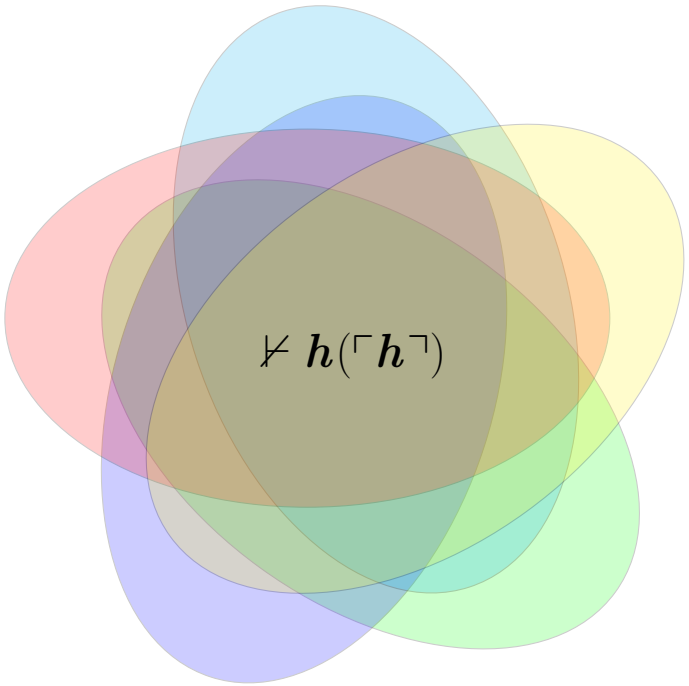
Logic and Set Theory

Benjamin Sambale

Version: April 1, 2026



Contents

Warning: This is an AI-translated version of my German lectures notes, performed by *Gemini 3 Flash Preview*. I have not checked whether Gemini introduced errors. Use with care!

Preface

The second half of these notes (Set Theory) originated within the framework of a seminar in the summer semester 2019 at the Friedrich Schiller University Jena. Only in 2025 did I supplement the first half (Logic) (this was not based on a specific course). It lies in the nature of the subject that one cannot seriously speak about logic without mentioning set-theoretic concepts such as element, set, function, and relation. This chicken-and-egg problem is usually bypassed by using these concepts only on the meta-level, i.e., colloquially. Circular reasoning is excluded, as the deep-seated results of logic are not required for the set-theoretic construction of mathematics. One must nevertheless keep in mind that due to Gödel's incompleteness theorems, large parts of mathematics cannot be founded one hundred percent. In a certain way, it is only a large thought experiment or game.

Even if the axiomatic construction of mathematics should be the foundation of all further theories, the script is not suitable for first-year students, because I assume a certain familiarity with basic concepts and proofs (for example from my script on linear algebra). In fact, the subtleties of logic and set theory are irrelevant for most other fields. Nevertheless, the theory as such is an exciting subject area.

I thank Claude Sonnet (4.6) and Boris Tschochner for pointing out errors.

Literature:

- D. W. Hoffmann, *Limits of Mathematics: A Journey Through the Key Areas of Mathematical Logic*, 3rd edition, Springer Spektrum, Wiesbaden, 2025
- E. Mendelson, *Introduction to mathematical logic*, 6th edition, CRC Press, Boca Raton, 2015
- C. Celluci, *The theory of Gödel*, Springer, Cham, 2022
- T. Jech, *Set Theory*, 3rd edition, Springer, Berlin, 2002

I. Logic

I.1. Calculi

Remark I.1.1. Before one can talk about mathematics at all, one must agree on a language. As for every language, one needs a *syntax* (e.g., Latin alphabet with rules of punctuation) and a context-dependent *semantics* (e.g., pear can stand for a fruit or be an abbreviation for a light bulb). It cannot be avoided that the simplest concepts cannot be further reduced to known things, but must be accepted as given (just as a toddler learns the words "yes" or "one" in their mother tongue). In this section, we present a general syntax of mathematics. Formulations such as "if and only if" and concepts such as "set" or "function" are for now only to be understood colloquially, i.e., on the *meta-level* (precise definitions follow in Definition I.2.3 or section II.1).

Definition I.1.2. A (HILBERT-)*calculus* $\mathcal{K}$ consists of the following things:

- *Alphabet*: Variables such as $a, b, c, \ldots$ and symbols such as $(,), \neg, =, \ldots$.
- *Formulas*: Sequences of finitely many characters of the alphabet according to certain rules (e. g. opened brackets must be closed).
- *Axioms*: Selected formulas.
- *Inference rules*, which describe how one can derive new formulas from known formulas.
- *Proofs*: Sequences of finitely many formulas $f_1, \ldots, f_n$, such that each f_i is an axiom or can be derived from f_j with $j < i$ by inference rules.

A formula f is called a *theorem* or *provable*, if it appears at the end of a proof. We write $\vdash f$ if necessary. If no proof for f exists, we write $\nvdash f$.

Remark I.1.3.

(i) Since proofs are finite and one can construct new variables (actually formulas) by concatenating variables (e. g. $a_1 = a$, $a_2 = aa$ etc.), a finite alphabet is sufficient. The number of formulas (and axioms, inference rules) will, however, usually be infinite.

(ii) We will always write (formal) proofs such that each line begins with $\vdash$ and contains exactly one formula. With increasing practice, we will later combine several proof steps in one line.

(iii) We denote inference rules in the form $\frac{f_1,\ldots,f_n}{g}$ (the formula g is derived from the formulas $f_1, \ldots, f_n$).

(iv) We will see that in practice it is not always possible to decide whether $\vdash f$ or $\nvdash f$ holds (see section I.8).

Example I.1.4. Let the calculus $\mathcal{K}$ be given by:

- Alphabet: Variables a, b (no symbols)

- Formulas: All words consisting of a and b including the empty word with 0 letters.
- Axioms: a
- Inference rules: $\frac{f_1 a f_2}{f_1 a b f_2}$, $\frac{f_1 b f_2}{f_1 a a f_2}$, $\frac{f_1 f_2 f_3 f_2 f_4}{f_1 f_3 f_4}$ for arbitrary formulas $f_1, \ldots, f_4$.

It holds that

$$\vdash a$$
$$\vdash ab$$
$$\vdash abb$$
$$\vdash abaa$$
$$\vdash ba$$

Since the last inference rule shortens the length of a formula, it is non-trivial to enumerate all theorems of $\mathcal{K}$. Since in every theorem the number of a's must be odd, $\nvdash aa$ holds. (Exercise I.2)

Remark I.1.5. It is desirable to prove as many theorems as possible with as few axioms and inference rules as possible. The following calculus is the foundation of almost all (two-valued) logics.

Definition I.1.6 (Łukasiewicz)**.** The calculus $\mathcal{A}$ of *propositional logic* consists of:

- The variables are called *elementary propositions* and are denoted by capital letters $A, B, \ldots$. The symbols are (,), $\neg$, $\Rightarrow$.
- The formulas are called *propositions* and are defined recursively: All elementary propositions are propositions. If f and g are propositions, then so are $(\neg f)$ and $(f \Rightarrow g)$.
- For all propositions f, g, h there are the following axioms:

$$(f \Rightarrow (g \Rightarrow f)) \tag{$\mathcal{A}_1$}$$
$$(((\neg f) \Rightarrow (\neg g)) \Rightarrow (g \Rightarrow f)) \tag{$\mathcal{A}_2$}$$
$$((f \Rightarrow (g \Rightarrow h)) \Rightarrow ((f \Rightarrow g) \Rightarrow (f \Rightarrow h))) \tag{$\mathcal{A}_3$}$$

- For propositions f and g, the *modus ponens*

$$\frac{f, (f \Rightarrow g)}{g} \tag{MP}$$

  is the only inference rule.

Remark I.1.7.

(i) The use of parentheses in the recursive definition of formulas guarantees the unique construction of a formula. To increase readability, we will nevertheless omit parentheses and agree that $\neg$ binds more strongly than $\Rightarrow$. The outermost pair of parentheses can generally be removed. Thus, $((\neg f) \Rightarrow g)$ simplifies to $\neg f \Rightarrow g$.

(ii) One can manage entirely without parentheses by using the so-called *Polish notation*, in which symbols are not placed between variables but to the left of them: $(\neg f \Rightarrow g) \Rightarrow \neg h$ becomes $\Rightarrow\Rightarrow \neg f g \neg h$.

(iii) Note that $\mathcal{A}$ possesses infinitely many axioms and inference rules. Strictly speaking, these are three *axiom schemata*. Various versions can be found in the literature, but they all lead to the same theorems. None of the three axiom schemata is dispensable (Exercise I.6). In fact, one can manage with only a single (significantly more complicated) axiom schema by MEREDITH:

$$((((a \Rightarrow b) \Rightarrow (\neg c \Rightarrow \neg d)) \Rightarrow c) \Rightarrow e) \Rightarrow ((e \Rightarrow a) \Rightarrow (d \Rightarrow a)).$$

(iv) To simplify proofs, we derive further inference rules. For statements f and g, one obtains from $(\mathcal{A}_1)$ and (MP) the inference rule

$$\frac{f}{g \Rightarrow f}. \tag{MP'}$$

(v) If one has found proofs for $f \Rightarrow g$ and $g \Rightarrow h$, then one obtains a proof for $f \Rightarrow h$:

$$\begin{aligned}
&\vdash f \Rightarrow g \\
&\vdash g \Rightarrow h \\
&\vdash f \Rightarrow (g \Rightarrow h) && \text{(MP')} \\
&\vdash (f \Rightarrow (g \Rightarrow h)) \Rightarrow ((f \Rightarrow g) \Rightarrow (f \Rightarrow h)) && (\mathcal{A}_3) \\
&\vdash (f \Rightarrow g) \Rightarrow (f \Rightarrow h) && \text{(MP)} \\
&\vdash f \Rightarrow h && \text{(MP)}
\end{aligned}$$

We can therefore use the inference rule *Modus barbara*

$$\frac{f \Rightarrow g,\ g \Rightarrow h}{f \Rightarrow h} \tag{MB}$$

.

Example I.1.8. For every statement f in $\mathcal{A}$, it holds that

$$\begin{aligned}
&\vdash f \Rightarrow ((f \Rightarrow f) \Rightarrow f) && (\mathcal{A}_1) \\
&\vdash (f \Rightarrow ((f \Rightarrow f) \Rightarrow f)) \Rightarrow ((f \Rightarrow (f \Rightarrow f)) \Rightarrow (f \Rightarrow f)) && (\mathcal{A}_3) \\
&\vdash (f \Rightarrow (f \Rightarrow f)) \Rightarrow (f \Rightarrow f) && \text{(MP)} \\
&\vdash f \Rightarrow (f \Rightarrow f) && (\mathcal{A}_1) \\
&\vdash f \Rightarrow f && \text{(MP)}
\end{aligned}$$

Definition I.1.9. Let $f_1, \ldots, f_n$ be formulas of a calculus. We say f_n can be proven *under the assumption* of $f_1, \ldots, f_{n-1}$ if a proof for f_n exists in which $f_1, \ldots, f_{n-1}$ may be used as additional axioms. If applicable, we write $f_1, \ldots, f_{n-1} \vdash f_n$. This shortens formal proofs significantly and corresponds to the practical procedure in all parts of mathematics (let $\epsilon > 0 \ldots$).

Lemma I.1.10 (Deduction Lemma)**.** *For propositions $f_1, \ldots, f_{n+1}$ in $\mathcal{A}$, $f_1, \ldots, f_n \vdash f_{n+1}$ holds if and only if $f_1, \ldots, f_{n-1} \vdash f_n \Rightarrow f_{n+1}$. In particular, $f_1 \vdash f_2$ is equivalent to $\vdash f_1 \Rightarrow f_2$.*

Proof. If one has a proof of $f_n \Rightarrow f_{n+1}$ under the assumption of $f_1, \ldots, f_{n-1}$, then one can add f_n as an axiom and derive f_{n+1} with (MP). Conversely, let us assume that

$$\begin{aligned}
&\vdash g_1 \\
&\vdots \\
&\vdash g_m
\end{aligned}$$

is a proof of $f_{n+1} = g_m$ under the assumption of $f_1, \ldots, f_n$. From this, we construct a proof for $f_n \Rightarrow f_{n+1}$ in which f_n no longer occurs as an axiom. Specifically, we replace each g_i in sequence with $f_n \Rightarrow g_i$. There are three cases for this:

(i) If g_i is an axiom or one of $f_1, \ldots, f_{n-1}$, then

$$\begin{aligned} &f_1, \ldots, f_{n-1} \vdash g_i \\ &f_1, \ldots, f_{n-1} \vdash f_n \Rightarrow g_i \end{aligned} \qquad \text{(MP')}$$

(ii) If $g_i = f_n$, then we replace g_i with the proposition $f_n \Rightarrow f_n$, which is provable according to Example I.1.8.

(iii) Now let g_i be derived from g_j and $g_j \Rightarrow g_i$ with $j < i$ by means of (MP). We already know that our new proof contains the lines $\vdash f_n \Rightarrow g_j$ and $\vdash f_n \Rightarrow (g_j \Rightarrow g_i)$. We can therefore argue as follows:

$$\begin{aligned} &f_1, \ldots, f_{n-1} \vdash f_n \Rightarrow g_j \\ &f_1, \ldots, f_{n-1} \vdash f_n \Rightarrow (g_j \Rightarrow g_i) \\ &f_1, \ldots, f_{n-1} \vdash (f_n \Rightarrow (g_j \Rightarrow g_i)) \Rightarrow ((f_n \Rightarrow g_j) \Rightarrow (f_n \Rightarrow g_i)) && (\mathcal{A}_3) \\ &f_1, \ldots, f_{n-1} \vdash (f_n \Rightarrow g_j) \Rightarrow (f_n \Rightarrow g_i) && \text{(MP)} \\ &f_1, \ldots, f_{n-1} \vdash f_n \Rightarrow g_i \end{aligned}$$

In the end, one obtains $\vdash f_n \Rightarrow g_m$, i. e., $\vdash f_n \Rightarrow f_{n+1}$ as desired. The second statement is the special case $n = 1$. □[1]

Lemma I.1.11. *For arbitrary propositions f, g and h in $\mathcal{A}$, the following hold:*

(i) $\frac{f \Rightarrow (f \Rightarrow g)}{f \Rightarrow g}$

(ii) $\vdash \neg\neg f \Rightarrow f$.

(iii) $\vdash f \Rightarrow \neg\neg f$.

(iv) $\vdash (f \Rightarrow g) \Rightarrow (\neg g \Rightarrow \neg f)$.

(v) $\neg f \Rightarrow (f \Rightarrow g)$.

(vi) $\vdash f \Rightarrow ((f \Rightarrow g) \Rightarrow g)$.

(vii) $\vdash (f \Rightarrow g) \Rightarrow ((g \Rightarrow h) \Rightarrow (f \Rightarrow h))$.

(viii) $\vdash f \Rightarrow (\neg g \Rightarrow \neg(f \Rightarrow g))$.

(ix) $\vdash \neg(f \Rightarrow g) \Rightarrow f$.

(x) $\vdash (f \Rightarrow \neg f) \Rightarrow \neg f$.

(xi) $\vdash (\neg f \Rightarrow f) \Rightarrow f$.

(xii) $(f \Rightarrow g) \Rightarrow ((\neg f \Rightarrow g) \Rightarrow g)$.

[1] This symbol marks the end of a proof (on the meta-level).

Proof.

(i)

$$\begin{aligned}
&\vdash f \Rightarrow (f \Rightarrow g) \\
&\vdash (f \Rightarrow (f \Rightarrow g)) \Rightarrow ((f \Rightarrow f) \Rightarrow (f \Rightarrow g)) && (\mathcal{A}_3) \\
&\vdash (f \Rightarrow f) \Rightarrow (f \Rightarrow g) && (\text{MP}) \\
&\vdash f \Rightarrow f && (\text{I.1.8}) \\
&\vdash f \Rightarrow g && (\text{MP})
\end{aligned}$$

(ii)

$$\begin{aligned}
&\vdash \neg\neg f \Rightarrow (\neg\neg\neg\neg f \Rightarrow \neg\neg f) && (\mathcal{A}_1) \\
&\vdash (\neg\neg\neg\neg f \Rightarrow \neg\neg f) \Rightarrow (\neg f \Rightarrow \neg\neg\neg f) && (\mathcal{A}_2) \\
&\vdash \neg\neg f \Rightarrow (\neg f \Rightarrow \neg\neg\neg f) && (\text{MB}) \\
&\vdash (\neg f \Rightarrow \neg\neg\neg f) \Rightarrow (\neg\neg f \Rightarrow f) && (\mathcal{A}_2) \\
&\vdash \neg\neg f \Rightarrow (\neg\neg f \Rightarrow f) && (\text{MB}) \\
&\vdash \neg\neg f \Rightarrow f && (\text{i})
\end{aligned}$$

(iii)

$$\begin{aligned}
&\vdash \neg\neg\neg f \Rightarrow \neg f && (\text{ii}) \\
&\vdash (\neg\neg\neg f \Rightarrow \neg f) \Rightarrow (f \Rightarrow \neg\neg f) && (\mathcal{A}_2) \\
&\vdash f \Rightarrow \neg\neg f && (\text{MP})
\end{aligned}$$

(iv)

$$\begin{aligned}
&\vdash \neg\neg f \Rightarrow f && (\text{ii}) \\
f \Rightarrow g &\vdash f \Rightarrow g \\
f \Rightarrow g &\vdash \neg\neg f \Rightarrow g && (\text{MB}) \\
&\vdash g \Rightarrow \neg\neg g && (\text{iii}) \\
f \Rightarrow g &\vdash \neg\neg f \Rightarrow \neg\neg g && (\text{MB}) \\
&\vdash (\neg\neg f \Rightarrow \neg\neg g) \Rightarrow (\neg g \Rightarrow \neg f) && (\mathcal{A}_2) \\
f \Rightarrow g &\vdash \neg g \Rightarrow \neg f && (\text{MP}) \\
&\vdash (f \Rightarrow g) \Rightarrow (\neg g \Rightarrow \neg f) && (\text{Lemma I.1.10})
\end{aligned}$$

(v)

$$\begin{aligned}
&\vdash \neg f \Rightarrow (\neg g \Rightarrow \neg f) && (\mathcal{A}_1) \\
\neg f &\vdash \neg g \Rightarrow \neg f && (\text{Lemma I.1.10}) \\
&\vdash (\neg g \Rightarrow \neg f) \Rightarrow (f \Rightarrow g) && (\mathcal{A}_2) \\
\neg f &\vdash f \Rightarrow g && (\text{MB}) \\
&\vdash \neg f \Rightarrow (f \Rightarrow g) && (\text{Lemma I.1.10})
\end{aligned}$$

(vi)

$$
\begin{aligned}
f, f \Rightarrow g &\vdash f \Rightarrow g \\
f, f \Rightarrow g &\vdash g && \text{(Lemma I.1.10)} \\
f &\vdash (f \Rightarrow g) \Rightarrow g && \text{(Lemma I.1.10)} \\
&\vdash f \Rightarrow ((f \Rightarrow g) \Rightarrow g) && \text{(Lemma I.1.10)}
\end{aligned}
$$

(vii)

$$
\begin{aligned}
f \Rightarrow g, g \Rightarrow h &\vdash f \Rightarrow g \\
f \Rightarrow g, g \Rightarrow h &\vdash g \Rightarrow h \\
f \Rightarrow g, g \Rightarrow h &\vdash f \Rightarrow h && \text{(MB)} \\
f \Rightarrow g &\vdash (g \Rightarrow h) \Rightarrow (f \Rightarrow h) && \text{(Lemma I.1.10)} \\
&\vdash (f \Rightarrow g) \Rightarrow ((g \Rightarrow h) \Rightarrow (f \Rightarrow h)) && \text{(Lemma I.1.10)}
\end{aligned}
$$

(viii)

$$
\begin{aligned}
&\vdash f \Rightarrow ((f \Rightarrow g) \Rightarrow g) && \text{(vi)} \\
f &\vdash (f \Rightarrow g) \Rightarrow g && \text{(Lemma I.1.10)} \\
&\vdash ((f \Rightarrow g) \Rightarrow g) \Rightarrow (\neg g \Rightarrow \neg(f \Rightarrow g)) && \text{(iv)} \\
f &\vdash \neg g \Rightarrow \neg(f \Rightarrow g) && \text{(MP)} \\
&\vdash f \Rightarrow (\neg g \Rightarrow \neg(f \Rightarrow g)) && \text{(Lemma I.1.10)}
\end{aligned}
$$

(ix)

$$
\begin{aligned}
&\vdash \neg f \Rightarrow (f \Rightarrow g) && \text{(v)} \\
&\vdash (\neg f \Rightarrow (f \Rightarrow g)) \Rightarrow (\neg(f \Rightarrow g) \Rightarrow \neg\neg f) && \text{(iv)} \\
&\vdash \neg(f \Rightarrow g) \Rightarrow \neg\neg f && \text{(MP)} \\
&\vdash \neg\neg f \Rightarrow f && \text{(ii)} \\
&\vdash \neg(f \Rightarrow g) \Rightarrow f && \text{(MB)}
\end{aligned}
$$

(x)

$$
\begin{aligned}
&\vdash f \Rightarrow (\neg\neg f \Rightarrow \neg(f \Rightarrow \neg f)) && \text{(viii)} \\
f &\vdash \neg\neg f \Rightarrow \neg(f \Rightarrow \neg f) && \text{(Lemma I.1.10)} \\
&\vdash f \Rightarrow \neg\neg f && \text{(iii)} \\
f &\vdash f \Rightarrow \neg(f \Rightarrow \neg f) && \text{(MB)} \\
f &\vdash \neg(f \Rightarrow \neg f) && \text{(Lemma I.1.10)} \\
&\vdash f \Rightarrow \neg(f \Rightarrow \neg f) && \text{(Lemma I.1.10)} \\
&\vdash (f \Rightarrow \neg(f \Rightarrow \neg f)) \Rightarrow (\neg\neg(f \Rightarrow \neg f) \Rightarrow \neg f) && \text{(iv)} \\
&\vdash \neg\neg(f \Rightarrow \neg f) \Rightarrow \neg f && \text{(MP)} \\
&\vdash (f \Rightarrow \neg f) \Rightarrow \neg\neg(f \Rightarrow \neg f) && \text{(iii)} \\
&\vdash (f \Rightarrow \neg f) \Rightarrow \neg f && \text{(MB)}
\end{aligned}
$$

(xi)

$$\vdash (\neg f \Rightarrow \neg\neg f) \Rightarrow \neg\neg f \qquad \text{(x)}$$
$$\vdash \neg\neg f \Rightarrow f \qquad \text{(ii)}$$
$$\vdash (\neg f \Rightarrow \neg\neg f) \Rightarrow f \qquad \text{(MB)}$$
$$\vdash (\neg f \Rightarrow f) \Rightarrow (\neg f \Rightarrow \neg\neg f) \qquad \text{(iv)}$$
$$\vdash (\neg f \Rightarrow f) \Rightarrow f \qquad \text{(MB)}$$

(xii)

$$\vdash (f \Rightarrow g) \Rightarrow (\neg g \Rightarrow \neg f) \qquad \text{(iv)}$$
$$f \Rightarrow g \vdash \neg g \Rightarrow \neg f \qquad \text{(I.1.10)}$$
$$\vdash (\neg g \Rightarrow \neg f) \Rightarrow ((\neg f \Rightarrow g) \Rightarrow (\neg g \Rightarrow g)) \qquad \text{(vii)}$$
$$f \Rightarrow g \vdash (\neg f \Rightarrow g) \Rightarrow (\neg g \Rightarrow g) \qquad \text{(MP)}$$
$$f \Rightarrow g, \neg f \Rightarrow g \vdash \neg g \Rightarrow g \qquad \text{(Lemma I.1.10)}$$
$$\vdash (\neg g \Rightarrow g) \Rightarrow g \qquad \text{(xi)}$$
$$f \Rightarrow g, \neg f \Rightarrow g \vdash g \qquad \text{(MP)}$$
$$f \Rightarrow g \vdash (\neg f \Rightarrow g) \Rightarrow g \qquad \text{(Lemma I.1.10)}$$
$$\vdash (f \Rightarrow g) \Rightarrow ((\neg f \Rightarrow g) \Rightarrow g) \qquad \text{(Lemma I.1.10)}$$

□

I.2. Interpretations

Remark I.2.1. We now consider the semantics of calculi, i. e. we give formulas a meaning.

Definition I.2.2. An *interpretation* of a calculus $\mathcal{K}$ gives the formulas of $\mathcal{K}$ a meaning (e. g. the variable a could stand for the natural number 5).

Definition I.2.3.

- The *standard interpretation* of propositional logic assigns to all elementary propositions the value *true* (**t**) or *false* (**f**). The symbols (and) are naturally interpreted as parentheses. The symbols $\neg$ and $\Rightarrow$ stand for *not* and *implies*, respectively. Naturally, $\neg\mathbf{t} = \mathbf{f}$ and $\neg\mathbf{f} = \mathbf{t}$. The meaning of $\Rightarrow$ can be specified by a *truth table*:

A	B	$A \Rightarrow B$
t	**t**	**t**
t	**f**	**f**
f	**t**	**t**
f	**f**	**t**

- Instead of "f implies g" we also say: "from f follows g" or "if f holds, then also g". One calls $g \Rightarrow f$ the *converse* of $f \Rightarrow g$.

- A proposition f that is always true for every possible assignment of its variables is called a *tautology*. If applicable, we say f *holds*[2] and write $\vDash f$. Otherwise we write $\nvDash f$. We will show in Theorem I.2.13 that the tautologies are exactly the theorems provable in $\mathcal{A}$.

Remark I.2.4.

(i) The idea of deriving statements through as few axioms as possible goes back to Euclid's Elements. In them, he reduced, for example, the Pythagorean theorem to simple relationships between points and lines. Only much later did Hilbert detach the axioms of Euclidean geometry from their interpretation and thus created the foundation for other geometries.[3]

(ii) To present statements clearly, we introduce the following abbreviations:[4]

$$\begin{aligned} f \wedge g &:= \neg(f \Rightarrow \neg g), \\ f \vee g &:= \neg f \Rightarrow g, \\ f \Leftrightarrow g &:= (f \Rightarrow g) \wedge (g \Rightarrow f). \end{aligned}$$

The interpretation results as follows:

A	B	$A \Rightarrow B$	$A \wedge B$	$A \vee B$	$A \Leftrightarrow B$
t	**t**	**t**	**t**	**t**	**t**
t	**f**	**f**	**f**	**t**	**f**
f	**t**	**t**	**f**	**t**	**f**
f	**f**	**t**	**f**	**f**	**t**

From this, the meaning can be easily read: $\wedge$, $\vee$, $\Leftrightarrow$ stand for *and* (*conjunction*), *or* (*disjunction*) or *equivalent*. Instead of "f is equivalent to g" we also say "f and g are equivalent" or "f holds if and only if g holds". To save parentheses, we agree that $\neg$ binds more strongly than $\wedge$ and $\vee$.

(iii) Alternatively, one can define the calculus with the symbols $\neg$ and $\vee$ (or $\wedge$) and subsequently define $f \Rightarrow g := \neg f \vee g$ (or $f \Rightarrow g := \neg(f \wedge \neg g)$). In fact, one can get by with only one symbol (plus the pair of parentheses):

$$f \circledast g := \neg(f \vee g)$$

(Exercise I.5).

(iv) In contrast to everyday language usage, the mathematical *or* is not synonymous with *either or*. That is, the statement $\mathbf{t} \vee \mathbf{t}$ is true. In computer science, the term XOR is used for *either or*. Note also that $\mathbf{f} \Rightarrow \mathbf{t}$ is a true statement (if the premise is not fulfilled, nothing needs to be checked). Example: If Kurt Gödel is still alive, then Gottlob Frege is the Emperor of China.

(v) It is often falsely assumed that an implication also implies its converse (this phenomenon is called *affirmation of the consequent*). Example: The best table tennis players are Chinese $\not\Rightarrow$ All Chinese are good at table tennis. Instead of the missing causality, however, a *correlation* can exist between these statements (see statistics).

(vi) One can also interpret propositional logic arithmetically by using 1 instead of **t** and 0 instead of **f**. One then obtains $\neg A = 1 - A$, $A \Rightarrow B = \max(1 - A, B)$ (maximum of $1 - A$ and B), $A \wedge B = \min(A, B) = A \cdot B$ (minimum of A and B) and $A \vee B = \max(A, B)$. In this context, one speaks of *Boolean algebra*.

[2] We have already used this way of speaking in the formulation of Lemma I.1.11.
[3] See script for Synthetic Geometry
[4] The symbol := on the meta-level states that the left side is defined by the right side.

(vii) In *many-valued* logic, further values are allowed in addition to **f** and **t**. In *fuzzy logic*, even every real number between 0 and 1 is allowed as a "truth value". This has applications in control engineering and artificial intelligence.

(viii) With the following tautologies, statements can often be simplified.

Theorem I.2.5. *For arbitrary propositions f, g and h, the following hold:*

(i) $\models \neg\neg f \Leftrightarrow f$ (*double negation*).

(ii) $\models f \vee \neg f$ (*law of excluded middle*).

(iii) $\models \neg(f \wedge \neg f)$ (*law of contradiction*).

(iv) $\models (f \wedge f) \Leftrightarrow f$ *and* $\models (f \vee f) \Leftrightarrow f$ (*idempotence*).

(v) $\models (f \Rightarrow g) \Leftrightarrow (\neg g \Rightarrow \neg f)$ (*contraposition*).

(vi) $\models (f \wedge g) \Leftrightarrow (g \wedge f)$, $\models (f \vee g) \Leftrightarrow (g \vee f)$ *and* $\models (f \Leftrightarrow g) \Leftrightarrow (g \Leftrightarrow f)$ (*commutativity*).

(vii) $\models ((f \wedge g) \wedge h) \Leftrightarrow (f \wedge (g \wedge h))$, $\models ((f \vee g) \vee h) \Leftrightarrow (f \vee (g \vee h))$, $\models ((f \Leftrightarrow g) \Leftrightarrow h) \Leftrightarrow (f \Leftrightarrow (g \Leftrightarrow h))$. (*associativity*)

(viii) $\models (f \wedge (g \vee h)) \Leftrightarrow ((f \wedge g) \vee (f \wedge h))$, $\models (f \vee (g \wedge h)) \Leftrightarrow ((f \vee g) \wedge (f \vee h))$. (*distributivity*)

(ix) $\models \neg(f \wedge g) \Leftrightarrow (\neg f \vee \neg g)$ *and* $\models \neg(f \vee g) \Leftrightarrow (\neg f \wedge \neg g)$ (De Morgan*'s laws*).

Proof. All propositions can be easily verified by truth tables. □

Remark I.2.6.

(i) A mapping f that depends on elementary statements $A_1, \ldots, A_n$ and takes the value **t** or **f** is called a *Boolean function*. The values of f can be listed with a truth table, e. g.

A_1	A_2	A_3	f
t	**t**	**t**	**t**
t	**f**	**t**	**f**
f	**t**	**t**	**f**
f	**f**	**t**	**t**
t	**t**	**f**	**f**
t	**f**	**f**	**f**
f	**t**	**f**	**f**
f	**f**	**f**	**t**

Each row for which f is true can be described by a true statement of the form $B_1 \wedge \ldots \wedge B_n$, where $B_i = A_i$ or $B_i = \neg A_i$ holds for each i. By connecting these statements with $\vee$, one obtains a statement equivalent to f. In the example above:

$$(A_1 \wedge A_2 \wedge A_3) \vee (\neg A_1 \wedge \neg A_2 \wedge A_3) \vee (\neg A_1 \wedge \neg A_2 \wedge \neg A_3).$$

This can be simplified according to Theorem I.2.5 to

$$(A_1 \wedge A_2 \wedge A_3) \vee (\neg A_1 \wedge \neg A_2).$$

By applying double negation and De Morgan's laws, one obtains an equivalent statement of the form $(\ldots \vee \ldots \vee \ldots) \wedge (\ldots) \wedge$. In the example:

$$(\neg A_1 \vee \neg A_2 \vee \neg A_3) \wedge (A_1 \vee A_2).$$

(ii) The *satisfiability problem* (short SAT) deals with the question of whether a given statement f is true for a suitable assignment of the elementary statements. If f depends on n elementary statements, then in the worst case 2^n cases must be considered. The SAT problem belongs to the complexity class NP. This means that the value of f for a given assignment of the variables can be determined in polynomial runtime (in n) (for example, by a calculation in Boolean algebra). The SAT problem is even NP-complete (Theorem of Cook), i. e. every other NP problem can be reduced to SAT in polynomial runtime. One of the greatest open problems in theoretical computer science is whether the classes NP and P coincide.[5] If one finds a general algorithm with polynomial runtime that determines whether an arbitrary f is satisfiable, then one would have proven P = NP. Since this is considered very unlikely, it is desirable to prove statements on the syntactic level through axioms and rules of inference (apart from the fact that statements in more powerful calculi can depend on infinitely many parameters and then can no longer be verified by truth tables anyway).

