

## Chapter 13

# The Axioms of Set Theory ZFC

In this chapter, we shall present and discuss the axioms of Zermelo-Fraenkel Set Theory including the Axiom of Choice, denoted ZFC. It will turn out that within this axiom system, we can develop all of first-order mathematics, and therefore, the axiom system ZFC serves as foundation of mathematics. We will start with Zermelo's first axiomatisation of Set Theory and will show how basic mathematics can be developed within this system. Then we will introduce Zermelo's Axiom of Choice, Fraenkel's Axiom Schema of Replacement, and the Axiom of Foundation. Finally we will discuss the notions of ordinal and cardinal numbers.

Before we begin presenting the axioms of Set Theory, let us say a few words about Set Theory in general: The signature of Set Theory  $\mathcal{L}_{ST}$  contains only one non-logical symbol, namely the binary **membership relation**, denoted  $\in$ , so,  $\mathcal{L}_{ST} = \{\in\}$ . Furthermore, there exists just one type of objects, namely *sets*. However, to make life easier, instead of  $\in(a, b)$  we write  $a \in b$  (or on rare occasions also  $b \ni a$ ) and say that “ $a$  is an element of  $b$ ”, or that “ $a$  belongs to  $b$ ”. Furthermore, we write  $a \notin b$  as an abbreviation of  $\neg(a \in b)$ . Later we will extend the signature of Set Theory  $\mathcal{L}_{ST}$  by defining some constants (like “ $\emptyset$ ” and “ $\omega$ ”), relations (like “ $\subseteq$ ”), and operations (like the power set operation “ $\mathcal{P}$ ”), but as we know from Chapter 6, all what can be expressed in Set Theory using defined constants, functions, and relations, can also be expressed by formulae containing just the non-logical binary relation symbol “ $\in$ ”.

### Zermelo's Axiom System Z

In 1905, Zermelo began to axiomatise Set Theory and in 1908 he published his first axiomatic system consisting of the following seven axioms:

1. Axiom der Bestimmtheit  
which corresponds to the Axiom of Extensionality

2. Axiom der Elementarmengen  
which includes the Axiom of Empty Set as well as the Axiom of Pairing
3. Axiom der Aussonderung  
which corresponds to the Axiom Schema of Separation
4. Axiom der Potenzmenge  
which corresponds to the Axiom of Power Set
5. Axiom der Vereinigung  
which corresponds to the Axiom of Union
6. Axiom der Auswahl  
which corresponds to the Axiom of Choice
7. Axiom des Unendlichen  
which corresponds to the Axiom of Infinity

The axioms 1–5 and axiom 7 (*i.e.*, all axioms except the Axiom of Choice), form the so-called *Zermelo’s axiom system*, denoted  $Z$ , which will be discussed below.

Let us start with the axiom which states the existence of a set, namely the so-called empty-set.

#### 0. The Axiom of Empty Set

$$\exists x \forall z (z \notin x).$$

This axiom postulates the existence of a set without any elements, *i.e.*, an empty set.

#### 1. The Axiom of Extensionality

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

This axiom says that any sets  $x$  and  $y$  having the same elements are equal. Notice that the converse—which is  $x = y$  implies that  $x$  and  $y$  have the same elements—is just a consequence of the logical axiom  $L_{15}$ .

The Axiom of Extensionality also shows that the empty set, postulated by the Axiom of Empty Set, is unique. For assume that there are two empty sets  $x_0$  and  $x_1$ , then we have  $\forall z (z \notin x_0 \wedge z \notin x_1)$ , which implies that  $\forall z (z \in x_0 \leftrightarrow z \in x_1)$ , and therefore,  $x_0 = x_1$ . So, with the Axiom of Empty Set and the Axiom of Extensionality we can prove  $\exists! x \forall z (z \notin x)$ , and therefore, we can denote the unique empty set by the constant symbol  $\emptyset$ .

Similarly, we define the binary relation symbol “ $\subseteq$ ”, called **subset**, by stipulating

$$x \subseteq y :\iff \forall z (z \in y \rightarrow z \in x).$$

Notice that for every  $x$  we have  $\emptyset \subseteq x$ . Furthermore, we define the binary relation symbol " $\subsetneq$ ", called **proper subset**, by stipulating

$$x \subsetneq y : \iff x \subseteq y \wedge x \neq y.$$

So far, we have at least one set, namely the empty set  $\emptyset$ , for which we have  $\emptyset \subseteq \emptyset$ .

## 2. The Axiom of Pairing

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

Notice that by the Axiom of Extensionality, the set  $u$  is uniquely defined by the sets  $x$  and  $y$ . So, we can define the binary function symbol " $\{ \cdot, \cdot \}$ " by stipulating

$$\{x, y\} = u : \iff \forall z (z \in u \leftrightarrow (z = x \vee z = y)).$$

Notice that by the Axiom of Extensionality we have  $\{x, x\} = \{x\}$ . Thus, by the Axiom of Pairing, if  $x$  is a set, then also  $\{x\}$  is a set. Now, starting with  $\emptyset$ , an iterated application of the Axiom of Pairing yields for example the sets  $\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots$ , and  $\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots$ .

Notice also that by the Axiom of Extensionality we have  $\{x, y\} = \{y, x\}$ . So, it does not matter in which order the elements of a 2-element set are written down. However, with the Axiom of Pairing we can easily define **ordered pairs**, denoted  $\langle x, y \rangle$ , as follows:

$$\langle x, y \rangle := \{\{x\}, \{x, y\}\}.$$

It is not hard to show that  $\langle x, y \rangle = \langle x', y' \rangle$  iff  $x = x'$  and  $y = y'$ . Thus, we can define the binary function symbol " $\langle \cdot, \cdot \rangle$ " by stipulating

$$\langle x, y \rangle = u : \iff \forall z (z \in u \leftrightarrow (z = \{x\} \vee z = \{x, y\})).$$

Similarly, one could also define ordered triples, ordered quadruples, *et cetera*, but the notation becomes quite hard to read. However, when we have more axioms at hand we can easily define arbitrarily large tuples.

