Set Theory

2012/13

by Peter Koepke

Die Mengenlehre ist das Fundament
der gesamten Mathematik
(Felix Hausdorff,
Grundzüge der Mengenlehre, 1914)

1 Introduction

Georg Cantor characterized sets as follows:

> Unter einer *Menge* verstehen wir jede Zusammenfassung M von bestimmten, wohlunterschiedenen Objekten m unsrer Anschauung oder unseres Denkens (welche die "Elemente" von M genannt werden) zu einem Ganzen.

Felix Hausdorff in *Grundzüge* formulated shorter:

> Eine Menge ist eine Zusammenfassung von Dingen zu einem Ganzen, d.h. zu einem neuen Ding.

Sets are ubiquitous in mathematics. According to Hausdorff

> Differential- und Integralrechnung, Analysis und Geometrie arbeiten in Wirklichkeit, wenn auch vielleicht in verschleiernder Ausdrucksweise, beständig mit unendlichen Mengen.

In current mathematics, *many* notions are explicitly defined using sets. The following example indicates that notions which are not set-theoretical *prima facie* can be construed set-theoretically:

f is a real funktion $\equiv$ f is a **set** of ordered pairs $(x, f(x))$ of real numbers, such that ... ;

(x, y) is an ordered pair $\equiv$ (x, y) is a **set** ...$\{x, y\}$... ;

x is a real number $\equiv$ x is a left half of a Dedekind cut in $\mathbb{Q}$ $\equiv$ x is a **subset** of $\mathbb{Q}$, such that ... ;

r is a rational number $\equiv$ r is an **ordered pair** of integers, such that ... ;

z is an integer $\equiv$ z is an **ordered pair** of natural numbers (= non-negative integers);

$\mathbb{N} = \{0, 1, 2, ...\}$;

0 is the empty **set**;

1 is the **set** $\{0\}$;

2 is the **set** $\{0, 1\}$; etc. etc.

We shall see that *all* mathematical notions can be reduced to the notion of *set*.

Besides this foundational role, set theory is also the mathematical study of the *infinite*. There are infinite sets like $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$ which can be subjected to the constructions and analyses of set theory; there are various degrees of infinity which lead to a rich theory of infinitary combinatorics.

In this course, we shall first apply set theory to obtain the standard foundation of mathematics and then turn towards "pure" set theory.

2 The Language of Set Theory

If m is an *element* of M one writes $m \in M$. If all mathematical objects are reducible to sets, *both sides* of these relation have to be sets. This means that set theory studies the $\in$-relation $m \in M$ for arbitrary *sets* m and M. As it turns out, this is sufficient for the purposes of set theory and mathematics. In set theory variables range over the class of all sets, the $\in$-relation is the only undefined structural component, every other notion will be defined from the $\in$-relation. Basically, set theoretical statement will thus be of the form

$$...\forall x...\exists y......x \in y...u \equiv v...,$$

belonging to the first-order predicate language with the only given predicate $\in$.

To deal with the complexities of set theory and mathematics one develops a comprehensive and intuitive language of abbreviations and definitions which, eventually, allows to write familiar statements like

$$e^{i\pi} = -1$$

and to view them as statements within set theory.

The language of set theory may be seen as a low-level, internal language. The language of mathematics possesses high-level "macro" expressions which abbreviate low-level statements in an efficient and intuitive way.

3 Russell's Paradox

Cantor's naive description of the notion of set suggests that for any mathematical statement $\varphi(x)$ in one free variable x there is a *set* y such that

$$x \in y \leftrightarrow \varphi(x),$$

i.e., y is the collection of all sets x which satisfy φ.

This axiom is a basic principle in Gottlob Frege's *Grundgesetze der Arithmetik, 1893*, Grundgesetz V, Grundgesetz der Wertverläufe.

Bertrand Russell noted in 1902 that setting $\varphi(x)$ to be $x \notin x$ this becomes

$$x \in y \leftrightarrow x \notin x,$$

and in particular for $x = y$:

$$y \in y \leftrightarrow y \notin y.$$

Contradiction.

This contradiction is usually called Russell's paradox, antinomy, contradiction. It was also discovered slightly earlier by Ernst Zermelo. The paradox shows that the formation of sets as collections of sets by *arbitrary* formulas is not consistent.

4 The Zermelo-Fraenkel Axioms

The difficulties around Russell's paradox and also around the axiom of choice lead Zermelo to the formulation of axioms for set theory in the spirit of the axiomatics of David Hilbert of whom Zermelo was an assistant at the time.

Zermelo's main idea was to restrict Frege's Axiom V to formulas which correspond to mathematically important formations of collections, but to avoid arbitrary formulas which can lead to paradoxes like the one exhibited by Russell.

The original axiom system of Zermelo was extended and detailed by Abraham Fraenkel (1922), Dmitry Mirimanoff (1917/20), and Thoralf Skolem.

We shall discuss the axioms one by one and simultaneously introduce the logical language and useful conventions.

4.1 Set Existence

The *set existence axiom*

$$\exists x \forall y \neg y \in x,$$

like all axioms, is expressed in a language with quantifiers $\exists$ ("there exists") and $\forall$ ("for all"), which is familiar from the ϵ-δ-statements in analysis. The *language of set theory* uses variables x, y, ... which may satisfy the binary relations $\in$ or $=$: $x \in y$ ("x is an *element of* y") or $x = y$. These elementary *formulas* may be connected by the *propositional connectives* $\wedge$ ("and"), $\vee$ ("or"), $\rightarrow$ ("implies"), $\leftrightarrow$ ("is equivalent"), and $\neg$ ("not"). The use of this language will be demonstrated by the subsequent axioms.

The axiom expresses the existence of a set which has no elements, i.e., the existence of the *empty set*.

4.2 Extensionality

The *axiom of extensionality*

$$\forall x \forall x' (\forall y (y \in x \leftrightarrow y \in x') \rightarrow x = x')$$

expresses that a set is exactly determined by the collection of its elements. This allows to prove that there is exactly one empty set.

Lemma 1. $\forall x \forall x' (\forall y \neg y \in x \wedge \forall y \neg y \in x' \rightarrow x = x')$.

Proof. Consider x, x' such that $\forall y \neg y \in x \wedge \forall y \neg y \in x'$. Consider y. Then $\neg y \in x$ and $\neg y \in x'$. This implies $\forall y (y \in x \leftrightarrow y \in x')$. The axiom of extensionality implies $x = x'$. □

Note that this proof is a usual mathematical argument, and it is also a *formal proof* in the sense of mathematical logic. The sentences of the proof can be derived from earlier ones by purely formal deduction rules. The rules of natural deduction correspond to common sense figures of argumentation which treat hypothetical objects as if they would concretely exist.

4.3 Pairing

The *pairing axiom*

$$\forall x \forall y \exists z \forall u (u \in z \leftrightarrow u = x \vee u = y)$$

postulates that for all sets x, y there is set z which may be denoted as

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

This formula, including the new notation, is equivalent to the formula

$$\forall u (u \in z \leftrightarrow u = x \vee u = y).$$

In the sequel we shall extend the small language of set theory by hundreds of symbols and conventions, in order to get to the ordinary language of mathematics with notations like

$$\mathbb{N}, \mathbb{R}, \sqrt{385}, \pi, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \int_a^b f'(x) \mathrm{dx} = f(b) - f(a), \text{etc.}$$

Such notations are chosen for intuitive, pragmatic, or historical reasons.

Using the notation for unordered pairs, the pairing axiom may be written as

$$\forall x \forall y \exists z\, z = \{x, y\}.$$

By the axiom of extensionality, the term-like notation has the expected behaviour. E.g.:

Lemma 2. $\forall x \forall y \forall z \forall z' (z = \{x, y\} \wedge z' = \{x, y\} \rightarrow z = z')$.

Proof. Exercise. □

Note that we implicitly use several notational conventions: variables have to be chosen in a reasonable way, for example the symbols z and z' in the lemma have to be taken different and different from x and y. We also assume some operator priorities to reduce the number of brackets: we let $\wedge$ bind stronger than $\vee$, and $\vee$ stronger than $\rightarrow$ and $\leftrightarrow$.

We used the "term" $\{x, y\}$ to occur within set theoretical formulas. This abbreviation is than to be expanded in a natural way, so that officially all mathematical formulas are formulas in the "pure" $\in$-language. We want to see the notation $\{x, y\}$ as an example of a *class term*. We define uniform notations and convention for such abbreviation terms.

4.4 Class Terms

The extended language of set theory contains class terms and notations for them. There are axioms for class terms that fix how extended formulas can be reduced to formulas in the unextended $\in$-language of set theory.

Definition 3. *A* class term *is of the form* $\{x|\varphi\}$ *where* x *is a variable and* $\varphi \in L^{\in}$*. The usage of these class terms is defined recursively by the following axioms: If* $\{x|\varphi\}$ *and* $\{y|\psi\}$ *are class terms then*

- $u \in \{x|\varphi\} \leftrightarrow \varphi\frac{u}{x}$, *where* $\varphi\frac{u}{x}$ *is obtained from* φ *by (resonably) substituting the variable* x *by the variable* u *;*
- $u = \{x|\varphi\} \leftrightarrow \forall v\, (v \in u \leftrightarrow \varphi\frac{v}{x})$*;*
- $\{x|\varphi\} = u \leftrightarrow \forall v\, (\varphi\frac{v}{x} \leftrightarrow v \in u)$*;*
- $\{x|\varphi\} = \{y|\psi\} \leftrightarrow \forall v\, (\varphi\frac{v}{x} \leftrightarrow \psi\frac{v}{y})$*;*
- $\{x|\varphi\} \in u \leftrightarrow \exists v(v \in u \wedge v = \{x|\varphi\}$*;*
- $\{x|\varphi\} \in \{y|\psi\} \leftrightarrow \exists v(\psi\frac{v}{y} \wedge v = \{x|\varphi\})$*.*

A term *is either a variable or a class term.*

Definition 4.

a) $\emptyset := \{x|x \neq x\}$ *is the* empty set*;*

b) $V := \{x|x = x\}$ *is the* universe *(of all sets);*

c) $\{x, y\} := \{u|u = x \vee u = y\}$ *is the* unordered pair *of* x *and* y *.*

Lemma 5.

a) $\emptyset \in V$*.*

b) $\forall x, y\ \{x, y\} \in V$*.*

Proof. a) By the axioms for the reduction of abstraction terms, $\emptyset \in V$ is equivalent to the following formulas

$$\exists v(v = v \wedge v = \emptyset)$$
$$\exists v\, v = \emptyset$$
$$\exists v\, \forall w\, (w \in v \leftrightarrow w \neq w)$$
$$\exists v \forall w\, w \notin v$$

which is equivalent to the axiom of set existence. So $\emptyset \in V$ is another way to write the axiom of set existence.

b) $\forall x, y\ \{x, y\} \in V$ abbreviates the formula

$$\forall x, y \exists z(z = z \wedge z = \{x, y\}).$$

This can be expanded equivalently to the pairing axiom

$$\forall x, y \exists z \forall u (u \in z \leftrightarrow u = x \vee u = y). \qquad \square$$

So a) and b) are concise equivalent formulations of the axiom Ex and Pair.