(iii) In the following, we assume that the symbols of propositional logic and their standard interpretation are present in every calculus.

Definition I.2.7. A calculus with an interpretation is called

- *consistent* or *contradiction-free*, if no formula f can be proven together with its negation ($\nvdash f$ or $\nvdash \neg f$).
- *negation-complete*, if every formula f or its negation can be proven ($\vdash f$ or $\vdash \neg f$).
- *sound*, if every sentence f is true (from $\vdash f$ follows $\vDash f$)
- *complete*, if every true statement f is provable (from $\vDash f$ follows $\vdash f$).

Remark I.2.8.

(i) Consistency and negation-completeness are purely syntactic properties that do not depend on the meaning of the symbol $\neg$.

(ii) In an inconsistent calculus, every statement g can be proven:

$\vdash f$	(given from inconsistency)
$\vdash \neg f$	(given from inconsistency)
$\vdash \neg f \Rightarrow (f \Rightarrow g)$	(Lemma I.1.11(v))
$\vdash f \Rightarrow g$	(MP)
$\vdash g$	(MP)

Such a system cannot be sound, because otherwise f and $\neg f$ would be true. Since mathematics serves not least as a foundation for the natural sciences, one is primarily interested in sound systems.

[5] This is one of the seven *Millennium Problems*, for whose solution one million dollars each are offered, see `https://www.claymath.org/millennium-problems/`.

Theorem I.2.9. *Propositional logic with the standard interpretation is sound and consistent, but not negation-complete.*

Proof. For correctness, we first show that the three axioms of the calculus are tautologies. Suppose that $(\mathcal{A}_1)$ is false for certain propositions f and g. Then f must be true and $g \Rightarrow f$ false. However, this is only possible if f is false. This contradiction shows that $(\mathcal{A}_1)$ is a tautology. If $(\mathcal{A}_2)$ is false, then $\neg f \Rightarrow \neg g$ holds and $g \Rightarrow f$ is false. This implies that g holds, but f does not. But then $\neg f \Rightarrow \neg g$ would be false. Finally, let $(\mathcal{A}_3)$ be false. We conduct the argument in a tabular form, where the value of a proposition is placed under the connecting $\Rightarrow$:

$(f$	$\Rightarrow$	$(g$	$\Rightarrow$	$h))$	$\Rightarrow$	$((f$	$\Rightarrow$	$g)$	$\Rightarrow$	$(f$	$\Rightarrow$	$h))$
					f							
t									**f**			
t							**t**				**f**	
t							**t**			**t**		**f**
t		**t**				**t**		**t**		**t**		**f**
	t		**f**	↯[6]								

Thus, all axioms are tautologies. If f and $f \Rightarrow g$ are true, it follows from the interpretation of $\Rightarrow$ that g must also be true. The application of (MP) therefore produces only tautologies. This shows the correctness of $\mathcal{A}$. According to Remark I.2.8, $\mathcal{A}$ is consistent.

Since every elementary proposition A can be both true and false, neither A nor $\neg A$ can be proven. Thus, $\mathcal{A}$ cannot be negation-complete. □

Remark I.2.10.

(i) Note that ($\vDash A$ or $\vDash B$) is not equivalent to $\vDash A \vee B$ (choose $B = \neg A$).

(ii) To prove the completeness of propositional logic, the following lemmas are required.

Lemma I.2.11. *Let $f_1, \ldots, f_{n+1}$ be propositions in $\mathcal{A}$. If $f_1, \ldots, f_n \vdash f_{n+1}$ and $f_1, \ldots, f_{n-1}, \neg f_n \vdash f_{n+1}$ hold, then $f_1, \ldots, f_{n-1} \vdash f_{n+1}$ also holds.*

Proof. According to Lemma I.1.10, it holds that

$$
\begin{aligned}
f_1, \ldots, f_n &\vdash f_{n+1} \\
f_1, \ldots, f_{n-1} &\vdash f_n \Rightarrow f_{n+1} \\
f_1, \ldots, f_{n-1} &\vdash \neg f_n \Rightarrow f_{n+1} \\
&\vdash (f_n \Rightarrow f_{n+1}) \Rightarrow ((\neg f_n \Rightarrow f_{n+1}) \Rightarrow f_{n+1}) && \text{(Lemma I.1.11(xii))} \\
f_1, \ldots, f_{n-1} &\vdash (\neg f_n \Rightarrow f_{n+1}) \Rightarrow f_{n+1} && \text{(MP)} \\
f_1, \ldots, f_{n-1} &\vdash f_{n+1} && \text{(MP)}
\end{aligned}
$$

□

Lemma I.2.12 (Kalmár)**.** *Let f be a statement in $\mathcal{A}$ constructed from elementary statements $A_1, \ldots, A_n$. Let $x_1, \ldots, x_n$ be arbitrary truth values, i. e. $x_i = \boldsymbol{f}$ or $x_i = \boldsymbol{t}$ for $i = 1, \ldots, n$. Let $A_i' := A_i$ if $x_i = \boldsymbol{t}$ and $A_i' := \neg A_i$ if $x_i = \boldsymbol{f}$ for $i = 1, \ldots, n$. If one replaces each A_i by x_i in f, then f becomes true or false. In the first case we set $f' := f$ and in the second $f' := \neg f$. Then $A_1', \ldots, A_n' \vdash f'$ holds.*

[6] Contradiction symbol

Proof. We can assume that f contains only the symbols $(,)$, $\neg$ and $\Rightarrow$, i. e. no abbreviations like $\wedge$ or $\vee$. Let $m = m(f)$ be the total number of all $\neg$ and $\Rightarrow$ in f. In the case $m(f) = 0$, $f = A_i$ for some i. Then $f' = A'_i$ and $A'_1, \ldots, A'_n \vdash f'$. Now let $m > 0$ and the claim be already proven for all statements g with $m(g) < m$.

Case 1: $f = \neg g$ with $m(g) < m$.
In the case $f' = f$, $g' = \neg g = f = f'$ and $A'_1, \ldots, A'_n \vdash g'$ by induction. Now let $f' = \neg f$. Then $g' = g$. From Lemma I.1.11 it follows that

$$\begin{aligned} &A'_1, \ldots, A'_n \vdash g \\ &A'_1, \ldots, A'_n \vdash g \Rightarrow \neg\neg g \\ &A'_1, \ldots, A'_n \vdash \neg\neg g \end{aligned}$$

with $\neg\neg g = \neg f = f'$.

Case 2: $f = (g \Rightarrow h)$ with $m(g), m(h) < m$.
First let $g' = \neg g$. Then $f' = f$. By induction,

$$\begin{aligned} &A'_1, \ldots, A'_n \vdash \neg g \\ &A'_1, \ldots, A'_n \vdash \neg g \Rightarrow (g \Rightarrow h) && \text{(Lemma I.1.11(v))} \\ &A'_1, \ldots, A'_n \vdash g \Rightarrow h \end{aligned}$$

Now let $g' = g$ and $h' = h$. Then $f' = f$ and it holds that

$$\begin{aligned} &A'_1, \ldots, A'_n \vdash h \\ &A'_1, \ldots, A'_n \vdash h \Rightarrow (g \Rightarrow h) && (\mathcal{A}_1) \\ &A'_1, \ldots, A'_n \vdash g \Rightarrow h && \text{(MP)} \end{aligned}$$

Finally, let $g' = g$ and $h' = \neg h$. Then $f' = \neg f = \neg(g \Rightarrow h)$ and

$$\begin{aligned} &A'_1, \ldots, A'_n \vdash g \\ &A'_1, \ldots, A'_n \vdash \neg h \\ &A'_1, \ldots, A'_n \vdash g \Rightarrow (\neg h \Rightarrow \neg(g \Rightarrow h)) && \text{(Lemma I.1.11(viii))} \\ &A'_1, \ldots, A'_n \vdash \neg h \Rightarrow \neg(g \Rightarrow h) && \text{(MP)} \\ &A'_1, \ldots, A'_n \vdash \neg(g \Rightarrow h) && \text{(MP)} \end{aligned}$$

□

Theorem I.2.13. *Propositional logic with the standard interpretation is complete.*

Proof. Let f be a tautology constructed from the elementary statements $A_1, \ldots, A_n$. For every assignment of $A_1, \ldots, A_n$, f is true. From Lemma I.2.12 and Lemma I.2.11 it therefore follows that

$$\begin{aligned} A_1, \ldots, A_n &\vdash f \\ A_1, \ldots, \neg A_n &\vdash f \\ A_1, \ldots, A_{n-1} &\vdash f \\ A_1 \ldots, \neg A_{n-1} &\vdash f \\ &\vdots \\ &\vdash f \end{aligned}$$

□

Remark I.2.14.

(i) The tautologies found in Theorem I.2.5 can now be used like axioms in the calculus. From the associativity of $\wedge$, $\vee$ and $\Leftrightarrow$ it follows that the statements $f \wedge g \wedge h$, $f \vee g \vee h$ and $f \Leftrightarrow g \Leftrightarrow h$ also make sense without parentheses. The law of excluded middle allows for indirect proof by contradiction: If a statement A can be led to a contradiction, then $\neg A$ must hold.

(ii) There are situations in which one can prove $A \Rightarrow B$ and $\neg A \Rightarrow B$. Without knowing whether A holds, one can in any case derive the validity of B (Lemma I.2.11). This is sometimes referred to as a *non-constructive* proof. Example: There exist irrational real numbers x, y, such that x^y is rational. Proof: It is well known that $\sqrt{2}$ is irrational (Theorem II.6.14). If $\sqrt{2}^{\sqrt{2}}$ is rational, then we are finished. Otherwise $\sqrt{2}^{\sqrt{2}}$ is irrational and

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}^2} = \sqrt{2}^2 = 2$$

is rational. Without knowing which case occurs, we have proven the claim. The theory of *intuitionism* developed by BROUWER rejects such proofs. For this, a calculus with weaker axioms and inference rules must be used, in which the law of excluded middle is unprovable. Since many important theorems of mathematics remain unprovable in this framework, intuitionism never prevailed.

(iii) The completeness of propositional logic allows for verifying theorems by mechanical derivation in the calculus. However, it is by no means clear how to find such a proof (cf. proof of Lemma I.1.11). But that is exactly what generally constitutes the appeal of mathematics! With the programming language *Prolog* and the proof assistant *lean*, logical derivations can be constructed with the computer.

I.3. Predicate Logic

Remark I.3.1. In mathematics, one generally only speaks about things that can be defined intrinsically (questions like "is there a God?" belong to philosophy). Since propositional logic is obviously far too primitive to express simple theorems like $1+1=2$, we will expand our calculus step by step. To improve readability, we occasionally replace the metalanguage with primitive symbols of set theory such as $\in$, $\subseteq$ or $\cup$ (see section II.1).

Definition I.3.2. The *predicate logic* (*first-order*) $\mathcal{P}^1 = \mathcal{P}$ is a calculus with the following properties:

- Alphabet: variables and constants ($a, b, \ldots, 0, 1, \ldots$), functions ($\alpha, \beta, \ldots$), predicates ($A, B, \ldots$), symbols (,), $\neg$, $\Rightarrow$, $\forall$ (*universal quantifier*). Functions and predicates depend on a finite number of parameters (also called arguments). If α or A depends on $x_1, \ldots, x_n$, then α or A is called *n-ary* and one writes $\alpha(x_1, \ldots, x_n)$ or $A(x_1, \ldots, x_n)$. For technical reasons, we always assume that the alphabet is countable (see Remark II.5.2).
- As a preliminary stage of formulas, *terms* are defined recursively: variables and constants are terms. If $t_1, \ldots, t_n$ are terms and φ is an n-ary function, then $\varphi(t_1, \ldots, t_n)$ is also a term.
- Formulas: If $t_1, \ldots, t_n$ are terms and P is an n-ary predicate, then $P(t_1, \ldots, t_n)$ is a formula. If f and g are formulas and x is a variable, then $(\neg f)$, $(f \Rightarrow g)$ and $(\forall x f)$ are also formulas. It is not required that x occurs in f.

- We define recursively when a variable x occurs *free* in a formula f: If f is a term or of the form $P(t_1, \ldots, t_n)$, then x is free. If x is free in f, then it is also free in $\neg f$ and in $\forall y f$, where y is different from x. The occurrence of x in $\forall x f$, on the other hand, is called *bound*. If f has the form $g \Rightarrow h$ and x occurs free in g or h, then x is also free in f (x can occur both free and bound in f). Variables occurring free in f are often specified as arguments, as with functions: $f(x_1, \ldots, x_n)$. A formula in which no variable occurs free is called *closed*. Terms without variables (i.e., constructions of constants and functions) are also called *closed* (terms generally do not contain universal quantifiers).
- One can replace every free occurrence of a variable x in a formula f by a term t. For this we write $f(x \leftarrow t)$ or briefly $f(t)$, if misunderstandings are excluded.[7] We always assume that the replacement is *collision-free*, i. e., that no variable from t becomes bound in f (this can often be achieved by suitable renaming of the variables).
- Axioms: For all formulas f, g, h, the axioms $(\mathcal{A}_1)$, $(\mathcal{A}_2)$ and $(\mathcal{A}_3)$ of propositional logic hold. For all variables x and all terms t, the following additionally hold:

$$((\forall x(f \Rightarrow g)) \Rightarrow (f \Rightarrow (\forall x g))) \qquad \text{if } x \text{ does not occur free in } f \qquad (\mathcal{P}_1)$$

$$(\forall x f) \Rightarrow (f(x \leftarrow t)) \qquad \text{if collision-free} \qquad (\mathcal{P}_2)$$

- Rules of inference: Modus ponens (MP) and *generalization*

$$\frac{f}{(\forall x f)} \qquad \text{(G)}$$

  for every formula f and every variable x.

As in every calculus, one defines proofs (under assumptions) and $\vdash$.

Example I.3.3. Let σ be a 1-ary function and P a 2-ary predicate in $\mathcal{P}$. Then

$$f := (\forall x(P(x, y) \Rightarrow (\forall y(\neg P(\sigma(y), x)))))$$

is a formula in which x occurs only bound and y occurs both free and bound. If z is another variable, then

$$f(y \leftarrow z) = (\forall x(P(x, z) \Rightarrow (\forall y(\neg P(\sigma(y), x)))))$$

is a collision-free substitution. The substitution $f(y \leftarrow x)$, however, would not be collision-free.

Remark I.3.4.

(i) The symbols $\wedge$, $\vee$ and $\Leftrightarrow$ are used as abbreviations as usual. In addition to the bracket conventions from Remark I.2.4, we agree that $\forall$ binds more strongly than $\Rightarrow$ and $\Leftrightarrow$, but not more strongly than the remaining symbols. Therefore, $\forall x f \Rightarrow g$ stands for $(\forall x f) \Rightarrow g$.

(ii) From the countability of the alphabet, it follows that all formulas in $\mathcal{P}$ can be counted (see Example II.5.3). One can dispense with constants if one allows 0-ary functions instead.

(iii) Many of the results from section I.1, in particular the inference rules (MP') and (MP), remain valid in $\mathcal{P}$ as well. Because of the new rule (G), however, the deduction lemma generally only holds for closed formulas (Exercise I.10). Since (G) was not available in the proof of Lemma I.1.11, Lemma I.1.11 holds without restriction for formulas in $\mathcal{P}$ (cf. Exercise I.11).

[7] The new symbol $\leftarrow$ is used here merely as an abbreviation to avoid having to write out the actual replacement of x.

(iv) As a replacement for the deduction lemma, we introduce *deduction* as a new inference rule:

$$\frac{g,\ f \Rightarrow (g \Rightarrow h)}{f \Rightarrow h}. \tag{D}$$

It is valid because

$$\begin{aligned}
g &\vdash f \Rightarrow g && \text{(MP')}\\
g,\ f \Rightarrow (g \Rightarrow h) &\vdash f \Rightarrow (g \Rightarrow h)\\
&\vdash (f \Rightarrow (g \Rightarrow h)) \Rightarrow ((f \Rightarrow g) \Rightarrow (f \Rightarrow h)) && (\mathcal{A}_3)\\
g,\ f \Rightarrow (g \Rightarrow h) &\vdash (f \Rightarrow g) \Rightarrow (f \Rightarrow h) && \text{(MP)}\\
g,\ f \Rightarrow (g \Rightarrow h) &\vdash f \Rightarrow h && \text{(MP)}
\end{aligned}$$

(v) From the combination of $(\mathcal{P}_2)$ and (G), we obtain *specialization* as a new inference rule

$$\frac{f}{f(x \leftarrow t)} \qquad \text{if collision-free.} \tag{S}$$

This holds in particular if t is closed or f contains no universal quantifiers. Furthermore,

$$\vdash \forall x f \Rightarrow f, \tag{$\mathcal{P}_2'$}$$

holds, because the "substitution" $x \leftarrow x$ is always collision-free (only free occurrences of x are "substituted"). If x does not occur free in f, then the converse can also be proven:

$$\begin{aligned}
&\vdash f \Rightarrow f && \text{(Example I.1.8)}\\
&\vdash \forall x(f \Rightarrow f) && \text{(G)}\\
&\vdash (\forall x(f \Rightarrow f)) \Rightarrow (f \Rightarrow \forall x f) && (\mathcal{P}_1)\\
&\vdash f \Rightarrow \forall x f && \text{(MP)}
\end{aligned}$$

According to the inference rules, $\vdash f$ is generally equivalent to $\vdash \forall x f$ (even if x occurs free in f). By appending further universal quantifiers (for each free variable in f), one can transform f into a closed formula in this way.

(vi) If several variables of a formula are replaced, the order must be observed. To avoid collisions, one can create new variables and use them as temporary storage:

$$\begin{aligned}
&\vdash f(x, y)\\
&\vdash f(z, y) && \text{(S)}\\
&\vdash f(z, x) && \text{(S)}\\
&\vdash f(y, x) && \text{(S)}
\end{aligned}$$

(vii) If one adds further axioms, one speaks generally of a *first-order* calculus.

Definition I.3.5.

(i) An *interpretation* of $\mathcal{P}$ consists of a set U (*universe*) and a mapping I. Each constant c is interpreted as an element in U, i.e., $I(c) \in U$. Variables also represent elements in U, but are not assigned a fixed value. The symbols (,), $\neg$, $\Rightarrow$, $\wedge$, $\vee$ and $\Leftrightarrow$ have the same meaning as in the standard interpretation of propositional logic. The new symbol $\forall$ means *for all* (see (iii)).

(ii) Each n-ary function φ of $\mathcal{P}$ is interpreted as an "ordinary" mapping $I(\varphi)\colon U^n \to U$.[8] For a closed term t, it therefore holds that $I(t) \in U$. Predicates are properties or relations that hold or do not hold for their parameters (an n-ary predicate formally corresponds to a relation, i.e., a subset of U^n, see Definition II.2.1).

(iii) A formula of the form $P(t_1, \ldots, t_n)$ is interpreted as true if $t_1, \ldots, t_n$ are in relation with respect to $I(P)$. If the t_i contain variables, then the relation must be valid in general for every assignment of these variables. A formula of the form $\forall x f$ is true if and only if $I(f) = \mathbf{t}$ holds for every assignment of x in U.

(iv) If $I(f)$ holds, then (U, I) is called a *model* for f and one writes $\vDash_{(U,I)} f$. Analogously, (U, I) is a model for a set M of formulas if $I(f)$ holds for every f in M. If every interpretation of $\mathcal{P}$ is a model for f, then f is called a *tautology* and one writes (as before) $\vDash f$ (in propositional logic, however, we only considered the standard interpretation for this). If (U, I) is a model for every sentence in $\mathcal{P}$, then (U, I) is called a *model* for $\mathcal{P}$.

Remark I.3.6.

(i) As on the syntactic level (Remark I.3.4), $\vDash_{(U,I)} f$ and $\vDash_{(U,I)} \forall x f$ are equivalent for every formula f. Therefore, (I, U) is already a model for a set M of formulas if $I(f) = \mathbf{t}$ holds for every closed formula f in M.

(ii) For closed formulas f, either f or $\neg f$ is true with respect to a fixed interpretation. However, if f has free variables, then f and $\neg f$ can both be false (e. g. $f := P(x)$ for a predicate that holds for some x and not for others). In this sense, predicate logic cannot be negation-complete. Even if f is closed, neither f nor $\neg f$ needs to be a tautology, because f could be false in one interpretation, while $\neg f$ is false in another interpretation.

(iii) Formulas of the type $\forall x(f \Rightarrow \forall x g)$ are indeed permitted, but misleading, since the outer universal quantifier has no effect on g. In such cases, it is helpful to replace g by $g(x \leftarrow y)$ and to use $\forall x(f \Rightarrow \forall y g)$.

(iv) In addition to the universal quantifier, one introduces as an abbreviation the *existential quantifier* $\exists$ as a new symbol with the interpretation *there exists*:

$$\exists x f := \neg(\forall x \neg f).$$

The formula corresponds to De Morgan's rule in an arbitrary universe (There exists an x with $f(x)$ if and only if it is not the case that for all x, $f(x)$ is false.) For every closed term t, it holds that

$$\begin{aligned}
&\vdash \forall x \neg f \Rightarrow \neg f(x \leftarrow t) && (\mathcal{P}_2)\\
&\vdash (\forall x \neg f \Rightarrow \neg f(t)) \Rightarrow (\neg\neg f(t) \Rightarrow \exists x f) && (\text{Lemma I.1.11(iv)})\\
&\vdash \neg\neg f(t) \Rightarrow \exists x f && (\text{MP})\\
&\vdash f(t) \Rightarrow \neg\neg f(t) && (\text{Lemma I.1.11(iii)})\\
&\vdash f(t) \Rightarrow \exists x f && (\text{MB})
\end{aligned}$$

Theorem I.3.7. *Every provable formula in $\mathcal{P}$ is a tautology.*

[8] Precise definition in section II.2.

Proof. The axioms $(\mathcal{A}_1)$, $(\mathcal{A}_2)$ and $(\mathcal{A}_3)$ are tautologies, since we assume the standard interpretation of $\mathcal{A}$. Let f and g be formulas such that x does not occur free in f. To verify the validity of $(\mathcal{P}_1)$, we can assume $\vDash_{(U,I)} \forall x(f \Rightarrow g)$ for an arbitrary interpretation (I, U) according to Theorem I.2.5. If $I(f) = \mathbf{f}$, then $(\mathcal{P}_1)$ becomes true overall. So let $I(f) = \mathbf{t}$. Since x does not occur free in f, $f(x)$ holds for all x in U. On the other hand, $f(x) \Rightarrow g(x)$ also holds for all x. With (MP) it follows that $\vDash_{(U,I)} \forall x g$. Thus $(\mathcal{P}_1)$ is a tautology. If f is true for all x with respect to (I, U), then it is also true for $x = t$ for a specific term t, provided the substitution is collision-free. This shows that $(\mathcal{P}_2)$ is also a tautology.

As in $\mathcal{A}$, (MP) yields only tautologies. If f is a tautology, then f is a true statement for every possible interpretation of the variables. In particular, $\forall x f$ is a tautology. This confirms the validity of (G). □

Example I.3.8.

(i) Let $\mathcal{N}$ be a first-order calculus with the constant 0, a 1-ary function σ and a 2-ary predicate G. As new axioms we add:

$$\vdash \forall x G(x, \sigma(x))$$
$$\vdash \neg\exists x G(x, 0)$$

An obvious interpretation I is obtained with the universe of natural numbers $U = \{0, 1, \ldots\}$,[9] the successor function $I(\sigma)(x) := x + 1$ and the greater-than relation $I(G)(x, y) \Leftrightarrow x < y$. The axioms state that every number is smaller than its successor and no number is smaller than 0. Thus (U, I) is a model for $\mathcal{N}$. This by no means implies that all known properties of G and σ can be proven in $\mathcal{N}$. For example, (U', I') with $U' = \{0, 1\}$, $I'(\sigma)(0) = I'(\sigma)(1) = 1$ and $I'(G)(x, y) \Leftrightarrow y = 1$ is also a model for $\mathcal{N}$. The formula

$$\neg\exists x G(x, x)$$

which is valid in (I, U) becomes false in (I', U'). It can therefore not be proven in $\mathcal{N}$.

(ii) A classical example for the use of quantifiers is the continuity of a real function f at a point x_0. The set of real numbers serves as the universe.[10] Instead of the usual variables ϵ and δ, we use the Latin letters e and d according to our convention. In addition to the constant 0 introduced in (i) and the greater-than relation G, one needs the 2-ary distance function δ with the interpretation $I(\delta)(x, y) = |x - y|$. This yields the following formula:

$$\forall e\Big(G(0, e) \Rightarrow \exists d\Big(G(0, d) \wedge \forall x\big(G(\delta(x, x_0), d) \Rightarrow G(\delta(f(x), f(x_0)), e)\big)\Big)\Big).$$

(iii) In a first-order calculus, the equality relation = cannot be fully expressed. Suppose there is a predicate P with suitable axioms such that, with respect to an interpretation (U, I), the statement $P(x, y)$ is true for all x, y in U if and only if $x = y$ holds. One can now enlarge the universe U by adding to each u in U a "copy" u' in a "parallel universe". Each variable in a formula f can optionally be interpreted as u or u' without changing the validity of f. In this new interpretation, P no longer has the desired property, because $P(u, u')$ is true. Thus, there can be no tautology that links P with the equality relation.

Definition I.3.9. In *predicate logic with equality* $\mathcal{P}^=$ one supplements $\mathcal{P}$ with the symbol =, which is interpreted as the equality sign. If s and t are terms, then let $s = t$ be a formula. For every formula f

[9] The natural numbers are formally defined in Example II.4.9.
[10] Defined in Definition II.6.6.

and all variables x and y we supplement the following axioms:

$$x = x \qquad (\mathcal{P}_1^=)$$
$$(x = y) \Rightarrow (f(y \leftarrow x) \Rightarrow f) \qquad \text{if collision-free} \qquad (\mathcal{P}_2^=)$$

Remark I.3.10.

(i) We agree that $=$ binds more strongly than $\Rightarrow$. Instead of $\neg(x = y)$ one writes $x \neq y$.

(ii) In every interpretation $x = x$ is obviously true, i. e. $(\mathcal{P}_1^=)$ is a tautology. Axiom $(\mathcal{P}_2^=)$ guarantees that one can replace variables in formulas by equal variables. This too is a tautology. Thus Theorem I.3.7 carries over to $\mathcal{P}^=$.

(iii) With the equality sign it can be expressed that *exactly* one element with a certain property exists. For this one often uses the following abbreviation:

$$\exists! x f := (\exists x f) \wedge \forall y (f(x \leftarrow y) \Rightarrow y = x).$$

Example I.3.11. Predicate logic with equality is suitable for defining mathematical groups. For this, let e be a constant (for the neutral element) and σ a 2-ary function (for the group operation). We extend $\mathcal{P}^=$ by the following axioms:

$$\vdash \sigma(\sigma(x, y), z) = \sigma(x, \sigma(y, z)) \qquad \text{(associativity)}$$
$$\vdash \sigma(x, e) = x \qquad \text{(neutrality)}$$
$$\vdash \exists y(\sigma(x, y) = e) \qquad \text{(existence of inverse elements)}$$

Let $\mathcal{G}$ be the resulting calculus. As is well known, in every group neutrality from the left also holds, i. e. $\sigma(e, x) = x$ is a tautology.[11] From Gödel's Completeness Theorem I.4.6 it will follow that $\sigma(e, x) = x$ is a theorem in $\mathcal{G}$. On the other hand $\nvdash \sigma(x, y) = \sigma(y, x)$, since not every group is abelian.

Lemma I.3.12. *For all terms t, u, v in $\mathcal{P}^=$:*

(i) $\vdash t = t$.

(ii) $\vdash t = u \Leftrightarrow u = t$.

(iii) $\vdash t = u \Rightarrow (u = v \Rightarrow t = v)$.

Proof. Since no quantifiers occur in the formulas, we can assume by (S) that t, u and v are variables. Now (i) is equal to $(\mathcal{P}_1^=)$.

(ii)

$$\vdash t = t \qquad (\mathcal{P}_1^=)$$
$$\vdash t = u \Rightarrow (t = t \Rightarrow u = t) \qquad (\mathcal{P}_2^=)$$
$$\vdash t = u \Rightarrow u = t \qquad \text{(D)}$$

For reasons of symmetry, $\vdash t = u \Rightarrow u = t$ also holds. The claim follows from Exercise I.4.

[11] See Group Theory Notes

(iii)

$$\vdash t = u \Rightarrow u = t \tag{ii}$$
$$\vdash u = t \Rightarrow (u = v \Rightarrow t = v) \tag{$\mathcal{P}_2^=$}$$
$$\vdash t = u \Rightarrow (u = v \Rightarrow t = v) \tag{MB}$$

□

Lemma I.3.13. *Let $t_1, \ldots, t_n, u_1, \ldots, u_n$ be terms, φ an n-ary function and P an n-ary predicate in $\mathcal{P}^=$. Then*

(i) $\vdash t_1 = u_1 \Rightarrow (t_2 = u_2 \Rightarrow \ldots \Rightarrow (t_n = u_n \Rightarrow \varphi(u_1, \ldots, u_n) = \varphi(t_1, \ldots, t_n)) \ldots)$

(ii) From $\vdash t_i = u_i$ *for* $i = 1, \ldots, n$ *follows* $\vdash P(t_1, \ldots, t_n) \Leftrightarrow P(u_1, \ldots, u_n)$.

Proof. Since no quantifiers occur, we can assume that $t_1, \ldots, t_n, u_1, \ldots, u_n$ are variables.

(i) Let $f_k(u_k, \ldots, u_n) := (t_k = u_k \Rightarrow \ldots \Rightarrow (t_n = u_n \Rightarrow \varphi(t_1, \ldots, t_n) = \varphi(t_1, \ldots, t_{k-1}, u_k, \ldots, u_n)) \ldots)$ for $k = 1, \ldots, n$. Because of

$$\vdash \varphi(t_1, \ldots, t_n) = \varphi(t_1, \ldots, t_n) \tag{I.3.12}$$
$$\vdash t_n = u_n \Rightarrow (\varphi(t_1, \ldots, t_n) = \varphi(t_1, \ldots, t_n) \Rightarrow \varphi(t_1, \ldots, t_n) = \varphi(t_1, \ldots, t_{n-1}, u_n)) \tag{$\mathcal{P}_2^=$}$$
$$\vdash t_n = u_n \Rightarrow \varphi(t_1, \ldots, t_n) = \varphi(t_1, \ldots, t_{n-1}, u_n) \tag{D}$$

$\vdash f_n$ holds. Suppose f_{k+1} is already proven. Then

$$\vdash f_{k+1}$$
$$\vdash t_k = u_k \Rightarrow (f_{k+1} \Rightarrow (t_{k+1} = u_{k+1} \Rightarrow \ldots \varphi(t_1, \ldots, t_n) = \varphi(t_1, \ldots, t_{k-1}, u_k, \ldots, u_n) \ldots) \tag{$\mathcal{P}_2^=$}$$
$$\vdash f_k \tag{D}$$

holds. Finally, $\vdash f_1$ holds.

