Mathematical Logic and Set Theory

Mgr. Libor Běhounek, Ph.D.
RNDr. Martina Daňková, Ph.D.

University of Ostrava
2020
(revised 2025)

This coursebook was written as part of project IRP202012

0 Preface

This text has been written as a coursebook for the course *Mathematical Logic and Set Theory* of the undergraduate study program *Applied Mathematics* at the University of Ostrava. However, it can also serve as an introduction to these areas of mathematics for students of other disciplines and courses, as it is self-contained and does not assume any special knowledge beyond the normal scope of high-school mathematics.

The purpose of this coursebook motivated several intentional departures from the usual textbook exposition of logic and set theory. One of them was the decision to present informal set theory first and leave its axiomatic foundation and the abstract formalism of mathematical logic for later chapters.

Thus, we initially present set theory in its pre-axiomatic form, in which it was developed in the late 19th and early 20th centuries by Cantor and his followers (Chapters 1–3). We then proceed with the basic formalism of classical propositional and predicate logic (Chapters 4–5) and conclude with a brief outline of the modern conception of axiomatic set theory over classical predicate logic (Chapter 6).

Our exposition of set theory relies on sets known from high-school mathematics (sets of numbers, of points, etc.). Hence, in contrast to the axiomatic construction of set theory, we first examine the cardinalities of these familiar sets and introduce the beth-series of cardinal numbers, whereas the ordinal numbers, well-orderings, and alephs are only introduced later. Moreover, cardinal and ordinal numbers are introduced by more intuitive ways than the artificial definitions of axiomatic set theory. The latter are presented, for the sake of completeness, in the final chapter.

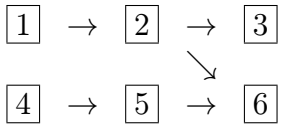
The exposition of mathematical logic in Chapters 4 and 5 mostly employs the formalism of the book [3, Ch. 3], as it is easily comprehensible and may benefit students who later choose to study formal fuzzy logic.

To keep the contents of the course within reasonable bounds, some topics had to be omitted. In the part on mathematical logic, almost all propositions and theorems are given without proofs, and the content is limited to the syntax and semantics of propositional and predicate logic. The proofs as well as additional topics can be found in more comprehensive textbooks on mathematical logic, e.g., [1, 2].

The topics left out of the chapters on set theory in spite of being useful in general mathematics include Zorn's Lemma and the theory of binary relations. An interested reader can study them from additional sources, e.g., [8, 9, 10]. (Some of the mentioned textbooks may be available online even if the links have not been given in references on p. 65 because of their uncertain stability.)

Although the coursebook is designed to be sufficiently detailed for self-study, it is not intended to completely replace classroom instruction. The exercises scattered throughout the text are rather a selection of sample problems than a complete workbook for the course. Some proofs (esp. in Chapter 2) have complicated mathematical notation, but there are actually simple ideas behind them that can easily be explained in the classroom. (In some cases, illustrative explanations can be found in the recommended literature, esp. [9].) Additionally, a classroom lecture can contain more examples and explanatory remarks than a condensed coursebook.

M. Daňková is the primary author of the chapters on logic (4–5) and L. Běhounek is the primary author of those on set theory (1–3, 6); please inform them of any errors found. Some of the chapters assume the knowledge of previous chapters, while others are largely independent. The dependencies between chapters are shown in the following diagram:



Contents:

1. Introductory Concepts ... 5
2. Cardinalities of Sets ... 11
3. Ordinal Numbers and Well-Orderings ... 29
4. Propositional Logic ... 37
5. Predicate Logic ... 49
6. Axiomatic Set Theory ... 57
7. Recommended Literature ... 65

1 Introductory Concepts

In this chapter, we recall a few concepts that will be needed further on, fix notation for sets and logic symbols, and provide an initial account of the notion of set.

Some Preliminaries

We assume the knowledge of basic concepts of high-school mathematics, including the following number systems and their arithmetic:

- *Natural numbers* $0, 1, 2, 3, \ldots$ In set theory, the number 0 is always counted among natural numbers.
- *Integers,* comprising the natural numbers and the negative integers $-1, -2, \ldots$
- *Rational numbers,* which can be defined as irreducible integer fractions with positive denominators.
- *Real numbers.* For our purposes it will suffice to construe reals as infinite decimal representations, with the following qualification:

Since some reals have two decimal representations (e.g., $1.0000\ldots = 0.9999\ldots$), we exclude the representations with trailing 9's in order to prevent ambiguity. We do the same for numeral bases other than decimal: e.g., we identify the number $1/2$ with the binary representation $0.1000\ldots$ and exclude the representation $0.0111\ldots$.

- *Complex numbers* can be identified with ordered pairs of reals.

Recall that real numbers serve as the coordinates of *points* in Euclidean spaces, i.e., there is a one-to-one correspondence between the reals and the points on a line. Similarly, ordered pairs of reals correspond to points in a plane, etc.

Notation 1 The ordered pair of objects a, b will be denoted by $\langle a, b\rangle$, the closed interval from a to b by $[a, b]$, and the open interval by (a, b).

Logic Symbols

Certain phrases used in mathematical texts carry a fixed meaning and occur so frequently that they have been assigned special names and symbols.

Notation 2 (Logic symbols) We will use the following logic symbols and their names:

- $\wedge$ = "and" = *conjunction*
- $\vee$ = "or" (inclusive) = *disjunction*
- $\neg$ = "it is not the case that ..." = *negation*
- $\rightarrow$ = "if ..., then ..." = *implication*
- $\leftrightarrow$ = "if and only if" = *equivalence*
- $(\forall x)$ = "for all x it is the case that ..." = *the universal quantifier*
- $(\exists x)$ = "there exists x such that ..." = *the existential quantifier*

The scope of logic symbols need be indicated by parentheses, e.g., $(x > 1 \wedge x < 2) \vee x = 0$. To save on parentheses, we adopt the convention that the symbols $\rightarrow, \leftrightarrow$ bind less tightly than the other logic symbols.

Negation is often represented simply by crossing the relevant symbol: e.g., $x \neq 5$ stands for $\neg(x = 5)$. The phrase "if and only if" is often shortened to *iff*.

The expressions of the forms $(\exists x)(x < \tau \wedge \Psi)$ and $(\forall x)(x < \tau \rightarrow \Psi)$ can be abbreviated as $(\exists x < \tau)\Psi$ and $(\forall x < \tau)\Psi$, for any condition Ψ and any binary relation in place of $<$.

Example 1 Examples of mathematical statements written with logic symbols:

- The assertion "If $x^2 = 1$, then $x = 1$ or $x = -1$" can be written as:

$$x^2 = 1 \rightarrow (x = 1 \vee x = -1).$$

- The expression $(\forall a)(a + a = 3a)$ represents a false claim (which one?), whereas $(\exists a)(a + a = 3a)$ expresses a true statement (why?).

- The statement that "for every number there is a larger number" can be written as $(\forall x)(\exists y)(y > x)$. The statement that "there is the least number" can be written as $(\exists x)(\forall y)(x \leq y)$.

Note the importance of specifying the *range of variables,* as it may affect the truth of a claim. For instance, the last statement of Example 1 is true for natural numbers, but false for real numbers.

Exercise 1 Interpret the following logical expressions in natural language. Which statements do they express? Which of them are true?

(Here, the symbol $\mid$ denotes divisibility, $\|$ parallelism, and $\perp$ perpendicularity. The variables a, b, c, m, n range over positive integers; x, ε over reals; and p, q, r over lines in a plane.)

(a) $(\exists x)(x \geq 0 \wedge x^2 = 2)$

(b) $(\forall n)\big(n > 2 \rightarrow \neg(\exists a, b, c)(a^n + b^n = c^n)\big)$

(c) $(\exists \varepsilon > 0)(\forall n)\big(\varepsilon < \frac{1}{n}\big)$

(d) $(\forall p, q, r)(p \perp r \wedge q \perp r \wedge p \neq q \rightarrow p \parallel q)$

(e) $n > 1 \wedge (\forall m)(m \mid n \rightarrow m = 1 \vee m = n)$

Exercise 2 Write the statements using logic notation. Use the variables $x, y, \ldots$ for integers and $p, q, \ldots$ for lines. (N.B.: To be able to use logic symbols, one may first need to equivalently rephrase the statements.)

(a) The square of every integer is non-negative.

(b) Perpendicular lines are never parallel.

(c) There are two different integers whose squares equal 1.

(d) There is at most one x such that $x^3 = 343$.

(e) There is a unique x such that $x^3 = 343$.

Elements and Sets

The beginnings of set theory. The study of sets was initially motivated by investigation of ever more complex parts of the real line (such as the domains of continuity for trigonometric series) in mathematical analysis. The notion of set was first introduced by Bernard Bolzano in his book *The Paradoxes of the Infinite,* published 1851. The systematic study of sets began with Georg Cantor in 1873.



Bernard Bolzano



Georg Cantor

Cantor's definition of set. Initially, our exposition will be based on Cantor's informal definition of set (1895):

Definition 1 (Set) By a *set* we are to understand any collection into a whole of definite, distinct objects of our perception or of our thought; these are called the *elements* of the set.

Example 2 Examples of sets:

- The set $\mathbb{N}$ of all natural numbers, $\mathbb{Z}$ of all integers, $\mathbb{Q}$ of all rational numbers, $\mathbb{R}$ of all reals, and $\mathbb{C}$ of all complex numbers.
- The interval $[a, b]$ is the set of all real numbers x such that $a \leq x \leq b$.
- Set-theoretically, geometric figures are construed as sets of points.

Membership of an element in a set.

- The expression $x \in A$ indicates that x is an element of the set A. We also say that x *belongs* to (or is a *member* of) A. Examples: $3 \in \mathbb{N}$, $\pi \in [3, 4]$.
- The expression $x \notin A$ indicates that x is not an element of the set A. Examples: $-1 \notin \mathbb{N}$, $\sqrt{2} \notin \mathbb{Q}$.

Set-theoretic principles. Cantor's definition, in fact, only provides an initial explication of the concept of set and will require additional clarifications. Such clarifications are often called *set-theoretic principles.* Let us present two of them right now:

Principle of Bivalence: *In (classical) set theory we only consider such sets A that for all elements x, exactly one of the cases $x \in A$ and $x \notin A$ is true.*

Collections of elements that fail to satisfy the Principle of Bivalence (e.g., such that are delimited by imprecise or paradoxical conditions) are studied in various *non-classical* set theories (such as fuzzy set theory). In this coursebook, however, we restrict ourselves to the classical, 'Cantorian' set theory in which the Principle of Bivalence is assumed.

Principle of Extensionality: *Sets are construed as being determined by their elements; i.e., if a set A has the same elements as a set B (regardless of order, manner of specification, etc.), then A and B are actually the same set $A = B$.* Formally:

$$(\forall x)(x \in A \leftrightarrow x \in B) \rightarrow A = B \tag{1}$$

Example 3 The set $\mathbb{N}$ of all natural numbers is equal to the set of all integers from the interval $(-\frac{1}{2}, +\infty)$.

Notation 3 We use the usual set-builder notation (also called the *comprehesion terms*):

- The set comprising exactly the elements $a_1, \ldots, a_n$ is denoted by $\{a_1, \ldots, a_n\}$. If the elements form a regular sequence, an ellipsis may be used; e.g., $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- The set of exactly those elements x that have a property Φ is denoted by $\{x \mid \Phi\}$: e.g.,

$$\{2, 4, 6, 8, \ldots\} = \{2n \mid n \in \mathbb{N} \wedge n > 0\}$$
$$\{a_1, \ldots, a_n\} = \{x \mid x = a_1 \vee \ldots \vee x = a_n\}$$

The expression $\{x \mid x \in A \wedge \Psi\}$ can be abbreviated as $\{x \in A \mid \Psi\}$, e.g., $\mathbb{N} = \{z \in \mathbb{Z} \mid z \geq 0\}$.

The empty set. The set that contains no elements is called the *empty set* and is denoted by $\emptyset$. Example: $\{x \in \mathbb{R} \mid x^2 = -1\} = \emptyset$.

The Principle of Extensionality entails that there can only be *one* empty set. (Explain why.)

N.B.: The empty set is not "nothing". Rather, it can be likened to an "empty container".

One-element sets. In set theory, it is important to distinguish between an *element* x and the *one-element set* $\{x\}$. One-element sets are also called *singletons.*

Example 4 The element π is a real *number,* while the singleton $\{\pi\}$ is a *set* of real numbers, containing the single element π. It is the case that $\pi \in \mathbb{R}$, but $\{\pi\} \notin \mathbb{R}$.

Definition 2 (Elementary set operations) The *union, intersection,* and *difference* of the sets A, B are defined as follows:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$
$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$
$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$

We say that sets A and B are *disjoint* if $A \cap B = \emptyset$.

Example 5

- The set of irrational real numbers is defined as $\mathbb{R} \setminus \mathbb{Q}$.
- The intervals $[0, 1]$ and $[2, 3]$ are disjoint. The set $\mathbb{Z}$ is disjoint with $\mathbb{R} \setminus \mathbb{Q}$.

Exercise 3 Are the following collections sets? (If not, why?—Take into account Cantor's definition as well as the set-theoretic principles.)

(a) The collection of all small numbers; (b) the collection of drops in the sea; (c) the collection of all those onboard a ship who are shaved by the ship's barber, who shaves exactly those who do not shave themselves; (d) the collection of all natural numbers smaller than 0.

Exercise 4 (a) Can a given comprehension term denote two different sets? (b) Can two different comprehension terms denote the same set? (c) Can it happen that $\{a, b, c\} = \{a, b\}$ for some values of a, b, c? If not, why? If so, when? (d) Can a set be disjoint with itself? If so, how many such sets exist?

Exercise 5 Determine the sets: $[0, 1] \cup [1, 2]$, $[0, 1] \cap [1, 2]$, $[0, 1] \setminus [1, 2]$.

2 Cardinalities of Sets

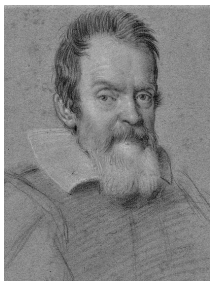
In this chapter we study the problem of comparing the sizes of sets. The concept of *cardinality,* which generalizes the notion of the "number of elements" so that it can be applied to finite as well as infinite sets, is a pivotal concept in set theory that has many applications in general mathematics.

Set Inclusion and Set Equivalence

Galileo's Paradox. Perfect squares are clearly *fewer* than all natural numbers, as only some natural numbers are perfect squares. However, perfect squares can be paired off with all natural numbers in a one-to-one correspondence—so, simultaneously, there are *as many* perfect squares as natural numbers:

$$\begin{array}{ccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \\ 0 & 1 & 4 & 9 & 16 & 25 & 36 & 49 & 64 & \cdots \end{array}$$

Galilei presented this paradox in his dialogue *Two New Sciences* (1638); he concluded that infinite quantities cannot be compared. Cantor's set theory resolves the paradox by distinguishing two ways of comparing infinite sets: by *inclusion* and by *equivalence.*



Galileo Galilei

Definition 3 (Inclusion) We say that a set A is a *subset* of a set B and write $A \subseteq B$ if every element of A is also an element of B. In symbols:

$$A \subseteq B \leftrightarrow (\forall x)(x \in A \rightarrow x \in B) \tag{2}$$

The relation $A \subseteq B$ is called *inclusion.* The expression $\neg(A \subseteq B)$ can be abbreviated as $A \nsubseteq B$. The relation $A \subseteq B \wedge A \neq B$ is usually written as $A \subset B$ or $A \subsetneq B$ and called *proper inclusion* (we then say that A is a *proper subset* of B).

Example 6 $[0, \pi) \subset \mathbb{R}$; a cube is a (proper) subset of its circumscribed ball; $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Proposition 1 *Some properties of inclusion:*

1. $A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$
2. $A \subseteq B \wedge B \subseteq A \rightarrow A = B$
3. $\emptyset \subseteq A, \quad A \subseteq A$

Remark 1 Mathematical claims with omitted quantifiers are understood as being valid for all values of the variables, i.e., as if quantified universally. The last claim of Proposition 1 thus means $(\forall A)(A \subseteq A)$.

Inclusion vs. membership. In set theory, it is important to distinguish carefully between membership and inclusion: membership is a relation between an element and a set, while inclusion is a relation between two sets (determined by which elements they have).

Example 7

- The number π is an element but not a subset of the set $\mathbb{R}$ (as π is a real number and not a set of real numbers). In symbols: $\pi \in \mathbb{R}$, but $\pi \not\subseteq \mathbb{R}$. By contrast, $\{\pi\} \subseteq \mathbb{R}$, while $\{\pi\} \notin \mathbb{R}$.
- The set $\mathbb{N}$ is a subset but not an element of the set $\mathbb{Z}$ (as every natural number is an integer, but the set of natural numbers is not an integer). In symbols: $\mathbb{N} \subseteq \mathbb{Z}$, but $\mathbb{N} \notin \mathbb{Z}$.

Inclusion vs. size comparison. While inclusion can be regarded as a criterion for comparing sets by size, it leaves many pairs of sets incomparable: e.g., $\{1, 3, 5\} \not\subseteq \{5, \pi, \sqrt{2}\}$ as well as $\{5, \pi, \sqrt{2}\} \not\subseteq \{1, 3, 5\}$, even though both sets have exactly three elements, i.e., are "the same size". The method of pairing off elements as in Galileo's Paradox turns out to be a more suitable way of comparing the sizes of sets: e.g., all three-element sets indeed come out the same size by pairing. This method motivates the notions of *bijection* and *set equivalence*.

Definition 4 (Bijection) A *bijection* between the sets A and B is a one-to-one pairing of the elements of both sets, so that each element of A is paired with exactly one element of B and each element of B is paired with exactly one element of A.

The fact that the pairing F is a bijection between the sets A and B is written as $F\colon A \leftrightarrow B$. Another term for a bijection is a *one-to-one correspondence*.

Example 8 The assignment $F\colon n \mapsto n^2$ (for all $n \in \mathbb{N}$) is a bijection between the set of natural numbers and the set of perfect squares, $F\colon \mathbb{N} \leftrightarrow \{n^2 \mid n \in \mathbb{N}\}$.

Definition 5 (Set equivalence) If there is a bijection $F\colon A \leftrightarrow B$, we say that the sets A and B are *equivalent* and write $A \approx B$.

Synonymous terms in use: the sets A and B are *set-equivalent, equipotent, equipollent, equinumerous,* or *the same cardinality.*

Example 9

- $\{5, \pi, \sqrt{2}\} \approx \{1, 2, 3\}$. Proof: a bijective pairing is, e.g., $5 \mapsto 1$, $\pi \mapsto 2$, $\sqrt{2} \mapsto 3$.
- $\mathbb{N} \approx \{n^2 \mid n \in \mathbb{N}\}$, e.g., by $F\colon n \mapsto n^2$ for all $n \in \mathbb{N}$.
- $[0, 1] \approx [0, 5]$, e.g., by the bijection $G\colon x \mapsto 5x$ for all $x \in [0, 1]$.

A resolution to Galileo's Paradox. In *one* sense (namely, that of inclusion), square numbers are fewer than natural numbers; in *another* sense, though (namely, that of set equivalence), there are as many of them:

$$\{n^2 \mid n \in \mathbb{N}\} \subset \mathbb{N}, \text{ but } \{n^2 \mid n \in \mathbb{N}\} \approx \mathbb{N}.$$

Of the two, the notion of set equivalence reflects the sizes of sets better: for instance, finite sets are equivalent if and only if they have the same number of elements.

Exercise 6

(a) Find all proper subsets of the set $\{5, \pi, \sqrt{2}\}$.

(b) Find all valid inclusions between the sets $\emptyset$, $\{1, 2\}$, $[0, \pi)$, and $\{1, \pi, \sqrt{4}\}$.

Exercise 7 Prove the set-equivalences:

(a) $\mathbb{N} \approx \{2n \mid n \in \mathbb{N}\}$

(b) $\mathbb{N} \approx \mathbb{N} \setminus \{1, 3, 5\}$

(c) $\mathbb{N} \approx \mathbb{N} \cup \{\pi\}$

(d) $\mathbb{N} \approx \mathbb{Z}$

Exercise 8 Find bijections that prove the following set equivalences:

(a) $[0, 1] \approx [2, 6]$

(b) $[a, b] \approx [c, d]$ if $a < b$ and $c < d$

(c) $\mathbb{R} \approx \mathbb{R} \setminus \{0\}$

(d) $[0, 1] \approx [0, 1) \approx (0, 1)$

(e) $(-1, 1) \approx \mathbb{R} \approx (0, +\infty)$

Exercise 9 Prove by finding a bijection:

(a) Any two line segments are equivalent.

(b) Any two circles are equivalent.

(c) Any two squares are equivalent.

(d) A closed disk is equivalent to a square.

(e) A line is equivalent to a parabola.

(f) A line segment is equivalent to a line as well as a half-line.

(g) A disk is equivalent to a plane and a plane to a half-plane.

Countable and Uncountable Sets

Exercises 7–9 showed us that various infinite sets are equivalent to one another. This suggests the question: are perhaps *all* infinite sets mutually equivalent? It turns out that the answer is "no": for instance, $\mathbb{N} \not\approx \mathbb{R}$. An elegant method to prove that there are no bijections between these two (and also some other) sets is the so-called *Cantor's diagonal argument.*

Theorem 1 $\mathbb{N} \not\approx \mathbb{R}$.