We also introduce *bounded quantifiers* to simplify notation.

Definition 6. *Let A be a term. Then $\forall x \in A\, \varphi \leftrightarrow \forall x (x \in A \rightarrow \varphi)$ and $\exists x \in A\, \varphi \leftrightarrow \exists x\, (x \in A \wedge \varphi)$.*

Definition 7. *Let $x, y, z, \ldots$ be variables and $X, Y, Z, \ldots$ be class terms. Define*

a) $X \subseteq Y \leftrightarrow \forall x \in X\, x \in Y$, *$X$ is a* subclass *of Y;*

b) $X \cup Y := \{x | x \in X \vee x \in Y\}$ *is the* union *of X and Y;*

c) $X \cap Y := \{x | x \in X \wedge x \in Y\}$ *is the* intersection *of X and Y;*

d) $X \setminus Y := \{x | x \in X \wedge x \notin Y\}$ *is the* difference *of X and Y;*

e) $\bigcup X := \{x | \exists y \in X\, x \in y\}$ *is the* union *of X;*

f) $\bigcap X := \{x | \forall y \in X\, x \in y\}$ *is the* intersection *of X;*

g) $\mathcal{P}(X) := \{x | x \subseteq X\}$ *is the* power class *of X;*

h) $\{X\} := \{x | x = X\}$ *is the* singleton set *of X;*

i) $\{X, Y\} := \{x | x = X \vee x = Y\}$ *is the* (unordered) pair *of X and Y;*

j) $\{X_0, \ldots, X_{n-1}\} := \{x | x = X_0 \vee \ldots \vee x = X_{n-1}\}$.

One can prove the well-known boolean properties for these operations. We only give a few examples.

Proposition 8. $X \subseteq Y \wedge Y \subseteq X \rightarrow X = Y$.

Proposition 9. $\bigcup \{x, y\} = x \cup y$.

Proof. We show the equality by two inclusions:
($\subseteq$). Let $u \in \bigcup \{x, y\}$. $\exists v (v \in \{x, y\} \wedge u \in v)$. Let $v \in \{x, y\} \wedge u \in v$. $(v = x \vee v = y) \wedge u \in v$.
Case 1. $v = x$. Then $u \in x$. $u \in x \vee u \in y$. Hence $u \in x \cup y$.
Case 2. $v = y$. Then $u \in y$. $u \in x \vee u \in y$. Hence $u \in x \cup y$.

Conversely let $u \in x \cup y$. $u \in x \vee u \in y$.
Case 1. $u \in x$. Then $x \in \{x, y\} \wedge u \in x$. $\exists v (v \in \{x, y\} \wedge u \in v)$ and $u \in \bigcup \{x, y\}$.
Case 2. $u \in y$. Then $x \in \{x, y\} \wedge u \in x$. $\exists v (v \in \{x, y\} \wedge u \in v)$ and $u \in \bigcup \{x, y\}$. $\square$

Exercise 1. Show: a) $\bigcup V = V$. b) $\bigcap V = \emptyset$. c) $\bigcup \emptyset = \emptyset$. d) $\bigcap \emptyset = V$.

4.5 Ordered Pairs

Combining objects into ordered pairs (x, y) is taken as an undefined fundamental operation of mathematics. We cannot use the unordered pair $\{x, y\}$ for this purpose, since it does not respect the order of entries:

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

We have to introduce some asymmetry between x and y to make them distinguishable. Following Kuratowski and Wiener we define:

Definition 10. $(x, y) := \{\{x\}, \{x, y\}\}$ *is the* ordered pair *of x and y.*

The definition involves substituting class terms within class terms. We shall see in the following how these class terms are eliminated to yield pure $\in$-formulas.

Lemma 11. $\forall x \forall y \exists z\, z = (x, y)$.

Proof. Consider sets x and y. By the pairing axiom choose u and v such that $u=\{x\}$ and $v=\{x,y\}$. Again by pairing choose z such that $z=\{u,v\}$. We argue that $z=(x,y)$. Note that

$$(x,y)=\{\{x\},\{x,y\}\}=\{w|w=\{x\}\vee w=\{x,y\}\}.$$

Then $z=(x,y)$ is equivalent to

$$\forall w(w\in z\leftrightarrow w=\{x\}\vee w=\{x,y\}),$$
$$\forall w(w=u\vee w=v\leftrightarrow(w=\{x\}\vee w=\{x,y\}),$$

and this is true by the choice of u and v. □

The KURATOWSKI-pair satisfies the fundamental property of ordered pairs:

Lemma 12. $(x,y)=(x',y')\rightarrow x=x'\wedge y=y'$.

Proof. Assume $(x,y)=(x',y')$, i.e.,
(1) $\{\{x\},\{x,y\}\}=\{\{x'\},\{x',y'\}\}$.
Case 1. $x=y$. Then

$\{x\}=\{x,y\}$,
$\{\{x\},\{x,y\}\}=\{\{x\},\{x\}\}=\{\{x\}\}$,
$\{\{x\}\}=\{\{x'\},\{x',y'\}\}$,
$\{x\}=\{x'\}$ and $x=x'$,
$\{x\}=\{x',y'\}$ and $y'=x$.

Hence $x=x'$ and $y=x=y'$ as required.
Case 2. $x\neq y$. (1) implies

$\{x'\}=\{x\}$ or $\{x'\}=\{x,y\}$.

The right-hand side would imply $x=x'=y$, contradicting the case assumption. Hence

$\{x'\}=\{x\}$ and $x'=x$.

Then (1) implies

$\{x,y\}=\{x',y'\}=\{x,y'\}$ and $y=y'$. □

Exercise 2.

a) Show that $\langle x,\ y\rangle := \{\{x,\ \emptyset\},\ \{y,\ \{\emptyset\}\}\}$ also satisfies the fundamental property of ordered pairs (F. HAUSDORFF).

b) Can $\{x,\{y,\emptyset\}\}$ be used as an ordered pair?

Exercise 3. Give a set-theoretical formalization of an ordered-*triple* operation.

4.6 Relations and Functions

Ordered pairs allow to introduce *relations* and *functions* in the usual way. One has to distinguish between *sets* which are relations and functions, and *class terms* which are relations and functions.

Definition 13. *A term R is a* relation *if all elements of R are ordered pairs, i.e., $R\subseteq V\times V$. Also write Rxy or xRy instead of $(x,y)\in R$. If A is a term and $R\subseteq A\times A$ then R is a* relation *on A.*

Note that this definition is really an *infinite schema* of definitions, with instances for all terms R and A. The subsequent extensions of our language are also infinite definition schemas. We extend the term language by parametrized collections of terms.

Definition 14. *Let $t(\vec{x})$ be a term in the variables $\vec{x}$ and let φ be an $\in$-formula. Then $\{t(\vec{x})|\varphi\}$ stands for $\{z|\exists\vec{x}(\varphi\wedge z=t(\vec{x}))\}$.*

Definition 15. *Let R,S,A be terms.*

a) The domain *of R is* $\mathrm{dom}(R):=\{x|\exists y\, x\, R\, y\}$.

b) The range *of R is* $\mathrm{ran}(R):=\{y|\exists x\, x\, R\, y\}$.

c) The field *of R is* $\mathrm{field}(R):=\mathrm{dom}(R)\cup\mathrm{ran}(R)$.

d) *The* restriction *of R to A is* $R \upharpoonright A := \{(x, y) | x R y \wedge x \in A\}$.

e) *The* image *of A under R is* $R[A] := R'' A := \{y | \exists x \in A\, x R y\}$.

f) *The* preimage *of A under R is* $R^{-1}[A] := \{x | \exists y \in A\, x R y\}$.

g) *The* composition *of S and R ("S after R") is* $S \circ R := \{(x, z) | \exists y\, (x R y \wedge y S z)\}$.

h) *The* inverse *of R is* $R^{-1} := \{(y, x) | x R y\}$.

Relations can play different roles in mathematics.

Definition 16. *Let R be a relation.*

a) *R is* reflexive *iff* $\forall x \in \mathrm{field}(R)\ x R x$.

b) *R is* irreflexive *iff* $\forall x \in \mathrm{field}(R)\ \neg x R x$.

c) *R is* symmetric *iff* $\forall x, y\, (x R y \rightarrow y R x)$.

d) *R is* antisymmetric *iff* $\forall x, y\, (x R y \wedge y R x \rightarrow x = y)$.

e) *R is* transitive *iff* $\forall x, y, z\, (x R y \wedge y R z \rightarrow x R z)$.

f) *R is* connex *iff* $\forall x, y \in \mathrm{field}(R)\, (x R y \vee y R x \vee x = y)$.

g) *R is an* equivalence relation *iff R is reflexive, symmetric and transitive.*

h) *Let R be an equivalence relation. Then* $[x]_R := \{y | y R x\}$ *is the* equivalence class *of x modulo R.*

It is possible that an equivalence class $[x]_R$ is not a set: $[x]_R \notin V$. Then the formation of the collection of all equivalence classes modulo R may lead to contradictions. Another important family of relations is given by *order relations*.

Definition 17. *Let R be a relation.*

a) *R is a* partial order *iff R is reflexive, transitive and antisymmetric.*

b) *R is a* linear order *iff R is a connex partial order.*

c) *Let A be a term. Then R is a* partial order on A *iff R is a partial order and* $\mathrm{field}(R) = A$.

d) *R is a* strict partial order *iff R is transitive and irreflexive.*

e) *R is a* strict linear order *iff R is a connex strict partial order.*

Partial orders are often denoted by symbols like $\leqslant$, and strict partial orders by $<$. A common notation in the context of (strict) partial orders R is to write

$$\exists p R q\, \varphi \text{ and } \forall p R q \varphi \text{ for } \exists p (p R q \wedge \varphi) \text{ and } \forall p (p R q \rightarrow \varphi) \text{ resp.}$$

One of the most important notions in mathematics is that of a *function*.

Definition 18. *Let F be a term. Then F is a* function *if it is a relation which satisfies*

$$\forall x, y, y'\ (x F y \wedge x F y' \rightarrow y = y').$$

If F is a function then

$$F(x) := \{u | \forall y\, (x F y \rightarrow u \in y)\}$$

is the value *of F at x.*

If F is a function and $x F y$ then $y = F(x)$. If there is no y such that $x F y$ then $F(x) = V$; the "value" V at x may be read as "undefined". A function can also be considered as the (indexed) sequence of its values, and we also write

$$(F(x))_{x \in A} \text{ or } (F_x)_{x \in A} \text{ instead of } F: A \rightarrow V.$$

We define further notions associated with functions.