(ii) We have

$$\vdash t_1 = u_1 \Rightarrow (P(t_1, \ldots, t_n) \Rightarrow P(t_1, \ldots, t_n) \Rightarrow P(t_1, \ldots, t_n) \Rightarrow P(u_1, t_2, \ldots, t_n)) \tag{$\mathcal{P}_2^=$}$$
$$\vdash P(t_1, \ldots, t_n) \Rightarrow P(u_1, t_2, \ldots, t_n) \tag{MP}$$
$$\vdash t_2 = u_2 \Rightarrow (P(t_1, \ldots, t_n) \Rightarrow P(u_1, t_2, \ldots, t_n) \Rightarrow P(t_1, \ldots, t_n) \Rightarrow P(u_1, u_2, t_3, \ldots, t_n)) \tag{$\mathcal{P}_2^=$}$$
$$\vdash P(t_1, \ldots, t_n) \Rightarrow P(u_1, u_2, t_3, \ldots, t_n) \tag{D}$$
$$\vdots$$
$$\vdash P(t_1, \ldots, t_n) \Rightarrow P(u_1, \ldots, u_n)$$

For reasons of symmetry, $\vdash P(u_1, \ldots, u_n) \Rightarrow P(t_1, \ldots, t_n)$ also holds. The claim follows from Exercise I.4. □

I.4. The Model Existence Theorem

Remark I.4.1. Up to now, we had proven the consistency of a calculus by providing a model. In this section, we show that this is always possible for first-order calculi.

Definition I.4.2.

- Let M be a set of formulas in a first-order calculus $\mathcal{K}$ with equality. We call M *consistent*, if no formula f exists such that $M \vdash f$ and $M \vdash \neg f$. This means that one obtains a consistent calculus if one adds the formulas in M as axioms to $\mathcal{K}$ (for this, $\mathcal{K}$ itself must be consistent).
- A consistent set M of formulas is called *closed*, if for every formula f in $\mathcal{K}$ the following holds:

  (i) $\vdash f$ or $\vdash \neg f$.

  (ii) If $\neg\forall x f \in M$, then there exists a closed term t such that $\neg f(x \leftarrow t) \in M$.

Lemma I.4.3. *Let M be a closed set of formulas in a first-order calculus $\mathcal{K}$ with equality. Let x be a variable and f, g formulas in $\mathcal{K}$. Then*

(i) From $M \vdash f$ it follows that $f \in M$.

(ii) $f \Rightarrow g$ lies in M if and only if $\neg f$ or g lie in M.

(iii) $\forall x f$ lies in M if and only if $f(x \leftarrow t)$ lies in M for every closed term t.

Proof.

(i) Since M is consistent, $M \nvdash \neg f$ holds and $\neg f$ cannot lie in M. By definition, $f \in M$.

(ii) Let $f \Rightarrow g \in M$. Suppose that neither $\neg f$ nor g lie in M. Then $f, \neg g \in M$ and M would be inconsistent:

$$\begin{aligned} &M \vdash f \Rightarrow g \\ &M \vdash f \\ &M \vdash g && \text{(MP)} \\ &M \vdash \neg g \end{aligned}$$

Conversely, if $\neg f \in M$, then

$$\begin{aligned} M &\vdash \neg f \\ M &\vdash \neg f \Rightarrow (f \Rightarrow g) && \text{(Lemma I.1.11(v))} \\ M &\vdash f \Rightarrow g && \text{(MP)} \\ f &\Rightarrow g \in M && \text{(i)} \end{aligned}$$

If $g \in M$, then

$$\begin{aligned} M &\vdash g \\ M &\vdash f \Rightarrow g && \text{(MP')} \\ f &\Rightarrow g \in M && \text{(i)} \end{aligned}$$

(iii) If $\forall x f$ lies in M, then $M \vdash f(t)$ follows for all closed terms t by (S). By (i), $f(t) \in M$ for all t. Conversely, if $\forall x f$ does not lie in M, then $\neg\forall x f \in M$ holds. By definition, there exists a closed term t with $\neg f(t) \in M$, i.e., $f(t)$ does not lie in M. □

Lemma I.4.4. *Let M be a consistent set of formulas in a first-order calculus $\mathcal{K}$ with equality. Then there exists a set of formulas $\hat{M}$ in a first-order calculus $\hat{\mathcal{K}}$ with the following properties:*

(i) $\hat{\mathcal{K}}$ differs from $\mathcal{K}$ only by a larger alphabet.

(ii) $\hat{M}$ contains M.

(iii) $\hat{M}$ is closed.

Proof. We obtain $\hat{\mathcal{K}}$ from $\mathcal{K}$ by adding new constants $c_1, c_2, \ldots$ that are not yet present in $\mathcal{K}$. According to Remark I.3.4, the closed formulas in $\hat{\mathcal{K}}$ can be enumerated: $f_1, f_2, \ldots$. We inductively define sets of formulas $M_0, M_1, \ldots$ with the following properties:

(a) M_i is consistent.

(b) M_{i+1} contains M_i.

(c) M_i contains only finitely many of the c_i.

Obviously, $M_0 := M$ satisfies these properties. Suppose M_i is already defined. If M_i becomes inconsistent by adding f_i, let $M_{i+1} := M_i$. We now assume that M_i is consistent by adding f_i. If f_i does not have the form $\neg\forall x g$, then $M_{i+1} := M_i \cup \{f_i\}$ satisfies the properties (a)–(c). Finally, let $f_i = \neg\forall x g$. Because of c, there exists a c_j that occurs neither in M_i nor in f_i. We set $M_{i+1} := M_i \cup \{f_i, \neg g(x \leftarrow c_j)\}$. Suppose M_{i+1} is inconsistent. Since $g(c_j)$ is closed, the deduction lemma may be applied (Exercise I.10). It holds that

$$
\begin{aligned}
&M_i, f_i, \neg g(c_j) \vdash g(c_j) \\
&\qquad M_i, f_i \vdash \neg g(c_j) \Rightarrow g(c_j) && \text{(Lemma I.1.10)} \\
&\qquad M_i, f_i \vdash (\neg g(c_j) \Rightarrow g(c_j)) \Rightarrow g(c_j) && \text{(Lemma I.1.11(xi))} \\
&\qquad M_i, f_i \vdash g(c_j) && \text{(MP)} \\
&\qquad M_i, f_i \vdash \forall x g && \text{(Exercise I.12)} \\
&\qquad M_i, f_i \vdash \neg f_i
\end{aligned}
$$

But then $M_i \cup \{f_i\}$ would be inconsistent. Thus (a) (and trivially also (b), (c)) must hold.

We now show that $\hat{M} := \bigcup_{i \geq 0} M_i$ is closed. Suppose $\hat{M}$ is inconsistent. Then one could derive a contradictory formula like $f \wedge \neg f$ from $\hat{M}$. A corresponding proof consists of only finitely many formulas that are axioms or lie in some M_i. But then M_i would be inconsistent in contradiction to (a). Now let us assume there is a formula f in $\hat{\mathcal{K}}$ with $\hat{M} \nvdash f$ and $\hat{M} \nvdash \neg f$. According to Remark I.3.6, we may assume that f is closed. Then there exist i and j with $f_i = f$ and $f_j = \neg f$. Since f_i cannot lie in M_{i+1}, $M_{i+1} = M_i$ holds by construction. This implies that $M_i \cup \{f\}$ is inconsistent. Analogously, $M_j \cup \{\neg f\}$ is also inconsistent. It follows that $\hat{M} \vdash f$ and $\hat{M} \vdash \neg f$ in contradiction to the consistency of $\hat{M}$. Finally, let $f_i := \neg\forall x g$ be in $\hat{M}$. By construction, $M_{i+1} = M_i \cup \{f_i, \neg g(c_j)\}$ for some j. In particular, $\neg g(c_f)$ is in $\hat{M}$. Thus $\hat{M}$ is closed. □

Theorem I.4.5 (Model Existence Theorem)**.** *Every consistent set M of formulas in a first-order calculus $\mathcal{K}$ with equality has a model. In particular, every consistent first-order calculus has a model.*

Proof (HENKIN). According to Lemma I.4.4, M can be extended to a closed set $\hat{M}$ in a larger calculus $\hat{\mathcal{K}}$. Since a model for $\hat{M}$ can be restricted to $\mathcal{K}$, we can assume $\mathcal{K} = \hat{\mathcal{K}}$ and $M = \hat{M}$. For terms t and u, let $u \sim t$ if and only if $M \vdash t = u$. According to Lemma I.3.12, $\sim$ is an equivalence relation. We denote the equivalence class of t by $[t]$. As the universe U, we choose the set of equivalence classes $[t]$ for all closed terms t.[12] For constants c in $\mathcal{K}$, let $I(c) := [c] \in U$. Variables stand for unspecified equivalence classes $[t]$. For an n-ary function φ and $[t_1], \ldots, [t_n] \in U$, let

$$I(\varphi)([t_1], \ldots, [t_n]) := [\varphi(t_1, \ldots, t_n)].$$

This is well-defined according to Lemma I.3.13, i. e., the definition does not depend on the choice of representatives of $[t_i]$. For an n-ary predicate P, let $I(P)([t_1], \ldots, [t_n]) := \mathbf{t}$ if and only if $P(t_1, \ldots, t_n) \in M$. This is also well-defined according to Lemma I.3.13.

According to Remark I.3.6, it suffices to show that a closed formula f lies in M if and only if $I(f) = \mathbf{t}$ holds. As in the proof of Lemma I.2.12, we argue by the number of symbols $\neg$, $\Rightarrow$, and $\forall$ in f. Suppose f has the form $t = u$ for closed terms t and u. Then by definition $f \in M$ if and only if $[t] = [u]$. Thus $f \in M$ if and only if $I(f) = \mathbf{t}$. If f has the form $P(t_1, \ldots, t_n)$, then $[t_1], \ldots, [t_n] \in U$ and the claim follows from the definition of I. Next, let f be equal to $\neg g$ for a closed formula g. In the case $f \in M$, then $g \notin M$ because M is consistent. By induction $I(g) = \mathbf{f}$, i. e., $I(f) = I(\neg g) = \mathbf{t}$. Conversely, if $I(f) = \mathbf{t}$, then $g \notin M$ follows. Since M is closed, $f \in M$ holds. Now let f be equal to $g \Rightarrow h$ for closed formulas g and h. In the case $f \in M$, then $\neg g \in M$ or $h \in M$ according to Lemma I.4.3. By induction $I(\neg g) = \mathbf{t}$ or $I(h) = \mathbf{t}$. From Theorem I.2.5 it follows that $I(f) = I(\neg g \vee h) = \mathbf{t}$. Conversely, let $I(f) = \mathbf{t}$. Since g and h are closed, it follows that $I(\neg g) = \mathbf{t}$ or $I(h) = \mathbf{t}$. According to Lemma I.4.3, $f \in M$.

Finally, let $f = \forall x g$. In the case $f \in M$, then $g(t) \in M$ for every closed term according to $(\mathcal{P}_2)$. Since U consists of the (equivalence classes of) closed terms, $I(f) = \mathbf{t}$. Conversely, if $I(f) = \mathbf{t}$, then $g(t)$ is true for every closed term t. By induction it follows that $g(t) \in M$ for all t. From Lemma I.4.3 one obtains $f \in M$.

The second claim follows from the first by choosing M to be the set of all sentences of $\mathcal{K}$. □

Theorem I.4.6 (GÖDELs Completeness Theorem)**.** *Every tautology in $\mathcal{P}^=$ is provable.*

Proof. Let us assume there exists a non-provable tautology f in $\mathcal{P}^=$. Wlog. let f be closed. By adding the axiom $\neg f$, one obtains the calculus $\mathcal{K}$. Assume that $\mathcal{K}$ is inconsistent. According to Remark I.2.8, f can be proven in $\mathcal{K}$. With respect to $\mathcal{P}^=$, this means

$$\begin{aligned} \neg f &\vdash f \\ &\vdash \neg f \Rightarrow f && \text{(Lemma I.1.10)} \\ &\vdash (\neg f \Rightarrow f) \Rightarrow f && \text{(Lemma I.1.11(xi))} \\ &\vdash f && \text{(MP)} \end{aligned}$$

This contradiction shows that $\mathcal{K}$ is consistent. According to the Model Existence Theorem, there exists a model for $\mathcal{K}$ in which $\neg f$ is true and f is false. Then f cannot be a tautology. Thus $\mathcal{P}^=$ is complete. □

Remark I.4.7. Attention: The Completeness Theorem does not state that $\mathcal{P}^=$ is complete with respect to every interpretation (cf. Theorem I.7.6).

Theorem I.4.8 (Compactness Theorem[13])**.** *A set M of formulas in a first-order calculus with equality*

[12] The axiom of choice is required to show that U is indeed a set, see Lemma II.2.3.

[13] also called *finiteness theorem*

has a model if every finite subset of M has a model.

Proof. If M has no model, then M is inconsistent according to the Model Existence Theorem. A contradiction with axioms from M can already be derived from finitely many such axioms. Therefore, a certain finite subset of M also cannot have a model. Contradiction. □

Corollary I.4.9. *In $\mathcal{P}^=$, it cannot be expressed when a universe is finite.*

Proof. Assume there exists a formula f in $\mathcal{P}^=$ that is true in an arbitrary interpretation (U, I) if and only if U is finite. We can extend $\mathcal{P}$ by 1-ary predicates $P_1, P_2, \ldots$ that do not occur in f. The formula

$$f_n := \exists x_1 P_1 \wedge \exists x_2 (P_2 \wedge \neg P_1) \wedge \ldots \wedge \exists x_n (P_n \wedge \neg P_{n-1} \wedge \ldots \wedge \neg P_1)$$

is true in (I, U) only if U has at least n elements. Let M be the (infinite) set of formulas $f, f_1, f_2, \ldots$. For every finite subset N of M, there exists an n with $f_m \notin N$ for all $m \geq n$. If U has exactly n elements, then (U, I) is a model of N. According to the Compactness Theorem, M also has a model (U, I). Because of $I(f) = \mathbf{t}$, U is finite. If U had exactly n elements, then $I(f_{n+1}) = \mathbf{f}$ would hold. Contradiction. □

Remark I.4.10. In *second*-order predicate logic $\mathcal{P}^2$ (with equality), formulas of the form $\forall P \ldots$ and $\forall \varphi \ldots$ for predicates P and functions φ are allowed. Let σ be a 1-ary function. The formulas

$$f := \forall x \forall y (\sigma(x) = \sigma(y) \Rightarrow x = y),$$
$$g := \forall x \exists y (\sigma(y) = x)$$

express whether σ is injective or surjective, respectively.[14] The formula $\forall \sigma (f \Rightarrow g)$ is true in an interpretation (U, I) if and only if every injective function $U \to U$ is surjective. As is well known, this is equivalent to the finiteness of U. Therefore, $\mathcal{P}^2$ can express more than $\mathcal{P}^1$. The proof of Corollary I.4.9 also shows that the model existence theorem is false in $\mathcal{P}^2$.

I.5. Peano Arithmetic

Remark I.5.1. We have already made implicit use of the natural numbers, for example in the notation $f_1, \ldots, f_n$. In this section, we introduce the natural numbers and their arithmetic axiomatically.

Definition I.5.2.

(i) *Peano Arithmetic* $\mathcal{PA}$ is a first-order predicate logic with equality and the following properties:

- Alphabet: variables $a, b, \ldots$, constant 0, symbols (,), $\neg$, $\Rightarrow$, $\forall$, $'$, $+$, $\cdot$ (no functions or predicates)
- Terms: variables and 0 are terms. If t, u are terms, then so are (t'), $(t + u)$ and $(t \cdot u)$.
- Formulas: If t and u are terms, then $t = u$ is a formula. For formulas f, g and every variable x, $\neg f$, $f \Rightarrow g$ and $\forall x f$ are also formulas.

[14] See Definition II.2.5

- Axioms: For variables x, y and formulas f, g, h, the following hold:

$$f \Rightarrow (g \Rightarrow f) \qquad (\mathcal{A}_1)$$
$$(\neg f \Rightarrow \neg g) \Rightarrow (g \Rightarrow f) \qquad (\mathcal{A}_2)$$
$$(f \Rightarrow (g \Rightarrow h)) \Rightarrow ((f \Rightarrow g) \Rightarrow (f \Rightarrow h)) \qquad (\mathcal{A}_3)$$
$$\forall x(f \Rightarrow g) \Rightarrow (f \Rightarrow (\forall x g)) \quad \text{if } x \text{ does not occur free in } f \qquad (\mathcal{P}_1)$$
$$\forall x f \Rightarrow f(x \leftarrow t) \quad \text{if collision-free} \qquad (\mathcal{P}_2)$$
$$x = x \qquad (\mathcal{P}_1^=)$$
$$(x = y) \Rightarrow (f(y \leftarrow x) \Rightarrow f) \quad \text{if collision-free} \qquad (\mathcal{P}_2^=)$$
$$\neg((x') = 0), \qquad (\Sigma_1)$$
$$(x') = (y') \Rightarrow x = y, \qquad (\Sigma_2)$$
$$(x + 0) = x, \qquad (+_1)$$
$$(x + (y')) = ((x + y)'), \qquad (+_2)$$
$$(x \cdot 0) = 0, \qquad (\times_1)$$
$$(x \cdot (y')) = ((x \cdot y) + x), \qquad (\times_2)$$
$$f(x \leftarrow 0) \Rightarrow \big(\forall x(f(x) \Rightarrow f(x')) \Rightarrow \forall x f\big) \qquad (\mathcal{I})$$

- Rules of inference: (MP) and (G).

(ii) The *standard interpretation* (U, I) uses the universe of natural numbers $U = \mathbb{N} = \{0, 1, \ldots\}$. Obviously, 0 is interpreted as zero, $+$ as addition and $\cdot$ as multiplication. Furthermore, let $x' := x + 1$ be the successor function as in Example I.3.8. We write $\vDash_{\mathbb{N}} f$, if a formula f is true with respect to $(\mathbb{N}, I)$.

Remark I.5.3.

(i) Instead of the symbols $'$, $+$ and $\cdot$, one could also introduce 1- or 2-ary functions. However, the symbol notation is more economical. It is easy to see that the (proof of) Lemma I.3.13 remains correct for these "functions". In particular, the converse of (Σ_2) holds, i. e. $\vdash x = y \Rightarrow x' = y'$.

(ii) As before, we use the abbreviations $\wedge$, $\vee$, $\Leftrightarrow$, $\exists$ and $\neq$. To save parentheses, we agree that $'$ binds more strongly than all other symbols. Additionally, $\cdot$ shall bind more strongly than $+$ (multiplication before addition) and $\cdot$, $+$ bind more strongly than $=$ and $\Rightarrow$. Thus, (Σ_1) has the form $x' \neq 0$ and $((x \cdot y) + (z')) = 0$ shortens to $x \cdot y + z' = 0$.

(iii) Axiom (Σ_1) states that 0 has no predecessor. According to (Σ_2), the successor function is injective. Addition and multiplication are defined recursively for all natural numbers by $(+_1)$, $(+_2)$, $(\times_1)$ and $(\times_2)$. The usual calculation rules are proven in Lemma I.5.5. Axiom $(\mathcal{I})$ describes the (already used) principle of mathematical induction.

(iv) It is easy to see that the standard interpretation of $\mathcal{PA}$ is a model. In particular, $\mathcal{PA}$ is consistent. However, if one wants to use $\mathcal{PA}$ to define $\mathbb{N}$, then this model is not available. We will return to this in Remark I.7.8.

(v) It is natural to introduce the abbreviations $1 := 0'$, $2 := 1'$ etc. To be able to distinguish between variables and constants, let $\overline{n}$ be the constant in $\mathcal{PA}$ that corresponds to the natural number $n \in \mathbb{N}$.

Example I.5.4. It holds that

$$\begin{aligned}
&\vdash 1+0=1 && (+_1)\\
&\vdash (1+0)'=2 && \text{(Lemma I.3.13)}\\
&\vdash 1+0'=(1+0)' && (+_2)\\
&\vdash 1+1=2 && \text{(Lemma I.3.12)}
\end{aligned}$$

In the *Principia Mathematica* by Whitehead-Russell, this formula is proven after over 300 pages of formal argumentation.

Lemma I.5.5. *For all terms t, u, v in $\mathcal{PA}$ it holds that*

(i) $\vdash 0+t=t$

(ii) $\vdash t'+u=(t+u)'$

(iii) $\vdash t+u=u+t$ *(commutativity)*

(iv) $\vdash u=v\Rightarrow t+u=t+v$

(v) $\vdash t+(u+v)=(t+u)+v$ *(associativity)*

(vi) $\vdash t\cdot u=u\cdot t$ *(commutativity)*

(vii) $\vdash t\cdot(u\cdot v)=(t\cdot u)\cdot v$ *(associativity)*

(viii) $\vdash t\cdot(u+v)=t\cdot u+t\cdot v$ *(distributivity)*

Proof. Since none of the formulas contain quantifiers, we can assume by (S) that t, u and v are variables.

(i) For $f:=(0+t=t)$ it holds that

$$\begin{aligned}
&\vdash f(0) && (+_1)\\
&\vdash f(0)\Rightarrow\big(\forall t(f(t)\Rightarrow f(t'))\Rightarrow\forall t f\big) && (\mathcal{I})\\
&\vdash \forall t(f(t)\Rightarrow f(t'))\Rightarrow\forall t f && \text{(MP)}\\
&\vdash f\Rightarrow(0+t)'=t' && \text{(Lemma I.3.13)}\\
&\vdash 0+t'=(0+t)' && (+_2,\text{S})\\
&\vdash f\Rightarrow f(t') && \text{(Lemma I.3.12)}\\
&\vdash \forall t\big(f(t)\Rightarrow f(t')\big) && \text{(G)}\\
&\vdash f && (\text{MP},\mathcal{P}_2')
\end{aligned}$$

(ii) For $f(u) := (t' + u = (t + u)')$ it holds that

$$\begin{aligned}
&\vdash t + 0 = t && (+_1)\\
&\vdash (t + 0)' = t' && \text{(Lemma I.3.13)}\\
&\vdash t' + 0 = t' && \text{(Remark I.3.4)}\\
&\vdash f(0) && \text{(Lemma I.3.12)}\\
&\vdash \forall u(f(u) \Rightarrow f(u')) \Rightarrow \forall u f && ((\mathcal{I}), \text{(MP)})\\
&\vdash t' + u' = (t' + u)' && ((+_2), \text{Remark I.3.4})\\
&\vdash f(u) \Rightarrow (t' + u)' = (t + u)'' && \text{(Lemma I.3.13)}\\
&\vdash f(u) \Rightarrow t' + u' = (t + u)'' && \text{(Lemma I.3.12)}\\
&\vdash t + u' = (t + u)' && (+_2)\\
&\vdash (t + u')' = (t + u)'' && \text{(Lemma I.3.13)}\\
&\vdash f(u) \Rightarrow t' + u' = (t + u')' && \text{(Lemma I.3.12)}\\
&\vdash \forall u(f(u) \Rightarrow f(u')) && \text{(G)}\\
&\vdash f && (\text{(MP)}, \text{Remark I.3.4})
\end{aligned}$$

(iii) For $f(u) := (t + u = u + t)$ it holds that

$$\begin{aligned}
&\vdash f(0) && ((+_1), \text{(i)}, \text{Lemma I.3.12})\\
&\vdash f(0) \Rightarrow \big(\forall u(f(u) \Rightarrow f(u')) \Rightarrow \forall u f\big) && (\mathcal{I})\\
&\vdash f \Rightarrow (t + u)' = (u + t)' && \text{(Lemma I.3.13)}\\
&\vdash t + u' = (t + u)' && (+_2)\\
&\vdash u' + t = (u + t)' && \text{(ii)}\\
&\vdash f \Rightarrow t + u' = u' + t && \text{(Lemma I.3.13)}\\
&\vdash \forall u(f(u) \Rightarrow (f(u'))) && \text{(G)}\\
&\vdash f && (\text{(MP)}, \text{(I.3.4)})
\end{aligned}$$

(iv) Here one can manage without $(\mathcal{I})$. For $f(u) := (t + u = t + v)$ it holds that

$$\begin{aligned}
&\vdash u = v \Rightarrow (f(v \leftarrow u) \Rightarrow f) && (\mathcal{P}_2^=)\\
&\vdash (u = v \Rightarrow (t + v = t + v \Rightarrow f)) \Rightarrow ((u = v \Rightarrow t + v = t + v) \Rightarrow (u = v \Rightarrow f)) && (\mathcal{A}_3)\\
&\vdash (u = v \Rightarrow t + v = t + v) \Rightarrow (u = v \Rightarrow f) && \text{(MP)}\\
&\vdash t + v = t + v && \text{(Lemma I.3.12)}\\
&\vdash u = v \Rightarrow t + v = t + v && ((\mathcal{A}_1), \text{(MP)})\\
&\vdash u = v \Rightarrow f && \text{(MP)}
\end{aligned}$$

(v) For $f(v) := (t + (u + v) = (t + u) + v)$ it holds that

$$\begin{aligned}
&\vdash u + 0 = u && (+_1)\\
&\vdash t + (u + 0) = t + u && \text{(iv)}\\
&\vdash (t + u) + 0 = t + u && ((+_1), \text{(S)})\\
&\vdash f(0) && \text{(Lemma I.3.12)}\\
&\vdash \forall v(f(v) \Rightarrow f(v')) \Rightarrow \forall v f && ((\mathcal{I}), \text{(MP)})\\
&\vdash f(v) \Rightarrow (t + (u + v))' = ((t + u) + v)' && \text{(Lemma I.3.13)}\\
&\vdash u + v' = (u + v)' && (+_2)\\
&\vdash t + (u + v') = t + (u + v)' && \text{(iv)}\\
&\vdash t + (u + v)' = (t + (u + v))' && (+_2)\\
&\vdash (t + u) + v' = ((t + u) + v)' && ((+_2), \text{Remark I.3.4})\\
&\vdash f(v) \Rightarrow t + (u + v') = (t + u) + v' && \text{(Lemma I.3.12)}\\
&\vdash \forall v(f(v) \Rightarrow f(v')) && \text{(G)}\\
&\vdash f && (\text{(MP)}, \text{Remark I.3.4})
\end{aligned}$$

(vi),(vii) Exercise I.14.

(vi) For $f(v) := ((t + u) \cdot v = t \cdot v + u \cdot v)$ it holds that

$$\begin{aligned}
&\vdash (u + u) \cdot 0 = 0 && (\times_1)\\
&\vdash t \cdot 0 + u \cdot 0 = 0 && ((\times_1), (+_1))\\
&\vdash f(0) && \text{(Lemma I.3.12)}\\
&\vdash \forall v(f(v) \Rightarrow f(v')) \Rightarrow \forall v f && ((\mathcal{I}), \text{(MP)})\\
&\vdash f(v) \Rightarrow (t + u) \cdot v + (t + u) = (t \cdot v + u \cdot v) + (t + u) && \text{(iv)}\\
&\vdash (t + u) \cdot v' = (t + u) \cdot v + (t + u) && (\times_2)\\
&\vdash (t \cdot v + u \cdot v) + (t + u) = (t \cdot v + t) + (u \cdot v + u) && (\text{(v)}, \text{(iii)})\\
&\vdash (t \cdot v + t) + (u \cdot v + u) = (t \cdot v') + (u \cdot v') && (\text{(iv)}, (\times_2))\\
&\vdash f(v) \Rightarrow f(v') && \text{(Lemma I.3.12)}\\
&\vdash f && (\text{(G)}, \text{(MP)}, \text{Remark I.3.4})
\end{aligned}$$

□

I.6. Representability

Remark I.6.1. In predicate logic, predicates are interpreted as relations. As a replacement for the predicates missing in $\mathcal{PA}$, we will define formulas that correspond to relations and functions on $\mathbb{N}^k$. If $R \subseteq \mathbb{N}^k$ is a relation, we write $R(x_1, \ldots, x_n)$ for the statement $(x_1, \ldots, x_n) \in R$. In the case $k = 2$, one usually defines a separate symbol such as $\sim$ and writes $x \sim y$ if $(x, y) \in R$.

Definition I.6.2.

- A relation $R \subseteq \mathbb{N}^n$ is *represented* by a formula f in $\mathcal{PA}$ if for all $x_1, \ldots, x_n \in \mathbb{N}$: $R(x_1, \ldots, x_n)$ if and only if $\vDash_{\mathbb{N}} f(\overline{x_1}, \ldots, \overline{x_n})$.

- A function $\varphi\colon \mathbb{N}^n \to \mathbb{N}$ is *represented* by a formula f if the corresponding relation is represented by f, i. e. for all $x_1, \dots, x_n \in \mathbb{N}$, $\varphi(x_1, \dots, x_n) = y$ if and only if $\vDash_{\mathbb{N}} f(\overline{x_1}, \dots, \overline{x_n}, \overline{y})$.

If one is only interested in the existence of f, one says R or φ are *representable*.

Example I.6.3.

(i) The equality relation $=$ is represented by definition by the formula $f(x, y) := (x = y)$. The successor function $x \mapsto x + 1$ is represented by $x' = y$. Analogously, addition and multiplication are represented by their corresponding symbols.

(ii) In Example I.3.8, we had defined the less-than relation as a predicate. Here it is represented by the formulas

$$x \leq y := \exists z(x + z = y) \qquad x < y := \exists z(x + z' = y).$$

(iii) The divisibility relation can be represented by

$$x \mid y := \exists z(x \cdot z = y).$$

(iv) When attempting to represent the power function $\varphi(x, y) := x^y$, one encounters the problem of representing recursive calls such as $x^y = x^{y-1} \cdot x$. For this, we need tools.

Lemma I.6.4 (Gödel's $\boldsymbol{\beta}$-function)**.** *There exists a representable function $\boldsymbol{\beta}\colon \mathbb{N}^3 \to \mathbb{N}$ with the following property: For $k, n_0, \dots, n_k \in \mathbb{N}$, there exist $a, b \in \mathbb{N}$ with $\boldsymbol{\beta}(a, b, i) = n_i$ for $i = 0, \dots, k$.*

Proof. We define $\boldsymbol{\beta}$ directly via the following formula

$$\boldsymbol{\beta}(a, b, x) = y \iff \vDash_{\mathbb{N}} \big(\overline{y} < (1 + \overline{x}' \cdot \overline{b})\big) \wedge \exists c\big(\overline{y} + c \cdot (1 + \overline{x}' \cdot \overline{b}) = \overline{a}\big).$$

The right side describes y as the smallest non-negative remainder in the division of a by $1 + (x + 1)b$. In particular, $\boldsymbol{\beta}$ is well-defined and representable.

To show that $\boldsymbol{\beta}$ has the desired property, let $r := \max(k, n_0, n_1, \dots, n_k)$ and $b := r!$ (factorial[15]). For $i = 0, \dots, k$ let $d_i := 1 + (i + 1)b$. Suppose there exists a common prime divisor p of d_i and d_j with $i \neq j$. Then p also divides $d_i - d_j = b(i - j)$. In the case $p \mid b$ it would follow that $p \nmid d_i$. Since p is a prime number, $p \mid i - j$ must hold. But then $p \leq k$ and $p \mid k! \mid r! = b$, which we had already excluded. Therefore $d_0, \dots, d_k$ are pairwise coprime. According to the Chinese Remainder Theorem[16] there exists an $a \in \mathbb{N}$ with $n_i \equiv a \pmod{d_i}$ for $i = 0, \dots, k$. By definition $n_i \leq r \leq b < d_i$. This shows $\boldsymbol{\beta}(a, b, i) = n_i$ for $i = 0, \dots, k$. □

Definition I.6.5. For $x_1, \dots, x_n \in \mathbb{N}$ we write $\vec{x} := (x_1, \dots, x_n) \in \mathbb{N}^n$. A function $\alpha\colon \mathbb{N}^n \to \mathbb{N}$ is called (*primitive*) *recursive*, if it has one of the following forms:

- $n = 1$ and $\alpha = \zeta$ with $\zeta(x) = 0$ for all $x \in \mathbb{N}$ (*zero function*).
- $n = 1$ and $\alpha = \alpha_\prime$ with $\alpha_\prime(x) = x + 1$ for all $x \in \mathbb{N}$ (successor function).
- $\alpha = \pi^n_k$ with $\pi^n_k(\vec{x}) = x_k$ for a fixed $1 \leq k \leq n$ (k-th *projection*).
- $\alpha(\vec{x}) = \beta\big(\gamma_1(\vec{x}), \dots, \gamma_k(\vec{x})\big)$ for recursive functions $\beta\colon \mathbb{N}^k \to \mathbb{N}$ and $\gamma_1, \dots, \gamma_k\colon \mathbb{N}^n \to \mathbb{N}$ (*composition*).

