n) = \varphi(m + 1_\mathbb{N}) + \varphi(n).\end{aligned}$$

Similarly for multiplication the base case is trivial. Suppose $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ for some $m \in \mathbb{N}$. Then

$$\begin{aligned}\varphi((m + 1_\mathbb{N}) \cdot n) &= \varphi(m \cdot n + n)\\ &= \varphi(m \cdot n) + \varphi(n)\\ &= \varphi(m) \cdot \varphi(n) + \varphi(n)\\ &= (\varphi(m) + 1_N) \cdot \varphi(n) = \varphi(m + 1_\mathbb{N}) \cdot \varphi(n).\end{aligned}$$

We conclude N is isomorphic to $\mathbb{N}$. $\square$

This characterisation of the natural numbers lets us talk about the natural numbers without explicitly giving the definition of them. This is because the properties are independent of the definition chosen. For example, one may also define the natural numbers as Zermelo did, where $0 = \varnothing$ and $S(n) = \{n\}$[3]. Zermelo's definition is in a sense just as good, because one can prove all the same properties as we did. However, this definition turns out to be less convenient to do so with. The fact that we can now talk about the natural numbers without giving an explicit definition justifies how one has been doing arithmetic with them throughout ones life: there exists a unique structure that aligns with our intuition for the natural numbers, hence the arithmetic we have been doing was done in some model of this structure. Mathematics have allowed us to formally assure us these numbers actually exist and that they are what we think they are.

Given that that the set $\mathbb{N}$ now satisfies our intuition, we can put it to use to define a sequence. Contrary to a set, a sequence is a list where we can distinguish its first, second, third, and so forth element. The natural numbers yield a simple way to define this mathematically.

Definition 2.1.21 (Sequence)**.** A function $f : X \to Y$ is called a sequence if $\mathrm{dom}(f) = \mathbb{N}$, in which case we write f_n instead of $f(n)$.

Another common operation on the natural numbers is exponentiation. The reader may question why we have not defined this operation yet. The reason for that is that, algebraically speaking, exponentiation does not have many nice properties. It for example lacks associativity and commutativity. It will be useful later though, which is why we will define it now. We will define it similarly to how we defined addition multiplication; exponentiation is repeated multiplication. Here we choose to define it using the predecessor function.

Definition 2.1.22 (Exponentiation of natural numbers)**.** We define exponentiation as the map $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by[4]

$$m^n = \begin{cases} 1 & \text{if } n = 0 \\ m^{P(n)} \cdot m & \text{else} \end{cases}.$$

2.2 The integers

For a long time negative quantities were considered nonsense. One can count to three apples, but certainly not to negative three apples. This changed when many years after the discovery of the natural numbers, Chinese mathematicians explained how to do arithmetic with them in *Nine Chapters on Arithmetic* [24]:

> 正負術曰：同名相除，異名相益，正無入負之，負無入正之。
> 其異名相除，同名相益，正無入正之，負無入負之。

[3]This was also the way in which the Axiom of Infinity was originally stated. Notably, even without altering the axiom the existence of Zermelo's natural numbers follows from the existence of $\mathbb{N}$ and the Axiom Schema of Replacement.

[4]Under this definition 0^0 is defined as 1. This fits the definition well and is generally considered to be more useful than leaving it undefined.

Like signs subtract. Opposite signs add. Positive without extra, make negative; negative without extra makes positive. Opposite signs subtract; same signs add; positive without extra, make positive; negative without extra, make negative.

A useful interpretation of negative numbers is debt. When in debt, ones balance would be negative. One can then nullify this debt by paying it off. This idea of being able to nullify quantities gives rise to the invertibility property of the integers.

Intuitively the integers can be thought of as natural numbers with a sign; plus or minus. Mathematically, this is indeed also a way to construct them. For instance, one could consider the union of all pairs $(+, n)$ and $(-, n)$ for $n \in \mathbb{N}$ where $+$ and $-$ are any two distinct sets. Immediately a problem arises though, there should be only one additive identity, but currently both $(+, 0)$ and $(-, 0)$ exist. This can be fixed by excluding 0 and manually adding in an additive identity. Already this construction creates a lot of case-work.

Instead of this, one could think of the integers as differences of natural numbers. For example "$-2 = 2 - 4$", so the integer -2 would be represented by the pair $(2, 4)$. Of course, there are many such pairs that yield -2, the most natural of which being $0 - 2$ as we can just leave out the zero. We need to unify all these pairs in equivalence classes. Two integers should be equivalent when "$a - b = c - d$". Since we have not defined what subtraction is, we must rephrase this in terms of addition. We reach the following definition. Define the relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by

$$(a, b) \sim (c, d) \iff a + d = c + b. \tag{2.1}$$

The relation is now completely stated in terms of addition of natural numbers, which we have defined in the previous section. To consider the equivalence classes as representing the integers, we need to show $\sim$ defines an equivalence relation.

Lemma 2.2.1. *The relation $\sim$ as stated in Equation* (2.1) *defines an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

Proof. The proof is rather trivial. $\sim$ is reflexive by the reflexivity axiom of equality, symmetric by the symmetry axiom of equality and transitive by the transitivity axiom of equality. □

With this, we can define the integers as the quotient set of $\sim$.

Definition 2.2.2 (Integers)**.** Define the set $\mathbb{Z}$ of integers by $\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim$.

For $x \in \mathbb{N}$ we will denote the integer $[(x, 0)]$ by x and $[(0, x)]$ by $-x$. For example, the integer $[(0, 2)]$ is written -2. With the definition of the integers done, we can start to define the basic operations on them. Note that all these definitions can be informally derived by thinking of $[(a, b)]$ as "$a - b$".

Definition 2.2.3 (Addition of integers)**.** We define addition as the map $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by

$$[(a, b)] + [(c, d)] = [(a + c, b + d)].$$

It should be verified that this mapping is independent of the chosen representatives. For that, suppose $(a, b) \sim (e, f)$ and $(c, d) \sim (g, h)$. Hence

$a + f = e + b$ and $c + h = g + d$ so that $a + c + f + g = e + g + b + d$ and therefore $(a + c, b + d) \sim (e + g, f + h)$.

Note that it is not as natural to think of addition as repeated succession anymore. This is because of the presence of negative numbers. It would be unclear how $1 + (-2)$ would be the same as applying the successor function -2 times to 1. This is a trend that will continue as we progress in the construction of the real numbers; our intuitive definitions of addition and multiplications will no longer hold. However, our intuition for how they should behave, guide the way to define them.

As with the natural numbers, we wish to characterise the integers by proving properties they have. Importantly, unlike the natural numbers, the integers have inverses. For instance, -2 is the additive inverse of 2. This fact is entirely by construction; we defined the integers to be the difference of natural numbers. This extra property leads to the following definition.

Definition 2.2.4 (Abelian (or commutative) group)**.** Let $+$ be a binary operation on X. Then $(X, +)$ is an abelian group if it is a commutative monoid and every number has an additive inverse.

Inverse. $\forall x \in X \exists y \in X(x + y = 0)$.

If $0 \in X$, we will write write $-x$ to denote y. If not, we will write x^{-1} to denote y. The former notation is common for addition, and the latter notation is common for multiplication.

Proposition 2.2.5. $(\mathbb{Z}, +)$ *is an abelian group.*

Proof. With all the hard word done for the natural numbers in Proposition 2.1.8, we can simply delegate the proofs for the integers to properties about the natural numbers. The identity element is $[(0, 0)]$ as 0 is the identity element for the natural numbers. Associativity and commutativity follow because addition is associative and commutative in the natural numbers. What is new is that the integers have additive inverses.

Inverse. Let $[(a, b)] \in \mathbb{Z}$ be arbitrary. Then for $-[(a, b)] := [(b, a)] \in \mathbb{Z}$ we have
$[(a, b)] + [(b, a)] = [(a + b, b + a)] = [(a + b, a + b)] = [(0, 0)]$.

□

The next operation we will define is multiplication. This definition can be derived similar to how addition was derived.

Definition 2.2.6 (Multiplication of integers)**.** We define multiplication as the map $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by

$$[(a, b)] \cdot [(c, d)] = [(a \cdot c + b \cdot d, a \cdot d + b \cdot c)].$$

To verify $\cdot$ is a function, suppose $(a, b) \sim (e, f)$ and $(c, d) \sim (g, h)$. Hence $a+f = e+b$ and $c+h = g+d$ so that $c\cdot(a+f)+d\cdot(e+b)+h\cdot(e+b)+g\cdot(a+f) = c \cdot (e + b) + d \cdot (a + f) + h \cdot (a + f) + g \cdot (e + b)$. Then by the cancellation law it follows that $a \cdot c + b \cdot d + e \cdot h + f \cdot g = e \cdot g + f \cdot h + a \cdot d + b \cdot c$. Thus $(a \cdot c + b \cdot d, a \cdot d + b \cdot c) \sim (e \cdot g + f \cdot h, e \cdot h + f \cdot g)$. Henceforth we will only state that one should verify a mapping is well-defined, but not prove it.

Again, note that multiplication is no longer repeated addition as this will fail for negative numbers. Because addition now has inverses, the combined structure of addition and multiplication also improves with this change. This yields the following definition.

Definition 2.2.7 (Commutative ring)**.** Let $+$ and $\cdot$ be binary operations on X. Then $(X, +, \cdot)$ is a commutative ring if it is a commutative semiring and moreover $(X, +)$ is an abelian group.

Proposition 2.2.8. *$(\mathbb{Z}, +, \cdot)$ is a commutative ring.*

Proof. By Proposition 2.2.5 we have already established that $(\mathbb{Z}, +)$ is an abelian group. The multiplicative identity is $1 := [(1, 0)] \in \mathbb{Z}$ as for all $[(a, b)] \in \mathbb{Z}$ we have $[(a, b)] \cdot [(1, 0)] = [(a + 0, 0 + b)] = [(a, b)]$. The fact that $(\mathbb{Z}, \cdot)$ is a commutative monoid follows quite directly from the properties of multiplication of natural numbers we proved in Proposition 2.1.11. For instructiveness, we will give the proof for associativity.

Associativity. We must show that for $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ and $z \in \mathbb{Z}$ we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$. The symbol for multiplication of natural numbers will be omitted for readability. We have

$$\begin{aligned}
&([(a, b)] \cdot [(c, d)]) \cdot [(e, f)] \\
&= [(ac + bd, ad + bc)] \cdot [(e, f)] \\
&= [(e(ac + bd) + f(ad + bc), f(ac + bd) + e(ad + bc))] \\
&= [(abd + ace + adf + bcf, acf + ade + bce + bdf)]
\end{aligned}$$

and

$$\begin{aligned}
&[(a, b)] \cdot ([(c, d)] \cdot [(e, f)]) \\
&= [(a, b)] \cdot [(ce + df, cf + de)] \\
&= [(a(ce + df) + b(cf + de), a(cf + de) + b(ce + df))] \\
&= [(abd + ace + adf + bcf, acf + ade + bce + bdf)].
\end{aligned}$$

We see that these two expressions are equal, as required.

□

The last operation we will define on the integers is the order. This operation can also be intuitively derived.

Definition 2.2.9 (Order on integers)**.** We define the order on $\mathbb{Z}$ as $[(a, b)] \leq [(c, d)]$ if $a + d \leq c + b$.

One should verify that this definition is independent of the representatives chosen. Where the natural numbers had an ordered commutative semiring structure, the integers have an ordered commutative ring structure.

Proposition 2.2.10. *$(\mathbb{Z}, +, \cdot, \leq)$ is an ordered commutative ring.*

Proof. By Proposition 2.2.8 $(\mathbb{Z}, +, \cdot)$ is a commutative ring. Showing that $(\mathbb{Z}, \leq)$ is a total-order and that the order is preserved under addition and multiplication remains.

Transitive. Suppose $[(a,b)] \leq [(c,d)]$ and $[(c,d)] \leq [(e,f)]$. We want to show that $[(a,b)] \leq [(e,f)]$. We have $a+d \leq c+b$ and $c+f \leq e+d$. By adding f to the first inequality and b to the second, we obtain $a+d+f \leq c+b+f$ and $c+f+b \leq e+d+b$. By transitivity of the order on natural numbers we have $a+d+f \leq e+d+b$. By the cancellation law of the order on natural numbers we find $a+f \leq e+b$.

Antisymmetric. Suppose $[(a,b)] \leq [(c,d)]$ and $[(c,d)] \leq [(a,b)]$. We need to show that this implies $[(a,b)] = [(c,d)]$. We have $a+d \leq c+b \leq a+d$ and so $c+b = a+d$ by antisymmetry of the order on natural numbers.

Strongly connected. By strongly connectedness of the natural numbers we find $a+d \leq c+b$ or $c+b \leq a+d$.

OR1. Suppose $[(a,b)] \leq [(c,d)]$ and let $[(e,f)]$ be arbitrary. We want to show that $[(a,b)] + [(e,f)] \leq [(c,d)] + [(e,f)]$. We have

$$\begin{aligned} a+d \leq c+b &\iff a+d+e+f \leq c+b+e+f \\ &\iff [(a+e, b+f)] \leq [(c+e, d+f)] \\ &\iff [(a,b)] + [(e,f)] \leq [(c,d)] + [(e,f)]. \end{aligned}$$

OR2. Suppose $[(a,b)] \leq [(c,d)]$ and $[(e,f)] \geq 0$. We need to show that $[(a,b)] \cdot [(e,f)] \leq [(c,d)] \cdot [(e,f)]$. We have $a+d \leq c+b$ and $f \leq e$. Let $x = a+d$ and $y = c+b$, so $x \leq y$. We need to show that $x \cdot e + y \cdot f \leq x \cdot f + y \cdot e$. We will prove this by induction on e. For the base case $e = 0$ we have $f \leq 0$, so $f = 0$ as well, after which the base case follows. Next, suppose $x \leq y$ and $f \leq e$ implies $x \cdot e + y \cdot f \leq x \cdot f + y \cdot e$ for some $e \in \mathbb{N}$. Suppose $f \leq S(e)$ and $x \leq y$. If $f = S(e)$ then the result is immediate. Else we have $f \leq e$. Then

$$\begin{aligned} x \cdot S(e) + y \cdot f = x \cdot e + x + y \cdot f &\leq x \cdot f + y \cdot e + x \\ &\leq x \cdot f + y \cdot e + y = x \cdot f + y \cdot S(e). \end{aligned}$$

The converse is true as well as long as $[(e,f)] \neq 0$, which we will need later on. We need to show that $x \leq y$ when $x \cdot e + y \cdot f \leq x \cdot f + y \cdot e$ and $f < e$. We will use induction on x (this is equivalent to induction on a or d). The base case $x = 0$ follows because $y \geq 0$ for all $y \in \mathbb{N}$. For the induction step, suppose $x \cdot e + y \cdot f \leq x \cdot f + y \cdot e$ and $f < e$ implies $x \leq y$ for some $x \in \mathbb{N}$. Suppose $S(x) \cdot e + y \cdot f \leq S(x) \cdot f + y \cdot e$. By distributivity and the fact that $f < e$ we find $x \cdot e + e + y \cdot f \leq x \cdot f + e + y \cdot e$. Hence $x \cdot e + y \cdot f < x \cdot f + y \cdot e$ and by the induction hypothesis $x \leq y$. Now if $x = y$ we find $0 < 0$, so we must have $x \neq y$. Hence $S(x) \leq y$.

□

Note that, in contrast to the natural numbers, the integers are not well-ordered. This is because the well-foundedness property fails. The integers, as a subset of themselves, have no least element.

It is often stated that $\mathbb{N} \subseteq \mathbb{Z}$. However, this is technically false! The set $\mathbb{N}$ is a completely different set compared to $\mathbb{Z}$. Despite this, we still like to think that the integers contain the natural numbers, as well as their negatives. To rigorise

this, we can embed $\mathbb{N}$ into $\mathbb{Z}$ while keeping the properties the natural numbers had. This entails showing that the addition and multiplication of integers is compatible with the addition and multiplication of natural numbers, and that the order of integers is compatible with the order of natural numbers. More formally, we show that there exists an injective totally semiring homomorphism between $(\mathbb{N}, +, \cdot, \leq)$ and $(\mathbb{Z}, +, \cdot, \leq)$.

Proposition 2.2.11 (Embedding of $\mathbb{N}$ in $\mathbb{Z}$)**.** *There exists an injective ordered semiring homomorphism between* $(\mathbb{N}, +, \cdot, \leq)$ *and* $(\mathbb{Z}, +, \cdot, \leq)$*.*

Proof. Define $f : \mathbb{N} \to \mathbb{Z}$ by $f(n) = [(n, 0)]$. Clearly $f(0) = [(0, 0)] = 0$. For injectivity, suppose $f(m) = f(n)$. This implies $m = n$ as $[(m, 0)] = [(n, 0)]$ means $(m, 0) \sim (n, 0)$ and so $m = n$. We further want to show that $f(m+n) = f(m) + f(n)$. We see

$$f(m + n) = [(m + n, 0)] = [(m, 0)] + [(n, 0)] = f(m) + f(n).$$

Similarly for multiplication we see

$$f(m \cdot n) = [(m \cdot n, 0)] = [(m, 0)] \cdot [(n, 0)] = f(m) \cdot f(n).$$

For the order, suppose $m \leq n$. Then $f(m) = [(m, 0)] \leq [(n, 0)] = f(n)$. □

With this, the natural numbers can be viewed as a subset of the integers by considering $f(\mathbb{N})$. Indeed, the function f restricted to its range defines an ordered semiring isomorphism between $\mathbb{N}$ and $f(\mathbb{N}) \subseteq \mathbb{Z}$.

Even though the integers are not well-ordered, by Proposition 2.2.11 its positive elements are in fact well-ordered. This might not seem like much, but along with the structure we gave the integers, this is enough to characterise the integers. This is because we can use the well-ordering of the positive integers to reason about the negative integers.