## 3. The Axiom of Union

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

With this axiom we can define the unary function symbol " $\bigcup$ ", called **union**, by stipulating

$$\bigcup x = u : \iff \forall z (z \in u \leftrightarrow \exists w \in x (z \in w)).$$

Informally, for all sets  $x$  there exists the union of  $x$  which consists of all sets which belong to at least one element of  $x$ . For example  $x = \bigcup \{x\}$ .

Similarly, we define the binary function symbol “ $\cup$ ” by stipulating

$$x \cup y = u : \iff u = \bigcup \{x, y\}.$$

The set  $x \cup y$  is called the **union** of  $x$  and  $y$ .

Now, with the Axiom of Union and the Axiom of Pairing, and by stipulating  $x + 1 := x \cup \{x\}$ , we can build for example the following sets:  $0 := \emptyset$ ,  $1 := 0 + 1 = 0 \cup \{0\} = \{0\}$ ,  $2 := 1 + 1 = 1 \cup \{1\} = \{0, 1\}$ ,  $3 := 2 + 1 = 2 \cup \{2\} = \{0, 1, 2\}$ , and so on. This construction leads to the following definition:

A set  $x$  such that  $\forall y(y \in x \rightarrow (y \cup \{y\}) \in x)$  is called **inductive**. More formally, we define the unary relation symbol “ind” by stipulating

$$\text{ind}(x) : \iff \forall y(y \in x \rightarrow (y \cup \{y\}) \in x).$$

Obviously, the empty set  $\emptyset$  is inductive, i.e.,  $\text{ind}(\emptyset)$ , but of course, this definition only makes sense if also some other inductive sets exist. However, in order to make sure that also non-empty inductive sets exist we need the following axiom.

#### 4. The Axiom of Infinity

$$\exists I(\emptyset \in I \wedge \text{ind}(I)),$$

Informally, the Axiom of Infinity postulates the existence of a non-empty inductive set containing  $\emptyset$ . All the sets  $0, 1, 2, \dots$  constructed above—which we recognise as natural numbers—must belong to every inductive set. So, if there were a set which contains just the natural numbers, it would be the “smallest” inductive set containing the empty set. In order to construct this set, we need some more axioms.

#### 5. The Axiom Schema of Separation

For each formula  $\varphi(z, p_1, \dots, p_n)$  with  $\text{free}(\varphi) \subseteq \{z, p_1, \dots, p_n\}$ , the following formula is an axiom:

$$\forall x \forall p_1 \dots \forall p_n \exists y \forall z (z \in y \leftrightarrow (z \in x \wedge \varphi(z, p_1, \dots, p_n))).$$

Informally, for each set  $x$  and every first-order formula  $\varphi(z)$ ,  $\{z \in x : \varphi(z)\}$  is a set. One can think of the sets  $p_1, \dots, p_n$  as parameters of  $\varphi$ , which are usually some fixed sets.

As a first application of the Axiom Schema of Separation we define the *intersection* of two sets  $x_0$  and  $x_1$ : We use  $x_0$  as a parameter and let  $\varphi(z, x_0) \equiv z \in x_0$ . Then, by the Axiom Schema of Separation, there exists a set  $y = \{z \in x_1 : \varphi(z, x_0)\}$ , i.e.,

$$z \in y \leftrightarrow (z \in x_1 \wedge z \in x_0).$$

In other words, for any sets  $x_0$  and  $x_1$ , the collection of all sets which belong to both,  $x_0$  and  $x_1$ , is a set. This set is called the **intersection** of  $x_0$  and  $x_1$  and is

denoted by  $x_0 \cap x_1$ . More formally, we define the binary function symbol “ $\cap$ ”

$$x_0 \cap x_1 = y : \iff \forall z \in y (z \in y \leftrightarrow z \in x_1 \wedge z \in x_0).$$

In general, for non-empty sets  $x$  we define the unary function symbol “ $\bigcap$ ” by stipulating

$$\bigcap x = y : \iff y = \{u \in \bigcup x : \forall z \in x (u \in z)\},$$

which is the intersection of all sets which belong to  $x$ . In order to see that  $\bigcap x$  is a set which is uniquely determined by  $x$ , let  $\varphi(z, x) \equiv \forall y \in x (z \in y)$  and apply the Axiom Schema of Separation to  $\bigcup x$ . Notice that  $x \cap y = \bigcap \{x, y\}$ .

Another example is when  $\varphi(z, y) \equiv z \notin y$ , where  $y$  is a parameter. In this case,  $\{z \in x : z \notin y\}$  is a set, denoted  $x \setminus y$ , which is called the **set-theoretic difference** of  $x$  and  $y$ . More formally, we define the binary function symbol “ $\setminus$ ” by stipulating

$$x \setminus y = u : \iff \forall z \in u (z \in u \leftrightarrow z \in x \wedge z \notin y).$$

The next axiom gives us for any set  $x$  the set of all subsets of  $x$ .

### 6. The Axiom of Power Set

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

Informally, the Axiom of Power Set states that for each set  $x$  there is a set  $\mathcal{P}(x)$ , called the **power set** of  $x$ , which consists of all subsets of  $x$ . More formally, we define the unary function symbol “ $\mathcal{P}$ ” by stipulating

$$\mathcal{P}(x) = y : \iff \forall z (z \in y \leftrightarrow z \subseteq x).$$

### The Set $\omega$

As an application of the axioms we have so far, we define the smallest non-empty inductive set containing  $\emptyset$ , denoted by  $\omega$ , which will be the smallest set containing the natural numbers (see Chapter 16): By the Axiom of Infinity, there exists a non-empty inductive set  $I_0$ . Now, with the Axiom of Power Set and the Axiom Schema of Separation, we can define the set

$$\omega := \bigcap \{X \in \mathcal{P}(I_0) : \emptyset \in X \wedge \text{ind}(X)\}.$$

We have to show that the set  $\omega$  is the smallest set which is inductive and contains  $\emptyset$ : By definition,  $\omega$  is inductive and contains  $\emptyset$ . Now, let  $I$  be an inductive set with  $\emptyset \in I$ , and let  $X_0 := \omega \cap I$ . On the one hand,  $X_0$  is inductive and  $\emptyset \in X_0$ . On the other hand, since  $X_0 \subseteq \omega$ , we have  $X_0 \in \mathcal{P}(I_0)$ , which implies that  $\omega \subseteq X_0$ .