Proof by Cantor's diagonal argument: By contradiction, assume that $F\colon \mathbb{N} \leftrightarrow \mathbb{R}$. For every $n \in \mathbb{N}$, let $F(n) = \sum_{i=0}^{\infty} d_{n,i} \cdot 10^{-i}$ be the unique (see p. 5) decimal representation of $F(n)$. Take the decimal expansion $r = \sum_{i=0}^{\infty} d_i \cdot 10^{-i}$, where $d_i = 1$ if $d_{i,i} = 0$, and $d_i = 0$ if $d_{i,i} \neq 0$. Clearly $r \in \mathbb{R}$ (as the expansion has no trailing 9's) and $F(n) \neq r$ (as $d_{n,n} \neq d_n$), for any $n \in \mathbb{N}$. Thus, F is not bijective—a contradiction. □

Corollary 1 Hence, $\mathbb{Z} \not\approx \mathbb{R}$ either, as $\mathbb{Z} \approx \mathbb{N} \not\approx \mathbb{R}$. Similarly, $\mathbb{N} \not\approx [0, 1]$, as $[0, 1] \approx \mathbb{R}$; etc.

Thus, the infinite cardinality of $\mathbb{R}$ is *different* from that of $\mathbb{N}$ or $\mathbb{Z}$. More specifically, real numbers are *more numerous* (by cardinality) than natural numbers: as shown by Cantor's diagonal argument, the set $\mathbb{N}$ can be bijectively mapped onto a subset of $\mathbb{R}$ but in no way onto the whole set $\mathbb{R}$. This latter relationship turns out to be a suitable criterion for comparing finite as well as infinite cardinalities:

Definition 6 (Subvalence) We say that a set A is *subvalent* to a set B if there is a bijection between the set A and a subset of B. Notation: $A \preceq B$.

Bijections between A and a subset of B are also called *injections* or *one-to-one functions* from A into B.

The notation $A \prec B$ (*strict subvalence*) means that $A \preceq B$, but $A \not\approx B$. If $A \prec B$, we also say that A has a *smaller cardinality* than B.

Example 10

- Cantor's diagonal argument shows that $\mathbb{N} \prec \mathbb{R}$. Consequently, $\mathbb{Z} \prec \mathbb{R}$, $\mathbb{N} \prec [0,1]$, etc.
- Every finite set is strictly subvalent to any infinite set.
- In finite sets, an m-element set is subvalent to an n-element set if and only if $m \leq n$. In particular, $\emptyset$ is subvalent to every set (so it has the smallest cardinality).

The smallest infinite cardinality. The cardinality of $\mathbb{N}$ is the smallest (by subvalence) among all infinite sets, as follows from the next proposition:

Proposition 2 *If a set A is infinite, then $\mathbb{N} \preceq A$.*

Proof If A is infinite, then we can pick its elements one by one, each different from all previously picked elements, and enumerate them sequentially by the natural numbers $0, 1, 2, \ldots$ (If there were no remaining elements at the n-th step, then A would have only $n-1$ elements, so A would be finite, contrary to the assumption.) So we assign:

$$\begin{aligned} 0 &\mapsto a_0 \in A \neq \emptyset \\ 1 &\mapsto a_1 \in A \smallsetminus \{a_0\} \neq \emptyset \\ 2 &\mapsto a_2 \in A \smallsetminus \{a_0, a_1\} \neq \emptyset \\ &\ldots \end{aligned}$$

In this way we form, step by step, a bijection between $\mathbb{N}$ and a subset $\{a_0, a_1, \ldots\} \subseteq A$; so $\mathbb{N} \preceq A$. □

Countable sets. Thus, by Proposition 2, sets equivalent to $\mathbb{N}$ have the smallest infinite cardinality. Note that by the definition of set equivalence to $\mathbb{N}$, they are those sets whose elements can be enumerated by the natural numbers (or arranged into an infinite sequence). This property motivates the following classification:

Definition 7 A set A is *countable* if $A \preceq \mathbb{N}$; otherwise, it is *uncountable*.

Example 11 Countable and uncountable sets:

- The sets $\mathbb{N}$, $\mathbb{Z}$, and all sets equivalent to these (e.g., any of their infinite subsets, $\mathbb{Z} \cup \{\mathrm{e}, \pi, \sqrt{2}\}$, etc., see Exercise 7), as well as all finite sets are *countable*.
- By Theorem 1, the set $\mathbb{R}$ and all sets equivalent to $\mathbb{R}$ (e.g., any non-degenerate real interval, a line, a line segment, a circle, etc., see Exercise 8) are *uncountable*.

Remark 2 Some authors use the term "countable" to refer only to infinite countable sets; when including finite sets, they use the phrase "at most countable".

Uncountable sets. The next natural question is: are all uncountable sets equivalent to $\mathbb{R}$? In other words, are there just two infinite cardinalities, one countable and one uncountable? A variant of Cantor's diagonal argument shows that the answer is "no" again. For instance, the set of real functions of a real variable, usually denoted by $\mathbb{R}^{\mathbb{R}}$, has a larger cardinality than $\mathbb{R}$:

Proposition 3 $\mathbb{R} \prec \mathbb{R}^{\mathbb{R}}$.

Proof Let every $r \in \mathbb{R}$ be mapped to a real function of a real variable, $f_r \in \mathbb{R}^{\mathbb{R}}$. We will construct a function $g \in \mathbb{R}^{\mathbb{R}}$ which is not assigned to any $r \in \mathbb{R}$, as follows: for every $r \in \mathbb{R}$ let $g(r) = f_r(r) + 1$. Note that for all $r \in \mathbb{R}$, $g \neq f_r$ since $g(r) \neq f_r(r)$. Thus, any pairing between real numbers and functions from $\mathbb{R}^{\mathbb{R}}$ leaves some function out, so $\mathbb{R} \not\approx \mathbb{R}^{\mathbb{R}}$. Trivially, though, $\mathbb{R} \preceq \mathbb{R}^{\mathbb{R}}$—e.g., by mapping each $r \in \mathbb{R}$ to the corresponding constant function. □

Thus, there are at least two uncountable cardinalities (we will see later that there are, in fact, many more). They have been named as follows.

Definition 8 We say that:

- The set A has the *cardinality of the continuum* if $A \approx \mathbb{R}$.
- The set A has the *cardinality of the powerset of the continuum* if $A \approx \mathbb{R}^{\mathbb{R}}$.

Infinite cardinal numbers. The cardinality of a finite set is determined by the number of its elements; finite cardinalities can thus be identified with natural numbers. To label the cardinalities of infinite sets, we will need new, infinite numbers.

Notation 4

- The cardinality of infinite countable sets is denoted by $\aleph_0$ (aleph-naught or aleph-zero).
- The cardinality of the continuum is denoted by $\mathfrak{c}$ (the fraktur c).
- The cardinality of the powerset of the continuum is denoted by $2^{\mathfrak{c}}$ (two to the power of $\mathfrak{c}$).
- In general, the cardinality of a set A is denoted by $|A|$.

Example 12 Examples of cardinalities:

$$|\emptyset| = 0, \quad \left|\{x \in \mathbb{R} \mid x^2 = 1\}\right| = 2, \quad |\mathbb{N}| = |\mathbb{Z}| = \aleph_0, \quad |\mathbb{R}| = |(0,1)| = \mathfrak{c}, \quad |\mathbb{R}^{\mathbb{R}}| = 2^{\mathfrak{c}}.$$

The numbers that represent finite or infinite cardinalities are called *cardinal numbers*, or *cardinals* for short (from Latin *numerus cardinalis* = cardinal numeral; they answer the question, "how many?"). The finite cardinals are the ordinary natural numbers; of the infinite cardinals, we already know three: $\aleph_0$, $\mathfrak{c}$, and $2^{\mathfrak{c}}$. They can be ordered by size (i.e., by subvalence) as follows:

$$0 < 1 < 2 < 3 < \cdots < \aleph_0 < \mathfrak{c} < 2^{\mathfrak{c}}$$

Later we will introduce many other (mainly larger) cardinals and define their arithmetic.

Exercise 10 Find out the cardinalities of the following sets and determine which of them are countable: (a) $\{2\pi\}$; (b) the set of all prime numbers; (c) $\mathbb{R} \cup \{+\infty, -\infty\}$.

The Cantor–Schröder–Bernstein Theorem

The theorem associated with the names of Cantor, Schröder, and Bernstein (although its first sound proof appears to be due to Dedekind) shows that the set-equivalence of A and B can be established by finding two injections—from A to B and vice versa. This is often much easier than trying to directly construct a bijection between A and B.


Ernst Schröder


Felix Bernstein


Richard Dedekind

Theorem 2 (Cantor–Schröder–Bernstein) *If $A \preceq B$ and $B \preceq A$, then $A \approx B$.*

The proof will employ standard notation:

Notation 5

- The *image* of a set X under a mapping F, i.e., the set of elements that are assigned by F to the elements of X, is denoted by $F[X]$.
- If F and G are mappings, then $F \circ G$ denotes their *composition,* which is the mapping $F \circ G\colon x \mapsto z$ if $F\colon x \mapsto y$ and $G\colon y \mapsto z$. (Observe: the composition of bijections is a bijection.)

Proof of the Cantor–Schröder–Bernstein Theorem:

Let $A \preceq B \preceq A$; thus there exist $F\colon A \leftrightarrow F[A] \subseteq B$ and $G\colon B \leftrightarrow G[B] \subseteq A$. Let us define:

$$\begin{aligned} A_0 &= A \\ B_0 &= B \\ A_{i+1} &= G[B_i] \subseteq A_i \\ B_{i+1} &= F[A_i] \subseteq B_i \end{aligned}$$

for all $i \in \mathbb{N}$. Since $B \approx G[B] = A_1$, it suffices to prove that $A \approx A_1$. Let us furthermore define:

$$\begin{aligned} C &= \bigcap_{i\in\mathbb{N}} A_i = \{x \mid (\forall i \in \mathbb{N})(x \in A_i)\} \\ D &= \bigcup_{i\in\mathbb{N}} (A_{2i} \smallsetminus A_{2i+1}) = \{x \mid (\exists i \in \mathbb{N})(x \in A_{2i} \smallsetminus A_{2i+1})\} \\ E &= \bigcup_{i\in\mathbb{N}} (A_{2i+1} \smallsetminus A_{2i+2}) = \{x \mid (\exists i \in \mathbb{N})(x \in A_{2i+1} \smallsetminus A_{2i+2})\} \\ D_1 &= \bigcup_{i\in\mathbb{N}} (A_{2i+2} \smallsetminus A_{2i+3}) = \{x \mid (\exists i \in \mathbb{N})(x \in A_{2i+2} \smallsetminus A_{2i+3})\} \end{aligned}$$

Observe that $A = D \cup E \cup C$ and $A_1 = D_1 \cup E \cup C$. Moreover, $(F \circ G)[A_{2i} \setminus A_{2i+1}] = A_{2i+2} \setminus A_{2i+3}$, so $(F \circ G)[D] = D_1$. Hence the mapping $F \circ G$ is a bijection between D a D_1, and so $D \approx D_1$. □

Example 13 $[0,1] \cap \mathbb{Q} \approx (0,\pi) \cap \mathbb{Q}$ since the mappings $F\colon q \mapsto q+1$ for all rational $q \in [0,1]$ and $G\colon r \mapsto r/4$ for all rational $r \in (0,\pi)$ are injections between the two sets.

Corollary 2 If $A \subseteq B$ and $B \preceq A$, then $A \approx B$.

Proof If $A \subseteq B$, then also $A \preceq B$, since the mapping $x \mapsto x$ for all $x \in A$ is an injection from A to B. The claim then follows by the Cantor–Schröder–Bernstein Theorem. □

Thus, if $A \subseteq B$, then the equivalence $A \approx B$ can be proved just by finding an injection from B to A.

Example 14 $[0,1) \approx [0,1]$ since the mapping $x \mapsto x/2$ for all $x \in [0,1]$ is an injection to $[0,1)$.

Exercise 11 Let $A = [0,1]$ a $B = [0,1)$. Define the injections $F\colon A \to B$ and $G\colon B \to A$ by setting $F(x) = x/2$ for all $x \in A$ and $G(y) = y/2$ for all $y \in B$. Using this pair of injections, construct a bijection between A and B by the procedure from the proof of Theorem 2. Determine the sets A_i, B_i, C, D, D_1, E and the mapping $F \circ G\colon D \leftrightarrow D_1$ from the proof. Compare the resulting bijection with your solution to Exercise 8d.

Exercise 12 Prove that the interiors of any two polygons are set-equivalent.

Cartesian Products

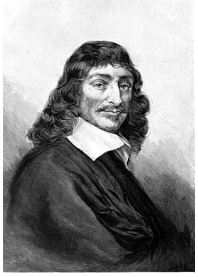
Definition 9 (Cartesian product) The *Cartesian product* of sets A and B is the set $A \times B$ of all ordered pairs $\langle a, b\rangle$ such that $a \in A$ and $b \in B$.

The Cartesian product of sets $A_1, \ldots, A_n$ is the set $A_1 \times \cdots \times A_n$ of all ordered n-tuples $\langle a_1, \ldots, a_n\rangle$ such that $a_1 \in A_1$, …, $a_n \in A_n$.

Formally:

$$A \times B = \{\langle a, b\rangle \mid a \in A \wedge b \in B\}$$
$$A_1 \times \cdots \times A_n = \{\langle a_1, \ldots, a_n\rangle \mid a_1 \in A_1 \wedge \ldots \wedge a_n \in A_n\}$$

If $A_1 = A_2 = \cdots = A_n = A$, then $A_1 \times \cdots \times A_n$ is called the *Cartesian power* and can be written as $A^n = A \times \cdots \times A$. For instance, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ (cf. the Cartesian coordinate system in a plane).



René Descartes (Cartesius)

Bijections and injections. The notion of Cartesian product makes it possible, among other things, to represent the concepts of bijection and injection (see Definitions 4 and 6) in terms of *sets.* In particular, a bijective or injective mapping between sets A and B can be regarded as the set of ordered pairs $\langle \mathit{argument}, \mathit{value} \rangle$, i.e., a subset of the Cartesian product $A \times B$, required to satisfy the appropriate condition of one-to-one assignment.

Definition 10 (Bijection and injection, as sets) A *bijection* between the sets A and B is any subset F of the Cartesian product $A \times B$ such that:

$$(\forall x \in A)(\exists! y \in B)\big(\langle x, y\rangle \in F\big) \wedge (\forall y \in B)(\exists! x \in A)\big(\langle x, y\rangle \in F\big),$$

where the quantifier $\exists!$ abbreviates "there exists a unique" (cf. Exercise 2e).

An *injection* from A to B is a bijection between A and a subset $C \subseteq B$.

If F is a bijection or injection, then $\langle x, y\rangle \in F$ is more commonly written as $F(x) = y$.

Cardinalities of Cartesian products. If A and B are finite sets such that $|A| = m$ and $|B| = n$, then naturally $|A \times B| = m \cdot n$. The case of infinite sets is treated in the following propositions.

Proposition 4 *The sets $\mathbb{N}^2$, $\mathbb{Z}^2$, $\mathbb{Q}$ are countable.*

Proof For a bijection $\pi\colon \mathbb{N}^2 \leftrightarrow \mathbb{N}$ we can take, e,g., the so-called *Cantor pairing function:*

$$\pi(m, n) = \tfrac{1}{2}(m + n)(m + n + 1) + n$$

Thus, $\mathbb{N}^2 \approx \mathbb{N}$. Since $\mathbb{Z} \approx \mathbb{N}$ (Exercise 7d), $\mathbb{Z}^2 \approx \mathbb{N}^2 \approx \mathbb{N}$ as well.

Rationals are irreducible integer fractions, i.e., pairs of integers; therefore $\mathbb{Q} \preceq \mathbb{Z}^2 \approx \mathbb{N}$. □

Corollary 3 Thus, as well, $\mathbb{N} \approx \mathbb{Q}^2 \approx \mathbb{N}^3 \approx \mathbb{Z}^4$, etc.

Proposition 5 $\mathbb{R}^2 \approx \mathbb{R}$.

Proof By Exercise 8 we have $\mathbb{R} \approx [0, 1)$, so it suffices to prove $[0, 1)^2 \approx [0, 1)$. Clearly, $[0, 1) \preceq [0, 1)^2$; so by the Cantor–Schröder–Bernstein Theorem, we only need to find an injection $F\colon [0, 1)^2 \to [0, 1)$.

Let every pair of reals $r_1, r_2 \in [0, 1)$ with the decimal representations $r_1 = \sum_{i=1}^{\infty} d_{1,i} \cdot 10^{-i}$ and $r_2 = \sum_{i=1}^{\infty} d_{2,i} \cdot 10^{-i}$ be assigned the decimal expansion

$$F(r_1, r_2) = \sum_{i=1}^{\infty} d_{1,i} \cdot 10^{-2i+1} + \sum_{i=1}^{\infty} d_{2,i} \cdot 10^{-2i}.$$

Clearly, $F(r_1, r_2) \in \mathbb{R}$ (as the decimal expansion could end in repeating 9's only if r_1 and r_2 did), and F is injective (justify!). □

Corollary 4 Thus also, e.g., $\mathbb{R} \approx \mathbb{C} \approx \mathbb{R}^3$; a line segment is equivalent to a square, a disk, a cube, a hyperboloid; etc.

Proposition 6 *If A and B are countable, then $A \cup B$ and $A \times B$ are countable as well.*

Proof If $A, B \preceq \mathbb{N}$, then $A \cup B \preceq \mathbb{Z} \approx \mathbb{N}$ and $A \times B \preceq \mathbb{N} \times \mathbb{N} \approx \mathbb{N}$. □

Proposition 7 *If A and B have the cardinality of the continuum, then also $A \cup B$ and $A \times B$ have the cardinality of the continuum.*

Proof If $A, B \approx \mathbb{R}$, then $\mathbb{R} \preceq A \cup B \preceq [0,1) \cup [1,2) = [0,2) \approx \mathbb{R}$ and $A \times B \approx \mathbb{R} \times \mathbb{R} \approx \mathbb{R}$. □

Corollary 5 The set $\mathbb{R} \setminus \mathbb{Q}$ of irrational numbers is uncountable.

Proof If the set $\mathbb{R} \setminus \mathbb{Q}$ were countable, then so would be the set $(\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q} = \mathbb{R}$, by Proposition 6; however, by Theorem 1, the latter set is uncountable—a contradiction. (A more involved argument shows that $\mathbb{R} \setminus \mathbb{Q}$ has, in fact, the cardinality of the continuum.) □

Exercise 13 Determine the cardinalities of the following sets: $\mathbb{N} \times \emptyset$, $\mathbb{N} \times \{0\}$, $\mathbb{R} \times \{1,2\}$, $\mathbb{R} \times \mathbb{N}$.

Sets of Sets

Sets as elements of sets. By Cantor's definition (see Defintion 1 on p. 7), a set is a collection of elements into *a whole;* so it is a definite, distinct object of our thought. Therefore, by the same definition, it can be an element of other sets.

Example 15 Examples of sets of sets: the set of all real intervals; the set of all triangles in a plane; the set of all subsets of $\mathbb{N}$; etc.

Elements of elements. Besides membership and inclusion (see p. 12), one must also distinguish between membership in *a set* and membership in *an element* of the set.

- N.B.: An element of an element of a set A need not be an element of A. Example: Let $A = \{\{1,2,3\}, \{3,4,5\}\}$. Then $1 \notin A$; rather, $1 \in \{1,2,3\} \in A$. Note: $\{1,2,3\}$ is not a subset but an element of A.
- Understand the difference: $\emptyset \neq \{\emptyset\} \neq \{\{\emptyset\}\}$.

Definition 11 (Union and intersection of a set of sets) The *union* of a set of sets $\mathscr{A}$ is the set of elements that belong to *at least one* element of $\mathscr{A}$. Notation: $\bigcup \mathscr{A}$.

The *intersection* of a set of sets $\mathscr{A}$ is the set of elements that belong to *all* of the elements of $\mathscr{A}$. Notation: $\bigcap \mathscr{A}$.

Formally:

$$\bigcup \mathscr{A} = \{x \mid (\exists A \in \mathscr{A})(x \in A)\}$$
$$\bigcap \mathscr{A} = \{x \mid (\forall A \in \mathscr{A})(x \in A)\}$$

Common notation (analogously for $\bigcap$):

$$\bigcup_{i \in I} A_i = \bigcup \{A_i \mid i \in I\}, \quad \bigcup_{i=0}^{\infty} A_i = \bigcup \{A_i \mid i \in \mathbb{N}\}.$$

Example 16 $\bigcup_{n=0}^{\infty} [-n, n] = \mathbb{R}$; $\bigcap_{n=1}^{\infty} (-\frac{1}{n}, \frac{1}{n}) = \{0\}$.

Example 17 Observe:

$$\bigcup \{A, B\} = A \cup B, \quad \bigcap \{A, B\} = A \cap B.$$

Proposition 8 *The union of countably many countable sets is countable.*

Proof Without loss of generality we can assume that the countable sets A_i for $i \in \mathbb{N}$ are infinite and mutually disjoint. (Realize: if they are not, the cardinality of their union will not be bigger.) For every $i \in \mathbb{N}$, let $F_i \colon \mathbb{N} \leftrightarrow A_i$. Then the assignment $G \colon \langle i, j \rangle \mapsto F_i(j)$ for all $i, j \in \mathbb{N}$ is a bijection between the countable set $\mathbb{N}^2$ and $\bigcup_{i \in \mathbb{N}} A_i$. □

Corollary 6 The set $\mathbb{A}$ of algebraic numbers (i.e., roots of non-zero polynomials with integer coefficients) is countable. Consequently, the set $\mathbb{R} \setminus \mathbb{A}$ of all real transcendental numbers is uncountable (it can be shown to have the cardinality of the continuum).