Definition 19. *Let F, A, B be terms.*

a) *F is a* function from A to B, *or* $F: A \rightarrow B$, *iff F is a function,* $\mathrm{dom}(F) = A$, *and* $\mathrm{range}(F) \subseteq B$.

b) *F is a* partial function from A to B, *or* $F: A \rightharpoonup B$, *iff F is a function,* $\mathrm{dom}(F) \subseteq A$, *and* $\mathrm{range}(F) \subseteq B$.

c) *F is a* surjective *function from A to B iff $F: A \rightarrow B$ and* $\mathrm{range}(F) = B$.

d) *F is an* injective *function from A to B iff $F: A \rightarrow B$ and*

$$\forall x, x' \in A\ (x \neq x' \rightarrow F(x) \neq F(x'))$$

e) *F is a* bijective *function from A to B, or $F: A \leftrightarrow B$, iff $F: A \rightarrow B$ is surjective and injective.*

f) ${}^A B := \{f \mid f: A \rightarrow B\}$ *is the class of all functions from A to B.*

One can check that these functional notions are consistent and agree with common usage:

Exercise 4. Define a relation $\sim$ on V by

$$x \sim y \longleftrightarrow \exists f\, f: x \leftrightarrow y.$$

One say that x and y are *equinumerous* or *equipollent*. Show that $\sim$ is an equivalence relation on V. What is the equivalence class of $\emptyset$? What is the equivalence class of $\{\emptyset\}$?

Exercise 5. Consider functions $F: A \rightarrow B$ and $F': A \rightarrow B$. Show that

$$F = F' \text{ iff } \forall a \in A\ F(a) = F'(a).$$

4.7 Unions

The *union axiom* reads

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

Lemma 20. *The union axiom is equivalent to $\forall x \bigcup x \in V$.*

Proof. Observe the following equivalences:
$\forall x \bigcup x \in V$
$\leftrightarrow \forall x \exists y\, (y = y \wedge y = \bigcup x)$
$\leftrightarrow \forall x \exists y \forall z (z \in y \leftrightarrow z \in \bigcup x)$
$\leftrightarrow \forall x \exists y \forall z (z \in y \leftrightarrow \exists w \in x\, z \in w)$
which is equivalent to the union axiom. □

Note that the union of x is usually viewed as the union of all *elements* of x:

$$\bigcup x = \bigcup_{w \in x} w,$$

where we define

$$\bigcup_{a \in A} t(a) = \{z \mid \exists a \in A\, z \in t(a)\}.$$

Graphically $\bigcup x$ can be illustrated like this:

Combining the axioms of pairing and unions we obtain:

Lemma 21. $\forall x_0, \ldots, x_{n-1}\, \{x_0, \ldots, x_{n-1}\} \in V$.

Note that this is a *schema* of lemmas, one for each ordinary natural number n. We prove the schema by complete induction on n.

Proof. For $n=0,1,2$ the lemma states that $\emptyset\in V$, $\forall x\ \{x\}\in V$, and $\forall x,y\ \{x,y\}\in V$ resp., and these are true by previous axioms and lemmas. For the induction step assume that the lemma holds for n, $n\geqslant 1$. Consider sets $x_0,\ldots,x_n$. Then

$$\{x_0,\ldots,x_n\}=\{x_0,\ldots,x_{n-1}\}\cup\{x_n\}.$$

The right-hand side exists in V by the inductive hypothesis and the union axiom. □

4.8 Separation

It is common to form a subset of a given set consisting of all elements which satisfy some condition. This is codified by the *separation schema*. For every $\in$-formula $\varphi(z,x_1,\ldots,x_n)$ postulate:

$$\forall x_1\ldots\forall x_n\forall x\exists y\forall z\,(z\in y\leftrightarrow z\in x\wedge\varphi(z,x_1,\ldots,x_n)).$$

Using class terms the schema can be reformulated as: for every term A postulate

$$\forall x\,A\cap x\in V.$$

The crucial point is the restriction to the given set x. The unrestricted, FREGEan version $A\in V$ for every term A leads to the RUSSELL antinomy. We turn the antinomy into a consequence of the separation schema:

Theorem 22. *$V\notin V$.*

Proof. Assume that $V\in V$. Then $\exists x\,x=V$. Take x such that $x=V$. Let R be the RUSSELLian class:

$$R:=\{x|x\notin x\}.$$

By separation, $y:=R\cap x\in V$. Note that $R\cap x=R\cap V=R$. Then

$$y\in y\leftrightarrow y\in R\leftrightarrow y\notin y,$$

contradiction. □

This simple but crucial theorem leads to the distinction:

Definition 23. *Let A be a term. Then A is a* proper class *iff $A\notin V$.*

Set theory deals with sets and proper classes. Sets are the favoured objects of set theory, the axiom mainly state favorable properties of sets and set existence. Sometimes one says that a term A *exists* if $A\in V$. The intention of set theory is to construe important mathematical classes like the collection of natural and real numbers as sets so that they can be treated set-theoretically. ZERMELO observed that this is possible by requiring some set existences together with the *restricted* separation principle.

Exercise 6. Show that the class $\{\{x\}|x\in V\}$ of *singletons* is a proper class.

4.9 Power Sets

The *power set axiom* in class term notation is

$$\forall x\,\mathcal{P}(x)\in V.$$

The power set axiom yields the existence of function spaces.

Definition 24. *Let A,B be terms. Then*

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

is the cartesian product *of A and B.*

Exercise 7.

By the specific implementation of KURATOWSKI ordered pairs:

Lemma 25. $A\times B\subseteq\mathcal{P}(\mathcal{P}(A\cup B))$.

Proof. Let $(a,b)\in A\times B$. Then

$$\begin{array}{rcl} a,b & \in & A\cup B \\ \{a\},\{a,b\} & \subseteq & A\cup B \\ \{a\},\{a,b\} & \in & \mathcal{P}(A\cup B) \\ (a,b)=\{\{a\},\{a,b\}\} & \subseteq & \mathcal{P}(A\cup B) \\ (a,b)=\{\{a\},\{a,b\}\} & \in & \mathcal{P}(\mathcal{P}(A\cup B)) \end{array}$$

□

Theorem 26.

a) $\forall x,y\ x\times y\in V$.

b) $\forall x,y\ {}^xy\in V$.

Proof. Let x,y be sets. a) Using the axioms of pairing, union, and power sets, $\mathcal{P}(\mathcal{P}(x\cup y))\in V$. By the previous lemma and the axiom schema of separation,

$$x\times y=(x\times y)\cap\mathcal{P}(\mathcal{P}(x\cup y))\in V.$$

b) ${}^xy\subseteq\mathcal{P}(x\times y)$ since a function $f\colon x\to y$ is a subset of $x\times y$. By the separation schema,

$${}^xy={}^xy\cap\mathcal{P}(x\times y)\in V.$$

□

Note that to "find" the sets in this theorem one has to apply the power set operation repeatedly. We shall see that the universe of all sets can be obtained by iterating the power set operation.

The power set axiom leads to higher *cardinalities*. The theory of cardinalities will be developed later, but we can already prove CANTOR's theorem:

Theorem 27. *Let* $x\in V$.

a) There is an injective map $f\colon x\to\mathcal{P}(x)$.

b) There does not exist an injective map $g\colon\mathcal{P}(x)\to x$.

Proof. a) Define the map $f\colon x\to\mathcal{P}(x)$ by $u\mapsto\{u\}$. This is a set since

$$f=\{(u,\{u\})|u\in x\}\subseteq x\times\mathcal{P}(x)\in V.$$

f is injective: let $u,u'\in x$, $u\neq u'$. By extensionality,

$$f(u)=\{u\}\neq\{u'\}=f(u').$$

b) Assume there were an injective map $g\colon\mathcal{P}(x)\to x$. Define the CANTORean set

$$c=\{u|u\in x\wedge u\notin g^{-1}(u)\}\in P(x)$$

similar to the class R in RUSSELL's paradox.

Let $u_0=g(c)$. Then $g^{-1}(u_0)=c$ and

$$u_0\in c\leftrightarrow u_0\notin g^{-1}(u_0)=c.$$

Contradiction. □

4.10 Replacement

If every element of a set is definably *replaced* by another set, the result is a set again. The *schema of replacement* postulates for every term F:

$$F \text{ is a function} \to\forall x F[x]\in V.$$

Lemma 28. *The replacement schema implies the separation schema.*

Proof. Let A be a term and $x\in V$.
Case 1. $A\cap x=\emptyset$. Then $A\cap x\in V$ by the axiom of set existence.
Case 2. $A\cap x\neq\emptyset$. Take $u_0\in A\cap x$. Define a map $F\colon x\rightarrow x$ by

$$F(u)=\begin{cases} u\,, \text{ if } u\in A\cap x \\ u_0\,, \text{ else}\end{cases}$$

Then by replacement

$$A\cap x=F[x]\in V$$

as required. □

4.11 Infinity

All the axioms so far can be realized in a domain of finite sets, see exercise ???. The true power of set theory is set free by postulating the existence of *one* infinite set and continuing to assume the axioms. The *axiom of infinity* expresses that the set of "natural numbers" exists. To this end, some "number-theoretic" notions are defined.

Definition 29.

a) $0:=\emptyset$ *is the number* zero.

b) *For any term* t, $t+1:=t\cup\{t\}$ *is the* successor *of* t.

These notions are reasonable in the later formalization of the natural numbers. The axiom of infinity postulates the existence of a set which contains 0 and is closed under successors

$$\exists x\,(0\in x\wedge\forall n\in x\;n+1\in x).$$

Intuitively this says that there is a set which contains all natural numbers. Let us define set-theoretic analogues of the standard natural numbers:

Definition 30. *Define*

a) $1:=0+1$;

b) $2:=1+1$;

c) $3:=2+1$; ...

From the context it will be clear, whether "3", say, is meant to be the standard number "three" or the set theoretical object

$$\begin{aligned} 3 &= 2\cup\{2\} \\ &= (1+1)\cup\{1+1\} \\ &= (\{\emptyset\}\cup\{\{\emptyset\}\})\cup\{\{\emptyset\}\cup\{\{\emptyset\}\}\} \\ &= \{\emptyset,\{\emptyset\},\{\emptyset\}\cup\{\{\emptyset\}\}\}. \end{aligned}$$

The set-theoretic axioms will ensure that this interpretation of "three" has the important number-theoretic properties of "three".

4.12 Foundation

The *axiom schema of foundation* provides structural information about the set theoretic universe V. It can be reformulated by postulating, for any term A:

$$A\neq\emptyset\rightarrow\exists x\in A\;A\cap x=\emptyset.$$

Viewing $\in$ as some kind of order relation this means that every non-empty class has an $\in$-minimal element $x\in A$ such that the $\in$-predecessors of x are not in A. Foundation excludes circles in the $\in$-relation:

Lemma 31. *Let n be a natural number $\geqslant 1$. Then there are* no $x_0, \ldots, x_{n-1}$ *such that*

$$x_0 \in x_1 \in \ldots \in x_{n-1} \in x_0 .$$

Proof. Assume not and let $x_0 \in x_1 \in \ldots \in x_{n-1} \in x_0$. Let

$$A = \{x_0, \ldots, x_{n-1}\}.$$

$A \neq \emptyset$ since $n \geqslant 1$. By foundation take $x \in A$ such that $A \cap x = \emptyset$.
Case 1. $x = x_0$. Then $x_{n-1} \in A \cap x = \emptyset$, contradiction.
Case 2. $x = x_i$, $i > 0$. Then $x_{i-1} \in A \cap x = \emptyset$, contradiction. □

Exercise 8. Show that $x \neq x + 1$.

