Chapter 1

# Counting to Infinity

## Introduction

The general purpose of this chapter is to provide tools for comparing sizes of infinities. To this aim we develop in 1.3-1.6 the notion of *ordinals* which constitute a natural infinite extension of natural numbers. Ordinals classify well-ordered sets and are a natural device for using transfinite induction. A fundamental and very useful fact is that ordinals are endowed with arithmetic operations extending those of natural numbers, even though some classical properties do not extend (for instance addition of ordinals is no longer commutative).

Building on the notion of ordinals, we develop in 1.7-1.10 the concept of *cardinals*, which is the right notion to compare the size of sets. Unlike the case of ordinals, one needs to assume the validity of the Axiom of Choice (which we discuss in 1.7) to develop a full fledged theory of cardinals. In the last sections of this chapter, we study cardinal arithmetic, which appears to have a much richer theory of exponentation than ordinal arithmetic.

## 1.1. Naive Set Theory

In this chapter we shall use the notions of *set* and *natural number* in the same way as in any mathematical textbook, that is, in a naive sense,

without further questioning. It is only in the last chapter that we shall introduce the classical ZFC system of axioms of Zermelo-Fraenkel (plus the Axiom of Choice). We shall see that the notions and results of this first chapter remain valid in the more formal *axiomatic Set Theory*, using only the axioms of ZFC. We shall thus develop Cantor's theory of ordinal and cardinal numbers from this naive point of view.

When $A$ and $B$ are sets, we denote by $A \cup B$, $A \cap B$ and by $A \setminus B$ their set-theoretic *union*, *intersection* and *difference*, respectively. More generally, if $I$ is a set and $(A_i)_{i \in I}$ is a family of sets indexed by $I$, we denote its union by $\bigcup_{i \in I} A_i$ and its intersection by $\bigcap_{i \in I} A_i$; thus we have $x \in \bigcup_{i \in I} A_i$ if and only $x \in A_i$ for some $i \in I$ and $x \in \bigcap_{i \in I} A_i$ if and only $x \in A_i$ for every $i \in I$.

We write $A \subseteq B$ if $A$ is a *subset* of $B$, and $A \subset B$ if $A$ is a *proper subset* of $B$. The *power set* of $A$ is denoted by $\mathcal{P}(A)$. It is the set of subsets of $A$; thus $C \in \mathcal{P}(A)$ if and only if $C \subseteq A$.

We denote by $\mathbb{N}$ the set $\{0, 1, 2, ...\}$ of natural numbers, and we write $\mathbb{N}^*$ for $\mathbb{N} \setminus \{0\}$.

We will make constant use of the *extensionality principle* according to which two sets containing the same elements are equal.

We shall also make use of the *comprehension principle* which states that given a set $A$ and a property $P$ of sets, there exists a set whose elements are exactly those elements of $A$ that satisfy property $P$. We defer to Section 6.2 for a more precise formulation.

## 1.2. The Cantor and Cantor-Bernstein Theorems

The existence of an injective, surjective or bijective function between two sets may be seen as a way to compare their "size". We start with two results going in that direction.

**Theorem 1.2.1** (Cantor). *Let $A$ be a set. There is no surjection $A \to \mathcal{P}(A)$.*

**Proof.** Let $f : A \to \mathcal{P}(A)$ be a map. Consider the set

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

For every $x \in A$ with $f(x) = B$, we have $x \in B$ if and only if $x \notin B$. Hence $B$ does not belong to the image of $f$. □

**Theorem 1.2.2** (Cantor-Bernstein). *Let $A$ and $B$ be sets, and let $f : A \to B$ and $g : B \to A$ be injective maps. Then there exists a bijection $h : B \to A$.*

**Proof.** We may assume $A$ is a subset of $B$ and $f$ is the inclusion map. Indeed, one may replace $A$ by $f(A)$ and $g$ by $f \circ g$. Now set $C = \{g^n(x) \mid n \in \mathbb{N},\ x \in B \setminus A\}$. Define a map $h : B \to A$ by $h(c) = g(c)$ when $c \in C$ and $h(x) = x$ when $x \in B \setminus C$. The map $h$ is surjective: indeed, any $x \in A \cap C$ is of the form $x = g(y)$ for some $y \in C$ and for any $x \in A \setminus C$, $x = h(x)$. It is also clearly injective. □

**Definition.** Let $X$ and $Y$ be sets. One says that $X$ and $Y$ are *equinumerous*, and writes $X \sim Y$, if there exists a bijection between $X$ and $Y$; one says $X$ is *subnumerous* to $Y$, and writes $X \preccurlyeq Y$, if there exists an injection $X \to Y$.

Using this terminology, the Cantor-Bernstein Theorem may be restated as: if $X \preccurlyeq Y$ and $Y \preccurlyeq X$, then $X \sim Y$.

## 1.3. Orders

This section and the next one are devoted to preliminary results on ordered sets that are needed to develop the theory of ordinals.

**Definition.** A *partial order* $<$ on a set $X$ is a binary relation (that is, given by a subset of $X \times X$) which is *transitive* (if $x < y$ and $y < z$ then $x < z$) and *antireflexive* ($x \not< x$). If furthermore, for every $x, y \in X$ one has $x < y$, $x = y$ or $y < x$, one says $<$ is a *total order*.

One writes $x \leq y$ to mean $x < y$ or $x = y$, $x > y$ for $y < x$, and $x \geq y$ for $y \leq x$.

If $Y \subseteq X$, $y \in Y$ is a *smallest element* if for every $y'$ in $Y$, $y \leq y'$. It is a *minimal element* if for every $y'$ in $Y$, $y' \not< y$. One similarly defines a *largest element* and a *maximal element*. A *lower bound* of $Y$ is an element of $X$ which is $\leq$ all elements in $Y$. An *infimum* of $Y$ is a largest element in the set of lower bounds of $Y$. One similarly defines the notion of *upper bound* and *supremum*.

Note that in a partial order, if $a \leq b$ and $b \leq a$ then $a = b$. Thus smallest and largest elements are unique, which is in general not the case for minimal or maximal elements.

**Remark 1.3.1.** If $<$ is a partial order, $\leq$ is a *reflexive* relation ($x \leq x$ for every $x \in X$), transitive and *antisymmetric* (if $x \leq y$ and $y \leq x$ then $x = y$).

Conversely, if $\leq$ is a binary relation on a set $X$ which is reflexive, transitive and antisymmetric then the relation $<$ defined by $x < y :\Leftrightarrow (x \leq y \text{ and } x \neq y)$ is a partial order on $X$.

**Proof.** Exercise. □

**Definition.**

(1) Let $<$ be a partial order on $X$. We say $<$ is *well-founded* if any non-empty subset of $X$ contains a minimal element.

(2) A *well-order* is a well-founded total order.

**Remark 1.3.2.** Let $<$ be a partial order on $X$.

(1) The map $a \mapsto X_{\leq a} = \{x \in X \mid x \leq a\}$ identifies $(X, <)$ with a subset $Y$ of $\mathcal{P}(X)$ endowed with the partial order induced by $\subset$.

(2) $<$ is well-founded if and only if there is no infinite decreasing sequence in $X$.

(3) $<$ is a well-order if and only if every non-empty subset of $X$ contains a smallest element.

**Proof.** The proofs of (1) and (3) are left as exercises.

Let us prove (2). If $(X, <)$ is not well-founded, there exists a subset $\emptyset \neq Y \subseteq X$ without minimal element. By induction on $n \in \mathbb{N}$ one may construct $y_n \in Y$ such that $y_{n+1} < y_n$. Conversely, if $(y_n)_{n\in\mathbb{N}}$ is a decreasing sequence, it is clear that $Y = \{y_n \mid n \in \mathbb{N}\}$ does not contain a minimal element. □

**Example 1.3.3.**

(1) The usual order $<$ on $\mathbb{Z}$ is a non-well-founded total order. Its restriction to $\mathbb{N}$ is a well-order.

(2) For every set $X$, the relation $\subset$ is a partial order on $\mathcal{P}(X)$ which is well-founded if and only if $X$ is finite.[1]

(3) The restriction of a partial order (resp. total, well-founded) on $X$ to $Y \subseteq X$ is a partial order (resp. total, well-founded) on $Y$.

## 1.4. Operations on Orders

**Definition.** Let $X$ and $Y$ be partially ordered sets.

(1) The *ordered sum* of $X$ and $Y$, denoted by $X + Y$, is the partially ordered set consisting of pairs $(x, 0)$ with $x \in X$ and $(y, 1)$ with $y \in Y$, the order being defined as follows: $(a, i) < (b, j)$ if $i < j$ or if $i = j$ and $a < b$.

(2) The *reverse lexicographic product* of $X$ and $Y$ is defined by endowing the cartesian product $X \times Y$ with the order: $(x, y) < (x', y')$ if $y < y'$ or if $y = y'$ and $x < x'$. It is still denoted by $X \times Y$.

By an *isomorphism* between two partially ordered sets $X$ and $Y$ we mean a bijection $f$ between $X$ and $Y$ such that for any $x, x' \in X$ one has $x < x'$ if and only if $f(x) < f(x')$.

**Lemma 1.4.1.**

(1) *The ordered sum of total orders* (*resp. well-founded partial orders*) *is a total order* (*resp. well-founded*).

(2) *The reverse lexicographic product of two total orders* (*resp. well-founded partial orders*) *is a total order* (*resp. well-founded*).

(3) *Let $X$, $Y$ and $Z$ be partially ordered. We have the following canonical isomorphisms of partially ordered sets:*
   (a) $(X + Y) + Z \cong X + (Y + Z)$.
   (b) $(X \times Y) \times Z \cong X \times (Y \times Z)$.
   (c) $X \times (Y + Z) \cong (X \times Y) + (X \times Z)$.

**Proof.** The only non-trivial point to check is that the reverse lexicographic product of two well-founded partially ordered sets is well-founded.

[1] By a *finite* set we mean a set into which $\mathbb{N}$ does not inject.

Let $X$ and $Y$ be two well-founded partially ordered sets. Let $Z$ be a non-empty subset of $X \times Y$. We denote by $\pi : X \times Y \to Y$ the projection on the second factor. The order on $Y$ being well-founded, there exists a minimal element $y_0$ in $\pi(Z) \subseteq Y$. Since the order on $X$ is well-founded, there is a minimal element $x_0$ in the (non-empty) set $Z_{y_0} = \{x \in X \mid (x, y_0) \in Z\}$. It is clear that $(x_0, y_0)$ is minimal in $Z$. □

**Definition.** Let $X$ and $Y$ be totally ordered sets. We assume that $X$ admits a smallest element 0. One defines the partially ordered set $X^{(Y)}$ as follows. As a set, it is the set of functions from $Y$ to $X$ with finite support, that is, the subset of the set $X^Y$ of all functions $Y \to X$ consisting of functions $f : Y \to X$ such that

$$\mathrm{supp}(f) := \{y \in Y \mid f(y) \neq 0\}$$

is finite. One sets $f < g$ if there exists $y \in Y$ such that $f(y) < g(y)$ and $f(y') = g(y')$ for every $y' > y$.