So,  $\omega$  is the unique inductive set containing  $\emptyset$ , which is contained in every inductive set containing  $\emptyset$ .

Later in Chapter 16 we shall see that  $\omega$  is the domain of the standard model of Peano Arithmetic PA.

## Functions, Relations, and Models

With the axioms we have so far (*i.e.*, with Zermelo's axiom system Z), we can define notions like functions and relations.

### Cartesian Products and Functions

Let us define first Cartesian products: For arbitrary sets  $A$  and  $B$  we define the binary function symbol called **Cartesian product**  $A \times B$  by stipulating

$$A \times B := \{\langle x, y \rangle : x \in A \wedge y \in B\}$$

where  $\langle x, y \rangle = \{\{x\}, \{x, y\}\}$ . Thus, the Cartesian product of two sets  $A$  and  $B$  is a subset of  $\mathcal{P}(\mathcal{P}(A \cup B))$ .

Now, we define **functions**  $f : A \rightarrow B$  which map the elements of a set  $A$  to elements of a set  $B$  as certain subsets of  $A \times B$ . The set of all such functions is denoted  ${}^A B$ , where we define

$${}^A B := \{f \subseteq A \times B : \forall x \in A \exists! y \in B (\langle x, y \rangle \in f)\}.$$

For  $f \in {}^A B$  (*i.e.*,  $f : A \rightarrow B$ ), we usually write  $f(x) = y$  instead of  $\langle x, y \rangle \in f$ . and say that  $y$  is the image of  $x$  under  $f$ . If  $S \subseteq A$ , then the **image** of  $S$  under  $f$  is denoted by  $f[S] = \{f(x) : x \in S\}$  and  $f|_S = \{\langle x, y \rangle \in f : x \in S\}$  is the restriction of  $f$  to  $S$ . Furthermore, for a function  $f : A \rightarrow B$ ,  $f[A]$  is called the **range** of  $f$ , denoted  $\text{ran}(f)$ .

*Some special functions:*

- A function  $f : A \rightarrow B$  is **surjective**, or **onto**, if

$$\forall y \in B \exists x \in A (f(x) = y).$$

In order to emphasise the fact that  $f$  is surjective, one can write  $f : A \twoheadrightarrow B$ .

- A function  $f : A \rightarrow B$  is **injective**, also called **one-to-one**, if we have

$$\forall x_1 \in A \forall x_2 \in A (f(x_1) = f(x_2) \rightarrow x_1 = x_2).$$

In order to emphasise the fact that  $f$  is injective, one can write  $f : A \hookrightarrow B$ .

- A function  $f : A \rightarrow B$  is **bijective** if it is injective and surjective. If  $f : A \rightarrow B$  is bijective, then

$$\forall y \in B \exists! x \in A (\langle x, y \rangle \in f)$$

which implies that

$$f^{-1} := \{ \langle y, x \rangle : \langle x, y \rangle \in f \} \in {}^B A$$

is a function which is even bijective. So, if there is a bijective function from  $A$  to  $B$ , then there is also one from  $B$  to  $A$  and we sometimes just say that there is a **bijection between**  $A$  and  $B$ . Notice that if  $f : A \hookrightarrow B$  is injective, then  $f$  is a bijection between  $A$  and  $f[A]$ .

- If  $f$  is a function from  $A$  to  $B$  and  $g$  is a function from  $B$  to  $C$ , then the composition  $g \circ f$  is a function from  $A$  to  $C$ , where

$$g \circ f := \{ \langle x, z \rangle \in A \times C : \exists y \in B (\langle x, y \rangle \in f \wedge \langle y, z \rangle \in g) \}.$$

### Cartesian Products and Relations

Let us turn back to Cartesian products: Assume that for each  $\iota \in I$  (for some set  $I$ ) we have assigned a non-empty set  $A_\iota$ . Then the set

$$\prod_{\iota \in I} A_\iota := \{ f \in {}^I A : \forall \iota \in I (f(\iota) \in A_\iota) \}$$

is called the Cartesian product of the sets  $A_\iota$  ( $\iota \in I$ ). Notice that if all sets  $A_\iota$  are equal to a given set  $A$ , then  $\prod_{\iota \in I} A_\iota = {}^I A$ .

If  $I = n$  for some  $n \in \omega$ , in abuse of notation we also write  $A^n$  instead of  ${}^n A$  by identifying  ${}^n A$  with the set

$$A^n = \underbrace{A \times \dots \times A}_{n\text{-times}}$$

Let us now consider subsets of finite Cartesian products: For any set  $A$  and any  $n \in \omega$ , a set  $R \subseteq A^n$  is called an  **$n$ -ary relation** on  $A$ . If  $n = 2$ , then  $R \subseteq A \times A$  is also called a **binary relation**. For binary relations  $R$  we usually write  $xRy$  instead of  $\langle x, y \rangle \in R$ .

*Order relations:*

- A binary relation  $R$  on  $A$  is a **linear ordering** on  $A$ , if for any elements  $x, y \in A$  we have  $xRy$  or  $x = y$  or  $yRx$ , where these three cases are mutually exclusive.
- A linear ordering  $R$  on  $A$  is a **well-ordering** on  $A$ , if every non-empty subset  $S \subseteq A$  has an  $R$ -minimal element, i.e., there exists a  $x_0 \in S$  such that for each  $y \in S$  we have  $x_0 R y$ . Notice, that since  $R$  is a linear ordering, the  $R$ -minimal element  $x_0$  is unique. If there is a well-ordering  $R$  on  $A$ , then we say

that  $A$  is *well-orderable*. The problem whether each set is well-orderable has to be postponed until we have the Axiom of Choice.

Other important binary relations are the so-called equivalence relations: Let  $S$  be an arbitrary non-empty set. A binary relation “ $\sim$ ” on  $S$  is an **equivalence relation** if it is

- *reflexive* (i.e., for all  $x \in S$ :  $x \sim x$ ),
- *symmetric* (i.e., for all  $x, y \in S$ :  $x \sim y \leftrightarrow y \sim x$ ), and
- *transitive* (i.e., for all  $x, y, z \in S$ :  $x \sim y \wedge y \sim z \rightarrow x \sim z$ ).