Exercise 9. Show that the successor function $x \mapsto x + 1$ is injective.

Exercise 10. Show that the term $\{x, \{x, y\}\}$ may be taken as an ordered pair of x and y.

Theorem 32. *The foundation scheme is equivalent to the following,* PEANO*-type, induction scheme: for every term B postulate*

$$\forall x \, (x \subseteq B \rightarrow x \in B) \rightarrow B = V.$$

This says that if a "property" B is inherited by x if all elements of x have the property B, then every set has the property B.

Proof. ($\rightarrow$) Assume B were a term which did not satisfy the induction principle:

$$\forall x \, (x \subseteq B \rightarrow x \in B) \text{ and } B \neq V.$$

Set $A = V \setminus B \neq \emptyset$. By foundation take $x \in A$ such that $A \cap x = \emptyset$. Then

$$u \in x \rightarrow u \notin A \rightarrow u \in B,$$

i.e., $x \subseteq B$. By assumption, B is inherited by x: $x \in B$. But then $x \notin A$, contradiction.
($\leftarrow$) Assume A were a term which did not satisfy the foundation scheme:

$$A \neq \emptyset \text{ and } \forall x \in A \; A \cap x \neq \emptyset.$$

Set $B = V \setminus A$. Consider $x \subseteq B$. Then $A \cap x = \emptyset$. By assumption, $x \notin A$ and $x \in B$. Thus $\forall x \, (x \subseteq B \rightarrow x \in B)$. The induction principle implies that $B = V$. Then $A = \emptyset$, contradiction. □

This proof shows, that the induction principle is basically an equivalent formulation of the foundation principle. The $\in$-relation is taken as some binary relation without reference to specific properties of this relation. This leads to:

Exercise 11. A relation R on a domain D is called *wellfounded*, iff for all terms A

$$\emptyset \neq A \wedge A \subseteq D \rightarrow \exists x \in A \; A \cap \{y \mid yRx\} = \emptyset.$$

Formulate and prove a principle for R-induction on D which coressponds to the assumption that R is wellfounded on D.

4.13 Set Theoretic Axiom Schemas

Note that the axiom system introduced is an infinite informal *set* of axioms. It seems unavoidable that we have to go back to some previously given set notions to be able to define the collection of set theoretical axioms - another example of the frequent circularity in foundational theories.

Definition 33. *The system* ZF *of the* ZERMELO-FRAENKEL axioms of set theory *consists of the following axioms:*

a) *The* set existence axiom (Ex)*:*

$$\exists x \forall y \neg y \in x$$

- *there is a set without elements, the* empty set.

b) *The* axiom of extensionality (Ext)*:*

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

- a set is determined by its elements, sets having the same elements are identical.

c) *The* pairing axiom (Pair)*:*

$$\forall x \forall y \exists z \forall w\, (u \in z \leftrightarrow u = x \vee u = y).$$

- z is the unordered pair of x and y.

d) *The* union axiom (Union)*:*

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists w (w \in x \wedge z \in w))$$

- y is the union of all elements of x.

e) *The* separation schema (Sep) *postulates for every $\in$-formula $\varphi(z, x_1, \ldots, x_n)$:*

$$\forall x_1 \ldots \forall x_n \forall x \exists y \forall z\, (z \in y \leftrightarrow z \in x \wedge \varphi(z, x_1, \ldots, x_n))$$

- this is an infinite scheme of axioms, the set z consists of all elements of x which satisfy φ.

f) *The* powerset axiom (Pow)*:*

$$\forall x \exists y \forall z (z \in y \leftrightarrow \forall w (w \in z \rightarrow w \in x))$$

- y consists of all subsets of x.

g) *The* replacement schema (Rep) *postulates for every $\in$-formula $\varphi(x, y, x_1, \ldots, x_n)$:*

$$\forall x_1 \ldots \forall x_n (\forall x \forall y \forall y' ((\varphi(x, y, x_1, \ldots, x_n) \wedge \varphi(x, y', x_1, \ldots, x_n)) \rightarrow y = y') \rightarrow \\ \forall u \exists v \forall y\, (y \in v \leftrightarrow \exists x (x \in u \wedge \varphi(x, y, x_1, \ldots, x_n))))$$

- v is the image of u under the map defined by φ.

h) *The* axiom of infinity (Inf)*:*

$$\exists x (\exists y\, (y \in x \wedge \forall z \neg z \in y) \wedge \forall y (y \in x \rightarrow \exists z (z \in x \wedge \forall w (w \in z \leftrightarrow w \in y \vee w = y))))$$

- by the closure properties of x, x has to be infinite.

i) *The* foundation schema (Found) *postulates for every $\in$-formula $\varphi(x, x_1, \ldots, x_n)$:*

$$\forall x_1 \ldots \forall x_n (\exists x \varphi(x, x_1, \ldots, x_n) \rightarrow \exists x (\varphi(x, x_1, \ldots, x_n) \wedge \forall x' (x' \in x \rightarrow \neg \varphi(x', x_1, \ldots, x_n))))$$

- if φ is satisfiable then there are $\in$-minimal elements satisfying φ.

4.14 ZF in Class Notation

Using class terms, the ZF can be formulated concisely:

Theorem 34. *The* ZF *axioms are equivalent to the following system; we take all free variables of the axioms to be universally quantified:*

a) *Ex:* $\emptyset \in V$.

b) *Ext:* $x \subseteq y \wedge y \subseteq x \rightarrow x = y$.

c) *Pair:* $\{x, y\} \in V$.

d) *Union:* $\bigcup x \in V$.

e) *Sep:* $A \cap x \in V$.

f) *Pow:* $\mathcal{P}(x) \in V$.

g) *Rep:* F *is a function* $\rightarrow F[x] \in V$.

h) *Inf:* $\exists x\, (0 \in x \wedge \forall n \in x\; n + 1 \in x)$.

i) *Found:* $A \neq \emptyset \rightarrow \exists x \in A\; A \cap x = \emptyset$.

This axiom system can be used as a foundation for all of mathematics. Axiomatic set theory considers various axiom systems of set theory.

Definition 35. *The axiom system* ZF^- *consists of the* ZF*-axioms except the power set axiom. The system* EML *("elementary set theory") consists of the axioms* Ex*,* Ext*,* Pair*, and* Union*.*

Exercise 12. Consider the axiom system HF consisting of the axioms of EML together with the induction principle: for every term B postulate

$$\forall x, y\,(x \subseteq B \wedge y \in B \rightarrow x \cup \{y\} \in B) \rightarrow B = V.$$

Show that every axiom of ZF except Inf is provable in HF, and that HF proves the *negation* of Inf (HF axiomatizes the **h**eriditarily **f**inite sets, i.e., those sets such that the set itself and all its iterated elements are finite).

5 Ordinal Numbers

We had defined some "natural numbers" in set theory. Recall that

$$\begin{aligned} 0 &= \emptyset \\ 1 &= 0+1 = 0 \cup \{0\} = \{0\} \\ 2 &= 1+1 = 1 \cup \{1\} = \{0,1\} \\ 3 &= 2+1 = 2 \cup \{2\} = \{0,1,2\} \\ &\vdots \end{aligned}$$

We would then like to have $\mathbb{N} = \{0, 1, 2, 3, ...\}$. To obtain a set theoretic formalization of numbers we note some properties of the informal presentation:

1. "Numbers" are ordered by the $\in$-relation:

   $$m < n \text{ iff } m \in n.$$

   E.g., $1 \in 3$ but not $3 \in 1$.

2. On each "number", the $\in$-relation is a *strict linear order*: $3 = \{0, 1, 2\}$ is strictly linearly ordered by $\in$.

3. "Numbers" are "complete" with respect to smaller "numbers"

   $$i < j < m \rightarrow i \in m.$$

   This can be written with the $\in$-relation as

   $$i \in j \in m \rightarrow i \in m.$$

Definition 36.

a) *A is* transitive, $\mathrm{Trans}(A)$*, iff* $\forall y \in A \forall x \in y\, x \in A$.

b) *x is an* ordinal (number), $\mathrm{Ord}(x)$*, if* $\mathrm{Trans}(x) \wedge \forall y \in x\, \mathrm{Trans}(y)$.

c) *Let* $\mathrm{Ord} := \{x | \mathrm{Ord}(x)\}$ *be the class of all ordinal numbers.*

We shall use small greek letter $\alpha, \beta, ...$ as variables for ordinals. So $\exists \alpha \varphi$ stands for $\exists \alpha \in \mathrm{Ord}\ \varphi$, and $\{\alpha | \varphi\}$ for $\{\alpha | \mathrm{Ord}(\alpha) \wedge \varphi\}$.

Exercise 13. Show that arbitrary unions and intersections of transitive sets are again transitive.

We shall see that the ordinals extend the standard natural numbers. Ordinals are particularly adequate for enumerating infinite sets.

Theorem 37.

a) $0 \in \mathrm{Ord}$.

b) $\forall \alpha\ \alpha + 1 \in \mathrm{Ord}$.

Proof. a) Trans($\emptyset$) since formulas of the form $\forall y \in \emptyset ...$ are tautologously true. Similarly $\forall y \in \emptyset$ Trans(y).
b) Assume $\alpha \in \mathrm{Ord}$.
(1) Trans($\alpha + 1$).
Proof. Let $u \in v \in \alpha + 1 = \alpha \cup \{\alpha\}$.
Case 1. $v \in \alpha$. Then $u \in \alpha \subseteq \alpha + 1$, since α is transitive.
Case 2. $v = \alpha$. Then $u \in \alpha \subseteq \alpha + 1$. *qed*(1)
(2) $\forall y \in \alpha + 1\, \mathrm{Trans}(y)$.
Proof. Let $y \in \alpha + 1 = \alpha \cup \{\alpha\}$.
Case 1. $y \in \alpha$. Then Trans(y) since α is an ordinal.
Case 2. $y = \alpha$. Then Trans(y) since α is an ordinal. □

Exercise 14.

a) Let $A \subseteq \mathrm{Ord}$ be a term, $A \neq \emptyset$. Then $\bigcap A \in \mathrm{Ord}$.

b) Let $x \subseteq \mathrm{Ord}$ be a set. Then $\bigcup x \in \mathrm{Ord}$.

Theorem 38. Trans(Ord).

Proof. This follows immediately from the transitivity definition of Ord. □

Exercise 15. Show that Ord is a proper class. (Hint: if $\mathrm{Ord} \in V$ then $\mathrm{Ord} \in \mathrm{Ord}$.)

Theorem 39. *The class* Ord *is strictly linearly ordered by* $\in$, *i.e.,*

a) $\forall \alpha, \beta, \gamma\, (\alpha \in \beta \wedge \beta \in \gamma \rightarrow \alpha \in \gamma)$.

b) $\forall \alpha\, \alpha \notin \alpha$.

c) $\forall \alpha, \beta\, (\alpha \in \beta \vee \alpha = \beta \vee \beta \in \alpha)$.