Theorem 2.2.12 (Uniqueness of $\mathbb{Z}$)**.** $(\mathbb{Z}, +, \cdot, \leq)$ *is the unique ordered commutative ring whose positive elements are well-ordered.*

Proof. By Proposition 2.2.10 we know that $\mathbb{Z}$ is an ordered commutative ring. From Proposition 2.2.11 it follows that the positive elements of $\mathbb{Z}$ are well-ordered. Suppose Z also satisfies these requirements. We will define $\varphi : \mathbb{Z} \to Z$ as in the proof of Theorem 2.1.20. That is, define $\varphi(0_\mathbb{Z}) = 0_Z$ and $\varphi(a + 1_\mathbb{Z}) = \varphi(a) + 1_Z$. Knowing that we want φ to become a homomorphism, using $0_Z = \varphi(0_\mathbb{Z}) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a)$, the definition $\varphi(-a) = -\varphi(a)$ is induced. This defines φ for all integers. By the proof of Theorem 2.1.20 we know that φ is an ordered semiring isomorphism with respect to natural number addition, multiplication and order. Hence by Proposition 2.2.11 we can use that if $a \geq 0$ and $b \geq 0$ we have $\varphi(a + b) = \varphi(a) + \varphi(b)$ and $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. If further $a \leq b$ we have $\varphi(a) \leq \varphi(b)$. We will use this to prove that φ is an ordered ring isomorphism.

Ring homomorphism. Clearly $\varphi(0_\mathbb{Z}) = 0_Z$ and $\varphi(1_\mathbb{Z}) = 1_Z$. We will first show addition is preserved when $a + b \geq 0_\mathbb{Z}$. Then a or b is nonnegative. If both are, we are done. By commutativity we may assume $a \geq 0_\mathbb{Z}$. We will argue by induction on a. The base case is trivial. For the induction step, suppose $\varphi(a + b) = \varphi(a) + \varphi(b)$ when $a + b \geq 0_\mathbb{Z}$, $a \geq 0_\mathbb{Z}$ and $b < 0_\mathbb{Z}$.

Suppose $a + 1_\mathbb{Z} + b \geq 0_\mathbb{Z}$, $a + 1_\mathbb{Z} \geq 0_\mathbb{Z}$ and $b < 0_\mathbb{Z}$. If $a + b < 0_\mathbb{Z}$, then $a + 1_\mathbb{Z} = -b$. So $\varphi(a + 1_\mathbb{Z} + b) = \varphi(0_\mathbb{Z}) = \varphi(a + 1_\mathbb{Z}) + \varphi(b)$. Otherwise $a + b \geq 0_\mathbb{Z}$ and therefore $a > 0_\mathbb{Z}$, so by the induction hypothesis $\varphi(a+b) = \varphi(a) + \varphi(b)$. Hence $\varphi(a + 1_\mathbb{Z} + b) = \varphi(a) + \varphi(b) + 1_Z = \varphi(a + 1_\mathbb{Z}) + \varphi(b)$.

When $a + b \leq 0_\mathbb{Z}$, we have $-a - b \geq 0_\mathbb{Z}$. Then for the reason as above, we may take $-a \geq 0_\mathbb{Z}$. Then by the previous case $\varphi(a + b) = -\varphi(-a - b) = -\varphi(-a) - \varphi(-b) = \varphi(a) + \varphi(b)$.

Similarly for multiplication we have $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ for $a \geq 0_\mathbb{Z}$ and $b \geq 0_\mathbb{Z}$. Then if $a < 0_\mathbb{Z}$ and $b \geq 0_\mathbb{Z}$ we have $\varphi(a \cdot b) = -\varphi((-a) \cdot b) = -\varphi(-a) \cdot \varphi(b) = \varphi(a) \cdot \varphi(b)$. By commutativity the case when $b < 0_\mathbb{Z}$ and $a \geq 0_\mathbb{Z}$ follows too. Lastly if $a < 0_\mathbb{Z}$ and $b < 0_\mathbb{Z}$ we have $\varphi(a \cdot b) = \varphi((-a) \cdot (-b)) = \varphi(-a) \cdot \varphi(-b) = \varphi(a) \cdot \varphi(b)$.

Injective. Suppose $\varphi(a) = \varphi(b)$. We want to show that $a = b$. Without loss of generality, suppose $a \leq b$. Because φ preserves addition, we have $\varphi(0_\mathbb{Z}) = 0_Z = \varphi(b) - \varphi(a) = \varphi(b - a)$. Since $b - a \geq 0$ we have $b - a = 0_\mathbb{Z}$ as required.

Surjective. We will first prove every positive element is attained. By way of contradiction, suppose there exists a $z \in Z$ with $z > 0_Z$ such that for all $a \in \mathbb{Z}$ we have $\varphi(a) \neq z$. Because the positive elements of Z are well-ordered, we can take a minimal such element z. Then $z - 1_Z < z$, so there exists an $a \in \mathbb{Z}$ such that $\varphi(a) = z - 1_Z$. But then $z = z - 1_Z + 1_Z = \varphi(a) + 1_Z = \varphi(a + 1_\mathbb{Z})$, a contradiction. Now let $z \leq 0$ be arbitrary. Then $-z \geq 0$. For $z = 0_Z$ we have $\varphi(0_\mathbb{Z}) = 0_Z$. Else $-z > 0$, so there exists an $a \in \mathbb{Z}$ for which $\varphi(a) = -z$. We find $\varphi(-a) = -\varphi(a) = z$.

Order homomorphism. Suppose $a \leq b$. Then $0_\mathbb{Z} \leq b - a$, so $0_Z = \varphi(0_\mathbb{Z}) \leq \varphi(b - a)$. By the fact φ preserves addition, we have $0_Z \leq \varphi(b) + \varphi(-a) = \varphi(b) - \varphi(a)$. Hence $\varphi(a) \leq \varphi(b)$.

We conclude Z is isomorphic to $\mathbb{Z}$. □

2.3 The rational numbers

Rational numbers arise naturally as fractions or ratios. The following is Definition 3 in Book V of Euclid's[5] *Elements* [12]:

> Λόγος ἐστὶ δύο μεγεθῶν ὁμογενῶν ἡ κατὰ πηλικότητά ποια σχέσις.
>
> *A ratio is a sort of relation in respect of size between two magnitudes of the same kind.*

That is, the fraction (ratio) "$\frac{1}{4}$" is meant to denote one-fourths of something. Four times this quantity yields the whole. Mathematically this would mean that "$4 \cdot \frac{1}{4} = 1$". In other words, by definition "$\frac{1}{4}$" would be the multiplicative inverse of 4. Therefore mathematically the fractions add multiplicative inverses to the integers.

Out of any number system, perhaps the rational numbers have the most intuitive construction. When thinking of rational numbers as fractions, we know

[5] Much of Book V was likely inspired by Eudoxus' theory of proportion.

more than one fraction can represent a single rational number. For example $4/2 = 2/1$. In general, two rational numbers a/b and c/d are equal if $a \cdot d = c \cdot b$. This is precisely the relation that we will use to define the rational numbers. Define the relation $\sim$ on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ by

$$(a, b) \sim (c, d) \iff a \cdot d = c \cdot b. \tag{2.2}$$

Here the pair (a, b) represents the fraction a/b. We now wish to consider the rational numbers as equivalence classes of fractions.

Lemma 2.3.1. *The relation $\sim$ as stated in Equation (2.2) defines an equivalence relation on $\mathbb{Z} \times \mathbb{Z}$.*

Proof. The proof follows immediately by the axioms of equality. □

We will now define the rational numbers.

Definition 2.3.2 (Rational numbers)**.** Define the set $\mathbb{Q}$ of rational numbers by $\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})/\sim$.

We will denote the rational number $[(a, b)]$ by a/b or $\frac{a}{b}$. Additionally if $b = 1$ we will write just a. The integer a is called the numerator, and the integer b is called the denominator. The fact that the rational numbers are equivalence classes is baked in to the notation of them as fractions. Compare this to the integers, where one never writes $a - b$ to denote an integer. Because of the fact that fractions represent equivalence classes, we can pick representations that are convenient for proving statements about the rational numbers. For example, we can assume without loss of generality that every fraction has a positive denominator. This is because $(a, b) \sim (-a, -b)$, one of which necessarily has a positive denominator.

Now we will define the operations on the rational numbers. Like with the integers, these definitions can be derived informally by performing the arithmetic one is used to on fractions. Furthermore, the proofs for the properties these operations have are quite trivial and will be mostly skipped over.

Definition 2.3.3 (Addition of rational numbers)**.** We define addition as the map $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ defined by

$$[(a, b)] + [(c, d)] = [(a \cdot d + b \cdot c, b \cdot d)].$$

It can be verified that this defines a function. Addition of rational numbers has no new properties that addition of integers did not have. The structure of addition therefore remains an abelian group.

Proposition 2.3.4. *$(\mathbb{Q}, +)$ is an abelian group.*

Proof. The properties all follow by Proposition 2.2.5. The additive identity is $0 := [(0, 1)] \in \mathbb{Q}$ as $[(a, b)] + [(0, 1)] = [(a + 0, b)] = [(a, b)]$. The additive inverse for $[(a, b)] \in \mathbb{Q}$ is $-[(a, b)] := [(-a, b)] \in \mathbb{Q}$ as $[(a, b)] + [(-a, b)] = [(a \cdot b + -a \cdot b, b \cdot b)] = [(0, 1)]$. □

For fractions, multiplication is performed componentwise. This allows for the following simple definition.

Definition 2.3.5 (Multiplication of rational numbers)**.** We define multiplication as the map $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ defined by

$$[(a, b)] \cdot [(c, d)] = [(a \cdot c, b \cdot d)].$$

It can be verified that $\cdot$ is a function. Unlike rational number addition, rational number multiplication does have a new property compared to integer multiplication. (Nonzero) rational numbers now have a multiplicative inverse. This gives addition and multiplication of rational numbers the most algebraically rich structure we will encounter in our construction of the real numbers. This structure has the following definition.

Definition 2.3.6 (Field)**.** Let $+$ and $\cdot$ be binary operations on X. Then $(X, +, \cdot)$ is a field if $(X, +, \cdot)$ is a commutative ring and $(X \setminus \{0\}, \cdot)$ is a group.

Proposition 2.3.7. $(\mathbb{Q}, +, \cdot)$ *is a field.*

Proof. By Proposition 2.3.4 we have that $(\mathbb{Q}, +)$ is an abelian group. It follows by Proposition 2.2.8 that $(\mathbb{Q}, \cdot)$ is a commutative monoid. It is easy to see that the multiplicative identity is $1 := [(1, 1)] \in \mathbb{Q}$. Additionally, the rational numbers have multiplicative inverses.

Inverse. Let $[(a, b)] \in \mathbb{Q}$ with $[(a, b)] \neq 0$ be arbitrary. Then for $[(a, b)]^{-1} := [(b, a)] \in \mathbb{Q}$ we have $[(a, b)] \cdot [(b, a)] = [(a \cdot b, b \cdot a)] = [(1, 1)]$.

For distributivity, one should note that $[(ca, cb)] = [(a, b)]$ for all nonzero $c \in \mathbb{Z}$ and $[(a, b)] \in \mathbb{Q}$, after which it follows quickly. □

Lastly we define the order on $\mathbb{Q}$.

Definition 2.3.8 (Order on rational numbers)**.** Choose representatives $[(a, b)] \in \mathbb{Q}$ and $[(c, d)] \in \mathbb{Q}$ such that $b > 0$ and $c > 0$. We define the order on $\mathbb{Q}$ as $[(a, b)] \leq [(c, d)]$ if $a \cdot d \leq c \cdot b$.

It can be verified that this ordering is independent of the representatives chosen.

Proposition 2.3.9. $(\mathbb{Q}, +, \cdot, \leq)$ *is an ordered field.*

Proof. By Proposition 2.3.7 $(\mathbb{Q}, +, \cdot)$ is a field. It remains to show that $(\mathbb{Q}, \leq)$ is a total order and that the field operations behave well with the order. Antisymmetry and strongly connectedness follow directly by the respective properties of the order on integers.

Transitive. Suppose $[(a, b)] \leq [(c, d)]$ and $[(c, d)] \leq [(e, f)]$. We want to show that $[(a, b)] \leq [(e, f)]$. We have $a \cdot d \leq b \cdot c$ and $c \cdot f \leq d \cdot e$. Because we chose representatives with a positive denominator, we find $a \cdot d \cdot f \leq b \cdot c \cdot f \leq b \cdot d \cdot e$. By the cancellation law we additionally proved for the integers we find $a \cdot f \leq b \cdot e$.

OR1. Suppose $[(a, b)] \leq [(c, d)]$ and let $[(e, f)]$ be arbitrary. We want to show that $[(a, b)] + [(e, f)] \leq [(c, d)] + [(e, f)]$. We have $a \cdot d \leq c \cdot b$, so $a \cdot d \cdot f \cdot f \leq c \cdot b \cdot f \cdot f$. Adding $b \cdot d \cdot e \cdot f$ on both sides and using distributivity, we find $(a \cdot f + b \cdot e) \cdot d \cdot f \leq b \cdot f \cdot (c \cdot f + d \cdot e)$. Hence $[(a \cdot f + b \cdot e, b \cdot f)] \leq [(c \cdot f + d \cdot e, d \cdot f)]$ and so $[(a, b)] + [(e, f)] \leq [(c, d)] + [(e, f)]$ as required. Note that all steps are in fact equivalences, so the converse follows too.

OR2. Suppose $[(a,b)] \leq [(c,d)]]$ and let $[(e,f)] \geq 0$ with $f > 0$ be arbitrary. We need to show that $[(a,b)] \cdot [(e,f)] \leq [(c,d)] \cdot [(e,f)]$. We have $a \cdot d \leq c \cdot b$ and $e \geq 0$. Hence $e \cdot f \geq 0$ and so $a \cdot e \cdot d \cdot f \leq c \cdot e \cdot b \cdot f$. Here also all steps are equivalences, proving the converse.

□

We have just shown that $\mathbb{Q}$ is an ordered field. In fact, it turns out that $\mathbb{Q}$ is in a sense the smallest ordered field. This should make sense; starting from the natural numbers the only extensions we did added in the necessary numbers so that the additive and multiplicative inverses exist. We did not add any extra numbers that were not necessary for this purpose. Before we formalise this, we will first show that $\mathbb{Z}$ can be embedded in $\mathbb{Q}$; we would like to say that $\mathbb{Z} \subseteq \mathbb{Q}$. This works transitively; because $\mathbb{N}$ could be embedded in $\mathbb{Z}$, showing that $\mathbb{Z}$ can be embedded in $\mathbb{Q}$ means that $\mathbb{N}$ can also be embedded in $\mathbb{Q}$. This allows us to say $\mathbb{N} \subseteq \mathbb{Q}$. Formally the embedding would be the composition of the embeddings of $\mathbb{N}$ in $\mathbb{Z}$ and $\mathbb{Z}$ in $\mathbb{Q}$.

Proposition 2.3.10 (Embedding of $\mathbb{Z}$ in $\mathbb{Q}$)**.** *There exists an injective ordered semiring homomorphism between* $(\mathbb{Z}, +, \cdot, \leq)$ *and* $(\mathbb{Q}, +, \cdot, \leq)$*.*

Proof. Define $f : \mathbb{Z} \to \mathbb{Q}$ by $f(a) = [(a,1)]$. Clearly $f(0) = [(0,1)] = 0$. Suppose $f(a) = f(b)$, then $a = b$ as we have $(a,1) \sim (b,1)$. Furthermore we will show that $f(m+n) = f(m) + f(n)$. We see

$$f(a+b) = [(a+b,1)] = [(a,1)] + [(b,1)] = f(a) + f(b).$$

Similarly for multiplication we see

$$f(a \cdot b) = [(a \cdot b, 1)] = [(a,1)] \cdot [(b,1)] = f(a) \cdot f(b).$$

For the order, suppose $a \leq b$. Then $f(a) = [(a,1)] \leq [(b,1)] = f(b)$. □

We can now talk as the integers being contained in the rational numbers, and thereby also the natural numbers being contained in the rational numbers. With that, we now formalise the fact that $\mathbb{Q}$ is the smallest ordered field in the following theorem.

Theorem 2.3.11 ($\mathbb{Q}$ is the smallest ordered field)**.** *Every ordered field has a subfield isomorphic to* $(\mathbb{Q}, +, \cdot)$[6]*.*

Proof. Let $(\mathbb{K}, +, \cdot, \leq)$ be an ordered field. We will show that there is a field embedding of $\mathbb{Q}$ in $\mathbb{K}$. We will define $\varphi : \mathbb{Q} \to \mathbb{K}$ as in the proof of Theorem 2.2.12. In short, define $\varphi(0_{\mathbb{Q}}) = 0_{\mathbb{K}}$ and $\varphi(q + 1_{\mathbb{Q}}) = \varphi(q) + 1_{\mathbb{K}}$. This defines φ for all natural numbers. We extended this to the integers by defining $\varphi(-q) = -\varphi(q)$. To define φ on all of its domain, we note that every rational number can be written as $p \cdot q^{-1}$ for integers p and q. We thus want $1_{\mathbb{K}} = \varphi(1_{\mathbb{Q}}) = \varphi(q \cdot q^{-1}) = \varphi(q) \cdot \varphi(q^{-1})$, inducing $\varphi(p \cdot q^{-1}) = \varphi(p) \cdot \varphi(q)^{-1}$. Of course, the representation of a rational number as $p \cdot q^{-1}$ is not unique. It is simple to verify that φ is well-defined.

[6] A subfield is of a field $\mathbb{K}$ is a subset of $\mathbb{K}$ that satisfies the field axioms with respect to the operations inherited by $\mathbb{K}$.

By the proof of Theorem 2.2.12 we know that φ is an ordered ring isomorphism with respect to integer addition, multiplication and order. Hence by Proposition 2.3.10 we can use that for $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ we have $\varphi(a+b) = \varphi(a)+\varphi(b)$ and $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. If further $a \leq b$ then $\varphi(a) \leq \varphi(b)$. We will use this to show that φ defines a field embedding. We will drop the equivalence class brackets in the calculations for the sake of simplicity.