Proof Left as an exercise. Hint: There are only countably many polynomials of order n with integer coefficients (why?) and each has at most n roots. □

Exercise 14 (Hilbert's Hotel) In Hilbert's Hotel there are $\aleph_0$ single rooms. The hotel is fully occupied.

(a) Another guest comes. Is it possible to reassign rooms to the current guests so as to accommodate the new guest?

(b) A bus with $\aleph_0$ additional guests comes. Is it possible to reassign rooms to the current guests so as to accommodate all the new guests?

(c) $\aleph_0$ buses come, each with $\aleph_0$ further guests. Is it possible to reassign rooms to the current guests so as to accommodate all of the arriving guests?



David Hilbert

Remark 3 The problems in Exercise 14 are classic, and the name *Hilbert's Hotel* is commonly used in the mathematical literature when referring to this property of infinite cardinalities.

Proposition 9 *The union of countably many sets of the cardinality of the continuum has the cardinality of the continuum.*

Proof Assume (again with no loss of generality) that for all $i \in \mathbb{N}$ we have mutually disjoint sets $A_i \approx \mathbb{R} \approx [i, i+1)$. Then $\bigcup_{i \in \mathbb{N}} A_i \approx \bigcup_{i \in \mathbb{N}} [i, i+1) = [0, +\infty) \approx \mathbb{R}$. □

Definition 12 (Power set) The set of all subsets of a set A is called the *power set* (or *powerset*) of A and is denoted by $\mathscr{P}(A)$. Formally: $\mathscr{P}(A) = \{X \mid X \subseteq A\}$.

Example 18 Examples of power sets:

- $\mathscr{P}(\mathbb{R}) = \{X \mid X \subseteq \mathbb{R}\}$ is the set of all subsets of the real line. E.g., $\mathbb{Q} \in \mathscr{P}(\mathbb{R})$ since $\mathbb{Q} \subseteq \mathbb{R}$.
- $\mathscr{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

- $\mathscr{P}(\{a\}) = \{\emptyset, \{a\}\}$.
- $\mathscr{P}(\emptyset) = \{\emptyset\}$.
- Observe and justify: If $|A| = n \in \mathbb{N}$, then $|\mathscr{P}(A)| = 2^n$.

Proposition 10 $\mathscr{P}(\mathbb{N}) \approx \mathbb{R}$.

Proof We will find injections $F\colon [0,1) \to \mathscr{P}(\mathbb{N})$ and $G\colon \mathscr{P}(\mathbb{N}) \to [0,1)$. Let each real $r \in [0,1)$ with the binary representation $r = \sum_{i=0}^{\infty} b_i \cdot 2^{-(i+1)}$ (without trailing 1's) be matched with the set $F(r) = \{i \in \mathbb{N} \mid b_i = 1\} \in \mathscr{P}(\mathbb{N})$. Vice versa, let each set $A \subseteq \mathbb{N}$ be matched with the decimal number $G(A) = \sum_{i=0}^{\infty} d_i \cdot 10^{-(i+1)}$, where $d_i = 1$ if $i \in A$, and $d_i = 0$ if $i \notin A$. Both mappings are clearly injective (justify!). □

Proposition 11 $\mathscr{P}(\mathbb{R}) \approx \mathbb{R}^{\mathbb{R}}$.

Proof The subvalence $\mathscr{P}(\mathbb{R}) \preceq \mathbb{R}^{\mathbb{R}}$ holds since every subset $A \subseteq \mathbb{R}$ can be injectively matched with its *characteristic function* $\chi_A \in \mathbb{R}^{\mathbb{R}}$, where $\chi_A(x) = 1$ if $x \in A$, and $\chi_A(x) = 0$ if $x \notin A$. The converse subvalence $\mathbb{R}^{\mathbb{R}} \preceq \mathscr{P}(\mathbb{R})$ holds as well, because every real function $F \in \mathbb{R}^{\mathbb{R}}$ can injectively be assigned its *graph* $\{\langle x, F(x)\rangle \mid x \in \mathbb{R}\} \subseteq \mathbb{R}^2$; thus $\mathbb{R}^{\mathbb{R}} \preceq \mathscr{P}(\mathbb{R}^2) \approx \mathscr{P}(\mathbb{R})$. □

Thus, we have proved that $\mathscr{P}(\mathbb{N})$ has the cardinality of the continuum and $\mathscr{P}(\mathbb{R})$ has the cardinality of the powerset of the continuum. In both cases, the cardinality of the power set is larger than the cardinality of the original set: $\mathscr{P}(\mathbb{N}) \approx \mathbb{R} \succ \mathbb{N}$ and $\mathscr{P}(\mathbb{R}) \approx \mathbb{R}^{\mathbb{R}} \succ \mathbb{R}$. This is no coincidence: later we will see that the cardinality of $\mathscr{P}(A)$ is always larger than that of A.

Exercise 15 Let $\mathcal{A} = \{\{1,2\},\{2,3\}\}$. Determine the sets: $\bigcap \mathcal{A}$, $\bigcup \mathcal{A}$, $\mathscr{P}(\mathcal{A})$.

Exercise 16 Determine the sets: $\bigcap_{n=0}^{\infty}[n, +\infty)$; $\bigcap_{x\in\mathbb{R}}[0, e^x)$; $\bigcup \mathscr{P}(\mathbb{N})$; $\bigcap \mathscr{P}(\mathbb{N})$; the intersection of all diameters of a given circle. (Justify your answers.)

Subsets of the Continuum

We have seen that many seemingly large sets of reals (e.g., $\mathbb{Q}$ and $\mathbb{R} \cap \mathbb{A}$—see Corollaries 5 and 6) are only countable. Now, by contrast, we will see that some apparently "almost empty" sets have the cardinality of the continuum.

Cantor's set. Take the interval $[0,1]$ and remove its open middle third $\left(\frac{1}{2}, \frac{2}{3}\right)$; take the two remaining intervals $\left[0, \frac{1}{3}\right]$ and $\left[\frac{2}{3}, 1\right]$ and remove their open middle thirds, $\left(\frac{1}{9}, \frac{2}{9}\right)$ and $\left(\frac{7}{9}, \frac{8}{9}\right)$; take the four remaining intervals and remove their open middle thirds; and so on, *ad infinitum.* The set of reals that remain in the interval $[0,1]$ after this process is called Cantor's set. The set can be formally defined as follows:

Definition 13 *Cantor's set* is the set of reals $\mathbb{D} = \bigcap_{n=0}^{\infty} D_n$, where:

$$D_n = [0,1] \setminus \bigcup_{i=1}^{n} \bigcup_{k=1}^{3^{i-1}} \left(\tfrac{3k-2}{3^i}, \tfrac{3k-1}{3^i}\right). \tag{3}$$

Note that after the n-th step, the set D_n contains the union of 2^n closed intervals of length $1/3^n$; so we have removed intervals of the total length $1 - (2/3)^n$. Thus, after all the steps are completed, the total length of the removed intervals is 1, and so the measure of $\mathbb{D}$ is 0. However, $\mathbb{D}$ is not empty; in fact, $\mathbb{D}$ has the cardinality of the continuum:

Proposition 12 $\mathbb{D} \approx \mathbb{R}$.

Proof First observe that $\mathbb{D}$ contains exactly those reals from $[0,1]$ that have a ternary representation not containing the digit 1. (Contrary to the convention established on p. 5, here we permit expansions with trailing 2's; thus, e.g., $1/3 \in \mathbb{D}$ on the basis of the ternary representation $0.02222\ldots$.) This is because the n-th step of (3) removes from D_n exactly those numbers that require the digit 1 at the n-th place of the ternary expansion.

We construct an injection $F\colon [0,1) \to \mathbb{D}$ as follows: let the number $r \in [0,1)$ with the binary representation $r = \sum_{n=1}^{\infty} b_i \cdot 2^{-n}$ be assigned the number $F(r) = \sum_{n=1}^{\infty} 2b_i \cdot 3^{-n}$. In other words, all occurrences of the digit 1 in the *binary* representation of r are replaced with the digit 2, and the result is understood as the *ternary* representation of $F(r)$. Verify for yourself that $F(r) \in \mathbb{D}$ and that F is injective; thus, $\mathbb{R} \approx [0,1) \preceq \mathbb{D} \subseteq \mathbb{R}$, so $\mathbb{D} \approx \mathbb{R}$ by the Cantor–Schröder–Bernstein Theorem (cf. Corollary 2). □

The existence of countable dense sets (such as $\mathbb{Q}$ and $\mathbb{R} \cap \mathbb{A}$) and, oppositely, uncountable nowhere dense sets (such as $\mathbb{D}$) hints that the cardinalities of subsets of the real line cannot be easily assessed just on the basis of their topological properties.

Cardinality and measure. Determining the cardinalities of sets would be purposeless if they had no significant mathematical consequences. An example of such consequences is the fact that all countable subsets of $\mathbb{R}$ have *measure zero,* i.e., can be covered by a union of intervals of arbitrarily small total length:

Proposition 13 *Every countable set of reals has measure* 0.

Proof Let $A \subseteq \mathbb{R}$ be countable and let ε be an arbitrarily small positive real number. We will cover the elements of A by intervals of the total length not exceeding ε. The set A is countable, therefore its elements can be ordered into a sequence $a_0, a_1, a_2, \ldots$. Let us cover each element $a_n \in A$ by the interval $(a_n - \varepsilon/2^{n+2}, a_n + \varepsilon/2^{n+2})$. Observe that the total length of these intervals is $\varepsilon/2 + \varepsilon/4 + \varepsilon/8 + \cdots = \varepsilon$ and that all elements of A are covered. □

As an exercise, you can analogously show that every countable subset of $\mathbb{C}$ or of the N-dimensional Euclidean space has measure 0 too. (Hint: instead of an interval, take a disk, ball, or N-dimensional hyperball of volume $\varepsilon/2^{n+1}$.)

Corollary 7 The sets $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{A}$ have measure 0. By contrast, the set $[0,1] \setminus \mathbb{Q}$ has, consequently, measure $1 - 0 = 1$. However, not all sets of measure 0 are countable: a counterexample is, e.g., Cantor's set $\mathbb{D}$.

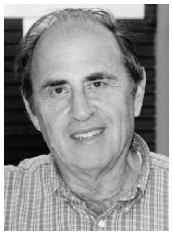
The continuum hypothesis. All subsets of $\mathbb{R}$ encountered so far have either been countable or had the cardinality of the continuum. This led Cantor (1878) to formulate a hypothesis which he then spent years trying in vain to prove:

Continuum Hypothesis (CH): *Each set of real numbers is either countable or has the cardinality of the continuum.*

Hilbert (1900) included the Continuum Hypothesis as the first item on his list of open problems for the 20th century. Gödel (1940) showed that CH cannot be refuted by using the accepted principles of set theory, and Cohen (1963) showed that CH cannot be proved with them either.



Kurt Gödel



Paul Cohen

Exercise 17 (Algorithmically computable numbers) Clarify to yourself:

1. What is the cardinality of the set of all possible strings of length n in a given finite alphabet (such as ASCII or Unicode)?

2. What cardinality does, therefore, the set of all possible finite strings in that alphabet have? (Hint: apply Proposition 8.)

3. What is, therefore, the cardinality of the set of all possible programs written in your favorite programming language? (Note that the choice of the programming language does not matter, as any sufficiently strong—so-called Turing-complete—programming language can emulate all commands of any other programming language.)

4. What is, then, the cardinality of the set of real numbers whose infinite decimal expansions can be printed out, digit by digit, by a computer program? (Conversely, how many reals are there that *cannot* be generated by any computer program?)

Additional Set-Theoretic Principles

CH as an additional set-theoretic principle. As mentioned in the previous section (p. 22), Cantor's Continuum Hypothesis (CH) can neither be proved nor refuted in set theory. Consequently, we can freely choose to adopt either CH or its negation as an additional *set-theoretic principle* (see p. 7), to stipulate the otherwise undetermined behavior of sets of reals.

If we adopt CH as valid, then the cardinality of the continuum $\mathfrak{c}$ is the second smallest infinite cardinality. If we adopt its negation (¬CH), then there are one or more other infinite cardinalities between $\aleph_0$ and $\mathfrak{c}$. Both variants of set theory—with CH and with ¬CH—are being studied, as well as variants in which neither of these principles is accepted and the existence of cardinalities between $\aleph_0$ and $\mathfrak{c}$ is left undetermined.

Further optional set-theoretic principles. There are further set-theoretic principles that we can either accept or reject, refining thereby Cantor's definition of a set. Let us briefly discuss a few of the most important ones.

In the previous sections, we have already tacitly used two principles that have not yet been explicitly stated. Though commonly accepted nowadays, they used to be controversial in the past: the *Principle of Infinity* and the *Principle of Choice*.

Principle of Infinity: *The totality of all natural numbers forms a set.*

Before the development of set theory, the prevailing view was that only *potentially infinite* (i.e., arbitrarily large finite) collections were legitimate. Paradoxes such as Galileo's (p. 11)

were commonly understood as demonstrating the inconsistency of *actually infinite* collections (such as $\mathbb{N}$).

Rejecting the Principle of Infinity amounts to the development of *finite set theory*. (Note that common set operations are closed on finite sets.)

The other principle we already used without mention in previous sections is the Principle of Choice.

Principle of Choice: *For each set of non-empty disjoint sets, there exists a set containing exactly one element from each of them (called a selection set).*

This principle was considered controversial (particularly in the beginning of the 20th century) because the elements of the selection set are left unspecified. It was argued that the selection set is therefore ill defined.

In many cases, the existence of a selection set can be proved without resorting to the Principle of Choice (see Exercise 18 below). The Principle of Choice, however, postulates the existence of a selection set even when we possess no explicit method of selecting the elements and have to make infinitely many arbitrary choices at once.

The Principle of Choice has some counter-intuitive consequences, but so has its negation. Just like CH, the Principle of Choice can neither be proved nor refuted from other principles of set theory (the irrefutability was shown by Gödel in 1940 and the unprovability by Cohen in 1963, as with CH).

Due to its non-constructive nature, it has become customary (especially in mathematical analysis) to explicitly mark each use of the Principle of Choice. In this coursebook, the Principle of Choice has so far been used to prove the following propositions:

- Proposition 2: the proof chose a next unspecified element infinitely many times. (The non-disjointness of the sets from which the elements were chosen was inessential—the proof can be modified to apply the Principle of Choice straightforwardly.)
- Propositions 8 and 9: for each of the infinitely many sets, the proofs tacitly selected *one* out of all bijections onto $\mathbb{N}$ or $[0, 1)$.

Exercise 18 As mentioned, a selection set can often be constructed even without recourse to the Principle of Choice. Define a selection set from an arbitrarily given non-empty set of disjoint:

(a) sets of natural numbers;

(b) open intervals of real numbers;

(c) polygons in a plane. (Hint: choose a coordinate system and use it to select a suitable point from each polygon.)

Non-well-founded sets. Can a set be its own element—e.g., $X = \{X\}$ or $Y = \{5, \pi, \sqrt{2}, Y\}$? The apparatus of set theory works well for such sets; however, one can have conceptual objections against them, as some of the elements they collect into a whole only come into existence by the very act of collecting them. Similar reservations apply to cycles of membership, such as $X = \{\{\{X\}\}\}$ and to infinite descents of membership, such as $\{\{\{\{\ldots\ \ldots\}\}\}\}$. To exclude them, the *Principle of Foundation* is often adopted as a further clarification of Cantor's definition:

Principle of Foundation: *Sets must be well-founded, i.e., the membership relation $\in$ must not form any infinite descending sequence $A \ni X_1 \ni X_2 \ni X_3 \ni \ldots$ (including cycles).*

In other words, each path of descent along $\in$ must sooner or later terminate with an element that has no elements of its own—so either with $\emptyset$ or with an *urelement* (i.e., an element which is not a set). The Principle of Foundation is also called the *Principle of Regularity*.

Cantor's Theorem

We have already hinted that there are sets of even larger cardinalities than that of the powerset of the continuum. The following theorem (due to Cantor and named after him) shows that the hierarchy of cardinalities is unbounded, as the powerset operation always produces a set with a larger cardinality.

Theorem 3 (Cantor) $A \prec \mathscr{P}(A)$.

Proof The subvalence $A \preceq \mathscr{P}(A)$ holds since the mapping that assigns $a \mapsto \{a\}$ for each $a \in A$ is injective; thus it suffices to show that $A \not\approx \mathscr{P}(A)$. We will prove that there is no bijection between A and $\mathscr{P}(A)$:

Assume that $F\colon A \to \mathscr{P}(A)$ is a bijection. Then the set $B = \{x \in A \mid x \notin F(x)\} \in \mathscr{P}(A)$ must be paired by F with some $z \in A$, i.e., $F(z) = B$. But then the definition of B says that z belongs to B if and only if $z \notin F(z) = B$, a contradiction. □

Corollary 8 There are infinitely many different infinite cardinalities:

$$\mathbb{N} \prec \mathscr{P}(\mathbb{N}) \prec \mathscr{P}(\mathscr{P}(\mathbb{N})) \prec \mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{N}))) \prec \cdots$$

Corollary 9 (Cantor's Paradox) Consider the set of all sets, $\mathrm{V} = \{A \mid A = A\}$. Since $\mathscr{P}(\mathrm{V})$ is a set of sets, we obtain that $\mathscr{P}(\mathrm{V}) \subseteq \mathrm{V}$, and thus $\mathscr{P}(\mathrm{V}) \preceq \mathrm{V}$. However, $\mathscr{P}(\mathrm{V}) \succ \mathrm{V}$ by Cantor's Theorem—a contradiction!

A resolution of Cantor's Paradox. By Cantor's definition (p. 7), a set is a "collection into a whole" of objects. Cantor's Paradox can be viewed as a proof that all sets *cannot* be collected into a whole; i.e., that there is no set of all sets.

Proper classes. Cantor's Paradox shows that the universe of sets cannot be regarded as a definite, completely formed object (a set). Such 'unactualizable' collections of elements are called *proper classes*. Cantor's Paradox can thus be formulated as a theorem, proved by contradiction in Corollary 9:

Corollary 10 The universe of sets V is a proper class.

Note that since proper classes cannot be regarded as definite, completely formed mathematical objects, they cannot be elements of sets (cf. Definition 1: "a collection of *definite objects*").

Nevertheless, some set-theoretic notions (namely those which do not refer to them as elements) can be applied to proper classes as well—e.g., the symbol $\in$ (for membership in proper classes), comprehension terms (Notation 3), elementary set operations (Definition 2), the relation of inclusion (Definition 3), and the operation of Cartesian product (Definition 9).

Exercise 19 Give reasons why the following claims hold for any set A: $A \in \mathrm{V}$; $\mathscr{P}(A) \subseteq \mathrm{V}$; $A \cap \mathrm{V} \subseteq A$; $\mathrm{V} = \{A \mid A \prec \mathscr{P}(A)\}$. Explain what is wrong with the apparently evident claim that $\mathrm{V} \in \{\mathrm{V}\}$.

Cardinal Numbers

In the preceding section we noted the existence of infinitely many infinite cardinalities (Corollary 8). Similarly to Notation 4 (p. 15), we are going to introduce further infinite cardinal numbers as their designators. We will also define the general notion of a cardinal number, by abstraction from the relation of set equivalence:

Definition 14 *Cardinal numbers* (or *cardinals* for short) are abstract mathematical objects assigned to sets in such a way that two sets A, B are assigned the same cardinal number if and only if $A \approx B$.

The cardinal number assigned to a set A is denoted by $|A|$ and called the *cardinality* of A. We use the variables $\kappa, \lambda, \mu, \ldots$ for cardinal numbers.

The cardinalities of finite sets (i.e., *finite cardinals*) can be identified with natural numbers: if A is an m-element set, we write $|A| = m$.

Prominent *infinite cardinals* are given special symbols (cf. Notation 4):

- $|\mathbb{N}| = \aleph_0$, $|\mathbb{R}| = \mathfrak{c}$, $|\mathscr{P}(\mathbb{R})| = 2^{\mathfrak{c}}$.
- The cardinalities of the sets

$$\mathbb{N},\ \mathscr{P}(\mathbb{N}),\ \mathscr{P}(\mathscr{P}(\mathbb{N})),\ \mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbb{N}))),\ \ldots$$

are denoted, respectively, by $\beth_0, \beth_1, \beth_2, \beth_3, \ldots$ (beth n). Thus,

$$\beth_0 = \aleph_0, \quad \beth_1 = \mathfrak{c}, \quad \beth_2 = 2^{\mathfrak{c}}, \quad \beth_3 = |\mathscr{P}(\mathbb{R}^{\mathbb{R}})|, \quad \ldots$$

Definition 15 (Cardinal arithmetic) Let $\kappa = |A|$, $\lambda = |B|$, and $A \cap B = \emptyset$. Then we define:

- $\kappa \leq \lambda$ if and only if $A \preceq B$.
- $\kappa + \lambda = |A \cup B|$.
- $\kappa \cdot \lambda = |A \times B|$.
- $\kappa^n = \kappa \cdot \ldots \cdot \kappa$ (n factors, $n \in \mathbb{N}$); we set $\kappa^0 = 1$.
- $2^\kappa = \big|\mathscr{P}(A)\big|$.

Proposition 14

1. The definition of cardinal arithmetic is sound, i.e., the defined values are independent of the choice of sets with cardinalities κ, λ.