**Proposition 1.4.2.** *Let $X, Y$ and $Z$ be totally ordered sets, and assume that $X$ admits a smallest element* 0.

(1) *The relation $<$ defines a total order on $X^{(Y)}$ which is well-founded when the orders on $X$ and $Y$ are both well-founded.*

(2) *There are canonical isomorphisms of totally ordered sets $X^{(Y+Z)} \cong X^{(Y)} \times X^{(Z)}$ and $X^{(Y \times Z)} \cong \left(X^{(Y)}\right)^{(Z)}$.*

**Proof.** The only non-trivial point to check is that if $X$ and $Y$ are well-ordered, then $X^{(Y)}$ is well-founded. Let $Z$ be a non-empty subset of $X^{(Y)}$. Let us prove that $Z$ contains a smallest element. If the constant function with value 0 belongs to $Z$, there is nothing to prove. Hence, we may assume $\mathrm{supp}(f) \neq \emptyset$ for every $f \in Z$. Let

$$Y_1 = \{s_1(f) \mid f \in Z\},$$

where $s_1(f) = \max(\mathrm{supp}(f))$. Let $y_1$ be the smallest element of $Y_1$, and set $Z_1' = \{f \in Z \mid s_1(f) = y_1\}$. The set $Z_1'$ is an *initial segment* of $Z$, in other words $f < g$ for every $f \in Z_1'$ and $g \in Z \setminus Z_1'$. Let $x_1$ be the smallest element of $\{f(y_1) \mid f \in Z_1'\}$. We set

$$Z_1 = \{f \in Z_1' \mid f(y_1) = x_1\}.$$

The set $Z_1$ is an initial segment of $Z_1'$. If $Z_1$ contains the function with constant value 0 outside $\{y_1\}$, we are done. Otherwise, we have $\mathrm{supp}(f) \setminus \{y_1\} \neq \emptyset$ for every $f \in Z_1$. Let $Y_2 = \{s_2(f) \mid f \in Z_1\}$, where $s_2(f) = \max(\mathrm{supp}(f) \setminus \{y_1\})$. Let $y_2$ be the smallest element of $Y_2$, and $x_2$ the smallest element of $\{f(y_2) \mid f \in Z_1 \text{ and } y_2 = s_2(f)\}$. We set $Z_2 = \{f \in Z_1 \mid s_2(f) = y_2 \text{ and } f(y_2) = x_2\}$. It is an initial segment of $Z_1$. If $Z_2$ contains the function with constant value 0 outside $\{y_1, y_2\}$, we are done, otherwise one continues in the same way, constructing $Y_3, y_3, Z_3', x_3, Z_3$ and so on. Since the sequence $(y_i)$ is strictly decreasing in $Y$, this process stops after a finite number of steps. □

## 1.5. Ordinal Numbers

A set $X$ is said to be *transitive* if for all $x \in X$ and $y \in x$ one has $y \in X$. This is equivalent to $x \in X \Rightarrow x \subseteq X$.

**Definition.** A set $X$ is an *ordinal* if it is transitive and if the relation $\{(x, y) \in X \times X \mid x \in y\}$ on $X$ defines a well-order on $X$.

**Proposition 1.5.1.** *Let $\alpha$ and $\beta$ be ordinals.*

(1) *$\emptyset$ is an ordinal.*

(2) *If $\alpha \neq \emptyset$, then $\emptyset \in \alpha$.*

(3) *$\alpha \notin \alpha$.*

(4) *If $x \in \alpha$, then $x = S_{<x} := \{y \in \alpha \mid y < x\}$.*

(5) *If $x \in \alpha$, then $x$ is an ordinal.*

(6) *$\beta \subseteq \alpha$ if and only if $\beta \in \alpha$ or $\beta = \alpha$.*

(7) *$x := \alpha \cup \{\alpha\}$ is an ordinal, denoted by $\alpha^+$.*

**Proof.** (1) is clear. For (2), one considers $x \in \alpha$ minimal. If $y \in x$, then $y \in \alpha$ by transitivity of $\alpha$, and $x$ would not be minimal. In (3), by antireflexivity, we have $x \notin x$ for every $x \in \alpha$. Thus $\alpha \in \alpha$ implies $\alpha \notin \alpha$. (4) follows from the fact that $<$ is given by $\in$. To prove (5), note that $\in$ restricts to a well-order on $x$, since $x \subseteq \alpha$. Furthermore, $x = S_{<x}$ is transitive, since $z \in y \in x \Rightarrow z < x \Rightarrow z \in S_{<x}$.

To prove the 'only if' part in (6), let us assume that $\beta \subset \alpha$. Let $x$ be minimal in $\alpha \setminus \beta$. Clearly $\beta \supseteq S_{<x}$ by minimality. Furthermore, if

$y \in \beta$, then $y \in x$ since otherwise $x \in y$ and $x \in \beta$. Hence $\beta = S_{<x} = x \in \alpha$. The other implication in (6) is clear, and the verification of (7) is immediate. □

**Proposition 1.5.2.** *Let $X$ be a non-empty set of ordinals. Then $\bigcap_{\alpha\in X} \alpha$ is a smallest element of $X$.*

**Proof.** The intersection of a family of transitive sets is transitive, and the restriction of a well-order to a subset is a well-order. Hence $\beta = \bigcap_{\alpha\in X} \alpha$ is an ordinal. We have $\beta \subseteq \alpha$ for every $\alpha \in X$. If $\beta \notin X$, then $\beta \in \alpha$ for every $\alpha \in X$, by Proposition 1.5.1(6). It follows that $\beta \in \beta$, which is absurd. □

**Theorem 1.5.3.** *Let $\alpha$ and $\beta$ be ordinals. Exactly one of the following properties holds:*

$$(1)\ \alpha \in \beta, \qquad (2)\ \alpha = \beta, \qquad (3)\ \beta \in \alpha.$$

**Proof.** One sets $X = \{\alpha, \beta\}$, and one applies Proposition 1.5.2. If $\alpha \cap \beta = \alpha$, then $\alpha \subseteq \beta$, hence $\alpha = \beta$ or $\alpha \in \beta$ by Proposition 1.5.1(6). Similarly, if $\alpha \cap \beta = \beta$, then $\alpha = \beta$ or $\beta \in \alpha$. The fact that these properties are mutually exclusive follows from the axioms of a partial order. □

**Notation.** From now on, we shall write $\alpha < \beta$ for $\alpha \in \beta$, and $\alpha \leq \beta$ for $\alpha \subseteq \beta$, when $\alpha$ and $\beta$ are ordinals.

**Proposition 1.5.4.** *Let $X$ be a set of ordinals. Then $b = \bigcup_{\alpha\in X} \alpha$ is an ordinal. Furthermore, if $\gamma$ is an ordinal with $\gamma < b$, there exists $\alpha \in X$ such that $\gamma \in \alpha$. We shall also write $b = \sup_{\alpha\in X} \alpha$.*

**Proof.** The set $b$ being the union of transitive sets, it is transitive. Furthermore, $b$ contains only ordinals. By Theorem 1.5.3, $\in$ induces a total order on $b$. If $\emptyset \neq Z \subseteq b$, then $\bigcap_{\alpha\in Z} \alpha$ is a smallest element of $Z$ by Proposition 1.5.2. This shows that the order given by $\in$ on $b$ is well-founded. □

An ordinal of the form $\alpha^+$ is called *a successor ordinal*. It is clear that $\alpha^+$ is the smallest ordinal $> \alpha$.

**Definition.** A *limit ordinal* is a non-empty ordinal which is not a successor.

**Proposition 1.5.5.** *For an ordinal $\lambda \neq \emptyset$, the following conditions are equivalent:*

(1) *$\lambda$ is a limit ordinal;*

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

**Proof.** (1)⇒(2). Let $\beta = \bigcup_{\alpha<\lambda} \alpha$ and $\lambda$ a limit. It is clear that $\beta \subseteq \lambda$. Conversely, assume $\alpha < \lambda$. Then $\alpha^+ \leq \lambda$ and it follows that $\alpha^+ < \lambda$ since $\lambda$ is a limit ordinal. The statement follows, since $\alpha \in \alpha^+ \subseteq \beta$.

(2)⇒(1). If $\lambda = \gamma^+$, then $\bigcup_{\alpha<\lambda} \alpha = \bigcup_{\alpha\leq\gamma} \alpha = \gamma < \lambda$. □

**Example 1.5.6.**

(1) One can recover the *natural numbers as ordinals* as follows. One sets $\underline{0} := \emptyset$, and inductively $\underline{n+1} := \underline{n}^+$ for $n \in \mathbb{N}$. For instance $\underline{1} = \{\emptyset\}$, $\underline{2} = \{\underline{0}, \underline{1}\} = \{\emptyset, \{\emptyset\}\}$, $\underline{3} = \{\underline{0}, \underline{1}, \underline{2}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

One proves by induction that $\underline{n}$ is an ordinal for every natural number $n$. We shall often identify $\underline{n}$ and $n$.

(2) One sets $\omega := \bigcup_{n\in\mathbb{N}} \underline{n}$. It is an ordinal by Proposition 1.5.4.

**Definition.** One says that an ordinal is *finite* if it is not a limit and none of its elements is a limit.

**Proposition 1.5.7.**

(1) *$\omega$ is the set of finite ordinals.*

(2) *$\omega$ is the smallest limit ordinal.*

**Proof.** One proves first, by induction on $n \in \mathbb{N}$, that all elements of $\omega$ are finite ordinals. Furthermore, $\alpha < \omega$ implies $\alpha^+ < \omega$. This proves (2). If $\alpha \notin \omega$, then $\omega \leq \alpha$, so either $\alpha = \omega$ or $\omega \in \alpha$. In both cases, $\alpha$ is not finite. This proves (1). □

**Lemma 1.5.8.** *Let $f : \alpha \to \alpha'$ be a strictly increasing map between two ordinals. Then $f(\beta) \geq \beta$ for every $\beta \in \alpha$. In particular, $\alpha \leq \alpha'$, and if $f$ is an isomorphism of ordered sets, then $\alpha = \alpha'$ and $f$ is equal to the identity.*

**Proof.** If there exists $\beta \in \alpha$ with $f(\beta) < \beta$, we consider $\beta_0$ minimal with that property. Since $f$ is strictly increasing, we have $f(f(\beta_0)) < f(\beta_0)$, which contradicts minimality.