Proof. a) Let $\alpha, \beta, \gamma \in \mathrm{Ord}$ and $\alpha \in \beta \wedge \beta \in \gamma$. Then γ is transitive, and so $\alpha \in \gamma$.
b) follows immediately from the non-circularity of the $\in$-relation.
c) Assume that there are "incomparable" ordinals. By the foundation schema choose $\alpha_0 \in \mathrm{Ord}$ $\in$-minimal such that $\exists \beta \neg(\alpha_0 \in \beta \vee \alpha_0 = \beta \vee \beta \in \alpha_0)$. Again, choose $\beta_0 \in \mathrm{Ord}$ $\in$-minimal such that $\neg(\alpha_0 \in \beta_0 \vee \alpha_0 = \beta_0 \vee \beta_0 \in \alpha_0)$. We obtain a contradiction by showing that $\alpha_0 = \beta_0$:

Let $\alpha \in \alpha_0$. By the $\in$-minimality of α_0, α is comparable with β_0: $\alpha \in \beta_0 \vee \alpha = \beta_0 \vee \beta_0 \in \alpha$. If $\alpha = \beta_0$ then $\beta_0 \in \alpha_0$ and α_0, β_0 would be comparable, contradiction. If $\beta_0 \in \alpha$ then $\beta_0 \in \alpha_0$ by the transitivity of α_0 and again α_0, β_0 would be comparable, contradiction. Hence $\alpha \in \beta_0$.

For the converse let $\beta \in \beta_0$. By the $\in$-minimality of β_0, β is comparable with α_0: $\beta \in \alpha_0 \vee \beta = \alpha_0 \vee \alpha_0 \in \beta$. If $\beta = \alpha_0$ then $\alpha_0 \in \beta_0$ and α_0, β_0 would be comparable, contradiction. If $\alpha_0 \in \beta$ then $\alpha_0 \in \beta_0$ by the transitivity of β_0 and again α_0, β_0 would be comparable, contradiction. Hence $\beta \in \alpha_0$.

But then $\alpha_0 = \beta_0$ contrary to the choice of β_0. □

Definition 40. *Let* $< : = \in \cap (\mathrm{Ord} \times \mathrm{Ord}) = \{(\alpha, \beta) | \alpha \in \beta\}$ *be the natural strict linear ordering of* Ord *by the* $\in$*-relation.*

Theorem 41. *Let* $\alpha \in \mathrm{Ord}$. *Then* $\alpha + 1$ *is the immediate successor of* α *in the* $\in$*-relation:*

a) $\alpha < \alpha + 1$;

b) if $\beta < \alpha + 1$, *then* $\beta = \alpha$ *or* $\beta < \alpha$.

Definition 42. *Let* α *be an ordinal.* α *is a* successor ordinal, $\mathrm{Succ}(\alpha)$, *iff* $\exists \beta\, \alpha = \beta + 1$. α *is a limit ordinal,* $\mathrm{Lim}(\alpha)$, *iff* $\alpha \neq 0$ *and* α *is not a successor ordinal. Also let*

$$\mathrm{Succ} := \{\alpha | \mathrm{Succ}(\alpha)\} \text{ and } \mathrm{Lim} := \{\alpha | \mathrm{Lim}(\alpha)\}.$$

The existence of limit ordinals will be discussed together with the formalization of the natural numbers.

5.1 Induction

Ordinals satisfy an *induction theorem* which generalizes *complete induction* on the integers:

Theorem 43. *Let $\varphi(x, v_0, \ldots, v_{n-1})$ be an $\in$-formula and $x_0, \ldots, x_{n-1} \in V$. Assume that the property $\varphi(x, x_0, \ldots, x_{n-1})$ is* inductive, *i.e.,*

$$\forall\alpha(\forall\beta\in\alpha\ \varphi(\beta, x_0, \ldots, x_{n-1}) \to \varphi(\alpha, x_0, \ldots, x_{n-1})).$$

Then φ holds for all ordinals:

$$\forall\alpha\, \varphi(\alpha, x_0, \ldots, x_{n-1}).$$

Proof. It suffices to show that

$$B = \{x|x \in \mathrm{Ord} \to \varphi(x, x_0, \ldots, x_{n-1})\} = V.$$

Theorem 32 implies

$$\forall x\, (x \subseteq B \to x \in B) \to B = V$$

and it suffices to show

$$\forall x\, (x \subseteq B \to x \in B).$$

Consider $x \subseteq B$. If $x \notin \mathrm{Ord}$ then $x \in B$. So assume $x \in \mathrm{Ord}$. For $\beta \in x$ we have $\beta \in B$, $\beta \in \mathrm{Ord}$, and so $\varphi(\beta, x_0, \ldots, x_{n-1})$. By the inductivity of φ we get $\varphi(x, x_0, \ldots, x_{n-1})$ and again $x \in B$. □

Induction can be formulated in various forms:

Exercise 16. Prove the following transfinite induction principle: Let $\varphi(x) = \varphi(x, v_0, \ldots, v_{n-1})$ be an $\in$-formula and $x_0, \ldots, x_{n-1} \in V$. Assume

a) $\varphi(0)$ (the initial case),

b) $\forall\alpha\, (\varphi(\alpha) \to \varphi(\alpha+1))$ (the successor step),

c) $\forall\lambda\in\mathrm{Lim}\ (\forall\alpha < \lambda\, \varphi(\alpha) \to \varphi(\lambda))$ (the limit step).

Then $\forall\alpha\, \varphi(\alpha)$.

5.2 Natural Numbers

We have $0, 1, \ldots \in \mathrm{Ord}$. We shall now define and study the set of *natural numbers/integers* within set theory. Recall the axiom of infinity:

$$\exists x\ (0 \in x \wedge \forall u \in x\ u + 1 \in x).$$

The set of natural numbers should be the $\subseteq$-smallest such x.

Definition 44. *Let $\omega = \bigcap\ \{x|0 \in x \wedge \forall u \in x\ u + 1 \in x\}$ be the* set of natural numbers. *Sometimes we write $\mathbb{N}$ instead of ω.*

Theorem 45.

a) $\omega \in V$.

b) $\omega \subseteq \mathrm{Ord}$.

c) $(\omega, 0, +1)$ *satisfy the* second order PEANO axiom, *i.e.,*

$$\forall x \subseteq \omega\, (0 \in x \wedge \forall n \in x\ n + 1 \in x \to x = \omega).$$

d) $\omega \in \mathrm{Ord}$.

e) ω *is a limit ordinal.*

Proof. a) By the axiom of infinity take a set x_0 such that

$$0 \in x_0 \wedge \forall u \in x_0\ u + 1 \in x_0.$$

Then

$$\omega = \bigcap\ \{x|0 \in x \wedge \forall u \in x\ u + 1 \in x\} = x_0 \cap \bigcap\ \{x|0 \in x \wedge \forall u \in x\ u + 1 \in x\} \in V$$

by the separation schema.
b) By a), $\omega\cap\mathrm{Ord}\in V$. Obviously $0\in\omega\cap\mathrm{Ord}\wedge\forall u\in\omega\cap\mathrm{Ord}\ u+1\in\omega\cap\mathrm{Ord}$. So $\omega\cap\mathrm{Ord}$ is one factor of the intersection in the definition of ω and so $\omega\subseteq\omega\cap\mathrm{Ord}$. Hence $\omega\subseteq\mathrm{Ord}$.
c) Let $x\subseteq\omega$ and $0\in x\wedge\forall u\in x\ u+1\in x$. Then x is one factor of the intersection in the definition of ω and so $\omega\subseteq x$. This implies $x=\omega$.
d) By b), every element of ω is transitive and it suffices to show that ω is transitive. Let

$$x=\{n|n\in\omega\wedge\forall m\in n\ m\in\omega\}\subseteq\omega.$$

We show that the hypothesis of c) holds for x. $0\in x$ is trivial. Let $u\in x$. Then $u+1\in\omega$. Let $m\in u+1$. If $m\in u$ then $m\in\omega$ by the assumption that $u\in x$. If $m=u$ then $m\in x\subseteq\omega$. Hence $u+1\in x$ and $\forall u\in x\ u+1\in x$. By b), $x=\omega$. So $\forall n\in\omega\, n\in x$, i.e.,

$$\forall n\in\omega\forall m\in n\ m\in\omega.$$

e) Of course $\omega\neq 0$. Assume for a contradiction that ω is a successor ordinal, say $\omega=\alpha+1$. Then $\alpha\in\omega$. Since ω is closed under the $+1$-operation, $\omega=\alpha+1\in\omega$. Contradiction. □

Thus the axiom of infinity implies the existence of the set of natural numbers, which is also the smallest limit ordinal. The axiom of infinity can now be reformulated equivalently as:
h) Inf: $\omega\in V$.

5.3 Recursion

Recursion, often called induction, over the natural numbers is a ubiquitous method for defining mathematical object. We prove the following *recursion theorem* for ordinals.

Theorem 46. *Let $G: V\to V$. Then there is a canonical class term F, given by the subsequent proof, such that*

$$F:\mathrm{Ord}\to V \text{ and } \forall\alpha\ F(\alpha)=G(F\restriction\alpha).$$

We then say that F is defined recursively *(over the ordinals) by the* recursion rule *G. F is unique in the sense that if another term F' satisfies*

$$F':\mathrm{Ord}\to V \text{ and } \forall\alpha\ F'(\alpha)=G(F'\restriction\alpha)$$

then $F=F'$.

Proof. We say that $H:\mathrm{dom}(H)\to V$ is *G-recursive* if

$$\mathrm{dom}(H)\subseteq\mathrm{Ord}, \mathrm{dom}(H) \text{ is transitive, and } \forall\alpha\in\mathrm{dom}(H)\ H(\alpha)=G(H\restriction\alpha).$$

(1) Let H,H' be G-recursive. Then H,H' are *compatible*, i.e., $\forall\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\ H(\alpha)=H'(\alpha)$.
Proof. We want to show that

$$\forall\alpha\in\mathrm{Ord}\ (\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\to H(\alpha)=H'(\alpha)).$$

By the induction theorem it suffices to show that $\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\to H(\alpha)=H'(\alpha)$ is inductive, i.e.,

$$\forall\alpha\in\mathrm{Ord}\ (\forall y\in\alpha\ (y\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\to H(y)=H'(y))\to(\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\to H(\alpha)=H'(\alpha))).$$

So let $\alpha\in\mathrm{Ord}$ and $\forall y\in\alpha\ (y\in\mathrm{dom}(H)\cap\mathrm{dom}(H')\to H(y)=H'(y))$. Let $\alpha\in\mathrm{dom}(H)\cap\mathrm{dom}(H')$. Since $\mathrm{dom}(H)$ and $\mathrm{dom}(H')$ are transitive, $\alpha\subseteq\mathrm{dom}(H)$ and $\alpha\subseteq\mathrm{dom}(H')$. By assumption

$$\forall y\in\alpha\ H(y)=H'(y).$$

Hence $H\restriction\alpha=H'\restriction\alpha$. Then

$$H(\alpha)=G(H\restriction\alpha)=G(H'\restriction\alpha)=H'(\alpha).$$

qed(1)

Let

$$F := \bigcup \{f \mid f \text{ is } G\text{-recursive}\}.$$

be the union of the class of all *approximations* to the desired function F.
(2) F is G-recursive.
Proof. By (1), F is a function. Its domain $\mathrm{dom}(F)$ is the union of transitive classes of ordinals and hence $\mathrm{dom}(F) \subseteq \mathrm{Ord}$ is transitive.