Ring homomorphism. Let $p = [(a,b)] \in \mathbb{Q}$ and $q = [(c,d)] \in \mathbb{Q}$ be arbitrary. Then

$$\begin{aligned}
\varphi(p+q) &= \varphi\left(\frac{a}{b} + \frac{c}{d}\right) = \varphi\left(\frac{a \cdot d + c \cdot b}{b \cdot d}\right) \\
&= \varphi(a \cdot d + c \cdot b) \cdot \varphi(b \cdot d)^{-1} \\
&= (\varphi(a \cdot d) + \varphi(c \cdot b)) \cdot \varphi(b \cdot d)^{-1} \\
&= \varphi(a \cdot d) \cdot \varphi(b \cdot d)^{-1} + \varphi(c \cdot b) \cdot \varphi(b \cdot d)^{-1} \\
&= \varphi(a \cdot d \cdot (b \cdot d)^{-1}) + \varphi(c \cdot b \cdot (b \cdot d)^{-1}) \\
&= \varphi\left(\frac{a}{b}\right) + \varphi\left(\frac{c}{d}\right) = \varphi(p) + \varphi(q).
\end{aligned}$$

Moreover

$$\begin{aligned}
\varphi(p \cdot q) &= \varphi\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \varphi\left(\frac{a \cdot c}{b \cdot d}\right) \\
&= \varphi(a \cdot c) \cdot \varphi(b \cdot d)^{-1} \\
&= \varphi(a) \cdot \varphi(c) \cdot (\varphi(b) \cdot \varphi(d))^{-1} \\
&= \varphi(a) \cdot \varphi(b)^{-1} \cdot \varphi(c) \cdot \varphi(d)^{-1} \\
&= \varphi\left(\frac{a}{b}\right) \cdot \varphi\left(\frac{c}{d}\right) = \varphi(p) \cdot \varphi(q).
\end{aligned}$$

Order homomorphism. Let $p = [(a,b)] \in \mathbb{Q}$ and $q = [(c,d)] \in \mathbb{Q}$ with $b > 0$ and $d > 0$ be arbitrary. Suppose $p \leq q$, so $a \cdot d \leq c \cdot b$. Then

$$\begin{aligned}
\varphi(a \cdot d) &\leq \varphi(c \cdot b) \\
\varphi(a) \cdot \varphi(d) &\leq \varphi(c) \cdot \varphi(b) \\
\varphi(a) \cdot \varphi(b)^{-1} &\leq \varphi(c) \cdot \varphi(d)^{-1} \\
\varphi(a/b) &\leq \varphi(c/d)
\end{aligned}$$

where we used that $\varphi(b) \geq 0$ implies that $\varphi(b)^{-1} \geq 0$.

Injective. Let $p = [(a,b)] \in \mathbb{Q}$ and $q = [(c,d)] \in \mathbb{Q}$ be arbitrary. Suppose that $\varphi(p) = \varphi(q)$. We have,

$$\begin{aligned}
\varphi\left(\frac{a}{b}\right) &= \varphi\left(\frac{c}{d}\right) \\
\varphi(a) \cdot \varphi(b)^{-1} &= \varphi(c) \cdot \varphi(d)^{-1} \\
\varphi(a) \cdot \varphi(d) &= \varphi(c) \cdot \varphi(b) \\
\varphi(a \cdot d) &= \varphi(c \cdot b).
\end{aligned}$$

Hence $a \cdot d = c \cdot b$, so $p = q$.

We thus find that $\varphi(\mathbb{Q}) \subseteq \mathbb{K}$ is isomorphic to $\mathbb{Q}$. $\square$

Note that the proof of Theorem 2.3.11 explicitly constructs a subfield that is isomorphic to $\mathbb{Q}$. This is also the unique subfield isomorphic to $\mathbb{Q}$. In general, the subfield constructed this way is called the prime subfield. For ordered fields, this prime subfield coincides with $\mathbb{Q}$.

Chapter 3

The real numbers

Introduction

While the natural numbers, integers and rational numbers have a mostly standard construction, the real numbers do not. In *The real numbers - a survey of constructions* [31] Weiss listed 19 (!) constructions of the real numbers. According to the paper these were most, if not all, constructions known at that time (2015). This increase in the ways the real numbers can be constructed in a way reflects their important distinction from the rational numbers. It is also evidence that their construction is likely not as straightforward as the constructions of the other number systems were. This is then also what makes their construction particularly interesting.

We will give three constructions. The first two constructions are the earliest and also most common formal constructions. They both date back to 1872. They are similar in nature, as they both lead to a central concept in the characterisation of the real numbers: completeness. The fact that the rational numbers seem to be incomplete dates back to as early as Ancient Greece. Completeness is what will distinguish the real numbers from the rational numbers. Intuitively a space is complete when it no longer has any holes. What these holes are precisely is dependent on the notion of completeness that is induced by the construction. Briefly put, by making an observation about something that does not hold in the rational numbers, the real numbers are constructed by addressing this deficiency.

The third construction is special. It is much more recent, and has an entirely different approach. Here the the focus is not so much on what properties the rational numbers lack, but on how the real numbers can be viewed. In fact, the rational numbers are skipped over entirely; the real numbers will be directly built from the integers.

Especially in the first two constructions, we will appeal to our intuition of what the real numbers should satisfy. Based on these intuitions, we will prove certain properties for each construction. This ensures that what we are constructing also aligns with what we want to construct.

In Section 3.1 we will give the first construction, the construction by Dedekind. In Section 3.2 we will walk through Cantor's construction. The last construction, by Schanuel, will be covered in Section 3.3. Their equivalence will

be proven in Section 3.4. We will do this by showing they all satisfy a particular characterisation of the real numbers. A comparison of the constructions will be given in Section 3.5. We will end with some closing remarks and possibilities for further research in Section 3.6.

3.1 Dedekind's construction

Dedekind observed the following about the rational numbers he denoted R [7]:

> Ist a eine bestimmte Zahl, so zerfallen alle Zahlen des Systems R in zwei Klassen, A_1 und A_2, deren jede unendlich viele Individuen enthält; die erste Klasse A_1 umfaßt alle Zahlen a_1, welche $< a$ sind, die zweite Klasse A_2 umfaßt alle Zahlen a_2, welche $> a$ sind; [...].
>
> *If a is a certain number, then all numbers in the system R fall into two classes, A_1 and A_2, each of which contains infinitely many individuals; the first class A_1 includes all numbers a_1 which are $< a$, the second class A_2 includes all numbers a_2 which are $> a$; [...].*

He called such a division a "Schnitte" (cut). Curiously, Dedekind did not come up with this idea himself. He was inspired by Euclid, who wrote the following in Definition 5 of Book V of *Elements* over two millennia earlier [12]!

> Ἐν τῷ αὐτῷ λόγῳ μεγέθη λέγεται εἶναι πρῶτον πρὸς δεύτερον καὶ τρίτον πρὸς τέταρτον, ὅταν τὰ τοῦ πρώτου καὶ τρίτου ἰσάκις πολλαπλάσια τῶν τοῦ δευτέρου καὶ τετάρτου ἰσάκις πολλαπλασίων καθ' ὁποιονοῦν πολλαπλασιασμὸν ἑκάτερον ἑκατέρου ἢ ἅμα ὑπερέχῃ ἢ ἅμα ἴσα ἢ ἅμα ἐλλείπῃ ληφθέντα κατάλληλα.
>
> *Magnitudes are said to be in the same ratio, the first to the second and the third to the fourth, when, if any equimultiples whatever are taken of the first and third, and any equimultiples whatever of the second and fourth, the former equimultiples alike exceed, are alike equal to, or alike fall short of, the latter equimultiples respectively taken in corresponding order.*

That is, a ratio of two numbers (here to be understood as a rational number) is defined by the three classes of rational numbers it produces; those less than it, equal to it, and greater than it. Euclid himself took this from Eudoxus' theory of proportions. Even though the necessary mathematics were not there yet for Euclid to construct the real numbers, the ideas were long present. To actually construct the real numbers, Dedekind importantly noted the following:

> Aber man überzeugt sich leicht, daß auch unendlich viele Schnitte existieren, welche nicht durch rationale Zahlen hervorgebracht werden.
>
> *But one can easily convince oneself that there are also infinitely many cuts which are not produced by rational numbers.*

He gives the following example. Let D be a positive integer that is not the square of an integer. Then there exists a positive integer λ such that

$$\lambda^2 < D < (\lambda + 1)^2.$$

He then continues to prove that the cut defined by the squares of rational numbers less than D and greater than D is not produced by any rational number. Dedekind observed that, contrary to the rational numbers, the real numbers do intuitively have the property that every cut is produced by a real number. It was this insight, which Dedekind deemed trivial

> Wie schon gesagt, glaube ich nicht zu irren, wenn ich annehme, daß jedermann die Wahrheit dieser Behauptung sofort zugeben wird; die meisten meiner Leser werden sehr enttäuscht sein, zu vernehmen, daß durch diese Trivialität das Geheimnis der Stetigkeit enthüllt sein soll.
>
> *As I have already said, I do not think I am mistaken in assuming that everyone will immediately admit the truth of this statement; most of my readers will be very disappointed to hear that the secret of continuity is revealed by this triviality.*

that revealed the "Geheimnis der Stetigkeit" (secret of continuity). To start, we will first give the following definition.

Definition 3.1.1 (Partition)**.** A partition $\mathcal{F}$ of a set X is a family of subsets of X such that

- $\varnothing \notin \mathcal{F}$,
- $\bigcup \mathcal{F} = X$,
- $\forall A \in \mathcal{F} \forall B \in \mathcal{F} (A \neq B \implies A \cap B = \varnothing)$.

The cuts, now to be called Dedekind cuts, can then be defined as follows.

Definition 3.1.2 (Dedekind cut)**.** A Dedekind cut of $\mathbb{Q}$ is a partition into two subsets (A, B) of $\mathbb{Q}$ such that A is closed downwards

$$\forall q \in A \forall p \in \mathbb{Q} (p < q \implies p \in A),$$

B is closed upwards

$$\forall q \in B \forall p \in \mathbb{Q} (p > q \implies p \in B)$$

and A does not contain a greatest element

$$\forall p \in A \exists q \in A (q > p).$$

Figure 3.1 is an example of a Dedekind cut. Hence intuitively, the cuts are of the form "$(-\infty, a)$" so that every element of A is less than every element in B. Notice that A being closed downloads implies B is closed upwards. This means that for a partition (A, B) being a Dedekind cut only imposes restrictions on the first set A. The set B is then completely determined by A. We can therefore uniquely identify the partition (A, B) by its first component A. With this, we can define the real numbers as the set of all Dedekind cuts.

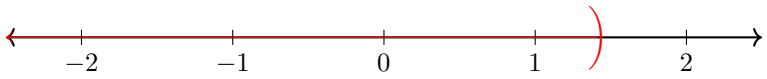

Figure 3.1: The Dedekind cut $\{q \in \mathbb{Q} \mid q < 0 \vee q \cdot q < 2\}$

Definition 3.1.3 (Real numbers)**.** Define the set $\mathbb{R}_D$ of (Dedekind) real numbers by

$$\mathbb{R}_D := \{A \in \mathcal{P}(\mathbb{Q}) \mid A \text{ is a Dedekind cut of } \mathbb{Q}\}.$$

Most operations on the Dedekind cuts are easy to define, like addition.

Definition 3.1.4 (Addition of real numbers)**.** Define addition as the map $\mathbb{R}_D \times \mathbb{R}_D \to \mathbb{R}_D$ defined by

$$A + B = \{a + b \in \mathbb{Q} \mid a \in A \wedge b \in B\}.$$

One can verify that $A + B$ is again a Dedekind cut.

Proposition 3.1.5. *$(\mathbb{R}_D, +)$ is an abelian group.*

Proof. We will prove each requirement.

Commutative. Let $A \in \mathbb{R}_D$ and $B \in \mathbb{R}_D$ be arbitrary. We have

$$\begin{aligned} A + B &= \{a + b \in \mathbb{Q} \mid a \in A \wedge b \in B\} \\ &= \{b + a \in \mathbb{Q} \mid b \in B \wedge a \in A\} = B + A. \end{aligned}$$

Identity. Define $0 := \{q \in \mathbb{Q} \mid q < 0\}$. Then 0 is a Dedekind cut. Further we need to show that

$$A + 0 = \{a + q \in \mathbb{Q} \mid a \in A \wedge q < 0\}$$

is equal to A. It is clear that $A \subseteq A + 0$. Let $a + q \in \mathbb{Q}$ with $a \in A$ and $q < 0$ be arbitrary. Because A is closed downwards we have that since $a + q < a$ we also have $a + q \in A$. We conclude $A + 0 = A$.

Associative. Let $A \in \mathbb{R}_D$, $B \in \mathbb{R}_D$ and $C \in \mathbb{R}_D$ be arbitrary. Then

$$\begin{aligned} A + (B + C) &= A + \{b + c \in \mathbb{Q} \mid b \in B \wedge c \in C\} \\ &= \{a + x \in \mathbb{Q} \mid a \in A \wedge x \in \{b + c \in \mathbb{Q} \mid b \in B \wedge c \in C\}\} \\ &= \{a + (b + c) \in \mathbb{Q} \mid a \in A \wedge b \in B \wedge c \in C\} \\ &= \{(a + b) + c \in \mathbb{Q} \mid a \in A \wedge b \in B \wedge c \in C\} \\ &= \{x + c \in \mathbb{Q} \mid x \in \{a + b \in \mathbb{Q} \mid a \in A \wedge b \in B\} \wedge c \in C\} \\ &= \{a + b \in \mathbb{Q} \mid a \in A \wedge b \in B\} + C \\ &= (A + B) + C. \end{aligned}$$

Inverse. Let $A \in \mathbb{R}_D$ be arbitrary. Take $-A := \{q - b \in \mathbb{Q} \mid q < 0 \wedge b \in \mathbb{Q} \setminus A\}$. Then $-A$ is a Dedekind cut and

$$\begin{aligned} A + (-A) &= \{a + (q - b) \in \mathbb{Q} \mid q < 0 \wedge a \in A \wedge b \in \mathbb{Q} \setminus A\} \\ &= \{q + (a - b) \in \mathbb{Q} \mid q < 0 \wedge a \in A \wedge b \in \mathbb{Q} \setminus A\} \\ &= \{q + p \in \mathbb{Q} \mid q < 0 \wedge p < 0\} \\ &= \{q \in \mathbb{Q} \mid q < 0\} = 0. \end{aligned}$$

□

Unfortunately, multiplication is slightly harder to define. A naive definition would be $A \cdot B = \{a \cdot b \in \mathbb{Q} \mid a \in A \wedge b \in B\}$. Recall that intuitively the cuts are of the form "$(-\infty, a)$". We would for example want that "$(-\infty, -1) \cdot (-\infty, -1) = (-\infty, 1)$". With this definition however, since -2 is in both intervals, $-2 \cdot -2 = 4$ would be in the resulting interval. We therefore need to ignore the negative numbers and add them back in manually. We also need to consider the sign of both numbers in separate cases. For this reason, we will first define the order on the real numbers. Luckily this is very straightforward.

Definition 3.1.6 (Order on real numbers)**.** Define the order on $\mathbb{R}_D$ as $A \leq B$ if $A \subseteq B$.

We want to define multiplication for negative real numbers in terms of multiplication of nonnegative real numbers. That means we need the fact that if $A < 0$ then $-A > 0$. We will thus prove that $\leq$ is a total order and that the order is preserved under addition.

Proposition 3.1.7. *$(\mathbb{R}_D, +, \leq)$ is an ordered abelian group.*

Proof. By Proposition 3.1.5 we know that $(\mathbb{R}_D, +)$ is an abelian group. It remains to show that $(\mathbb{R}_D, \leq)$ is a total order and that the order is preserved under addition. Transitivity follows by transitivity of $\subseteq$ and antisymmetry follows directly by the Axiom of Extensionality.

Strongly connected. By way of contradiction, suppose $A \not\leq B$ and $B \not\leq A$. Then there exists an $a \in A$ such that $a \notin B$ and a $b \in B$ such that $b \notin A$. By strongly connectedness of $\mathbb{Q}$, we may without loss of generality assume $a < b$. Since B is closed downwards we must have $a \in B$, a contradiction.

OR1. Let $A \in \mathbb{R}_D$, $B \in \mathbb{R}_D$ and $C \in \mathbb{R}_D$ be arbitrary and suppose $A \leq B$. We want to show that $A + C \leq B + C$. Let $a + c \in A + C$ be arbitrary. Since $A \subseteq B$ we know $a \in B$. Hence $a + c \in B + C$.

□

If we now have $A < 0$, we see that $-A > 0$ by adding $-A$ to both sides. Now we can define multiplication.

Definition 3.1.8 (Multiplication of real numbers)**.** Define multiplication as the map $\mathbb{R}_D \times \mathbb{R}_D \to \mathbb{R}_D$ defined by

$$A \cdot B = \begin{cases} \{a \cdot b \in \mathbb{Q} \mid a \in A \wedge a \geq 0 \wedge b \in B \wedge b \geq 0\} \cup 0 & \text{if } A \geq 0 \wedge B \geq 0 \\ -((-A) \cdot B) & \text{if } A < 0 \wedge B \geq 0 \\ -(A \cdot (-B)) & \text{if } A \geq 0 \wedge B < 0 \\ (-A) \cdot (-B) & \text{if } A < 0 \wedge B < 0 \end{cases}.$$

It can be verified that $A \cdot B$ is a Dedekind cut. $\mathbb{R}_D$ has the following structure.

Proposition 3.1.9. *$(\mathbb{R}_D, +, \cdot, \leq)$ is an ordered field.*

Proof. By Proposition 3.1.7 we know that $(\mathbb{R}_D, +, \leq)$ is a totally ordered abelian group. It remains to show that $(\mathbb{R}_D, +, \cdot)$ is a field and that the order is preserved under multiplication. Throughout the proof we will assume all real numbers to be nonnegative. The cases for negative values are similar. Denote $\mathbb{R}_D^{\geq 0} = \{A \in \mathbb{R}_D \mid A \geq 0\}$. The proofs for associativity and distributivity are omitted.