The statement about an isomorphism $f$ follows by applying the result to $f$ as well as to $f^{-1}$. □

**Theorem 1.5.9** (Classification of well-orders by ordinals)**.** *Every well-ordered set $X$ is isomorphic, as an ordered set, to some ordinal. Furthermore, the ordinal and the isomorphism are both unique.*

**Proof.** Uniqueness follows from Lemma 1.5.8. To prove existence, let us first note that for every $x \in X$, any isomorphism between $S_{<x}$ and an ordinal $\alpha$ can be extended to an isomorphism between $S_{\leq x} = S_{<x} \cup \{x\}$ and $\alpha^+$. Let

$$Y = \{y \in X \mid \text{ there exists } f : S_{\leq y} \cong \alpha \text{ for some ordinal } \alpha\}.$$

By uniqueness, for $y \in Y$, the ordinal $\alpha = \alpha(y)$ and the isomorphism $f = f_y$ are unique. Let us prove $Y = X$. Otherwise, there would exist $x \in X$ minimal in $X \setminus Y$. For $y < x$ we have an isomorphism $f_y : S_{\leq y} \cong \alpha(y)$. Furthermore, these isomorphisms form a coherent family in the sense that for every $y' < y < x$ we have $f_y \restriction_{S_{\leq y'}} = f_{y'}$. (To see this, note that an initial segment of an ordinal is an ordinal.) We set

$$\alpha = \sup_{y<x} \alpha(y) \text{ and } f : S_{<x} \to \alpha,\ f(y) := f_y(y).$$

It is clear that $f$ is well defined and induces an isomorphism of ordered sets between $S_{<x}$ and $\alpha$. By the observation made at the beginning, $f$ may be extended to an isomorphism between $S_{\leq x}$ and $\alpha^+$, which leads to a contradiction. So we have $Y = X$. To conclude, one uses the same kind of argument, setting $\alpha(X) := \sup_{x \in X} \alpha(x)$ and $f : X \cong \alpha(X)$, $x \mapsto f_x(x)$. □

**Remark 1.5.10** (Transfinite induction)**.** Let $P$ be a property of ordinals. One assumes:

- $\emptyset$ satisfies $P$;
- for every ordinal $\alpha$: if $\alpha$ satisfies $P$, then $\alpha^+$ satisfies $P$;
- for every limit ordinal $\lambda$: if every $\alpha < \lambda$ satisfies $P$, then $\lambda$ satisfies $P$.

Then every ordinal satisfies $P$.

## 1.6. Ordinal Arithmetic

If $\alpha$ and $\beta$ are ordinals, by Theorem 1.5.9 there is a unique ordinal isomorphic to the ordered sum of $\alpha$ and $\beta$, which one denotes by $\alpha+\beta$. One similarly defines $\alpha\beta$ as the unique ordinal isomorphic to the reverse lexicographic product $\alpha\times\beta$ and $\alpha^\beta$ as the unique ordinal isomorphic to the ordered set $\alpha^{(\beta)}$. Note that $0^\beta$ has still to be defined: one sets $0^0 := 1$ and $0^\beta := 0$ for every $\beta > 0$.

**Proposition 1.6.1** (Ordinal addition)**.** *Let $\alpha, \beta$ and $\gamma$ be ordinals.*

(1) $\alpha + 0 = 0 + \alpha = \alpha$.

(2) $\alpha + 1 = \alpha^+$.

(3) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, *in particular* $\alpha + \beta^+ = (\alpha + \beta)^+$.

(4) $\alpha < \beta$ *if and only if there exists an ordinal* $\delta > 0$ *such that* $\beta = \alpha + \delta$.

(5) *If* $\beta < \gamma$, *then* $\alpha + \beta < \alpha + \gamma$ *for every* $\alpha$. *In particular, one may simplify on the left:* $\alpha + \beta = \alpha + \gamma \Rightarrow \beta = \gamma$.

(6) *If* $\lambda$ *is a limit, then* $\alpha + \lambda = \sup_{\beta<\lambda}(\alpha + \beta)$ (*continuity*).

(7) $1 + \alpha = \alpha + 1$ *when* $\alpha$ *is finite, otherwise* $1 + \alpha = \alpha$.

**Proof.** (1) and (2) are clear, and (3) follows from Lemma 1.4.1. For the non-trivial implication in (4), one easily checks that the ordinal $\delta$ isomorphic to the well-ordered set $\beta \setminus \alpha$ does the job.

(5) If $\beta < \gamma$, by (2) and (4) one has $\gamma = \beta+\delta$, hence $\alpha+\gamma = (\alpha+\beta)+\delta$, for some $\delta > 0$.

(6) $\alpha + \lambda \geq \sup_{\beta<\lambda}(\alpha + \beta)$ follows from (5). Conversely, suppose $\alpha \leq \mu < \alpha + \lambda$. Then $\mu = \alpha + \delta$ for some $\delta$ with $0 \leq \delta < \lambda$. Since $\lambda$ is a limit, one has $\delta^+ < \lambda$, hence $\mu < \alpha + \delta^+ \leq \sup_{\beta<\lambda}(\alpha + \beta)$.

(7) One proves by induction on $n \in \mathbb{N}$ that $1 + n = n + 1$. By (6) we have $1 + \omega = \omega$. Finally, $\alpha \geq \omega$ can be written as $\alpha = \omega + \beta$, hence $1 + \alpha = 1 + \omega + \beta = \omega + \beta = \alpha$. □

From now on, we shall allow the omission of parentheses, using the convention that exponentiation ties are stronger than multiplication and

that multiplication ties are stronger than addition. For instance, one should read $\alpha\beta + \gamma$ as $(\alpha\beta) + \gamma$, and $\gamma\alpha^\beta$ as $\gamma\left(\alpha^\beta\right)$.

**Proposition 1.6.2** (Ordinal multiplication)**.** *Let $\alpha, \beta, \gamma$ be ordinals.*

(1) $\alpha 0 = 0\alpha = 0$.

(2) $\alpha 1 = 1\alpha = \alpha$.

(3) $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

(4) $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$, *in particular* $\alpha\beta^+ = \alpha\beta + \alpha$.

(5) $2\omega = \omega < \omega 2 = \omega + \omega$.

(6) *Assume $\alpha \neq 0$. If $\beta < \gamma$, then $\alpha\beta < \alpha\gamma$. In particular, one may simplify on the left: $\alpha\beta = \alpha\gamma \Rightarrow \beta = \gamma$.*

(7) *If $\lambda$ is a limit ordinal, then $\alpha\lambda = \sup_{\beta<\lambda} \alpha\beta$ (continuity).*

**Proof.** (1) and (2) are clear, (3) and (4) follow from Lemma 1.4.1. For (6), it suffices to note that if $\beta < \gamma$ then $\gamma = \beta + \delta$ for some $\delta > 0$, hence $\alpha\gamma = \alpha\beta + \alpha\delta$ by (4) from which it follows that $\alpha\gamma > \alpha\beta$.

(7) One may assume $\alpha \neq 0$. Let $\lambda$ be a limit ordinal. The inequality $\alpha\lambda \geq \sup_{\beta<\lambda} \alpha\beta =: \delta$ follows from (6). Conversely, let $\gamma < \alpha\lambda$. Euclidean division, proved in the next lemma, provides a pair of ordinals $(\rho, \mu)$ such that $\gamma = \alpha\mu + \rho$, with $\rho < \alpha$. Since $\mu < \lambda$ by (6), we have $\mu^+ < \lambda$ because $\lambda$ is a limit ordinal, hence $\gamma = \alpha\mu + \rho < \alpha\mu + \alpha = \alpha\mu^+ \leq \delta$. In (5), $2\omega = \omega$ follows from (7), the other statements being clear. □

**Lemma 1.6.3** (Euclidean division)**.** *Let $\alpha$ and $\beta$ be ordinals, with $\alpha \neq 0$. Then there exists a unique pair of ordinals $(\rho, \mu)$ such that $\rho < \alpha$ and $\beta = \alpha\mu + \rho$.*

**Proof.** Uniqueness: Assume $\alpha\mu + \rho = \alpha\mu' + \rho'$ with $\rho, \rho' < \alpha$. If $\mu < \mu'$, then $\alpha\mu + \rho < \alpha\mu^+ \leq \alpha\mu' \leq \alpha\mu' + \rho'$, which is absurd. Hence $\mu = \mu'$ by symmetry, and one obtains $\rho = \rho'$ after simplifying.

Existence: When $\beta = 0$ there is nothing to prove. Assume $\beta \neq 0$. The mapping $f_0 : \beta \to \alpha \times \beta$, $x \mapsto (0, x)$ is strictly increasing, hence $\beta \leq \alpha\beta$ by Lemma 1.5.8. If $\beta = \alpha\beta$, one sets $\mu = \beta$ and $\rho = 0$. Otherwise, we have $\beta \in \alpha\beta$. Let $f$ be the unique isomorphism of ordered sets between $\alpha\beta$ and $\alpha \times \beta$. One sets $(\rho, \mu) = f(\beta)$. Since $S_{<(\rho,\mu)} \cong (\alpha \times \mu) + \rho$ it follows that $\beta = \alpha\mu + \rho$. □

Note that we have only used properties (1)–(4) and (6) from Proposition 1.6.2 in our proof of Euclidean division, thus avoiding circularity.

**Proposition 1.6.4** (Ordinal exponentiation)**.** *Let $\alpha, \beta, \gamma$ be ordinals.*

(1) *For every $\alpha$, we have $\alpha^0 = 1$, $\alpha^1 = \alpha$ and $1^\alpha = 1$. If $\alpha \neq 0$, then $0^\alpha = 0$.*

(2) *$\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma$, in particular $\alpha^{\beta^+} = \alpha^\beta \alpha$.*

(3) *$\left(\alpha^\beta\right)^\gamma = \alpha^{\beta\gamma}$.*

(4) *If $\alpha > 1$ and $\beta < \gamma$, then $\alpha^\beta < \alpha^\gamma$.*

(5) *If $\lambda$ is a limit ordinal and $\alpha \neq 0$, then $\alpha^\lambda = \sup_{\beta<\lambda} \alpha^\beta$ (continuity).*

**Proof.** (1) is checked directly, and statements (2) and (3) follow from Proposition 1.4.2.

(4) $\beta < \gamma \Rightarrow \gamma = \beta + \delta$ for some $\delta > 0$. Hence $\alpha^\gamma = \alpha^{\beta+\delta} = \alpha^\beta \alpha^\delta$. But $\alpha^\delta > 1$ since as a set $\alpha^{(\delta)}$ contains at least two elements. It follows that $\alpha^\gamma > \alpha^\beta$ by Proposition 1.6.2(6).