Let $\alpha \in \mathrm{dom}(F)$. Take some G-recursive function$f$ such that $\alpha \in \mathrm{dom}(f)$. Since $\mathrm{dom}(f)$ is transitive, we have

$$\alpha \subseteq \mathrm{dom}(f) \subseteq \mathrm{dom}(F).$$

Moreover

$$F(\alpha) = f(\alpha) = G(f \upharpoonright \alpha) = G(F \upharpoonright \alpha).$$

qed(2)
(3) $\forall \alpha\ \alpha \in \mathrm{dom}(F)$.
Proof. By induction on the ordinals. We have to show that $\alpha \in \mathrm{dom}(F)$ is inductive in the variable α. So let $\alpha \in \mathrm{Ord}$ and $\forall y \in \alpha\ y \in \mathrm{dom}(F)$. Hence $\alpha \subseteq \mathrm{dom}(F)$. Let

$$f = F \upharpoonright \alpha \cup \{(\alpha, G(F \upharpoonright \alpha))\}.$$

f is a function with $\mathrm{dom}(f) = \alpha + 1 \in \mathrm{Ord}$. Let $\alpha' < \alpha + 1$. If $\alpha' < \alpha$ then

$$f(\alpha') = F(\alpha') = G(F \upharpoonright \alpha') = G(f \upharpoonright \alpha').$$

if $\alpha' = \alpha$ then also

$$f(\alpha') = f(\alpha) = G(F \upharpoonright \alpha) = G(f \upharpoonright \alpha) = G(f \upharpoonright \alpha').$$

Hence f is G-recursive and $\alpha \in \mathrm{dom}(f) \subseteq \mathrm{dom}(F)$. *qed*(3)

The extensional uniqueness of F follows from (1) □

Theorem 47. *Let $a_0 \in V$, $G_{\mathrm{succ}}: \mathrm{Ord} \times V \to V$, and $G_{\lim}: \mathrm{Ord} \times V \to V$. Then there is a canonically defined class term $F: \mathrm{Ord} \to V$ such that*

a) $F(0) = a_0$ *;*

b) $\forall \alpha\, F(\alpha + 1) = G_{\mathrm{succ}}(\alpha, F(\alpha))$*;*

c) $\forall \lambda \in \mathrm{Lim}\ F(\lambda) = G_{\lim}(\lambda, F \upharpoonright \lambda)$.

Again F is unique in the sense that if some F' also satisfies a)-c) then $F = F'$.

We say that F is recursively defined *by the properties a)-c).*

Proof. We incorporate a_0, G_{succ}, and $G_{\lim}$ into a single recursion rule $G: V \to V$,

$$G(f) = \begin{cases} a_0 \text{ , if } f = \emptyset, \\ G_{\mathrm{succ}}(\alpha, f(\alpha)) \text{ , if } f: \alpha + 1 \to V, \\ G_{\lim}(\lambda, f) \text{ , if } f: \lambda \to V \text{ and } \mathrm{Lim}(\lambda), \\ \emptyset \text{ , else.} \end{cases}$$

Then the term $F: \mathrm{Ord} \to V$ defined recursively by the recursion rule G satisfies the theorem. □

In many cases, the *limit rule* will just require to form the union of the previous values so that

$$F(\lambda) = \bigcup_{\alpha < \lambda} F(\alpha).$$

Such recursions are called *continuous* (at limits).

5.4 Ordinal Arithmetic

We extend the recursion rules of standard integer arithmetic continuously to obtain transfinite version of the arithmetic operations. The initial operation of ordinal arithmetic is the +1-operation defined before. Ordinal arithmetic satisfies some but not all laws of integer arithmetic.

Definition 48. *Define* ordinal addition $+: \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ *recursively by*

$$\begin{aligned} \delta + 0 &= \delta \\ \delta + (\alpha + 1) &= (\delta + \alpha) + 1 \\ \delta + \lambda &= \bigcup_{\alpha < \lambda} (\delta + \alpha) \text{ , for limit ordinals } \lambda \end{aligned}$$

Definition 49. *Define* ordinal multiplication $\cdot : \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ *recursively by*

$$\begin{aligned} \delta \cdot 0 &= 0 \\ \delta \cdot (\alpha + 1) &= (\delta \cdot \alpha) + \delta \\ \delta \cdot \lambda &= \bigcup_{\alpha < \lambda} (\delta \cdot \alpha) \text{ , for limit ordinals } \lambda \end{aligned}$$

Definition 50. *Define* ordinal exponentiation $\_^{-} : \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ *recursively by*

$$\begin{aligned} \delta^0 &= 1 \\ \delta^{\alpha+1} &= \delta^\alpha \cdot \delta \\ \delta^\lambda &= \bigcup_{\alpha < \lambda} \delta^\alpha \text{ , for limit ordinals } \lambda \end{aligned}$$

Exercise 17. Explore which of the standard *ring axioms* hold for the ordinals with addition and multiplication. Give proofs and counterexamples.

Exercise 18. Show that for any ordinal α , $\alpha + \omega$ is a limit ordinal. Use this to show that the class Lim of all limit ordinals is a proper class.

6 Number Systems

We are now able to give set-theoretic formalizations of the standard number systems with their arithmetic operations.

6.1 Natural Numbers

Definition 51. *The structure*

$$\mathbb{N} := (\omega, + \upharpoonright (\omega \times \omega), \cdot \upharpoonright (\omega \times \omega), < \upharpoonright (\omega \times \omega), 0, 1)$$

is called the structure of natural numbers, *or* arithmetic. *We sometimes denote this structure by*

$$\mathbb{N} := (\omega, +, \cdot, <, 0, 1).$$

$\mathbb{N}$ is an adequate formalization of arithmetic within set theory since $\mathbb{N}$ satisfies all standard arithmetical axioms.

Exercise 19. Prove:

a) $+[\omega \times \omega] := \{m + n | m \in \omega \wedge n \in \omega\} \subseteq \omega$.

b) $\cdot [\omega \times \omega] := \{m \cdot n | m \in \omega \wedge n \in \omega\} \subseteq \omega$.

c) Addition and multiplication are commutative on ω .

d) Addition and multiplication satisfy the usual monotonicity laws with respect to $<$.

Definition 52. *We define the structure*

$$\mathbb{Z} := (\mathbb{Z}, +^{\mathbb{Z}}, \cdot^{\mathbb{Z}}, <^{\mathbb{Z}}, 0^{\mathbb{Z}}, 1^{\mathbb{Z}})$$

of integers *as follows:*

a) Define an equivalence relation $\approx$ *on* $\mathbb{N} \times \mathbb{N}$ *by*

$$(a, b) \approx (a', b') \text{ iff } a + b' = a' + b.$$

b) *Let* $a - b := [(a,b)]_{\approx}$ *be the equivalence class of* (a,b) *in* $\approx$*. Note that every* $a - b$ *is a set.*

c) *Let* $\mathbb{Z} := \{a - b | a \in \mathbb{N} \wedge b \in \mathbb{N}\}$ *be the set of* integers.

d) *Define the* integer addition $+^{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *by*

$$(a - b) +^{\mathbb{Z}} (a' - b') := (a + a') - (b + b').$$

e) *Define the* integer multiplication $\cdot^{\mathbb{Z}} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *by*

$$(a - b) \cdot^{\mathbb{Z}} (a' - b') := (a \cdot a' + b \cdot b') - (a \cdot b' + a' \cdot b).$$

f) *Define the strict linear order* $<^{\mathbb{Z}}$ *on* $\mathbb{Z}$ *by*

$$(a - b) <^{\mathbb{Z}} (a' - b') \text{ iff } a + b' < a' + b.$$

g) *Let* $0^{\mathbb{Z}} := 0 - 0$ *and* $1^{\mathbb{Z}} := 1 - 0$.

Exercise 20. Check that the above definitions are *sound*, i.e., that they do not depend on the choice of representatives of equivalence classes.

Exercise 21. Check that $\mathbb{Z}$ satisfies (a sufficient number) of the standard axioms for rings.

The structure $\mathbb{Z}$ extends the structure $\mathbb{N}$ in a natural and familiar way: define an injective map $e: \mathbb{N} \to \mathbb{Z}$ by

$$n \mapsto n - 0.$$

The embedding e is a *homomorphism*:

a) $e(0) = 0 - 0 = 0^{\mathbb{Z}}$ and $e(1) = 1 - 0 = 1^{\mathbb{Z}}$;

b) $e(m + n) = (m + n) - 0 = (m + n) - (0 + 0) = (m - 0) +^{\mathbb{Z}} (n - 0) = e(m) +^{\mathbb{Z}} e(n)$;

c) $e(m \cdot n) = (m \cdot n) - 0 = (m \cdot n + 0 \cdot 0) - (m \cdot 0 + n \cdot 0) = (m - 0) \cdot^{\mathbb{Z}} (n - 0) = e(m) \cdot^{\mathbb{Z}} e(n)$;

d) $m < n \leftrightarrow m + 0 < n + 0 \leftrightarrow (m - 0) <^{\mathbb{Z}} (n - 0) \leftrightarrow e(m) <^{\mathbb{Z}} e(n)$.

By this injective homomorphism, one may consider $\mathbb{N}$ as a *substructure* of $\mathbb{Z}$: $\mathbb{N} \subseteq \mathbb{Z}$.

6.2 Rational Numbers

Definition 53. *We define the structure*

$$\mathbb{Q}_0^+ := (\mathbb{Q}_0^+, +^{\mathbb{Q}}, \cdot^{\mathbb{Q}}, <^{\mathbb{Q}}, 0^{\mathbb{Q}}, 1^{\mathbb{Q}})$$

of non-negative rational numbers *as follows:*

a) *Define an equivalence relation* $\asymp$ *on* $\mathbb{N} \times (\mathbb{N} \setminus \{0\})$ *by*

$$(a,b) \asymp (a',b') \text{ iff } a \cdot b' = a' \cdot b.$$

b) *Let* $\frac{a}{b} := [(a,b)]_{\asymp}$ *be the equivalence class of* (a,b) *in* $\asymp$*. Note that* $\frac{a}{b}$ *is a set.*

c) *Let* $\mathbb{Q}_0^+ := \{\frac{a}{b} | a \in \mathbb{N} \wedge b \in (\mathbb{N} \setminus \{0\})\}$ *be the set of* non-negative rationals.

d) *Define the* rational addition $+^{\mathbb{Q}} : \mathbb{Q}_0^+ \times \mathbb{Q}_0^+ \to \mathbb{Q}_0^+$ *by*

$$\frac{a}{b} +^{\mathbb{Q}} \frac{a'}{b'} := \frac{a \cdot b' + a' \cdot b}{b \cdot b'}.$$

e) *Define the* rational multiplication $\cdot^{\mathbb{Q}} : \mathbb{Q}_0^+ \times \mathbb{Q}_0^+ \to \mathbb{Q}_0^+$ *by*

$$\frac{a}{b} \cdot^{\mathbb{Q}} \frac{a'}{b'} := \frac{a \cdot a'}{b \cdot b'}.$$

f) *Define the strict linear order* $<^{\mathbb{Q}}$ *on* $\mathbb{Q}_0^+$ *by*

$$\frac{a}{b} <^{\mathbb{Q}} \frac{a'}{b'} \text{ iff } a \cdot b' < a' \cdot b.$$

g) *Let* $0^{\mathbb{Q}} := \frac{0}{1}$ *and* $1^{\mathbb{Q}} := \frac{1}{1}$.