Commutative. Let $A \in \mathbb{R}_D^{\geq 0}$ and $B \in \mathbb{R}_D^{\geq 0}$ be arbitrary. We want to show that $A \cdot B = B \cdot A$. We have

$$\begin{aligned} A \cdot B &= \{a \cdot b \in \mathbb{Q} \mid a \in A \wedge a \geq 0 \wedge b \in B \wedge b \geq 0\} \cup 0 \\ &= \{b \cdot a \in \mathbb{Q} \mid b \in B \wedge b \geq 0 \wedge a \in A \wedge a \geq 0\} \cup 0 = B \cdot A. \end{aligned}$$

Identity. Define $1 := \{q \in \mathbb{Q} \mid q < 1\}$. Then 1 is a Dedekind cut. Let $A \in \mathbb{R}_D^{\geq 0}$ be arbitrary. We have

$$\begin{aligned} A \cdot 1 &= \{a \cdot q \in \mathbb{Q} \mid a \in A \wedge a \geq 0 \wedge q < 1 \wedge q \geq 0\} \cup 0 \\ &= \{a \in \mathbb{Q} \mid a \in A \wedge a \geq 0\} \cup 0 \\ &= \{a \in \mathbb{Q} \mid a \in A\} = A, \end{aligned}$$

where we used that multiplying a by $0 \leq q < 1$ cannot result in a leaving A or $a < 0$.

Inverse. Let $A \in \mathbb{R}_D$ be arbitrary with $A > 0$. Define $A^{-1} := \{q/b \in \mathbb{Q} \mid q < 1 \wedge b \in \mathbb{Q} \setminus A\}$. Then

$$\begin{aligned} A \cdot A^{-1} &= \{a \cdot (q/b) \in \mathbb{Q} \mid a \in A \wedge a \geq 0 \wedge q < 1 \wedge b \in \mathbb{Q} \setminus A \wedge q \geq 0\} \cup 0 \\ &= \{q \cdot (a/b) \in \mathbb{Q} \mid a \in A \wedge a \geq 0 \wedge q < 1 \wedge b \in \mathbb{Q} \setminus A \wedge q \geq 0\} \cup 0 \\ &= \{q \cdot p \in \mathbb{Q} \mid q < 1 \wedge q \geq 0 \wedge p < 1 \wedge p \geq 0\} \cup 0 \\ &= \{q \in \mathbb{Q} \mid q < 1 \wedge q \geq 0\} \cup 0 \\ &= \{q \in \mathbb{Q} \mid q < 1\} = 1, \end{aligned}$$

where we used that multiplying q by $0 \leq a/b < 1$ cannot result in $q > 1$ or $q < 0$.

OR2. Let $A \in \mathbb{R}_D^{\geq 0}$, $B \in \mathbb{R}_D^{\geq 0}$ and $C \in \mathbb{R}_D^{\geq 0}$ with $A \leq B$ be arbitrary. We wish to show that $A \cdot C \leq B \cdot C$. Let $a \cdot c \in A \cdot C$ be arbitrary. Then $a \in B$ as $A \subseteq B$. Hence $A \cdot C \leq B \cdot C$.

□

We just showed that $\mathbb{R}_D$ is an ordered field. In Proposition 2.3.9 we saw that $\mathbb{Q}$ also has this structure. However, $\mathbb{R}_D$ has an important property $\mathbb{Q}$ does not have. That is, $\mathbb{Q}$ has Dedekind cuts that are not produced by rational numbers. Since we constructed $\mathbb{R}_D$ by filling these holes, we expect that $\mathbb{R}_D$ no longer has any. This is indeed the case, and is known as Dedekind-completeness. This is the secret of continuity Dedekind alluded to.

Proposition 3.1.10 ($\mathbb{R}_D$ is Dedekind-complete)**.** *For every Dedekind cut A of $\mathbb{R}_D$ there exists an $x \in \mathbb{R}_D$ such that $A = \{a \in \mathbb{R}_D \mid a < x\}$.*

Proof. Let A be a Dedekind cut of $\mathbb{R}_D$. Define $x = \bigcup A$. Then x is the result of combining all Dedekind cuts that exist in A. We claim that $A = \{a \in \mathbb{R}_D \mid a < x\}$. To show $x \in \mathbb{R}_D$ we need to show that x is a Dedekind cut of $\mathbb{Q}$. Clearly x is nonempty and not equal to $\mathbb{Q}$. To show that x is closed downwards, suppose $p < q$ for any $q \in x$ and $p \in \mathbb{Q}$. Since $q \in x$ we have that there exists an $a \in A$ such that $q \in a$. Since a is closed downwards we must have $p \in a$ and hence $p \in x$. By a similar argument x does not contain a greatest element. Next we will show $A \subseteq \{a \in \mathbb{R}_D \mid a < x\}$. Let $a \in A$ be arbitrary. Since we have $a \subseteq x$, by definition also $a \leq x$. And since A has no greatest element, there exists a $b \in A$ such that $a < b \leq x$. Thus $a \neq x$. Lastly we will show $\{a \in \mathbb{R}_D \mid a < x\} \subseteq A$. Let $a \in \mathbb{R}_D$ with $a < x$ be arbitrary. Take $p \in x \setminus a$. Then we have $a \subseteq \{q \in \mathbb{Q} \mid q < p\}$. If we now take $b \in A$ with $p \in b$, we find $a \subseteq \{q \in \mathbb{Q} \mid q < p\} \subseteq b$ and hence $a \in A$. □

Instead of Dedekind-completeness, in the literature one often refers to this property as the least-upper-bound property of the real numbers. This equivalent property is more practical, whereas the Dedekind-completeness property is more instructional. To state the least-upper-bound property, we will first state two definitions on which it depends.

Definition 3.1.11 (Bounded (above) set)**.** Let $(X, \leq)$ be a total order. Let $A \subseteq X$ be a subset of X. Then A is bounded if $\exists S \in X \forall x \in A(|x| \leq S)$ and bounded above if $\exists S \in X \forall x \in A(x \leq S)$. We say that A is unbounded (above) when it is not bounded (above).

Definition 3.1.12 (Supremum)**.** Let $(X, \leq)$ be a total order. Let $A \subseteq X$ be a subset of X. Then $S \in X$ is a supremum of A if

- $\forall x \in A(x \leq S)$,
- $\forall T \in X((\forall x \in A(x \leq T)) \implies S \leq T)$.

By the antisymmetry of the order it quickly follows that the supremum is unique.

The first requirement of Definition 3.1.12 is that the supremum is an upper bound, the second is that it is the least upper bound; it is less than or equal to all other upper bounds. The least-upper-bound property can be stated as follows.

Definition 3.1.13 (Least-upper-bound property)**.** An ordered field $\mathbb{K}$ satisfies the least-upper-bound property when every bounded above subset of $\mathbb{K}$ has a supremum.

We will now prove Dedekind-completeness and the least-upper-bound property are in fact equivalent.

Proposition 3.1.14. *Let $\mathbb{K}$ be an ordered field. Then $\mathbb{K}$ is Dedekind-complete if and only if $\mathbb{K}$ satisfies the least-upper-bound property.*

Proof. Suppose $\mathbb{K}$ is Dedekind-complete. Let A be a bounded above subset of $\mathbb{K}$. If A has a maximum M, then it is clear it is also the supremum. Therefore suppose A has no greatest element. Define $B = \bigcup\{\{b \in \mathbb{K} \mid b < a\} \in \mathcal{P}(\mathbb{K}) \mid a \in A\}$. It is routine to verify that B is a Dedekind cut. Hence there exists an $S \in \mathbb{K}$ such that $B = \{b \in \mathbb{K} \mid b < S\}$. We will show that S is the supremum

of A. Let $a \in A$ be arbitrary. Since A has no greatest element, there is a $b \in A$ such that $b > a$. Since $\{c \in \mathbb{K} \mid c < b\} \subseteq B$, we have $a \in B$ and so $a < S$. Let T be another upper bound of A and by way of contradiction suppose $T < S$. Then $T \in B$. Hence there exists an $a \in A$ such that $T \in \{c \in \mathbb{K} \mid c < a\}$, so $T < a$. This contradicts that T is an upper bound of A.

Now suppose $\mathbb{K}$ satisfies the least-upper-bound property. Let A be a Dedekind cut of A. Then A is clearly bounded above, so there exists a supremum S of A. We will prove that $A = \{a \in \mathbb{K} \mid a < S\}$. Let $a \in A$ be arbitrary. Because A has no greatest element, we have $S \notin A$. Hence $a < S$ because S is an upper bound of A. Now let $a \in \mathbb{K}$ with $a < S$ be arbitrary. Then a is not an upper bound of A, so there exists a $b \in A$ for which $b > a$. Because A is closed downwards we find $a \in A$. □

By Theorem 2.3.11 there exists an embedding from $\mathbb{Q}$ to $\mathbb{R}_D$. Even though we gave a constructive proof, it is practical to state the embedding explicitly. The embedding is given by $f : \mathbb{Q} \to \mathbb{R}_D$ defined by $f(q) = \{a \in \mathbb{Q} \mid a < q\}$. It can be readily verified f is indeed an embedding.

3.2 Cantor's construction

The next construction, usually attributed to Cantor[1], uses a certain sense of closeness of members of a sequence. In his own words [4]:

> [...] ich fordre, dass nach Annahme einer beliebig kleinen rationalen Zahl ϵ eine endliche Anzahl von Gliedern der Menge abgeschieden werden kann, so dass die übrig bleibenden paarweise einen Unterschied haben, der seiner absoluten Grösse nach kleiner ist als ϵ.
>
> *[...] I require that after assuming an arbitrarily small rational number ϵ, a finite number of members of the set can be separated so that the remaining pairs have a difference that is smaller in absolute size than ϵ.*

This notion of closeness may be familiar to the reader. Today sequences with this property are called Cauchy sequences. Cantor used these Cauchy sequences (or "Fundamentalreihe" as he called them) to construct the real numbers. See Figure 3.2 for an example of a Cauchy sequence[2].

With "absoluten Grösse" (absolute in size) Cantor meant that the sign of a number is unimportant; only its magnitude is. For this, we will introduce a new function.

Definition 3.2.1 (Absolute value function)**.** We define the absolute value function as the map $\mathbb{Q} \to \{q \in \mathbb{Q} \mid q \geq 0\}$ defined by

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

[1] It is actually due to Méray, who published his work three years earlier [22].

[2] Decimal expansions are also Cauchy sequences but are hard to define for irrational numbers without prior knowledge of them.

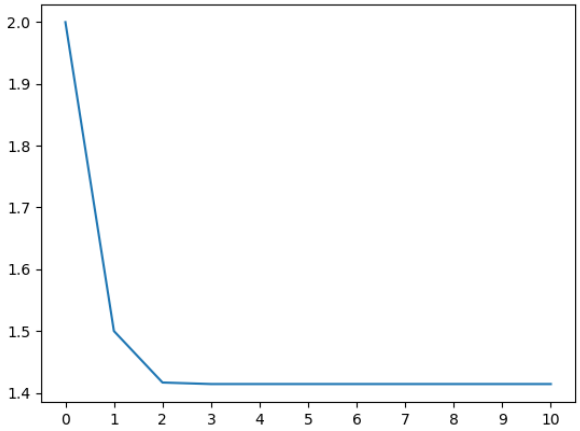

Figure 3.2: The Cauchy sequence $(q_n) : \mathbb{N} \to \mathbb{Q}$ defined by $q_0 = 2$ and $q_{n+1} = (q_n + 2/q_n)/2$

Cantor considered Cauchy sequences of rational numbers. For a given Cauchy sequence, he stated that "Der Reihe hat eine bestimmte Grenze b" (the sequence has a certain limit b) [5]. That is, since a Cauchy sequence is a sequence for which its values get closer and closer together, Cantor argued it must have a limit. These limits are precisely the real numbers. This however, is slightly inaccurate. To see why, we will now formally state what it means for a sequence to be Cauchy, and to have a limit (to converge).

Definition 3.2.2 (Cauchy sequence)**.** A sequence $(q_n) : \mathbb{N} \to \mathbb{Q}$ is Cauchy if

$$\forall \epsilon > 0_{\mathbb{Q}} \exists N \in \mathbb{N} \forall m \geq N \forall n \geq N (|q_m - q_n| < \epsilon).$$

Definition 3.2.3 (Convergent sequence)**.** A sequence $(q_n) : \mathbb{N} \to \mathbb{Q}$ is convergent if

$$\exists q \in \mathbb{Q} \forall \epsilon > 0_{\mathbb{Q}} \exists N \in \mathbb{N} \forall n \geq N (|q_n - q| < \epsilon),$$

in which case we write $q_n \to q$.

Crucially convergence of a rational sequence requires the existence of a rational number to which it converges; its limit. Cauchy sequences do not require this. But if every rational Cauchy sequence has a limit (it converges), it too must be a rational number. That is, we would not have constructed the real numbers at all. That must mean that not every rational Cauchy sequence converges. This is indeed the case. In particular, the Cauchy sequences that do not converge, reveal "holes" in the rational numbers. These holes are precisely the irrational numbers; the real numbers which are not rational. In particular, the Cauchy sequence from Figure 3.2 is not convergent.

Since the Cauchy sequences reveal the gaps in the rational numbers, the Cauchy sequences are what will represent the real numbers. Note that more than one Cauchy sequence can represent a single real number, though. A trivial case of this is when the first term in a sequence is changed to an arbitrary other

rational number. This will not affect the Cauchy property a sequence has. For this reason, we will have to define a relation on these Cauchy sequences and unify them in equivalence classes. We will do this as follows. Define the relation $\sim$ on $C_{\mathbb{Q}} := \{(q_n) \in \mathbb{Q}^{\mathbb{N}} \mid (q_n) \text{ is Cauchy}\}$ by

$$(p_n) \sim (q_n) \iff |p_n - q_n| \to 0. \tag{3.1}$$

Two Cauchy sequences are related when the sequence defined by the absolute value of their difference converges to 0. This allows us to unify the Cauchy sequences that approximate the same real number.

Lemma 3.2.4. *The relation $\sim$ as defined in Equation* (3.1) *is an equivalence relation.*

Proof. Reflexivity and symmetry follow quite directly. Transitivity follows from the triangle inequality, which we will assume the reader is familiar with. □

As such, we will now define the real numbers as the equivalence classes of $\sim$.

Definition 3.2.5 (Real numbers)**.** Define the set $\mathbb{R}_C$ of (Cantor) real numbers by $\mathbb{R}_C := C_{\mathbb{Q}}/\sim$.

Part of the elegance of this construction is that all operations work pointwise.

Definition 3.2.6 (Addition of real numbers)**.** Define addition as the map $\mathbb{R}_C \times \mathbb{R}_C \to \mathbb{R}_C$ defined by

$$[(p_n)] + [(q_n)] = [(p_n + q_n)].$$

Definition 3.2.7 (Multiplication of real numbers)**.** Define multiplication as the map $\mathbb{R}_C \times \mathbb{R}_C \to \mathbb{R}_C$ defined by

$$[(p_n)] \cdot [(q_n)] = [(p_n \cdot q_n)].$$

One should verify that both these functions are well-defined, and in particular that when (p_n) and (q_n) are Cauchy sequences, then so are $(p_n + q_n)$ and $(p_n \cdot q_n)$. Because the operations work pointwise, the properties of addition and multiplication are mostly immediate from their properties on $\mathbb{Q}$.

Proposition 3.2.8. $(\mathbb{R}_C, +, \cdot)$ *is a field.*

Proof. Most properties follow directly by the properties on the rational numbers as shown in Proposition 2.3.7. The additive identity is $0 := [(0)]$ as for any $[(q_n)] \in \mathbb{R}_C$ we have $[(q_n)] + [(0)] = [(q_n + 0)] = [(q_n)]$. The additive inverse is $-[(q_n)] := [(-q_n)]$ as $[(q_n)]+[(-q_n)] = [(q_n - q_n)] = [(0)] = 0$. The multiplicative identity is $1 := [(1)]$ as $[(q_n)] \cdot [(1)] = [(q_n \cdot 1)] = [(q_n)]$. We need to be a little bit careful for the the multiplicative inverse. We would want to say that it is $[(q_n)]^{-1} := [(q_n^{-1})]$. However, we might have that $q_n = 0$ for various $n \in \mathbb{N}$. Furthermore, (q_n^{-1}) might not be Cauchy for general (q_n). We will show that when $q_n \not\to 0$, there exists an $N \in \mathbb{N}$ such that for all $n \geq N$ we have $q_n \neq 0$, and moreover that (q_n^{-1}) is then Cauchy. Because $q_n \not\to 0$, there exists an $\epsilon > 0$ such that for all $m \in \mathbb{N}$ there exists an $n \geq m$ for which $|q_n| > \epsilon$. Because (q_n) is Cauchy, there exists an $N \in \mathbb{N}$ such that for all $m \geq N$ we have $|q_n - q_m| < \epsilon/2$. Then $-\epsilon/2 < q_n - q_m < \epsilon/2$ so that $-\epsilon/2 + q_m < q_n < \epsilon/2 + q_m$. Hence $\epsilon < |q_n| < \epsilon/2 + |q_m|$, so $|q_m| > \epsilon/2 > 0$. We will now show (q_n^{-1}) is

Cauchy. Like before, take $\epsilon > 0$ and for any $N \in \mathbb{N}$ take $n \geq N$ for which $|q_n| > \epsilon$. Because (q_n) is Cauchy, there exists an $N \in \mathbb{N}$ such that for $m \geq N$ we have $|q_m - q_n| < \epsilon \cdot \epsilon \cdot \epsilon$. Without loss of generality suppose $q_m > \epsilon$. Then $|1/q_m - 1/q_n| = |q_n - q_m|/|q_m \cdot q_n| < \epsilon \cdot \epsilon \cdot \epsilon/(\epsilon \cdot \epsilon) = \epsilon$. We conclude that for $[(q_n)] \neq 0$ we can thus pick a nonzero representative (q_n) to define $[(q_n)]^{-1} = [(q_n^{-1})]$. This is the inverse as $[(q_n)] \cdot [(q_n^{-1})] = [(q_n \cdot q_n^{-1})] = [(1)] = 1$. □

The order also works pointwise, but for the tail of the sequence. The first few terms of the sequence need not obey the order, it only matters how the sequence behaves after a certain point.