Let us prove the non-trivial inequality in (5). Let $f \in \alpha^{(\lambda)}$. One may assume $f$ is not the constant function with value 0. Then $s_1(f) < \lambda$, and hence $\beta = s_1(f)^+ < \lambda$, which proves there exists a strictly increasing function $S_{\leq f} \to \alpha^{(\beta)}$. One concludes by Lemma 1.5.8. □

**Remark 1.6.5.** The following formulas would allow us to define ordinal addition, multiplication and exponentiation by transfinite induction:

- $\alpha + 0 = \alpha$, $\alpha + \beta^+ = (\alpha + \beta)^+$, and $\alpha + \lambda = \sup_{\beta<\lambda}(\alpha + \beta)$ for $\lambda$ a limit ordinal.
- $\alpha 0 = 0$, $\alpha\beta^+ = \alpha\beta + \alpha$, and $\alpha\lambda = \sup_{\beta<\lambda}(\alpha\beta)$ for $\lambda$ a limit ordinal.
- Assume $\alpha \neq 0$. Then one has $\alpha^0 = 1$, $\alpha^{\beta^+} = \alpha^\beta \alpha$, and $\alpha^\lambda = \sup_{\beta<\lambda}\left(\alpha^\beta\right)$ for $\lambda$ a limit ordinal.

## 1.7. The Axiom of Choice

Given a family of sets $(X_i)_{i\in I}$, one defines their *product* as

$$\prod_{i\in I} X_i = \left\{ f : I \to \bigcup_{i\in I} X_i \;\middle|\; f(i) \in X_i \text{ for all } i \in I \right\}.$$

**Definition.** The *Axiom of Choice* (AC) states that the product of a family of non-empty sets is non-empty: if $X_i \neq \emptyset$ for all $i \in I$, then $\prod_{i\in I} X_i \neq \emptyset$.

In the Zermelo-Fraenkel system of axioms ZF, (AC) is equivalent to *Zorn's Lemma* and also to *Zermelo's Theorem*. We shall prove these equivalences in the last chapter of this book, and accept them for the moment.

**Definition.** A partially ordered set $X$ is *inductive* if any totally ordered subset $Y \subseteq X$ admits an upper bound in $X$. (In particular, such an $X$ is non-empty).

**Zorn's Lemma.** Every inductive partially ordered set admits a maximal element.

**Zermelo's Theorem** (Wohlordnungssatz)**.** Every set can be well-ordered.

## 1.8. Cardinal Numbers

We now assume, until the end of the penultimate chapter, that the Axiom of Choice holds.

**Definition.** An ordinal is a *cardinal* if it is not equinumerous to a smaller ordinal.

**Example 1.8.1.**

(1) Any finite ordinal is a cardinal.

(2) The ordinal $\omega$ is a cardinal. When considered as a cardinal it will be denoted by $\aleph_0$.

(3) If $\alpha$ is an infinite ordinal, then $\alpha^+$ is not a cardinal. (Indeed, $\alpha^+$ and $\alpha$ are equinumerous.)

**Proposition 1.8.2.** *Any set $X$ is equinumerous to a unique cardinal, denoted by* $\mathrm{card}(X)$.

**Proof.** By Zermelo's Theorem and Theorem 1.5.9, $X$ is equinumerous to an ordinal $\alpha$. Let $\beta \leq \alpha$ be minimal such that $\beta$ is equinumerous to $\alpha$. Then $\beta$ is a cardinal and is in bijection with $X$. Uniqueness is clear. □

**Proposition 1.8.3.** *Let $X$ and $Y$ be sets and assume that $X$ is non-empty. The following statements are equivalent:*

(1) $\mathrm{card}(X) \leq \mathrm{card}(Y)$.

(2) *There exists an injective map $X \to Y$.*

(3) *There exists a surjective map $Y \to X$.*

**Proof.** (1)⇒(2) is easy.

(2)⇒(3): Let $f : X \to Y$ be an injective map. As $X$ is non-empty, one may fix $x_0 \in X$. One defines a surjective map $g : Y \to X$ by setting $g(y) := x_0$ if $y \notin \mathrm{im}(f) = \{f(x) \mid x \in X\}$, and $g(y) := f^{-1}(y)$ otherwise.

(3)⇒(1): If there exists a surjective map $Y \to X$, then there exists a surjection $g : \lambda = \mathrm{card}(Y) \to \kappa = \mathrm{card}(X)$. The map $f$ sending $\alpha \in \kappa$ to the minimal $\beta \in \lambda$ such that $g(\beta) = \alpha$ provides an injection $\kappa \to \lambda$. In particular, $\kappa$ is in bijection with some ordinal $\gamma \leq \lambda$. (One takes $\gamma$ as the unique ordinal which is isomorphic to the well-order induced on $\mathrm{im}(f)$.) □

**Definition.** A set $X$ is said to be *countable* if $\mathrm{card}(X) \leq \aleph_0$, and *finite* if $\mathrm{card}(X) < \aleph_0$.

**Proposition 1.8.4.** *Let $X$ be a set of cardinals. Then $\lambda = \sup_{\kappa \in X} \kappa$ is a cardinal.*

**Proof.** If $\alpha < \lambda$, then $\alpha < \kappa$ for some $\kappa \in X$. Since $\kappa$ is a cardinal, we have $\kappa = \mathrm{card}(\kappa) \leq \mathrm{card}(\lambda)$, and hence $\alpha < \mathrm{card}(\lambda)$. This proves that $\lambda$ is not equinumerous to some smaller ordinal. □

**Notation.** From now on, $\kappa, \lambda$, etc. will denote cardinals.

There is no largest cardinal. Indeed, if $\kappa$ is a cardinal, then $\lambda := \mathrm{card}(\mathcal{P}(\kappa)) > \kappa$ by Cantor's Theorem. In particular, the set of all cardinals $\leq \lambda$ that are $> \kappa$ is non-empty. We denote by $\kappa^+$ its smallest element, called the *cardinal successor* of $\kappa$. To avoid confusion, from now on the ordinal successor of $\alpha$ will be denoted by $\alpha + 1$.

**Definition.** The $\aleph$-*hierarchy* assigns to any ordinal a cardinal as follows:

- $\aleph_0 := \omega$.
- $\aleph_{\alpha+1} := \aleph_\alpha^+$.
- $\aleph_\alpha := \sup_{\beta<\alpha} \aleph_\beta$, if $\alpha$ is a limit ordinal.

By transfinite induction, one proves that $\alpha < \beta \Rightarrow \aleph_\alpha < \aleph_\beta$. In combination with the next result, it follows that the $\aleph$-hierarchy provides a strictly increasing enumeration of the infinite cardinals by the ordinals.

**Proposition 1.8.5.** *Every infinite cardinal is of the form $\aleph_\alpha$ for some $\alpha$.*

**Proof.** Let $\kappa$ be an infinite cardinal. The function $\beta \mapsto \aleph_\beta$ is strictly increasing on $\kappa + 1$, and it takes its values in $\aleph_{\kappa+1}$. Thus $\aleph_\kappa \geq \kappa$ by Lemma 1.5.8, and hence $\aleph_{\kappa+1} > \kappa$. Let $\alpha \leq \kappa + 1$ be minimal with $\aleph_\alpha > \kappa$. Since $\kappa \geq \aleph_0$, we have $\alpha > 0$. If $\alpha$ were a limit ordinal, by definition we would have $\kappa \in \bigcup_{\beta<\alpha} \aleph_\beta$, and hence $\kappa \in \aleph_\beta$ for some $\beta < \alpha$, which would contradict the minimality of $\alpha$. Thus $\alpha = \beta + 1$ and also $\aleph_\beta \leq \kappa < \aleph_{\beta+1} = \aleph_\beta^+$. Since $\aleph_\beta^+$ is the cardinal successor of $\aleph_\beta$, necessarily $\aleph_\beta = \kappa$. □

## 1.9. Operations on Cardinals

If $X$ and $Y$ are sets, one denotes by $X + Y$ their disjoint union, by $X \times Y$ their cartesian product and by $X^Y$ the set of maps from $Y$ to $X$. If $\kappa$ and $\lambda$ are cardinals, one denotes by $\kappa + \lambda$ the cardinal of their disjoint union, by $\kappa\lambda$ the cardinal of their cartesian product and by $\kappa^\lambda$ the cardinal of the set of maps from $\lambda$ to $\kappa$. These operations are respectively called *cardinal addition*, *cardinal multiplication* and *cardinal exponentiation*.

They should not be confused with the corresponding ordinal operations. For instance $2^\omega = \omega = \aleph_0 < 2^{\aleph_0}$; also $\aleph_0 2 = \aleph_0$, but $\omega < \omega 2$. It is clear that on finite cardinals all of these operations correspond to the usual arithmetic operations. Note that $\mathrm{card}(X+Y) = \mathrm{card}(X) + \mathrm{card}(Y)$, $\mathrm{card}(X \times Y) = \mathrm{card}(X)\mathrm{card}(Y)$ and $\mathrm{card}(X^Y) = \mathrm{card}(X)^{\mathrm{card}(Y)}$.

The proof of the following statements is immediate, using Proposition 1.8.3.

**Proposition 1.9.1.** *Let $\kappa, \lambda$ and $\mu$ be cardinals.*

(1) *Cardinal addition and multiplication are commutative and associative, multiplication is distributive with respect to addition, $\kappa^{\lambda+\mu} = \kappa^\lambda \kappa^\mu$, $(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$ and $(\kappa\lambda)^\mu = \kappa^\mu \lambda^\mu$.*

(2) *If $\kappa \leq \lambda$, then $\kappa + \mu \leq \lambda + \mu$, $\kappa\mu \leq \lambda\mu$ and $\kappa^\mu \leq \lambda^\mu$ (when $\kappa > 0$) and $\mu^\kappa \leq \mu^\lambda$ (when $\mu > 0$).* □

**Proposition 1.9.2.** *One has* $\mathrm{card}(\mathbb{R}) = 2^{\aleph_0}$.

**Proof.** There is an injection $h : 2^{\aleph_0} \to \mathbb{R}$ sending a sequence $(a_i)_{i\in\mathbb{N}}$ to the sum $\sum_i a_i 2^{-i}$ if the support of the sequence is infinite, and to $2 + \sum_i a_i 2^{-i}$ otherwise. This proves that $2^{\aleph_0} \leq \mathrm{card}(\mathbb{R})$. On the other hand, the image of $h$ contains the interval $(0, 1)$ which is equinumerous to $\mathbb{R}$ (for instance via $x \mapsto 1/\pi \arctan(x) + 1/2$); hence $\mathrm{card}(\mathbb{R}) \leq 2^{\aleph_0}$. □

**Proposition 1.9.3** (Hessenberg's Theorem)**.** *For every infinite cardinal $\kappa$, one has $\kappa\kappa = \kappa$.*

**Proof.** By induction on $\alpha$, we will prove that $\aleph_\alpha \aleph_\alpha = \aleph_\alpha$.

For $\alpha = 0$ this is clear. Indeed, the mapping $\alpha_2 : \mathbb{N}^2 \to \mathbb{N}$ defined by $\alpha_2(m, n) := 1/2(m + n + 1)(m + n) + n$ is bijective.