2. The following holds:

$$0 < 1 < 2 < 3 < \cdots < \aleph_0 < \mathfrak{c} < \beth_2 < \beth_3 < \beth_4 < \cdots$$

3. The arithmetic of finite cardinalities coincides with the arithmetic of natural numbers.

4. Examples of valid identities:

$$\aleph_0 + 1 = \aleph_0, \quad \aleph_0 + \aleph_0 = \aleph_0, \quad \mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}, \quad 2^{\aleph_0} = \mathfrak{c}, \quad \ldots$$

5. $2^{\beth_n} = \beth_{n+1}$ *for every* $n \in \mathbb{N}$.

Proof The proof is left as an exercise. Hints for some of the claims:

1. The soundness of Definition 15 can be proved by composing the appropriate injections and bijections: e.g., if $A' \approx A \preceq B \approx B'$, then $A' \preceq B'$.

4. $\mathbb{N} \cup \{-1\} \approx \mathbb{N}$, $\mathbb{N} \cup \big(\mathbb{Z} \cap (-\infty, 0)\big) = \mathbb{Z} \approx \mathbb{N}$, $\mathbb{R} \times \mathbb{R} \approx \mathbb{R}$, $\mathscr{P}(\mathbb{N}) \approx \mathbb{R}$. □

Proposition 15 (Laws of cardinal arithmetic)

1. Commutativity and associativity of cardinal addition and multiplication:

$$\kappa + \lambda = \lambda + \kappa \qquad (\kappa + \lambda) + \mu = \kappa + (\lambda + \mu)$$
$$\kappa \cdot \lambda = \lambda \cdot \kappa \qquad (\kappa \cdot \lambda) \cdot \mu = \kappa \cdot (\lambda \cdot \mu)$$

2. Neutral and absorbing elements:

$$\kappa + 0 = \kappa, \quad \kappa \cdot 0 = 0, \quad \kappa \cdot 1 = \kappa$$

3. Distributivity:

$$\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu, \quad 2^{\kappa+\lambda} = 2^\kappa \cdot 2^\lambda$$

4. Monotonicity: If $\kappa_1 \leq \kappa_2$, then:

$$\kappa_1 + \lambda \leq \kappa_2 + \lambda, \quad \kappa_1 \cdot \lambda \leq \kappa_2 \cdot \lambda, \quad 2^{\kappa_1} \leq 2^{\kappa_2}$$

5. Addition and multiplication of infinite cardinals: If at least one of the cardinals $\kappa, \lambda \neq 0$ is infinite, then:

$$\kappa + \lambda = \max(\kappa, \lambda), \quad \kappa \cdot \lambda = \max(\kappa, \lambda)$$

Proof Most of the claims follow directly from the properties of set operations (e.g., the distributivity of cardinal multiplication follows from the identity $A \times (B \cup C) = (A \times B) \cup (A \times C)$, which can be easily verified); in some other cases, one can easily find a suitable bijection (e.g., $A \times B \approx B \times A$) or injection (e.g., $A \cup B \preceq A' \cup B$ if $A \preceq A'$); therefore we leave claims 1–4 as exercises. Claim 5 is equivalent to the Principle of Choice; its proof exceeds the scope of this coursebook. □

Cardinal "multiplication tables". The previous propositions let us determine the values of arithmetical operations for certain prominent cardinal numbers (e.g., finite or equal to $\beth_n$ for $n \in \mathbb{N}$):

$+$	n	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
m	$m{+}n$	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\aleph_0$	$\aleph_0$	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\beth_2$	$\beth_2$	$\beth_2$	$\beth_2$	$\beth_2$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

$\cdot$	0	n	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
0	0	0	0	0	0	$\cdots$
m	0	$m{\cdot}n$	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\aleph_0$	0	$\aleph_0$	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\mathfrak{c}$	0	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\beth_2$	$\cdots$
$\beth_2$	0	$\beth_2$	$\beth_2$	$\beth_2$	$\beth_2$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

κ	n	$\aleph_0$	$\mathfrak{c}$	$\beth_2$	$\beth_3$	$\cdots$
2^κ	2^n	$\mathfrak{c}$	$\beth_2$	$\beth_3$	$\beth_4$	$\cdots$

Proposition 16 *Cardinal numbers form a proper class (denoted by* Card*).*

Proof It suffices to show that for each set A of cardinal numbers there exists a cardinal λ strictly larger than all $\kappa \in A$. For each $\kappa \in A$, take a set A_κ such that $|A_\kappa| = \kappa$. Then by Cantor's Theorem we have that $\mathscr{P}\big(\bigcup_{\kappa\in A} A_\kappa\big) \succ \bigcup_{\kappa\in A} A_\kappa \supseteq A_\kappa$, so $\lambda = \big|\mathscr{P}\big(\bigcup_{\kappa\in A} A_\kappa\big)\big| > \big|\bigcup_{\kappa\in A} A_\kappa\big| \geq |A_\kappa| = \kappa$, for each $\kappa \in A$. □

Corollary 11 In particular, let $A_0 = \mathbb{N}$ and $A_{n+1} = \mathscr{P}(A_n)$ for all $n \in \mathbb{N}$. Define $A_\omega = \bigcup_{n\in\mathbb{N}} A_n$, $\beth_\omega = |A_\omega|$, and $\beth_{\omega+1} = |\mathscr{P}(A_\omega)|$. The proof of Proposition 16 shows that $\beth_{\omega+1} > \beth_n$ for all $n \in \mathbb{N}$, but note that $\beth_\omega > \beth_n$ for all $n \in \mathbb{N}$ as well, since $A_\omega \supseteq A_{n+1} \succ A_n$ for each $n \in \mathbb{N}$. Furthermore, by Cantor's Theorem:

$$\beth_\omega < 2^{\beth_\omega} = \beth_{\omega+1} < 2^{\beth_{\omega+1}} = \beth_{\omega+2} < 2^{\beth_{\omega+2}} = \beth_{\omega+3} < \cdots$$

and so on, beyond all bounds.

Exercise 20

(a) Calculate: $(\aleph_0 + 1)^2$, $2^{\aleph_0+1}$, $2 \cdot \aleph_0 + 1$.

(b) Compare the cardinals $2^{\beth_k\cdot(\beth_m+\beth_n)}$, $2^{\beth_n} + 2^{\beth_m\cdot\beth_k}$ for $k, m, n \in \mathbb{N}$.

(c) Order the cardinals by size: $2^{\aleph_0} + \aleph_0^2$, $\mathfrak{c}^2 + 2^{\mathfrak{c}}$, $\mathfrak{c}^0$, $2 \cdot (2 + \aleph_0)^2$, $\beth_4$, $2^{\beth_2}$.

3 Ordinal Numbers and Well-Orderings

Another central notion of set theory which finds numerous applications in general mathematics is a special type of ordering of elements, called a *well-ordering*. Positions in well-orderings are indicated by a separate kind of numbers—the so-called *ordinal numbers*.

Ordinal Numbers

By iterating the operations of powerset and union at the end of the previous chapter (Corollary 11), we generated an unbounded "transfinite" sequence of infinite cardinals:

$$\beth_0 < \beth_1 < \beth_2 < \cdots \quad < \beth_\omega < \beth_{\omega+1} < \beth_{\omega+2} < \cdots \quad < \beth_{\omega+\omega} < \beth_{\omega+\omega+1} < \cdots \quad \cdots \quad (4)$$

To label the indices in this transfinite sequence, we need new infinite numbers ($\omega, \omega+1$, $\omega+2, \dots$). Unlike cardinal numbers, which represent *amounts* ("how many?"), the new numbers represent *positions* ("where in the sequence?"). By analogy with the distinction between cardinal numerals (one, two, three, ...) and ordinal numerals (first, second, third, ...), the positional numbers are called *ordinal*.

Note a distinctive feature of the transfinite sequence (4) of cardinals $\beth_\alpha$: given any set of cardinals from the sequence, one can construct (by powerset or union—see Corollary 11) the nearest larger cardinal in the sequence. To be suitable for indexing the cardinals $\beth_\alpha$, the sequence of ordinal numbers must share the same property. The definition of ordinal numbers will therefore be based on a principle that ensures this characteristic.

Definition 16 *Ordinal numbers* (or *ordinals* for short) are abstract mathematical objects obtained by the following *generating principle:*

For every set of ordinal numbers there exists the nearest larger ordinal number.

In other words, we postulate that for every set A of ordinals there exists the smallest ordinal β such that $\beta > \alpha$ for every ordinal $\alpha \in A$.

The transfinite sequence of ordinals. Regardless of how many ordinals exist, we can always form the empty set of ordinals. Hence by the generating principle there exists the least ordinal (larger than all elements of the empty set, which is vacuously true); let us denote it by 0. Thence by the same generating principle, the set of ordinals $\{0\}$ brings forth the nearest larger ordinal; let us denote it by 1. Now take the set of already generated ordinals $\{0, 1\}$, which again must be followed by the nearest larger ordinal; let us denote it by 2; etc. By induction we observe that every natural number represents an ordinal. Consequently, the set $\mathbb{N}$ is a set of ordinals and so must be followed by the nearest larger ordinal; let us denote it by ω. Further, the set of ordinals $\mathbb{N} \cup \{\omega\}$ must have the nearest successor; let us denote it by $\omega + 1$; etc.

This way, we generate the unbounded transfinite sequence of ordinal numbers:

$$\begin{aligned}
&0 < 1 < 2 < 3 < \cdots \ < \omega < \omega+1 < \omega+2 < \omega+3 < \cdots \ < \omega+\omega = \\
&= \omega\cdot 2 < \omega\cdot 2+1 < \cdots \ < \omega\cdot 3 < \omega\cdot 3+1 < \cdots \ < \omega\cdot 4 < \cdots \ \cdots \ < \omega\cdot\omega = \\
&= \omega^2 < \omega^2+1 < \cdots \ < \omega^2+\omega < \omega^2+\omega+1 < \cdots \ < \omega^2+\omega\cdot 2 < \cdots \ < \omega^2+\omega\cdot\omega = \\
&= \omega^2\cdot 2 < \omega^2\cdot 2+1 < \cdots \ < \omega^2\cdot 3 < \cdots \ < \omega^2\cdot\omega = \omega^3 < \cdots \ < \omega^\omega < \cdots \ < \omega^\omega\cdot\omega = \\
&= \omega^{\omega+1} < \cdots \ < \omega^{\omega\cdot 2} < \cdots \ < \omega^{\omega\cdot\omega} = \omega^{\omega^2} < \cdots \ < \omega^{\omega^\omega} < \cdots \ < \omega^{\omega^{\omega^\omega}} < \cdots \ < \omega^{\omega^{\omega^{\omega^{\cdots}}}} =
\end{aligned}$$

$$= \varepsilon_0 < \varepsilon_0 + 1 < \cdots < \varepsilon_0^{\varepsilon_0} < \cdots < \varepsilon_0^{\varepsilon_0^{\varepsilon_0^{\cdots}}} = \varepsilon_1 < \cdots < \varepsilon_{\varepsilon_0} < \cdots < \varepsilon_{\varepsilon_{\varepsilon_{\varepsilon_{\cdots}}}} < \cdots \cdots <$$
$$< \omega_1 < \omega_1 + 1 < \cdots \cdots \cdots$$

and so on, beyond all bounds.

Definition 17 (Classification of ordinals) We say that an ordinal is *isolated* if it has the nearest predecessor (i.e., if it is a *successor* ordinal) or is equal to 0; otherwise we call it a *limit* ordinal.

We call an ordinal *finite* if the set of all its predecessors is finite (and analogously for *countable* ordinals). Finite ordinals are identified with natural numbers.

Notation 6 We use Greek letters $\alpha, \beta, \gamma, \ldots$ as variables for ordinal numbers. The first infinite ordinal is denoted by ω and the first uncountable ordinal by ω_1. The system of all ordinals is denoted by Ord. Intervals of ordinal numbers are written as usual, e.g., $[\alpha, \beta) = \{\gamma \in \mathrm{Ord} \mid \alpha \leq \gamma < \beta\}$.

Example 19 The ordinals 0, 6, $\omega + 1$, $\omega^2 + 3$, $\omega^\omega + \omega + 4$ are isolated. The ordinals ω, $\omega \cdot 2$, $\omega^2 + \omega$, $\omega^4 + \omega^2 \cdot 3$, ω^ω, ω_1 are limit. The set of natural numbers can be equated with the ordinal interval $[0, \omega)$.

The class of ordinal numbers. The generating principle of Definition 16 entails that the totality of ordinal numbers does not form a set:

Proposition 17 *The system* Ord *of ordinal numbers is a proper class.*

Proof If all ordinals formed a set, then by Definition 16, it would be succeeded by the nearest larger ordinal, which would thus not be its member—a contradiction. □

Thus, similarly to sets, ordinal numbers are, in a sense, 'too many' to be collectable into a whole without arriving at a contradiction (cf. p. 25). Concordantly, the class of all ordinals cannot be mapped injectively into a set:

Proposition 18 *For any set A, there exists no injection of the whole class* Ord *into A.*

Proof Let us first prove by contradiction that there is no bijection between Ord and any set B. Such a bijection $F\colon \mathrm{Ord} \leftrightarrow B$ would order the elements of B into the same transfinite sequence as the ordinal numbers. Thus by the generating principle of Definition 16, for each set $C \subseteq B$ there would exist an element of B not belonging to C. Now taking the whole set B for C (as B is one of its own subsets), we obtain the existence of an element of B not belonging to B—a contradiction.

Consequently, as there are no bijections between the class Ord and any set B, no injection of Ord into any set A can exist either (since by Definition 6, an injection into A is a bijection onto a set $B \subseteq A$). □

Exercise 21 Determine which of the following ordinals are isolated, limit, finite, countable, uncountable: 10^{100}, ω^{100}, $\omega^2 + \omega$, $\omega^\omega + 2$, $\omega^\omega \cdot 2$, $\omega^{\omega+2}$, $\omega_1 + \omega + 2$.

Exercise 22 Explain whether there exists (a) the largest finite ordinal; (b) the least infinite ordinal; (c) the largest countable ordinal; (d) the largest ordinal.

Well-Ordered Sets

Proposition 19 *Every non-empty set of ordinals has the least element.*

Proof Let A be a non-empty set of ordinals. Consider the set $B = \{\beta \in \mathrm{Ord} \mid (\forall \alpha \in A)\ (\beta < \alpha)\}$ of all strict lower bounds of A. By the generating principle of Definition 16, there is the smallest ordinal γ that is larger than all ordinals from B. We will show that γ is the least element of A.

By the definition of B, all elements of A are strict upper bounds of B; and the ordinal γ has been defined as the *smallest* of all strict upper bounds of B; so γ is a lower bound of A.

It remains to prove that γ is an element of A. We have shown that γ is a lower bound of A; if $\gamma \notin A$, then γ would be a *strict* lower bound of A, and so an element of B. However, γ was defined as the nearest *larger* ordinal to B—a contradiction. □

Definition 18 Orderings such that each non-empty subset of their domain has the least element are called *well-orderings.*

Example 20 Examples of well-orderings:

- By Proposition 19, ordinal numbers are well-ordered by size.
- The following sets of numbers are also well-ordered by size: every set of natural numbers, every set of integers bounded from below, the set $\{2^n - 2^{-m} \mid m, n \in \mathbb{N}\}$. (Justify!)
- The real interval $[0, 1]$ is not well-ordered by size, as, e.g., the set $\{2^{-n} \mid n \in \mathbb{N}\} \subseteq [0, 1]$ has no least element.

Proposition 20 *Selected properties of well-orderings:*

1. In a well-ordered set, every pair of its elements is comparable (in other words, well-orderings are linear orderings).

2. In a well-ordering, there is no strictly decreasing infinite sequence $a_0 > a_1 > a_2 > \cdots$

Proof

1. For any elements a, b of the set consider the least element of the set $\{a, b\}$.
2. By contradiction: the set $\{a_0, a_1, a_2, \ldots\}$ would have no least element. □

The following direct corollary of Propositions 19 and 20.2 may at first appear surprising, in view of the unbounded transfinite progression of the ordinals in the upward direction:

Corollary 12 Every strictly decreasing sequence of ordinals is finite.

Transfinite induction. Theorems that involve ordinal numbers or well-orderings can often be proved by a method called *transfinite induction.* The method is based on the following theorem.

Theorem 4 (on transfinite induction) *Let* $X \subseteq \mathrm{Ord}$ *be a class of ordinals such that for every ordinal* α*, the following implication holds: if* $[0, \alpha) \subseteq X$*, then* $\alpha \in X$*. Then* $X = \mathrm{Ord}$*.*

Proof By contradiction: Assume that $\gamma \notin X$ for some ordinal γ. Then, by Proposition 19, the non-empty set $\{\beta \leq \gamma \mid \beta \notin X\}$ has the least element; let us denote it by α. Since α is the least ordinal not belonging to X, we obtain that $[0, \alpha) \subseteq X$. In that case, however, the theorem's assumption implies that $\alpha \in X$; a contradiction. □

By Theorem 4, the claim that a given statement is true for all ordinals can be proved by verifying the *induction step* for each ordinal α: *if the statement holds for all predecessors of α, then it holds as well for α.*

The use of transfinite induction to construct or define a mathematical object is also called *transfinite recursion*. In practice, proofs by transfinite induction and constructions by transfinite recursion often distinguish the cases for zero, successors, and limit ordinals (cf., e.g., Definition 22 on p. 35). In some definitions and proofs, transfinite induction is used only up to some bound (e.g., to ω^ω) or until the elements of some set are exhausted (as in the proof of Theorem 5 below).

Theorem 5 (Zermelo) *Every set can be well-ordered.*

Proof Let A be any set. We will use transfinite recursion to assign successive ordinal numbers to the elements of A; this transfers the well-ordering of ordinals to A.

Let us perform the induction step of the transfinite recursion: as an induction hypothesis, assume that we have already constructed an injection $F\colon [0,\alpha) \leftrightarrow B \subseteq A$. If $B = A$, we are done. Otherwise, select an element $a \in A \setminus B$ and set $F(\alpha) = a$. This extends the domain of F to include α, thereby completing the induction step (cf. Theorem 4).

To finish the proof, it suffices to realize that for some α, the transfinite recursion will terminate (by exhausting all elements of A): otherwise we would obtain an injection of the whole proper class Ord into A, in contradiction to Proposition 18. Thus for some α, the whole set A will be numbered by ordinals smaller than α and therefore well-ordered. □



Ernst Zermelo

Remark 4 Note that the proof of Zermelo's Theorem made use of the Principle of Choice (find out in which step). Conversely, Zermelo's Theorem entails the Principle of Choice (so they are in fact equivalent), as it is easy to construct a selection set for any system of well-ordered non-empty sets (verify—cf. Exercise 18a). The Principle of Choice is also used in the following two corollaries of Zermelo's Theorem.

Corollary 13 Cardinal numbers are well-ordered by size.

Proof For every cardinal $\kappa = |A|$, let ι_κ be the least ordinal such that there exists a bijection $F\colon [0,\iota_\kappa) \leftrightarrow A$. The ordinal ι_κ is well-defined, as the proof of Theorem 5 shows that there is a bijection between A and $[0,\alpha)$ for some $\alpha \in \mathrm{Ord}$, and so by Proposition 19 there is the least such α. Moreover, if $\kappa \neq \kappa'$ then $\iota_\kappa \neq \iota_{\kappa'}$ (why?).

Each cardinal κ can thus be identified with the ordinal ι_κ, called the *initial ordinal* of cardinality κ. Initial ordinals are well-ordered by size (Proposition 19), and the ordering coincides with that of the corresponding cardinals (clarify to yourself why a larger cardinality has a larger initial ordinal). □

Corollary 14 For any sets A, B, it is the case that $A \preceq B$ or $B \preceq A$.

Proof The claim follows directly from Corollary 13 and Proposition 20.1. □

The transfinite sequence of cardinals. By Corollary 13, the class Card of all cardinal numbers is well-ordered by size (assuming the Principle of Choice). Consequently, the cardinals can be indexed in ascending order by ordinals (cf. the proof of Theorem 5).

Notation 7 Let us sort all infinite cardinals in ascending order by size and index them with successive ordinal numbers. Then the infinite cardinal indexed by the ordinal α is denoted by $\aleph_\alpha$.

We thus obtain the transfinite sequence of all infinite cardinals:

$$\aleph_0 < \aleph_1 < \aleph_2 < \cdots < \aleph_\omega < \aleph_{\omega+1} < \cdots < \aleph_{\omega\cdot 2} < \cdots \tag{5}$$

Since the transfinite sequence (5) contains *all* infinite cardinal numbers, there are no further cardinals between any of its adjacent elements $\aleph_\alpha, \aleph_{\alpha+1}$. Contrast this with the transfinite sequence (4), p. 29, in which intermediary cardinalities may exist—e.g., between $\beth_0$ and $\beth_1$, unless the Continuum Hypothesis (CH) is assumed.

This shows that CH can equivalently be formulated as the claim that $\beth_1 = \aleph_1$ (or, $2^{\aleph_0} = \aleph_1$). The question whether the transfinite series (4) of cardinals $\beth_\alpha$ can have 'gaps' anywhere other than between $\beth_0$ and $\beth_1$ motivates a generalization of CH to all cardinalities:

Generalized Continuum Hypothesis (GCH): $\beth_\alpha = \aleph_\alpha$ *for all ordinals* α.

As with CH, the validity of GCH is independent of other principles of set theory, and so it can be freely adopted or rejected as an additional principle of set theory.

Exercise 23 Determine which of the following sets are well-ordered (in the usual ordering of numbers by size): $\{2, 4, 6, 8\}$, $\mathbb{Z}$, $\{\frac{1}{n+1} \mid n \in \mathbb{N}\}$, $\{1 - 10^{-n} \mid n \in \mathbb{N}\} \cup \{1, 2\}$, $\emptyset$. For those which are well-ordered: number their elements in ascending order by an initial segment of Ord and determine the least unused ordinal (the so-called *order type* of the well-ordering—see Definition 19 below).