[15] See Definition II.5.6
[16] See Number Theory Notes

- $n \geq 2$ and
$$\alpha(\vec{x}) = \begin{cases} \beta(x_2, \ldots, x_n) & \text{if } x_1 = 0 \\ \gamma\big(\alpha(x_1 - 1, x_2, \ldots, x_n), x_1 - 1, x_2, \ldots, x_n\big) & \text{if } x_1 > 0 \end{cases}$$
with recursive functions $\beta\colon \mathbb{N}^{n-1} \to \mathbb{N}$ and $\gamma\colon \mathbb{N}^{n+1} \to \mathbb{N}$ (*recursion*).

Example I.6.6.

(i) If $1 \leq i_1, \ldots, i_k \leq n$ are arbitrary indices and $\varphi\colon \mathbb{N}^k \to \mathbb{N}$ is recursive, then so is
$$\psi(\vec{x}) := \varphi(x_{i_1}, \ldots, x_{i_k}) = \varphi\big(\pi^n_{i_1}(\vec{x}), \ldots \pi^n_{i_k}(\vec{x})\big).$$
We can therefore permute, add, or remove parameters without hesitation (especially in the recursion rule).

(ii) The zero function ζ^n in n variables is obtained recursively by $\zeta^1 := \zeta$ and
$$\zeta^{n+1}(x_0, \ldots, x_n) = \begin{cases} \zeta^n(\vec{x}) & \text{if } x_0 = 0, \\ \zeta^n(x_0 - 1, x_2, \ldots, x_n) & \text{if } x_0 > 0 \end{cases}$$
(note (i)). By composition with the successor function, one obtains the constant functions
$$\kappa^n_c(\vec{x}) := c$$
for a fixed $c \in \mathbb{N}$. In the following, we will therefore substitute constants directly instead of κ.

(iii) The identity[17] $\mathbb{N} \to \mathbb{N}$, $x \mapsto x$ is realized by π^1_1.

(iv) Addition $\alpha_+(x, y) = x + y$ is recursive, because
$$\alpha_+(x, y) = \begin{cases} y & \text{if } x = 0, \\ \alpha_\prime(\alpha_+(x - 1, y)) & \text{if } x > 0. \end{cases}$$

(v) Multiplication $\alpha_\times(x, y) = x \cdot y$ is recursive, because
$$\alpha_\times(x, y) = \begin{cases} 0 & \text{if } x = 0, \\ \alpha_+\big(\alpha_\times(x - 1, y), y\big) & \text{if } x > 0. \end{cases}$$

(vi) The power function $\alpha_\wedge(x, y) = y^x$ is recursive, because
$$\alpha_\wedge(x, y) = \begin{cases} 1 & \text{if } x = 0, \\ \alpha_\times\big(\alpha_\wedge(x - 1, y), y\big) & \text{if } x > 0. \end{cases}$$

(vii) The factorial $\alpha_!(x) = x! = 1 \cdot 2 \cdot \ldots \cdot x$ is recursive, because
$$\alpha_!(x) = \begin{cases} 1 & \text{if } x = 0, \\ \alpha_\times(\alpha_!(x - 1), x) & \text{if } x > 0. \end{cases}$$
For better readability, we will from now on use the terms $x + y$, $x \cdot y = xy$, x^y and $x!$ in the usual form.

[17] See Example II.2.6

(viii) The predecessor function $\sigma_-(x) := \begin{cases} x-1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \end{cases}$ is recursive. For this, we first define

$$\tau(x,y) := \begin{cases} 0 & \text{if } x = 0 \\ x-1 & \text{if } x > 0 \end{cases}$$

and then $\sigma_-(x) = \tau(x,0)$.

(ix) The truncated subtraction $\alpha_-(x,y) := \begin{cases} y-x & \text{if } x < y \\ 0 & \text{otherwise} \end{cases}$ is recursive, because

$$\alpha_-(x,y) := \begin{cases} y & \text{if } x = 0 \\ \sigma_-\big(\alpha_-(x-1,y)\big) & \text{if } x > 0. \end{cases}$$

Thus, the absolute difference function

$$|x-y| := \alpha_-(x,y) + \alpha_-(y,x)$$

also becomes recursive.

(x) The functions

$$\overline{\operatorname{sgn}}(x) := \alpha_-(x,1) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x > 0 \end{cases}$$

$$\operatorname{sgn}(x) := \overline{\operatorname{sgn}}(\overline{\operatorname{sgn}}(x)) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x > 0 \end{cases}$$

are recursive. One calls sgn the *signum function*.

Definition I.6.7. A relation $R \subseteq \mathbb{N}^n$ is called (*primitive*) *recursive*, if a recursive function $\chi_R \colon \mathbb{N}^n \to \mathbb{N}$ with

$$R(\vec{x}) \iff \chi_R(\vec{x}) = 0 \qquad (\vec{x} \in \mathbb{N}^n)$$

exists.

Remark I.6.8.

(i) One calls χ_R a *characteristic* function of R. By composition with the recursive signum function sgn, one can assume that χ_R is *normalized*, i.e., it takes the value 1 outside of R. Thereby χ_R is uniquely determined.

(ii) If $R, S \subseteq \mathbb{N}^n$ are recursive relations, then so are $\neg R := \mathbb{N}^n \setminus R$, $R \cup S$ and $R \cap S$ with characteristic functions $\overline{\operatorname{sgn}} \circ \chi_R$,[18] $\chi_R \chi_S$ and $\chi_R + \chi_S$ respectively.

(iii) If $R \subseteq \mathbb{N}^n$ and $\varphi_1, \ldots, \varphi_n \colon \mathbb{N} \to \mathbb{N}$ are recursive, then so is the relation

$$S(\vec{x}) := R\big(\varphi_1(x_1), \ldots, \varphi_n(x_n)\big),$$

with characteristic function $\chi_S(\vec{x}) = \chi_R\big(\varphi_1(x_1), \ldots, \varphi_n(x_n)\big)$.

[18] See Definition II.2.5

(iv) From now on we use the abbreviations popular in mathematics

$$\forall x < y\, f := \forall x(x < y \Rightarrow f),$$
$$\exists x < y\, f := \exists x(x < y \wedge f)$$

and their variants with $\leq$, $>$ and $\geq$.

Theorem I.6.9. *Every recursive function and every recursive relation is representable in $\mathcal{PA}$.*

Proof. The zero function ζ is represented by the formula $f(x, y) := (y = 0)$. We have already represented the successor function in Example I.6.3. The k-th projection π^n_k is represented by $x_k = y$. Let $\beta, \gamma_1, \ldots, \gamma_k$ be recursively represented by formulas $b, c_1, \ldots, c_k$. Then the composition $\alpha(\vec{x}) = \beta(\gamma_1(\vec{x}), \ldots, \gamma_k(\vec{x}))$ is represented by

$$f(x, y) := \exists y_1 \ldots \exists y_k\big(c_1(\vec{x}, y_1) \wedge \ldots \wedge c_k(\vec{x}, y_k) \wedge b(y_1, \ldots, y_k, y)\big).$$

Finally, let α be obtained via recursion from σ and ρ, which are represented by s and t respectively. Let Gödel's $\boldsymbol{\beta}$-function from Lemma I.6.4 be represented by the formula g. For all $x_1, \ldots, x_n \in \mathbb{N}$ there exist $a, b \in \mathbb{N}$ with $\boldsymbol{\beta}(a, b, i) = \alpha(i, x_2, \ldots, x_n)$ for $i = 0, \ldots, x_1$. Thus there exist $y_1, y_2 \in \mathbb{N}$ with

$$\vDash_{\mathbb{N}} g(\overline{a}, \overline{b}, \overline{x}', \overline{y_1}) \wedge g(\overline{a}, \overline{b}, \overline{x}, \overline{y_2}) \wedge t(\overline{y_2}, \overline{x}, \overline{x_2}, \ldots, \overline{x_n}, \overline{y_1})$$

for $x < x_1$. So α is represented by

$$f(x, y) := \exists a \exists b\Big(\exists y_0\big(g(a, b, 0, y_0) \wedge s(x_2, \ldots, x_n, y_0)\big) \wedge g(a, b, x_1, y)\Big)$$
$$\wedge \forall x < x_1 \exists y_1\Big(g(a, b, x', y_1) \wedge \exists y_2\big(g(a, b, x, y_2) \wedge t(y_2, x_2, \ldots, x_n, y_1)\big)\Big)$$

By induction, it follows that every primitive recursive function is representable.

Now let $R \subseteq \mathbb{N}^n$ be a recursive relation with characteristic function χ. Then there exists a formula f with

$$R(\vec{x}) \iff \chi(\vec{x}) = 0 \iff \vDash_{\mathbb{N}} f(\overline{x_1}, \ldots, \overline{x_n}, 0).$$

Thus R is represented by the formula $f(\vec{x}, 0)$. □

Lemma I.6.10. *Let $R \subseteq \mathbb{N}^{n+1}$ be a recursive relation and $\gamma\colon \mathbb{N} \to \mathbb{N}$ a recursive function. Then the following relations and functions respectively are recursive:*

(i) $R_\forall(x_0, \vec{x}) \iff \forall y \leq \gamma(x_0)\, R(y, \vec{x})$

(ii) $R_\exists(x_0, \vec{x}) \iff \exists y \leq \gamma(x_0)\, R(y, \vec{x})$

(iii) $\varphi(x_0, \vec{x}) = \begin{cases} 0 & \text{if } (y, \vec{x}) \notin R \text{ for all } y \leq \gamma(x_0), \\ \min\limits_{y \leq \gamma(x_0)} R(y, \vec{x}) & \text{otherwise} \end{cases}$

Proof. Let χ_R be a characteristic function of R.

(i) We first assume that $\gamma = \pi^1_1$ is the identity. Then

$$\lambda(x_0, \vec{x}) := \begin{cases} \chi_R(0, \vec{x}) & \text{if } x_0 = 0, \\ \lambda(x_0 - 1, \vec{x}) + \chi_R(x_0, \vec{x}) & \text{if } x_0 > 0 \end{cases}$$

is a recursive characteristic function of $R_\forall$. The general case is obtained by composition $\chi_\forall(x_0, \vec{x}) := \lambda(\gamma(x_0), \vec{x})$.

(ii) The proof proceeds analogously with

$$\lambda(x_0, \vec{x}) := \begin{cases} \chi_R(0, \vec{x}) & \text{if } x_0 = 0, \\ \lambda(x_0 - 1, \vec{x})\chi_R(x_0, \vec{x}) & \text{if } x_0 > 0. \end{cases}$$

(iii) The recursive function

$$\delta(s, t, u) := \operatorname{sgn}(\overline{\operatorname{sgn}}(s)\overline{\operatorname{sgn}}(t)u)$$

is 1 if and only if $s = t = 0 < u$ and 0 otherwise. Thus

$$\tau(y, \vec{x}) := \begin{cases} 0 & \text{if } y = 0, \\ \delta\big(\tau(y-1, \vec{x}), \chi_R(y, \vec{x}), \chi_R(y-1, \vec{x})\big)y & \text{if } y > 0 \\ \quad + \overline{\operatorname{sgn}}\big(\delta(\tau(y-1, \vec{x}), \chi_R(y, \vec{x}), \chi_R(y-1, \vec{x}))\big)\tau(y-1, \vec{x}) & \end{cases}$$

is recursive. The expression $\delta(\tau(y-1, \vec{x}), \chi_R(y, \vec{x}), \chi_R(y-1, \vec{x}))$ determines the smallest y for which $R(y, \vec{x})$ is satisfied. The second summand of the formula guarantees that τ no longer changes for larger y. Thus $\varphi(x_0, \vec{x}) = \tau(\gamma(x_0), \vec{x})$ is recursive. □

Lemma I.6.11. *The following relations and functions are recursive and thus representable in $\mathcal{PA}$:*

(i) $x = y$, $x < y$, $x \mid y$

(ii) $\Pr(x) \iff x$ *is a prime number*

(iii) $\rho(n) = n$*-th prime number in* $\mathbb{N}$ ($\rho(0) = 2$, $\rho(1) = 3$ *etc.*)

(iv) $\lambda(x) = \max_k(\rho(k) \mid x)$ *for* $x > 0$

(v) $\epsilon(x, k) = \max_r(\rho(k)^r \mid x)$ *for* $x > 0$

(vi) $\mu(x, k, e) = x\rho(k)^{e-\epsilon(k,x)}$ *for* $x > 0$ (*the exponent of* $\rho(k)$ *in the prime factorization of* x *is replaced by* e)

Proof.

(i) Although we already know from Example I.6.3 that these relations are representable, we must nevertheless prove recursiveness for later applications. Obviously, $|x-y|$ is a recursive characteristic function of $x = y$. The function $\overline{\operatorname{sgn}}(\alpha_-(x, y))$ serves as the characteristic function for $x < y$. Because of

$$x \mid y \iff \exists z \leq y(xz = y)$$

$x \mid y$ is recursive by Lemma I.6.10.[19]

(ii) x is a prime number if and only if

$$x > 1 \wedge \forall y \leq x(y \mid x \Rightarrow (y = 1 \vee y = x)).$$

Obviously, $x > 1$, $y = 1$ and $y = x$ are recursive relation. By (i) and Remark I.6.8, $y \mid x \Rightarrow (y = 1 \vee y = x)$ is recursive. By Lemma I.6.10, Pr is also recursive.

[19]The term $z \leq y$ merely serves to satisfy the requirement of Lemma I.6.10.

(iii) We first define the recursive function

$$\gamma(x) := \begin{cases} 2 & \text{if } x = 0, \\ \gamma(x-1)! + 1 & \text{otherwise.} \end{cases}$$

Certainly $\rho(0) \leq \gamma(0)$. Let $\rho(n) \leq \gamma(n)$ be already shown inductively. Since $\rho(0)\rho(1)\dots\rho(n)+1$ is not divisible by any of the prime numbers $\rho(0), \dots, \rho(n)$, it holds that $\rho(n+1) \leq \rho(n)! + 1 \leq \gamma(n)! + 1 = \gamma(n+1)$.[20] By Lemma I.6.10,

$$\tau(x,y) := \begin{cases} 2 & \text{if } x = 0 \\ \min\limits_{z \leq \gamma(x)} (z > y \wedge \Pr(z)) & \text{if } n > 0 \end{cases}$$

is recursive. Therefore, so is

$$\rho(x) = \begin{cases} 2 & \text{if } x = 0, \\ \tau(x, \rho(x-1)) & \text{if } x > 0. \end{cases}$$

(iv) For $\rho(k) \mid x$ and $x > 0$, it holds that $k \leq \rho(k) \leq x$. By (iii), Remark I.6.8 and Lemma I.6.10, the relation

$$S(x,y) \;:\Longleftrightarrow\; x = 0 \vee \forall k \leq x \big(k \leq y \vee \rho(k) \nmid x\big)$$

is recursive. Thus, so is $\lambda(x) = \min_{y \leq x} S(x,y)$ (the values $\lambda(0) = \lambda(1) = 0$ are irrelevant).

(v) For $x, k \in \mathbb{N}$, it holds that $x < 2^x \leq \rho(k)^x$ and therefore $\rho(k)^x \nmid x$ provided $x > 0$. The relation

$$R(x,y,z) \iff x = 0 \vee \rho(z)^{y+1} \nmid x$$

is recursive by Example I.6.6 and Remark I.6.8. Thus, so is $\epsilon(x,k) = \min_{y \leq x} R(x,y,k)$ (with $\epsilon(0,k) = 0$).

(vi) According to the statements already proven,

$$\mu(x,k,e) = \Big(\min_{y \leq x} \big(y\rho(k)^{\epsilon(x,k)} = x\big)\Big)\rho(k)^e$$

is recursive (with $\mu(0,k,e) = 0$). □

Remark I.6.12. With Lemma I.6.11, recursions can be defined more flexibly by considering not only the direct predecessor $\alpha(x_1 - 1, x_2, \dots, x_n)$, but several predecessors. We illustrate this using the *Fibonacci function* $\varphi\colon \mathbb{N} \to \mathbb{N}$ with $\varphi(0) = \varphi(1) = 1$ and $\varphi(n+1) = \varphi(n) + \varphi(n-1)$ for $n > 0$. According to Lemma I.6.11,

$$\tau(x) := \begin{cases} 6 & \text{if } x = 0, \\ 2^{\epsilon(\tau(x-1),1)} \cdot 3^{\epsilon(\tau(x-1),0)+\epsilon(\tau(x-1),1)} & \text{if } x > 0 \end{cases}$$

is recursive. We define $\varphi(x) := \epsilon(\tau(x), 0)$. Then it holds that

$$\begin{aligned} \varphi(0) &= \epsilon(6,0) = 1, \\ \varphi(1) &= \epsilon(\tau(0),1) = 1, \\ \varphi(n+1) &= \epsilon(\tau(n),1) = \epsilon(\tau(n-1),0) + \epsilon(\tau(n-1),1) = \varphi(n-1) + \epsilon(\tau(n),0) = \varphi(n-1) + \varphi(n) \end{aligned}$$

as desired.

[20] By Bertrand's postulate, $\rho(n+1) \leq 2\rho(n)$ already holds. Thus, $\mu(n) = 2^{n+1}$ would suffice. See Number Theory notes.

I.7. Gödel's Incompleteness Theorems

Remark I.7.1. It clearly holds that $\mathcal{PA}$ is negation-incomplete, because one can prove neither $x = 0$ nor $x \neq 0$ (both formulas are false in the standard interpretation, cf. Exercise I.15). Gödel's first incompleteness theorem implies that there are even closed formulas with this property. In particular, $\mathcal{PA}$ is incomplete. Gödel's idea was to arithmetically express a formula f with the meaning "f is not provable". If f were false, then one could prove f and $\mathcal{PA}$ would be inconsistent. Consequently, f must be true and thus unprovable. In order to be able to speak arithmetically about formulas, one encodes them by numbers as follows.

Definition I.7.2. The elements of the alphabet of $\mathcal{PA}$ are called *symbols* in the following. They are numbered with odd numbers:

Symbol s	(	)	$\neg$	$\Rightarrow$	$\forall$	$'$	$+$	$\cdot$	$=$	0	x	y	z	$\cdots$
Number $\#s$	1	3	5	7	9	11	13	15	17	19	21	23	25	$\cdots$

Let $p_0, p_1, \ldots = 2, 3, \ldots$ be the prime numbers ($p_i = \rho(i)$ with the notation from Lemma I.6.11). For an arbitrary sequence $s = s_0 \ldots s_n$ of symbols of the alphabet, let

$$\ulcorner s \urcorner := p_0^{\#s_0} p_1^{\#s_1} \ldots p_n^{\#s_n}$$

be the *Gödel number* of s. If a proof B consists of formulas $f_0, \ldots, f_n$, then let

$$\ulcorner B \urcorner := p_0^{\ulcorner f_0 \urcorner} \ldots p_n^{\ulcorner f_n \urcorner}$$

be the *Gödel number* of B. We also say: $\ulcorner s \urcorner$ or $\ulcorner B \urcorner$ *encodes* s or B.

Example I.7.3. It holds that

$$\ulcorner \forall x(x + 0 = x) \urcorner = 2^9 3^{21} 5^1 7^{21} 11^{13} 13^{19} 17^{17} 19^{21} 23^3.$$

Remark I.7.4. As is well known, every positive natural number has a unique prime factorization. Since individual symbols have odd Gödel numbers, sequences of symbols have even Gödel numbers with odd prime exponents, and proofs have Gödel numbers with even prime exponents, each of these objects is uniquely determined by its Gödel number. Obviously, not every natural number encodes such an object (e. g. 18).

Lemma I.7.5. *The following functions and relations are representable in $\mathcal{PA}$:*

(i) $\varphi(x, y) = \begin{cases} \ulcorner st \urcorner & \text{if } x \text{ and } y \text{ encode symbol sequences } s \text{ and } t \text{ respectively} \\ 0 & \text{otherwise} \end{cases}$

(ii) $T(x) \iff x$ *is the Gödel number of a term*

(iii) $F(x) \iff x$ *is the Gödel number of a formula*

(iv) $V(x, y, k) \iff y$ *encodes a variable that occurs free at position k in f with $x = \ulcorner f \urcorner$*

(v) $\psi(x, y, z) = \begin{cases} \ulcorner f(w \leftarrow t) \urcorner & \text{if } x = \ulcorner f \urcorner \text{ (formula)}, y = \ulcorner w \urcorner \text{ (variable)} \\ & \text{and } z = \ulcorner t \urcorner \text{ (closed term)} \\ 0 & \text{otherwise} \end{cases}$

(vi) $B(x,y) \iff$ *x is the Gödel number of a proof of the formula with Gödel number y*

Proof.

(i) According to Lemma I.6.11, there are recursive functions that determine the prime factorization of a number. Therefore, one can represent when x and y are Gödel numbers of character strings s and t, respectively. Let us assume that this is the case. Furthermore, the largest prime divisor $\rho(k)$ of x can be determined with a recursive function. Using Lemma I.6.11, one can replace y by

$$\tilde{y} := p_{k+1}^{\epsilon(y,0)} p_{k+2}^{\epsilon(y,1)} \dots$$

Finally, one computes $\varphi(x,y) = x\tilde{y}$ recursively. As a recursive function, φ is representable according to Theorem I.6.9.

(ii) Every term t is built from a sequence of "sub-terms" $t_0, \dots, t_n$, such that $t_n = t$ and for each i one of the following statements holds:

- t_i is 0 or a variable
- t_i is (t_j') for some $j < i$
- t_i is $(t_j + t_k)$ or $(t_j \cdot t_k)$ for certain $j, k < i$

There exist $a, b \in \mathbb{N}$ with $\boldsymbol{\beta}(a,b,i) = \ulcorner t_i \urcorner$ for $i = 0, \dots, k$ (Lemma I.6.4). Obviously,

$$\begin{aligned} R_0(x) &\iff x \text{ encodes } 0 \iff x = 2^{19} \\ R_v(x) &\iff x \text{ encodes a variable} \iff x = 2^r \text{ with } r \geq 21 \text{ odd} \end{aligned}$$

are recursive relations. Due to (i), the following functions are representable:

$$\varphi_{\prime}(x) := \begin{cases} \ulcorner (s') \urcorner & \text{if } x \text{ encodes the character string } s \\ 0 & \text{otherwise} \end{cases}$$

$$\varphi_{+}(x,y) := \begin{cases} \ulcorner (s+t) \urcorner & \text{if } x,\ y \text{ encode the character strings } s \text{ and } t, \text{ respectively} \\ 0 & \text{otherwise} \end{cases}$$

$$\varphi_{\times}(x,y) := \begin{cases} \ulcorner (s \cdot t) \urcorner & \text{if } x,\ y \text{ encode the character strings } s \text{ and } t, \text{ respectively} \\ 0 & \text{otherwise} \end{cases}$$

It holds that

$$\begin{aligned} T(x) \iff \exists n \exists a \exists b \Big(& \boldsymbol{\beta}(a,b,n) = x \wedge \forall i \leq n \Big(R_0(\boldsymbol{\beta}(a,b,i)) \\ & \vee R_v(\boldsymbol{\beta}(a,b,i)) \vee \exists j < i \big(\varphi_{\prime}(\boldsymbol{\beta}(a,b,j)) = \boldsymbol{\beta}(a,b,i) \big) \\ & \vee \exists j < i \, \exists k < i \big(\varphi_{+}(\boldsymbol{\beta}(a,b,j), \boldsymbol{\beta}(a,b,k)) = \boldsymbol{\beta}(a,b,i) \big) \\ & \vee \exists j < i \, \exists k < i \big(\varphi_{\times}(\boldsymbol{\beta}(a,b,j), \boldsymbol{\beta}(a,b,k)) = \boldsymbol{\beta}(a,b,i) \big) \Big) \Big) \end{aligned}$$

Replacing R_v, $\boldsymbol{\beta}$ and the various φ therein by corresponding formulas (cf. proof of Theorem I.6.9), one obtains a formula that represents T.[21]

[21] One can show with a bit more effort that T is recursive. For this, one must show according to Lemma I.6.10 that n, a and b are bounded by a recursive function in x.

(iii) Similar to (ii), every formula f is built from "sub-formulas" $f_0, \dots, f_n$, such that $f_n = f$ and for each i one of the following statements holds:

- $i < n$ and f_i is a term
- f_i is $(f_j = f_k)$ for terms f_j, f_k with $j, k < i$
- f_i is $(\neg f_j)$ for some $j < i$ and f_j is not a term
- f_i is $(f_j \Rightarrow f_k)$ with $j, k < i$ and f_j, f_k are not terms
- f_i is $(\forall f_j f_k)$ with $j, k < i$, f_j is a variable and f_k not a term

The following functions are representable according to Lemma I.6.11:

$$\varphi_{=}(x,y) := \begin{cases} \ulcorner (s=t) \urcorner & \text{if } x \text{ and } y \text{ encode the character strings } s \text{ and } t \\ 0 & \text{otherwise} \end{cases}$$

$$\varphi_{\neg}(x) := \begin{cases} \ulcorner (\neg s) \urcorner & \text{if } x \text{ encodes the character string } s \\ 0 & \text{otherwise} \end{cases}$$

$$\varphi_{\Rightarrow}(x,y) := \begin{cases} \ulcorner (s \Rightarrow t) \urcorner & \text{if } x,\ y \text{ encode the character strings } s \text{ and } t, \text{ respectively} \\ 0 & \text{otherwise} \end{cases}$$

$$\varphi_{\forall}(x,y) := \begin{cases} \ulcorner (\forall w s) \urcorner & \text{if } x \text{ encodes the variable } w \text{ and } y \text{ encodes the character string } s \\ 0 & \text{otherwise} \end{cases}$$

It holds that

$$\begin{aligned} F(x) \iff \exists n \exists a \exists b \Big(& \boldsymbol{\beta}(a,b,n) = x \wedge \forall i \leq n \Big(\big(i < n \wedge T(\boldsymbol{\beta}(a,b,i))\big) \\ & \vee \exists j < i \big(\exists k < i (T(\boldsymbol{\beta}(a,b,j)) \wedge T(\boldsymbol{\beta}(a,b,k)) \\ & \quad \wedge \varphi_{=}\big(\boldsymbol{\beta}(a,b,j), \boldsymbol{\beta}(a,b,k)\big) = \boldsymbol{\beta}(a,b,i))\big) \\ & \vee \exists j < i \big(\neg T(\boldsymbol{\beta}(a,b,j)) \wedge \varphi_{\neg}(\boldsymbol{\beta}(a,b,j)) = \boldsymbol{\beta}(a,b,i)\big) \\ & \vee \exists j < i \big(\exists k < i (\neg T(\boldsymbol{\beta}(a,b,j)) \wedge \neg T(\boldsymbol{\beta}(a,b,k)) \\ & \quad \wedge \varphi_{\Rightarrow}\big(\boldsymbol{\beta}(a,b,j), \boldsymbol{\beta}(a,b,k)\big) = \boldsymbol{\beta}(a,b,i))\big) \\ & \vee \exists j < i \big(\exists k < i (R_v(\boldsymbol{\beta}(a,b,j)) \wedge \neg T(\boldsymbol{\beta}(a,b,k)) \wedge \\ & \quad \varphi_{\forall}\big(\boldsymbol{\beta}(a,b,j), \boldsymbol{\beta}(a,b,k)\big) = \boldsymbol{\beta}(a,b,i))\big)\Big)\Big) \end{aligned}$$

By replacing T, R_v and the φ, one obtains a formula that represents F.

(iv) According to (iii), we can assume that x encodes a formula f and y encodes a variable w. With Lemma I.6.11, one sees that the relation

$$V_0(x,y,k) \iff w \text{ stands at position } k \text{ in } f$$

is recursive. To check whether w actually occurs freely at position k, we consider $f = s_0 \dots s_n$ as a character string. One must check, on the one hand, whether $\forall w$ occurs to the left of s_k and, on the other hand, whether between $\forall x$ and s_k there are at least as many opening as closing parentheses. We recall that by definition all formulas are bounded by parentheses. Let

$$\gamma_x(y,i) := \begin{cases} 0 & \text{if } i = 0 \text{ or } i > k, \\ \gamma_x(y,i-1) + 1 & \text{if } s_i = (\text{ and } (s_{i-2}s_{i-1} = \forall w \text{ or } \gamma_x(i-1) > 0), \\ \gamma_x(y,i-1) - 1 & \text{if } s_i =) \text{ and } \gamma_x(i-1) > 0, \\ \gamma_x(y,i-1) & \text{otherwise.} \end{cases}$$

The case distinctions can be bundled into a single recursive call by linear combinations of suitable characteristic functions as in the proof of Lemma I.6.10. Therefore, γ_x is recursive. It holds that $\gamma_x(k) = 0$ if and only if x occurs freely at position k in f. Formally,

$$\gamma(x, y, i) := \begin{cases} \gamma_x(y, i) & \text{if } x \text{ encodes a character string} \\ 0 & \text{otherwise} \end{cases}$$

is recursive. Combining all conditions, one obtains

$$V(x, y, k) \iff F(x) \wedge R_v(y) \wedge V_0(x, y, k) \wedge \gamma(x, y, k) = 0.$$

(v) As before, we can check whether x encodes a formula f and y encodes a variable w. The relation T from (ii) can be easily modified so that it is only true for closed terms t. With (iv), the positions of all free occurrences of w in f can be identified. With (i), one can realize the substitution $w \leftarrow t$. It should be noted that new prime factors are added, provided t is not the constant 0. Since t is assumed to be closed, there are no collisions to consider.

(vi) We can assume that x encodes a formula f. A proof of f is a sequence of formulas $f_0, \ldots, f_n$, such that each f_i is an axiom or was obtained from f_j with $j < i$ by rules of inference. We can thus argue as in (iii). Whether an f_i is an axiom can in principle (albeit very tediously) be verified by a corresponding sequence of sub-formulas. For $(\mathcal{P}_2^=)$, one can use (v). We refrain from writing down the details.[22] Checking the two rules of inference, on the other hand, is again relatively simple. □

Theorem I.7.6 (Gödels first incompleteness theorem)**.** *Peano arithmetic is incomplete with respect to the standard interpretation, i. e. there exist true statements that cannot be proven.*

Proof. Let $\boldsymbol{b}$ be a formula that represents the proof relation B from Lemma I.7.5. We call a formula f with exactly one free variable x *unary* (i. e. x occurs at least once free in f). Whether f is unary can be represented using Lemma I.7.5. We recall that $n \in \mathbb{N}$ represents the closed term $\overline{n} = 0''^{\ldots\prime}$. According to Lemma I.7.5, the so-called *diagonal function*

$$\delta(x) := \begin{cases} \ulcorner f(\overline{x}) \urcorner & \text{if } x = \ulcorner f \urcorner \text{ for a unary formula } f \\ 0 & \text{otherwise} \end{cases}$$

is represented by a formula $\boldsymbol{d}$. The formula

$$\boldsymbol{g}(x, y) := \exists z(\boldsymbol{d}(y, z) \wedge \boldsymbol{b}(x, z))$$

represents the relation "x is the Gödel number of a proof of $f(\overline{y})$ with $y = \ulcorner f \urcorner$". Thus, the unary formula

$$\boldsymbol{h}(y) := \forall x \neg \boldsymbol{g}(x, y),$$

represents the property that no proof for $f(\overline{y})$ with $y = \ulcorner f \urcorner$ exists. If $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ were provable, then $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ would be true, since $\mathcal{PA}$ is sound with respect to the standard interpretation. But then precisely no proof for $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ would exist. This contradiction shows that $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ is unprovable and thus true. □

Corollary I.7.7. *There are closed formulas in $\mathcal{PA}$ that can be neither proven nor refuted.*

Proof. According to Theorem I.7.6, there exists a true closed formula f with $\nvdash f$. Since $\mathcal{PA}$ is sound, the false statement $\neg f$ cannot be proven either. □

[22] Gödel defined a total of 46 auxiliary functions.