Definition 3.2.9 (Order on real numbers)**.** Define the order on $\mathbb{R}_C$ as $[(p_n)] \leq [(q_n)]$ if there exists an $N \in \mathbb{N}$ such that for all $n \geq N$ it is true that $p_n \leq q_n$.

That is, (p_n) is eventually smaller than (q_n). It can be checked that this is well-defined. Before proving $\mathbb{R}_C$ is an ordered field, we will give two more usual definitions.

Definition 3.2.10 (Maximum, minimum)**.** Let $(X, \leq)$ be a total order. Let $A \subseteq X$ be a subset of X. Then $M \in A$ is the maximum of A when $a \leq M$ for all $a \in A$, in which case we write $\max(A) = M$. Similarly $M \in A$ is the minimum when $M \leq a$ for all $a \in A$, in which case we write $\min(A) = M$.

Proposition 3.2.11. *$(\mathbb{R}_C, +, \cdot, \leq)$ is an ordered field.*

Proof. By Proposition 3.2.8 it remains to show $(\mathbb{R}_C, \leq)$ is a total order and that addition and multiplication behave nicely over the order.

Transitive. Suppose $[(p_n)] \leq [(q_n)]$ and $[(q_n)] \leq [(r_n)]$. Then there exists $N_1 \in \mathbb{N}$ such that $p_n \leq q_n$ for all $n > N_1$ and $N_2 \in \mathbb{N}$ such that $q_n \leq r_n$ for all $n > N_2$. Take $N = \max\{N_1, N_2\}$. Then for $n > N$ we have both $p_n \leq q_n$ and $q_n \leq r_n$. By transitivity of the order on rational numbers we have $p_n \leq r_n$.

Antisymmetric. Suppose $[(p_n)] \leq [(q_n)]$ and $[(q_n)] \leq [(p_n)]$. Then there exists an $N \in \mathbb{N}$ such that for all $n > N$ we have $p_n \leq q_n$ and $q_n \leq p_n$, so $p_n = q_n$.

Strongly connected. Suppose $[(p_n)] \neq [(q_n)]$. We need to show that $[(p_n)] < [(q_n)]$ or $[(p_n)] > [(q_n)]$. Since $[(p_n)] \neq [(q_n)]$ we have that there exists an $\epsilon > 0$ such that for all $N \in \mathbb{N}$ there exists $n \geq N$ for which $|p_n - q_n| \geq \epsilon$. Since (p_n) and (q_n) are Cauchy, there exists $N \in \mathbb{N}$ such that for all $m \geq N$ and $n \geq N$ we have both $|p_m - p_n| < \epsilon$ and $|q_m - q_n| < \epsilon$, so $p_n - \epsilon < p_m < p_n + \epsilon$ and $q_m - \epsilon < q_n < q_m + \epsilon$. For this N there exists an $n \geq N$ so that either $p_n - q_n \geq \epsilon$ or $p_n - q_n \geq -\epsilon$. In the first case we find for all $m \geq N$ that $p_m > p_n - \epsilon \geq q_n > q_m - \epsilon > q_m$. Hence $[(p_m)] \geq [(q_m)]$. The other case follows similarly.

OR1. Suppose $[(p_n)] \leq [(q_n)]$ and let $[(r_n)]$ be arbitrary. Then there exists an $N \in \mathbb{N}$ such that $p_n \leq q_n$ for all $n > N$. For this N we then also have $p_n + r_n \leq q_n + r_n$.

OR1. Suppose $[(p_n)] \leq [(q_n)]$ and $[(r_n)] \geq 0$. Then there exists an $N_1 \in \mathbb{N}$ such that $p_n \leq q_n$ for all $n > N_1$. There also exists an $N_2 \in \mathbb{N}$ such that $r_n \geq 0$ for all $n > N_2$. For $N = \max\{N_1, N_2\}$ we then have $p_n + r_n \leq q_n + r_n$.

□

We just showed that $\mathbb{R}_C$ is an ordered field. It is clear how the pointwise definitions of all operations made the proofs for the structure of $\mathbb{R}_C$ very simple. Thus far, $\mathbb{Q}$ has the same structure. However, like with the Dedekind real numbers being Dedekind-complete, we now expect that the Cantor real numbers are Cauchy-complete. That is, every real Cauchy sequence should also be a convergent sequence.

Proposition 3.2.12 ($\mathbb{R}_C$ is Cauchy-complete)**.** *Every real Cauchy sequence is a convergent sequence.*

Proof. Let $(x_n) : \mathbb{N} \to \mathbb{R}_C$ be a Cauchy sequence. Then for each $n \in \mathbb{N}$, the real number x_n is an equivalence class of sequences itself. That is, we have a sequence of equivalent classes of sequences. We are in the following situation.

$$\begin{aligned} x_0 &= [(x_{0,0}, x_{0,1}, x_{0,2}, x_{0,3}, x_{0,4}, \dots)] \\ x_1 &= [(x_{1,0}, x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}, \dots)] \\ x_2 &= [(x_{2,0}, x_{2,1}, x_{2,2}, x_{2,3}, x_{2,4}, \dots)] \\ x_3 &= [(x_{3,0}, x_{3,1}, x_{3,2}, x_{3,3}, x_{3,4}, \dots)] \\ x_4 &= [(x_{4,0}, x_{4,1}, x_{4,2}, x_{4,3}, x_{4,4}, \dots)] \\ &\vdots \end{aligned} \tag{3.2}$$

To show every Cauchy sequence is convergent, we need to find a candidate limit. This limit, being a real number, is then also an equivalence class of Cauchy sequences. We thus need to find a candidate Cauchy sequence. Before we do this, we need to pick the representatives more cleverly. Because we picked arbitrary representatives, we do not have any control over their convergence to show this. Using subsequences we can control the convergence rate with something uniform. Let $s_n = 1/n$. Since each $(x_{n,k})$ is Cauchy, there exists a $K \in \mathbb{N}$ such that for all $k \geq K$ and $l \geq K$ we have $|x_{n,k} - x_{n,l}| < s_n/6$. Hence we can take the subsequence $(x_{n,K+k})$ so that for all $k \in \mathbb{N}$ and $l \in \mathbb{N}$ we have $|x_{n,K+k} - x_{n,K+l}| < s_n/6$. Notice that $(x_{n,k}) \sim (x_{n,K+k})$, so from now on we will assume the representatives have the property that $|x_{n,k} - x_{n,l}| < s_n/6$ for all $k \in \mathbb{N}$ and $l \in \mathbb{N}$.

Since (x_n) is Cauchy, for every $i \in \mathbb{N}$ there is an $N_i \in \mathbb{N}$ such that for $m \geq N_i$ and $n \geq N_i$ we have

$$\begin{aligned} |x_m - x_n| &= |[(x_{m,0}, x_{m,1}, x_{m,2}, \dots)] - [(x_{n,0}, x_{n,1}, x_{n,2}, \dots)]| \\ &= |[(x_{m,0} - x_{n,0}, x_{m,1} - x_{n,1}, x_{m,2} - x_{n,2}, \dots)]| < s_i/6, \end{aligned}$$

so by unwinding Definition 3.2.9 there is a $K \in \mathbb{N}$ such that for $k \geq K$ we have $|x_{m,k} - x_{n,k}| < s_i/6$. Further note that we can take N_i so that $N_i > i$ and $N_{i+1} > N_i$ by taking N_i to be the maximum over $i + 1$ and $N_j + 1$ for all $j < i$. To remove the constraint on k, we let $m \in \mathbb{N}$ with $m \geq N_i$ and $n \in \mathbb{N}$ with $n \geq N_i$ be arbitrary and take K such that for $k \geq K$ we have $|x_{m,k} - x_{n,k}| < s_i/6$. Then for all $l \in \mathbb{N}$ we have

$$\begin{aligned} |x_{m,l} - x_{n,l}| &\leq |x_{m,l} - x_{m,k}| + |x_{m,k} - x_{n,k}| + |x_{n,k} - x_{n,l}| \\ &< s_m/6 + s_i/6 + s_n/6 \\ &< s_i/6 + s_i/6 + s_i/6 = s_i/2. \end{aligned}$$

Now we are ready to construct the candidate sequence. Define the sequence $(y_i) : \mathbb{N} \to \mathbb{Q}$ by $y_i = x_{N_i,N_i}$. Intuitively, these are diagonal elements in Equation (3.2) that are far enough down and to the right such that they are close enough to each other. We will show that (y_i) is Cauchy and in fact $x_n \to x$ for $x = [(y_i)]$. Let $k \in \mathbb{N}$ be arbitrary. Then for $i \geq k$ and $j \geq k$ we have

$$\begin{aligned} |y_i - y_j| &= |x_{N_i,N_i} - x_{N_j,N_j}| \\ &\leq |x_{N_i,N_i} - x_{N_i,N_j}| + |x_{N_i,N_j} - x_{N_j,N_j}| \\ &< s_{N_i}/2 + s_k/2 \\ &< s_k/2 + s_k/2 = s_k. \end{aligned}$$

So $|y_i - y_j| \to 0$ because $s_k \to 0$. We have now established that $x \in \mathbb{R}_C$. It remains to show that $x_n \to x$. Let $k \in \mathbb{N}$ be arbitrary. For $i \geq k$, $n \geq N_i$ and $l \geq N_i$ we have

$$\begin{aligned} |x_{n,l} - x_{N_l,N_l}| &\leq |x_{n,l} - x_{n,N_l}| + |x_{n,N_l} - x_{N_l,N_l}| \\ &< s_n/2 + s_k/2 \\ &\leq s_k/2 + s_k/2 = s_k. \end{aligned}$$

So

$$\begin{aligned} |x_n - x| &= |[(x_{n,0}, x_{n,1}, x_{n,2}, \dots)] - [(x_{N_0,N_0}, x_{N_1,N_1}, x_{N_2,N_2}, \dots)]| \\ &= |[(x_{n,0} - x_{N_0,N_0}, x_{n,1} - x_{N_1,N_1}, x_{n,2} - x_{N_2,N_2}, \dots)]| < s_k \end{aligned}$$

for large enough n. Hence $x_n \to x$. □

We thus have a set $\mathbb{R}_C$ that contains no holes in the sense of Cauchy-completeness. This coincides with the intuition we have for what the real numbers should be. One may wonder whether this completion achieves the same as the Dedekind-completion. It turns out that for general ordered fields this is not the case. That is, there exists ordered Cauchy-complete fields that are not Dedekind-complete. The missing requirement is the Archimedean property. We will prove the resulting equivalence in Section 3.4.

Definition 3.2.13 (Ordered Archimedean field)**.** Let $(\mathbb{K}, +, \cdot, \leq)$ be an ordered field. By Theorem 2.3.11 there exists a copy of $\mathbb{Q}$ in $\mathbb{K}$, so that we can think of $\mathbb{N}$ as a subset of $\mathbb{K}$. Then $\mathbb{K}$ is Archimedean if

$$\forall x \in \mathbb{K} \exists n \in \mathbb{N}(n > x).$$

This statement is sometimes also called the axiom of Archimedes.

Although attributed to Archimedes, it was Euclid who essentially stated the Archimedean property in *Elements*. He wrote the following in Definition 4 of Book V [12]:

> Λόγον ἔχειν πρὸς ἄλληλα μεγέθη λέγεται, ἃ δύναται πολλαπλασιαζόμενα ἀλλήλων ὑπερέχειν.
>
> *Magnitudes are said to have a ratio to one another which can, when multiplied, exceed one another.*

The Archimedean property is closely related to the (non)existence of infinite and infinitesimal numbers. A number is infinite if it is greater than any multiple of the multiplicative unit. A number is infinitesimal if no multiple of it exceeds the multiplicative unit. If a field is Archimedean, these elements do not exist. To align with our intuition, in order for the set $\mathbb{R}_C$ to adequately represent the real numbers, we must therefore show that $\mathbb{R}_C$ is Archimedean. We will have to use the construction of $\mathbb{R}_C$ as by the aforementioned equivalence just the field axioms and Cauchy-completeness are not enough. For this we will prove the Archimedean property for $\mathbb{Q}$ first.

Lemma 3.2.14. $(\mathbb{Q}, +, \cdot, \leq)$ *satisfies the Archimedean property.*

Proof. Let $q \in \mathbb{Q}$ be arbitrary. If $q < 0$ we can take $n = 0$. Suppose $q \geq 0$. Then $q = a/b$ for some $a \in \mathbb{N}$ and $b \in \mathbb{N} \setminus \{0\}$. Since $b \geq 1$ we have $q \leq b \cdot q = a$. Then $n = a + 1 > q$. □

To use this fact, we will need the explicit embedding of $\mathbb{Q}$ in $\mathbb{R}_C$. By Theorem 2.3.11 an embedding exists, but here we need it explicitly. The embedding is given by $f : \mathbb{Q} \to \mathbb{R}_C$ defined by $f(q) = [(q)]$. It can be readily verified f is indeed an embedding, and that it is the same embedding as in the above-mentioned theorem. We need one more lemma before we can prove the Archimedean property for $\mathbb{R}_C$.

Lemma 3.2.15. *For all $x = [(q_n)] \in \mathbb{R}_C$ there exists a $y \in \mathbb{Q}$ such that $y > x$.*

Proof. Because (q_n) is Cauchy, for all $\epsilon > 0$ there exists an $N \in \mathbb{N}$ such that for $m \geq N$ and $n \geq N$ we have $|q_m - q_n| < \epsilon$. We can make this hold for all $m \in \mathbb{N}$ and $n \in \mathbb{N}$ by taking the subsequence (q_{N+n}) and observing that $(q_n) \sim (q_{N+n})$. Then by taking $\epsilon = 1$ we find $q_m < q_0 + 1$ for all $m \in \mathbb{N}$. Hence $q_0 + 1 > x$, with $q_0 + 1 \in \mathbb{Q}$. □

The above proof can be modified to show that any Cauchy sequence is bounded, something we will use later. Now we prove that $\mathbb{R}_C$ is Archimedean.

Proposition 3.2.16. $(\mathbb{R}_C, +, \cdot, \leq)$ *is an ordered Cauchy-complete Archimedean field.*

Proof. We have that $(\mathbb{R}_C, +, \cdot, \leq)$ is an ordered field by Proposition 3.2.11. By Proposition 3.2.12 it is Cauchy-complete. It remains to show the Archimedean property. Let $x = [(q_n)] \in \mathbb{R}_C$ be arbitrary. Then (q_n) is bounded by Lemma 3.2.15 so we can let M be a rational upper bound of (q_n). Define $y = [(M)]$. Then $y \in \mathbb{Q}$ by the embedding of $\mathbb{Q}$ in $\mathbb{R}_C$, and $y \geq x$. By Lemma 3.2.14 there is an $n \in \mathbb{N}$ such that $n > y$, so we conclude $n > y \geq x$. □

3.3 Schanuel's construction

While Cantor and Dedekind pioneered in rigorously defining the real numbers, to this day mathematicians are still trying to invent new ways to define them. One quite recent construction in particular sparked the interest of many mathematicians. This is the construction by Schanuel, developed in the 1980s. Sadly he never published his work. Instead he told other mathematicians about it, who went on to publish it. One of these publications is by Street [29]. We

will follow the work of A'Campo [1], who independently rediscovered it. Some proofs are omitted, these can be found in [1].

Having (supposedly) constructed the real numbers in the previous two constructions, for this construction we will assume some knowledge about the real numbers. Schanuel noticed that there exists a trivial correspondence between any real number $a \in \mathbb{R}$ and the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = a \cdot x$. Here the coefficient a is called the slope of f. To construct the real numbers, Schanuel's idea was to approximate f by restricting the domain and codomain of f to $\mathbb{Z}$. There are however multiple ways to do this, the approximations are not unique. See Figure 3.3 for a few examples.

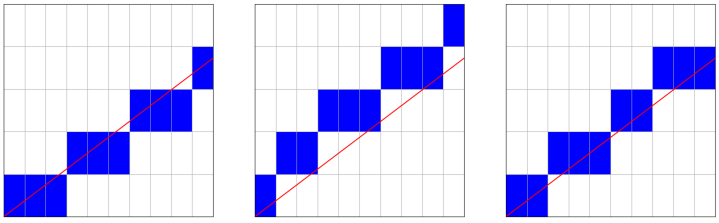

Figure 3.3: A linear function and three of its approximations

Whichever two reasonable approximations one chooses, the following should hold [26].

- When their underlying functions are equal, their difference should be bounded. That is, no two approximations of the same function can differ too much.
- When their underlying function are unequal, their difference should be unbounded. That is, two approximations should differ arbitrarily much when the underlying functions are unequal.

This induces an equivalence relation on the approximations of functions. Two approximations are regarded the same when their difference is bounded. We will now convert this intuition to mathematical statements. Recall from Definition 2.1.18 that a homomorphism f preserves addition, that is $f(a + b) = f(a) + f(b)$.

Definition 3.3.1 (Almost homomorphism)**.** A function $f : \mathbb{Z} \to \mathbb{Z}$ is an almost homomorphism if $\{f(a + b) - f(a) - f(b) \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}$ is bounded.

Definition 3.3.2 (Almost equal)**.** Almost homomorphisms $f : \mathbb{Z} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Z}$ are almost equal if $\{f(a) - g(a) \mid a \in \mathbb{Z}\}$ is bounded.

A function being an almost homomorphism means that it is a reasonable approximation of a linear function. It is almost linear. In particular, we measure the almostness of an almost homomorphism by $S_f = \max\{|f(a+b)-f(a)-f(b)| \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}$.