Ordinal Arithmetic

Order types of well-orderings. As can be shown by transfinite induction, the elements of any well-ordered set can be numbered in ascending order by the ordinals from the interval $[0, \alpha)$ for some ordinal number α. For each well-ordered set, the ordinal α is uniquely determined and is called the *order type* of the well-ordering. In more detail:

Definition 19 (Order type of a well-ordering) The ordinal α is the *order type* of a well-ordering $\trianglelefteq$ on a set A if there exists a bijection $F\colon [0, \alpha) \leftrightarrow A$ such that for all ordinals $\gamma, \beta < \alpha$, the following holds: $F(\gamma) \trianglelefteq F(\beta)$ if and only if $\gamma \leq \beta$.

Example 21 (See also Exercise 23.) Assuming the usual ordering of real numbers:

• The set $\{\sqrt{2}, \pi, 5\} \subseteq \mathbb{R}$ is well-ordered and has the order type 3, since its elements $\sqrt{2} < \pi < 5$ can be mapped in ascending order onto the ordinals $0 < 1 < 2$ from the ordinal interval $[0, 3) = \{0, 1, 2\}$, assigning $0 \mapsto \sqrt{2}$, $1 \mapsto \pi$, and $2 \mapsto 5$.

• The set $A = \{2 - 10^{-n} \mid n \in \mathbb{N}\} \cup \{2\} = \{1, 1.9, 1.99, 1.999, \ldots, 2\}$ has the order type $\omega + 1$ since the elements of A can be assigned to the elements of the ordinal interval $[0, \omega + 1) = \{0, 1, 2, \ldots, \omega\}$ in ascending order as follows: $n \mapsto 2 - 10^{-n}$ for $n \in \mathbb{N}$ and $\omega \mapsto 2$.

Arithmetic of ordinal numbers. Ordinal numbers, too, can be equipped with arithmetic operations of addition, multiplication, power, etc. Implicitly, we have already used these operations for naming ordinals in the transfinite sequence (e.g., $\omega + 1$, $\omega \cdot 2$, ω^2, etc., see page 29).

The arithmetic of finite ordinals coincides with that of finite cardinals, i.e., natural numbers. However, both arithmetics differ significantly for infinite numbers, despite using the same symbols $+$, $\cdot$, etc.

Ordinal addition. The ordinal sum $\alpha + \beta$ is defined as the order type that results from 'concatenating' well-orderings of order types α and β (in this order). In more detail:

Definition 20 (Ordinal sum) Let A and B be disjoint sets, and let $\leq_1$ be a well-ordering of A with order type α and $\leq_2$ a well-ordering of B with order type β. The ordinal sum $\alpha + \beta$ is defined as the order type of the union $A \cup B$ with the well-ordering $\leq$ such that it coincides with $\leq_1$ on A and with $\leq_2$ on B and for which we furthermore set $a \leq b$ whenever $a \in A$ and $b \in B$.

It can be shown that the definition of ordinal sum is sound, i.e., that it does not matter which well-ordered sets of the order types α and β are chosen.

Example 22 Examples of ordinal addition:

• $2 + 3 = 5$. Proof: If we concatenate two sequences such that the first consists of two elements and the second of three elements, then the resulting five-element sequence can be numbered by all ordinals from the interval $[0, 5)$.

• $1 + \omega = \omega$. Hint: Take, e.g., the sets $A = \{-1\}$ and $B = \mathbb{N}$ with the usual ordering of integers by size, and map the set $A \cup B$ in ascending order onto the interval $[0, \omega) = \mathbb{N}$.

• $\omega + 1 \neq \omega$. Hint: Consider the fact that well-ordered sets of order type ω (such as $\mathbb{N}$) have no last element, while well-ordered sets of order type $\omega + 1$ (such as $\mathbb{N} \cup \{+\infty\}$) do have the last element. Consequently, no exhaustive ascending mapping between well-ordered sets of these order types can exist. The ordinals from $[0, \omega)$ can only be mapped in ascending order onto an *initial segment* of a set of order type $\omega + 1$; therefore, $\omega + 1 > \omega$.

Ordinal multiplication. Informally speaking, the ordinal product $\alpha \cdot \beta$ is the order type of the well-ordering that arises by replacing each element in a well-ordered set of order type β with a well-ordered set of order type α. (Note the order of the factors; an appropriate reading of the ordinal product $\alpha \cdot \beta$ is: "α concatenated β times".)

Equivalently, $\alpha \cdot \beta$ is the order type of the Cartesian product of a set of type β with a set of type α when it is ordered 'by columns', i.e., sorted by the first component and resolving ties by the second component (the so-called *lexicographic order*). More precisely:

Definition 21 (Ordinal product) Let A and B be sets with well-orders $\leq_1, \leq_2$ of order types α and β, respectively. The ordinal product $\alpha \cdot \beta$ is defined as the order type of the Cartesian product $B \times A$ well-ordered by setting: $\langle a, b\rangle < \langle a', b'\rangle$ if and only if $a <_1 a' \vee (a = a' \wedge b <_2 b')$, for all $a, a' \in A$ and $b, b' \in B$.

Again, it can be shown that the definition of ordinal product is sound, i.e., independent of the choice of the well-ordered sets A, B of order types α and β.

Example 23 Examples of ordinal multiplication:

- $\omega \cdot 2 = \omega + \omega$, but $2 \cdot \omega = \omega$. (Check by expanding the definitions.)
- $(\omega + 1) \cdot 2 = \omega \cdot 2 + 1$, while $2 \cdot (\omega + 1) = \omega + 2$:

$$(\omega + 1) \cdot 2 = (\omega + 1) + (\omega + 1) = \omega + (1 + \omega) + 1 = \omega + \omega + 1 = \omega \cdot 2 + 1;$$
$$2 \cdot (\omega + 1) = 2 \cdot \omega + 2 \cdot 1 = \omega + 2.$$

Ordinal exponentiation. We can write the product $\alpha \cdot \alpha$ as α^2, the product $\alpha^2 \cdot \alpha$ as α^3, etc. The least ordinal that is larger than α^n for all $n < \omega$ is denoted by α^ω. Further, we define: $\alpha^{\omega+1} = \alpha^\omega \cdot \alpha$, $\alpha^{\omega+2} = \alpha^{\omega+1} \cdot \alpha$, and in this way we proceed along the whole transfinite sequence of ordinals. Formally, the ordinal power α^β can be defined by transfinite recursion, broken down into three cases based on whether the exponent is zero, a successor, or a limit ordinal:

Definition 22 (Ordinal power) Let α be any ordinal number. For every ordinal β, the power α^β is defined by transfinite recursion as follows:

- If $\beta = 0$, we set $\alpha^0 = 1$.
- If $\beta = \gamma + 1$, we set $\alpha^{\gamma+1} = \alpha^\gamma \cdot \alpha$.
- If β is limit, we define α^β as the least ordinal that is larger than α^γ for all $\gamma < \beta$. (This can be written as follows: $\alpha^\beta = \sup_{\gamma<\beta} \alpha^\gamma$.)

Example 24 Examples of ordinal exponentiation:

- 2^ω is defined as the smallest ordinal that is larger than $1, 2, 4, 8, 16, \ldots$. Thus, $2^\omega = \omega$.
- Applying the definition, we further obtain:

$$2^{\omega+1} = 2^\omega \cdot 2 = \omega \cdot 2, \quad 2^{\omega+2} = \omega \cdot 4, \quad 2^{\omega+n} = \omega \cdot 2^n, \quad 2^{\omega+\omega} = \omega \cdot \omega = \omega^2, \quad \ldots$$

The laws of ordinal arithmetic. The following are some of the general laws of ordinal arithmetic that can be proved by examining the order types of the respective sets or by transfinite induction.

Proposition 21 (Laws of ordinal arithmetic)

1. *Associativity of ordinal addition and multiplication:*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$
$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

2. *Left distributivity:*

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

3. *Monotonicity: If $\alpha_1 < \alpha_2$, then:*

$$\alpha_1 + \beta \leq \alpha_2 + \beta \qquad \beta + \alpha_1 < \beta + \alpha_2$$
$$\alpha_1 \cdot \beta \leq \alpha_2 \cdot \beta \qquad \beta \cdot \alpha_1 < \beta \cdot \alpha_2$$

Similar laws are valid for ordinal powers, but we omit them here for brevity. In contrast, some laws known from the arithmetic of natural or cardinal numbers are not generally valid for transfinite ordinals (see Exercise 25).

Exercise 24 Calculate:

(a) $\omega + 2 + \omega + 3$
(b) $3 \cdot (\omega + 2),\ (\omega + 2) \cdot 3$
(c) $\omega \cdot (\omega + 2),\ (\omega + 2) \cdot \omega$
(d) $(\omega + 2)^3,\ 3^{\omega+2}$

Exercise 25 Find counterexamples showing that in ordinal arithmetic,

1. Commutativity of addition and multiplication is not generally valid;

2. Right distributivity is not generally valid;

3. Proposition 21.3 cannot be strengthened to make the left-monotony laws strict (i.e., with $<$).

Exercise 26 Order by size:

(a) Ordinals: $\omega + 3,\ 3 \cdot \omega,\ 10^{100},\ \omega \cdot 2 + 1,\ \omega^2 + 1,\ \omega + \omega^2$.

(b) Cardinals: $\beth_{\omega+1}, \beth_\omega + 1, \beth_{\omega^2}, \beth_\omega^2, \aleph_0, 2^\mathfrak{c}$.

4 Propositional Logic

Classical mathematical logic. *Formal logic* is a theory of reasoning with purely formal objects or notions. In particular, *classical mathematical logic* studies a language of mathematics, a way of defining abstract mathematical notions, and rules for the reasoning of mathematicians when thinking about mathematical objects, their properties, and relationships.

- Mathematical *objects* are e.g., numbers, functions, sets, structures, circles.
- Rules for *reasoning* comprise generally accepted steps in proofs of mathematical claims.
- Mathematical theorems, propositions, or lemmas are the usual form of expressing properties and relationships between mathematical objects.

Propositional Logic. Propositional logic studies basic *logical connectives*. This study has two parts: *syntax* and *semantics*. On the syntax level, we formalize notions from mathematical practice such as axioms, derivation rules, proof, and provability. The semantics is about truthfulness, i.e., whether a proposition is true or false and how to check it.

The Formal Language of Propositional Logic

Any formal logical system has basic building blocks called symbols of a language using which propositions are created. Below, we describe one of the simplest languages of classical propositional logic with only one symbol for binary connective and one symbol for the truth value "false". The remaining connectives we derive using the basic symbols of the language.

Notation 8 (Compare with Notation 2) We reserve the following symbols $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ for logical connectives and $\top, \bot$ for logical constants, which we call *internal logical symbols*. They are called and read as follows:

symbol	name	reading
$\neg$	negation	IT IS NOT TRUE THAT
$\rightarrow$	implication	IF ... THEN
$\wedge$	conjunction	AND
$\vee$	disjunction	OR
$\leftrightarrow$	equivalence	IF AND ONLY IF
$\top$	tautology	TRUTH; VERUM
$\bot$	contradiction	FALSITY; FALSUM

Let At be a non-empty countable set of propositional variables not containing any internal logical symbols nor auxiliary symbols $(,), [,]$. We call members of At the *propositional atoms*.

Definition 23 The *language* of propositional logic $\mathcal{L}_{At}$ contains the following symbols:

(1) The set of atoms At

(2) The symbol for the logical implication $\rightarrow$

(3) The symbol for falsity $\bot$

(4) Auxiliary symbols (brackets); i.e.,

$$\mathcal{L}_{At} = At \cup \{\rightarrow\} \cup \{\bot\} \cup \{(,), [,]\}.$$

Formulas. Specific sentences formulated in natural language, which can be thought of as true or false, are translated to finite sequences of symbols from a logical language. We call these sequences *formulas*. In particular, propositional formulas consist of symbols of $\mathcal{L}_{At}$ that are determined by the following inductive definition.

Definition 24 (Propositional formula) Let $\mathcal{L}_{At}$ be a language of propositional logic over the set of atoms At. Then:

(a) Every atom $a \in At$ or $\bot$ is an *atomic* propositional formula.

(b) If A, B are formulas then $(A \rightarrow B)$ is a propositional formula.

(c) Every propositional formula is constructed in finite steps using rules (a)–(b).

Formulas constructed using the above inductive definition are often called *well-formed propositional formulas*. In the following, we will simply write "a formula" instead of "a propositional formula".

Every connected subsequence of symbols in a formula, which is itself a formula, is called its *subformula*. By the definition of formulas, every formula (up to atomic ones) is composed of subformulas by connectives.

Definition 25 (Subformula) Let A be a formula.

(a) A is a subformula of A.

(b) If A is of the form $(B \rightarrow C)$ then B and C are subformulas of A.

(c) Nothing else is a subformula of A.

Next, we introduce the remaining connectives and truth constant from Notation 8 as shortcuts of formulas over $\mathcal{L}_{At}$ of the following form:

$$\neg A =_{\text{def}} A \rightarrow \bot \tag{6}$$
$$A \wedge B =_{\text{def}} \neg(A \rightarrow \neg B) \tag{7}$$
$$A \vee B =_{\text{def}} \neg A \rightarrow B \tag{8}$$
$$A \leftrightarrow B =_{\text{def}} (A \rightarrow B) \wedge (B \rightarrow A) \tag{9}$$
$$\top =_{\text{def}} \neg\bot \tag{10}$$

Example 25 Consider $At = \{p, q, r\}$. Examples of propositional formulas over $\mathcal{L}_{At}$ are:

$$p, q, r, \neg p, \neg\neg\neg\neg p, \neg(r \rightarrow \neg q), \neg\neg(r \rightarrow \neg q), ((p \rightarrow \neg q) \vee \neg(r \rightarrow \neg q))$$

The following sequences of symbols are not formulas over $\mathcal{L}_{At}$:

$$pqr, \neg p\neg, \neg a, \wedge q\neg(a \rightarrow \neg b), \neg\neg r(\rightarrow \neg q), ((p \rightarrow\rightarrow q) \vee \neg(r \rightarrow \neg q))$$

Using the symbols of $\mathcal{L}_{At}$, we formalize propositions, which are particular sentences in the natural language of notifying character, where it is meaningful to ask whether they are true or false.

Example 26 For example, if At contains the symbols of alphabet $\{a, b, c, d, \ldots\}$:

- "If the weather is nice, then I go for a walk" is formalized as $(n \to w)$, where the atoms n, w represent the elementary propositions "the weather is nice" and "I go for a walk", respectively.
- "It is not so that the government raises the price of beer, and it will be re-elected" is formalized as $\neg(r \wedge e)$, where the atoms r, e represent "the government raises the price of beer" and "it (the government) will be re-elected", respectively.

Notation 9 We reduce number of parenthesis in formulas using the following rules:

- The outmost parentheses can be omitted.
- For multi-member conjunctions or disjunctions the enclose parentheses can be omitted.
- You can remove the parentheses that are obvious from the priority of the connectives given by Notation 2 (p. 5).

For better readability of formulas, we can replace round brackets by square ones.

Semantics of Propositional Logic

The semantics of classical mathematical logic relies heavily on two main principles:

1. *Principle of Bivalence: Every proposition is either true or false.*
(Compare with the Principle of Bivalence in set theory, p. 7.)

2. *Principle of Truth Functionality: The truth value of a formula follows from the truth values of its parts by applying special functions assigned to the logical connectives.*

One or both of these principles fail in so-called *non-classical logics* (e.g., in fuzzy logic and modal logic).

The truth of a proposition is encoded by the truth value **1**, while the falsity by **0**. Special functions from the second principle are called truth functions, which are functions with arguments and output values from truth values $\{\mathbf{0}, \mathbf{1}\}$.

Truth valuation. We will see in the following definition that the truth of a formula depends on its atomic elements.

Definition 26 Let F_{At} be a set of all well formed formulas over $\mathcal{L}_{At}$. A *truth valuation* of formulas is a function $\mathcal{D}\colon F_{At} \to \{\mathbf{0}, \mathbf{1}\}$ such that

$$\mathcal{D}(a) \in \{\mathbf{0}, \mathbf{1}\},\ a \in At, \tag{11}$$

$$\mathcal{D}(\bot) = \mathbf{0}, \tag{12}$$

$$\mathcal{D}(A \to B) = \mathcal{D}(A) \twoheadrightarrow \mathcal{D}(B), \tag{13}$$

where the truth function $\twoheadrightarrow$ is given by the following table:

$\twoheadrightarrow$	**0**	**1**
0	**1**	**1**
1	**0**	**1**

Exercise 27 Verify that the truth valuation of the derived connectives $\neg, \wedge, \vee, \leftrightarrow$ agree with the truth functions $\mathbf{\neg}, \mathbf{\wedge}, \mathbf{\vee}, \mathbf{\leftrightarrow}$ given by

$\mathbf{\neg}$	
0	**1**
1	**0**

$\mathbf{\wedge}$	**0**	**1**
0	**0**	**0**
1	**0**	**1**

$\mathbf{\vee}$	**0**	**1**
0	**0**	**1**
1	**1**	**1**

$\mathbf{\leftrightarrow}$	**0**	**1**
0	**1**	**0**
1	**0**	**1**

Example 27 There are two suspects in court. One of them always tells the truth and the other always just lies. Each of them said one sentence in his defense.

A: "We're both just telling the truth." (14)

B: "A tells a lie." (15)

Which of the suspects is truthful and which is a liar?

Solution: Denote "A tells a lie" by a and analogously, "B tells a lie" by b.

Then we can formalize (14) and (15) as:

$$\neg a \wedge \neg b, \quad a$$

Obviously, $\mathcal{D}(\neg a \wedge \neg b) = \mathbf{0}$ because, either $\mathcal{D}(a) = \mathbf{1}$ and $\mathcal{D}(b) = \mathbf{0}$, or the other way round. Hence, $\mathcal{D}(\neg a) = \mathbf{\neg 1} = \mathbf{0}$ and $\mathcal{D}(\neg b) = \mathbf{\neg 0} = \mathbf{1}$, and $\mathbf{0 \wedge 1} = \mathbf{0}$. The same result we obtain also for $\mathcal{D}(a) = \mathbf{0}$ and $\mathcal{D}(b) = \mathbf{1}$. Consequently, the suspect A told a lie, i.e., a sentence which is not true, and hence, A is the liar. Consequently, B always tells the truth, which can be verified from the formula a.

Solution 2: Alternatively, we can write all needed truth valuations of atoms a, b and subformulas of $\neg a \wedge \neg b$ in table form:

φ	a	b	$\neg a$	$\neg b$	$\neg a \wedge \neg b$
$\mathcal{D}_1(\varphi)$	**1**	**0**	**0**	**1**	**0**
$\mathcal{D}_2(\varphi)$	**0**	**1**	**1**	**0**	**0**

The last column only contains **0**'s, which means that the formula $\neg b \wedge \neg a$ is false for all possible truth valuations of b, a.

Definition 27 A formula A is a *tautology* if $\mathcal{D}(A) = \mathbf{1}$ for all truth valuations $\mathcal{D}$.

Definition 28 A formula A is a *contradiction* if $\mathcal{D}(A) = \mathbf{0}$ for all truth valuations $\mathcal{D}$.

Example 28 Consider again the formula $\neg b \wedge \neg a$ from Example 27 and check whether it is a tautology or contradiction.

φ	a	b	$\neg a$	$\neg b$	$\neg a \wedge \neg b$
$\mathcal{D}_1(\varphi)$	**1**	**0**	**0**	**1**	**0**
$\mathcal{D}_2(\varphi)$	**0**	**1**	**1**	**0**	**0**
$\mathcal{D}_3(\varphi)$	**1**	**1**	**0**	**0**	**0**
$\mathcal{D}_4(\varphi)$	**0**	**0**	**1**	**1**	**1**

From the truth values in the last column, it is clear that $\neg a \wedge \neg b$ is neither a contradiction nor a tautology.

But adding the requirement that only one of the suspect is a liar and the other is not, i.e., that $(a \wedge \neg b) \vee (b \wedge \neg a)$ is true, results in:

φ	a	b	$(a \wedge \neg b)$	$(b \wedge \neg a)$	$(a \wedge \neg b) \vee (b \wedge \neg a)$	$\neg a \wedge \neg b$
$\mathcal{D}_1(\varphi)$	**1**	**0**	**1**	**0**	**1**	**0**
$\mathcal{D}_2(\varphi)$	**0**	**1**	**0**	**1**	**1**	**0**
$\mathcal{D}_3(\varphi)$	**1**	**1**	**0**	**0**	**0**	**0**
$\mathcal{D}_4(\varphi)$	**0**	**0**	**0**	**0**	**0**	**1**

In all models where $(a \wedge \neg b) \vee (b \wedge \neg a)$ is true, $\neg a \wedge \neg b$ is false, and therefore, $\neg(\neg a \wedge \neg b)$ is true. (Cf. Definition 29 below.)

The table method. The process of writing all truth valuations in the form of a table, which (i) starts from all truth valuations of atoms present in the given formula, (ii) proceeds to more complex subformulas, and (iii) concludes with the truth valuations of the given formula, is called the *table method*.

Using tables of truth valuations, we can also check the logical consequence of a system of requirements, i.e., the formula, which is true provided that all requirements from the given system are true. The following definition reflects it.