Remark I.7.8.

(i) According to Gödel's completeness theorem, a non-provable formula f cannot be a tautology. Therefore, there must be so-called *non-standard models* for $\mathcal{PA}$ in which f is actually false. According to the theorem of TENNENBAUM, such models cannot be specified explicitly. They form the basis of *non-standard analysis* (see Remark II.9.3).

(ii) Gödel's proof also works in the weaker calculus of *Robinson arithmetic* $\mathcal{R}$. In this case, $(\mathcal{I})$ is replaced by

$$\vdash x = 0 \vee \exists y(y' = x)$$

(every number different from zero has a predecessor). In fact, there are simple non-provable true statements in $\mathcal{R}$. To see this, we extend the universe to $U := \mathbb{N} \cup \{\infty\}$, where ∞ has the following interpretation:

$$\infty' = x + \infty = \infty + x = \infty, \qquad x \cdot \infty = \infty \cdot x = \begin{cases} 0 & \text{if } x = 0 \\ \infty & \text{if } x \neq 0 \end{cases} \qquad (\text{for all } x \in U)$$

It is easy to check that $\mathcal{R}$ is correct with respect to this interpretation. The formula $x' \neq x$ is true in $\mathbb{N}$, but false in U. Thus, it cannot be proven. This provides a consistent incomplete calculus with little effort, which is, however, insufficient for higher mathematics.

(iii) Conversely, it can be shown that $\mathcal{PA}$ becomes complete with respect to the standard interpretation if one dispenses with multiplication (i.e., deletes the axioms $(\times_1)$ and $(\times_2)$).

(iv) If one defines Peano arithmetic as second-order predicate logic with the induction axiom

$$\forall P\big((P(0) \wedge \forall x(P(x) \Rightarrow P(x'))) \Rightarrow \forall x P\big)$$

(where P ranges over all predicates), then *Dedekind's isomorphism theorem* states that $\mathbb{N}$ is the only model up to isomorphism[23]. Theorem I.7.6 also holds in this version (without proof). Thus, the completeness theorem in $\mathcal{P}_2$ must in turn be false (cf. Remark I.4.10).

(v) So far, we had assumed the consistency of $\mathcal{PA}$ as given, modeled by $\mathbb{N}$. However, this contradicts the effort to place mathematics on an axiomatic foundation. Rather, one should define $\mathbb{N}$ through $\mathcal{PA}$. From this point of view, the consistency of $\mathcal{PA}$ must additionally be assumed in Theorem I.7.6 (see Theorem I.7.10). The representability of relations and functions must then occur purely syntactically. A function $\varphi\colon \mathbb{N}^n \to \mathbb{N}$ is, for example, *syntactically represented* by a formula f if for all $\vec{x} \in \mathbb{N}^n$:

$$\varphi(\vec{x}) = y \implies \vdash f(\overline{x_1}, \ldots, \overline{x_n}, y) \Leftrightarrow y = \overline{y}.$$

The formulas $\boldsymbol{b}$ and $\boldsymbol{h}$ constructed in Theorem I.7.6 must furthermore be replaced by

$$\tilde{\boldsymbol{b}}(x, y) :\Longleftrightarrow x \text{ is the Gödel number of a proof of } \ulcorner \neg f(\overline{y}) \urcorner \text{ with } y = \ulcorner f \urcorner$$
$$\tilde{\boldsymbol{h}}(y) := \forall x\big(\boldsymbol{b}(x, y) \Rightarrow \exists z < x \tilde{\boldsymbol{b}}(z, y)\big)$$

(*Rosser's trick*). Semantically, $g := \tilde{\boldsymbol{h}}(\ulcorner \tilde{\boldsymbol{h}} \urcorner)$ means something like:

If g is provable, then there exists a "shorter" proof for $\neg g$.

One can now carry out Gödel's proof with significantly more effort[24] and directly obtains the negation-incompleteness of $\mathcal{PA}$. We illustrate in Example I.7.9 how to prove the syntactic representability of addition.

[23] i.e., up to renaming of the natural numbers

[24] Even Gödel omits details at this point. See [D. W. Hoffmann, *Gödel's Incompleteness Theorems*, Springer, 2024].

(vi) It is natural to try to "complete" $\mathcal{PA}$ by adding further axioms. However, the syntactic version of the first incompleteness theorem sketched in (v) holds more generally in every consistent calculus that is expressive enough to formalize Peano arithmetic (we define such a calculus in Definition II.1.6). This insight destroyed Hilbert's long-held dream of being able to prove all true statements of mathematics with a system of axioms.

Example I.7.9.

(i) We show that the function $(x, y) \mapsto x + y$ is syntactically represented by the formula $f(x, y, z) := (x + y = z)$, i. e. $\vdash \overline{x} + \overline{y} = z \Leftrightarrow z = \overline{x + y}$. According to Lemma I.3.12 and Exercise I.4, it suffices to prove

$$\vdash \overline{x} + \overline{y} = \overline{x + y}.$$

For $y = 0$, this holds according to $(+_1)$. Now let $y > 0$ and $\vdash \overline{x} + \overline{y - 1} = \overline{x + y - 1}$ be already shown. Then it holds that

$$\begin{aligned}
&\vdash \overline{x} + \overline{y - 1} = \overline{x + y - 1} \\
&\vdash (\overline{x} + \overline{y - 1})' = \overline{x + y - 1}' && \text{(Lemma I.3.13)} \\
&\vdash \overline{x} + \overline{y - 1}' = (\overline{x} + \overline{y - 1})' && (+_2) \\
&\vdash \overline{x} + \overline{y - 1}' = \overline{x + y - 1}' && \text{(Lemma I.3.12)} \\
&\vdash \overline{x} + \overline{y} = \overline{x + y}
\end{aligned}$$

Note that the induction axiom $(\mathcal{I})$ is not needed.

(ii) Since the non-provable formula $\boldsymbol{h}(\ulcorner \boldsymbol{h} \urcorner)$ constructed in the proof of Theorem I.7.6 appears very esoteric, one might ask whether there are tangible non-provable formulas. The *Goodstein sequence* $(g_i(n))_{i \geq 1}$ of a natural number n is defined as follows: Set $g_1(n) := n$. Let $b > 1$. Write $g_{b-1}(n)$ in the b-adic representation,[25] e. g.

$$g_1(n) = n = 2^8 + 2^5 + 2 + 1$$

for $n = 291$ and $b = 2$. The exponents in this representation are iteratively also brought into the b-adic representation:

$$g_1(n) = 2^{2^{2+1}} + 2^{2^2+1} + 2 + 1.$$

Now all occurrences of b therein are replaced by $b + 1$ and subsequently 1 is subtracted:

$$g_2(n) = (3^{3^{3+1}} + 3^{3^3+1} + 3 + 1) - 1.$$

For $n = 4$, the first terms of the sequence are:

$$\begin{aligned}
&g_1(4) = 4 = 2^2, && g_2(4) = 3^3 - 1 = 26 = 2 \cdot 3^2 + 2 \cdot 3 + 2, \\
&g_3(4) = 2 \cdot 4^2 + 2 \cdot 4 + 1 = 41, && g_4(4) = 2 \cdot 5^2 + 2 \cdot 5 = 60, \\
&g_5(4) = 2 \cdot 6^2 + 2 \cdot 6 - 1 = 83 = 2 \cdot 6^2 + 6 + 5, && g_6(4) = 2 \cdot 7^2 + 7 + 4 = 109.
\end{aligned}$$

At first glance, the sequence seems to tend towards infinity. Surprisingly, however, $(g_i(4))$ reaches the value 0 for the first time for $i = 3 \cdot 2^{402653211} - 1$ (and then remains there because of $0 = 0 \cdot b^0$). In general, the formula

$$g := (\forall n \exists k g_k(n) = 0)$$

can indeed be expressed in $\mathcal{PA}$, but not proven. In Theorem II.4.28, we will prove g within the Zermelo-Fraenkel calculus of set theory.

[25] See Remark II.4.27

(iii) It is entirely conceivable that well-known open problems of number theory such as the *Goldbach conjecture* or the existence of infinitely many *twin primes* are not provable in $\mathcal{PA}$ (or larger calculi).

Theorem I.7.10 (GÖDEL's Second Incompleteness Theorem)**.** *The consistency of $\mathcal{PA}$ cannot be proven in $\mathcal{PA}$.*

Sketch of proof. Using the notation from the proof of Theorem I.7.6, the formula

$$\boldsymbol{e}(x) := \exists y\, \boldsymbol{b}(y, x)$$

represents the property that the formula with Gödel number x is provable. As is well known, every formula can be proven in an inconsistent system. The consistency of $\mathcal{PA}$ therefore corresponds to the formula $c := \neg\boldsymbol{e}(\overline{\ulcorner 0 \neq 0 \urcorner})$. We had sketched in Remark I.7.8 how one would prove the syntactic version of Theorem I.7.6 under the assumption of c. A formalized proof would thus end with the line

$$c \vdash \neg\boldsymbol{e}(\ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner)$$

[26]. Since the function δ from Theorem I.7.6 is syntactically represented in this context by $\boldsymbol{d}$ (see Remark I.7.8), it holds that

$$\vdash \boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, x) \Rightarrow x = \ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner \qquad (*)$$

If c were provable in $\mathcal{PA}$, one obtains:

$$\begin{aligned}
&\vdash \neg\boldsymbol{e}(\ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner)^{27} && \\
&\vdash y = \ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner \Rightarrow \big(\neg\boldsymbol{e}(\ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner) \Rightarrow \neg\boldsymbol{e}(y)\big) && \text{(Lemma I.3.12, } (\mathcal{P}_2^=)) \\
&\vdash y = \ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner \Rightarrow \neg\boldsymbol{e}(y) && \text{(D)} \\
&\vdash \boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \Rightarrow y = \ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner && (*) \\
&\vdash \boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \Rightarrow \neg\boldsymbol{e}(y) && \text{(MB)} \\
&\vdash \boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \Rightarrow \forall x \neg\boldsymbol{b}(x, y) && \text{(Def. } \exists\text{, Lemma I.1.11)} \\
&\vdash \forall x \neg\boldsymbol{b}(x, y) \Rightarrow \neg\boldsymbol{b}(x, y) && (\mathcal{P}_2') \\
&\vdash \boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \Rightarrow \neg\boldsymbol{b}(x, y) && \text{(MB)} \\
&\vdash \neg\big(\boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \wedge \boldsymbol{b}(x, y)\big) && \text{(Def. } \wedge\text{, Lemma I.1.11)} \\
&\vdash \forall y \neg\big(\boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \wedge \boldsymbol{b}(x, y)\big) && \text{(G)} \\
&\vdash \neg\boldsymbol{g}(x, \ulcorner \boldsymbol{h} \urcorner) && \text{(Def. } \boldsymbol{g}\text{)} \\
&\vdash \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner}) && \text{((G), Def. } \boldsymbol{h}\text{)}
\end{aligned}$$

This is a contradiction, because $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ is not provable according to the proof of Theorem I.7.6. □

Remark I.7.11. The consistency of $\mathcal{PA}$ can be proven in the calculus of Zermelo-Fraenkel set theory, which we introduce in Definition II.1.6.

[26] Strictly speaking, one would have to use Rosser's formula $\tilde{\boldsymbol{h}}(\ulcorner \tilde{\boldsymbol{h}} \urcorner)$.

[27] This statement itself is a semantic paradox: We have proven that there is no proof for the unprovable formula $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$.

I.8. Computability

Remark I.8.1. So far, we have ignored the question, important in practice, of how to find proofs. Since we always assume that the alphabet of a calculus $\mathcal{K}$ is countable, one can in principle go through all axioms and apply possible inference rules in each step (in $\mathcal{PA}$ one can go through all natural numbers and check in each case whether they encode a proof). In this way, every theorem is output after finitely many steps. However, if one is given an unprovable formula f, one will wait in vain for f to be found in this way. If $\mathcal{K}$ is negation-complete, then $\neg f$ will be found and one can terminate at this point (provided $\mathcal{K}$ is consistent). In this case, $\mathcal{K}$ is called *decidable*. We will show that there can be no decision algorithm for $\mathcal{PA}$ (Theorem I.8.21).

Definition I.8.2. The ACKERMANN *function* $\boldsymbol{\alpha}\colon \mathbb{N}^2 \to \mathbb{N}$ is recursively defined by

$$\boldsymbol{\alpha}(x,y) := \begin{cases} 2y+1 & \text{if } x = 0, \\ \boldsymbol{\alpha}(x-1,1) & \text{if } x > 0 \text{ and } y = 0, \\ \boldsymbol{\alpha}\big(x-1, \boldsymbol{\alpha}(x,y-1)\big) & \text{otherwise.} \end{cases}$$

For $k \in \mathbb{N}$ let $\boldsymbol{\alpha}_k(x) := \boldsymbol{\alpha}(k,x)$.

Example I.8.3. According to Lemma I.8.4(i), $\boldsymbol{\alpha}$ is well-defined, even if the explicit calculation requires a large number of recursive calls. We show $\boldsymbol{\alpha}_1(n) = 2^{n+2} - 1$ by induction on n. It holds that

$$\begin{aligned} &\boldsymbol{\alpha}_1(0) = \boldsymbol{\alpha}_0(1) = 3 = 2^2 - 1, \\ &\boldsymbol{\alpha}_1(n) = \boldsymbol{\alpha}_0(\boldsymbol{\alpha}_1(n-1)) = 2\boldsymbol{\alpha}_1(n-1) + 1 = 2(2^{n+1} - 1) + 1 = 2^{n+2} - 1. \end{aligned}$$

Lemma I.8.4. *For all $x, y, z, k \in \mathbb{N}$ the following holds:*

(i) $\boldsymbol{\alpha}_k$ *is recursive.*

(ii) $\boldsymbol{\alpha}(x, y+1) > \boldsymbol{\alpha}(x,y)$.

(iii) $\boldsymbol{\alpha}(x+1, y) > \boldsymbol{\alpha}(x,y)$.

(iv) $\boldsymbol{\alpha}(x+1, y) \geq \boldsymbol{\alpha}(x, y+1)$.

(v) $\boldsymbol{\alpha}(x+y+1, z) > \boldsymbol{\alpha}(x, \boldsymbol{\alpha}(y,z))$.

(vi) For every recursive function $\varphi\colon \mathbb{N}^n \to \mathbb{N}$ there exists a $k \in \mathbb{N}$ with $\varphi(\vec{x}) < \boldsymbol{\alpha}_k(\max(\vec{x}))$ for all $\vec{x} \in \mathbb{N}^n$.

Proof.

(i) Because of $\boldsymbol{\alpha}_0(x) = 2x+1$, $\boldsymbol{\alpha}_0$ is recursive. Let $k > 0$ and the claim be already proven for $k-1$. Then

$$\boldsymbol{\alpha}_k(x) = \begin{cases} \boldsymbol{\alpha}_{k-1}(1) & \text{if } x = 0, \\ \boldsymbol{\alpha}_{k-1}(\boldsymbol{\alpha}_k(x-1)) & \text{if } x > 0 \end{cases}$$

is recursive.

(ii) Induction on x: Obviously $\boldsymbol{\alpha}(0, y+1) = 2y+3 > 2y+1 = \boldsymbol{\alpha}(0, y)$ for all $y \in \mathbb{N}$. Let $x > 0$ and $\boldsymbol{\alpha}(x-1, y+1) > \boldsymbol{\alpha}(x-1, y)$ for all y be already shown. Induction on y: Because of $\boldsymbol{\alpha}(x-1, 1) > \boldsymbol{\alpha}(x-1, 0) \geq 1$, it holds that

$$\boldsymbol{\alpha}(x, 1) = \boldsymbol{\alpha}\big(x-1, \boldsymbol{\alpha}(x, 0)\big) = \boldsymbol{\alpha}\big(x-1, \boldsymbol{\alpha}(x-1, 1)\big) > \boldsymbol{\alpha}(x-1, 1) = \boldsymbol{\alpha}(x, 0).$$

Let $y > 0$ and $\boldsymbol{\alpha}(x, y) > \boldsymbol{\alpha}(x, y-1)$ be already shown. Then

$$\boldsymbol{\alpha}(x, y+1) = \boldsymbol{\alpha}\big(x-1, \boldsymbol{\alpha}(x, y)\big) > \boldsymbol{\alpha}\big(x-1, \boldsymbol{\alpha}(x, y-1)\big) = \boldsymbol{\alpha}(x, y).$$

(iii) Induction on x: Certainly $\boldsymbol{\alpha}(1, 0) = 3 > 1 = \boldsymbol{\alpha}(0, 0)$. For $y > 0$, $\boldsymbol{\alpha}(1, y-1) = 2^{y+1} - 1 > y$ holds according to Example I.8.3. It follows that

$$\boldsymbol{\alpha}(1, y) = \boldsymbol{\alpha}\big(0, \boldsymbol{\alpha}(1, y-1)\big) \overset{\text{(ii)}}{>} \boldsymbol{\alpha}(0, y).$$

Now let $x > 0$ and $\boldsymbol{\alpha}(x, y) > \boldsymbol{\alpha}(x-1, y)$ for all $y \in \mathbb{N}$ be already shown. Induction on y: For $y = 0$, $\boldsymbol{\alpha}(x+1, 0) = \boldsymbol{\alpha}(x, 1) > \boldsymbol{\alpha}(x-1, 1) = \boldsymbol{\alpha}(x, 0)$. Let $y > 0$ and $\boldsymbol{\alpha}(x+1, y-1) > \boldsymbol{\alpha}(x, y-1)$ be already shown. Then

$$\boldsymbol{\alpha}(x+1, y) = \boldsymbol{\alpha}\big(x, \boldsymbol{\alpha}(x+1, y-1)\big) > \boldsymbol{\alpha}\big(x, \boldsymbol{\alpha}(x, y-1)\big) > \boldsymbol{\alpha}\big(x-1, \boldsymbol{\alpha}(x, y-1)\big) = \boldsymbol{\alpha}(x, y).$$

(iv) Induction on y: For $y = 0$, $\boldsymbol{\alpha}(x+1, 0) = \boldsymbol{\alpha}(x, 1)$ holds by definition. Let $y > 0$ and $\boldsymbol{\alpha}(x+1, y-1) \geq \boldsymbol{\alpha}(x, y)$ for all $x \in \mathbb{N}$ be already shown. Then

$$\boldsymbol{\alpha}(x+1, y) = \boldsymbol{\alpha}\big(x, \boldsymbol{\alpha}(x+1, y-1)\big) \geq \boldsymbol{\alpha}\big(x, \boldsymbol{\alpha}(x, y)\big) \overset{\text{(iii)}}{>} \boldsymbol{\alpha}\big(x-1, \boldsymbol{\alpha}(x, y)\big) = \boldsymbol{\alpha}(x, y+1).$$

(v) It holds that

$$\boldsymbol{\alpha}(x+y+1, z) = \boldsymbol{\alpha}\big(x+y, \boldsymbol{\alpha}(x+y+1, z-1)\big) \overset{\text{(iv),(ii)}}{\geq} \boldsymbol{\alpha}\big(x+y, \boldsymbol{\alpha}(x+y, z)\big) \overset{\text{(iii),(ii)}}{>} \boldsymbol{\alpha}\big(x, \boldsymbol{\alpha}(y, z)\big).$$

(vi) For the zero function, the successor function, and the projections, one can choose $k = 0$. Let $\beta_1, \ldots, \beta_r, \gamma$ be recursive with corresponding constants $k(\beta_i)$ and $k(\gamma)$. Let $m := \max(k(\beta_1), \ldots, k(\beta_r))$ and $k := m + k(\gamma) + 1$. For $\vec{x} \in \mathbb{N}^n$ it holds that

$$\begin{aligned}
\gamma(\beta_1(\vec{x}), \ldots, \beta_r(\vec{x})) &< \boldsymbol{\alpha}_{k(\gamma)}(\max(\beta_1(\vec{x}), \ldots, \beta_r(\vec{x}))) \\
&\overset{\text{(ii)}}{\leq} \boldsymbol{\alpha}_{k(\gamma)}\big(\max\big(\boldsymbol{\alpha}_{k(\beta_1)}(\max(\vec{x})), \ldots, \boldsymbol{\alpha}_{k(\beta_r)}(\max(\vec{x}))\big)\big) \\
&\overset{\text{(iii)}}{\leq} \boldsymbol{\alpha}_{k(\gamma)}\big(\boldsymbol{\alpha}_m(\max(\vec{x}))\big) \overset{\text{(v)}}{\leq} \boldsymbol{\alpha}_k(\max(\vec{x})).
\end{aligned}$$

Finally, let

$$\varphi(\vec{x}) = \begin{cases} \beta(x_2, \ldots, x_n) & \text{if } x_1 = 0 \\ \gamma\big(\varphi(x_1 - 1, x_2, \ldots, x_n), x_1 - 1, x_2, \ldots, x_n\big) & \text{if } x_1 > 0 \end{cases}$$

with recursive β and γ. Let $m := k(\beta) + k(\gamma) + 1$. We first show

$$\varphi(\vec{x}) < \boldsymbol{\alpha}_m(x_1 + \max(x_2, \ldots, x_n))$$

by induction on x_1. This holds for $x_1 = 0$ because of $k(\beta) < m$. Now let $x_1 > 1$ and the claim be shown for $x_1 - 1$. Then

$$\begin{aligned}\varphi(\vec{x}) &< \boldsymbol{\alpha}_{k(\gamma)}\Big(\max\big(\boldsymbol{\alpha}_m\big(x_1 - 1 + \max(x_2, \ldots, x_n)\big), x_1 - 1, x_2, \ldots, x_n\big)\Big) \\ &= \boldsymbol{\alpha}_{k(\gamma)}\big(\boldsymbol{\alpha}_m(x_1 - 1 + \max(x_2, \ldots, x_n))\big) \overset{\text{(iii)}}{\leq} \boldsymbol{\alpha}\big(m-1, \boldsymbol{\alpha}\big(m, x_1 - 1 + \max(x_2, \ldots, x_n)\big)\big) \\ &= \boldsymbol{\alpha}_m(x_1 + \max(x_2, \ldots, x_n))\end{aligned}$$

The claim now follows with $k := m + 1$, because

$$\boldsymbol{\alpha}_m\big(x_1 + \max(x_2, \ldots, x_n)\big) \leq \boldsymbol{\alpha}_m(2\max(\vec{x})) < \boldsymbol{\alpha}_m(\boldsymbol{\alpha}_0(\max(\vec{x}))) < \boldsymbol{\alpha}_k(\max(\vec{x})). \qquad \square$$

Theorem I.8.5 (Ackermann)**.** *The Ackermann function is not recursive.*

Proof. Suppose $\boldsymbol{\alpha}$ is recursive. Then by Lemma I.8.4 there exists a $k \in \mathbb{N}$ with $\boldsymbol{\alpha}(x, x) < \boldsymbol{\alpha}_k(x) = \boldsymbol{\alpha}(k, x)$ for all $x \in \mathbb{N}$. This contradicts Lemma I.8.4 for $x > k$. $\square$

Definition I.8.6. A *Turing machine* $T = (A, Z, I)$ consists of the following things:

- a finite alphabet A with special symbol $\triangle \in A$
- a finite set of states Z with start state $\boldsymbol{s} \in Z$
- a set of instructions $I \subseteq Z \times A \times A \times \{\pm 1\} \times Z$

The machine operates on a tape infinite in both directions, which is written with symbols from A. At the beginning, a tape configuration $(\ldots, a_{-1}, a_0, a_1, \ldots)$ is given, where $a_i = \triangle$ holds for almost all i (i.e., except for finitely many exceptions). Furthermore, T is in state $\boldsymbol{s}$ and the read head is at tape position 0. The instructions define how T works. Suppose T is in state z and reads the symbol $a \in A$. If an instruction of the form $(z, a, \tilde{a}, r, \tilde{z})$ exists, then T replaces the symbol a with $\tilde{a}$ at the same position and changes to state $\tilde{z}$. If $r = -1$ (or $r = 1$), then the read head moves one position to the left (or right). Subsequently, a suitable instruction is sought again. We always assume that at most one instruction $(z, a, \tilde{a}, r, \tilde{z})$ exists for given z and a (i.e., T is *deterministic*). In particular, $|I| \leq |A||Z|$.[28] If there is no suitable instruction in a situation, then T stops (we say T *terminates*). It can happen that T never stops (for example if $|I| = |A||Z|$).

Remark I.8.7.

(i) We always assume that A contains at least one other symbol besides $\triangle$, say $1 \in A$. One can now interpret a natural number n as a tape configuration with n ones

$$(\ldots, \overset{-1}{\triangle}, \overset{0}{1}, \overset{1}{1}, \ldots, \overset{n-1}{1}, \overset{n}{\triangle}, \ldots)$$

(in the case $0, 1 \in A$ one could also use the binary representation of n, see Exercise I.17). We call n the *input* of T if this is the starting configuration of the tape. In the case $n = 0$ we speak of the *empty* tape. During the calculation, T can write on the tape with further symbols. If T terminates with a (necessarily finite) sequence of ones, we can interpret the result as $m \in \mathbb{N}$. In this case we write $T(n) := m$. If T does not terminate with a sequence of ones or does not terminate at all, then $T(n)$ is not defined. In this way, T determines a *partial* function $T\colon \mathbb{N} \rightharpoonup \mathbb{N}$.[29]

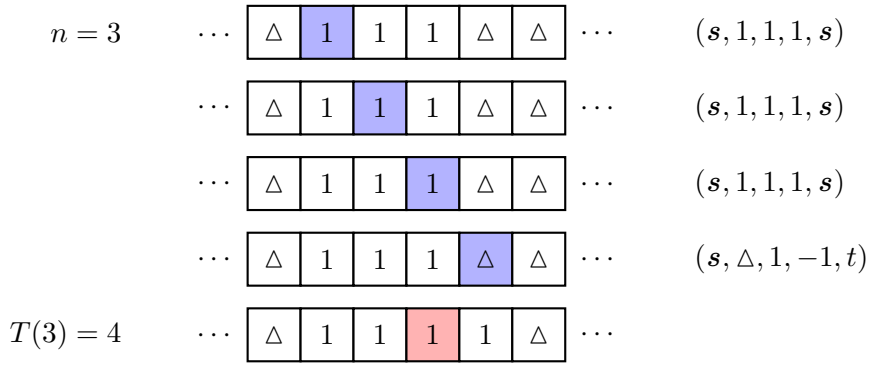
[28] For notation see Definition II.1.2.
[29] See Definition II.2.5

(ii) A Turing machine T is essentially uniquely determined by the set of instructions I, because symbols of the alphabet or states that do not occur in I have no influence on the operation of T.

(iii) There are numerous simulators for Turing machines on the internet with which one can experiment.[30]

Example I.8.8.

(i) The Turing machine T with instructions $I = \{(\boldsymbol{s}, 1, 1, 1, \boldsymbol{s}), (\boldsymbol{s}, \triangle, 1, -1, t)\}$ computes the successor $T(n) = n + 1$ for $n \in \mathbb{N}$.

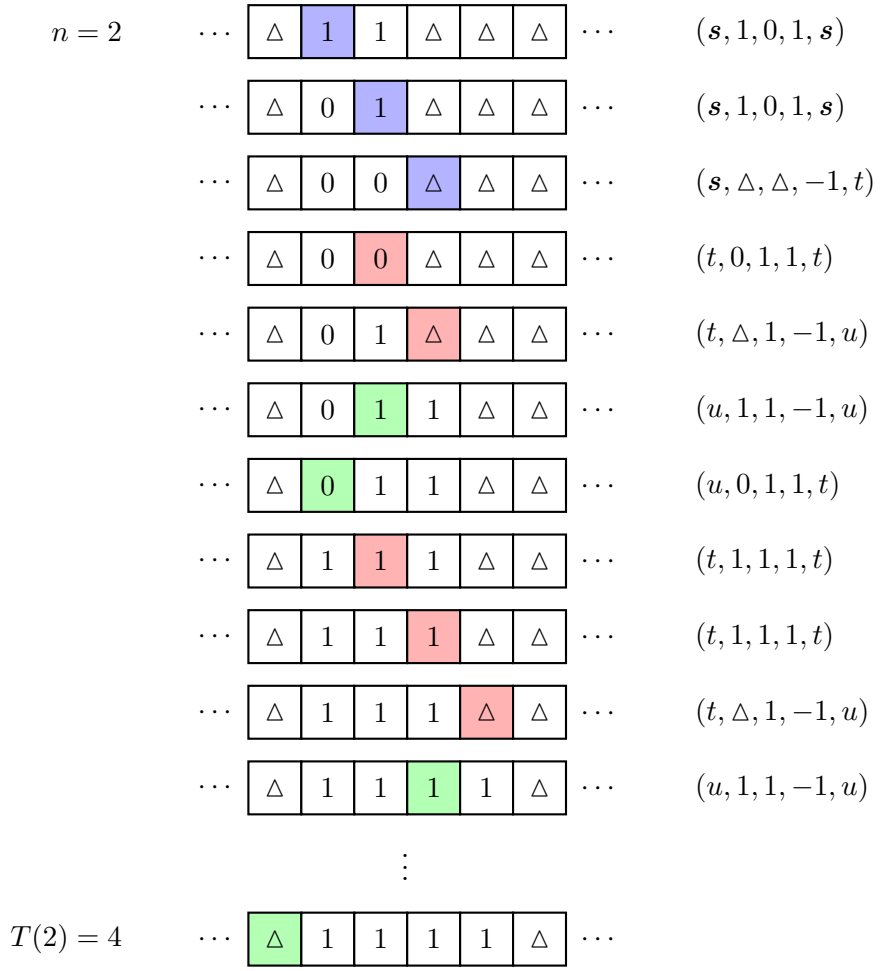


(ii) The Turing machine T with instructions

$$(\boldsymbol{s}, 1, 0, 1, \boldsymbol{s}), (\boldsymbol{s}, \triangle, \triangle, -1, t), (t, 0, 1, 1, t), (t, 1, 1, 1, t), (t, \triangle, 1, -1, u), (u, 1, 1, -1, u), (u, 0, 1, 1, t)$$

[30] For example `https://turingmachine.vassar.edu/` or `https://turingmachinesimulator.com/`.

computes $T(n) = 2n$ for $n > 0$.



Remark I.8.9. Although much more complex machines (e.g., quantum computers) are conceivable, they have so far not been able to compute more than Turing machines (though they can work more efficiently). Therefore, it is assumed that the *Church thesis* holds:

Everything that is intuitively computable can be computed by a Turing machine.

Definition I.8.10.

- A partial function $\varphi\colon \mathbb{N} \rightharpoonup \mathbb{N}$ is called *computable*, if a Turing machine T exists such that for all $n \in \mathbb{N}$: if $\varphi(n)$ is defined, then so is $T(n)$ and $\varphi(n) = T(n)$ as in Remark I.8.7.
- A function in several arguments $\varphi\colon \mathbb{N}^n \to \mathbb{N}$ is called *computable* if its "Gödelization" (Definition I.7.2)
$$\psi\colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto \begin{cases} \varphi(r_0, \dots, r_n) & \text{if } n = p_0^{r_0} \dots p_k^{r_k}, \\ 0 & \text{if } n = 0 \end{cases}$$
is computable.
- The existence of a computable function is equivalent to the existence of an *algorithm*. The steps of the algorithm correspond to the instructions of the Turing machine.

Example I.8.11. The zero function ζ is computed by the Turing machine $(\{\triangle, 1\}, \{\boldsymbol{s}\}, \{(\boldsymbol{s}, 1, \triangle, 1, \boldsymbol{s})\})$. According to Example I.8.8, the successor function is computable. The projection π_k^n is computable if and only if the recursive function $\epsilon(x, k)$ from Lemma I.6.11 is computable. According to Exercise I.19, the composition of computable functions is computable. One can show that indeed every recursive function is computable (without proof). The next theorem shows that the converse is false.