Let us now assume $\aleph_\beta \aleph_\beta = \aleph_\beta$ for every $\beta < \alpha$. One endows $\aleph_\alpha \times \aleph_\alpha$ with the following order:

$$\begin{aligned}(\beta, \gamma) < (\beta', \gamma') \text{ if } &\max(\beta, \gamma) < \max(\beta', \gamma'), \text{ or}\\ &\text{if } \max(\beta, \gamma) = \max(\beta', \gamma') \text{ and } \beta < \beta', \text{ or}\\ &\text{if } \max(\beta, \gamma) = \max(\beta', \gamma'), \beta = \beta' \text{ and } \gamma < \gamma'.\end{aligned}$$

One checks easily that this is a well-order. Furthermore, for every $\delta < \aleph_\alpha$, the set $\delta \times \delta$ is an initial segment for $<$. By Theorem 1.5.9, there is a unique isomorphism of ordered sets $f : \varepsilon \to \aleph_\alpha \times \aleph_\alpha$ with $\varepsilon$ an ordinal.

Assume $\varepsilon > \aleph_\alpha$. Then $\aleph_\alpha \in \varepsilon$ and $f(\aleph_\alpha) = (\beta_0, \gamma_0) \in \aleph_\alpha \times \aleph_\alpha$. Set $\delta_0 := \max(\beta_0, \gamma_0) + 1$. Since no infinite successor ordinal is a cardinal (by Example 1.8.1), we have $\delta_0 < \aleph_\alpha$ and the restriction of $f$ to $\aleph_\alpha$ is an injective map from $\aleph_\alpha$ to $\delta_0 \times \delta_0$, a set of cardinality

$$\mathrm{card}(\delta_0 \times \delta_0) = \mathrm{card}(\delta_0) \leq \delta_0 < \aleph_\alpha$$

by the induction hypothesis. This is a contradiction, and thus one has $\aleph_\alpha \aleph_\alpha \leq \aleph_\alpha$.

The inequality in the other direction is clear. □

**Example 1.9.4.** Let $\mathcal{T}$ be the set of all open subsets of $\mathbb{R}$. Then $\mathrm{card}(\mathcal{T}) = 2^{\aleph_0}$.

**Proof.** The mapping assigning to a real number $r \in \mathbb{R}$ the open interval $(r, +\infty)$ defines an injection from $\mathbb{R}$ to $\mathcal{T}$, which proves that $\mathrm{card}(\mathcal{T}) \geq 2^{\aleph_0}$.

Conversely, note that every open subset of $\mathbb{R}$ is a union of intervals of the form $(q, q + q')$, with $q \in \mathbb{Q}$ and $q' \in \mathbb{Q}_{>0}$. The mapping sending $Y \subseteq \mathbb{Q} \times \mathbb{Q}_{>0}$ to $\bigcup_{(q,q') \in Y} (q, q + q')$ provides a surjection of $\mathcal{P}(\mathbb{Q} \times \mathbb{Q}_{>0})$ to $\mathcal{T}$. Since $\mathbb{Q} \times \mathbb{Q}_{>0}$ is countable, one deduces that $2^{\aleph_0} \geq \mathrm{card}(\mathcal{T})$. □

**Proposition 1.9.5.**

(1) *Let $X$ and $Y$ be non-empty sets and assume that at least one of them is infinite. Then*

$$\mathrm{card}(X \cup Y) = \mathrm{card}(X \times Y) = \max(\mathrm{card}(X), \mathrm{card}(Y)).$$

(2) *Let $\kappa \geq \aleph_0$ and $\lambda > 0$ be cardinals. Then $\kappa + \lambda = \kappa\lambda = \max(\kappa, \lambda)$.*

(3) *Let $(X_i)_{i \in I}$ be a family of sets with at least one $X_i$ infinite. Then*

$$(*) \qquad \mathrm{card}\left(\bigcup_{i \in I} X_i\right) \leq \sup\left(\{\mathrm{card}(X_i) \mid i \in I\} \cup \{\mathrm{card}(I)\}\right).$$

*(In particular, a countable union of countable sets is countable.) If furthermore the sets $X_i$ are all non-empty and mutually disjoint, then equality holds in $(*)$.*

**Proof.** (1) Let $\kappa = \max(\mathrm{card}(X), \mathrm{card}(Y))$. We have

$$\kappa \leq \mathrm{card}(X \cup Y) \leq \kappa + \kappa = 2\kappa \leq \kappa\kappa$$

and $\kappa \leq \mathrm{card}(X \times Y) \leq \kappa\kappa$. One concludes by Hessenberg's Theorem.

(2) is a special case of (1).

(3) Let $X = \{(x_i, i) \mid x_i \in X_i \text{ for some } i \in I\}$ be the disjoint union of the sets $X_i$. There is a canonical surjection $X \to \bigcup_{i\in I} X_i$, hence it suffices to prove that

$$\operatorname{card}(X) \leq \sup\left(\{\operatorname{card}(X_i) \mid i \in I\} \cup \{\operatorname{card}(I)\}\right).$$

Let $\kappa = \sup\{\operatorname{card}(X_i) \mid i \in I\}$, and let $Y_i$ be the set of injective maps $X_i \to \kappa$. Since the sets $Y_i$ are all non-empty, by the Axiom of Choice there exists some $f = (f_i)_{i\in I} \in \prod_{i\in I} Y_i$. Consider $g : X \to \kappa \times I$, defined by $g((x_i, i)) := (f_i(x_i), i)$. The function $g$ is injective, hence $\operatorname{card}(X) \leq \kappa \operatorname{card}(I) = \max(\kappa, \operatorname{card}(I))$. The equality statement is clear. □

It follows from the preceding proposition that cardinal addition and multiplication is quite trivial for infinite cardinals. The situation for cardinal exponentiation is very different. In fact, the ZFC axioms are far from completely determining the values of cardinal exponentiation. For instance they do not allow to settle the continuum hypothesis:

**Definition.**

- The *Continuum Hypothesis* (CH) is the statement $2^{\aleph_0} = \aleph_1$.
- The *Generalized Continuum Hypothesis* (GCH) is the statement $2^\kappa = \kappa^+$ for every infinite cardinal $\kappa$.

If $(\kappa_i)_{i\in I}$ is a family of cardinals, we shall denote by $\sum_{i\in I} \kappa_i$ the cardinal of the disjoint union of the $\kappa_i$, and by $\prod_{i\in I} \kappa_i$ the cardinal of the product of the family.

**Theorem 1.9.6** (König's Theorem)**.** *Let $(\kappa_i)_{i\in I}$ and $(\lambda_i)_{i\in I}$ be families of cardinals with $\kappa_i < \lambda_i$ for every $i$. Then $\sum_{i\in I} \kappa_i < \prod_{i\in I} \lambda_i$.*

**Proof.** Let $f : \sum_{i\in I} \kappa_i \to \prod_{i\in I} \lambda_i$. For every $i$, $f$ induces a mapping $f_i : \kappa_i \to \lambda_i$ given by the $i$th component of the restriction of $f$ to $\kappa_i$. Since $\kappa_i < \lambda_i$, the set $B_i := \lambda_i \setminus \operatorname{im}(f_i)$ is non-empty for every $i$. By (AC) there exists some $b \in \prod_{i\in I} B_i \subseteq \prod_{i\in I} \lambda_i$. Clearly $b \notin \operatorname{im}(f)$. □

## 1.10. Cofinality

In this section we shall use the notion of cofinality to prove for instance that $2^{\aleph_0} \neq \aleph_\omega$.

**Definition.**

- Let $X$ be a totally ordered set. We say that a subset $Y \subseteq X$ is *cofinal* in $X$ if $Y$ is not bounded in $X$, that is, if for any $x \in X$ there exists $y \in Y$ such that $x \leq y$. We say that a function $f : Z \to X$ is *cofinal* if $\mathrm{im}(f)$ is cofinal in $X$.
- The *cofinality* of an ordinal $\alpha$, denoted by $\mathrm{cof}(\alpha)$, is the smallest ordinal $\beta$ such that there exists a cofinal function $\beta \to \alpha$.

**Example 1.10.1.**

(1) $\mathrm{cof}(0) = 0$.

(2) $\mathrm{cof}(\alpha + 1) = 1$ for any ordinal $\alpha$.

(3) $\mathrm{cof}(\omega) = \omega$.

**Proposition 1.10.2.** *Let $\alpha$ be an ordinal.*

(1) $\mathrm{cof}(\alpha) \leq \alpha$.

(2) $\mathrm{cof}(\alpha)$ *is a cardinal.*

(3) $\mathrm{cof}(\alpha)$ *is the smallest ordinal $\beta$ such that there exists a cofinal and strictly increasing map $\beta \to \alpha$.*

(4) $\mathrm{cof}(\mathrm{cof}(\alpha)) = \mathrm{cof}(\alpha)$.

**Proof.** (1) is clear, and (2) follows from the fact that any ordinal $\beta$ is in bijection with $\mathrm{card}(\beta) \leq \beta$.

(3) It is enough to provide some $\beta \leq \mathrm{cof}(\alpha)$ and a cofinal and strictly increasing map $\beta \to \alpha$. By hypothesis, there exists a cofinal map $h : \mathrm{cof}(\alpha) \to \alpha$. Let us define

$$X = \{x \in \mathrm{cof}(\alpha) \mid h(y) < h(x) \text{ for every } y < x\}.$$

The set $h(X) = \{h(x) \mid x \in X\}$ is cofinal in $\alpha$. Indeed, let $\gamma < \alpha$. By the cofinality of $h$, there exists $y \in \mathrm{cof}(\alpha)$ such that $h(y) \geq \gamma$. When $y$ is minimal with this property, we have $y \in X$.

Since $(X, <) \cong (\beta, \in)$ for some $\beta \leq \mathrm{cof}(\alpha)$, we are done, because the restriction of $h$ to $X$ is cofinal and strictly increasing.