Definition 29 (Tautological consequence) A formula A is a *tautological consequence* of a set of formulas T, written $T \models A$, if $\mathcal{D}(A) = \mathbf{1}$ for all truth valuations $\mathcal{D}$ such that $\mathcal{D}(B) = \mathbf{1}$ for all $B \in T$.

We call the formulas of T *special axioms* and T a *theory*.

Definition 30 Let T be a theory. A truth valuation $\mathcal{D}$ is a *model* of the theory T if $\mathcal{D}(A) = \mathbf{1}$ for all formulas $A \in T$. We denote this relation as $\mathcal{D} \models T$.

Example 29 Let $T = \{p, p \to q, \neg q \vee r\}$. Check whether r is a tautological consequence of T.

Solution:

φ	p	q	r	$\neg q$	$p \to q$	$\neg q \vee r$
$\mathcal{D}_1(\varphi)$	**1**	**0**	**0**	**1**	**0**	**1**
$\mathcal{D}_2(\varphi)$	**0**	**1**	**0**	**0**	**1**	**0**
$\mathcal{D}_3(\varphi)$	**0**	**0**	**1**	**1**	**1**	**1**
$\mathcal{D}_4(\varphi)$	**1**	**1**	**0**	**0**	**1**	**0**
$\mathcal{D}_5(\varphi)$	**1**	**0**	**1**	**1**	**0**	**1**
$\mathcal{D}_6(\varphi)$	**0**	**1**	**1**	**0**	**1**	**0**
$\mathcal{D}_7(\varphi)$	**1**	**1**	**1**	**0**	**1**	**1**
$\mathcal{D}_8(\varphi)$	**0**	**0**	**0**	**1**	**1**	**1**

All three formulas in T have only one model, $\mathcal{D}_7 \models T$; and in this truth valuation, r is also true. Consequently, $T \models r$.

Exercise 28 Check if the following claims hold, and find all models of the theories:

$$\begin{aligned}
\{\neg a, \neg a \vee b\} &\models b \\
\{a \to b, b \to c\} &\models a \to c \\
\{(a \to b) \wedge (b \to c)\} &\models a \to c \\
\{a \to b\} &\models (b \to c) \to (a \to c) \\
\{a_1, a_2, \ldots, a_n\} &\models a_1 \wedge a_2 \wedge \ldots \wedge a_n \\
\{a_1, a_2, \ldots, a_n\} &\models (\neg a_1 \to (\neg a_2 \to \ldots (\neg a_{n-1} \to a_n) \ldots))
\end{aligned}$$

Notation 10 In the sequel, we will shorten "if and only if" as "iff".

The following are properties of the tautological consequence.

Proposition 22 (Tautological consequence)

$$\begin{aligned}
T \cup \{A\} \models B \quad &\textit{iff} \quad T \models A \to B \\
\{A\} \models B \textit{ and } \{B\} \models A \quad &\textit{iff} \quad \models A \leftrightarrow B \\
\{A_1, A_2, \ldots, A_n\} \models B \quad &\textit{iff} \quad \{A_1 \wedge A_2 \wedge \ldots \wedge A_n\} \models B
\end{aligned}$$

Proof We give a proof of the first claim; the remaining ones are left to the readers.

$T \cup \{A\} \models B$ iff for all truth valuations $\mathcal{D}$ and $C \in T \cup \{A\}$, if $\mathcal{D}(C) = \mathbf{1}$ then $\mathcal{D}(B) = \mathbf{1}$ iff for all truth valuations $\mathcal{D}$ and $C \in T$, if $\mathcal{D}(C) = \mathbf{1}$ then $\mathcal{D}(A \to B) = \mathbf{1}$ iff $T \models A \to B$. □

Definition 31 We say that formulas A and B are *logically equivalent* and write $A \equiv B$ if for all truth valuations $\mathcal{D}$, $\mathcal{D}(A) = \mathcal{D}(B)$.

Observe that $A \equiv B$ iff $\models A \leftrightarrow B$.

Proposition 23 *Below, we give a list of basic equivalences between formulas.*

$$\begin{aligned}
\textit{idempotency of } \wedge \quad &\ldots \quad A \equiv A \wedge A \\
\textit{idempotency of } \vee \quad &\ldots \quad A \equiv A \vee A \\
\textit{law of excluded middle} \quad &\ldots \quad \top \equiv A \vee \neg A \\
\textit{law of contradiction} \quad &\ldots \quad \bot \equiv A \wedge \neg A \\
\textit{law of double negation} \quad &\ldots \quad A \equiv \neg\neg A
\end{aligned}$$

$$\begin{aligned}
\textit{De Morgan's law} \quad &\ldots \quad A \wedge B \equiv \neg(\neg A \vee \neg B) \\
\textit{De Morgan's law} \quad &\ldots \quad A \vee B \equiv \neg(\neg A \wedge \neg B) \\
\textit{translation of } \to \textit{ to } \vee \quad &\ldots \quad A \to B \equiv \neg A \vee B \\
\textit{translation of } \to \textit{ to } \wedge \quad &\ldots \quad A \to B \equiv \neg(A \wedge \neg B) \\
\textit{commutativity of } \vee \quad &\ldots \quad A \vee B \equiv B \vee A \\
\textit{commutativity of } \wedge \quad &\ldots \quad A \wedge B \equiv B \wedge A
\end{aligned}$$

$$\begin{aligned}
\textit{associativity of } \vee \quad &\ldots \quad A \vee (B \vee C) \equiv (A \vee B) \vee C \\
\textit{associativity of } \wedge \quad &\ldots \quad A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C \\
\textit{distributivity} \quad &\ldots \quad A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C) \\
\textit{distributivity} \quad &\ldots \quad A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)
\end{aligned}$$

Example 30 Find an equivalent formula containing only the connectives (a) $\{\neg, \vee\}$ and (b) $\{\neg, \wedge\}$ to the following formula:

$$\varphi =_{\text{def}} [a \to (\neg b \to c)] \wedge \neg[(c \to \neg b) \to \neg a]$$

Solution to (a): First, we apply the translation of $\to$ to $\vee$, then De Morgan's law. At this point, we could be done, but we will additionally reduce some negations using the law of double negation.

$$\begin{aligned} \varphi &\equiv [\neg a \vee (\neg\neg b \vee c)] \wedge \neg[\neg(\neg c \vee \neg b) \vee \neg a] \\ &\equiv \neg(\neg[\neg a \vee (\neg\neg b \vee c)] \vee \neg\neg[\neg(\neg c \vee \neg b) \vee \neg a]) \\ &\equiv \neg(\neg[\neg a \vee (b \vee c)] \vee [\neg(\neg c \vee \neg b) \vee \neg a]) \end{aligned}$$

Solution to (b): We solve this problem analogously as above:

$$\begin{aligned} \varphi &\equiv [\neg(a \wedge \neg(\neg\neg(b \wedge \neg c)))] \wedge \neg[\neg[(\neg[c \wedge \neg\neg b]) \wedge \neg\neg a]] \\ &\equiv [\neg(a \wedge \neg(b \wedge \neg c))] \wedge [\neg(c \wedge b) \wedge a] \end{aligned}$$

Normal forms. Directly from the definition of equivalent formulas, it follows that different formulas have the same truth table, and vice versa. There are several sets of connectives that can express all possible truth tables by combining members of the set into a propositional formula. The most known is the following set: $\{\wedge, \vee, \neg\}$, and formulas having a particular arrangement of atoms combined with these connectives are called *normal forms*. Below, we give the formal definition of this notion.

Definition 32 (Elementary conjunction and disjunction) Let I be a finite index set and $\{B_i\}_{i \in I}$ be a set of atomic formulas (atoms) or their negations, both of which are called *literals.* Then, a conjunction

$$\bigwedge_{j \in J} B_j$$

of pairwise disjoint literals is called an *elementary conjunction,* and analogously, a disjunction

$$\bigvee_{j \in J} B_j$$

of pairwise disjoint literals is called an *elementary disjunction,* for any $J \subseteq I$.

Definition 33 (Normal forms) Let A be a formula, $I = \{1, 2, \ldots, n\}$ and $\{C_i\}_{i \in I}$, $\{D_i\}_{i \in I}$ be sets of elementary conjunctions and disjunctions, respectively.

(a) We say that a formula $C_1 \vee C_2 \vee \ldots \vee C_n$ is in the *disjunctive normal form.*

(b) We say that a formula $D_1 \wedge D_2 \wedge \ldots \wedge D_n$ is in the *conjunctive normal form.*

(c) Let $A^\vee$ ($A^\wedge$) be a formula in the disjunctive (conjunctive) normal form. If $A \equiv A^\vee$ ($A \equiv A^\wedge$), then we say that $A^\vee$ ($A^\wedge$) is a *disjunctive (conjunctive) normal form of* A.

Proposition 24 (Normal forms) *To every formula A there exist disjunctive and conjunctive normal forms of A.*

Conversion of a formula into a normal form involves either (a) the use of logical equivalences, such as those from Proposition 23, e.g., double negation, De Morgan's laws, and distributivity;

or (b) the truth table, where the truth values in each row correspond with the truth valuation of a suitably chosen elementary conjunction or disjunction.

Example 31 Consider $\varphi \equiv_{\text{def}} a \wedge (b \to (c \vee a))$. Find disjunctive and conjunctive normal forms using (a) logical equivalences and (b) the truth table.

Solution to (a): We will use the translation of $\to$ to $\wedge$ and then the associativity of $\vee$:

$$a \wedge (b \to (c \vee a)) \equiv a \wedge (\neg b \vee (c \vee a)) \equiv a \wedge (a \vee \neg b \vee c) \equiv \varphi^{\wedge}$$

Using the distributivity and idempotence of $\wedge$, we obtain

$$\varphi^{\wedge} \equiv (a \wedge a) \vee (a \wedge \neg b) \vee (a \wedge c) \equiv a \vee (a \wedge \neg b) \vee (a \wedge c) \equiv \varphi^{\vee}.$$

The formulas $\varphi^{\vee}$ and $\varphi^{\wedge}$ are disjunctive and conjunctive normal forms of φ, respectively.

Solution to (b): The truth table of φ is the following:

ψ	a	b	c	φ
$\mathcal{D}_1(\psi)$	**1**	**0**	**0**	**1**
$\mathcal{D}_2(\psi)$	**0**	**1**	**0**	**0**
$\mathcal{D}_3(\psi)$	**0**	**0**	**1**	**0**
$\mathcal{D}_4(\psi)$	**1**	**1**	**0**	**1**
$\mathcal{D}_5(\psi)$	**1**	**0**	**1**	**1**
$\mathcal{D}_6(\psi)$	**0**	**1**	**1**	**0**
$\mathcal{D}_7(\psi)$	**1**	**1**	**1**	**1**
$\mathcal{D}_8(\psi)$	**0**	**0**	**0**	**0**

Observe a truth values of the following elementary conjunctions.

ψ	a	b	c	φ	$a \wedge \neg b \wedge \neg c$	$a \wedge b \wedge \neg c$
$\mathcal{D}_1(\psi)$	**1**	**0**	**0**	**1**	**1**	**0**
$\mathcal{D}_2(\psi)$	**0**	**1**	**0**	**0**	**0**	**0**
$\mathcal{D}_3(\psi)$	**0**	**0**	**1**	**0**	**0**	**0**
$\mathcal{D}_4(\psi)$	**1**	**1**	**0**	**1**	**0**	**1**
$\mathcal{D}_5(\psi)$	**1**	**0**	**1**	**1**	**0**	**0**
$\mathcal{D}_6(\psi)$	**0**	**1**	**1**	**0**	**0**	**0**
$\mathcal{D}_7(\psi)$	**1**	**1**	**1**	**1**	**0**	**0**
$\mathcal{D}_8(\psi)$	**0**	**0**	**0**	**0**	**0**	**0**

It is evident that the truth valuation of an elementary conjunction is **1** iff the truth valuation of all its literals are **1**; otherwise, it is **0**. Using this fact, we can construct elementary conjunctions for all such truth valuations and join them using $\vee$, which results in the disjunctive normal form $\varphi^{\vee}$.

ψ	a	b	c	φ	elem. conjunctions
$\mathcal{D}_1(\psi)$	**1**	**0**	**0**	**1**	$a \wedge \neg b \wedge \neg c$
$\mathcal{D}_2(\psi)$	**0**	**1**	**0**	**0**	
$\mathcal{D}_3(\psi)$	**0**	**0**	**1**	**0**	
$\mathcal{D}_4(\psi)$	**1**	**1**	**0**	**1**	$a \wedge b \wedge \neg c$
$\mathcal{D}_5(\psi)$	**1**	**0**	**1**	**1**	$a \wedge \neg b \wedge c$
$\mathcal{D}_6(\psi)$	**0**	**1**	**1**	**0**	
$\mathcal{D}_7(\psi)$	**1**	**1**	**1**	**1**	$a \wedge b \wedge c$
$\mathcal{D}_8(\psi)$	**0**	**0**	**0**	**0**	

The final disjunctive normal form for φ is

$$(a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge \neg c) \vee (a \wedge \neg b \wedge c) \vee (a \wedge b \wedge c).$$

Analogously we proceed in the case of a conjunctive normal form, where we use that the truth valuation of an elementary disjunction is **0** iff the truth valuation of all its literals are **0**; otherwise, it is **1**.

ψ	a	b	c	φ	$a \vee \neg b \vee c$	$a \vee b \vee \neg c$
$\mathcal{D}_1(\psi)$	**1**	**0**	**0**	**1**	**1**	**1**
$\mathcal{D}_2(\psi)$	**0**	**1**	**0**	**0**	**0**	**1**
$\mathcal{D}_3(\psi)$	**0**	**0**	**1**	**0**	**1**	**0**
$\mathcal{D}_4(\psi)$	**1**	**1**	**0**	**1**	**1**	**1**
$\mathcal{D}_5(\psi)$	**1**	**0**	**1**	**1**	**1**	**1**
$\mathcal{D}_6(\psi)$	**0**	**1**	**1**	**0**	**1**	**1**
$\mathcal{D}_7(\psi)$	**1**	**1**	**1**	**1**	**1**	**1**
$\mathcal{D}_8(\psi)$	**0**	**0**	**0**	**0**	**1**	**1**

All elementary disjunctions needed are listed below.

ψ	a	b	c	φ	elem. disjunctions
$\mathcal{D}_1(\psi)$	**1**	**0**	**0**	**1**	
$\mathcal{D}_2(\psi)$	**0**	**1**	**0**	**0**	$a \vee \neg b \vee c$
$\mathcal{D}_3(\psi)$	**0**	**0**	**1**	**0**	$a \vee b \vee \neg c$
$\mathcal{D}_4(\psi)$	**1**	**1**	**0**	**1**	
$\mathcal{D}_5(\psi)$	**1**	**0**	**1**	**1**	
$\mathcal{D}_6(\psi)$	**0**	**1**	**1**	**0**	$a \vee \neg b \vee \neg c$
$\mathcal{D}_7(\psi)$	**1**	**1**	**1**	**1**	
$\mathcal{D}_8(\psi)$	**0**	**0**	**0**	**0**	$a \vee b \vee c$

Finally, we glue all these elementary disjunction using $\wedge$, which results in the following conjunctive normal form of φ:

$$(a \vee \neg b \vee c) \wedge (a \vee b \vee \neg c) \wedge (a \vee \neg b \vee \neg c) \wedge (a \vee b \vee c)$$

This example demonstrates that formulas can have more than one normal form. From the truth table of a formula A, we generate normal forms in which each of its variables appears exactly once in every elementary disjunction and conjunction. Such normal forms are referred to as *full*.

In some cases, conversion into normal forms can lead to an exponential explosion of the formula.

Example 32 Consider the following formula for a finite n:

$$\varphi \equiv_{\text{def}} (a_1 \vee b_1) \wedge (a_2 \vee b_2) \wedge \ldots \wedge (a_n \vee b_n)$$

This formula is in the conjunctive normal form. Its conversion into a disjunctive normal form by sequential application of the distributivity law, however, results in 3^n elementary conjunctions.

For truth evaluations $\mathcal{D}$, it holds $\mathcal{D}(\varphi) = \mathbf{1}$ iff $\mathcal{D}(a_i \vee b_i) = \mathbf{1}$ for all $i = 1, 2, \ldots, n$ iff $\mathcal{D}(a_i) = \mathbf{1}$ or $\mathcal{D}(b_i) = \mathbf{1}$ for all $i = 1, 2, \ldots, n$. It means that for each couple of variables (a_i, b_i) there are three different truth evaluations fulfilling the requirement. Hence, there are 3^n elementary conjunction in the full disjunctive normal form.

Exercise 29 Find both normal forms of the following formulas:

(a) $a \to (((b \to c) \to b) \to a)$
(b) $a \to (a \to (a \to b))$
(c) $(a \to c) \wedge (b \to \neg c)$

Syntax of Propositional Logic

In mathematical logic, the syntactical part settles the basic laws for connectives in the form of axioms, specifies a rule for deriving new formulas, and studies the notion of provability.

The first step in describing the propositional calculus is choosing some formulas called axioms that describe the behavior of the basic connectives.

Definition 34 (Axioms) Let A, B, C be formulas. A *logical axiom* is a formula of the following form:

(CL1) $A \to (B \to A)$
(CL2) $(\neg A \to \neg B) \to (B \to A)$
(CL3) $(A \to (B \to C)) \to [(A \to B) \to (A \to C)]$

(CL1)–(CL3) are patterns for generating an infinite number of axioms; they are hence called *axiom schemes*.

In the description of the syntactic part of propositional logic, the next step is the introduction of an inference rule allowing the derivation of formulas without paying any attention to their actual meaning. Classical propositional logic has a single inference rule as a basis for argumentation and proving. It is the rule of *Modus Ponens* (MP) and it states the following, for arbitrary formulas A, B:

From A and $A \to B$ derive B.

Often, we write it formally as a scheme:

$$\text{(MP)} \qquad \frac{A, A \to B}{B}$$

We can now formalize the essential concepts on the syntax level, i.e., the notions of the proof and provability of propositional formulas.

Definition 35 (Proof) Let us consider a finite sequence of formulas $\mathcal{P} \equiv_{\text{def}} B_1, B_2, \ldots, B_n$. We say that $\mathcal{P}$ is a *proof* if each B_i is either a logical axiom or is derived by modus ponens from B_j, B_k for some $j, k < i$.

Definition 36 (Provability) A formula A is *provable*, written $\vdash A$, if there exists a proof $\mathcal{P}$ whose last formula is A.

Definition 37 (Provability in a theory) Let T be a set of formulas. A formula A is *provable in a theory* T, written $T \vdash A$, if there exists a finite sequence of formulas $\mathcal{P} \equiv_{\text{def}} B_1, B_2, \ldots, B_n$, where each B_i is either the logical axiom, or $B_i \in T$, or it is derived using modus ponens from B_j, B_k, where $j, k < i$, and the last formula in $\mathcal{P}$ is A.

The proofs of formulas of the form $A \to B$ in a theory T may often be quite complicated. Adding A to the theory T as a hypothesis and proving B in the theory $T \cup \{A\}$ is sometimes much simpler than a direct proof of the original formula. This method of conditional proof is based on the following theorem.

Theorem 6 (Deduction) *Let T be a theory and A, B be formulas. Then*

$$T \vdash A \to B \quad \textit{iff} \quad T \cup \{A\} \vdash B.$$

In the sequel, we will denote the use of the deduction theorem by (D).

Example 33 Find a proof of the formula

$$\varphi \equiv_{\text{def}} [a \to (b \to c)] \to [b \to (a \to c)].$$

Solution: The following sequence of formulas is a proof of φ:

$$\begin{array}{rcll}
\{a \to (b \to c), b, a\} & \vdash & b \to c & \text{(MP)} \\
\{a \to (b \to c), b, a\} & \vdash & c & \text{(MP)} \\
\{a \to (b \to c), b\} & \vdash & a \to c & \text{(D)} \\
\{a \to (b \to c)\} & \vdash & b \to (a \to c) & \text{(D)} \\
 & \vdash & [a \to (b \to c)] \to [b \to (a \to c)] & \text{(D)}
\end{array}$$

The following theorem provides us with the syntactic form of equivalent modifications and equivalent formulas.

Theorem 7 (Equivalence) *Let A' arise from A by replacing some subformulas $A_1, \ldots, A_n$ with formulas $A'_1, \ldots, A'_n$. If $\vdash A_i \leftrightarrow A'_i$ for all $i = 1, \ldots, n$ then $\vdash A \leftrightarrow A'$.*

We denote an application of the Equivalence Theorem by (E).

Completeness. The syntactic provability and semantic truth in models are two different characterizations of logically valid formulas. Intuitively, we expect that whatever is provable in the logical system is true. The following fundamental theorem of propositional logic confirms this natural expectation, and even more, it states that there is a proof of an

arbitrary true formula (tautology). The theorem was proved by Emil Post in his 1920 dissertation.



Emil Post

Theorem 8 (Completeness) *Let T be a theory and A a formula. Then*

$$T \vdash A \qquad \textit{iff} \qquad T \models A.$$

One of the principal problems when dealing with some mathematical theory is to decide whether it leads to a contradiction or not. If a theory does not lead to a contradiction, then it is called consistent; otherwise, it is contradictory. Since $\{\bot\} \vdash A$ for any formula A (as can easily be verified using the Completeness Theorem), the contradictoriness of a theory can be defined as follows:

Definition 38 A theory T is *contradictory* (or *inconsistent*) if $T \vdash A$ for every formula A. Otherwise, it is *consistent*.