Theorem I.8.12. *The Ackermann function is computable.*

Sketch of proof. Idea: Construct a Turing machine T that executes the recursive calls

$$\boldsymbol{\alpha}(x, y) = \boldsymbol{\alpha}\big(x - 1, \boldsymbol{\alpha}(x, y - 1)\big) = \ldots = \boldsymbol{\alpha}\big(x - 1, \boldsymbol{\alpha}(x - 1, \ldots, \boldsymbol{\alpha}(x, 0) \ldots)\big)$$

through suitable instructions. It suffices to pass the arguments as a tuple directly (instead of the Gödelization) to T. At the beginning, let (x, y) (for example as a sequence of ones separated by $\triangle$) be written on the tape. In each iteration, a sequence $(x_0, \ldots, x_n)$ is given. The instructions are

(i) If $n = 0$, then halt.

(ii) If $x_{n-1} = 0$, then replace (x_{n-1}, x_n) by $(2x_n + 1)$.

(iii) If $x_{n-1} > 0$ and $x_n = 0$, then replace (x_{n-1}, x_n) by $(x_{n-1} - 1, 1)$.

(iv) If $x_{n-1} > 0$ and $x_n > 0$, then replace (x_{n-1}, x_n) by $(x_{n-1} - 1, x_{n-1}, x_n - 1)$.

One must, of course, realize that this can be implemented with a Turing machine. □

Example I.8.13. The calculation of $\boldsymbol{\alpha}(2, 1)$ by a Turing machine proceeds as follows:

$$\begin{aligned}(2,1) &\to (1,2,0) \to (1,1,1) \to (1,0,1,0) \to (1,0,0,1) \to (1,0,3) \to (1,7) \to (0,1,6)\\ &\to (0,0,1,5) \to \ldots \to (0,0,0,0,0,0,0,0,1) \to (0,0,0,0,0,0,0,3) \to \ldots \to (511)\end{aligned}$$

Remark I.8.14. One can show that the class of computable functions coincides with the class of *μ-recursive* functions. These are partial functions φ that arise through (iterated) application of the *μ-operator*

$$\varphi(x) := \begin{cases} \min\limits_{k \in \mathbb{N}} \Big(\gamma(k, x) = 0 \wedge \forall l < k \big(\gamma(l, x) \text{ is defined}\big)\Big) & \text{if min exists} \\ \text{undefined} & \text{otherwise} \end{cases}$$

from (μ-)recursive (partial) functions $\gamma\colon \mathbb{N}^2 \to \mathbb{N}$. Note that, in contrast to Lemma I.6.10, the "search variable" k for the minimum is unbounded. If the minimum does not exist, the corresponding Turing machine does not halt.

Theorem I.8.15 (Halting Problem)**.** *There is no general algorithm that decides whether a given Turing machine terminates with a given input.*

Proof. Due to its finiteness, every Turing machine T can be uniquely described by a number $t \in \mathbb{N}$. Suppose the function $\varphi\colon \mathbb{N} \to \mathbb{N}$ with

$$\varphi(n) = \begin{cases} 1 & \text{if } n = 2^t 3^e \text{ and } T \text{ terminates with input } e, \\ 0 & \text{otherwise} \end{cases}$$

is computable. Then there exists a Turing machine M with $\varphi(n) = M(n)$ for all $n \in \mathbb{N}$. By adding further instructions, one obtains a Turing machine $\tilde{M}$ that terminates with input e if and only if $M(e) = 0$. In this case, let $\tilde{M}(e) = 1$. As in the proof of Theorem I.7.6, we use a diagonal argument. Let $\tilde{M}$ be encoded by $u \in \mathbb{N}$ and $n = 2^u 3^u$. In the case $\varphi(n) = 1$, $\tilde{M}$ terminates on input u (definition of φ), but then $\varphi(n) = M(n) = 0$ would hold. In the case $\varphi(n) = 0$, on the other hand, $\tilde{M}$ would not terminate on input u and $\varphi(n) = M(n) = 1$. Contradiction. □

Remark I.8.16.

(i) Suppose there is an algorithm that decides whether a Turing machine terminates at least on the empty tape. The following algorithm would then also decide the general halting problem: For a given Turing machine T and an input $e \in \mathbb{N}$, construct the Turing machine $\tilde{T}$ that first writes e onto the empty tape (this is always possible by defining a separate state for each step if necessary) and subsequently executes T. Now T terminates with input e if and only if $\tilde{T}$ terminates on the empty tape. Therefore, the halting problem on the empty tape is also undecidable.

(ii) The halting problem can be generalized much further: Let E be a non-trivial property concerning the behavior of a Turing machine T (e. g., whether T writes a 1 at position 10 or whether all outputs are smaller than 100). Non-trivial here only means that E holds neither for all nor for no Turing machine. The theorem of Rice states that no algorithm exists that decides whether a given Turing machine possesses property E. It follows from this that even the best compilers cannot find every bug in a program code.

(iii) There are so-called *universelle* Turing machines that can simulate any Turing machine given the appropriate input (precursor to a programmable computer). This is already possible with relatively small parameters such as $(|A|, |Z|, |I|) = (5, 5, 22)$.

Definition I.8.17. For $x, y \in \mathbb{N}$, let $\boldsymbol{\rho}(x, y)$ be the largest possible number of steps that a terminating Turing machine $T = (A, Z, I)$ with $|A| = x$ and $|Z| = y$ can execute on the empty tape (additionally set $\boldsymbol{\rho}(0, y) = 0 = \boldsymbol{\rho}(x, 0)$). Since there are only finitely many such machines due to $|I| \leq xy$, $\boldsymbol{\rho}$ is well-defined. One calls $\boldsymbol{\rho}$ the *Radó-Funktion* or *fleißiger Biber*.

Theorem I.8.18. *The Radó function is uncomputable.*

Proof. If $\boldsymbol{\rho}$ is computable, one obtains the following algorithm for the halting problem: Let a Turing machine $T = (A, Z, I)$ run for $\boldsymbol{\rho}(|A|, |Z|)$ steps on the empty tape. If T has not stopped by then, one knows that T never stops. This contradicts Remark I.8.16. □

Example I.8.19. One is mainly interested in the values $\boldsymbol{\rho}(2, n)$, i. e. Turing machines with alphabet $\{\triangle, 1\}$.[31] Traditionally, one also counts the last step when there is no more applicable instruction and the machine transitions into the "halting state". With this convention, one obtains

n	1	2	3	4	5
$\boldsymbol{\rho}(2, n)$	1	6	21	107	47.176.870

[31] The function $\mathbb{N} \to \mathbb{N}$, $n \mapsto \boldsymbol{\rho}(2, n)$ is also uncomputable. For this, one must show that every Turing machine can be simulated by a Turing machine with a 2-element alphabet.

where $\boldsymbol{\rho}(2,5)$ was only determined in the year 2024.[32] The following instructions describe a corresponding machine with five states:

$$\begin{array}{lllll} (a,\triangle,1,1,b), & (a,1,1,-1,c), & (b,\triangle,1,1,c), & (b,1,1,1,b), & (c,\triangle,1,1,d) \\ (d,1,\triangle,-1,e), & (d,\triangle,1,-1,a) & (d,1,1,-1,d), & (e,1,\triangle,-1,a) & \end{array}$$

The determination of $\boldsymbol{\rho}(2,6)$ is hopeless, as this value reaches orders of magnitude that can only be captured with special notation.

Lemma I.8.20. *Every computable function can be simulated on a Turing machine without using the negative half of the tape* (*i. e. one works on a* one-sided *infinite tape*).

Proof. Let $T = (A, Z, I)$ be a Turing machine. We define a new Turing machine $\tilde{T} := (\tilde{A}, \tilde{Z}, \tilde{I})$ with extended parameters as follows:

(i) Let $\boldsymbol{s}$ and $\tilde{\boldsymbol{s}}$ be the start states of T and $\tilde{T}$, respectively. At the beginning, a "stop mark" with a new symbol $\|$ is written onto the tape. For this purpose, the instructions $(\tilde{\boldsymbol{s}}, \triangle, \|, 1, \boldsymbol{s}), (\tilde{\boldsymbol{s}}, a, a, -1, \tilde{\boldsymbol{s}}) \in \tilde{I}$ for all $a \in A \setminus \{\triangle\}$ are used. If the tape is initially empty, then $\|$ is at position 0, and otherwise at position -1.

(ii) The instructions of T can be adopted into $\tilde{T}$ almost unchanged. We merely prevent $\tilde{T}$ from leaving "gaps" on the tape by writing a new replacement character ▲ instead of $\triangle$. Instructions of the form $(*,*,\triangle,*,*)$ are thus replaced by $(*,*,\blacktriangle,*,*)$. For every instruction of the form $(*,\triangle,*,*,*)$, one additionally needs the corresponding instruction $(*,\blacktriangle,*,*,*)$ in $\tilde{I}$. At the end, these characters can be replaced by $\triangle$ again.

(iii) If the read head moves onto the stop mark during execution, the tape content written so far shall be shifted one position to the right. The instructions $(z, \|, \|, 1, \tilde{z})$ for all $z \in Z$ cause the read head to slide from $\|$ to the right and put $\tilde{T}$ into a new state $\tilde{z} \in \tilde{Z}$. So that the execution can later be continued in state z, we write a new symbol $a_z \in \tilde{A}$ onto the tape: $(\tilde{z}, b, a_z, 1, z_b)$ for all $z \in Z$ and $b \in A$. Here, $z_b \in \tilde{Z}$ is a new state that serves as a buffer for the read symbol b. The actual shifting of the tape content happens through the instructions $(z_a, b, a, 1, z_b)$ for all $a, b \in A \cup \{\blacktriangle\}$ with $a \neq \triangle$. At the right end, $\tilde{T}$ is in state $z_\triangle$.

(iv) Through the instructions $(z_\triangle, a, a, -1, z_\triangle)$, $(z_\triangle, a_z, \triangle, -1, \tilde{z})$ and $(\tilde{z}, \|, \|, 1, z)$ for all $a \in A \cup \{\blacktriangle\}$ and $z \in Z$, the read head is guided back to the stop mark. Now $\tilde{T}$ can continue with the instructions from T.

(v) If T does not terminate, then $\tilde{T}$ will also not terminate and the tape content is irrelevant. Let us therefore assume that T terminates. Then for a pair $(z, a) \in \tilde{Z} \times \tilde{A}$ there is no matching instruction $(z, a, *, *, *)$. To remove the symbols ▲ introduced in (ii), we can introduce for each such pair (z, a) a new instruction $(z, a, a, -1, q)$ with a new "final state" $q \in \tilde{Z}$. In this state, $\tilde{T}$ moves to the left to $\|$ without changing anything. Subsequently, $\tilde{T}$ moves to the right applying $(q, \blacktriangle, \triangle, 1, q)$ until $\triangle$ appears on the tape for the first time. There $\tilde{T}$ terminates. □

Theorem I.8.21 (Turing)**.** *There is no general algorithm that decides whether a closed formula of Peano arithmetic is true.*

[32] See Quanta magazine

Proof. Idea: For every Turing machine $T = (A, Z, I)$, construct a closed formula f_T in $\mathcal{PA}$ that is true with respect to the standard interpretation if and only if T terminates on the empty tape. If one had an algorithm that decides whether f_T is true, then by Remark I.8.16 one would also have a procedure to solve the halting problem.

According to Lemma I.8.20, we can assume that T only describes the tape positions indexed by $\mathbb{N}$. Wlog. let $A := \{0, \ldots, a\}$ and $Z := \{0, \ldots, z\}$, where 0 stands for $\triangle$ and $\boldsymbol{s}$ respectively. Each step of T is described by a tuple $t := (z, i, a_0, \ldots, a_n)$, where $z \in Z$ is the current state, $i \in \mathbb{N}$ is the position of the read head, and $a_0, \ldots, a_n \in A$ is the tape content used so far. By means of Gödelization, t can be encoded in a number $x \in \mathbb{N}$. There are recursive functions $\alpha(x) = z$, $\beta(x) = i$, $\gamma(x) = n$, and $\delta(x, k) = a_k$, where $\delta(x, k) = 0$ for $k > n$. The initial state is described by the formula

$$f_s(x) := \big(\alpha(x) = 0 \wedge \beta(x) = 0 \wedge \gamma(x) = 0 \wedge \delta(x, 0) = 0\big).$$

For each instruction $I_j = (z, a, *, *, *) \in I$, there exists a formula

$$f_j(x) := \big(\alpha(x) = z \wedge \delta(x, \beta(x)) = a\big),$$

which is true if and only if I_j is applicable in configuration t. For $I = \{I_1, \ldots, I_l\}$, it holds that

$$f_c(x) := f_1 \vee \ldots \vee f_l$$

if and only if T does not stop in configuration t. The sequence of configurations $x_0, \ldots, x_m$ can be encoded with Gödel's $\boldsymbol{\beta}$-function, i.e., there exist $a, b \in \mathbb{N}$ with $\boldsymbol{\beta}(a, b, i) = x_i$ for $i = 0, \ldots, m$. The transition from $x := x_i$ to $y := x_{i+1}$ again depends on the existence of an instruction $I_j = (z, a, b, r, w)$:

$$\begin{aligned} g_j(x, y) := \Big(& f_j(x) \wedge \alpha(y) = w \wedge \beta(y) = \beta(x) + r \wedge \delta(y, \beta(x)) = b \\ & \wedge \big(\gamma(y) = \gamma(x) \vee (\gamma(y) = \gamma(x) + 1 \wedge \beta(x) = \gamma(x) \wedge r = 1)\big) \\ & \wedge \forall k \leq \gamma(y)(k = \beta(x) \vee \delta(x, k) = \delta(y, k))\Big) \end{aligned}$$

The following formula is true if and only if T terminates (after n steps):

$$f_T := \exists a \exists b \exists n \Big(f_s(\boldsymbol{\beta}(a, b, 0)) \wedge \neg f_c(\boldsymbol{\beta}(a, b, n)) \wedge \forall i < n \, \exists \, j \leq l \big(g_j(\boldsymbol{\beta}(a, b, i), \boldsymbol{\beta}(a, b, i + 1))\big)\Big)$$

Since the functions used are recursive, f_T can be represented in $\mathcal{PA}$ according to Theorem I.6.9. By substituting the constants (Definition I.6.2), f_T becomes a closed formula. □

Corollary I.8.22 (=Theorem I.7.6)**.** *Peano arithmetic is incomplete.*

Proof. Suppose $\mathcal{PA}$ were complete. For every closed formula f, it holds that $\vDash_{\mathbb{N}} f$ or $\vDash_{\mathbb{N}} \neg f$, thus also $\vdash f$ or $\vdash \neg f$. For every natural number n, one can recursively (and thus computably according to Example I.8.11) check whether n encodes a proof of f or $\neg f$. After finite time, one of the two cases must occur. This would provide a decision procedure for $\mathcal{PA}$ in contradiction to Theorem I.8.21. □

Remark I.8.23. For a first-order predicate logic $\mathcal{K}$ (with at least one n-ary predicate with $n \geq 2$), one can show in a similar way that no algorithm exists that decides whether a given formula is a tautology (*Church's Theorem*). According to the Completeness Theorem I.4.6, there is also no algorithm that decides whether a formula f is provable. In contrast to Corollary I.8.22, it is not sufficient to enumerate all theorems in $\mathcal{K}$, because it can happen that neither f nor $\neg f$ are provable (Remark I.3.6).

Exercises

Exercise I.1. Let $x, y \in \{1, 2, \ldots, 9\}$. The logician (S)iegfried knows only the sum $x + y$, while his colleague (P)etrus knows only the product xy. The two have the following strange conversation:

S: "I do not know x and y."
P: "I do not know x and y."
S: "I do not know x and y."
P: "I do not know x and y."
S: "I do not know x and y."
P: "I do not know x and y."
S: "I do not know x and y."
P: "I do not know x and y."
S: "I do not know x and y."
P: "Now I know x and y!"

Determine x and y.
Remark: Assume that S and P draw all possible correct logical conclusions.

Exercise I.2. Let $\mathcal{K}$ be the calculus from Example I.1.4. Show that a word l is provable in $\mathcal{K}$ if and only if l contains an odd number of a's.

Exercise I.3. Construct calculi $\mathcal{K}$ with the following properties:

(a) $\mathcal{K}$ is negation-complete, but not complete.

(b) $\mathcal{K}$ is consistent, but not sound.

Exercise I.4.

(a) Show that $\Rightarrow$ is not associative in $\mathcal{A}$, i. e.

$$\nvdash ((A \Rightarrow B) \Rightarrow C) \Rightarrow (A \Rightarrow (B \Rightarrow C))$$
$$\nvdash (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow C)$$

(b) Prove the inference rule $\frac{A \Rightarrow (B \Rightarrow C)}{B \Rightarrow (A \Rightarrow C)}$ in $\mathcal{A}$.
Hint: Due to Theorem I.2.13, one can use Theorem I.2.5.

(c) Prove the inference rule $\frac{A, B}{A \wedge B}$ in $\mathcal{A}$.

Exercise I.5. Show that one can describe $\mathcal{A}$ using only the symbols (,) and $\circledast$. Here, let $A \circledast B$ be equivalent to $\neg(A \vee B)$.

Exercise I.6. We define in $\mathcal{A}$ three "truth values" $0, 1, 2$ with the following interpretation:

A	B	$\neg A$	$A \Rightarrow B$
0	0	1	0
1	0	1	2
2	0	0	0
0	1		2
1	1		2
2	1		0
0	2		2
1	2		0
2	2		0

Statements with value 0 we call *true*. Show:

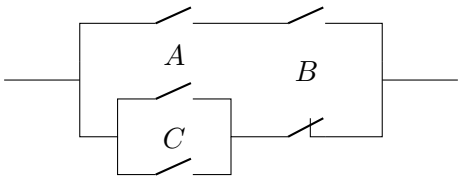
(a) Every statement derived from $(\mathcal{A}_2)$ and $(\mathcal{A}_3)$ is true.

(b) One cannot derive $(\mathcal{A}_1)$ from $(\mathcal{A}_2)$ and $(\mathcal{A}_3)$.

Remark: In a similar way, one can show the independence of $(\mathcal{A}_2)$ and $(\mathcal{A}_3)$.

Exercise I.7. You are a judge in a trial with two defendants, one of whom always tells the truth, while the other always lies. However, you do not know who tells the truth. With which yes-no question to one of the defendants can you solve the crime?
Note: Let A and B be the statements "defendant lies" and "defendant pleads not guilty". Construct the truth table for the Boolean function "defendant is guilty" and derive an equivalent formula.

Exercise I.8. With propositional logic, one can model simple circuits. Each elementary statement corresponds to a switch that allows or blocks the flow of current (e. g. a light switch). The statement $(A \wedge B) \vee ((A \vee C) \wedge \neg B)$ is true if and only if current flows in the following circuit:



(a) Construct a simpler circuit with equivalent behavior.

(b) A lamp in a room should be able to be switched on and off by two light switches independently of each other (operating a switch should always change the state of the lamp). Construct a corresponding circuit.

Exercise I.9. Construct a first-order predicate logic that models graphs.

Exercise I.10. Show:

(a) The deduction lemma I.1.10 holds for closed formulas in $\mathcal{P}$.

(b) In general, Lemma I.1.10 does not hold in $\mathcal{P}$, i. e. from $f \vdash g$ it does not necessarily follow that $\vdash f \Rightarrow g$.

Exercise I.11. Let f, g and h be formulas in $\mathcal{P}$. Prove the formula known from Lemma I.1.11

$$\vdash (f \Rightarrow g) \Rightarrow ((g \Rightarrow h) \Rightarrow (f \Rightarrow h))$$

without using Lemma I.1.10.
Remark: Supplement the proof steps of Lemma I.1.10 in the proof of Lemma I.1.11.

Exercise I.12. Let M be a set of formulas in a first-order calculus. Let $f(x)$ be a formula and c a constant which neither occurs in M nor in f. Show: $M \vdash f(x \leftarrow c)$ implies $M \vdash \forall x f$.

Exercise I.13. Show that every sound interpretation of Peano arithmetic has an infinite universe.

Exercise I.14. Prove $\vdash t \cdot u = u \cdot t$ and $\vdash t \cdot (u \cdot v) = (t \cdot u) \cdot v$ for terms t, u, v in $\mathcal{PA}$.

Exercise I.15. We assume that $\mathcal{PA}$ is consistent. Prove syntactically $\nvdash x = 0$ and $\nvdash x \neq 0$ without using the soundness of $\mathcal{PA}$.

Exercise I.16. Define an interpretation of Robinson arithmetic $\mathcal{R}$ with respect to which addition is not commutative.
Hint: $U := \mathbb{N} \cup \{a, b\}$.

Exercise I.17. Construct Turing machines T with alphabet $\{\triangle, 0, 1\}$ with

(a) $T(n) = 2n$ for all $n \in \mathbb{N}$.

(b) $T(n) = n + 1$ for all $n \in \mathbb{N}$.

The input and output should (in contrast to Example I.8.8) be in binary representation.

Exercise I.18. Show that every value of the Ackermann function has the form $2^n - 1$ with $n \geq 1$.

Exercise I.19. Show that $\varphi \circ \psi$ is computable if $\varphi, \psi \colon \mathbb{N} \to \mathbb{N}$ are computable.

Exercise I.20. Construct a Turing machine $T = (A, Z, I)$ with $|A| = |Z| = 2$ that halts on the empty tape after exactly five steps.

II. Set Theory

II.1. Sets

Remark II.1.1. In this chapter, we define and investigate a calculus that, based on the concept of sets, can express practically all parts of modern mathematics. We had already spoken intuitively of sets in chapter I. Cantor made the following attempt to describe a set in colloquial language.

Definition II.1.2 (Cantor)**.** A *set* M is a collection of definite, well-distinguished objects x of our intuition or of our thought into a whole. One then says: x is an *element* of M and writes $x \in M$ as well as $M = \{x : x \in M\}$ (respectively $x \notin M$ for $\neg(x \in M)$). The number $|M|$ of elements of M is called the *cardinality* or *power* of M. One calls M *empty*, *finite* or *infinite*, if M contains no elements, finitely many, or infinitely many elements, respectively.

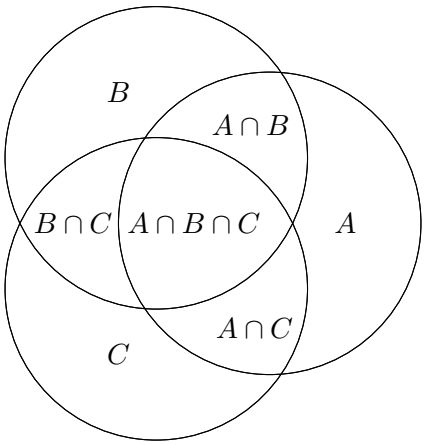
Remark II.1.3 (Russell's Paradox)**.** Definition II.1.2 is imprecise, because it allows sets that lead to logical contradictions. For example, let M be the set of all sets that do not contain themselves. The statement $M \in M$ can then be neither true nor false. Likewise, the notation $|M|$ for infinite sets is imprecise, because we will see that there are several infinite cardinalities (Definition II.5.1). To prevent such contradictions, we will establish a calculus in Definition II.1.6. In the following, we define the symbols required for this and their meaning.

Definition II.1.4. For sets A and B, let

$$\begin{aligned} A \cup B &:= \{x : x \in A \vee x \in B\} && (\textit{union}),\\ A \cap B &:= \{x : x \in A \wedge x \in B\} && (\textit{intersection}),\\ A \setminus B &:= \{x : x \in A \wedge x \notin B\} && (\textit{difference}). \end{aligned}$$

In the case $A \cup B = B$, A is a *subset* of B. One then writes $A \subseteq B$ or $A \subsetneq B$, if additionally $A \neq B$ (one then speaks of a *proper* subset). If A is not a subset of B, one writes $A \nsubseteq B$.

Remark II.1.5. Unions and intersections of sets can be represented graphically by Venn *diagrams*:



If more than three sets are involved, the general situation can no longer be represented by circles. The cover image shows a Venn diagram for five sets using ellipses.

Definition II.1.6 (Zermelo-Fraenkel)**.** The *Zermelo-Fraenkel calculus* $\mathcal{ZF}$ of set theory is a first-order predicate logic with equality. For variables, the Latin alphabet is used (lowercase letters are usually interpreted as elements and uppercase letters as sets). In addition to the usual symbols (Definition I.3.9), there are $\in$, $:$, $\{$, $\}$, $\cup$, $\cap$ and $\setminus$. The following axioms hold:

(1) (Axiom of infinity) There exists an infinite set M with $x \in M \Rightarrow x \cup \{x\} \in M$.

(2) (Axiom of extensionality) Sets are equal if and only if they contain the same elements.

(3) (Axiom of foundation) Every non-empty set M has an element $x \in M$ such that $M \cap x$ is empty.

(4) (Axiom of replacement) Let $A(x, y)$ be a predicate with the property $(A(x, y) \wedge A(x, z)) \Rightarrow y = z$. For every set B, there exists a set C with $x \in C \Leftrightarrow (\exists y \in B : A(x, y))$.

(5) (Axiom of union) For every set A, there exists a set B with the property $x \in B \Leftrightarrow (\exists C \in A : x \in C)$. One writes $B = \bigcup_{a \in A} a$.

(6) (Axiom of power set) For every set M, $\mathcal{P}(M) := \{N : N \subseteq M\}$ is also a set, which is called the *power set* of M.

(7) (Axiom of choice) If A is a set of non-empty sets, then there exists a set B that contains exactly one $x \in C$ for every $C \in A$.

Remark II.1.7.

(i) In the literature, one finds further (historically motivated) axioms, which can however be derived from those mentioned above. For example, the Axiom of Replacement implies the

Axiom of separation: If $A(x)$ is a predicate and B is a set, then there exists a set C with $x \in C \Leftrightarrow (x \in B \wedge A(x))$

(choose $A(x, y) := (x = y \wedge A(x))$). One writes $C = \{x \in B : A(x)\}$. From the Axiom of Infinity and the Axiom of Separation, one obtains the

Axiom of the empty set: There exists an empty set $\varnothing$.

(choose $A(x) := \mathbf{f}$). According to the Axiom of Extensionality, $\varnothing$ is the unique empty set. Finally, one obtains the

Axiom of pairing: For sets A and B, there exists a set C that has only A and B as elements.

For this, one applies the Axiom of Replacement to

$$M := \mathcal{P}(\mathcal{P}(\varnothing)) = \mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$$

with the predicate

$$A(x, y) := (x = \varnothing \wedge y = A) \vee (x = \{\varnothing\} \wedge y = B).$$

One writes $C = \{A, B\}$. With the Axiom of Union, it finally follows that $A \cup B$ is indeed a set. The Axiom of Separation guarantees that $A \cap B$ and $A \setminus B$ are also sets.

(ii) The Axiom of Foundation prevents Russell's paradox. We will see in Example II.4.9 that $\mathcal{ZF}$ can express Peano arithmetic. According to Gödel's Second Incompleteness Theorem I.7.10, one therefore cannot prove the consistency of $\mathcal{ZF}$ within $\mathcal{ZF}$. If $\mathcal{ZF}$ is indeed consistent (which most mathematicians assume), then according to Gödel's First Incompleteness Theorem I.7.6, there must be true statements that cannot be proven. The best-known example of this is the *Continuum Hypothesis* (see Remark II.5.12).

(iii) If one has (infinitely) many pairs of shoes, it is easy to choose exactly one shoe from each pair: choose the right shoe. If, on the other hand, one considers pairs of socks, this is no longer so clear. The Axiom of Choice guarantees that one can always make such a choice.

(iv) Some mathematicians dispense with the Axiom of Choice because it allows the construction of counterintuitive sets: the *Banach-Tarski Paradox*, for example, states that one can decompose a three-dimensional ball into finitely many pieces which, when reassembled differently, yield two balls of the same volume as the original ball.

(v) In rare cases, one needs objects that are too "large" to be sets. These are called *classes*. For example, the collection of all sets is a class (Remark II.5.12).

Definition II.1.8. Two sets A and B are called *disjoint*, if $A \cap B = \varnothing$. If applicable, we call $A \dot\cup B := A \cup B$ a *disjoint* union.

Lemma II.1.9. *For sets A, B and C, the following hold:*

(i) $A \cup A = A = A \cap A$ (*Idempotence*).

(ii) $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$ (*Commutativity*).

(iii) $(A \cup B) \cup C = A \cup (B \cup C)$ *and* $(A \cap B) \cap C = A \cap (B \cap C)$ (*Associativity*).

(iv) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *and* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (*Distributivity*).

(v) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ *and* $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ (*De Morgan's laws*).

(vi) $A \cap B \subseteq A \subseteq A \cup B$.

Proof. By logical deduction using Theorem I.2.5 or with Venn diagrams. For example

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow (x \in A \wedge (x \in B \cup C)) \Leftrightarrow (x \in A \wedge (x \in B \vee x \in C)) \\ &\Leftrightarrow ((x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)) \Leftrightarrow x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

□

II.2. Relations and Functions

Definition II.2.1.

(i) Let A and B be sets with $a \in A$ and $b \in B$. Then $(a, b) := \{\{a\}, \{a, b\}\}$ is called an (*ordered*) *pair* of a and b. In contrast to the set $\{a, b\}$, it holds that $(a, b) = (a', b') \Leftrightarrow (a = a' \wedge b = b')$.

(ii) The set
$$A \times B := \{(a, b) : a \in A \wedge b \in B\}$$
is called the *Cartesian product* of A and B.

(iii) Inductively, one defines *triples* $(a, b, c) := (a, (b, c))$ and more generally *n-tuples* $(a_1, \ldots, a_n) := (a_1, (a_2, \ldots, a_n))$ for $n \geq 2$. Analogously, $A_1 \times \ldots \times A_n := A_1 \times (A_2 \times \ldots \times A_n)$ for sets $A_1, \ldots, A_n$. Specifically, one sets $A^n := A \times \ldots \times A$ (n factors).

(iv) A *relation* on A is a subset $\sim \subseteq A \times A$. One then writes $a \sim b$ if $(a, b) \in \sim$. One calls $\sim$

- *reflexive*, if $\forall a \in A : a \sim a$.
- *symmetric*, if $\forall a, b \in A : (a \sim b \Rightarrow b \sim a)$.
- *antisymmetric*, if $\forall a, b \in A : (a \sim b \sim a \Rightarrow a = b)$.
- *transitive*, if $\forall a, b, c \in A : (a \sim b \sim c \Rightarrow a \sim c)$.
- *total*, if $\forall a, b \in A : (a \sim b \vee b \sim a)$.
- *equivalence relation*, if $\sim$ is reflexive, symmetric, and transitive.
- *order relation*, if $\sim$ is reflexive, antisymmetric, and transitive.

(v) If $\sim$ is an equivalence relation on the set A and $a \in A$, then $[a] := \{b \in A : a \sim b\} \subseteq A$ is called the *equivalence class* of a.

Example II.2.2. Let M be a set.

(i) The relation $M \times M$ is obviously an (uninteresting) equivalence relation on M.

(ii) The equality relation is the "smallest" reflexive relation on M. Furthermore, it is an equivalence relation.

(iii) The subset relation $\subseteq$ is an order relation on $\mathcal{P}(M)$. In the case $|M| > 1$, $\subseteq$ is not total, because $\{a\} \not\subseteq \{b\} \not\subseteq \{a\}$ for distinct $a, b \in M$.

(iv) If $\sim$ is an equivalence relation (or order relation) and $A \subseteq M$, then $\sim \cap A \times A$ is an equivalence relation (or order relation) on A.

Lemma II.2.3. *If $\sim$ is an equivalence relation on a set A, then there exists an $\mathcal{R} \subseteq A$ such that A is the disjoint union of the equivalence classes $[r]$ with $r \in \mathcal{R}$.*

Proof. Let $a, b \in A$ and $c \in [a] \cap [b]$. Then $a \sim c$ and $b \sim c$ hold. Since $\sim$ is symmetric, $c \sim b$ holds. Since $\sim$ is transitive, $a \sim b$ holds. For every $d \in [b]$, it thus holds that $a \sim b \sim d$ and $a \sim d$. This shows $[b] \subseteq [a]$ and analogously one obtains $[a] \subseteq [b]$. It follows that $[a] = [b]$. Thus, any two equivalence classes are either equal or disjoint. The existence of $\mathcal{R}$ now follows from the axiom of choice. $\square$

Remark II.2.4. In the situation of Lemma II.2.3, $\mathcal{R}$ is called a *system of representatives* for the equivalence classes.