The **equivalence class** of an element  $x \in S$ , denoted  $[x]^\sim$ , is the set  $\{y \in S : x \sim y\}$ . We would like to recall the fact that for any  $x, y \in S$  we have *either*  $[x]^\sim = [y]^\sim$  or  $[x]^\sim \cap [y]^\sim = \emptyset$ . A set  $A \subseteq S$  is a set of **representatives** if for each equivalence class  $[x]^\sim$ ,  $A$  has exactly one element in common with each equivalence class. We would like to mention that the existence of a set of representatives relies in general on the Axiom of Choice.

## Zermelo-Fraenkel Set Theory with Choice ZFC

In 1922, Fraenkel and Skolem independently improved and extended Zermelo’s original axiomatic system, and the final version was presented again by Zermelo in 1930. The two axioms we have to add to Zermelo’s system from 1908 are the Axiom Schema of Replacement and the Axiom of Foundation. In this section, we will present the remaining axioms of the so-called *Zermelo–Fraenkel Set Theory* with the Axiom of Choice, denoted ZFC, which consists of Zermelo’s axiom system  $Z$  together with the Axiom Schema of Replacement, the Axiom of Foundation, and the Axiom of Choice

### 7. The Axiom Schema of Replacement

For every first-order formula  $\varphi(x, y, p)$  with  $\text{free}(\varphi) = \{x, y\}$ , where  $p$  can be an ordered  $n$ -tuple of parameters, the following formula is an axiom:

$$\forall A \forall p (\forall x \in A \exists! y \varphi(x, y, p) \rightarrow \exists B \forall x \in A \exists y \in B \varphi(x, y, p)).$$

In order to reformulate the Axiom Schema of Replacement, we introduce the notion of a *class function*: Let  $\varphi(x, y)$  be a formula with  $\text{free}(\varphi) = \{x, y\}$  such that

$$\forall x \exists! y \varphi(x, y).$$

Then the unary function symbol  $F$ , defined by stipulating

$$F(x) = y :\iff \varphi(x, y)$$



is called a **class function**. Now, the Axiom Schema of Replacement states for every set  $A$  and for each class function  $F$ ,

$$F[A] = \{F(x) : x \in A\}$$

is a set. More informally, images of sets under functions are sets.

With the Axiom Schema of Replacement we can now define arbitrary Cartesian products: Let  $F$  be a class function and let  $I$  be an arbitrary set. Furthermore, for every  $\iota \in I$  let  $A_\iota := F(\iota)$  and let  $A := \bigcup F[I]$ . Then the set

$$\prod_{\iota \in I} A_\iota := \left\{ f \in {}^I A : \forall \iota \in I (f(\iota) \in A_\iota) \right\}$$

is called the Cartesian product of the sets  $A_\iota$  ( $\iota \in I$ ). As a matter of fact we would like to mention that with the axioms we have so far, we cannot prove that Cartesian products  $\prod_{\iota \in I} A_\iota$  of non-empty sets  $A_\iota$  are non-empty.

We also would like to mention that with the Axiom Schema of Replacement, the Axiom of Empty Set and the Axiom Schema of Separation are redundant (see EXERCISE 13.0).

### 8. The Axiom of Foundation

$$\forall x (\exists z (z \in x) \rightarrow \exists y \in x (y \cap x = \emptyset)).$$

As a consequence of the Axiom of Foundation we see that there is no infinite descending sequence  $x_0 \ni x_1 \ni x_2 \ni \dots$  since otherwise, the set  $\{x_0, x_1, x_2, \dots\}$  would contradict the Axiom of Foundation. In particular, there is no set  $x$  such that  $x \in x$  and there are also no cycles like  $x_0 \in x_1 \in \dots \in x_n \in x_0$ . As a matter of fact we would like to mention that if one assumes the Axiom of Choice, then the non-existence of such infinite descending sequences can be proved to be equivalent to the Axiom of Foundation.

The axiom system containing the axioms 0–8 is called **Zermelo–Fraenkel Set Theory** and is denoted by ZF.

### 9. The Axiom of Choice AC

$$\forall \mathcal{F} \exists f (f \text{ is a function from } \mathcal{F} \text{ to } \bigcup \mathcal{F} \wedge (\emptyset \notin \mathcal{F} \rightarrow \forall x \in \mathcal{F} (f(x) \in x))),$$

or equivalently,

$$\forall \mathcal{F} \left( \emptyset \notin \mathcal{F} \rightarrow \exists f \left( f \in {}^{\mathcal{F}} \bigcup \mathcal{F} \wedge \forall x \in \mathcal{F} (f(x) \in x) \right) \right).$$

Informally, every family of non-empty sets has a choice function.

One can show that AC is equivalent to the statement that Cartesian products of non-empty sets are non-empty. More formally, let  $\mathcal{F} = \{A_\iota : \iota \in I\}$  be a family of non-empty sets (i.e., for each  $\iota \in I$ ,  $A_\iota \neq \emptyset$ ). Then the Cartesian product  $\prod_{\iota \in I} A_\iota$  is non-empty. To see this, let  $f$  be a choice function of  $\mathcal{F}$ . Then

$$\left\{ \langle \iota, f(A_\iota) \rangle : \iota \in I \right\} \in \prod_{\iota \in I} A_\iota,$$

and hence,  $\prod_{\iota \in I} A_\iota$  is non-empty.

ZF together with the Axiom of Choice AC is denoted by ZFC. Later we shall see that the axiom system ZFC is a foundation of first-order mathematics.

## Well-Ordered Sets and Ordinal Numbers

In 1904, Zermelo [46] published his first proof of the so-called Well-Ordering Principle, which states that every set can be well-ordered every set can be well-ordered, and in 1908 he published a second proof (see [47]). In the proof presented below, we follow essentially Zermelo's first proof, but first we have to introduce the notion of ordinal numbers.