Note that A'Campo used different, but equivalent, definitions for almost homomorphisms and almost equality. He required that instead of bounded, the sets are finite. While this can be shown to be equivalent, we have not

defined finiteness of sets. To avoid this additional overhead we have stated the definitions in terms of boundedness.

This construction has also been given the name "Eudoxus real numbers", for example by Arthan in [2]. This is because they can be interpreted within the theory of proportions by Eudoxus. More specifically Definition 5 in Book 5 of Euclid's *Elements* gives rise to this construction. This is precisely the definition that gave rise to the Dedekind real numbers too. See [2] for the details regarding this. We will call them the Schanuel real numbers like we have done for the Dedekind and Cantor real numbers.

We will now mathematically state the relation on the almost homomorphisms. Define the relation $\sim$ on

$$\mathrm{AEnd}(\mathbb{Z}) := \{f \in \mathbb{Z}^{\mathbb{Z}} \mid f \text{ is an almost homomorphism}\}$$

by

$$f \sim g \iff f \text{ and } g \text{ are almost equal.} \tag{3.3}$$

Lemma 3.3.3. *The relation $\sim$ as defined in Equation* (3.3) *is an equivalence relation.*

Proof. Reflexivity is clear as the set $\{0\}$ is definitely bounded. Symmetry follows as any bound for $\{f(a) - g(b) \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}$ will also work for $\{-(f(a) - g(b)) \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}$. For transitivity, suppose $f \sim g$ and $g \sim h$. Define $A = \{f(a) - g(b) \mid a \in A \wedge b \in \mathbb{Z}\}$, $B = \{g(b) - h(c) \mid b \in \mathbb{Z} \wedge c \in \mathbb{Z}\}$ and $C = \{f(a) - h(c) \mid a \in \mathbb{Z} \wedge c \in \mathbb{Z}\}$. Then $C = A + B$. Since A and B are bounded, there exists an $M \in \mathbb{N}$ such that for all $a \in A$ we have $|a| \leq M$ and similarly an $N \in \mathbb{N}$ such that for all $b \in B$ we have $|b| \leq N$. Since $|a+b| \leq |a| + |b| \leq M + N$ we have that C is bounded. □

Definition 3.3.4 (Real numbers)**.** Define the set $\mathbb{R}_S$ of (Schanuel) real numbers by $\mathbb{R}_S := \mathrm{AEnd}(\mathbb{Z})/\sim$.

Definition 3.3.5 (Addition of real numbers)**.** Define addition as the map $\mathbb{R}_S \times \mathbb{R}_S \to \mathbb{R}_S$ defined by

$$[f] + [g] = [f + g].$$

It follows that $f + g$ is an almost homomorphism by the proof of transitivity of $\sim$. One should check that this operation is independent of the representative.

Proposition 3.3.6. $(\mathbb{R}_S, +)$ *is an abelian group.*

Proof. Because addition works pointwise, all properties follow directly by Proposition 2.2.5. The identity is the zero function $0 : \mathbb{Z} \to \mathbb{Z}$. The inverse of $[f] \in \mathbb{R}_S$ is given by $-[f] := [-f]$. □

Definition 3.3.7 (Multiplication of real numbers)**.** Define multiplication as the map $\mathbb{R}_S \times \mathbb{R}_S \to \mathbb{R}_S$ defined by

$$[f] \cdot [g] = [f \circ g].$$

One should verify that the composition of two almost homomorphisms is again an almost homomorphism, and that the resulting equivalence class is independent of the chosen representatives.

Next we will define the order on $\mathbb{R}_S$. For this, we will induce an order based on classifying the positive real numbers. Notice that linear functions that have a positive slope, also have a positive function value for $x > 0$. This can be translated to almost homomorphisms in terms of boundedness.

Definition 3.3.8 (Order on real numbers)**.** Say $[f] > 0$ when $f(\mathbb{N}) \cap \mathbb{N}$ is unbounded. Define the order on $\mathbb{R}_S$ as $[f] \leq [g]$ if $[f] = [g]$ or there exists a positive $[h] \in \mathbb{R}_S$ such that $[f] + [h] = [g]$.

One can verify that positivity of $[f]$ is independent of the representative. We have now defined all operations on the real $\mathbb{R}_S$. Before we show that these operations define an ordered field, we will establish a useful representation of the real numbers.

Definition 3.3.9 (Odd function)**.** A function $f : \mathbb{Z} \to \mathbb{Z}$ is odd when $f(-a) = -f(a)$ for all $a \in \mathbb{Z}$.

Lemma 3.3.10. *Every almost homomorphism is equivalent to an odd almost homomorphism.*

Proof. Let $f : \mathbb{Z} \to \mathbb{Z}$ be an almost homomorphism. Define $g : \mathbb{Z} \to \mathbb{Z}$ by $g(0) = 0$, $g(a) = f(a)$ for $a > 0$ and $g(a) = -f(-a)$ for $a < 0$. Then g is an almost homomorphism and odd. We also have $f \sim g$ as for $a > 0$ we have $f(a) - g(a) = f(a) - f(a) = 0$. Because f is an almost homomorphism, for $a < 0$ we have that $|f(a) + f(-a) - f(0)| \leq M$ for some $M \in \mathbb{N}$. Hence $|f(a) + f(-a)|$ is bounded. □

By Lemma 3.3.10 it follows that for a function $f : \mathbb{Z} \to \mathbb{Z}$ it suffices to show that $\{f(a+b) - f(a) - f(b) \mid a \in \mathbb{N} \wedge b \in \mathbb{N}\}$ is bounded to show it is an almost homomorphism. This lemma can be used to go one step further.

Definition 3.3.11 (Well-adjusted almost homomorphism)**.** An almost homomorphism $f : \mathbb{Z} \to \mathbb{Z}$ is well-adjusted if $|f(a+b) - f(a) - f(b)| \leq 1$ for all $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$.

Lemma 3.3.12 (Concentration lemma, Lemma 4 in [1])**.** *Every almost homomorphism is equivalent to a well-adjusted almost homomorphism.*

Using this lemma, one can obtain the following properties. Let $[f] \in \mathbb{R}_S$ be arbitrary. Assume f is well-adjusted.

(a) For all $a \in \mathbb{Z}$ we have $(|f(a+1) - f(a)| \leq |f(1)| + 1)$.

(b) We have $[f] > 0$ if and only if there exists an $a \in \mathbb{Z}$ such that $f(a) > 1$.

From this lemma, the following result can be proven.

Lemma 3.3.13 (Lemma 5 in [1])**.** *Let $f : \mathbb{Z} \to \mathbb{Z}$ be an almost homomorphism. If $f(\mathbb{Z})$ is unbounded then there exists $b \geq 0$ and $B \geq 0$ such that the following properties hold.*

$$\forall a \in \mathbb{Z} \forall n \in \mathbb{N}(|f(a+n) - f(a)| \leq n \cdot b),$$
$$\forall a \in \mathbb{Z} \forall n \in \mathbb{N}(|f(a + n \cdot B) - f(a)| \geq n).$$

Additionally for all $b \in \mathbb{Z}$ we have $f(a) = b$ for at most $2 \cdot B - 1$ different values of a.

With this, we are in good shape to prove that $\mathbb{R}_S$ is an ordered field.

Proposition 3.3.14. *$(\mathbb{R}_S, +, \cdot, \leq)$ is an ordered field.*

Proof. By Proposition 3.3.6 we have that $(\mathbb{R}_S, +, \cdot)$ is an abelian group. It remains to show that $(\mathbb{R}_S, +, \cdot)$ is a field, that $(\mathbb{R}_S, \leq)$ is a total order and that the order is preserved under addition and multiplication. Associativity of $\cdot$ follows because function composition is associative. We define the multiplicative identity as $1 := [\mathrm{i}]$ where $\mathrm{i} : \mathbb{Z} \to \mathbb{Z}$ is the identity function. Then for all $[f] \in \mathbb{R}_S$ we have $[f] \cdot [i] = [f \circ \mathrm{i}] = [f]$.

Commutative. Let $[f] \in \mathbb{R}_S$ and $[g] \in \mathbb{R}_S$ be arbitrary. Because the almostness of the almost homomorphisms f and g is bound by S_f and S_g respectively, we obtain the following estimate.

$$a \cdot f(g(a)) = f(a \cdot g(a)) + E_1 = f(g(a) \cdot a) + E_1 = g(a) \cdot f(a) + E_2 + E_1,$$

where $|E_1| \leq |a|S_f$ and $|E_2| \leq |g(a)|S_f \leq |a|(|g(1)|+S_g)S_f$. By symmetry we obtain a similar estimate for $a \cdot g(f(a))$. We find

$$\begin{aligned} |a \cdot f(g(a)) - a \cdot g(f(a))| &= |g(a) \cdot f(a) + E_2 + E_1 - f(a) \cdot g(a) - E_4 - E_3| \\ &= |E_2 + E_1 - E_4 - E_3| \\ &\leq |a|\big((|g(1)| + S_g)S_f + S_f \\ &\quad + (|f(1)| + S_f)S_g + S_g\big) \end{aligned}$$

and so

$$|f(g(a)) - g(f(a))| \leq S_f(|g(1)| + S_g + 1) + S_g(|f(1)| + S_f + 1).$$

We conclude $f \circ g$ and $g \circ f$ are equivalent, and hence $[f] \cdot [g] = [g] \cdot [f]$.

Inverse. Let $[f] \in \mathbb{R}_S$ with $[f] \neq 0$ be arbitrary. By commutativity it suffices to find a right inverse for $[f]$. That is, an almost homomorphism g such that $f \circ g \sim \mathrm{i}$. By Lemma 3.3.12 we can assume f is well-adjusted. For any $m \in \mathbb{Z}$ we can therefore find $n_m \in \mathbb{Z}$ for which $|m - f(n_m)| \leq |f(1)| + 1$. By well-ordering of $\mathbb{N}$ we can take n_m for which $|n_m|$ is least, and $n_m > 0$ when two different integers attain this minimum. This allows us to define the map $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(m) = n_m$. We will prove that g is the right inverse of f. We will first have to prove g is an almost homomorphism. We have

$$\begin{aligned} |f(g(a+b) - g(a) - g(b))| &= f(n_{a+b} - n_a - n_b) \\ &\leq |(a+b) - a - b| + 2 + 3(|f(1)| + 1) \\ &= 3|f(1)| + 5. \end{aligned}$$

Since $f(\mathbb{Z})$ is unbounded, it then follows by Lemma 3.3.13 that $\{g(a+b) - g(a) - g(b) \mid a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}$ is bounded. We further have $\mathrm{i} \sim f \circ g$ since $|m - f(g(m))| = |m - f(n_m)| \leq |f(1)| + 1$, so $\{i(m) - f(g(m)) \mid m \in \mathbb{Z}\}$ is bounded. We conclude $[f] \cdot [g] = 1$.

Distributive. Let $[f] \in \mathbb{R}_S$, $[g] \in \mathbb{R}_S$ and $[h] \in \mathbb{R}_S$ be arbitrary. Then $[f] \cdot ([g] + [h]) = [(g + h) \circ f] = [g \circ f] + [h \circ f] = [f \circ g] + [f \circ h]$.

Transitive. Suppose $[f] \leq [g]$ and $[g] \leq [h]$, that is $[g-f] \geq 0$ and $h-g \geq 0$. We need to show that $[h-f] \geq 0$. If $f \sim g$ or $g \sim h$ then the result trivially follows. We may assume that $g-f$ and $h-g$ are well-adjusted. Since $[g-f] > 0$ there exists $m \in \mathbb{N} \setminus \{0\}$ and $n \in \mathbb{N} \setminus \{0\}$ for which $g(m) - f(m) > 1$ and $h(n) - g(n) > 1$. Then $m \cdot n \geq m$ and $m \cdot n \geq n$ so that $h(m \cdot n) - f(m \cdot n) > 2$. Hence $[h-f] > 0$.

Antisymmetric. Suppose $[f] \leq [g]$ and $[g] \leq [f]$. If $[f] = [g]$ we are done. Else there exists positive $[h_1] \in \mathbb{R}_S$ and $[h_2] \in \mathbb{R}_S$ such that $[f + h_1] = [g]$ and $[g + h_2] = [f]$. Then $[g + h_2 + h_1] = [g]$, so $[h_1] = -[h_2]$. This must mean $[h_1] = [h_2] = 0$ as otherwise either $[h_1]$ or $[h_2]$ would be negative. Hence $[f] = [g]$.

Strongly connected. Let $[f] \in \mathbb{R}_S$ and $[g] \in \mathbb{R}_S$ be arbitrary. Assume $f-g$ is well-adjusted. If $f(a) - g(a) \in \{-1, 0, 1\}$ for all $a \in \mathbb{Z}$, then $f = g$. If not, then by the contrapositive there exists $a \in \mathbb{Z}$ for which $f(a) - g(a) < -1$ or $f(a) - g(a) > 1$. If $f(a) - g(a) < -1$ then $g(a) - f(a) > 1$, so $g - f > 0$. If $f(a) - g(a) > 1$ then $f - g > 0$.

OR1. Let $[f] \in \mathbb{R}_S$, $[g] \in \mathbb{R}_S$ and $[h] \in \mathbb{R}_S$ be arbitrary. If $[f] = [g]$ the result follows trivially. Suppose $[f] < [g]$. Then there exists a positive $[j] \in \mathbb{R}_S$ so that $[f] + [j] = [g]$. Then $[f] + [h] + [j] = [g] + [h]$, so $[f] + [h] < [g] + [h]$.

OR2. Let $[f] \in \mathbb{R}_S$, $[g] \in \mathbb{R}_S$ and $[h] \in \mathbb{R}_S$ with $[h] > 0$ be arbitrary. If $[f] = [g]$ the result follows trivially. Else there exists a positive $[j] \in \mathbb{R}_S$ such that $[f] + [j] = [g]$. Hence $[f] \cdot [h] + [j] \cdot [h] = [g] \cdot [h]$ by distributivity. Since $[j] \cdot [h] > 0$, we find $[f] \cdot [h] < [g] \cdot [h]$.

□

Since this construction did not give rise to a natural new notion of completeness, A'Campo proved that $\mathbb{R}_S$ is Dedekind-complete. In particular, he proved the equivalent statement to Dedekind-completeness formulated in Proposition 3.1.14. That is, each bounded above subset of $\mathbb{R}_S$ has a supremum.

Proposition 3.3.15. *$(\mathbb{R}_S, +, \cdot, \leq)$ is an ordered Dedekind-complete field.*

See [1] for the proof. Note that we have skipped over the rational numbers. Since they are still useful to know, we want to define them anyways. Therefore instead of defining an embedding, we will extract the rational numbers from the real numbers. Note that for integers a and b, the rational number "a/b" is the solution of $b \cdot x = a$.

Definition 3.3.16 (Rational numbers)**.** Define the rational numbers $\mathbb{Q}_{\mathbb{R}_S}$ by

$$\{[f] \in \mathbb{R}_S \mid \exists a \in \mathbb{Z} \exists b \in \mathbb{N} \setminus \{0\} \forall c \in \mathbb{Z}(f(c) = \min\{n \in \mathbb{N} \mid b \cdot n \geq a \cdot c\})\},$$

where f is extended oddly.

It can be shown that $\mathbb{Q}_{\mathbb{R}_S}$ is isomorphic to $\mathbb{Q}$. The isomorphism would be $f : \mathbb{Q} \to \mathbb{Q}_{\mathbb{R}_S}$ given by

$$f(a/b) = [(g : \mathbb{Z} \to \mathbb{Z}, g(c) = \min\{n \in \mathbb{N} \mid b \cdot n \geq a \cdot c\})].$$

This defines the rational numbers explicitly. Note that we already knew that the rational numbers exist in $\mathbb{R}_S$ by Theorem 2.3.11.

3.4 Uniqueness of $\mathbb{R}$

We have constructed three sets we all called the real numbers: $\mathbb{R}_D$, $\mathbb{R}_C$ and $\mathbb{R}_S$. Since we gave them the same name, it would also be favourable that they are the same mathematically. To do that, we will show that the properties each construction has are interchangeable, so that each set satisfies all the same properties. After that, we will show that any set that has these properties, is essentially the same set. This proves the structural equality of our three sets, and the uniqueness of the real numbers in general.

We asserted earlier that Cauchy-completeness is a weaker property than Dedekind-completeness. The missing requirement is the Archimedean property. We will now prove this.

Theorem 3.4.1. *Let $\mathbb{K}$ be an ordered field. Then $\mathbb{K}$ is a Cauchy-complete Archimedean field if and only if $\mathbb{K}$ is a Dedekind-complete field.*

Proof. For the forward direction suppose $\mathbb{K}$ is an ordered Cauchy-complete Archimedean field. Let A be a Dedekind cut of $\mathbb{K}$. We want to construct a Cauchy sequence that approaches the cutting point of A. Since the sequence is then convergent by Cauchy-completeness, we can prove the Dedekind cut A is then produced by some $x \in \mathbb{K}$, where x is the limit of the sequence.

Start by taking $x_0 = a$ for any $a \in A$. For $n \in \mathbb{N}$ define $x_{n+1} = x_n + k/2^n$ where k is the largest $k \in \mathbb{N}$ for which $x_n + k/2^n \in A$. We can do this as by the Archimedean property there exists a l such that $x_n + l/2^n$ is larger than any $b \in \mathbb{K} \setminus A$. By the well-ordering of $\mathbb{N}$ we can then take the minimal $k+1$ for which $x_n + (k+1)/2^n$ is in $\mathbb{K} \setminus A$ and less than or equal to $x_n + l/2^n$. Then k is the largest $k \in \mathbb{N}$ such that $x_n + k/2^n \in A$.