Definition II.2.5.

(i) Let A and B be sets. A *partial function* or *map* from A to B is a subset $f \subseteq A \times B$, such that for each $a \in A$ at most one $b \in B$ with $(a, b) \in f$ exists. One then writes $f(a) = b$ and

$$f\colon A \rightharpoonup B, \qquad a \mapsto f(a)$$

instead of $(a, b) \in f$. One calls $\{a \in A : \exists b : f(a) = b\}$ the *domain* and B the *codomain* of f.

(ii) If for each a exactly one $b \in B$ with $(a, b) \in f$ exists, then f is called *total* and one writes $f\colon A \to B$. Unless stated otherwise, we always assume that functions are total.

(iii) One calls $f(a)$ the *image* of $a \in A$ under f and $f(A) := \{f(a) : a \in A\} \subseteq B$ is the *image* of f. For $C \subseteq B$, $f^{-1}(C) := \{a \in A : f(a) \in C\} \subseteq A$ is the *preimage* of C under f.

(iv) One calls f

- *injective*, if $\forall a, a' \in A : (f(a) = f(a') \Rightarrow a = a')$.
- *surjective*, if $\forall b \in B : \exists a \in A : f(a) = b$, i. e. $f(A) = B$.
- *bijective* (or *bijection*), if f is injective and surjective. One then calls A and B *equinumerous*.
- *permutation*, if f is bijective and $A = B$. The set of all permutations on A is denoted by $\mathrm{Sym}(A)$.

(v) If $f\colon A \to B$ and $g\colon B \to C$ are functions, then so is $g \circ f\colon A \to C$ with $(g \circ f)(a) := g(f(a))$ for $a \in A$. One calls $g \circ f$ the *composition* (or *concatenation*) of f and g.

(vi) If $f\colon A \to B$ is a function and $C \subseteq A$, then the *restriction* $f_{|C}\colon C \to B$, $c \mapsto f(c)$ is also a function. Every partial function becomes total if one restricts it to its domain.

Example II.2.6.

(i) For every set A and $B \subseteq A$, $f\colon B \to A$, $b \mapsto b$ is an injective function, which is called *inclusion (map)* or *embedding*. In the case $B = A$, f is even bijective and one calls $\mathrm{id}_A := f$ the *identity* on A.

(ii) For sets A and B, $f\colon A \times B \to B \times A$, $(a, b) \mapsto (b, a)$ is certainly a bijection.

(iii) For an arbitrary index set I and sets A_i $(i \in I)$, one can define the Cartesian product $\bigtimes_{i \in I} A_i$ as the set of all functions $I \to \bigcup_{i \in I} A_i$ with $f(i) \in A_i$ for $i \in I$. For finite I, this is equivalent to our original definition. One therefore also writes the elements in $\bigtimes_{i \in I} A_i$ in the form $(a_i)_{i \in I}$.

(iv) Two finite sets A and B are obviously equinumerous if and only if $|A| = |B|$ (see also Theorem II.5.4).

Lemma II.2.7. *Let $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$ be functions with $A \neq \varnothing$. Then the following hold:*

(i) $(h \circ g) \circ f = h \circ (g \circ f) =: h \circ g \circ f$ *(associativity).*

(ii) If f and g are injective, then so is $g \circ f$.

(iii) If f and g are surjective, then so is $g \circ f$.

(iv) *If $g \circ f$ is injective, then f is injective.*

(v) *If $g \circ f$ is surjective, then g is surjective.*

(vi) *f is injective if and only if there exists a function $g\colon B \to A$ with $g \circ f = \mathrm{id}_A$.*

(vii) *f is surjective if and only if there exists a function $g\colon B \to A$ with $f \circ g = \mathrm{id}_B$.*

(viii) *f is bijective if and only if there exists a function $g\colon B \to A$ with $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. If applicable, g is uniquely determined and one calls $f^{-1} := g$ the* inverse function *of f.*

Proof.

(i) For $a \in A$ we have $((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a))) = h((g \circ f)(a)) = (h \circ (g \circ f))(a)$.

(ii) For $a, a' \in A$ with $(g \circ f)(a) = (g \circ f)(a')$ it holds that $g(f(a)) = g(f(a'))$, thus $f(a) = f(a')$ and $a = a'$.

(iii) It holds that $(g \circ f)(A) = g(f(A)) = g(B) = C$.

(iv) Let $f(a) = f(a')$ for $a, a' \in A$. Then $(g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a')$. Since $g \circ f$ is injective, it follows that $a = a'$. Thus f is injective.

(v) It holds that $C = (g \circ f)(A) = g(f(A)) \subseteq g(B) \subseteq C$, thus $g(B) = C$.

(vi) If $g \circ f = \mathrm{id}_A$, then f is injective according to (iv). Conversely, let f be injective and $c \in A$ be a fixed choice (note: $A \neq \varnothing$). We define $g\colon B \to A$ as follows: if $b = f(a)$ for some $a \in A$, let $g(b) := a$ and otherwise $g(b) := c$. Since f is injective, g is thereby well-defined. Furthermore, $(g \circ f)(a) = g(f(a)) = a$ for $a \in A$, thus $g \circ f = \mathrm{id}_A$.

(vii) If $f \circ g = \mathrm{id}_B$, then f is surjective according to (v). Conversely, let f be surjective, i. e. $f(A) = B$. According to the axiom of choice, there exists a function $g\colon B \to A$ with $g(b) \in f^{-1}(b)$ for all $b \in B$. Obviously, $(f \circ g)(b) = f(g(b)) = b$, i. e. $f \circ g = \mathrm{id}_B$.

(viii) If $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$, then f is injective and surjective according to (iv) and (v), thus also bijective. Conversely, let f be bijective. According to (vi) and (vii), there exist $g\colon B \to A$ and $h\colon B \to A$ with $g \circ f = \mathrm{id}_A$ and $f \circ h = \mathrm{id}_B$. Then $g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h$. This also shows that g is uniquely determined. □

Theorem II.2.8 (Cantor-Bernstein)**.** *Let A and B be sets with injective mappings $f\colon A \to B$ and $g\colon B \to A$. Then A and B have the same cardinality.*

Proof. We define $C_0 := A \setminus g(B)$ and $C_n := g(f(C_{n-1}))$ for $n \geq 1$. Furthermore, let $C := \bigcup_{n=0}^{\infty} C_n$ and $h\colon A \to B$ with

$$h(x) := \begin{cases} f(x) & \text{if } x \in C, \\ g^{-1}(x) & \text{if } x \notin C. \end{cases}$$

In the case $x \notin C$, we have $x \notin C_0$, i. e. $x \in g(B)$. Consequently, $g^{-1}(x)$ is uniquely determined by the injectivity of g and h is well-defined. Now let $x, y \in A$ with $h(x) = h(y)$. Suppose $x \in C$ and $y \notin C$. Then $f(x) = g^{-1}(y)$ and $g(f(x)) = y$. Let $x \in C_n$ for some $n \geq 0$. Then the contradiction $y = g(f(x)) \in g(f(C_n)) = C_{n+1} \subseteq C$ follows. Thus $x, y \in C$ or $x, y \notin C$ and one obtains $x = y$. Therefore h is injective.

Now let $y \in B$ be arbitrary. In the case $g(y) \notin C$, we have $h(g(y)) = g^{-1}(g(y)) = y$. So let $g(y) \in C_n$ for some $n \geq 1$. Then there exists an $x \in C_{n-1}$ with $g(f(x)) = g(y)$. From the injectivity of g it follows that $h(x) = f(x) = y$. Thus h is also surjective and bijective. □

Remark II.2.9. We give an interesting application of the Axiom of Choice.

Theorem II.2.10. *Let an arbitrary set of dwarfs with red or green hats be given. The dwarfs can see the hats of the other dwarfs, but not their own. They cannot communicate with each other. Then:*

(i) (Gabay-O'Connor) *There exists a strategy with which all but finitely many dwarfs guess their hat color correctly.*

(ii) (Lenstra) *There exists a strategy with which either all dwarfs guess their hat color correctly or all dwarfs guess their hat color incorrectly.*

(iii) There exists a strategy with which at least 50% *of all dwarfs guess their hat color correctly.*

Proof. Let Z be the set of dwarfs and $F := \{Z \to \{r, g\}\}$ the set of all hat distributions. For $f, f' \in F$, let $f \sim f'$ if f and f' differ at only finitely many positions. Obviously, $\sim$ defines an equivalence relation on F. According to the Axiom of Choice, one can choose a representative $f_0 \in F$ for each equivalence class $[f]$. Now let f be the given hat distribution. Then all dwarfs can determine f_0.

(i) Dwarf $z \in Z$ guesses $f_0(z)$ as his hat color. Since f differs from f_0 at only finitely many positions, all but finitely many dwarfs guess their hat color correctly.

(ii) Each dwarf $z \in Z$ can determine the finite cardinality

$$n(z) := \big|\{z' \in Z \setminus \{z\} : f_0(z') \neq f(z)\}\big|$$

If $n(z)$ is an even number, then z guesses his hat color $f_0(z)$ and otherwise the color different from $f_0(z)$. If f and f_0 differ at an even number of positions, then all dwarfs guess their hat color correctly. Otherwise, all dwarfs guess their hat color incorrectly.

(iii) We assume that the hats are uniformly distributed. Let $z \in Z$ be fixed and $h \in [f]$. Let $h' \in [f]$ with $h'(z) \neq h(z)$ and $h'(z') = h(z')$ for all $z' \in Z \setminus \{z\}$. Then $h \to h'$ is a permutation on $[f]$, such that the number of differences between f_0 and h as well as between f_0 and h' differ by exactly 1. Therefore, the two cases in (ii) occur equally frequently. □

Example II.2.11. Suppose there are only finitely many dwarfs. Then one can choose for f_0 the constant function with $f_0(z) = g$ for all $z \in Z$. If a dwarf sees an even number of red hats, he guesses his own hat color as green and otherwise as red. If there is an even number of red hats in total, then all dwarfs guess their hat color correctly.

II.3. Ordered Sets

Definition II.3.1. Let $\leq$ be an order relation on a set A and $B \subseteq A$.

(i) As usual, we use the notations $a \geq a'$ (if $a' \leq a$), $a < a'$ (if $a \leq a' \neq a$) and $a > a'$ (if $a' \leq a \neq a'$) for $a, a' \in A$.

(ii) An $a \in A$ is called

- *greatest* element, if $\forall a' \in A : a' \leq a$.
- *maximal* element, if $\forall a' \in A : (a \leq a' \Rightarrow a = a')$.

Analogously, one defines *least* and *minimal* elements of A.

(iii) An $a \in A$ is called an *upper bound* of B, if $\forall b \in B : b \leq a$. Analogously, one defines *lower bounds* of B.

(iv) A is called *well-ordered*, if every non-empty subset of A contains a least element.

(v) For $a \in A$ let $A^{<a} := \{a' \in A : a' < a\}$.

Remark II.3.2.

(i) In general, neither greatest elements, nor maximal elements, nor upper bounds exist. If $a \in A$ is a greatest element, then a is the unique greatest and the unique maximal element in A. One then writes $a = \max M$ (analogously $\min M$ for the least element). In totally ordered sets, the concepts of greatest element and maximal element coincide.

(ii) Well-ordered sets are always totally ordered. Conversely, a totally ordered set is already well-ordered if there is no infinite sequence of the form $a_0 > a_1 > \ldots$. In particular, every finite totally ordered set is well-ordered.

(iii) Every subset of a totally (well-)ordered set is totally (well-)ordered.

Example II.3.3. Let M be a finite set with $|M| > 1$. Let $P := \mathcal{P}(M) \setminus \{\varnothing\}$ be ordered by $\subseteq$. Then every singleton subset is a minimal element of P. On the other hand, P has no least element. Obviously, $\varnothing$ is a lower bound of P in $\mathcal{P}(M)$.

Theorem II.3.4 (Transfinite Induction)**.** *Let $(A, \leq)$ be a well-ordered set. Let $P(a)$ be a predicate such that for all $a \in A$:*

$$(\forall b \in A^{<a} : P(b)) \Longrightarrow P(a).$$

Then $P(a)$ holds for all $a \in A$.

Proof. If the set $\{a \in A : \neg P(a)\}$ were non-empty, there would be a least $a \in A$ with $\neg P(a)$. By modus ponens, $\forall b \in A^{<a} : P(b)$ would have to be false, i. e. there would exist a $b < a$ with $\neg P(b)$. Contradiction. □

Remark II.3.5. Note that this formulation of induction does not require a base case. If a is the smallest element of A, then $A^{<a} = \varnothing$ and $P(a)$ follows from the assumption.

Lemma II.3.6 (Zorn)**.** *Let M be an ordered set. If every totally ordered subset of M has an upper bound, then M contains a maximal element.*

Proof. [1] We assume the opposite. Since $\varnothing \subseteq M$ has an upper bound, $M \neq \varnothing$. Let A be a totally ordered subset of M and $x \in M$ an upper bound of A. Then x is not maximal. Therefore, there exists a $y \in M$ with $x < y$. In particular, $a < y$ for all $a \in A$. We call y a *strict* upper bound of A. According to the axiom of choice, there exists a function f that assigns a strict upper bound $f(A)$ to every totally ordered subset $A \subseteq M$. For $a \in A$, $A^{<a}$ is also totally ordered. We call A *admissible*, if A is well-ordered and $f(A^{<a}) = a$ for every $a \in A$. Obviously, $\varnothing$ is admissible. For every admissible subset $A \subseteq M$, $A \cup \{f(A)\}$ is also admissible, because

$$(A \cup \{f(A)\})^{<a} = \begin{cases} A^{<a} & \text{if } a \in A, \\ A & \text{if } a = f(A). \end{cases}$$

[1] A somewhat shorter proof can be found in my Algebra script.

Let $A, B \subseteq M$ be admissible with $A \neq B$, wlog. $B \not\subseteq A$. Since B is well-ordered, there exists a smallest element b in $B \setminus A$. Then $B^{<b} \subseteq A$.

Assumption: $B^{<b} \neq A$.
Since A is well-ordered, there exists a smallest element a of $A \setminus B^{<b}$. Then $A^{<a} \subseteq B^{<b}$. Because $B \not\subseteq A^{<a}$, there exists a smallest element c of $B \setminus A^{<a}$. Therefore, $B^{<c} \subseteq A^{<a} \subseteq B^{<b} \subseteq A$. In the case $b < c$, $b \in B^{<c} \subseteq A$ would hold, contradicting the choice of b. Thus $c \leq b$. In the case $c = b$, $A^{<a} = B^{<c}$. In the case $c < b$, $c \in B^{<b} \subseteq A$. Because $c \notin A^{<a}$, $c \geq a$, i. e. $A^{<a} \subseteq A^{<c} \cap B \subseteq B^{<c} \subseteq A^{<a}$. Therefore, in any case $A^{<a} = B^{<c}$. Since A and B are admissible, it follows that $a = f(A^{<a}) = f(B^{<c}) = c \leq b$. In the case $c = b$, $b = c = a \in A$ would hold, contradicting the choice of b. Thus $a = c < b$ and we have the contradiction $a = c \in B^{<b}$.

Thus $A = B^{<b} \subseteq B$ holds. In particular, the set $\mathcal{M}$ of all admissible subsets of M is totally ordered with respect to $\subseteq$. We show that $Z := \bigcup_{A \in \mathcal{M}} A \subseteq M$ is totally ordered with respect to $\leq$. For this, let $a, b \in Z$. Then there exist $A, B \in \mathcal{M}$ with $a \in A$ and $b \in B$. Since $\mathcal{M}$ is totally ordered with respect to $\subseteq$, wlog. $A \subseteq B$ and $a, b \in B$ holds. Since B is totally ordered, $a \leq b$ or $b \leq a$ holds. Now let $a \in A \in \mathcal{M}$. Because $A \subseteq Z$, $A^{<a} \subseteq Z^{<a}$. To prove the reverse inclusion, let $b \in Z^{<a}$, i. e. in particular $b < a$.

Assumption: $b \notin A$.
Let $b \in B \in \mathcal{M}$. Then $B \not\subseteq A$, i. e. $A = B^{<c}$ for some $c \in B$ according to the first part of the proof. Then one has the contradiction $b \geq c > a$.

Thus $A^{<a} = Z^{<a}$. We now show that Z is well-ordered. For this, let $\varnothing \neq X \subseteq Z$. Then there exists an $A \in \mathcal{M}$ with $X \cap A \neq \varnothing$ and a smallest element x in $X \cap A$. Thus $Z^{<x} = A^{<x}$ contains no elements from X, i. e. x is the smallest element in X. Finally, we show $Z \in \mathcal{M}$. For this, let $a \in A \in \mathcal{M}$. Then $Z^{<a} = A^{<a}$ and $a = f(A^{<a}) = f(Z^{<a})$. Thus Z is admissible. But then $Z \cup \{f(Z)\}$ is also admissible, contradicting $f(Z) \notin Z$. □

Remark II.3.7. Lemma II.3.6 also holds in the dual version for lower bounds and minimal elements by replacing $\leq$ with $\geq$.

Theorem II.3.8 (Well-ordering theorem)**.** *Every set can be well-ordered.*

Proof. Let M be a set and $\mathcal{M}$ the set of all pairs $(N, \leq_N)$, where $N \subseteq M$ is well-ordered by $\leq_N$. Since the empty set is well-ordered, $\mathcal{M} \neq \varnothing$. By

$$(N_1, \leq_1) \leq (N_2, \leq_2) :\Longleftrightarrow N_1 \subseteq N_2,\ \leq_1 \subseteq \leq_2,\ \forall x \in N_1, y \in N_2 \setminus N_1 : x < y$$

$\mathcal{M}$ is ordered. Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be totally ordered and $S := \bigcup_{(N, \leq_N) \in \mathcal{N}} N \subseteq M$. For $x, y \in S$ there exist $(N_1, \leq_1), (N_2, \leq_2) \in \mathcal{N}$ with $x \in N_1$ and $y \in N_2$. Since $\mathcal{N}$ is totally ordered, wlog. $N_1 \subseteq N_2$ holds. We define

$$x \leq_S y :\Longleftrightarrow x \leq_2 y.$$

If also $(N_3, \leq_3) \in \mathcal{N}$ with $x, y \in N_3$, then $(N_2, \leq_2) \leq (N_3, \leq_3)$ or $(N_3, \leq_3) \leq (N_2, \leq_2)$ holds, since $\mathcal{N}$ is totally ordered. Because of $\leq_2 \subseteq \leq_3$ or $\leq_3 \subseteq \leq_2$, it then holds that $x \leq_2 y \Leftrightarrow x \leq_3 y$. Therefore, $\leq_S$ does not depend on the choice of N_2. It is easy to show that $(S, \leq_S)$ is an ordered set. Let $\varnothing \neq T \subseteq S$ and $(N, \leq_N) \in \mathcal{N}$ with $T \cap N \neq \varnothing$. Let x be the smallest element of $T \cap N$ w.r.t. $\leq_N$. Let $y \in T$ be arbitrary. Then there exists $(N_1, \leq_1) \in \mathcal{N}$ with $y \in N_1$. In the case $y \in N$, $x \leq_N y$ and $x \leq_S y$. Otherwise, $(N, \leq) < (N_1, \leq_1)$ and $x <_S y$ by the definition of $\leq$ on $\mathcal{M}$. Therefore, x is the smallest element of T and S is well-ordered. Overall, $(S, \leq_S) \in \mathcal{M}$ is an upper bound of $\mathcal{N}$. By Zorn's Lemma, there exists a maximal element $(A, \leq_A) \in \mathcal{M}$. In the case $A \neq M$, there exists $b \in M \setminus A$. Then $A \cup \{b\}$

is well-ordered by defining $a < b$ for all $a \in A$. This contradicts the maximality of $(A, \leq_A)$. Thus $M = A$ is well-ordered. □

Remark II.3.9. If $(A_i)_{i \in I}$ is a family of non-empty sets, then $\bigcup_{i \in I} A_i$ can be well-ordered. One can then choose the smallest element of A_i for each A_i. In this way, the axiom of choice follows from the well-ordering theorem. Therefore, the axiom of choice, Zorn's Lemma, and the well-ordering theorem are equivalent to each other.

Definition II.3.10. A bijection $f\colon A \to B$ between ordered sets $(A, \leq_A)$ and $(B, \leq_B)$ is called an *isomorphism*, if $a \leq_A a' \iff f(a) \leq_B f(a')$ holds for all $a, a' \in A$. One then calls A and B *isomorphic* and writes $A \cong B$.

Remark II.3.11. Isomorphic ordered sets certainly have the same properties (total, well-ordered, ...). Every ordered set is isomorphic to itself via the identity. Furthermore, compositions and inverse mappings of isomorphisms are again isomorphisms. The isomorphism of ordered sets is therefore an equivalence relation. In the following, we determine a canonical system of representatives for the corresponding equivalence classes.

Lemma II.3.12. *Between well-ordered sets A and B, there exists at most one isomorphism $A \to B$.*

Proof. Let $f, g\colon A \to B$ be isomorphisms and $h := g^{-1} \circ f$. If $\{a \in A : h(a) < a\}$ is non-empty, then there exists a smallest element $a \in A$ with $h(a) < a$. Since h is an isomorphism, $h(h(a)) < h(a) < a$ also holds, in contradiction to the choice of a. Therefore, $h(a) \geq a$ for all $a \in A$. Repeating the argument with $h^{-1} = f^{-1} \circ g$, one obtains $h^{-1}(a) \geq a$, thus $a \geq h(a) \geq a$ for all $a \in A$. This shows $f = g$. □

II.4. Ordinal numbers

Definition II.4.1. A well-ordered set α is called an *ordinal number*, if $\alpha^{<x} = x$ holds for all $x \in \alpha$.

Remark II.4.2. Let α be an ordinal number with order relation $\leq$ and $x, y \in \alpha$. Then

$$x \leq y \iff \alpha^{<x} \subseteq \alpha^{<y} \iff x \subseteq y,$$

i. e. the relations $\leq$ and $\subseteq$ are identical. An ordinal number is thus already uniquely determined by the specification of a set. Furthermore,

$$x < y \iff x \in \alpha^{<y} \iff x \in y.$$

Lemma II.4.3. *For ordinal numbers α and β, the following hold:*

(i) *Every $x \in \alpha$ is an ordinal number.*

(ii) $\beta \in \alpha \iff \beta \subsetneq \alpha$.

(iii) $\alpha \subseteq \beta$ *or* $\beta \subseteq \alpha$.

(iv) $\alpha \cong \beta \Longrightarrow \alpha = \beta$.

Proof.

(i) Because $x = \alpha^{<x} \subseteq \alpha$, x is well-ordered. For $y \in x$, it holds that $x^{<y} = (\alpha^{<x})^{<y} = \alpha^{<y} = y$.

(ii) For $\beta \in \alpha$, it holds that $\beta = \alpha^{<\beta} \subseteq \alpha \setminus \{\beta\} \subsetneq \alpha$. Conversely, let $\beta \subsetneq \alpha$. Let x be the smallest element of $\alpha \setminus \beta$. Then $x = \alpha^{<x} \subseteq \beta$. For $y \in \beta$, conversely, $\beta^{<y} = y = \alpha^{<y}$. In the case $y > x$, it would follow that $x \in \alpha^{<y} \subseteq \beta$. Thus $y \leq x$ and $y < x$ because $x \notin \beta$. This shows $\beta \subseteq \alpha^{<x} = x$. Thus $\beta = x \in \alpha$.

(iii) Wlog. let $\alpha \nsubseteq \beta$. Let x be the smallest element of $\alpha \setminus \beta$. Then $x = \alpha^{<x} \subseteq \beta$. In the case $x \subsetneq \beta$, the contradiction $x \in \beta$ follows from (i) and (ii). Thus $\beta = \alpha^{<x} \subseteq \alpha$.

(iv) Let $f\colon \alpha \to \beta$ be an isomorphism and $A := \{x \in \alpha : f(x) \neq x\}$. Suppose A has a smallest element x. Then we obtain the contradiction

$$f(x) = f(\alpha^{<x}) = \{f(x') : x' < x\} = \{x' : x' < x\} = \alpha^{<x} = x.$$

Thus $M = \varnothing$. □

Lemma II.4.4. *Let A be a well-ordered set such that $A^{<x}$ is isomorphic to an ordinal for all $x \in A$. Then A itself is isomorphic to an ordinal.*

Proof. For $x \in A$, let α_x be the ordinal uniquely determined by Lemma II.4.3 with $A^{<x} \cong \alpha_x$. By Lemma II.3.12, there exists exactly one isomorphism $f_x\colon A^{<x} \to \alpha_x$. We show that

$$\begin{aligned} f\colon A &\to \{\alpha_x : x \in A\} =: M, \\ x &\mapsto \alpha_x \end{aligned}$$

is an isomorphism, where M is ordered by $\subseteq$. For $y < x$, it holds that $A^{<y} \subseteq A^{<x}$. Restricting f_x yields an isomorphism

$$A^{<y} \to f_x(A^{<y}) = \alpha_x^{<f_x(y)} = f_x(y) \in \alpha_x.$$

By Lemma II.4.3, $f_x(y)$ is an ordinal and it follows that $f_x(y) = \alpha_y$. This shows $\alpha_y \subsetneq \alpha_x$. Thus f is an isomorphism. Since A is well-ordered, so is M. For $\alpha_x \in M$, it holds that

$$M^{<\alpha_x} = \{\alpha_y : \alpha_y \subsetneq \alpha_x\} = \{f_x(y) : y \in A^{<x}\} = f_x(A^{<x}) = \alpha_x.$$

Thus M is an ordinal. □

Theorem II.4.5. *Every well-ordered set is isomorphic to exactly one ordinal.*

Proof. Uniqueness follows from Lemma II.4.3. By Lemma II.4.4, it suffices to show that all $A^{<x}$ ($x \in A$) are isomorphic to ordinals. Let $x \in A$ be minimal such that $A^{<x}$ is not isomorphic to any ordinal. For all $y \in A^{<x}$, $(A^{<x})^{<y} = A^{<y}$ is isomorphic to an ordinal. By Lemma II.4.4, $A^{<x}$ itself would then be isomorphic to an ordinal. □

Remark II.4.6. Ordinal numbers can therefore be viewed as representatives for the isomorphism classes of well-ordered sets.

Lemma II.4.7. *For every ordinal α, the* successor $\alpha^+ := \alpha \cup \{\alpha\}$ *is also an ordinal.*

Proof. As usual, α^+ is ordered by $\subseteq$. Let $\varnothing \neq A \subseteq \alpha^+$. In the case $A = \{\alpha\}$, α is the smallest element of A. Otherwise, the smallest element of $A \cap \alpha$ is also the smallest element of A. Thus, α^+ is well-ordered. For $x \in \alpha$, we have $(\alpha^+)^{<x} = \alpha^{<x} = x$. For $x = \alpha$, we have $(\alpha^+)^{<x} = \alpha = x$. Thus, α^+ is an ordinal. □

Remark II.4.8. For ordinals α and β, it holds that

$$\alpha < \beta \Longrightarrow \alpha \in \beta, \alpha \subsetneq \beta \Longrightarrow \alpha \cup \{\alpha\} \subseteq \beta \Longrightarrow \alpha^+ \leq \beta \Longrightarrow \alpha^+ < \beta^+.$$

Example II.4.9. The only finite ordinals are the *natural numbers*

$$0 := \varnothing, \qquad 1 := 0^+ = \{\varnothing\}, \qquad 2 := 1^+ = \{\varnothing, \{\varnothing\}\}, \qquad \ldots.$$

These numbers coincide with their (usual) cardinality. The smallest infinite ordinal is the set of natural numbers $\omega := \bigcup_{\alpha \in \omega} \alpha$ (Axiom of Infinity). Somewhat more common is the notation $\mathbb{N} := \{0, 1, \ldots\}$. Transfinite induction on $\mathbb{N}$ is called *mathematical induction*. We set $\mathbb{N}_+ := \mathbb{N} \setminus \{0\}$.

Theorem II.4.10. *Every set of ordinals is well-ordered with respect to* $\subseteq$.

Proof. A set $\mathcal{M}$ of ordinals is totally ordered with respect to $\subseteq$ according to Lemma II.4.3. Suppose $\mathcal{M}$ contains elements $\alpha_1 \supsetneq \alpha_2 \supsetneq \ldots$. From Lemma II.4.3 it follows that $\alpha_2, \alpha_2, \ldots \in \alpha_1$. But then α_1 cannot be well-ordered (with respect to $\subseteq$). □

Remark II.4.11 (Burali-Forti paradox)**.** The collection $\mathcal{M}$ of all ordinals is not a set: otherwise $\mathcal{M}$ would be well-ordered according to Theorem II.4.10. For $\alpha \in \mathcal{M}$ it then holds that

$$\mathcal{M}^{<\alpha} = \{\beta \in \mathcal{M} : \beta \subsetneq \alpha\} \overset{\text{II.4.3}}{=} \{\beta \in \mathcal{M} : \beta \in \alpha\} = \alpha,$$

i. e. $\mathcal{M}$ is itself an ordinal. This leads to the contradiction $\mathcal{M} \in \mathcal{M}$, i. e. $\mathcal{M} \subsetneq \mathcal{M}$.

Example II.4.12. If $(\alpha_i)_{i \in I}$ is an arbitrary family of ordinals, then $\alpha := \bigcup_{i \in I} \alpha_i$ is also an ordinal, because for every $x \in \alpha$ there exists an $i \in I$ with $x \in \alpha_i$ and $\alpha^{<x} = \alpha_i^{<x} = x$.

Definition II.4.13. An ordinal $\alpha > 0$ that has no largest element is called a *limit ordinal*.

Example II.4.14. As the smallest infinite ordinal, ω must be a limit ordinal.

Lemma II.4.15. *For every ordinal* $\alpha > 0$*, the following statements are equivalent:*

(1) α *is a limit ordinal.*

(2) α *has no predecessor, i. e.* $\alpha \neq \beta^+$ *for all ordinals* β*.*

(3) $\alpha = \bigcup_{\beta \in \alpha} \beta$*.*

Proof.

(1)⇒(2): In the case $\alpha = \beta^+$, β would be the largest element of α.

(2)⇒(3): For $\beta \in \alpha$, $\beta \subseteq \alpha$ holds. Let us assume that $\gamma := \bigcup_{\beta \in \alpha} \beta \subsetneq \alpha$ holds. According to Remark II.4.8 and (2), $\gamma^+ \in \alpha$. But then $\gamma^+ \in \gamma$ would hold.

(3)⇒(1): If α has a largest element γ, then $\bigcup_{\beta\in\alpha}\beta \subseteq \gamma < \alpha$ would hold. □

Definition II.4.16. For ordinals α, β, γ, one defines inductively

$$\alpha+\beta := \begin{cases} \alpha & \text{if } \beta = 0, \\ (\alpha+\gamma)^+ & \text{if } \beta = \gamma^+, \\ \bigcup\limits_{\gamma\in\beta} \alpha+\gamma & \text{if } \beta \text{ is a limit ordinal,} \end{cases}$$

$$\alpha\cdot\beta := \begin{cases} 0 & \text{if } \beta = 0, \\ (\alpha\cdot\gamma)+\alpha & \text{if } \beta = \gamma^+, \\ \bigcup\limits_{\gamma\in\beta} \alpha\cdot\gamma & \text{if } \beta \text{ is a limit ordinal,} \end{cases}$$

$$\alpha^\beta := \begin{cases} 1 & \text{if } \beta = 0, \\ \alpha^\gamma\cdot\alpha & \text{if } \beta = \gamma^+, \\ \bigcup\limits_{\gamma\in\beta} \alpha^\gamma & \text{if } \beta \text{ is a limit ordinal.} \end{cases}$$

As usual, we use the order of operations (multiplication before addition).

Example II.4.17. For all ordinals α, $\alpha+1 = (\alpha+0)^+ = \alpha^+$ and $\alpha\cdot 1 = \alpha\cdot 0+\alpha = \alpha$ holds.