### Ordinal Numbers

One of the most important concepts in Set Theory is the notion of *ordinal number*, which can be seen as a transfinite extension of the natural numbers. In order to define the concept of ordinal numbers, we must first give some definitions: Let  $z \in x$ . Then  $z$  is called an  **$\in$ -minimal element** of  $x$ , denoted  $\min_{\in}(z, x)$ , if  $\forall y (y \notin z \vee y \notin x)$ , or equivalently, for any  $y$  in  $z$  we have  $y \notin x$ , or more formally,

$$\min_{\in}(z, x) :\iff z \in x \wedge \forall y (y \in z \rightarrow y \notin x).$$

A set  $x$  is **ordered by  $\in$**  if for any sets  $y_1, y_2 \in x$  we have  $y_1 \in y_2$ , or  $y_1 = y_2$ , or  $y_1 \ni y_2$ , but we do not require the three cases to be mutually exclusive. More formally,

$$\text{ord}_{\in}(x) :\iff \forall y_1, y_2 \in x (y_1 \in y_2 \vee y_1 = y_2 \vee y_1 \ni y_2).$$

Now, a set  $x$  is called **well-ordered by  $\in$**  if it is ordered by  $\in$  and every non-empty subset of  $x$  has an  $\in$ -minimal element. More formally,

$$\text{wo}_{\in}(x) :\iff \text{ord}_{\in}(x) \wedge \forall y \in \mathcal{P}(x) (y \neq \emptyset \rightarrow \exists z \in y \min_{\in}(z, y)).$$

Further, a set  $x$  is called **transitive** if each element of  $x$  is a subset of  $x$ , i.e.,

$$\text{trans}(x) :\iff \forall y(y \in x \rightarrow y \subseteq x).$$

Notice that if  $x$  is transitive and  $z \in y \in x$ , then this implies  $z \in x$ . A set is called an **ordinal number**, or just an **ordinal**, if it is transitive and well-ordered by “ $\in$ ”, i.e.,

$$\text{ordinal}(x) :\iff \text{trans}(x) \wedge \text{wo}_\in(x).$$

Ordinal numbers are usually denoted by Greek letters like  $\alpha, \beta, \gamma, \lambda$ , *et cetera*, and the collection of all ordinal numbers is denoted by  $\Omega$ . We will see later that  $\Omega$  is not a set. However, we can consider “ $\alpha \in \Omega$ ” as an abbreviation of  $\text{ordinal}(\alpha)$ , which is just a property of  $\alpha$ , and thus, there is no harm in using the symbol  $\Omega$  in this way, even though  $\Omega$  is *not* an object of the set-theoretic universe.

Now, one can prove the following result (see, for example, Halbeisen [20, Ch. 3]).

FACT 13.1.

- (a) If  $\alpha \in \Omega$ , then either  $\alpha = \emptyset$  or  $\emptyset \in \alpha$ .
- (b) If  $\alpha \in \Omega$ , then  $\alpha \notin \alpha$ .
- (c) If  $\alpha, \beta \in \Omega$ , then  $\alpha \in \beta$  or  $\alpha = \beta$  or  $\alpha \ni \beta$ , where these three cases are mutually exclusive.
- (d) If  $\alpha \in \beta \in \Omega$ , then  $\alpha \in \Omega$ .
- (e) If  $\alpha \in \Omega$ , then also  $\alpha + 1 \in \Omega$ , where  $\alpha + 1 := \alpha \cup \{\alpha\}$ .
- (f)  $\Omega$  is transitive and is well-ordered by  $\in$ . More precisely,  $\Omega$  is transitive, is ordered by  $\in$ , and every non-empty collection  $C \subseteq \Omega$  has an  $\in$ -minimal element.
- (g) If  $\alpha, \beta \in \Omega$  and  $\alpha \in \beta$ , then  $\alpha + 1 \subseteq \beta$ . In other words,  $\alpha + 1$  is the least ordinal which contains  $\alpha$ .
- (h) For every ordinal  $\alpha \in \Omega$  we have either  $\alpha = \bigcup \alpha$  or there exists a  $\beta \in \Omega$  such that  $\alpha = \beta + 1$ .

Notice that if  $\Omega$  is a set, then by (f),  $\Omega$  is an ordinal number, and therefore  $\Omega \in \Omega$ , which contradicts (b). So, the collection of all ordinals  $\Omega$  is not a set, but a so-called *class*.

The last two facts lead to the following definitions: An ordinal  $\alpha$  is called a **successor ordinal** if there exists an ordinal  $\beta$  such that  $\alpha = \beta + 1$ ; otherwise, it is called a **limit ordinal**. In particular,  $\emptyset$  is a limit ordinal. Notice that  $\alpha \in \Omega$  is a limit ordinal if and only if  $\bigcup \alpha = \alpha$ .

With this definitions one can show that  $\omega$ , defined above as the least non-empty inductive set, is in fact the least non-empty limit ordinal. In particular we have  $\bigcup \omega = \omega$ .

Now we are ready to prove the following

THEOREM 13.2. *The Well-Ordering Principle is equivalent to the Axiom of Choice.*

*Proof.* ( $\Rightarrow$ ) Let  $\mathcal{F}$  be any family of non-empty sets and let “ $<$ ” be any well-ordering on  $\bigcup \mathcal{F}$ . Define  $f : \mathcal{F} \rightarrow \bigcup \mathcal{F}$  by stipulating  $f(x)$  being the  $<$ -minimal element of  $x$ .

( $\Leftarrow$ ) Let  $M$  be a set. If  $M = \emptyset$ , then  $M$  is well-ordered and we are done. So, assume that  $M \neq \emptyset$  and let  $\mathcal{P}^*(M) := \mathcal{P}(M) \setminus \{\emptyset\}$ . Further, let

$$f : \mathcal{P}^*(M) \rightarrow M$$

be an arbitrary but fixed choice function for the family  $\mathcal{P}^*(M)$ , which exists by the Axiom of Choice.