Proposition 25 *A theory $T \cup \{\neg A\}$ is contradictory iff $T \vdash A$.*

Proof If $T \cup \{\neg A\}$ is contradictory then $T \cup \{\neg A\} \vdash \bot$, and by (D), we obtain that $T \vdash \neg A \to \bot$. It is equivalent to $T \vdash \neg\neg A$, and moreover, $\neg\neg A$ is equivalent with A. Hence, by completeness, $T \vdash A$.

If $T \vdash A$ then also $T \cup \{\neg A\} \vdash A, \neg A, A \wedge \neg A$, where $A \wedge \neg A$ is a contradiction. From $A \wedge \neg A \to \bot$ and $\vdash \bot \to B$, using (MP), we obtain $T \cup \{\neg A\} \vdash B$, for an arbitrary formula B. □

5 Predicate Logic

Propositional calculus cannot capture the whole of mathematics, which uses expressions such as "there exists", "x and y are similar", or "lines are intersecting at point p". Therefore, we turn to the predicate (first-order) logic, which extends propositional logic to deal with quantifiers, relations, and functions.

The Formal Language of Predicate Logic

Definition 39 The formal language of classical (first-order) predicate calculus consists of:

(1) *Logical symbols:*

- An infinite countable set of object variables $x, y, \ldots$
- The logical constant for the falsity $\bot$
- The logical connective of implication $\rightarrow$
- The symbol for the general quantifier $\forall$
- Parentheses, brackets, and other punctuation symbols

(2) *Special symbols:*

- A countable set of object constants $\mathbf{c}, \mathbf{d}, \ldots$
- A set of function symbols of various arities $f, g, \ldots$
- A set of predicate symbols of various arities $P, Q, \ldots$

By $\mathcal{L}_S$, we denote the language of predicate logic with a set of special symbols S.

We design the following notion of *terms* to denote objects. Terms and *formulas*, represented as strings of symbols, are defined inductively using the so-called *formation rules*.

Definition 40 (Term)

(i) A variable x or constant $\mathbf{c}$ is an (atomic) term.

(ii) Let f be an n-ary function symbol and $t_1, \ldots, t_n$ terms. Then $f(t_1, \ldots, t_n)$ is a term.

(iii) Only expressions obtained by finitely many applications of rules (i) and (ii) are terms.

Definition 41 (Formula)

(i) The logical constant $\bot$ is an (atomic) formula.

(ii) Let P be an n-ary predicate symbol and $t_1, \ldots, t_n$ terms. Then $P(t_1, \ldots, t_n)$ is an (atomic) formula.

(iii) If A, B are formulas, then $A \rightarrow B$ is a formula.

(iv) If A is a formula and x is a variable, then $(\forall x)A$ is a formula.

(v) Only expressions obtained by finitely many applications of rules (i)–(iv) are formulas.

The derived connectives are defined as in the propositional logic by (6)–(10). The *existential quantifier* is derived from the universal one as follows:

$$(\exists x)A \equiv_{\text{def}} \neg(\forall x)\neg A \tag{16}$$

Due to the law of double negation, the universal and the existential quantifiers exhibit a duality. Consequently, we call them *dual*, i.e., $\forall$ is dual to $\exists$ and vice versa.

Definition 42

- An occurrence of the variable x is *bounded* in a formula φ if it is part of a subformula $(\forall x)B(x)$ or $(\exists x)B(x)$ of φ.
- An occurrence of the variable x in a formula φ which is not bounded is called *free*.
- A formula is *closed* if it does not contain any occurrence of a free variable.
- The formula that contains at least one occurrence of a free variable, is called *open*.

The substitution of variables in mathematical expressions is a common thing. However, it is necessary to follow certain rules not to get an expression that has a different meaning after the replacement. Consider, for example:

$$\varphi \equiv_{\text{def}} (\forall y)(y = 2 \cdot x), \quad \varphi' \equiv_{\text{def}} (\forall y)(y = 2 \cdot y)$$

Formula φ expresses a functional dependence between variables x and y, while φ', where x replaces y in φ, significantly differs from φ and yields a non-sense. The following definition states how to apply a substitution correctly.

Definition 43

- By $\varphi(x/t)$ we denote a formula in which the term t replaces all the free occurrences of the variable x.
- A term t is *substitutable* for a free variable in φ if there is no free variable y in t such that y would become bounded in $\varphi(x/t)$.

Example 34 The expressions

$$2^{2^n},\ x + y,\ f(x),\ h(x, f(x)),\ f(g(x))$$

are terms. The expressions

$$P(2^{2^n}),\ Q(y + x, f(x)),\ P(g(f(z)), f(x)),\ x < f(x)$$

are atomic formulas. The expression

$$\neg Q(y, f(x)) \to (\forall x)P(y, f(x)) \tag{17}$$

is a formula, where the first occurrence of x is free, the second is bounded, and both occurrences of y are free. Thus, (17) is an open formula.

Term $t_1 \equiv_{\text{def}} (y + z)$ is substitutable to φ for the variable y, while $t_2 \equiv_{\text{def}} (x + z)$ is not substitutable for y in (17) because a replacement of the second occurrence of y by t_2 would lead to the bounding of x in $(\forall x)P((x + z), f(x))$.

Remark 5 Predicate logic with the language of Definition 39 is more precisely called *first-order* predicate logic. In contrast, *second-* and *higher-order* predicate logic additionally contains predicates applicable to predicates (i.e., predicates of the second order) and further higher-order constructions. In this coursebook we only deal with first-order predicate logic.

Semantics of Predicate Logic

The semantics of predicate logic is based on a particular structure, which gives meaning to the symbols from the formal language.

Definition 44 Let $\mathcal{L}_S$ be a language of predicate logic. The *structure* for $\mathcal{L}_S$ is

$$\mathcal{D} =_{\text{def}} \langle D, P_D, \ldots, f_D, \ldots, \mathbf{c}_D, \ldots \rangle,$$

where D is a nontempty set; $P_D \subseteq D^n, \ldots$ are n-ary relations assigned to each n-ary predicate symbol $P, \ldots$; and $f_D \colon D^n \to D, \ldots$ are n-ary functions on D assiged to each n-ary functional symbol $f, \ldots$ Finally, $c_D \in D, \ldots$ are assigned to each constant symbol $\mathbf{c}, \ldots$ of $\mathcal{L}_S$.

Definition 45 (Interpretation) Let $\mathcal{D}$ be a structure for the language $\mathcal{L}_S$.

- An *evaluation of object variables* is a mapping e, which assigns the value $e(x) \in D$ to each variable x.
- Let e be an evaluation of object variables. An *evaluation of terms* induced by e in $\mathcal{D}$ is inductively defined as follows:

$$\begin{aligned} \mathcal{D}_e(\mathbf{c}) &= c, \quad c \in D, \\ \mathcal{D}_e(x) &= e(x), \\ \mathcal{D}_e(f(t_1, \ldots, t_n)) &= f_D(\mathcal{D}_e(t_1), \ldots, \mathcal{D}_e(t_n). \end{aligned}$$

- Let e be an evaluation of object variables and $t_1, \ldots, t_n$ be terms. Moreover, by $e(x/c)$ denote an evaluation that is identical with e except that it assigns an individual $c \in D$ to the variable x. An *interpretation of a formula* φ induced by e in a structure $\mathcal{D}$ is a truth value $\mathbf{0}$ or $\mathbf{1}$ denoted by $\mathcal{D}_e(\varphi)$ and defined inductively as follows:

φ	$\mathcal{D}_e(\varphi)$
$\bot$	$\mathbf{0}$
$P(t_1, \ldots, t_n)$	$\mathbf{1}$ iff $(\mathcal{D}_e(t_1), \ldots, \mathcal{D}_e(t_n)) \in P_D$
$A \to B$	$\mathcal{D}_e(A) \twoheadrightarrow \mathcal{D}_e(B)$
$(\forall x)A$	$\inf\{\mathcal{D}_{e(x/c)}(A) \mid c \in D\}$

Proposition 26 *Let $\mathcal{D}$ be a structure for the language $\mathcal{L}_S$ and e be an evaluation of the object variables. Then*

$$\begin{aligned} \mathcal{D}_e(A \wedge B) &= \mathcal{D}_e(A) \boldsymbol{\wedge} \mathcal{D}_e(B) \\ \mathcal{D}_e(A \vee B) &= \mathcal{D}_e(A) \boldsymbol{\vee} \mathcal{D}_e(B) \\ \mathcal{D}_e(A \leftrightarrow B) &= \mathcal{D}_e(A) \twoheadleftarrow\!\!\!\!\twoheadrightarrow \mathcal{D}_e(B) \\ \mathcal{D}_e((\exists x)A) &= \sup\{\mathcal{D}_{e(x/c)}(A) \mid c \in D\} \end{aligned}$$

Definition 46

- A formula φ is *satisfied* in $\mathcal{D}$ by the evaluation e, written $\mathcal{D}_e \models \varphi$, if $\mathcal{D}_e(\varphi) = \mathbf{1}$.
- A formula φ is *satisfiable* in $\mathcal{D}$ if it is satisfied by some evaluation e.
- A formula φ is *valid* in $\mathcal{D}$, written $\mathcal{D} \models \varphi$, if it is satisfied by all evaluations e. We also say that $\mathcal{D}$ is a *model* of φ.

Example 35 Let $S = \{f, \leq\}$ and $\mathcal{M} = \langle M, f_M, \leq_M \rangle$ be a structure for $\mathcal{L}_S$, where $M = \{0, 1, 2, 3, 4\}$, $\leq_M$ is a standard ordering of natural numbers, and $f_\mathcal{M}$ is defined as follows:

x	0	1	2	3	4
$f_M(x)$	1	2	2	2	3

Then a formula

$$\varphi \equiv_{\text{def}} (x \leq y) \to (f(x) \leq f(y))$$

is satisfied for e assigning $3, 2$ to x, y, respectively: in this case, $\mathcal{M}_e(x \leq y) = \mathbf{0}$ because $(3, 2) \notin \leq_M$, or equivalently $3 \not\leq_M 2$, and $\mathbf{0} \twoheadrightarrow a = \mathbf{1}$ for an arbitrary $a \in \{\mathbf{0}, \mathbf{1}\}$. Hence, φ is satisfiable in $\mathcal{M}$.

Moreover, φ is true in $\mathcal{M}$ because for all $c, d \in M$, if $c \leq_M d$, then

$$\mathcal{M}_{e(x/c, y/d)}(f(x) \leq f(y)) = \mathbf{1}.$$

Definition 47

- A formula φ is a *tautology* (or, is *logically true*), written $\models \varphi$, if it is true in every structure for the language $\mathcal{L}_S$.
- A formula φ is a *contradiction* if it does not have a model.
- *A model of a theory* (i.e., of a set of formulas) T is a structure $\mathcal{D}$ such that $\models_\mathcal{D} \varphi$ for all $\varphi \in T$. In symbols: $\mathcal{D} \models T$.
- A formula φ is a *logical consequence* of a theory T, written $T \models \varphi$, if φ is true in all models of T.

Example 36 Check whether $A(x) \models (\forall x)A(x)$.

Solution: A structure $\mathcal{D}$ is a model of $A(x)$ if it is satisfied by all evaluations, i.e., $\mathcal{D}_e(A(x)) = 1$ for all evaluations e. Consequently, $\mathcal{D}_{e(x/c)}(A(x)) = \mathbf{1}$ for all $c \in D$. Then also

$$\inf\{\mathcal{D}_{e(x/c)}(A(x)) \mid c \in D\} = \mathbf{1} \quad \text{iff} \quad \mathcal{D}((\forall x)A(x)) = \mathbf{1}.$$

Hence, $A(x) \models (\forall x)A(x)$ is valid.

Example 37 Check whether $\models A(x) \to (\forall x)A(x)$.

Solution: Consider a structure $\mathcal{D} = \langle \{a, b\}, A_D \rangle$, where $A_D = \{a\}$. Moreover, let e assign a to x. Then $\mathcal{D}_e(A(x)) = \mathbf{1}$ because $a \in A_D$. However, $\mathcal{D}_e((\forall x)A(x)) = \mathbf{0}$, and thus, $\not\models A(x) \to (\forall x)A(x)$.

Exercise 30 Find a structure $\mathcal{D}$ in which

$$\mathcal{D} \models A(x) \to (\forall x)A(x).$$

Exercise 31 (a) Find a set D and a function f on D such that the following is valid:

$$\text{There exists } x \in D \text{ such that } f(y) < x \text{ for all } y \in D. \tag{18}$$

(b) Find a set D and a function f on D such that (18) is not valid.

Exercise 32 Consider $D = \{1, 2, 3\}$ and a function f on D given by the following table:

x	1	2	3
$f(x)$	2	1	2

Check whether the following claims are valid:

(a) For all x there exists y such that $x = f(y)$.

(b) If there exists x such that $f(f(x)) = x$, then there exists x such that $f(x) = x$.

(c) If there exists y such that $f(y) = x$, then $f(f(x)) = x$.

Syntax of Predicate Logic

Definition 48 (Axioms) Let A, B, C be formulas, t be a term and x be an object variable. A *logical axiom* is a formula of the form (CL1)–(CL3) as well as the following form:

$$\begin{array}{ll} \text{(CL4)} & (\forall x)A(x) \to A(x/t) \\ \text{(CL5)} & (\forall x)(A \to B) \to (A \to (\forall x)B), \end{array}$$

where t is substitutable in A for x in (CL4), and x is not free in A in (CL5).

Classical predicate logic has two inference rules as a basis for argumentation and proving. These are: the rule of *Modus Ponens* (MP, see p. 46) and the rule of *Generalization* (GR) allowing derivation of a universally quantified formula from an arbitrary previously derived formula A:

$$\text{From } A \text{ derive } (\forall x)A.$$

We write it formally as a scheme:

$$\text{(GR)} \qquad \frac{A}{(\forall x)A}$$

Remark 6 (Predicate logic with equality) The equality sign $=$ is sometimes regarded as an internal logical symbol. In that case, predicate calculus is extended by the following *axioms of equality:*

$$\begin{array}{ll} \text{(EQ1)} & x = x \\ \text{(EQ2)} & [(x_1 = y_1) \wedge (x_2 = y_2) \wedge \cdots \wedge (x_n = y_n)] \to (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)) \\ \text{(EQ3)} & [(x_1 = y_1) \wedge (x_2 = y_2) \wedge \cdots \wedge (x_n = y_n)] \to (P(x_1, \ldots, x_n) = P(y_1, \ldots, y_n)) \end{array}$$

Semantically (in the sense of Definition 45), the logical symbol $=$ is interpreted by the equality relation in any structure $\mathcal{D}$, i.e., for any terms t_1, t_2,

$$\mathcal{D}(t_1 = t_2) = \mathbf{1} \quad \text{iff} \quad \mathcal{D}(t_1) = \mathcal{D}(t_2).$$

Provability in predicate logic. The notions of proof and provability of predicate formulas, as well as those of proof and provability of formulas in a theory, are defined in the same way as in propositional logic, except that we have more axioms and derivation rules at disposal.

The equivalence theorem also transmits to predicate logic without any change. However, the Deduction Theorem does not apply to arbitrary formulas, but only to closed ones.

Theorem 9 (Deduction) *Let T be a theory, A be a closed formula, and B be an arbitrary formula. Then:*

$$T \vdash A \to B \quad \textit{iff} \quad T \cup \{A\} \vdash B.$$

Example 38 Find a proof of $(\forall x)(\neg A \to B)$ from the theory $\{A\}$.

Solution:

$$\begin{array}{ll}
\vdash A \to (\neg B \to A), & \text{(CL1)} \\
\{A\} \vdash \neg B \to A, & \text{(MP)} \\
\vdash (\neg B \to A) \to (\neg A \to \neg\neg B), & \text{(CL2)} \\
\{A\} \vdash \neg A \to \neg\neg B, & \text{(MP)} \\
\{A\} \vdash \neg A \to B, & \text{(E)} \\
\{A\} \vdash (\forall x)(\neg A \to B). & \text{(GR)}
\end{array}$$

If A is a closed formula, then we can additionally prove $\vdash A \to (\forall x)(\neg A \to B)$ by (D); however, we cannot apply (D) if A is not closed.

Prenex forms of formulas. Some automated theorem proving procedures require that the input be a formula written as a string of quantifiers and bound variables, called the *prefix*, followed by a quantifier-free part, called the *matrix*.

Definition 49 A formula A is in a *prenex form* if it has the following form:

$$(Q_1 x_1)(Q_2 x_2) \ldots (Q_n x_n) B,$$

where:

(i) Each Q_i is one of the quantifiers $\forall, \exists$;

(ii) $x_1, x_2, \ldots, x_n$ are different variables;

(iii) B is an open formula.

The formula B is called the *matrix* and $(Q_1 x_1) \ldots (Q_n x_n)$ the *prefix* of A.

Theorem 10 (Prenex form) *For each formula A, there exists a formula B in a prenex form such that $\vdash A \leftrightarrow B$.*

When constructing an equivalent formula in a prenex form, we proceed by induction on the given formula's complexity, using *prenex operations.* Their task is to extract the quantifiers from the inside of the formula out.

Proposition 27 (Prenex operations)

(a) *Let $Q \in \{\exists, \forall\}$, $(Qx)B$ be a subformula of a formula A, and y not be free in B. Moreover, let A' be formed from A by replacing $(Qx)B$ with $(Qy)B(x/y)$. Then $\vdash A \leftrightarrow A'$, and A' is called a* variant *of A.*

Let $Q \in \{\exists, \forall\}$ be a quantifier, and let Q' denote its dual. Then, for arbitrary formulas A, B and a variable x not free in A, the following is valid:

$$\begin{array}{ll} \text{(b)} & \vdash \neg(Qx)B \leftrightarrow (Q'x)\neg B \\ \text{(c)} & \vdash (A \to (Qx)B) \leftrightarrow (Qx)(A \to B) \\ \text{(d)} & \vdash ((Qx)B \to A) \leftrightarrow (Q'x)(B \to A) \\ \text{(e)} & \vdash (A \wedge (Qx)B) \leftrightarrow (Qx)(A \wedge B) \\ \text{(f)} & \vdash (A \vee (Qx)B) \leftrightarrow (Qx)(A \vee B) \end{array}$$

We will refer to an application of prenex operations from Proposition 27 by using the abbreviations PO (a)–(f).

Example 39 Find prenex forms of the expressions:

$$\begin{array}{ll} \text{(a)} & (\exists y)(f(y) = x) \to (f(f(x)) = x) \\ \text{(b)} & (\exists x)(f(f(x)) = x) \to (\exists x)(f(x) = x) \end{array}$$

Solution to (a): We simply apply PO (d):

$$\vdash [(\exists y)(f(y) = x) \to (f(f(x)) = x)] \leftrightarrow (\forall y)[(f(y) = x) \to (f(f(x)) = x)]$$

Solution to (b): We must first produce a variant of the subformula on either side of the implication; thereby we obtain the following equivalent formula:

$$(\exists y)(f(f(y)) = y) \to (\exists x)(f(x) = x)$$

Now we apply PO (d) as in the previous example:

$$(\forall y)[(f(f(y)) = y) \to (\exists x)(f(x) = x)]$$

Finally, we apply PO (c):

$$(\forall y)(\exists x)[(f(f(y)) = y) \to (f(x) = x)]$$

The last formula is in a prenex form and is equivalent to the original one.

Exercise 33 Formalize and find prenex forms of the following expressions:

(i) "For any number $\varepsilon > 0$, there exists some number $\delta > 0$ such that for all x satisfying the condition $x_0 - \delta < x < x_0 + \delta$, the value of $f(x)$ satisfies $f(x_0) - \varepsilon < f(x) < f(x_0) + \varepsilon$."

(ii) "For every $\varepsilon > 0$ there exists $\delta > 0$ such that for all x, if $|x - x_0| < \delta$, then $|f(x) - f(x_0)| < \varepsilon$."

(iii) "For every x_0 and $\varepsilon > 0$ there exists $\delta > 0$ such that for all x, if we have $|x - x_0| < \delta$, then $|f(x) - f(x_0)| < \varepsilon$."

(iv) "For every $\varepsilon > 0$ there exists $\delta > 0$ such that for all x, y such that $|x - x_0| < \delta$, we have that $|f(x) - f(x_0)| < \varepsilon$."

(v) Compare the resulting formulas from (i)–(iv).

Completeness. A logic is complete when all its tautologies are theorems and vice-versa. That is, the formulas that are true under every interpretation of the language are syntactically derivable, and every syntactically derivable formula is valid with respect to the semantics. Kurt Gödel gave the proof of the completeness of first-order predicate logic in his doctoral dissertation of 1929; the result is known as Gödel's Completeness Theorem.

Theorem 11 (Completeness) *Let T be a theory and A a formula. Then:*

- $T \vdash A$ *iff* $T \models A$.
- *T is consistent (see Definition 38) iff it has a model.*

6 Axiomatic Set Theory

In this chapter, we return to set theory and introduce its modern conception as an axiomatic theory in first-order predicate logic.

The Formal Language of Set Theory

Set-theoretic notions from the perspective of formal logic. In the language of predicate logic (see Definitions 39–41), the set-theoretic notions introduced in Chapters 1–3 can be construed as follows:

- The symbol $\in$ denotes a relation between two objects. Therefore, it is a *binary predicate* (called the *membership predicate*).

- The expression $x \in A$ applies the predicate to two variables, and so it is an *atomic formula* of predicate logic. (We infix the membership predicate, i.e., write it between its arguments, in the same way as the equality predicate $=$.)

- Expressions representing set-theoretic statements by means of logical symbols (Notation 2, p. 5), such as $(\exists A)(\forall x)\neg(x \in A)$, are *formulas* of predicate logic.