(4) $\mathrm{cof}(\mathrm{cof}(\alpha)) \leq \mathrm{cof}(\alpha)$ follows from part (1). For the inequality in the other direction, let us consider the cofinal and strictly increasing functions $f : \mathrm{cof}(\mathrm{cof}(\alpha)) \to \mathrm{cof}(\alpha)$ and $g : \mathrm{cof}(\alpha) \to \alpha$, which are

possible by (3). Then the function $g \circ f : \mathrm{cof}(\mathrm{cof}(\alpha)) \to \alpha$ is cofinal, and hence $\mathrm{cof}(\alpha) \leq \mathrm{cof}(\mathrm{cof}(\alpha))$. □

We shall say that an infinite cardinal $\kappa$ is *regular* if $\mathrm{cof}(\kappa) = \kappa$, and *singular* if $\mathrm{cof}(\kappa) < \kappa$.

**Proposition 1.10.3.** *Any infinite cardinal which is a successor is regular. In particular $\aleph_1$ is regular.*

**Proof.** Let $\kappa = \aleph_{\beta+1} = \aleph_\beta^+$. Note that for a limit ordinal $\alpha$, a subset $X \subseteq \alpha$ is cofinal if and only if $\alpha = \bigcup_{\gamma \in X} \gamma$. (This follows from Proposition 1.5.5.) Consider a function $f : \lambda \to \kappa$ for some $\lambda < \kappa$. Then $\lambda \leq \aleph_\beta$ and it follows from Proposition 1.9.5(3) that $\mathrm{card}\left(\bigcup_{\beta<\lambda} f(\beta)\right) \leq \sup(\{\mathrm{card}(f(\beta)) \mid \beta < \lambda\} \cup \{\lambda\}) \leq \aleph_\beta$. Hence $f$ is not cofinal. □

**Proposition 1.10.4.** *If $\lambda$ is a limit ordinal, then* $\mathrm{cof}(\aleph_\lambda) = \mathrm{cof}(\lambda)$.

**Proof.** If $f : \alpha \to \lambda$ is cofinal, then $\tilde{f} : \alpha \to \aleph_\lambda$, $\beta \mapsto \aleph_{f(\beta)}$ is cofinal too, since $\aleph_\lambda = \bigcup_{\gamma<\lambda} \aleph_\gamma$ by definition. This proves $\mathrm{cof}(\aleph_\lambda) \leq \mathrm{cof}(\lambda)$. Conversely, let $g : \alpha \to \aleph_\lambda$ be cofinal. The map $\tilde{g} : \alpha \to \lambda$, defined by $\tilde{g}(\beta) = 0$ if $g(\beta)$ is finite, and $\tilde{g}(\beta) = \gamma$ if $\mathrm{card}(g(\beta)) = \aleph_\gamma$, is cofinal. □

**Proposition 1.10.5.** *Let $\kappa \geq 2$ and $\lambda \geq \aleph_0$ be cardinals. Then* $\mathrm{cof}\left(\kappa^\lambda\right) > \lambda$.

**Proof.** Consider a map $f : \alpha \to \kappa^\lambda$, with $\alpha$ some ordinal $\leq \lambda$. Since $f(\beta) < \kappa^\lambda$ for every $\beta < \alpha$, it follows from König's Theorem that

$$\mathrm{card}\left(\bigcup_{\beta<\alpha} f(\beta)\right) \leq \sum_{\beta<\alpha} \mathrm{card}(f(\beta)) < \prod_{\beta<\alpha} \left(\kappa^\lambda\right) = \kappa^{\lambda \cdot \mathrm{card}(\alpha)} \leq \kappa^\lambda.$$

Hence $f$ is not cofinal. □

**Corollary 1.10.6.** $2^{\aleph_0} \neq \aleph_\omega$.

**Proof.** We have $\mathrm{cof}(\aleph_\omega) = \mathrm{cof}(\omega) = \omega = \aleph_0 < \mathrm{cof}\left(2^{\aleph_0}\right)$. □

## 1.11. Exercises

**Exercise 1.11.1.**

(1) Prove that an ordinal $\alpha$ is a limit if and only if there is an ordinal $\beta \neq 0$ such that $\alpha = \omega\beta$.

(2) Prove that $\omega^2 = \omega\omega$ is not of the form $\delta + \omega$.

**Exercise 1.11.2** (Cantor normal form)**.** Let $\alpha$ be an ordinal $> 1$.

(1) Prove that $\alpha^\gamma \geq \gamma$ for any ordinal $\gamma$. (Is there any example with $\alpha^\gamma = \gamma$?)

(2) Let $\beta$ be an ordinal $> 0$. Prove that there exists an ordinal $\gamma$ such that $\alpha^\gamma \leq \beta < \alpha^{\gamma^+}$.

(3) Deduce that any ordinal $\beta$ can be expanded in basis $\alpha$: there exists a finite sequence of ordinals $\beta_1 > ... > \beta_n \geq 0$ and ordinals $k_i$ with $0 < k_i < \alpha$ such that

$$\beta = \alpha^{\beta_1} k_1 + ... + \alpha^{\beta_n} k_n.$$

Furthermore the natural number $n$ and the sequences $(\beta_i)$ and $(k_i)$ are unique.

The expansion into basis $\omega$ is called the *Cantor normal form*.

**Exercise 1.11.3** (Goodstein sequences)**.** Let $n, p$ be natural numbers, with $p \geq 2$. Let us define the iterated expansion of $n$ in basis $p$ as follows: first expand $n$ in basis $p$ (for instance if $n = 35$, $p = 2$, one has $35 = 2^5 + 2 + 1$). Then, expand the exponents in basis $p$ and so on, so that all numbers occurring are $< p$. For instance the iterated expansion of 35 in basis 2 is $35 = 2^{2^2+1} + 2 + 1$.

For $q \geq p \geq 2$, one defines a function $f_{p,q} : \mathbb{N} \to \mathbb{N}$ as follows. Let $n$ be a natural number. Then $f_{p,q}(n)$ is obtained by replacing all occurrences of $p$ in the iterated expansion of $n$ in basis $p$ by $q$. One similarly defines ordinal valued functions $f_{p,\omega}$ by replacing all occurrences of $p$ by $\omega$ (when $p > 2$, one writes the coefficients at the right of the $p^n$). For instance, $f_{2,3}(35) = 3^{3^3+1}+3+1 = 59053$ and $f_{3,\omega}(35) = f_{3,\omega}(3^3+3\cdot 2+2) = \omega^\omega + \omega \cdot 2 + 2$.

(1) Prove that $f_{q,r} \circ f_{p,q} = f_{p,r}$ for any $\omega \geq r > q > p \geq 2$.

(2) Prove that the functions $f_{p,\omega}$ are strictly increasing.

For any $a \in \mathbb{N}$, the *Goodstein sequence* attached to $a$ is the sequence $(g_n(a))_{n\geq 2}$ defined by $g_2(a) := a$ and

$$g_{n+1}(a) = \begin{cases} f_{n,n+1}(g_n(a)) - 1 & \text{if } g_n(a) \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

For $a = 5$, one has for instance $g_2(5) = 5$, $g_3(5) = 3^3 + 1 - 1 = 27$, $g_4(5) = 4^4 - 1 = 255$, and $g_5(5) = 5^3 \cdot 3 + 5^2 \cdot 3 + 5 \cdot 3 + 3 - 1 = 467$.

(3) Let $a$ be a natural number. Study the monotonicity of the sequence $f_{p,\omega}(g_p(a))$.

(4) Prove that for any $a \in \mathbb{N}$ there exists $s(a) \in \mathbb{N}$ such that $g_n(a) = 0$ when $n \geq s(a)$.

**Exercise 1.11.4** (The order topology)**.** On any totally ordered set $X$, one may define a topology, the *order topology*, generated by the open intervals, that is, by the sets of the form $(-\infty, b) = \{x \in X \mid x < b\}$, $(a, b) = \{x \in X \mid a < x < b\}$ or $(a, \infty)$, for $a, b \in X$.

(1) Prove that for any $X$, the order topology is Hausdorff.

(2) Let $\alpha$ and $\beta$ be ordinals endowed with the order topology. Prove the following statements:
   (a) $\alpha$ is discrete if and only if $\alpha \leq \omega$.
   (b) $\alpha$ is compact if and only if $\alpha$ is not a limit ordinal.
   (c) Suppose $f : \alpha \to \beta$ is a weakly increasing function, that is, $x \leq y \Rightarrow f(x) \leq f(y)$. Then $f$ is continuous if and only if, for any limit $\lambda \in \alpha$, $f(\lambda) = \sup_{\gamma<\lambda} f(\gamma)$.

**Exercise 1.11.5** (Ulam's Theorem)**.** An *Ulam matrix* is a family of subsets $U_{\alpha,n}$ of $\aleph_1$, $\alpha < \aleph_1$, $n < \omega$, such that

- for any $n < \omega$ and $\alpha, \beta < \aleph_1$ with $\alpha \neq \beta$, $U_{\alpha,n} \cap U_{\beta,n} = \emptyset$;
- for any $\alpha < \aleph_1$, the set $\aleph_1 \setminus \bigcup_{n<\omega} U_{\alpha,n}$ is at most countable.

(1) For any $\xi < \aleph_1$, let $f_\xi : \omega \to \aleph_1$ such that $\xi \subseteq \mathrm{im}(f_\xi)$. Set

$$U_{\alpha,n} = \{\xi < \aleph_1 \mid f_\xi(n) = \alpha\}.$$

Prove that $(U_{\alpha,n})$ is an Ulam matrix.

(2) Let $\mu : \mathcal{P}(\aleph_1) \to [0,1]$ be a $\sigma$-additive measure on $\aleph_1$, that is, $\mu(\bigcup_{n<\omega} A_n) = \sum_{n<\omega} \mu(A_n)$ for all families $(A_n)_{n<\omega}$ of pairwise disjoint subsets of $\aleph_1$. Prove that if $\mu(\{\alpha\}) = 0$ for every $\alpha < \aleph_1$, then $\mu$ is identically zero.

**Exercise 1.11.6** (Closed unbounded sets)**.** Let $\kappa > \aleph_0$ be a regular cardinal. A set $C \subseteq \kappa$ is said to be a *club* (closed unbounded) if it is closed and cofinal, that is, if it is cofinal in $\kappa$ and for any non-empty subset $A \subseteq C$, $\sup A \in C \cup \{\kappa\}$. A subset $S \subseteq \kappa$ is called *stationary* if $S \cap C \neq \emptyset$ for any club $C \subseteq \kappa$.

(1) Let $\lambda < \kappa$ and $(C_i)_{i<\lambda}$ be a family of clubs. Prove that $\bigcap_{i<\lambda} C_i$ is a club.