Now, an injective function

$$w_\alpha : \alpha \hookrightarrow M$$

from some ordinal  $\alpha \in \Omega$  into  $M$  is called an  **$f$ -set** if for all  $\gamma \in \alpha$  we have

$$w_\alpha(\gamma) = f(M \setminus \{w_\alpha(\delta) : \delta \in \gamma\}).$$

For example,  $w_1 = \{\langle 0, f(M) \rangle\}$  is an  $f$ -set – in fact,  $w_1$  is the unique  $f$ -set with domain  $\{0\}$ . In general, for every  $\alpha \in \Omega$  there is at most one  $f$ -set  $w_\alpha$  with domain  $\alpha$ . To see this, assume that  $w_\alpha$  and  $w'_\alpha$  are two distinct  $f$ -sets with domain  $\alpha$ . Because  $w_\alpha$  and  $w'_\alpha$  are distinct and  $\alpha \in \Omega$ , there exists an  $\in$ -minimal  $\gamma \in \alpha$  such that  $w_\alpha(\gamma) \neq w'_\alpha(\gamma)$ , but since for all  $\delta \in \gamma$  we have  $w_\alpha(\delta) = w'_\alpha(\delta)$ , this contradicts the fact that

$$w_\alpha(\gamma) = f(M \setminus \{w_\alpha(\delta) : \delta \in \gamma\}) = f(M \setminus \{w'_\alpha(\delta) : \delta \in \gamma\}) = w'_\alpha(\gamma).$$

So, if there exists an  $f$ -set  $w_\alpha$  for some  $\alpha \in \Omega$ , then this  $f$ -set  $w_\alpha$  is unique  $f$ -set with  $\text{dom}(w_\alpha) = \alpha$ . Moreover, if  $w_\beta$  and  $w_\alpha$  are  $f$ -sets and  $\beta \in \alpha$ , then  $w_\alpha|_\beta = w_\beta$  (i.e., the restriction of  $w_\alpha$  to  $\beta$  is equal to  $w_\beta$ ).

Because every  $f$ -set  $w_\alpha$  induces a well-ordering on  $\text{ran}(w_\alpha) \subseteq M$ , by the Axiom Schema of Separation, the collection of all  $f$ -sets is a set, say  $S$ . Now, on  $S$  we define the ordering “ $\prec$ ” as follows: For two distinct  $f$ -sets  $w_\alpha$  and  $w_\beta$ , let

$$w_\alpha \prec w_\beta \iff \alpha \in \beta.$$

Since the class  $\Omega$  is well-ordered by “ $\in$ ”,  $S$  is well-ordered by “ $\prec$ ”. Let  $w := \bigcup S$  and let

$$M' := \{x \in M : \exists \gamma \in \text{dom}(w)(w(\gamma) = x)\}.$$

Then  $M' = M$  and  $w \in S$ , since otherwise,  $w$  can be extended to the  $f$ -set

$$w \cup \{\langle \text{dom}(w), f(M \setminus M') \rangle\},$$

which is a contradiction to the definition of  $S$ . Therefore, the injective function  $w : \text{dom}(w) \hookrightarrow M$  is surjective. In other words, there exists an ordinal  $\alpha \in \Omega$  such that  $w$  is a bijection between  $\alpha$  and  $M$ . Finally, define the binary relation “ $<$ ” on  $M$  by stipulating

$$x < y : \iff w^{-1}(x) \in w^{-1}(y).$$

Then, since  $\alpha$  is well-ordered by “ $\in$ ”,  $M$  is well-ordered by “ $<$ ”.  $\dashv$

## Ordinal Arithmetic

The next result is the TRANSFINITE RECURSION THEOREM, which is a very powerful tool and is used, for example, to define ordinal arithmetic (see below) or to build the cumulative hierarchy of sets (see Chapter 14).

**THEOREM 13.3 (TRANSFINITE RECURSION THEOREM).** *Let  $F$  be a class function which is defined for all sets. Then there is a unique class function  $G$  defined on  $\Omega$  such that for each  $\alpha \in \Omega$  we have*

$$G(\alpha) = F(G|_{\alpha}), \quad \text{where } G|_{\alpha} = \{\langle \beta, G(\beta) \rangle : \beta \in \alpha\}.$$

By transfinite recursion we are able to define addition, multiplication, and exponentiation of arbitrary ordinal numbers (see EXERCISE 13.1):

**Ordinal Addition:** For arbitrary ordinals  $\alpha \in \Omega$  we define

- (a)  $\alpha + 0 := \alpha$ ,
- (b)  $\alpha + (\beta + 1) := (\alpha + \beta) + 1$ , for all  $\beta \in \Omega$ ,
- (c) and if  $\beta \in \Omega$  is non-empty and a limit ordinal, then  $\alpha + \beta := \bigcup_{\delta \in \beta} (\alpha + \delta)$ .

Notice that, for example,  $1 + \omega = \omega \neq \omega + 1$ , which shows that addition of ordinals is in general not commutative.

**Ordinal Multiplication:** For arbitrary ordinals  $\alpha \in \Omega$  we define

- (a)  $\alpha \cdot 0 := 0$ ,
- (b)  $\alpha \cdot (\beta + 1) := (\alpha \cdot \beta) + \alpha$ , for all  $\beta \in \Omega$ ,
- (c) and if  $\beta \in \Omega$  is a limit ordinal, then  $\alpha \cdot \beta := \bigcup_{\delta \in \beta} (\alpha \cdot \delta)$ .

Notice that, for example,  $2 \cdot \omega = \omega \neq \omega + \omega = \omega \cdot 2$ , which shows that multiplication of ordinals is in general not commutative.

**Ordinal Exponentiation:** For arbitrary ordinals  $\alpha \in \Omega$  we define

- (a)  $\alpha^0 := 1$ ,
- (b)  $\alpha^{\beta+1} := \alpha^{\beta} \cdot \alpha$ , for all  $\beta \in \Omega$ ,
- (c) and if  $\beta \in \Omega$  is non-empty and a limit ordinal, then  $\alpha^{\beta} := \bigcup_{\delta \in \beta} (\alpha^{\delta+1})$ .

By definition, we obtain that addition, multiplication, and exponentiation of ordinals are binary operations on  $\Omega$ , and addition and multiplication of ordinals are also associative.

Let us consider again the set  $\omega$ . The ordinals belonging to  $\omega$  are called **natural numbers**. Since  $\omega$  is the smallest non-empty limit ordinal, all natural numbers, except 0, are successor ordinals. Thus, for each  $n \in \omega$  we have either  $n = 0$  or there is an  $m \in \omega$  such that  $n = m + 1$ . Furthermore, if we define the binary ordering relation “ $<$ ” on  $\omega$  by stipulating

$$k < n : \iff k \in n$$

then for each  $n \in \omega$  we have  $n = \{k \in \omega : k < n\}$ , i.e.,  $n = \{0, 1, \dots, n-1\}$ . In particular, for every  $n \in \omega$ ,  $n$  is a set containing exactly  $n$  elements.