Again one can check the soundness of the definitions and the well-known laws of standard non-negative rational numbers. Also one may assume $\mathbb{N}$ to be embedded into $\mathbb{Q}_0^+$ as a substructure. The transfer from non-negative to *all* rationals, including negative rationals can be performed in analogy to the transfer from $\mathbb{N}$ to $\mathbb{Z}$.

Definition 54. *We define the structure*

$$\mathbb{Q} := (\mathbb{Q}, +^{\mathbb{Q}}, \cdot^{\mathbb{Q}}, <^{\mathbb{Q}}, 0^{\mathbb{Q}}, 1^{\mathbb{Q}})$$

of rational numbers *as follows:*

a) Define an equivalence relation $\approx$ *on* $\mathbb{Q}_0^+ \times \mathbb{Q}_0^+$ *by*

$$(p, q) \approx (p', q') \text{ iff } p + q' = p' + q.$$

b) Let $p - q := [(p, q)]_{\approx}$ *be the equivalence class of* (p, q) *in* $\approx$.

c) Let $\mathbb{Q} := \{p - q | p \in \mathbb{Q}_0^+ \wedge p \in \mathbb{Q}_0^+\}$ *be the set of* rationals.

Exercise 22. Continue the definition of the structure $\mathbb{Q}$ and prove the relevant properties.

6.3 Real Numbers

Definition 55. $r \subseteq \mathbb{Q}_0^+$ *is a* positive real number *if*

a) $\forall p \in r \forall q \in \mathbb{Q}_0^+ (q <^{\mathbb{Q}} p \rightarrow q \in r)$, *i.e., r is an initial segment of* $(\mathbb{Q}_0^+, <^{\mathbb{Q}})$;

b) $\forall p \in r \exists q \in r\, p <^{\mathbb{Q}} q$, *i.e., r is right-open in* $(\mathbb{Q}_0^+, <^{\mathbb{Q}})$;

c) $0 \in r \neq \mathbb{Q}_0^+$, *i.e., r is nonempty and bounded in* $(\mathbb{Q}_0^+, <^{\mathbb{Q}})$.

Definition 56. *We define the structure*

$$\mathbb{R}^+ := (\mathbb{R}^+, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, <^{\mathbb{R}}, 1^{\mathbb{R}})$$

of positive real numbers *as follows:*

a) Let $\mathbb{R}^+$ *be the set of* positive reals.

b) Define the real addition $+^{\mathbb{R}}: \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ *by*

$$r +^{\mathbb{R}} r' = \{p +^{\mathbb{Q}} p' | p \in r \wedge p' \in r'\}.$$

c) Define the real multiplication $\cdot^{\mathbb{R}}: \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ *by*

$$r \cdot^{\mathbb{R}} r' = \{p \cdot^{\mathbb{Q}} p' | p \in r \wedge p' \in r'\}.$$

d) Define the strict linear order $<^{\mathbb{R}}$ *on* $\mathbb{R}^+$ *by*

$$r <^{\mathbb{R}} r' \text{ iff } r \subseteq r' \wedge r \neq r'.$$

e) Let $1^{\mathbb{R}} := \{p \in \mathbb{Q}_0^+ | q <^{\mathbb{Q}} 1\}$.

We justify some details of the definition.

Lemma 57.

a) $\mathbb{R}^+ \in V$.

b) If $r, r' \in \mathbb{R}^+$ *then* $r +^{\mathbb{R}} r'$, $r \cdot^{\mathbb{R}} r' \in \mathbb{R}^+$.

c) $<^{\mathbb{R}}$ *is a strict linear order on* $\mathbb{R}^+$.

Proof. a) If $r \in \mathbb{R}^+$ then $r \subseteq \mathbb{Q}_0^+$ and $r \in \mathcal{P}(\mathbb{Q}_0^+)$. Thus $\mathbb{R}^+ \subseteq \mathcal{P}(\mathbb{Q}_0^+)$, and $\mathbb{R}^+$ is a set by the power set axiom and separation.
b) Let $r, r' \in \mathbb{R}^+$. We show that

$$r \cdot^{\mathbb{R}} r' = \{p \cdot^{\mathbb{Q}} p' | p \in r \wedge p' \in r'\} \in \mathbb{R}^+.$$

Obviously $r\cdot^{\mathbb{R}} r'\subseteq\mathbb{Q}_0^+$ is a non-empty bounded initial segment of $(\mathbb{Q}_0^+,<^{\mathbb{Q}})$.

Consider $p\in r\cdot^{\mathbb{R}} r'$, $q\in\mathbb{Q}_0^+$, $q<^{\mathbb{Q}} p$. Let $p=\frac{a}{b}\cdot^{\mathbb{Q}}\frac{a'}{b'}$ where $\frac{a}{b}\in r$ and $\frac{a'}{b'}\in r'$. Let $q=\frac{c}{d}$. Then $\frac{c}{d}=\frac{c\cdot b'}{d\cdot a'}\cdot^{\mathbb{Q}}\frac{a'}{b'}$, where

$$\frac{c\cdot b'}{d\cdot a'}=q\cdot^{\mathbb{Q}}\frac{b'}{a'}<^{\mathbb{Q}} p\cdot^{\mathbb{Q}}\frac{b'}{a'}=\frac{a}{b}\cdot^{\mathbb{Q}}\frac{a'}{b'}\cdot^{\mathbb{Q}}\frac{b'}{a'}=\frac{a}{b}\in r.$$

Hence $\frac{c\cdot b'}{d\cdot a'}\in r$ and

$$\frac{c}{d}=\frac{c\cdot b'}{d\cdot a'}\cdot^{\mathbb{Q}}\frac{a'}{b'}\in r\cdot^{\mathbb{R}} r'.$$

Similarly one can show that $r\cdot^{\mathbb{R}} r'$ is open on the right-hand side.

c) The transitivity of $<^{\mathbb{R}}$ follows from the transitivity of the relation $\subsetneqq$. To show that $<^{\mathbb{R}}$ is connex, consider $r,r'\in\mathbb{R}^+$, $r\neq r'$. Then r and r' are different subsets of $\mathbb{Q}_0^+$. Without loss of generality we may assume that there is some $p\in r'\setminus r$. We show that then $r<^{\mathbb{R}} r'$, i.e., $r\subsetneqq r'$. Consider $q\in r$. Since $p\notin r$ we have $p\not<^{\mathbb{Q}} q$ and $q\leqslant^{\mathbb{Q}} p$. Since r' is an initial segment of $\mathbb{Q}_0^+$, $q\in r'$. ☐

Exercise 23. Show that $(\mathbb{R}^+,\cdot^{\mathbb{R}},1^{\mathbb{R}})$ is a multiplicative group.

We can now construct the complete real line $\mathbb{R}$ from $\mathbb{R}^+$ just like we constructed $\mathbb{Z}$ from $\mathbb{N}$. Details are left to the reader. We can also proceed to define the structure $\mathbb{C}$ of complex numbers from $\mathbb{R}$.

Exercise 24. Formalize the structure $\mathbb{C}$ of complex numbers such that $\mathbb{R}\subseteq\mathbb{C}$.

6.4 Discussion

The constructions carried out in the previous subsections contained many arbitrary choices. One could, e.g., define rational numbers as *reduced* fractions instead of equivalence classes of fractions, ensure that the canonical embeddings of number systems are inclusions, etc. If such choices have been made in reasonable ways we obtain the following theorem, which contains everything one wants to know about the number systems. So the statements of the following theorem can be seen as first- and second-order axioms for these systems.

Theorem 58. *There are structures* $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},$ *and* $\mathbb{C}$ *with the following properties:*

a) *the domains of these structures which are also denoted by* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, *and* $\mathbb{C}$, *resp., satisfy*

$$\omega=\mathbb{N}\subseteq\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C};$$

b) *there are functions* $+\colon\mathbb{C}\times\mathbb{C}\to\mathbb{C}$ *and* $\cdot\colon\mathbb{C}\times\mathbb{C}\to\mathbb{C}$ *on* $\mathbb{C}$ *which are usually written as binary infix operations;*

c) $(\mathbb{C},+,\cdot,0,1)$ *is a field; for* $a,b\in\mathbb{C}$ *write* $a-b$ *for the unique element* z *such that* $a=b+z$ *; for* $a,b\in\mathbb{C}$ *with* $b\neq 0$ *write* $\frac{a}{b}$ *for the unique element* z *such that* $a=b\cdot z$ *;*

d) *there is a constant* i, *the* imaginary unit, *such that* $i\cdot i+1=0$ *and*

$$\mathbb{C}=\{x+i\cdot y\,|x,y\in\mathbb{R}\};$$

e) *there is a strict linear order* $<$ *on* $\mathbb{R}$ *such that* $(\mathbb{R},<,+\restriction\mathbb{R}^2,\cdot\restriction\mathbb{R}^2,0,1)$ *is an ordered field.*

f) $(\mathbb{R},<)$ *is* complete, *i.e., bounded subsets of* $\mathbb{R}$ *possess suprema:*

$$\forall X\subseteq\mathbb{R}\,(X\neq\emptyset\wedge\exists b\in\mathbb{R}\forall x\in X x<b\longrightarrow\exists b\in\mathbb{R}\,(\forall x\in X x<b\wedge\neg\exists b'<b\forall x\in X x<b'))$$

g) $\mathbb{Q}$ *is* dense *in* $(\mathbb{R},<)$*:*

$$\forall r,s\in\mathbb{R}\,(r<s\longrightarrow\exists a,b,c\in\mathbb{Q}\ a<r<b<s<c);$$

h) $(\mathbb{Q},+\restriction\mathbb{Q}^2,\cdot\restriction\mathbb{Q}^2,0,1)$ *is a field; moreover*

$$\mathbb{Q}=\left\{\frac{a}{b}\,|a\in\mathbb{Z},b\in\mathbb{Z}\setminus\{0\}\right\};$$

i) $(\mathbb{Z}, +\restriction\mathbb{Z}^2, \cdot\restriction\mathbb{Z}^2, 0, 1)$ *is a ring with a unit; moreover*

$$\mathbb{Z} = \{a - b \,|\, a, b \in \mathbb{N}\};$$

j) $+\restriction\mathbb{N}^2$ *agrees with ordinal addition on* ω *;* $\cdot\restriction\mathbb{N}^2$ *agrees with ordinal multiplication on* ω *;*

k) $(\mathbb{N}, +1, 0)$ *satisfies the second-order* PEANO *axioms, i.e., the successor function* $n \mapsto n+1$ *is injective,* 0 *is not in the image of the successor function, and*

$$\forall X \subseteq \mathbb{N}\,(0 \in X \wedge \forall n \in X n + 1 \in X \longrightarrow X = \mathbb{N}).$$

This theorem is all we require from the number systems. The details of the previous construction will not be used again.