(2) Let $(C_i)_{i<\kappa}$ be a family of clubs. Prove that the diagonal intersection $\triangle_{i<\kappa} C_i := \{\alpha < \kappa \mid \alpha \in \bigcap_{i<\alpha} C_i\}$ is a club.

(3) (Fodor's Lemma) Let $S \subseteq \kappa$ be a stationary set and suppose $f : S \to \kappa$ is a *regressive* map (that is, such that $f(\alpha) < \alpha$ for any $\alpha \in S$). Prove that there exists a stationary set $T \subseteq S$ such that $f$ is constant on $T$.

(4) (Solovay's Theorem for $\aleph_1$) Let $\kappa = \aleph_1$, and let $S \subseteq \aleph_1$ be a stationary set. Prove that $S$ can be written as the union of $\aleph_1$ pairwise disjoint stationary sets.

[Hint: For any limit ordinal $\alpha \in S$, write $\alpha = \sup_{n<\omega} a^\alpha_n$. Use this to define a regressive function to which one may apply Fodor's Lemma.]

**Exercise 1.11.7** (Solovay's Theorem)**.** Let $\kappa > \aleph_0$ be a regular cardinal. The aim of this exercise is to prove Solovay's Theorem: *Any stationary set $S \subseteq \kappa$ can be written as the union of $\kappa$ pairwise disjoint stationary sets.*

(1) For a cardinal $\lambda < \kappa$, let $E^\kappa_\lambda = \{\alpha < \kappa \mid \mathrm{cof}(\alpha) = \lambda\}$. Prove Solovay's Theorem when $S \subseteq E^\kappa_\omega$.

(2) Prove Solovay's Theorem when $S \subseteq \{\alpha < \kappa \mid \mathrm{cof}(\alpha) < \alpha\}$.

(3) Assume $S$ is a set of regular cardinals. Prove that

$$T = \{\alpha \in S \mid S \cap \alpha \text{ is not stationary in } \alpha\}$$

is stationary.

[Hint: Prove it by contradiction after noticing that if $C$ is a club, the set $C' \subseteq C$ of limits of points of $C$ is still a club.]

(4) Prove Solovay's Theorem in the general case.

[Hint: Prove it is enough to consider the case when $S$ is a set of regular cardinals. For $\alpha \in T$, consider a strictly increasing sequence $(a^\alpha_\xi : \xi < \kappa)$ with limit $\alpha$ such that $a^\alpha_\xi \notin S$. Then adapt the proof of (1).]

**Exercise 1.11.8** (Filters and ultrafilters)**.** Let $X$ be a non-empty set. A *filter* on $X$ is a set $F \subseteq \mathcal{P}(X)$ such that

(i) $X \in F, \emptyset \notin F$,

(ii) if $A, B \in F$, then $A \cap B \in F$, and

(iii) if $A \in F$ and $A \subseteq B$, then $B \in F$.

A set $\mathcal{B}$ of non-empty subsets of $X$ is a *filter basis* on $X$ if for any $A, B \in \mathcal{B}$ there is $C \in \mathcal{B}$ such that $C \subseteq A \cap B$.

(1) Prove that any filter basis $\mathcal{B}$ is contained in a minimal filter with respect to inclusion, denoted by $F_{\mathcal{B}}$.

(2) Let $J$ be a set and let $I$ be the set of finite subsets of $J$. For any $i \in I$, set $I_i = \{j \in I \mid i \subseteq j\}$. Prove that the set $\mathcal{B}$ whose elements are the sets $I_i$, $i \in I$, is a filter basis on $I$.

(3) Prove that when $X$ is infinite, the set of subsets of $X$ whose complement in $X$ is finite is a filter. This filter is called the *Fréchet filter*.

(4) An *ultrafilter* is a filter which is maximal with respect to inclusion. Prove that a filter $F$ on a non-empty set $X$ is an ultrafilter if and only if for any $A \subseteq X$, either $A$ or $X \setminus A$ belongs to $F$.

(5) Prove that for any $x \in X$, the set $U_x = \{Y \subseteq X \mid x \in Y\}$ is an ultrafilter on $X$. Such an ultrafilter is called *principal*.

(6) Prove that an ultrafilter is principal if and only if it contains a finite set as an element. Deduce that when $X$ is finite, any ultrafilter on $X$ is principal, and when $X$ is infinite, an ultrafilter $U$ is non-principal if and only if it contains the Fréchet filter as a subset.

(7) Prove that any filter is contained in some ultrafilter. In particular, on any infinite set there exists a non-principal ultrafilter.

**Exercise 1.11.9** (Hausdorff's Theorem)**.** The aim of this exercise is to prove the following result due to Hausdorff: *On an infinite set $X$ of cardinality $\kappa$, there exist $2^{(2^\kappa)}$ distinct ultrafilters.*

(1) A family $F$ of subsets of $X$ is said to be *free* if whenever $A_1, \ldots, A_n, B_1, \ldots, B_m$ are distinct elements of $F$, then $A_1 \cap \cdots \cap A_n \cap (X \setminus B_1) \cap \cdots \cap (X \setminus B_m)$ is non-empty. Prove that Hausdorff's Theorem is a consequence of the following statement: there exists a free family of cardinality $2^\kappa$.

(2) Consider the set $Y$ consisting of pairs $(F, (P_1, \ldots, P_n))$ with $F$ a finite subset of $X$ and $(P_1, \ldots, P_n)$ a finite sequence of of subsets of $F$. What is the cardinality of $Y$?

(3) To any $A \in \mathcal{P}(X)$ we assign a subset $A'$ of $X \cup Y$ as follows:
- if $x \in X$, then $x \in A'$ if and only if $x \in A$;
- if $y \in Y$ and $y = (F, (P_1, \ldots, P_n))$, then $y \in A'$ if and only if $A \cap F$ is one of the $P_i$'s.

Prove that the set of the $A'$ for $A \subseteq X$ is a free family (on $X \cup Y$).

(4) Conclude Hausdorff's Theorem.

**Exercise 1.11.10** (The continuum hypothesis for closed subsets of $\mathbb{R}$)**.** The aim of this exercise is to prove that the continuum hypothesis holds for closed subsets of the real line (Cantor's Theorem), that is, if $F \subseteq \mathbb{R}$ is closed, then either $F$ is countable or $\mathrm{card}(F) = 2^{\aleph_0}$.

Let $F \subseteq \mathbb{R}$ be a closed subset such that $\mathrm{card}(F) > \aleph_0$.

(1) Let $C$ be the set of $x \in F$ such that there is an open set $\Omega \subseteq \mathbb{R}$ which contains $x$ and satisfies $\mathrm{card}(\Omega \cap F) \leq \aleph_0$. Set $F' := F \setminus C$.

Prove the following properties:
(a) $C$ is countable,
(b) $F'$ is a closed subset of $\mathbb{R}$, and
(c) any non-empty open subset of $F'$ is uncountable.

(2) Let $I$ be an open interval such that $I \cap F' \neq \emptyset$.

Prove that for any $\epsilon > 0$ there are open intervals $I_0$ and $I_1$ of length at most $\epsilon$ such that $I_i \cap F' \neq \emptyset$ and $\overline{I_i} \subseteq I$ for $i = 0, 1$ and such that $\overline{I_0} \cap \overline{I_1} = \emptyset$. (Here, $\overline{J}$ denotes the closure of $J$.)

(3) Prove that there is an injection of $2^{\aleph_0}$ into $F'$.

(4) Prove Cantor's Theorem.

**Exercise 1.11.11.** A *tree* is a partial order $(T, <_T)$ such that for every $t \in T$, the set

$$\hat{t} := \{s \in T \mid s <_T t\}$$

is well-ordered. If $T$ has a smallest element, it is called the *root* of $T$.

The *height* of $t \in T$ is defined as the unique ordinal isomorphic to $(\hat{t}, <_T)$ and denoted by $\mathrm{ht}(t)$. Finally, $\mathrm{ht}(T) := \sup\{\mathrm{ht}(t) + 1 \mid t \in T\}$ is the *height* of $T$. For an ordinal $\alpha$ one sets $T(\alpha) = \{t \in T \mid \mathrm{ht}(t) = \alpha\}$.

A *branch* in a tree $(T, <_T)$ is a totally ordered subset which is maximal with respect to inclusion. It is called *cofinal* in $T$ if it non-trivially intersects any level $T(\alpha)$ for $\alpha < \mathrm{ht}(T)$.

Prove König's Lemma: If $T$ is a tree of height $\omega$ such that $T(n)$ is finite for every $n \in \omega$, then $T$ contains a cofinal branch.

**Exercise 1.11.12.**

(1) For $\alpha \in \aleph_1$, let $Y_\alpha$ be the set of strictly increasing non-cofinal maps from $\alpha$ to $\mathbb{Q}$. For $\beta < \alpha$, denote by $\rho^\alpha_\beta : Y_\alpha \to Y_\beta$ the (surjective) restriction map. Prove that there are countable subsets $X_\alpha \subseteq Y_\alpha$ such that for any $\alpha > \beta$, the following properties hold:
   (a) $\rho^\alpha_\beta(X_\alpha) = X_\beta$.
   (b) For any $f \in X_\beta$, any upper bound $q \in \mathbb{Q}$ of $\mathrm{im}(f)$ and any $\epsilon > 0$ there is $g \in X_\alpha$ with $\rho^\alpha_\beta(g) = f$ such that $\mathrm{im}(g)$ is bounded above by $q + \epsilon$.

(2) Let $\varprojlim_{\alpha \in \aleph_1} X_\alpha$ be the set of all $f = (f_\alpha) \in \prod_{\alpha \in \aleph_1} X_\alpha$ such that $\rho^\alpha_\beta(f_\alpha) = f_\beta$ for all $\beta < \alpha$. Prove that $\varprojlim_{\alpha \in \aleph_1} X_\alpha = \emptyset$.

(3) Deduce Aronszajn's Theorem: *There is an* Aronszajn tree*, that is, a tree $T$ of height $\aleph_1$ with $T(\alpha)$ countable for all $\alpha < \aleph_1$ such that $T$ does not admit a cofinal branch.*

## 1.12. Appendix: Hindman's Theorem

In this appendix we shall freely use the material on ultrafilters treated in Exercise 1.11.8. Let $E$ be a non-empty set and $\mathcal{U}(E)$ the set of all ultrafilters on $E$. When $E$ is infinite, there exist non-principal ultrafilters on $E$.

For a subset $A \subseteq E$, set $\langle A\rangle = \{U \in \mathcal{U}(E) \mid A \in U\}$.