With ordinal addition, multiplication, and exponentiation we can define sums, products, and powers of natural numbers within ZF. In fact, we can define these operations already in Z (see EXERCISE 13.4).

## Cardinal Numbers and Cardinal Arithmetic

One can show (see, for example, Halbeisen [20, Ch. 3]) that for each well-ordering “ $<$ ” of a set  $A$  there exists a unique ordinal  $\alpha$  and a unique bijective function  $f : A \rightarrow \alpha$  such that for all  $x, y \in A$ ,

$$x < y \iff f(x) \in f(y).$$

The unique ordinal  $\alpha$  which corresponds to a well-ordering “ $<$ ” of  $A$ , is called the **order type** of the well-ordering “ $<$ ”.

In the presence of AC we are now able to define cardinal numbers as ordinals: For any set  $A$  we define the cardinality of  $A$ , denoted  $|A|$ , by stipulating

$$|A| := \min \{ \alpha \in \Omega : \alpha \text{ is the order type of a well-ordering of } A \}.$$

By definition we have

$$|A| = \min \{ \alpha \in \Omega : \text{there is a bijection between } \alpha \text{ and } A \}.$$

In order to see that this definition makes sense, notice that by AC, every set  $A$  is well-orderable and that by the remark above, every well-ordering on  $A$  corresponds to exactly one ordinal. So, for each set  $A$ , the set of all order types of well-orderings of  $A$  is a non-empty set of ordinals. Let  $C \subseteq \Omega$  be this set of ordinals. Then, by FACT 13.1.(f),  $C$  has an  $\in$ -minimal element  $\min C$ , which shows that  $|A|$  is indeed an ordinal.

For example, we have  $|n| = n$  for every  $n \in \omega$ , and  $|\omega| = \omega$ , but in general, for  $\alpha \in \Omega$ , we do not have  $|\alpha| = \alpha$ . For example,  $|\omega + 1| \neq \omega + 1$ , since  $|\omega + 1| = \omega$

and  $\omega \neq \omega + 1$ . However, there are also other ordinals  $\alpha$  beside  $n \in \omega$  and  $\omega$  itself for which we have  $|\alpha| = \alpha$ , which leads to the following definition:

An ordinal number  $\kappa \in \Omega$  such that  $|\kappa| = \kappa$  is called a **cardinal number**, or just a **cardinal**. Cardinal numbers are usually denoted by Greek letters like  $\kappa, \lambda, \mu$ , *et cetera*, or by  $\aleph$ 's. For example, the cardinal number  $\omega$  is denoted by  $\aleph_0$ , which is the cardinality of countably infinite sets.

A cardinal  $\kappa$  is **infinite** if  $\kappa \notin \omega$ , otherwise, it is **finite**. In other words, a cardinal is finite if and only if it is a natural number.

Since cardinal numbers are just a special kind of ordinal, they are well-ordered by " $\in$ ". However, for cardinal numbers  $\kappa$  and  $\lambda$  we usually write  $\kappa < \lambda$  instead of  $\kappa \in \lambda$ , thus,

$$\kappa < \lambda \iff \kappa \in \lambda.$$

The next result implies that there are arbitrarily large cardinal numbers.

**THEOREM 13.4 (CANTOR'S THEOREM).** *For every set  $A$ ,  $|A| < |\mathcal{P}(A)|$ .*

*Proof.* Let  $A$  be an arbitrary set. Obviously we have  $|A| \leq |\mathcal{P}(A)|$ . If we would have  $|A| = |\mathcal{P}(A)|$ , then there would be a bijection between  $A$  and  $\mathcal{P}(A)$ . In particular, there would be a surjection  $A \rightarrow \mathcal{P}(A)$ . So, in order to prove  $|A| < |\mathcal{P}(A)|$ , it is enough to show that there is no surjection  $f : A \rightarrow \mathcal{P}(A)$ .

If  $A = \emptyset$ , then  $\mathcal{P}(A) = \{\emptyset\}$  and  $f = \emptyset$ , hence,  $f$  is not a surjection.

If  $A \neq \emptyset$ , consider the set

$$\Gamma := \{x \in A : x \notin f(x)\}.$$

On the one hand, since  $\Gamma \subseteq A$ ,  $\Gamma \in \mathcal{P}(A)$ . On the other hand, for each  $x \in A$  we have

$$x \in \Gamma \iff x \notin f(x),$$

and therefore, there is no  $x \in A$  such that  $f(x) = \Gamma$ , which shows that  $f$  is not surjective.  $\dashv$

For every cardinal  $\kappa$ , let

$$2^\kappa := |\mathcal{P}(\kappa)|.$$

So, THEOREM 13.4 states that for every cardinal  $\kappa$  we have  $\kappa < 2^\kappa$ .

Let  $\kappa$  be a cardinal. The smallest cardinal number which is greater than  $\kappa$  is denoted by  $\kappa^+$ , thus,

$$\kappa^+ = \min\{\alpha \in \Omega : \kappa < |\alpha|\}.$$

Notice that by THEOREM 13.4, for every cardinal  $\kappa$ ,  $\kappa < 2^\kappa$ . In particular, for every cardinal  $\kappa$ ,  $\{\alpha \in \Omega : \kappa < |\alpha|\}$  is non-empty and therefore  $\kappa^+$  exists.

A cardinal  $\mu$  is called a **successor cardinal** if there exists a cardinal  $\kappa$  such that  $\mu = \kappa^+$ ; otherwise, it is called a **limit cardinal**. In particular, every positive integer  $n \in \omega$  is a successor cardinal and  $\omega$  is the smallest non-zero limit cardinal. By induction on  $\alpha \in \Omega$  we define  $\aleph_{\alpha+1} := \aleph_\alpha^+$ , where  $\aleph_0 := \omega$ , and  $\aleph_\alpha := \bigcup_{\delta \in \alpha} \aleph_\delta$

for limit ordinals  $\alpha$ ; notice that  $\bigcup_{\delta \in \alpha} \aleph_\delta$  is a cardinal (see EXERCISE 13.2). In particular,  $\aleph_\omega$  is the smallest uncountable limit cardinal and  $\aleph_1 = \aleph_0^+$  is the smallest uncountable cardinal.