Recall a few abbreviations (see p. 7 and Notation 3): the expression $x \notin A$ abbreviates the formula $\neg(x \in A)$; the expression $(\forall x \in A)\varphi$ is short for $(\forall x)(x \in A \to \varphi)$; and $(\exists x \in A)\varphi$ is short for $(\exists x)(x \in A \wedge \varphi)$.

- The signs $\subseteq, \approx, \preceq$ are *binary predicate symbols;* the signs $\cup, \cap, \setminus, \times$ are *binary function symbols* and $\mathscr{P}, \bigcup, \bigcap$ *unary function symbols;* and $\emptyset$ is an *object constant.* The binary predicates and function symbols are usually written infix (i.e., between the arguments), similarly to $\in$ and $=$.

- Variables for elements or sets $(x, A, \mathcal{A}, \dots)$, object constants $(\emptyset, 5, \mathbb{N}, \dots)$, and function symbol applications (e.g., $A \cap B$, $\mathscr{P}(A \times B)$, $\bigcup \mathcal{A}, \dots$) are *terms,* i.e., expressions denoting objects of set theory.

- The notation $\langle x, y\rangle$ for ordered pairs can be regarded as a term, too: in this case, the function symbol is marked simply by the angle brackets $\langle \dots \rangle$, and its arguments are written inside. Similarly, the expression $\{x \mid \varphi(x_1, \dots, x_n)\}$ for any formula φ (see Notation 3 on p. 8) can be regarded as an n-ary term.

The language of set theory. Note that formulas containing symbols for defined set-theoretic notions can generally be reduced, by expanding the definitions, to formulas that, apart from logical symbols, only contain the predicates of membership and equality. For example:

- $A \subseteq B$ can be expanded into $(\forall x)(x \in A \to x \in B)$, cf. Definition 3;

- $X \in \bigcup \mathcal{A}$ can be expanded as $(\exists A)(A \in \mathcal{A} \wedge X \in A)$, cf. Definition 11; etc. (However, expanding the symbol for ordered pairs requires a trick which will be hinted at on p. 63.)

Set theory can thus be regarded as a formal theory over predicate logic with equality (see Remark 6 on p. 53) in the language containing the membership predicate $\in$ as the only special symbol. The rules of propositional and predicate logic (including, e.g., those of Propositions 23 and 27) can then be used to derive the properties of set-theoretic notions from their definitions. Examples of such proofs will be given below and as exercises.

Set-theoretic principles as axioms. In set theory, we assume the validity of the adopted set-theoretic principles, such as Extensionality, Foundation, and Choice. Consequently, the formulas expressing these principles can be employed in formal set-theoretic proofs as additional assumptions (i.e., *axioms* in the sense of Definition 29). An example of such use is the application of Extensionality in the proof of the following proposition.

Proposition 28

1. *To prove the set equality $A = B$, it suffices to prove the formula $x \in A \leftrightarrow x \in B$.*
2. *To prove the inclusion $A \subseteq B$, it is sufficient to prove the formula $x \in A \rightarrow x \in B$.*

Proof Assume we have a proof of the formula $x \in A \leftrightarrow x \in B$. By the Rule of Generalization (Definition 48), we can further derive $(\forall x)(x \in A \leftrightarrow x \in B)$. Applying the Rule of Modus Ponens (p. 46) to the latter formula and the formula expressesing the Principle of Extensionality, i.e., formula (1) on p. 8, we arrive at $A = B$.

To prove the second claim, we proceed analogously, using the right-to-left direction of formula (2) from the definition of inclusion (p. 11) in place of (1). □

Properties of elementary set operations. Elementary set operations $\cup, \cap, \setminus$ inherit the properties of the propositional connectives by which they are defined (see Definition 2, p. 8). Valid propositional equivalences or implications straightforwardly entail the corresponding set equalities and inclusions, as illustrated by the following examples.

Example 40 $(A \cap B) \cup (A \setminus B) = A$, as propositionally we have (verify!): $(p \wedge q) \vee (p \wedge \neg q) \equiv p$.

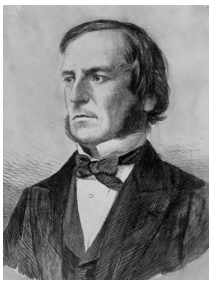
Proof Let us expand the left-hand side of the set equality by Definition 2 and apply the aforementioned propositional equivalence:

$$x \in (A \cap B) \cup (A \setminus B) \quad \text{iff} \quad (\underbrace{x \in A}_{p} \wedge \underbrace{x \in B}_{q}) \vee (\underbrace{x \in A}_{p} \wedge \underbrace{x \notin B}_{\neg q}) \quad \text{iff} \quad \underbrace{x \in A}_{p}.$$

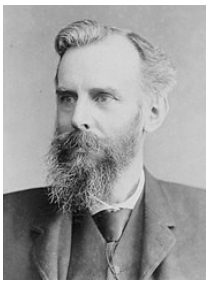
Thus, by Proposition 28, we obtain that $(A \cap B) \cup (A \setminus B) = A$. □

Exercise 34 Verify the propositional validity of $p \wedge \neg q \models p$ and use it to derive the set-theoretic law $A \setminus B \subseteq A$.

In this way, simple inclusions and identities between elementary set operations reduce to the propositional calculus. As a consequence, both elementary set operations $(\cup, \cap, \setminus)$ and propositional connectives $(\vee, \wedge, \neg)$ instantiate the same kind of algebraic structure—namely, that of a *Boolean algebra*. Valid inclusions and identities of elementary set theory can, therefore, be verified in the same way as in propositional logic—e.g., by using the *table method* (see p. 41) or *Venn diagrams* (known from high-school mathematics or easily found online). Observe that the areas in a Venn diagram correspond to the rows in a truth table for the propositions $p =$ "$x \in A$", $q =$ "$x \in B$", $r =$ "$x \in C$", $s =$ "$x \in D$".



George Boole



John Venn

Examples of formal proofs. Venn diagrams are sufficient only for proving simple identities and inclusions of elementary set theory. More complex set-theoretic propositions can be proved either by using informal considerations (as in Chapters 1–3) or by applying the formal laws of predicate logic.

In practice, we usually conduct formal proofs by chaining logically valid implications or equivalences, rather than directly using the axioms and rules of predicate logic. In such proofs, we make frequent tacit use of the Deduction and Equivalence Theorems for predicate logic (see Theorems 7 and 9) and apply the derived laws of propositional and predicate logic, such as De Morgan's laws, prenexation, the distributivity of connectives, etc. (Propositions 23 and 27). Let us present two examples of formal proofs in set theory:

Proposition 29 $A \cap \bigcup \mathscr{B} = \bigcup \{A \cap B \mid B \in \mathscr{B}\}$.

Proof By Proposition 28, it suffices to prove the following formula:

$$x \in A \cap \bigcup \mathscr{B} \leftrightarrow x \in \bigcup \{A \cap B \mid B \in \mathscr{B}\}.$$

We expand the definitions and apply the laws of predicate logic:

$$\begin{aligned} x \in A \cap \bigcup \mathscr{B} &\leftrightarrow x \in A \wedge x \in \bigcup \mathscr{B} \\ &\leftrightarrow x \in A \wedge (\exists B)(B \in \mathscr{B} \wedge x \in B) \\ &\leftrightarrow (\exists B)(x \in A \wedge B \in \mathscr{B} \wedge x \in B) \\ &\leftrightarrow (\exists B)(B \in \mathscr{B} \wedge x \in A \wedge x \in B) \\ &\leftrightarrow (\exists B)(B \in \mathscr{B} \wedge x \in A \cap B) \\ &\leftrightarrow x \in \bigcup \{A \cap B \mid B \in \mathscr{B}\} \end{aligned}$$

The equivalences follow from Definitions 2 and 11, prenexation (Proposition 27), and the commutativity and associativity of conjunction (Proposition 23).

(In this kind proofs, it is usually expedient to proceed 'from both ends inwards', trying to transform the expanded formulas into mutually equivalent forms.) □

Proposition 30 $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Proof Justify the following steps, citing the set-theoretic definitions and valid equivalences of propositional logic:

$$\begin{aligned}\langle x,y\rangle \in A \times (B \cup C) &\leftrightarrow x \in A \wedge y \in B \cup C\\ &\leftrightarrow x \in A \wedge (y \in B \vee q \in C)\\ &\leftrightarrow (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C)\\ &\leftrightarrow \langle x,y\rangle \in A \times B \vee \langle x,y\rangle \in A \times C\\ &\leftrightarrow \langle x,y\rangle \in (A \times B) \cup (A \times C).\end{aligned}$$ □

Exercise 35 Prove formally:

(a) $A \smallsetminus \bigcap \mathscr{B} = \bigcup \{A \smallsetminus B \mid B \in \mathscr{B}\}$

(b) $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$

Axiomatization of Set Theory

Naïve comprehension. An apparently desirable set-theoretic principle would be the possibility to define a set by any common property of elements—i.e., the so-called Principle of Unrestricted Comprehension:

Unrestricted Comprehension Principle: *Every property $\varphi(x)$ delimits the set $\{x \mid \varphi(x)\}$ of all elements that satisfy the property.*

Unfortunately, it turns out that adopting the Unrestricted Comprehension Principle would make set theory inconsistent:

Proposition 31 *The Principle of Unrestricted Comprehension leads to a contradiction.*

Proof As has already been shown in Corollary 9 (p. 25), the property of *being a set* does not delimit a set.

An even simpler proof (which avoids the need to prove Cantor's Theorem) is based on the so-called *Russell's Paradox,* i.e., on the observation that the property of *not being its own element* cannot delimit a set; in other words, that the class $\mathcal{R} = \{X \mid X \notin X\}$ is proper. The reason is that its definition immediately entails that $\mathcal{R} \in \mathcal{R} \leftrightarrow \mathcal{R} \notin \mathcal{R}$, which is a contradiction. □

The problem of distinguishing sets from proper classes. Cantor's and Russell's Paradoxes demonstrate that even some simple properties like $X = X$ or $X \notin X$ delimit proper classes rather than sets. How, then, can we find out if a given condition φ delimits a set rather than a proper class? It would be rather inconvenient to always take a given collection for a set and expect that contradictions may arise later.

A solution: cautious comprehension. It has been noted that certain set-theoretic constructions (including the operations of union, powerset, and replacement of elements) and existential principles (e.g., the Principle of Infinity) have never given rise to contradictions. The assumption that these constructions produce sets can, therefore, be adopted as a set-theoretic principle (of *'cautious' comprehension*).

Cautious Comprehension Principles:

1. $\mathbb{N}$ *is a set.*
2. *If A is a set, then its powerset $\mathscr{P}(A)$ is a set.*

3. *If $\mathcal{A}$ is a set of sets, then its union $\bigcup \mathcal{A}$ is a set.*

4. *If A is a set and $\varphi(x, y)$ is a formula determining a function, i.e., for each x there is at most one y such that $\varphi(x, y)$, then $\{y \mid (\exists x \in A)\varphi(x, y)\}$ is a set.*

Corollary 15 Some consequences of the Cautious Comprehension Principles (the proofs are left for Exercise 36):

1. If A is a set and $\varphi(x)$ a formula, then $\{x \in A \mid \varphi(x)\}$ is a set.
2. A finite number of arbitrary elements $x_1, \ldots, x_n$ form a set $\{x_1, \ldots, x_n\}$.
3. If A and B are sets, then $A \cup B$, $A \cap B$, $A \setminus B$, and $A \times B$ are sets.
4. If $\mathcal{A} \neq \emptyset$, then $\bigcap \mathcal{A}$ is a set.
5. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{R}^n, \mathscr{P}(\mathbb{R})$, etc., are sets.

It turns out that the Cautious Comprehension Principles are sufficient for most set-theoretic constructions. Together with set-theoretic principles introduced earlier (in particular, the principles of Extensionality, Foundation, and Choice), they can thus form an axiomatic foundation for set theory.

Definition 50 *Zermelo–Fraenkel set theory with the Axiom of Choice* (denoted by *ZFC*) is an axiomatic theory over classical first-order logic with equality. The language of ZFC comprises a single special symbol—namely, the binary predicate $\in$. The axioms of ZFC are as follows:

1. *Axiom of Extensionality:*

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

Notation: $x \subseteq y \equiv (\forall q)(q \in x \rightarrow q \in y)$.

2. *Axiom of Empty Set:*

$$(\exists z)(\forall q)(q \notin z)$$

Notation: $z = \emptyset$.

3. *Axiom of Pairing:*

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

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

4. *Axiom of Union:*

$$(\forall x)(\exists z)\big(q \in z \leftrightarrow (\exists u \in x)(q \in u)\big)$$

Notation: $z = \bigcup x$, $u \cup v = \bigcup \{u, v\}$.

5. *Axiom of Power Set:*

$$(\forall x)(\exists z)(\forall q)(q \in z \leftrightarrow q \subseteq x)$$

Notation: $z = \mathscr{P}(x)$.

6. *Axiom of Infinity:*

$$(\exists z)\big(\emptyset \in z \wedge (\forall q \in z)(q \cup \{q\} \in z)\big)$$

7. *Axioms of Separation:*

$$(\forall x)(\exists z)(\forall q)\big(q \in z \leftrightarrow q \in x \wedge \varphi(q)\big)$$

Notation: $z = \{q \in x \mid \varphi(q)\}$, $x \cap y = \{q \in x \mid q \in y\}$.

8. *Axioms of Replacement:*

$$(\forall u)(\forall v)(\forall w)\big(\psi(u,v) \wedge \psi(u,w) \to v = w\big) \to (\forall x)(\exists z)(\forall v)\big(v \in z \leftrightarrow (\exists u \in x)\psi(u,v)\big).$$

9. *Axiom of Foundation:*

$$(\forall x \neq \emptyset)(\exists u \in x)(u \cap x = \emptyset)$$

10. *Axiom of Choice:*

$$(\forall x)\big(\emptyset \notin x \wedge (\forall u \in x)(\forall v \in x)(u \neq v \to u \cap v = \emptyset) \to (\exists z)(\forall u \in x)(\exists q)(u \cap z = \{q\})\big)$$

Remarks on Definition 50.

- The axioms of ZFC formalize the set-theoretic principles introduced in previous chapters: Axiom 1 represents the Principle of Extensionality (p. 8); Axiom 6 is equivalent to the Principle of Infinity (p. 23); Axiom 9 is an equivalent form of the Principle of Foundation (p. 25); Axiom 10 represents the Principle of Choice (p. 24); and Axioms 2–8 formalize the Cautious Comprehension Principles and some of their consequences (p. 60 and Corollary 15).

- Axioms 7 a 8 are in fact *axiom schemata:* for every formula φ or ψ in the language of set theory, the schema produces an axiom. (Thus, ZFC has *infinitely many* axioms.)

- The axioms listed in Definition 50 are not independent of each other: Axiom 2 follows from Axiom 6; Axiom 3 follows from Axioms 2, 5 and 8; and Axioms 7 follow from Axioms 8. Thus, Axioms 1, 4–6, and 8–10 are sufficent for the axiomatization of ZFC. The redundant Axioms 2–3 and 7 are usually added because they allow us to introduce symbols (such as $\emptyset$, $\cup$, etc.) that make the formulation of the remaining axioms easier.

- Various alterations of ZFC are studied as well—e.g., ZFC with the Continuum Hypothesis (ZFC+CH, cf. p. 22), ZFC without the Axiom of Choice (ZF), etc. There are also entirely different axiomatic systems for set theory. Nevertheless, ZFC is currently the most commonly used axiomatization of set theory.

- ZFC knows only one kind of objects, namely sets. Mathematical objects of all other kinds (such as ordered pairs, numbers, etc.) are, in ZFC, modeled by suitable sets.

Exercise 36 Derive informally some claims (of your choice) of Corollary 15, using the Cautions Comprehension Principles introduced on p. 60.

Representation of Mathematical Objects in ZFC

Since the only objects of the theory ZFC are sets, all other mathematical objects we may need in ZFC have to be represented by suitable sets. In this concluding section we show how several kinds of mathematical objects can be modeled by sets.

Ordered pairs. Ordered pairs can be modeled as sets using the *Kuratowski definition:*

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}. \tag{19}$$

By Exercise 37 below, ordered pairs defined by (19) satisfy the characteristic property of ordered pairs, namely:

$$\langle a, b\rangle = \langle c, d\rangle \leftrightarrow a = c \wedge b = d.$$

Exercise 37 Prove that $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$ if and only if $a = c$ and $b = d$. (Hint: for the left-to-right direction, employ Extensionality.)

Natural numbers. The *von Neumann representation* identifies each natural number with the set of its predecessors, i.e.:

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

etc.; in general, $n + 1 = n \cup \{n\}$.

Exercise 38 Demonstrate that each von Neumann natural number is a *transitive set,* i.e., that each of its element is also its subset. (The proof is allowed to be informal—e.g., by mathematical induction rather than strictly by the axioms of ZFC.)



Kazimierz Kuratowski



John von Neumann

Number systems. In ZFC, the set $\mathbb{N}$ of natural numbers is defined as the smallest *inductive set,* i.e., the smallest set (of sets) such that it contains $\emptyset$ as an element and with each of its elements q it also contains $q \cup \{q\}$ as an element. The Axiom of Infinity from Definition 50 ensures the existence of at least one inductive set z; it can be shown that the smallest (w.r.t. inclusion) inductive set $\mathbb{N}$ is the intersection of all inductive subsets of z.

Integers can be defined as the ordered pairs $\langle s, n\rangle$ for $s \in \{0, 1\}$ and $n \in \mathbb{N}$; *rationals* as pairs of co-prime integers; *reals* as decimal representations, i.e., sets of ordered pairs $\langle i, d_i\rangle$, where $i \in \mathbb{N}$ and $d_i \in \mathbb{Z}$; and *complex* numbers as ordered pairs of reals. Sets representing $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ in ZFC can thus be obtained by suitable Axioms of Separation (Definition 50, Ax. 7) from the sets $\mathbb{N}^2$, $\mathscr{P}(\mathbb{N}^2)$, and $(\mathscr{P}(\mathbb{N}^2))^2$.

Ordinal numbers. In ZFC, ordinal numbers $\alpha \in \mathrm{Ord}$ are identified with the sets $[0, \alpha)$ of their predecessors. Thus, finite ordinals are identified with natural numbers, $\omega = \mathbb{N}$, $\omega + 1 = \omega \cup \{\omega\}$, etc.; in general, $\alpha + 1 = \alpha \cup \{\alpha\}$, and limit $\lambda = \bigcup_{\alpha<\lambda} \alpha$.

A common property delimiting the class of all ordinal numbers in ZFC is given, e.g., by the following (somewhat artificial) condition: ordinal numbers are transitive sets (see Exercise 38) well-ordered by the relation $\in$.

Cardinal numbers. In ZFC, *cardinal numbers* can be identified with initial ordinals (see p. 32), i.e., with such ordinals α that the ordinal interval $[0, \alpha)$ cannot be bijectively mapped onto any ordinal interval $[0, \beta)$ where $\beta < \alpha$. Thus, finite cardinals are identified with finite ordinals (i.e., natural numbers); $\aleph_0 = \omega$; $\aleph_1 = \omega_1$ (see Notation 6, p. 30), etc.; in general, $\aleph_\alpha = \omega_\alpha$.

The foundations of mathematics. It turns out that in a similar manner, virtually all mathematical concepts can be represented by sets and their usual properties be proved in ZFC by means of classical first-order logic. The set theory ZFC can thus serve as a foundational theory within which (almost) all contemporary mathematics can be developed purely by logical deduction. For this reason, logic and set theory are jointly regarded as the *foundations of mathematics*.

7 Recommended Literature

Logic (English):

[1] Elliott Mendelson: *Introduction to Mathematical Logic,* 4th edition. Chapman & Hall, 1997.

[2] Lou van den Dries: *Mathematical Logic Lecture Notes.* University of Illinois, 2019.

[3] Vilém Novák, Irina Perfilieva, & Jiří Mockoř: *Mathematical Principles of Fuzzy Logic* (Chapters 2–3). Springer, 1999.

Logic (Czech):

[4] Marie Duží: *Logika v praxi.* VŠB Technická univerzita Ostrava. (Online: `http://www.cs.vsb.cz/duzi/Logika_Praxe.pdf`)

[5] Jiří Raclavský: *Úvod do logiky: klasická výroková logika.* Masarykova univerzita Brno, 2015. (Online: `https://munispace.muni.cz/library/catalog/book/762`)

[6] Jiří Raclavský: *Úvod do logiky: klasická predikátová logika.* Masarykova univerzita Brno, 2015. (Online: `https://munispace.muni.cz/library/catalog/book/764`)

[7] Vítězslav Švejdar: *Logika: neúplnost, složitost a nutnost.* Academia, Praha, 2002.

Set theory (English):

[8] Herbert B. Enderton: *Elements of Set Theory.* Academic Press, 1977.

[9] Derek Goldrei: *Classic Set Theory: For Guided Independent Study.* Routledge, 1996.

[10] Karel Hrbacek & Thomas Jech: *Introduction to Set Theory,* 3rd edition. Marcel Dekker, 1999.

Set theory (Czech):

[11] Bohuslav Balcar & Petr Štěpánek. *Teorie množin.* Academia, Praha, 1986.

[12] Vladimír Kořínek: *Teorie množin, její vznik a vývoj.* Pokroky matematiky, fyziky a astronomie 10 (3): 131–160 (1965). (Online: `https://dml.cz/dmlcz/138238`)

[13] Bedřich Pospíšil: *Nekonečno v matematice.* Edice Cesta k vědění, sv. 48, Jednota českých matematiků a fyziků, Praha, 1949. (Online: `https://dml.cz/dmlcz/403221`)