**Lemma 1.12.1.** *The sets $\langle A\rangle$, for $\emptyset \neq A \subseteq E$, form a basis of open sets for a compact Hausdorff topology on $\mathcal{U}(E)$.*

**Proof.** We have $\langle A_1\rangle \cap \cdots \cap \langle A_n\rangle = \langle A_1 \cap \cdots \cap A_n\rangle$, which proves that the sets $\langle A\rangle$ form a basis of open sets for some topology. Furthermore, $\langle E \setminus A\rangle = \mathcal{U}(E) \setminus \langle A\rangle$, thus $\langle A\rangle$ is open and closed. In particular, the topology is Hausdorff.

Consider a covering $\bigcup_{i\in I} \Omega_i$ of $\mathcal{U}(E)$ by open subsets. To prove the existence of $I_0 \subseteq I$ finite such that $\bigcup_{i\in I_0} \Omega_i = \mathcal{U}(E)$ we may assume $\Omega_i = \langle A_i\rangle$ for any $i \in I$. If for some finite $I_0 \subseteq I$ one has $\bigcup_{i\in I_0} A_i = E$, we are done, since then $\bigcup_{i\in I_0} \langle A_i\rangle = \mathcal{U}(E)$. Otherwise, the set

$$\mathcal{B} = \left\{ \bigcap_{i\in I_0} E \setminus A_i \mid I_0 \subseteq I \text{ finite} \right\}$$

is a filter basis and is contained in some ultrafilter $U$ on $E$ by Exercise 1.11.8, which contradicts $\bigcup_{i\in I} \Omega_i = \mathcal{U}(E)$. □

Now consider $\mathcal{U}(\mathbb{N}^*)$. Let $k \in \mathbb{N}^*$, $A \subseteq \mathbb{N}^*$ and $U \in \mathcal{U}(\mathbb{N}^*)$. One sets $A - k := \mathbb{N}^* \cap \{a - k \mid a \in A\}$ and

$$A_U := \{k \in \mathbb{N}^* \mid A - k \in U\}.$$

**Lemma 1.12.2.** *For any $U \in \mathcal{U}(\mathbb{N}^*)$ and every $A, B \subseteq \mathbb{N}^*$, one has $\mathbb{N}^*_U = \mathbb{N}^*$, $(A \cap B)_U = A_U \cap B_U$ and $(\mathbb{N}^* \setminus A)_U = \mathbb{N}^* \setminus A_U$.*

**Proof.** These properties are easy consequences of the fact that for $k \in \mathbb{N}^*$ one has $\mathbb{N}^* - k = \mathbb{N}^*$, $(A-k)\cap(B-k) = A\cap B - k$ and $(\mathbb{N}^* \setminus A) - k = \mathbb{N}^* \setminus (A - k)$. The details are left as an exercise. □

For $U, V \in \mathcal{U}(\mathbb{N}^*)$, one sets $U \oplus V := \{A \subseteq \mathbb{N}^* \mid A_U \in V\}$.

**Lemma 1.12.3.**

(1) *For any $U, V \in \mathcal{U}(\mathbb{N}^*)$, $U \oplus V \in \mathcal{U}(\mathbb{N}^*)$.*

(2) *$\oplus$ is associative.*

(3) *For fixed $U$, the function $f_U : \mathcal{U}(\mathbb{N}^*) \to \mathcal{U}(\mathbb{N}^*)$, $V \mapsto U \oplus V$, is continuous.*

**Proof.** (1) It is clear that $\mathbb{N}^* \in U \oplus V$, and that for any $A \in U \oplus V$ and $A \subseteq B$ one has $B \in U \oplus V$. Stability of $U \oplus V$ under intersection and the fact that $A \in U \oplus V$ if and only if $\mathbb{N}^* \setminus A \notin U \oplus V$ are consequences of Lemma 1.12.2.

(2) One has $(A - k)_U = A_U - k$ (exercise). From this, one may deduce that $(A_U)_V = A_{U \oplus V}$. Indeed, for $l \in \mathbb{N}^*$, one has

$$\begin{aligned} l \in (A_U)_V &\Leftrightarrow A_U - l \in V \Leftrightarrow (A - l)_U \in V \\ &\Leftrightarrow A - l \in U \oplus V \Leftrightarrow l \in A_{U \oplus V}. \end{aligned}$$

If $U, V, W \in \mathcal{U}(\mathbb{N}^*)$, we deduce that

$$\begin{aligned} A \in U \oplus (V \oplus W) &\Leftrightarrow A_U \in V \oplus W \\ &\Leftrightarrow (A_U)_V = A_{U \oplus V} \in W \Leftrightarrow A \in (U \oplus V) \oplus W, \end{aligned}$$

which proves associativity of $\oplus$.

(3) Let $A \subseteq \mathbb{N}^*$. Continuity of $f_U$ follows from the following:

$$\begin{aligned} f_U^{-1}(\langle A \rangle) &= \{V \in \mathcal{U}(\mathbb{N}^*) \mid A \in U \oplus V\} \\ &= \{V \in \mathcal{U}(\mathbb{N}^*) \mid A_U \in V\} = \langle A_U \rangle. \end{aligned}$$

□

We shall say an ultrafilter $U$ on $\mathbb{N}^*$ is *idempotent* if $U \oplus U = U$.

**Proposition 1.12.4.** *There exists an idempotent ultrafilter in $\mathcal{U}(\mathbb{N}^*)$.*

**Remark 1.12.5.** For $m, n \in \mathbb{N}^*$, one can easily check that the sum of the corresponding principal ultrafilters is given by $U_m \oplus U_n = U_{m+n}$. In particular no principal ultrafilter is idempotent. □

**Proof of Proposition 1.12.4.** One considers the set

$$\mathbb{A} := \{\mathcal{A} \subseteq \mathcal{U}(\mathbb{N}^*) \mid \mathcal{A} \text{ is a non-empty closed set with } \mathcal{A} \oplus \mathcal{A} \subseteq \mathcal{A}\}.$$

The set $\mathbb{A}$ is non-empty since it contains $\mathcal{U}(\mathbb{N}^*)$. Furthermore the partial order on $\mathbb{A}$ given by $\supseteq$ is inductive. This follows from the fact that a

subset of a compact Hausdorff space is closed if and only if it is compact. Thus, if $(\mathcal{A}_i)_{i\in I}$ is a totally ordered subset of $\mathbb{A}$, then $\bigcap_{i\in I}\mathcal{A}_i \in \mathbb{A}$. By Zorn's Lemma, there exists $\mathcal{B} \in \mathbb{A}$ which is minimal for inclusion.

Let $U \in \mathcal{B}$. We shall prove that $U \oplus U = U$.

First, we consider $\mathcal{B}' := U \oplus \mathcal{B} \subseteq \mathcal{B}$. Since $f_U$ is continuous, the set $\mathcal{B}' = f_U(\mathcal{B})$ is compact (hence closed). Furthermore, if $V_1, V_2 \in \mathcal{B}$, one has $(U \oplus V_1) \oplus (U \oplus V_2) = U \oplus W$ for some $W \in \mathcal{B}$, since $\mathcal{B} \oplus \mathcal{B} \subseteq \mathcal{B}$. This proves that $\mathcal{B}' \oplus \mathcal{B}' \subseteq \mathcal{B}'$. Hence we have $\mathcal{B}' \in \mathbb{A}$, and thus $\mathcal{B}' = \mathcal{B}$ by minimality of $\mathcal{B}$. In particular, there exists $V' \in \mathcal{B}$ such that $U \oplus V' = U$.

Set $\mathcal{V}' = \{V' \in \mathcal{B} \mid U \oplus V' = U\}$. By continuity of the map $f_U$, $\mathcal{V}' = f_U^{-1}(\{U\}) \cap \mathcal{B}$ is closed, and we just proved it is non-empty. If $V', V'' \in \mathcal{V}'$, then $U \oplus (V' \oplus V'') = (U \oplus V') \oplus V'' = U \oplus V'' = U$. Thus $\mathcal{V}'$ is closed under $\oplus$ and it belongs to $\mathbb{A}$. It follows that $\mathcal{V}' = \mathcal{B}$ by minimality of $\mathcal{B}$. In particular, $U \in \mathcal{V}'$, hence $U \oplus U = U$. □

For a subset $A \subseteq \mathbb{N}^*$, one denotes by

$$\Sigma_A := \left\{ \sum_{k\in A_0} k \mid A_0 \subseteq A \text{ finite} \right\}$$

the set of finite sums of distinct elements of $A$.

**Theorem 1.12.6** (Hindman's Theorem)**.** *Let $\chi : \mathbb{N}^* \to \{1, \dots, n\}$ be any function. Then there exists $B \subseteq \mathbb{N}^*$ infinite such that $\chi$ is constant on $\Sigma_B$.*

**Proof.** Let $U = U \oplus U \in \mathcal{U}(\mathbb{N}^*)$ be an idempotent ultrafilter as provided by Proposition 1.12.4. There then exists a unique $i_0 \leq n$ such that $\chi^{-1}(i_0) \in U$. Set $A := \chi^{-1}(i_0)$. We will prove the existence of an infinite set $B \subseteq A$ such that $\Sigma_B \subseteq A$, which will complete the proof.

As $U = U \oplus U$, for any $C \in U$ one has $C_U \in U$, hence $C \cap C_U \in U$. In particular, $C \cap C_U$ is infinite. Furthermore, for any $k \in C \cap C_U$ one has $(C - k) \cap C \in U$.

By induction on $n \in \mathbb{N}$, one defines a decreasing sequence $(A^n)_{n\in\mathbb{N}}$ in $U$ and a strictly increasing sequence of integers $(k_n)_{n\in\mathbb{N}}$ as follows. One sets $A^0 := A$ and one chooses $k_0 \in A^0 \cap A^0_U$. Assuming $A^n$ and $k_n$ already constructed, one sets $A^{n+1} := (A^n - k_n) \cap A^n \in U$, and one

chooses some $k_{n+1} > k_n$ such that $k_{n+1} \in A^{n+1} \cap A_U^{n+1}$. This is possible since $A^{n+1} \cap A_U^{n+1}$ is infinite.

Now $B = \{k_n \mid n \in \mathbb{N}\}$ is an infinite subset of $A$. Let $I$ be a finite non-empty subset of $\mathbb{N}$. We now prove by induction on $\mathrm{card}(I)$ that $\sum_{i\in I} k_i \in A^{\min I}$. If $I$ is a singleton, this is clear. Assume now that $\mathrm{card}(I) = m+1$ for some $m > 0$ and let $i_0 < ... < i_m$ be the elements of $I$. By induction we know that

$$k_{i_1} + ... + k_{i_m} \in A^{i_1} \subseteq A^{i_0+1} = A^{i_0} \cap (A^{i_0} - k_{i_0}).$$

It follows that $k_{i_0} + ... + k_{i_m} \in A^{i_0}$ as claimed. We have thus proved that $\Sigma_B \subseteq A$. □