The Continuum Hypothesis (CH) states that  $2^{\aleph_0} = \aleph_1$ , and the Generalised Continuum Hypothesis (GCH) states that for all  $\alpha \in \Omega$ ,  $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ .

The collection  $\{\aleph_\alpha : \alpha \in \Omega\}$  is the class of all infinite cardinals, *i.e.*, for every infinite cardinal  $\kappa$  there is an  $\alpha \in \Omega$  such that  $\kappa = \aleph_\alpha$ . Notice that the collection of cardinals is—like the collection of ordinals—a proper *class* and not a *set*.

Cardinal addition, multiplication, and exponentiation are defined as follows:

*Cardinal addition:* For cardinals  $\kappa$  and  $\mu$ , let

$$\kappa + \mu := |(\kappa \times \{0\}) \dot{\cup} (\mu \times \{1\})|.$$

*Cardinal multiplication:* For cardinals  $\kappa$  and  $\mu$ , let

$$\kappa \cdot \mu := |\kappa \times \mu|.$$

*Cardinal exponentiation:* For cardinals  $\kappa$  and  $\mu$ , let

$$\kappa^\mu := |\mu \kappa|.$$

As a consequence of the definition we get the following

**FACT 13.5.** *Addition and multiplication of cardinals is associative and commutative and we have the distributive law for multiplication over addition, and for all cardinals  $\kappa, \lambda, \mu$ , we have*

$$\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu, \quad \kappa^{\mu \cdot \lambda} = (\kappa^\lambda)^\mu, \quad (\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu.$$

Furthermore, we have

**FACT 13.6.** *For any ordinal numbers  $\alpha, \beta \in \Omega$  we have*

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \aleph_{\alpha \cup \beta} = \max\{\aleph_\alpha, \aleph_\beta\}.$$

*In particular, for every infinite cardinal  $\kappa$  and for every  $n \in \omega$  we have  $\kappa^n = \kappa$ .*

For a cardinal  $\kappa$ , let  $\text{fin}(\kappa)$  denote the set of all finite subsets of  $\kappa$  and let  $\text{seq}(\kappa)$  denote the set of all finite sequences we can build with elements of  $\kappa$ . As a consequence of FACT 13.6 we have (see EXERCISE 13.3)

**FACT 13.7.** *For every infinite cardinal  $\kappa$  we have*

$$\kappa = |\text{fin}(\kappa)| = |\text{seq}(\kappa)|.$$



## NOTES

In 1905, Zermelo began to axiomatise Set Theory and in 1908 he published his first axiomatic system consisting of the seven axioms mentioned above. In 1930, he presented in [49] his second axiomatic system, which he called the ZF-system, in which he incorporated ideas of Fraenkel [10], Skolem [40], and von Neumann [32, 33, 34]. In fact, he added the Axiom Schema of Replacement (which was already used implicitly by Cantor in 1899) and the Axiom of Foundation to his former system, cancelled the Axiom of Infinity and did not explicitly mention the Axiom of Choice. More details can be found, for example, in the notes of Halbeisen [20, Ch. 3].

## EXERCISES

- 13.0 (a) Show that the Axiom of Empty Set follows from the Axiom Schema of Replacement.  
 (b) Show that the Axiom Schema of Separation follows from the Axiom Schema of Replacement.

*Hint:* Let  $A$  be a set and let  $\varphi(x)$  be a formula with  $\text{free}(\varphi) = \{x\}$ . Furthermore, let  $\psi(x, y)$  be the formula

$$(\varphi(x) \wedge y = x) \vee (\neg\varphi(x) \wedge y = \{A\}).$$

Then  $\psi(x, y)$  is a class function  $F$  and

$$F[A] \setminus \{\{A\}\} = \{x \in A : \varphi(x)\}.$$

- 13.1 (a) Define by transfinite recursion addition of ordinals.

*Hint:* For each  $\alpha \in \Omega$  define a class function  $F_\alpha$  by stipulating  $F_\alpha(x) := \emptyset$  if  $x$  is not a function; if  $x$  is a function, then let

$$F_\alpha(x) = \begin{cases} \alpha & \text{if } x = \emptyset, \\ x(\beta) \cup \{x(\beta)\} & \text{if } \text{dom}(x) = \beta + 1 \text{ and } \beta \in \Omega, \\ \bigcup_{\delta \in \beta} x(\delta) & \text{if } \text{dom}(x) = \beta \text{ and } \beta \in \Omega \setminus \{\emptyset\} \text{ is a limit ordinal,} \\ \emptyset & \text{otherwise.} \end{cases}$$

- (b) Define by transfinite recursion multiplication of ordinals.  
 (c) Define by transfinite recursion exponentiation of ordinals.

- 13.2 For limit ordinals  $\alpha \in \Omega$ ,  $\bigcup_{\delta \in \alpha} \aleph_\delta$  is a cardinal

*Hint:* Let  $\lambda := \bigcup_{\delta \in \alpha} \aleph_\delta$ . Then  $\lambda$  is an ordinal, and if  $|\lambda| < \lambda$ , then there is a  $\delta \in \alpha$  such that  $|\lambda| = \aleph_\delta$ .

- 13.3 (a) If  $\kappa$  is an infinite cardinal, then  $\kappa = |\text{seq}(\kappa)|$ .

*Hint:* Notice that

$$|\text{seq}(\kappa)| = \left| \bigcup_{n \in \omega} \kappa^n \right| = \aleph_0 \cdot \kappa.$$

- (b) If  $\kappa$  is an infinite cardinal, then  $\kappa = |\text{fin}(\kappa)|$ .

- 13.4 Show that addition, multiplication, and exponentiation of natural numbers (*i.e.*, of elements of  $\omega$ ) can be defined within the axiom system Z. In particular, addition, multiplication, and exponentiation of ordinals in  $\omega$  can be defined without the Axiom Schema of Replacement (*i.e.*, without the help of the TRANSFINITE RECURSION THEOREM).