Remark 59. In set theory the set $\mathbb{R}$ of reals is often identified with the sets ${}^{\omega}\omega$ or ${}^{\omega}2$, basically because all these sets have the same cardinality. We shall come back to this in the context of cardinality theory.

7 Sequences

The notion of a *sequence* is crucial in many contexts.

Definition 60.

a) *A set* w *is an* α-sequence *iff* $w: \alpha \rightarrow V$*; then* α *is called the* length *of the* α*-sequence* w *and is denoted by* $|\alpha|$*.* w *is a* sequence *iff it is an* α*-sequence for some* α *. A sequence* w *is called* finite *iff* $|w| < \omega$ *.*

b) *A finite sequence* $w: n \rightarrow V$ *may be denoted by its enumeration* $w_0, ..., w_{n-1}$ *where we write* w_i *instead of* $w(i)$*. One also writes* $w_0...w_{n-1}$ *instead of* $w_0, ..., w_{n-1}$ *, in particular if* w *is considered to be a* word *formed out of the* symbols $w_0, ..., w_{n-1}$ *.*

c) *An* ω*-sequence* $w: \omega \rightarrow V$ *may be denoted by* $w_0, w_1, ...$ *where* $w_0, w_1, ...$ *suggests a definition of* w *.*

d) *Let* $w: \alpha \rightarrow V$ *and* $w': \alpha' \rightarrow V$ *be sequences. Then the* concatenation $w\hat{\ }w': \alpha + \alpha' \rightarrow V$ *is defined by*

$$(w\hat{\ }w')\restriction\alpha = w\restriction\alpha \text{ and } \forall i < \alpha'\; w\hat{\ }w'(\alpha + i) = w'(i).$$

e) *Let* $w: \alpha \rightarrow V$ *and* $x \in V$*. Then the* adjunction wx *of* w *by* x *is defined as*

$$wx = w\hat{\ }\{(0, x)\}.$$

Sequences and the concatenation operation satisfy the algebraic laws of a *monoid* with cancellation rules.

Proposition 61. *Let* w, w', w'' *be sequences. Then*

a) $(w\hat{\ }w')\hat{\ }w'' = w\hat{\ }(w'\hat{\ }w'')$.

b) $\emptyset\hat{\ }w = w\hat{\ }\emptyset = w$.

c) $w\hat{\ }w' = w\hat{\ }w'' \rightarrow w' = w''$.

There are many other operations on sequences. One can *permute* sequences, substitute elements of a sequence, etc.

7.1 (ω-)Sequences of Reals

ω-sequences are particularly prominent in analysis. One may now define properties like

$$\lim_{i \rightarrow \infty} w_i = z \text{ iff } \forall \varepsilon \in \mathbb{R}^+ \exists m < \omega \forall i < \omega\; (i \geqslant m \rightarrow (z - \varepsilon < w_i \wedge w_i < z + \varepsilon))$$

or

$$\forall x{:}\,\omega \to \mathbb{R}\,(\lim_{i\to\infty} x_i = a \to \lim_{i\to\infty} f(x_i) = f(a)).$$

If $x_0, x_1, \ldots$ is given then the partial sums

$$\sum_{i=0}^{n} x_i$$

are defined recursively as

$$\sum_{i=0}^{0} x_i = 0 \quad \text{and} \quad \sum_{i=0}^{n+1} x_i = (\sum_{i=0}^{n} x_i) + x_n\,.$$

The map $\varphi{:}\,{}^{\omega}2 \to \mathbb{R}$ defined by

$$\varphi((x_i)_{i<\omega}) = \sum_{i=0}^{\infty} \frac{x_i}{2^{i+1}} = \lim_{n\to\infty} \sum_{i=0}^{n} \frac{x_i}{2^{i+1}}\,.$$

maps the function space ${}^{\omega}2$ surjectively onto the real interval

$$[0,1] = \{r \in \mathbb{R} \mid 0 \leqslant r \leqslant 1\}.$$

Such maps are the reason that one often identifies ${}^{\omega}2$ with $\mathbb{R}$ in set theory.

7.2 Symbols and Words

Languages are mathematical objects of growing importance. Mathematical logic takes terms and formulas as mathematical material. Terms and formulas are finite sequences of symbols from some alphabet. We represent the standard symbols $=$, $\in$, etc. by some set-theoretical terms $\dot{=}$, $\dot{\in}$, etc. Note that details of such a formalization are highly arbitrary. One really only has to *fix* certain sets to denote certain symbols.

Definition 62. *Formalize the* basic set-theoretical symbols *by*

a) $\dot{=} = 0,\ \dot{\in} = 1,\ \dot{\wedge} = 2,\ \dot{\vee} = 3,\ \dot{\to} = 4,\ \dot{\leftrightarrow} = 5,\ \dot{\neg} = 6,\ \dot{(} = 7,\ \dot{)} = 8,\ \dot{\exists} = 9,\ \dot{\forall} = 10.$

b) *Variables* $\dot{v}_n = (1, n)$ *for* $n < \omega$.

c) *Let* $L_{\in} = \{\dot{=}, \dot{\in}, \dot{\wedge}, \dot{\vee}, \dot{\to}, \dot{\leftrightarrow}, \dot{\neg}, \dot{(}, \dot{)}, \dot{\exists}, \dot{\forall}\} \cup \{(1, n) | n < \omega\}$ *be the* alphabet of set theory.

d) *A* word *over* $L_{\in}$ *is a finite sequence with values in* $L_{\in}$ *.*

e) *Let* $L_{\in}^{*} = \{w \mid \exists n < \omega\ w{:}\, n \to L_{\in}\}$ *be the set of all words over* $L_{\in}$ *.*

f) *If* φ *is a standard set-theoretical formula, we let* $\dot{\varphi} \in L_{\in}^{*}$ *denote the formalization of* φ. *E.g.,* $\dot{\mathrm{Ex}} = \dot{\exists}\dot{v}_0\dot{\forall}\dot{v}_1\dot{\neg}\dot{v}_1\dot{\in}\dot{v}_0$ *is the formalization of the set existence axiom. If the intention is clear, one often omits the formalization dots and simply writes* $\dot{\mathrm{Ex}} = \exists v_0 \forall v_1 \neg v_1 \in v_0$ *.*

This formalization can be developed much further, so that the notions and theorems of first-order logic are available in the theory ZF. By carrying out the definition of the axiom system ZF *within* set theory, one obtains a term $\dot{\mathrm{ZF}}$ which represents ZF within ZF. This (quasi) self-referentiality is the basis for limiting results like the GÖDEL incompleteness theorems.

8 The von Neumann Hierarchy

We use ordinal recursion to obtain more information on the universe of all sets.

Definition 63. *Define the* von Neumann Hierarchy $(V_\alpha)_{\alpha \in \mathrm{Ord}}$ *by recursion:*

a) $V_0 = \emptyset$ *;*

b) $V_{\alpha+1} = \mathcal{P}(V_\alpha)$ *;*

c) $V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$ *for limit ordinals* λ *.*

We show that the von Neumann hierarchy is indeed a (fast-growing) hierarchy

Lemma 64. *Let* $\beta < \alpha \in \mathrm{Ord}$*. Then*

a) $V_\beta \in V_\alpha$

b) $V_\beta \subseteq V_\alpha$

c) V_α *is transitive*

Proof. We conduct the proof by a simultaneous induction on α.
$\alpha = 0$: $\emptyset$ is transitive, thus a)-c) hold at 0.
For the *successor case* assume that a)-c) hold at α. Let $\beta < \alpha + 1$. By the inductive assumption, $V_\beta \subseteq V_\alpha$ and $V_\beta \in \mathcal{P}(V_\alpha) = V_{\alpha+1}$. Thus a) holds at $\alpha + 1$. Consider $x \in V_\alpha$. By the inductive assumption, $x \subseteq V_\alpha$ and $x \in V_{\alpha+1}$. Thus $V_\alpha \subseteq V_{\alpha+1}$. Then b) at $\alpha + 1$ follows by the inductive assumption. Now consider $x \in V_{\alpha+1} = \mathcal{P}(V_\alpha)$. Then $x \subseteq V_\alpha \subseteq V_{\alpha+1}$ and $V_{\alpha+1}$ is transitive.
For the *limit case* assume that α is a limit ordinal and that a)-c) hold at all $\gamma < \alpha$. Let $\beta < \alpha$. Then $V_\beta \in V_{\beta+1} \subseteq \bigcup_{\gamma<\alpha} V_\gamma = V_\alpha$ hence a) holds at α. b) is trivial for limit α. V_α is transitive as a union of transitive sets. □

The V_α are nicely related to the ordinal α.

Lemma 65. *For every* α*,* $V_\alpha \cap \mathrm{Ord} = \alpha$*.*

Proof. Induction on α. $V_0 \cap \mathrm{Ord} = \emptyset \cap \mathrm{Ord} = \emptyset = 0$.
For the *successor case* assume that $V_\alpha \cap \mathrm{Ord} = \alpha$. $V_{\alpha+1} \cap \mathrm{Ord}$ is transitive, and every element of $V_{\alpha+1} \cap \mathrm{Ord}$ is transitive. Hence $V_{\alpha+1} \cap \mathrm{Ord}$ is an ordinal, say $\delta = V_{\alpha+1} \cap \mathrm{Ord}$. $\alpha = V_\alpha \cap \mathrm{Ord}$ implies that $\alpha \in V_{\alpha+1} \cap \mathrm{Ord} = \delta$ and $\alpha + 1 \leqslant \delta$. Assume for a contradiction that $\alpha + 1 < \delta$. Then $\alpha + 1 \in V_{\alpha+1}$ and $\alpha + 1 \subseteq V_\alpha \cap \mathrm{Ord} = \alpha$, contradiction. Thus $\alpha + 1 = \delta = V_{\alpha+1} \cap \mathrm{Ord}$.
For the *limit case* assume that α is a limit ordinal and that $V_\beta \cap \mathrm{Ord} = \beta$ holds for all $\beta < \alpha$. Then

$$V_\alpha \cap \mathrm{Ord} = (\bigcup_{\beta<\alpha} V_\beta) \cap \mathrm{Ord} = \bigcup_{\beta<\alpha} (V_\beta \cap \mathrm{Ord}) = \bigcup_{\beta<\alpha} \beta = \alpha.$$

□