To see that (x_n) is Cauchy, by way of contradiction suppose for $m \leq n$ that $x_n > x_m + 1/2^{m-1}$. Since $x_n \in A$, we also have $x_m + 1/2^{m-1} \in A$. But that means $x_m + 1/2^{m-1} = x_{m-1} + (k_{m-1}+1)/2^{m-1} \in A$, violating maximality of k_{m-1}. Hence $|x_m - x_n| \leq 1/2^{m-1}$, so (x_n) is Cauchy. Therefore $x_n \to x$ for some $x \in \mathbb{K}$. We claim that A is the Dedekind cut produced by x; that is $A = \{a \in \mathbb{K} \mid a < x\}$. We will first show $\{a \in \mathbb{K} \mid a < x\} \subseteq A$ by contrapositive. Suppose $a \notin A$. Then $a \geq x_n$ for all $n \in \mathbb{N}$. Hence $a \geq x$. To show $A \subseteq \{a \in \mathbb{K} \mid a < x\}$, let $a \in A$ be arbitrary and by way of contradiction suppose $a \geq x$. Then $a \geq x \geq x_n$ for all $n \in \mathbb{N}$. Since A contains no greatest element, there is a $b \in A$ such that $b > a$. Then by the Archimedean property we can find an $n \in \mathbb{N}$ for which $a + 1/2^n < b$. Since $x_{n+1} + 1/2^n \notin A$ we have $b < x_{n+1} + 1/2^n$ so that $b - 1/2^n < x_{n+1} \leq a$, a contradiction. We conclude $\mathbb{K}$ is Dedekind-complete.

For the converse suppose $\mathbb{K}$ is an ordered Dedekind-complete field. To prove $\mathbb{K}$ is Archimedean, by way of contradiction suppose there exists an $x \in \mathbb{K}$ such that for all $n \in \mathbb{N}$ we have $n < x$. Then $\mathbb{N}$ is bounded above by x, so by Proposition 3.1.14 there exists a supremum S of $\mathbb{N}$. Then $S - 1$ is not an upper bound, so there exists an $m \in \mathbb{N}$ such that $m > S - 1$, hence $S < m + 1$. But $m + 1 \in \mathbb{N}$, contradicting that S is an upper bound. Hence $\mathbb{K}$ is Archimedean.

Next, let $(x_n) : \mathbb{N} \to \mathbb{K}$ be a Cauchy sequence. To show (x_n) is convergent we need to find a candidate limit. Because we have Dedekind-completeness, perhaps a natural idea is to consider the suprema of the elements of (x_n). For all $n \in \mathbb{N}$ define $A_n = \{x_m \in \mathbb{K} \mid m \geq n\}$. Since A_n is bounded because Cauchy sequences are, by Proposition 3.1.14 it has a supremum S_n. Then (S_n) is a

bounded decreasing sequence. We will prove (S_n) is convergent. Notice that $(-S_n)$ is a bounded increasing sequence, so that we can define $-S$ to be the supremum of $\{-S_n \in \mathbb{K} \mid n \in \mathbb{N}\}$. Then since $-S$ is the supremum, for every $\epsilon > 0$ there exists an $N \in \mathbb{N}$ such that $-S_N > -S - \epsilon$. Now because $(-S_N)$ is increasing, for $n \geq N$ we have

$$|-S-(-S_n)| = -S-(-S_n) \leq -S-(-S_N) < \epsilon.$$

We conclude $-S_n \to -S$ and therefore also $S_n \to S$. Define $B_n = \{-x_m \in \mathbb{K} \mid m \geq n\}$. Since B_n is also bounded, it has a supremum T_n. By a similar argument $T_n \to T$ where T is the supremum of $\{T_n \in \mathbb{K} \mid n \in \mathbb{N}\}$. We will show $S = T$. Let $\epsilon > 0$ be arbitrary. Take $N \in \mathbb{N}$ to be maximum of the N necessary for the Cauchy property, such that $S_N > S - \epsilon$ and such that $T_N < T + \epsilon$. Then

$$\begin{aligned} |S-T| &= |S - S_N + S_N + T_N - T_N - T| \\ &\leq |S-S_N| + |S_N - T_N| + |T - T_N| \\ &< \epsilon + \epsilon + \epsilon = 3\epsilon. \end{aligned}$$

Since this holds for all $\epsilon > 0$, we must have $S = T$. We will now show $x_n \to S$. Let $\epsilon > 0$ be arbitrary. Take $N \in \mathbb{N}$ such that for $n \geq N$ we have $x_n > S - \epsilon$ and $x_n < S + \epsilon$. Then $S - \epsilon < x_n < S + \epsilon$, so

$$-\epsilon < x_n - S < \epsilon \implies |x_n - S| < \epsilon.$$

We conclude $x_n \to S$. □

We conclude by the above theorem, and by Propositions 3.1.10, 3.2.16 and 3.3.15 that all of $\mathbb{R}_D$, $\mathbb{R}_C$ and $\mathbb{R}_S$ are Dedekind-complete, Cauchy-complete and satisfy the Archimedean property. We will now show that any ordered field with these properties is essentially the same field. Like we have done thus far, we want to reuse the definition of the function φ we used in the proof of Theorem 2.3.11. There we were able to induce a definition for φ for the integers based on the natural numbers, and for the rational numbers based on the integers. However, it is not immediately clear how one would induce a definition for the real numbers based on the rational numbers.

We saw that Cauchy sequences allowed us to expose the real numbers from the rational numbers. Given that real Cauchy sequences are now also convergent, perhaps we can define φ for the real numbers by constructing rational sequences that converge to the real numbers. The image of the sequence under φ would then also be a rational sequence. We would then want this image sequence to converge as well, so to induce a definition for the real numbers. We want this to be the case in the codomain of φ as well. That is, now that we can define φ for the real numbers, we want to be sure that with this we can reach all numbers in the codomain. Informally put, we want to be able to approximate the values in the codomain by the rational numbers that exist in the codomain. The following proposition assures that this is the case for any Archimedean field.

Proposition 3.4.2 ($\mathbb{Q}$ is dense in any ordered Archimedean field)**.** *Let $(R, +, \cdot, \leq)$ be an ordered Archimedean field. By Theorem 2.3.11 there exists a copy of $\mathbb{Q}$ in R. Then for any $x \in R$ and $y \in R$ with $x < y$ there exists a $q \in \mathbb{Q}$ such that $x < q < y$.*

Proof. By the Archimedean property there exists an $n \in \mathbb{N}$ such that $n > 1/(y-x)$. Rewriting yields $n \cdot x + 1 < n \cdot y$. It can be verified that again by the Archimedean property, along with the well-ordering of $\mathbb{N}$, there exists a minimal $m \in \mathbb{Z}$ such that $n \cdot x < m$. Because this m is minimal, we have $m-1 \leq n \cdot x < m$. Thus $n \cdot x < m \leq n \cdot x + 1 < n \cdot y$. We conclude $n \cdot x < m < n \cdot y$ so that $x < m/n < y$. □

With this, we can now turn to proving the uniqueness of the real numbers. It was Huntington who in 1903 first characterised the real numbers using a set of properties they should satisfy [13]. We will state the uniqueness in terms of Cauchy-completeness and the Archimedean property. We will do this because we will use Proposition 3.4.2 and Cauchy-completeness intensively. Of course, by Theorem 3.4.1 this can be equivalently stated in terms of Dedekind-completeness.

Theorem 3.4.3 (Uniqueness of $\mathbb{R}$)**.** $(\mathbb{R}, +, \cdot, \leq)$ *is the unique ordered Cauchy-complete Archimedean field.*

Proof. Let $\mathbb{R}_C$ be the Cantor real numbers. Let R be an ordered Cauchy-complete Archimedean field. We will start to define $\varphi : \mathbb{R}_C \to R$ as in the proof of Theorem 2.3.11. Briefly put, define $\varphi(0_{\mathbb{R}_C}) = 0_R$ and $\varphi(q + 1_{\mathbb{R}_C}) = \varphi(q) + 1_R$. We then extended this to the integers by $\varphi(-q) = -\varphi(q)$. In the same way we extended φ to the rational numbers by $\varphi(p \cdot q^{-1}) = \varphi(p) \cdot \varphi(q)^{-1}$. This yielded an ordered field isomorphism with respect to rational number addition, multiplication and order. To extend φ to all of its domain, we will extend φ using sequences. Notice that $\varphi(\mathbb{Q})$ is isomorphic to $\mathbb{Q}$ by Theorem 2.3.11. Let $(x_n) : \mathbb{N} \to \mathbb{Q}$ be a Cauchy (hence convergent) sequence, so $x_n \to x$ for some $x \in \mathbb{R}_C$. We will show $(\varphi(x_n))$ is Cauchy too. Let $\epsilon > 0_{\mathbb{Q}}$ be arbitrary. Because (x_n) is Cauchy, we can take N such that for all $m \geq N$ and $n \geq N$ we have $|x_m - x_n| < \varphi^{-1}(\epsilon)$. Then $-\varphi^{-1}(\epsilon) < x_m - x_n < \varphi^{-1}(\epsilon)$ so that $-\epsilon < \varphi(x_m) - \varphi(x_n) < \epsilon$ because φ is an ordered field isomorphism on $\mathbb{Q}$. Hence $|\varphi(x_m) - \varphi(x_n)| < \epsilon$. We conclude $(\varphi(x_n))$ as a function $\mathbb{N} \to \mathbb{Q}$ is Cauchy. It remains to verify it is Cauchy as a function $\mathbb{N} \to R$ as well. For this we use that $\mathbb{Q}$ is dense in R by Proposition 3.4.2. Then for any $\epsilon > 0_R$ we can find a smaller positive $\epsilon \in \mathbb{Q}$, proving $(\varphi(x_n))$ is Cauchy as a function $\mathbb{N} \to R$. We therefore have $\varphi(x_n) \to y$ for some $y \in R$. We define $\varphi(x) = y$. Since every real number can be approximated by rational Cauchy sequences, this defines φ for all real numbers. One should verify this extension is well-defined. That is, the mapping of φ should be independent of the sequence chosen. This follows by showing that when $x_n \to 0_{\mathbb{R}_C}$ we also have $\varphi(x_n) \to 0_R$. As this follows reasoning identical to what we did above, we will not do it again. We will turn to showing that φ defines an ordered field isomorphism.

Field homomorphism. Clearly $\varphi(0_{\mathbb{R}_C}) = 0_R$ and $\varphi(1_{\mathbb{R}_C}) = 1_R$. Let $x \in \mathbb{R}_C$ and $y \in \mathbb{R}_C$ be arbitrary. There exists rational sequences $(x_n) : \mathbb{N} \to \mathbb{Q}$ and $(y_n) : \mathbb{N} \to \mathbb{Q}$ such that $x_n \to x$ and $y_n \to y$. Then $\varphi(x_n + y_n) \to \varphi(x+y)$ and $\varphi(x_n + y_n) = \varphi(x_n) + \varphi(y_n) \to x + y$. Since limits are unique, we have $\varphi(x + y) = \varphi(x) + \varphi(y)$.

Similarly $\varphi(x_n \cdot y_n) \to \varphi(x \cdot y)$ and $\varphi(x_n \cdot y_n) = \varphi(x_n) \cdot \varphi(y_n) \to \varphi(x) \cdot \varphi(y)$. Hence $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

Injective. Injectivity follows from the fact that φ is a field homomorphism. Indeed, suppose $\varphi(x) = \varphi(y)$ for some $x \in \mathbb{R}_C$ and $y \in \mathbb{R}_C$. We want to show that $x = y$. We have $\varphi(x - y) = 0_R$. Let $z = x - y$. By way of contradiction, suppose $z \neq 0_{\mathbb{R}_C}$. Then $\varphi(z) \cdot \varphi(z^{-1}) = \varphi(1_{\mathbb{R}_C}) = 1_R$. Since $\varphi(z) = 0_R$ it follows that $0_R \cdot \varphi(z^{-1}) = 1_R$, a contradiction.

Order homomorphism. Let $x \in \mathbb{R}_C$ and $y \in \mathbb{R}_C$ with $x \leq y$ be arbitrary. There exists rational Cauchy sequences $(x_n) : \mathbb{N} \to \mathbb{Q}$ and $(y_n) : \mathbb{N} \to \mathbb{Q}$ such that $x_n \to x$, $y_n \to y$ and additionally with the property that $x_n \leq y_n$ for all $n \in \mathbb{N}$. Then $\varphi(x_n) \leq \varphi(y_n)$ for all $n \in \mathbb{N}$ so that $\varphi(x) \leq \varphi(y)$.

Surjective. Let $y \in R$ be arbitrary. We will prove there exists a sequence $(y_n) : \mathbb{N} \to \mathbb{Q}$ such that $y_n \to y$. Because $\mathbb{Q}$ is dense in R, for all $n \in \mathbb{N}$ we can take $y_n \in \mathbb{Q}$ such that $y - 1/n < y_n < y + 1/n$. Let $\epsilon > 0_R$ be arbitrary. By the Archimedean property we can find an $N \in \mathbb{N}$ such that $1/N < \epsilon$. Then for $n \geq N$ we find $|y_n - y| < 1/n \leq 1/N < \epsilon$. We conclude $y_n \to y$. The restriction of φ to $\varphi|_{\mathbb{Q}} : \mathbb{Q} \to \varphi(\mathbb{Q})$ is an isomorphism so by bijectivity of $\varphi|_{\mathbb{Q}}$ we can define the sequence $(x_n) : \mathbb{N} \to \mathbb{Q}$ by $x_n = \varphi|_{\mathbb{Q}}^{-1}(y_n)$. By similar reasoning as above, we find that (x_n) is Cauchy, and Cauchy as a function $\mathbb{N} \to R$ as well. It therefore converges to some $x \in \mathbb{R}_C$. For this x we have $\varphi(x) = y$.

□

We have done it; we have proven the existence and uniqueness of the real numbers. We are now free to write $\mathbb{R}$ without any subscript, without the need for specifying its precise set-theoretic definition, and without the need for specifying its properties; as we have been doing all our lives.

3.5 Comparison of the constructions

In this section we will take a step back and remove our blindfolds for knowledge exterior to what we have established so far. That means that we will assume knowledge of other fields in mathematics to give a more informed overview of the constructions.

Before comparing the constructions themselves, we will look at their structure in terms of sets, see also [3]. Note that we built the rational numbers as equivalence classes of pairs of integers. Let α extract these equivalence classes from the pairs. That is $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z})_\alpha$. We find the following compositions of the real numbers.

$$\begin{aligned}
\mathbb{R}_D &= (\mathcal{P}\left((\mathbb{Z} \times \mathbb{Z})_\alpha\right))_\delta, \\
\mathbb{R}_C &= (\mathbb{N} \to (\mathbb{Z} \times \mathbb{Z})_\alpha)_\gamma, \\
\mathbb{R}_S &= (\mathbb{Z} \to \mathbb{Z})_\sigma,
\end{aligned}$$

where δ extracts the Dedekind cuts, γ the Cauchy sequences and σ the almost homomorphisms. We see that purely constructionally, the Schanuel real numbers are the most simple. Where the other constructions have two restrictions, the Schanuel real numbers have only one.

Let us now consider Dedekind's construction. In his construction, each real number is represented by a single Dedekind cut. This is advantageous, as it

makes any function (relation) defined on them almost automatically univalent. It only would only remain to show it is total.

Dedekind's construction also generalises well to general ordered sets. In fact, the order need not satisfy strongly connectedness, in which case it is called a partial order. This generalised completion is known as the Dedekind–MacNeille completion, and works as follows. Let $(S, \leq)$ be a partial order. For $A \subseteq S$ define $\operatorname{upp}(A) = \{s \in S \mid \forall a \in A(s \geq a)\}$. Then $\operatorname{upp}(A)$ are the upper bounds of A. Similarly define the lower bounds of A as $\operatorname{low}(A) = \{s \in S \mid \forall a \in A(s \leq a)\}$. A cut of S is then a pair (A, B) for which $\operatorname{upp}(A) = B$ and $\operatorname{low}(B) = A$. In this case one also has $\operatorname{low}(\operatorname{upp}(A)) = A$, so $(A, \operatorname{upp}(A))$ is a cut. Hence similar to Dedekind cuts, one can focus only on the set A. Then the sets of cuts of S is the completion of S. Note that applying this completion to the rational numbers does not result in the real numbers; it results in the extended real numbers. These are the real numbers along with two elements assuming the roles of negative and positive infinity. This is because Dedekind cuts required $A \neq \varnothing$ and $A \neq \mathbb{Q}$, whereas this generalised completion does not require that. The cut $A = \varnothing$ behaves like negative infinity, the cut $A = \mathbb{Q}$ behaves like positive infinity.

Contrary to Dedekind real numbers, Cantor real numbers are represented by equivalence classes. Since operations on equivalence classes are defined in terms of their representatives, it is often necessary to verify the operation (relation) is both total and univalent. While this is often readily done, sometimes it is not immediately clear. For example, in general the reciprocal of a Cauchy sequence is not Cauchy. Only because we could cherry-pick the representatives, we were able to make this work.

Similar to Dedekind's construction, Cantor's construction can be easily generalised. Let X be a set and let $d : (X \times X) \to \mathbb{R}$ be a function. Then (X, d) is a metric space[3] when for all $x \in X$, $y \in X$ and $z \in X$ one has

- $d(x, y) \geq 0$,
- $d(x, y) = 0 \iff x = y$,
- $d(x, y) = d(y, x)$,
- $d(x, y) \leq d(x, z) + d(z, y)$.

Cauchy sequences can then be defined as sequences for which $d(x_m, x_n)$ gets arbitrarily small for large enough $m \in \mathbb{N}$ and $n \in \mathbb{N}$. The Cauchy-completion of X is then the set of equivalent Cauchy sequences, where two Cauchy sequences are equivalent when their difference converges to zero. When X additionally is an ordered abelian group, it induces the metric defined by $d(x, y) = |y - x|$. This metric is precisely the metric we used for the construction of the Cantor real numbers.

Schanuel's construction also relied on equivalence classes, making operations on his real numbers subject to a proof of well-definedness. Though as with Cantor's construction, these are usually not too difficult. Contrary to Cantor's construction though, no assumption on the representative has to be done. All almost homomorphisms remain almost homomorphisms under addition and multiplication.

[3]Even more generally, one can consider Cauchy filters in a uniform space. See [15] for more information.

Schanuel's construction skips over the rational numbers, and therefore avoids all proofs related to them. However, one may object that the rational numbers are to be constructed at some point anyway, because of their usefulness in many occasions. Frankly without them, there is no such thing as rational and irrational numbers. However, Theorem 2.3.11 asserts that $\mathbb{Q}$ must exist in $\mathbb{R}_S$, which is sufficient to know for most cases. If explicit representations of rational numbers in $\mathbb{R}_S$ are sought after, we saw that one can construct $\mathbb{Q}$ as a subfield of $\mathbb{R}_S$. It would have to be shown first that they are indeed isomorphic to $\mathbb{Q}$, though.

3.6 Further research

Given that completeness characterised the real numbers, one may wonder whether there exists a notion of completeness that the real numbers lack. One direction to explore is that of non-Archimedean ordered fields. These include number systems like the surreal [6] and hyperreal [11] numbers. These are number systems that contain infinitely small and infinitely large numbers, which the real numbers certainly do not. However, one should wonder in what sense these number systems are actually more complete than the real numbers. They are, for example, still not closed under inversion; infinity ("1/0") remains not a number. It turns out that the surreal numbers are "saturated" [23]. The saturation property mandates that for any two subsets[4] A and B of surreal numbers such that every element of A is less than every element of B, there exists a surreal number larger than all elements of A and smaller than all elements of B. This fails in the real numbers: take any Dedekind cut. Note that the saturation property is a stronger property than Dedekind-completeness.

Related to the surreal and hyperreal numbers are the extended real numbers. These add two quantities (∞ and $-\infty$) to the real numbers that behave like positive and negative infinity. For example one would have $\infty + a = \infty$ for all $a \in \mathbb{R}$. Contrary to the surreal and hyperreal numbers, the extended real numbers are closed under inversion. Furthermore, as we alluded to before, the Dedekind–MacNeille completion of the rational numbers yields the extended real numbers. In these senses it would make them more complete. They are also "topologically compact"; every subset has a supremum. They however no longer form a field. Even worse, they satisfy none of the properties of a field. This is because expressions like "$\infty - \infty$" are usually left undefined. The extended real numbers are used in particular in measure theory, where sets are allowed to have infinite measure, functions are allowed to attain infinity and integrals may evaluate to infinity [30].

Another direction one might venture is that of complex numbers, quaternions, octonions and further[5]. Landau was likely the first to fully describe the construction of the natural numbers all the way to the complex numbers [18]. As far as completeness goes, the complex numbers are the most interesting. They satisfy "algebraic closure", meaning that any (nonconstant) polynomial has a root in the complex numbers. This fails in the real numbers: consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x \cdot x + 1$. Beyond the complex numbers

[4] Note that the surreal numbers are too large to form a set, they form a proper class. However the saturation property only applies to subsets.

[5] They can be indefinitely extended using the Cayley–Dickson construction [9].

it is unclear whether they satisfy any reasonable notion of completeness that the complex numbers do not satisfy. The octonions and further are interesting mostly for other reasons.

It is in general hard to define what a completion or completeness property is or would have to be. If anything, they are classified by the following principle: the space achieved by a completion must be complete with respect to the completeness property the space was completed with. For instance, the Dedekind real numbers are Dedekind-complete and the Cantor real numbers are Cauchy-complete.

Note that all the completions we discussed lost properties the real numbers enjoyed. The surreal numbers are no longer Archimedean, the extended real numbers no longer form a field and the complex numbers can no longer be equipped with an order such that it becomes an ordered field. It seems in this sense the real numbers are at some sort of maximal structure. If one tries to go any higher, the foundation one stands on will lower.

Bibliography

[1] N. A'Campo. *A natural construction for the real numbers*. 2003. arXiv: math/0301015 [math.GN]. URL: https://arxiv.org/abs/math/0301015.

[2] R. D. Arthan. *The Eudoxus Real Numbers*. 2004. arXiv: math/0405454 [math.HO]. URL: https://arxiv.org/abs/math/0405454.

[3] A. Borovik, R. Jin, and M. G. Katz. "An Integer Construction of Infinitesimals: Toward a Theory of Eudoxus Hyperreals." In: *Notre Dame Journal of Formal Logic* 53.4 (Jan. 2012). ISSN: 0029-4527. DOI: 10.1215/00294527-1722755. URL: http://dx.doi.org/10.1215/00294527-1722755.

[4] G. Cantor. *Grundlagen einer allgemeinen Mannigfaltigkeitslehre. ein mathematisch-philosophischer Versuch in der Lehre des Unendlichen*. Teubner, 1883. URL: https://digital.slub-dresden.de/data/kitodo/gruneialm_313523215/gruneialm_313523215_tif/jpegs/gruneialm_313523215.pdf.

[5] G. Cantor. "Ueber die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen." In: *Mathematische Annalen* 5 (1872), pp. 123–132. URL: http://eudml.org/doc/156562.

[6] J. H. Conway. *On Numbers and Games*. Academic Press, 1976.

[7] R. Dedekind. *Stetigkeit und irrationale Zahlen*. Friedrich Vieweg und Sohn, 1872.

[8] R. Dedekind. *Was sind und was sollen die Zahlen?* Friedrich Vieweg und Sohn, 1888.

[9] L. E. Dickson. "On Quaternions and Their Generalization and the History of the Eight Square Theorem." In: *Annals of Mathematics* 20.3 (1919), pp. 155–171.

[10] H. B. Enderton. *A Mathematical Introduction to Logic*. 2nd ed. Academic Press, 2001.

[11] R. Goldblatt. *Lectures on the Hyperreals. An Introduction to Nonstandard Analysis*. Springer-Verlag, 1998.

[12] T. L. Heath. *The Thirteen Books of Euclid's Elements*. 2nd ed. Vol. 2. Dover Publications, 1926.

[13] E. V. Huntington. "Complete Sets of Postulates for the Theory of Real Quantities." In: *Transactions of the American Mathematical Society* 4.3 (1903), pp. 358–370.

[14] S. Kangshen, J. N. Crossley, and S. W-C Lun. *The Nine Chapters on the Mathematical Art Companion and Commentary*. Oxford University Press, 1999. ISBN: 0 19 853936 3.

[15] J .L. Kelley. *General Topology*. Springer Publishing, 1975.

[16] K. Kunen. *Set Theory. An Introduction to Independence Proofs*. Elsevier, 1992.

[17] K. Kuratowski. "Sur la notion de l'ordre dans la Théorie des Ensembles." In: *Fundamenta Mathematicae* 2 (1921), pp. 161–171. ISSN: 1730-6329. DOI: 10.4064/fm-2-1-161-171. URL: http://dx.doi.org/10.4064/fm-2-1-161-171.

[18] E. Landau. *Grundlagen der Analysis. Das Rechnen mit ganzen, rationalen, irrationalen, komplexen Zahlen*. Akademische Verlagsgesellschaft, 1930.

[19] S. R. Lay. *Analysis with an introduction to proof*. 5th ed. Pearson, 2014.

[20] A. Levy. *Basic Set Theory*. Springer-Verlag, 1979.

[21] E. Mendelson. *Introduction to Mathematical Logic*. 4th ed. Chapman & Hall, 1997.

[22] R. Méray. "Remarques sur la nature des quantités définies par la condition de servir de limites à des variables données." In: *Revue des sociétés savantes: Sciences mathématiques, physiques et naturelles* (1869). URL: https://gallica.bnf.fr/ark:/12148/bpt6k2026062/f280.item.

[23] M. Michael. "On theories categorical in uncountable powers." In: *Proceedings of the National Academy of Sciences of the United States of America* 49 (2 1963), pp. 213–216.

[24] *Nine Chapters on Arithmetic*. See [14] for a translation. Chinese Text Project. URL: https://ctext.org/nine-chapters.

[25] G. Peano. *Arithmetices principia. nova methodo exposita*. Fratres Bocca, 1989.

[26] D. Piponi. *Defining the Reals*. 2006. URL: http://blog.sigfpe.com/2006/05/defining-reals.html.

[27] B. Russell. *The philosophy of logical atomism*. Routledge Classics. London, England: Routledge, 2009.

[28] T. Skolem. "Über die Nicht-charakterisierbarkeit der Zahlenreihe mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschließlich Zahlenvariablen." In: *Fundamenta Mathematicae* 23 (1934), pp. 150–161.

[29] R. Street. "An efficient construction of the real numbers." In: *Gazette - Australian Mathematical Society* (1985). URL: https://andrescaicedo.wordpress.com/wp-content/uploads/2014/09/ross-street-an-efficient-construction-of-real-numbers.pdf.

[30] M. Veraar, E. Lorist, and Z. Nieraeth. *Measure and Integration*. Lecture notes on AM2090.

[31] I. Weiss. *The real numbers - a survey of constructions*. 2015. arXiv: 1506.03467 [math.HO]. URL: https://arxiv.org/abs/1506.03467.

[32] E. Zermelo. "Untersuchungen über die Grundlagen der Mengenlehre. I." In: *Mathematische Annalen* 65 (1908), pp. 261–281. URL: http://eudml.org/doc/158344.

Appendix A

First-order logic

Zermelo–Fraenkel set theory, as the name suggests, is a theory. Without going go too deep into mathematical logic, a theory is a collection of statements, formally called sentences. The axioms of **ZF**, being by assumption true sentences, are therefore part of the theory. Using the axioms, one can prove more statements, which are also part of the theory. The theory of **ZF** thus consists of all the statements one can prove from the axioms by the rules of inference[1].

In particular, **ZF** is a first-order theory with equality. First-order refers to the logical framework that is being worked in; first-order logic. With equality means that an additional primitive symbol ("=") is added into the language that expresses equality between two objects. First-order logic is an extension of zeroth-order logic, or more commonly called propositional logic. A proposition is a statement that can be true or false. For instance, $\pi = 3$ is a proposition, in this case a false proposition. Propositional logic is the study of combining these propositions, usually denoted by variables, using logical connectives. The logical connectives generally include $\wedge$ ("and"), $\vee$ ("or"), $\implies$ ("implies"), $\iff$ ("is equivalent to") and $\neg$ ("not"). See Tables A.1-A.5 for how these connectives behave. Here **T** denotes truth and **F** denotes falsity. Along with parentheses ("(" and ")") to disambiguate the notation, one can then combine these symbols to create more complex propositions. First-order logic expands upon propositional logic by allowing to make statements that quantify over objects. Where propositional logic is all about propositions, first-order logic is all about predicates. The universal quantifier ("$\forall$") allows the creation of a predicate that mandates a certain proposition to be true for all objects. Similarly, the existential quantifier ("$\exists$") allows the creation of a predicate that mandates a certain proposition to be true for at least one object. Additionally, the theory of **ZF** adds one more nonlogical symbol to the language. This is the symbol "$\in$", which denotes set membership. To summarise, the language of a first-order theory with equality consists of the following symbols.

- Variables (letters, subscripted letters, etc.)
- Logical connectives ("$\wedge$", "$\vee$", "$\implies$", "$\iff$" and "$\neg$")
- Quantifiers ("$\forall$", "$\exists$")

[1] Mendelson defines a theory just to be the set of axioms [21].

- Equality symbol ("=")
- Set membership symbol ("∈")
- Parentheses ("(" and ")")

A sequence of symbols of the language of a first-order theory is called a formula. Not any sequence of symbols is valid, though. Clearly ") $\in \implies x\exists\neg$)" is rubbish. One can define well-formed formulas recursively as follows.

- $x = y$ and $x \in y$ are well-formed formulas.
- If φ is a well-formed formula, so is $\neg\varphi$.
- If φ and ψ are well-formed formulas, so are $\varphi \bullet \psi$, where $\bullet$ denotes any of $\wedge$, $\vee$, $\implies$ or $\iff$.
- If φ is a well-formed formula, so are $\forall x(\varphi)$ and $\exists x(\varphi)$.

Because general formulas are of little interest, henceforth we will refer to well-formed formulas as just formulas. To declare dependence of formulas on variables, the notion of free and bound variables is used. A variable is free in a formula if it can be changed freely; it is a placeholder. A variable is bound if it is bound by a specific operator, like a quantifier.

The universal quantifier is defined formally by the rule of universal instantiation. This rule states the following. Let φ be a formula with free variables among x. Then

$$\forall x(\varphi(x)) \implies A\{x \mapsto t\},$$

where $A\{x \mapsto t\}$ means replacing every occurrence of x in A with t. The existential quantifier is then usually defined in terms of the universal quantifier: we write $\exists x(\varphi(x))$ to mean $\neg(\forall x(\neg\varphi(x)))$.

P	Q	$P \wedge Q$
F	**F**	**F**
F	**T**	**F**
T	**F**	**F**
T	**T**	**T**

Table A.1: Logical conjuction

P	Q	$P \vee Q$
F	**F**	**F**
F	**T**	**T**
T	**F**	**T**
T	**T**	**T**

Table A.2: Logical disjunction

P	Q	$P \implies Q$
F	**F**	**T**
F	**T**	**T**
T	**F**	**F**
T	**T**	**T**

Table A.3: Logical implication

P	Q	$P \iff Q$
F	**F**	**T**
F	**T**	**F**
T	**F**	**F**
T	**T**	**T**

Table A.4: Logical biconditional

P	$\neg P$
F	**T**
T	**F**

Table A.5: Logical negation

The axioms of equality can then be formulated as follows.

Reflexivity. $\forall x(x = x)$.

Symmetry. $\forall x \forall y(x = y \implies y = x)$.

Transitivity. $\forall x \forall y \forall z(x = y \wedge y = z \implies x = z)$.

Substitution for function symbols. Let f be a function symbol of arity at least one. Then $\forall x \forall y(x = y \implies f(x) = f(y))$.

Substitution for formulas. Let φ be a formula with free variables among x and nonfree variable y. Then $\forall x \forall y(x = y \implies (\varphi(x) \implies (\varphi(y))))$.

Note that the substitution axioms are actually axiom schemas, one for each function symbol or formula. With this, all of mathematics can be formulated. However, one has to look no further than elementary school mathematics to find symbols that are not part of this language. For instance, numbers are not part of the language, nor is addition of them. For this reason, definitional extensions exist. One can simply add to the alphabet of a theory to create a larger language. Proposition A.1.1 asserts that this extension is indeed formally logically justified. A similar result can be proven for relation symbols.

Proposition A.1.1 (Definitional extension with function symbol, Proposition 2.28 in [21])**.** *Let T be a theory with equality. Assume that $\vdash_T \exists! y \varphi(y, x_1, \ldots, x_n)$. Let T' be the theory (with equality) obtained by adding the n-ary function symbol f and the proper axiom $\varphi(f(x_1, \ldots, x_n), x_1, \ldots, x_n)$, as well as all logical axioms. Then there exists a transformation of each wff ϕ of T' onto a wff ϕ' of T such that*

(a) If f does not occur in ϕ, then ϕ' is ϕ.

(b) $(\neg\phi)'$ is $\neg(\phi')$.

(c) $(\phi \implies \psi)'$ is $\phi' \implies \psi'$.

(d) $(\forall x \phi)'$ is $\forall x(\phi')$.

(e) $\vdash_{T'} (\phi \iff \phi')$.

(f) If $\vdash_{T'} \phi$ then $\vdash_T \phi'$.

Hence if ϕ does not contain f and $\vdash_{T'} \phi$, then $\vdash_T \phi$. In particular, adding the function symbol does not add to the theory.

There is a last, yet exceptionally important thing we have not mentioned. This concerns first-order theories, in our case **ZF**. Technically one does not work in just **ZF**, one works in a model of **ZF**. A model or interpretation of a theory is a structure in which the theory is true. The model contains all the sets one can work with, and is therefore also known as the domain of discourse. When working in a particular model of a first-order theory, all quantifiers are bound by the model; they only see what is inside the model. This means that when working in a model M, the assumed domain of discourse is M, meaning that every quantification $\forall x$ or $\exists x$ is to be interpreted as $\forall x \in M$ and $\exists x \in M$. This may seem unimportant, but has real implications. For example, when

one makes a statement about every subset of an arbitrary set, the statement may not have the intended meaning. That is because to actually quantify over arbitrary subsets, the sets would have to be members of $\mathcal{P}(M)$, which is strictly larger than M. Therefore in first-order logic, the statement only says something about the subsets present in M, but fails to state something about all the subsets in $\mathcal{P}(M) \setminus M$. This renders the statement much weaker than intended. One example of this is the definition of well-foundedness as stated in Definition 2.1.15. Thus, when working in **ZF**, being a first-order theory, one cannot prove well-foundedness of the natural numbers for all subsets. This means that even though one can prove well-foundedness for subsets that are members of M, it may be the case that some subsets that are members of $\mathcal{P}(M) \setminus M$ are not well-founded. In this sense, every property can be axiomatisable in some order of logic. Here well-foundedness is axiomatisable in second-order logic and provably not in any lesser order logic, so it is a second-order property. That is, in second-order logic the quantifiers are bound by $\mathcal{P}(M)$, which is sufficient for the definition of well-foundedness. When it is the case that a model of some structure is not isomorphic to the intended structure, the model is called nonstandard. And indeed, in a first-order theory nonstandard models of any infinite number system exist, which is a consequence of a theorem due to Löwenheim and Skolem [28]. A nonstandard model has real implications. For example, there exists models of the real numbers that do not contain π, or any transcendental number for that matter. This is because any first-order statement involving the real numbers is also true for just the real algebraic numbers. Yet in a standard model of the real numbers almost all numbers are transcendental. Related to this is the case when the model M of **ZF** is countable. Since **ZF** can prove the existence of uncountable ordinals, it can prove the existence of sets which are strictly larger than the model itself. This peculiar result is known as Skolem's paradox. It is not actually a paradox, but merely a peculiarity, because the uncountable ordinal is not actually uncountable. From inside the model it "thinks" it is, but from the outside it is not.