Lemma II.4.18. *For ordinal numbers α and β, the following holds:*

(i) $\alpha+\beta \cong \alpha\cup(1\times\beta)$, *where* $\alpha\cup(1\times\beta)$ *is ordered by*

$$(1,b) < (1,b') \iff b < b', \qquad a < (1,b) \qquad (a\in\alpha,\ b,b'\in\beta).$$

[2]

(ii) $\alpha\cdot\beta \cong \alpha\times\beta$, *where* $\alpha\times\beta$ *is equipped with the* anti-lexicographical *order*

$$(a,b) < (a',b') \ :\iff\ b < b' \vee (b = b' \wedge a < a') \qquad (a,a'\in A,\ b,b'\in B).$$

(iii) $\alpha^\beta \cong \{f\colon \beta\to\alpha : |b\in\beta : f(b)\neq 0| < \infty\}$ *with the order*

$$f < g \ :\iff\ \exists b\in\beta\big(f(b) < g(b) \wedge \forall c > b\, f(c) = g(c)\big) \qquad (f,g\colon\beta\to\alpha).$$

Proof. We use transfinite induction on the well-ordered set $\alpha+\beta$ (resp. $\alpha\cdot\beta$, α^β).

(i) For $\beta = 0$ there is nothing to show, because $1\times\beta = \varnothing$. Let $\beta = \gamma^+$ and $\alpha+\gamma \cong \alpha\cup(1\times\gamma)$. Then

$$\alpha+\beta = (\alpha+\gamma)^+ \cong (\alpha\cup(1\times\gamma))^+ \cong \alpha\cup(1\times\gamma^+) \cong \alpha\cup(1\times\beta).$$

Now let β be a limit ordinal. Then

$$\alpha+\beta = \bigcup_{\gamma\in\beta}\alpha+\gamma \cong \bigcup_{\gamma\in\beta}\alpha\cup(1\times\gamma) \cong \alpha\cup\bigcup_{\gamma\in\beta}1\times\gamma \cong \alpha\cup(1\times\beta).$$

[2]The construction $1\times\beta$ guarantees that α and $1\times\beta$ are always disjoint (note: $\alpha\subseteq\beta$ or $\beta\subseteq\alpha$).

(ii) For $\beta = 0$ we have $\alpha \times \beta = \varnothing = 0$. For $\beta = \gamma^+$ and $\alpha \cdot \gamma \cong \alpha \times \gamma$ it holds that

$$\alpha \cdot \beta = \alpha \cdot \gamma + \alpha \overset{\text{(i)}}{\cong} (\alpha \times \gamma) \cup (1 \times \alpha) \cong \alpha \times \beta.$$

For a limit ordinal β we have

$$\alpha \cdot \beta = \bigcup_{\gamma \in \beta} \alpha \cdot \gamma \cong \bigcup_{\gamma \in \beta} \alpha \times \gamma \cong \alpha \times \Big(\bigcup_{\gamma \in \beta} \gamma \Big) \cong \alpha \times \beta.$$

(iii) Let

$$P(\alpha, \beta) := \big\{ f \colon \beta \to \alpha : |\{b \in \beta : f(b) \neq 0\}| < \infty \big\}.$$

By definition, every function $\beta \to \alpha$ is a subset of $\beta \times \alpha$. In the case $\beta = 0$, $\varnothing$ is the only such subset. This shows $P(\alpha, 0) = 1 = \alpha^0$. Let $\beta = \gamma^+$ and $\alpha^\gamma \cong P(\alpha, \gamma)$. For $(f, a) \in P(\alpha, \gamma) \times \alpha$ let $g \colon \beta \to \alpha$ with $g(c) = f(c)$ for $c \in \gamma$ and $g(\{\gamma\}) = a$. Obviously

$$\alpha^\beta = \alpha^\gamma \cdot \alpha \cong P(\alpha, \gamma) \times \alpha \to P(\alpha, \beta), \qquad (f, a) \mapsto g$$

is an isomorphism, i. e. $\alpha^\beta \cong P(\alpha, \beta)$. Analogously

$$\bigcup_{\gamma \in \beta} \alpha^\gamma \cong \bigcup_{\gamma \in \beta} P(\alpha, \gamma) \cong P(\alpha, \beta),$$

by extending $f \in P(\alpha, \gamma)$ to β by setting $f(b) = 0$ for $b \in \beta \setminus \gamma$. □

Remark II.4.19. For natural numbers α and β, it follows that $|\alpha + \beta| = |\alpha| + |\beta|$, $|\alpha \cdot \beta| = |\alpha||\beta|$ and $|\alpha^\beta| = |\alpha|^{|\beta|}$ from Lemma II.4.18. Therefore $\alpha + \beta$, $\alpha \cdot \beta$ and α^β coincide with the usual arithmetic operations on $\mathbb{N}$.

Lemma II.4.20. *For ordinal numbers α, β, γ the following holds:*

(i) Let $\beta < \gamma$. Then $\alpha + \beta < \alpha + \gamma$. If $\alpha > 0$ (resp. $\alpha > 1$), then $\alpha \cdot \beta < \alpha \cdot \gamma$ (resp. $\alpha^\beta < \alpha^\gamma$).

(ii) Let β be a limit ordinal. Then $\alpha + \beta$ is a limit ordinal. If $\alpha > 0$ (resp. $\alpha > 1$), then $\alpha \cdot \beta$ (resp. α^β) is also a limit ordinal.

Proof.

(i) We argue by transfinite induction on $\alpha + \gamma$. The case $\gamma = 0$ is excluded. Let $\gamma = \delta^+$. Because $\beta \in \gamma = \delta \cup \{\delta\}$, we have $\beta \leq \delta$. By induction and Remark II.4.8 it follows that $\alpha + \beta \leq \alpha + \delta$ and $\alpha + \beta < (\alpha + \delta)^+ = \alpha + \gamma$. Now let γ be a limit ordinal. Then $\beta^+ \in \gamma$ and

$$\alpha + \beta < \alpha + \beta^+ \leq \bigcup_{\delta \in \gamma} \alpha + \delta = \alpha + \gamma.$$

For the second assertion let $\alpha > 0$. For $\gamma = \delta^+$ we have $\alpha \cdot \beta \leq \alpha \cdot \delta$ and

$$\alpha \cdot \beta < \alpha \cdot \delta + 1 \leq \alpha \cdot \delta + \alpha = \alpha \cdot \delta^+ = \alpha \cdot \beta.$$

For a limit ordinal γ one obtains

$$\alpha \cdot \beta < \alpha \cdot \beta^+ \leq \bigcup_{\delta \in \gamma} \alpha \cdot \delta = \alpha \cdot \beta.$$

Finally, let $\alpha > 1$. For $\gamma = \delta^+$ we then have

$$\alpha^\beta \leq \alpha^\delta \overset{\text{II.4.17}}{=} \alpha^\delta \cdot 1 < \alpha^\delta \cdot \alpha = \alpha^\gamma.$$

For a limit ordinal γ we have

$$\alpha^\beta < \alpha^{\beta^+} \leq \bigcup_{\delta\in\gamma} \alpha^\delta = \alpha^\gamma.$$

(ii) Since $\beta \cong 1 \times \beta$ has no greatest element, by Lemma II.4.18 $\alpha + \beta \cong \alpha \cup (1 \times \beta)$ also cannot have a greatest element. Therefore $\alpha + \beta$ is a limit ordinal. For $\alpha > 0$, $\alpha \cdot \beta \cong \alpha \times \beta$ also has no greatest element. Finally, let $\alpha > 1$ and $f\colon \beta \to \alpha$ with $|\{b \in \beta : f(b) \neq 0\}| < \infty$. Then there exist $g\colon \beta \to \alpha$ and $b \in \beta$ with $g(b) = 1$, $g(c) = 0$ for $c \neq b$ and $f(c) = 0$ for $c \geq b$. Now $f < g$. Thus α^β has no greatest element. □

Lemma II.4.21. *For ordinal numbers α, β, γ the following holds:*

(i) $0 + \beta = \beta$, $0 \cdot \beta = 0$, $1 \cdot \beta = \beta$, $1^\beta = 1$ *and* $\alpha^1 = \alpha$.

(ii) $(\alpha + \beta) + \gamma \cong \alpha + (\beta + \gamma)$ *and* $(\alpha \cdot \beta) \cdot \gamma \cong \alpha \cdot (\beta \cdot \gamma)$.

(iii) $\alpha \cdot (\beta + \gamma) \cong \alpha \cdot \beta + \alpha \cdot \gamma$.

(iv) $\alpha^{\beta+\gamma} \cong \alpha^\beta \cdot \alpha^\gamma$ *and* $(\alpha^\beta)^\gamma \cong \alpha^{\beta\cdot\gamma}$.

Proof. For the first three statements we use Lemma II.4.18:

(i)

$$\begin{aligned} 0 + \beta &\cong \varnothing \cup (1 \times \beta) \cong \beta, & 0 \cdot \beta &\cong \varnothing \times \beta = 0, & 1 \cdot \beta &\cong 1 \times \beta \cong \beta, \\ 1^\beta &\cong \{f\colon \beta \to \{\varnothing\}\} \cong 1, & \alpha^1 &\cong \{f\colon \{\varnothing\} \to \alpha\} \cong \alpha. \end{aligned}$$

(ii)

$$\begin{aligned} (\alpha + \beta) + \gamma &\cong (\alpha + \beta) \cup (1 \times \gamma) \cong (\alpha \cup (1 \times \beta)) \cup (1 \times \gamma) \cong \alpha \cup (1 \times (\beta \cup (1 \times \gamma))) \\ &\cong \alpha \cup (1 \times (\beta + \gamma)) \cong \alpha + (\beta + \gamma), \\ (\alpha \cdot \beta) \cdot \gamma &\cong (\alpha \times \beta) \times \gamma \cong \alpha \times (\beta \times \gamma) \cong \alpha \cdot (\beta \cdot \gamma). \end{aligned}$$

(iii)

$$\alpha \cdot (\beta + \gamma) \cong \alpha \times (\beta \cup (1 \times \gamma)) \cong (\alpha \times \beta) \cup (1 \times (\alpha \times \gamma)) \cong \alpha \cdot \beta + \alpha \cdot \gamma.$$

(iv) For $\gamma = 0$ we have $\alpha^{\beta+\gamma} = \alpha = \alpha^\beta \cdot 1 = \alpha^\beta \cdot \alpha^\gamma$ and $(\alpha^\beta)^\gamma = 1 = \alpha^{\beta\cdot\gamma}$. For $\gamma = \delta^+$ or $\gamma = \bigcup_{\delta\in\gamma} \delta$ it holds respectively that

$$\begin{aligned} \alpha^{\beta+\gamma} &= \alpha^{(\beta+\delta)^+} = \alpha^{\beta+\delta} \cdot \alpha = (\alpha^\beta \cdot \alpha^\delta) \cdot \alpha \overset{\text{(ii)}}{=} \alpha^\beta \cdot (\alpha^\delta \cdot \alpha) = \alpha^\beta \cdot \alpha^\gamma, \\ \alpha^{\beta+\gamma} &= \alpha^{\bigcup_{\delta\in\gamma} \beta+\delta} = \bigcup_{\delta\in\gamma} \alpha^{\beta+\delta} = \bigcup_{\delta\in\gamma} \alpha^\beta \cdot \alpha^\delta = \alpha^\beta \cdot \bigcup_{\delta\in\gamma} \alpha^\delta = \alpha^\beta \cdot \alpha^\gamma. \end{aligned}$$

For the second assertion it now follows analogously that

$$\begin{aligned} (\alpha^\beta)^\gamma &= (\alpha^\beta)^\delta \cdot \alpha^\beta = \alpha^{\beta\cdot\delta} \cdot \alpha^\beta = \alpha^{\beta\cdot\delta+\beta} = \alpha^{\beta\cdot\gamma}, \\ (\alpha^\beta)^\gamma &= \bigcup_{\delta\in\gamma} (\alpha^\beta)^\delta = \bigcup_{\delta\in\gamma} \alpha^{\beta\cdot\delta} = \alpha^{\bigcup_{\delta\in\gamma} \beta\cdot\delta} = \alpha^{\beta\cdot\gamma}. \end{aligned}$$

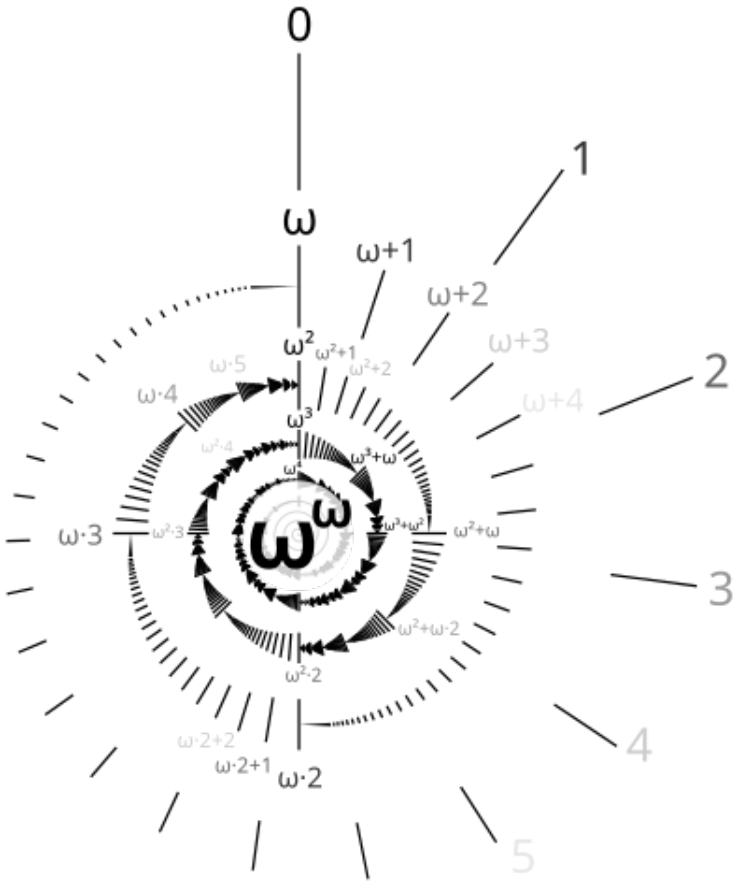
□

Remark II.4.22. Attention: The addition and multiplication of ordinal numbers is not commutative:

$$1+\omega=\bigcup_{n\in\omega}1+n=\omega\neq\omega+1 \qquad\qquad 2\cdot\omega=\bigcup_{n\in\omega}2\cdot n=\omega\neq\omega+\omega=\omega\cdot 2.$$

As a result, the "right-sided" distributive law and one power law also fail:

$$\begin{aligned}(1+1)\cdot\omega&=\omega\neq\omega+\omega,\\ (\omega\cdot 2)^2&=(\omega\cdot 2)\cdot(\omega\cdot 2)=\omega\cdot(2\cdot\omega)\cdot 2=\omega^2\cdot 2<\omega^2\cdot 2^2.\end{aligned}$$



Lemma II.4.23. *For ordinal numbers $\alpha>1$ and β, we have $\beta\leq\alpha^\beta$.*

Proof. For $\beta=0$, we even have $\beta<1=\alpha^\beta$. For $\beta=\gamma^+$, inductively

$$\gamma\leq\alpha^\gamma=\alpha^\gamma\cdot 1<\alpha^\gamma\cdot\alpha=\alpha^\beta$$

and therefore $\beta\leq\alpha^\beta$. For a limit ordinal β, we have

$$\beta=\bigcup_{\gamma\in\beta}\gamma\subseteq\bigcup_{\gamma\in\beta}\alpha^\gamma=\alpha^\beta.$$ □

Example II.4.24. In Lemma II.4.23, equality can occur: $2^\omega=\bigcup_{n\in\omega}2^n=\omega$.

Lemma II.4.25 (Euclidean division)**.** *For all ordinal numbers α and $\beta > 0$, there exist uniquely determined ordinal numbers γ, δ with $\alpha = \beta \cdot \gamma + \delta$ and $\delta < \beta$.*

Proof. According to Lemma II.4.20 and Exercise II.6, $\beta \cdot \alpha^+ > \beta \cdot \alpha \geq 1 \cdot \alpha = \alpha$. Therefore, there exists a smallest ordinal number $\gamma \leq \alpha$ with $\beta \cdot \gamma^+ > \alpha$. Let us assume that $\beta \cdot \gamma > \alpha$ holds. Then γ must be a limit ordinal. Because of $\beta \cdot \gamma = \bigcup_{\delta \in \gamma} \beta \cdot \delta$, there exists a $\delta \in \gamma$ with $\alpha < \beta \cdot \delta < \beta \cdot \delta^+$. But then $\gamma \leq \delta$ by the choice of γ. This contradiction shows $\beta \cdot \gamma \leq \alpha$. If equality holds, one can set $\delta = 0 < \beta$. So let $\beta \cdot \gamma < \alpha$. Let δ ($\leq \alpha$) be the smallest ordinal number with $\beta \cdot \gamma + \delta^+ > \alpha$. As before, one shows $\beta \cdot \gamma + \delta \leq \alpha$. If $\beta \cdot \gamma + \delta < \alpha$ were true, then $\beta \cdot \gamma + \delta^+ \leq \alpha$ would also hold by Remark II.4.8. Thus $\beta \cdot \gamma + \delta = \alpha$. In the case $\delta \geq \beta$, we would have

$$\alpha = \beta \cdot \gamma + \delta \geq \beta \cdot \gamma + \beta = \beta \cdot \gamma^+$$

in contradiction to the choice of γ. This shows the existence of γ and δ.

Let also $\alpha = \beta \cdot \tilde{\gamma} + \tilde{\delta}$ with $\tilde{\delta} < \beta$. Then $\alpha < \beta \cdot \tilde{\gamma} + \beta = \beta \cdot \tilde{\gamma}^+$ and $\gamma \leq \tilde{\gamma}$. For reasons of symmetry, it follows that $\gamma = \tilde{\gamma}$. Because of $\alpha < \beta \cdot \gamma + \tilde{\delta}^+$, we also have $\delta \leq \tilde{\delta}$. Again, it follows that $\delta = \tilde{\delta}$. □

Theorem II.4.26 (Cantor normal form)**.** *Let $\beta > 1$ be an ordinal number. For every ordinal number α, there exist uniquely determined ordinal numbers $a_0, \ldots, a_n \in \beta$ and $\gamma_0 > \ldots > \gamma_n$ with $\gamma_0 \leq \alpha$ and*

$$\alpha = \beta^{\gamma_0} \cdot a_0 + \beta^{\gamma_1} \cdot a_1 + \ldots + \beta^{\gamma_n} \cdot a_n.$$

Proof. Transfinite induction on α: In the case $\alpha = 0$, the claim holds with $n = 0 = a_0 = \gamma_0$. Let $\alpha > 0$. According to Lemma II.4.20 and Lemma II.4.23, $\beta^{\gamma_0^+} > \beta^\alpha \geq \alpha$. Therefore, there exists a smallest ordinal $\gamma_0 \leq \alpha$ with $\beta^{\gamma_0^+} > \alpha$. Let us assume $\beta^{\gamma_0} > \alpha$. Then γ_0 is a limit ordinal and there exists a $\delta \in \gamma_0$ with $\alpha < \beta^\delta < \beta^{\delta^+}$. This yields the contradiction $\gamma_0 \leq \delta$. Thus $\beta^{\gamma_0} \leq \alpha$. Euclidean division yields unique ordinals a_0 and $\delta < \beta^{\gamma_0}$ with $\alpha = \beta^{\gamma_0} \cdot a_0 + \delta$. In the case $a_0 \geq \beta$, it would be

$$\alpha \geq \beta^{\gamma_0} \cdot a_0 \geq \beta^{\gamma_0} \cdot \beta = \beta^{\gamma_0^+} > \alpha$$

according to Lemma II.4.20. Thus $a_0 \in \beta$. Because of $\delta < \beta^{\gamma_0} \leq \alpha$, there exist inductively $a_1, \ldots, a_n \in \beta$ and $\gamma_1 > \ldots > \gamma_n$

$$\delta = \beta^{\gamma_1} \cdot a_1 + \ldots + \beta^{\gamma_n} \cdot a_n.$$

In the case $\gamma_1 \geq \gamma_0$, it would be $\delta \geq \beta^{\gamma_1} \geq \beta^{\gamma_0} > \delta$ according to Lemma II.4.20. This proves the existence of the normal form.

Assume that also

$$\alpha = \beta^{\tilde{\gamma}_0} \cdot \tilde{a}_0 + \ldots + \beta^{\tilde{\gamma}_m} \cdot \tilde{a}_m.$$

From $\tilde{a}_m < \beta$ it follows that

$$\begin{aligned} \alpha &< \beta^{\tilde{\gamma}_0} \cdot \tilde{a}_0 + \ldots + \beta^{\tilde{\gamma}_m} \cdot \beta = \beta^{\tilde{\gamma}_0} \cdot \tilde{a}_0 + \ldots + \beta^{\tilde{\gamma}_m^+} \leq \beta^{\tilde{\gamma}_0} \cdot \tilde{a}_0 + \ldots + \beta^{\tilde{\gamma}_{m-1}} \tilde{a}_{m-1} + \beta^{\tilde{\gamma}_{m-1}} \\ &= \beta^{\tilde{\gamma}_0} \cdot \tilde{a}_0 + \ldots + \beta^{\tilde{\gamma}_{m-1}} \cdot \tilde{a}_{m-1}^+ \leq \beta^{\tilde{\gamma}_0} \cdot \tilde{a}_0 + \ldots + \beta^{\tilde{\gamma}_{m-1}^+} \leq \ldots \leq \beta^{\tilde{\gamma}_0^+}. \end{aligned}$$

The choice of γ_0 yields $\gamma_0 \leq \tilde{\gamma}_0$. For reasons of symmetry, $\gamma_0 = \tilde{\gamma}_0$ holds. The uniqueness of the remaining coefficients now follows inductively from the Euclidean division. □

Remark II.4.27.

(i) In the Cantor normal form, one may change neither the order of the summands $\beta^{\alpha_i} \cdot a_i$ nor the position of the coefficients a_i. According to Remark II.4.22, for example, ω is the normal form of $1 + \omega = \omega^0 + \omega^1$ and of $2 \cdot \omega$.

(ii) In the case $b := \beta \in \mathbb{N}$ and $\alpha \in \mathbb{N}$, one obtains the *b-adic expansion*

$$\alpha = a_0 + a_1 b + a_2 b^2 + \ldots + a_n b^n$$

of α with $0 \leq b_i < b$ for $i = 0, \ldots, n$ (according to Remark II.4.19, one may change the sorting here). For $b = 2$ (resp. $b = 10$), one speaks of the *binary representation* (resp. *decimal representation*) of α.

Theorem II.4.28 (Goodstein)**.** *For the Goodstein sequence* $(g_i(n))_{i \geq 1}$ *from Example I.7.9,* $\lim_{i \to \infty} g_i(n) = 0$ *holds for all* $n \in \mathbb{N}$*.*

Proof. For $n \in \mathbb{N}$ we define $h_1(n) := n$. For $b > 1$, write n in the "iterated" b-adic expansion (as with $g_{b-1}(n)$), where the summands and coefficients are arranged as in the Cantor normal form. One obtains $h_b(n)$ by replacing all b with ω in this representation. For example,

$$h_3(68) = h_3(3^3 \cdot 2 + 3^2 + 3 + 2) = \omega^\omega \cdot 2 + \omega^2 + \omega + 2.$$

According to Lemma II.4.20, $h_b(n) < h_b(n+1)$ holds for all $b \geq 1$. In the case $n < b$, $h_b(n) = n$. In all other cases, $h_b(n) \geq \omega > n$. In any case, $h_b(n) \geq n$. As is well known, one obtains $g_b(n)$ from $g_{b-1}(n)$ by first replacing all b with $b+1$ in the iterated b-adic expansion and then subtracting 1. Since it makes no difference whether one replaces b directly with ω or first with $b+1$ and then with ω, it holds that

$$h_b(g_{b-1}(n)) = h_{b+1}(g_b(n) + 1) > h_{b+1}(g_b(n)) > h_{b+2}(g_{b+1}(n)) > \ldots.$$

Since $h_b(g_{b-1}(n))$ is well-ordered as an ordinal number, there must exist an $i \in \mathbb{N}$ with $h_{i+1}(g_i(n)) = 0$. Then $g_i(n) = 0$ as well. □

II.5. Cardinal Numbers

Definition II.5.1. Every set M can be well-ordered according to the Well-Ordering Theorem. According to Theorem II.4.5, M with this well-ordering is isomorphic to an ordinal number. Let $\mathcal{M}$ be the set of all ordinal numbers that are isomorphic to M with respect to some ordering. According to Theorem II.4.10, $\mathcal{M}$ possesses a smallest element, which is called the *cardinal number* $|M|$ of M. We use Fraktur letters such as $\mathfrak{a}$ for cardinal numbers to distinguish them from ordinal numbers.

Remark II.5.2.

(i) As ordinal numbers, cardinal numbers $\mathfrak{a}$ and $\mathfrak{b}$ can always be compared, i.e., $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$ holds. We then write $\mathfrak{a} \leq \mathfrak{b}$ or $\mathfrak{b} \leq \mathfrak{a}$. For arbitrary sets A and B, the inequality $|A| \leq |B|$ is equivalent to the existence of an injective mapping $A \to B$. The Cantor-Bernstein Theorem is therefore nothing more than the antisymmetry of $\leq$.

(ii) For every cardinal number $\mathfrak{a}$, $|\mathfrak{a}| = \mathfrak{a}$ holds.

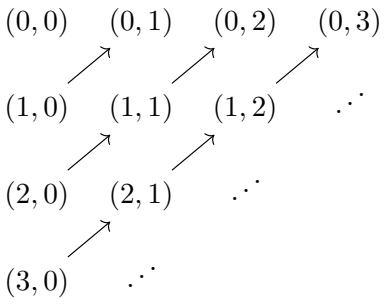
(iii) All natural numbers and ω itself are cardinal numbers. In the following, we use the notation $\mathbb{N}$ to consider ω as a cardinal number. Thus, $|\omega| = \mathbb{N}$ holds.

(iv) A set M is called *countable* (or *uncountable*), if $|M| = \mathbb{N}$ (or $|M| > \mathbb{N}$). In the first case, the elements of M can be indexed with $\mathbb{N}$, i.e., $M = \{a_0, a_1, \ldots\}$.

Example II.5.3.

(i) The map $f\colon \omega^+ \to \omega$ with $f(\omega) := 0$ and $f(n) := n^+$ for $n \in \omega$ is a bijection. This shows $|\omega^+| = \mathbb{N}$. In particular, ω^+ is an ordinal number, but not a cardinal number.

(ii) The set $\omega \times \omega$ can be enumerated "diagonally" by numbering pairs with a constant sum:



The underlying bijection

$$\omega^2 \to \omega, \qquad (n, m) \mapsto m + \sum_{k=0}^{n+m} k = m + \frac{(n+m)(n+m+1)}{2}$$

is called the *Cantor pairing function*. Another bijection can be found in Exercise II.5. In particular, $|\omega \times \omega| = \mathbb{N}$.

(iii) Let $A_1, A_2, \ldots$ be a family of at most countable sets, i. e. there exist injective maps $f_i\colon A_i \to \mathbb{N}$. Let $A := \bigcup_{i\in\mathbb{N}} A_i$. For $a \in A$ there exists a minimal i with $a \in A_i$. Now $g\colon A \to \mathbb{N} \times \mathbb{N}$, $a \mapsto (i, f_i(a))$ is injective. According to (i), A is at most countable.

(iv) If α and β are countable ordinal numbers, then $\alpha + \beta$, $\alpha \cdot \beta$ and α^β are also countable, because each of these sets can be written inductively as a countable union of countable sets.

Theorem II.5.4. *Two sets are equinumerous if and only if they have the same cardinal number.*

Proof. Let A and B be sets. If $|A| = |B|$ holds, then A and B are equinumerous. Conversely, if A and B are equinumerous, then $|A|$ and $|B|$ are also equinumerous. Let $f\colon |A| \to |B|$ be a bijection. For $x, y \in |A|$ it then holds that

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

Therefore f is an isomorphism. From Lemma II.4.3 it follows that $|A| = |B|$. □

Remark II.5.5. We have seen in Remark II.4.22 that the arithmetic of ordinal numbers has some flaws. For cardinal numbers, we define arithmetic operations that satisfy almost all the usual laws. For addition and multiplication, one can adopt the interpretation from Lemma II.4.18 while disregarding the order relation.

Definition II.5.6. For cardinal numbers $\mathfrak{a}$ and $\mathfrak{b}$ we define

$$\mathfrak{a} + \mathfrak{b} := |\mathfrak{a} \cup (1 \times \mathfrak{b})|, \qquad \mathfrak{a} \cdot \mathfrak{b} := |\mathfrak{a} \times \mathfrak{b}|,$$
$$\mathfrak{a}^{\mathfrak{b}} := |\{f\colon \mathfrak{b} \to \mathfrak{a}\}|, \qquad \mathfrak{a}! := |\operatorname{Sym}(\mathfrak{a})|.$$

One calls $\mathfrak{a}!$ the *factorial* of $\mathfrak{a}$. As with ordinal numbers, we use the order of operations: multiplication and exponentiation before addition.

Remark II.5.7. For an arbitrary family of cardinal numbers $(\mathfrak{a}_i)_{i\in I}$ one defines more generally

$$\sum_{i\in I}\mathfrak{a}_i := \Big|\bigcup_{i\in I}\{i\}\times\mathfrak{a}_i\Big|, \qquad\qquad \prod_{i\in I}\mathfrak{a}_i := \Big|\bigtimes_{i\in I}\mathfrak{a}_i\Big|.$$

If all $\mathfrak{a}_i \neq 0$, then the axiom of choice shows $\prod_{i\in I}\mathfrak{a}_i \neq 0$. For cardinal numbers $\mathfrak{a}$ and $\mathfrak{b}$ it holds that $\sum_{a\in\mathfrak{a}}\mathfrak{b} = \mathfrak{a}\cdot\mathfrak{b}$ and $\prod_{a\in\mathfrak{a}}\mathfrak{b} = \mathfrak{b}^{\mathfrak{a}}$ (Example II.2.6).

Theorem II.5.8. *For sets A and B it holds that*

(i) $|A\cup B| + |A\cap B| = |A| + |B|$,

(ii) $|A\times B| = |A|\cdot|B|$,

(iii) $|A^B| = |A|^{|B|}$,

(iv) $|\mathcal{P}(A)| = 2^{|A|}$,

(v) $|\operatorname{Sym}(A)| = |A|!$.

Proof. For the construction of suitable bijections (Theorem II.5.4) one can assume that A and B are cardinal numbers. Then (ii), (iii) and (v) are settled. For (i) one uses the bijection $f\colon (A\cup B)\cup(1\times(A\cap B)) \to A\cup(1\times B)$ with

$$f(x) := \begin{cases} x & \text{if } x\in A\setminus B,\\ (0,x) & \text{if } x\in B,\end{cases}$$
$$f(0,x) := x \qquad (x\in A\cap B).$$

For (iv) one uses the bijection $f\colon \mathcal{P}(A)\to 2^A$, $B\mapsto f_B$ with

$$f_B(x) := \begin{cases} 1 & \text{if } x\in B,\\ 0 & \text{if } x\notin B.\end{cases}$$

□

Theorem II.5.9. *For cardinal numbers $\mathfrak{a},\mathfrak{b},\mathfrak{c}$ the following calculation rules hold:*

$$\begin{array}{ccc}
\mathfrak{a}+0=\mathfrak{a}, & \mathfrak{a}+\mathfrak{b}=\mathfrak{b}+\mathfrak{a}, & (\mathfrak{a}+\mathfrak{b})+\mathfrak{c}=\mathfrak{a}+(\mathfrak{b}+\mathfrak{c}),\\
\mathfrak{a}\cdot 1=\mathfrak{a}, & \mathfrak{a}\cdot\mathfrak{b}=\mathfrak{b}\cdot\mathfrak{a}, & (\mathfrak{a}\cdot\mathfrak{b})\cdot\mathfrak{c}=\mathfrak{a}\cdot(\mathfrak{b}\cdot\mathfrak{c}),\\
\mathfrak{a}^0=1, & \mathfrak{a}^1=\mathfrak{a}, & 1^{\mathfrak{a}}=1,\\
\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}}=\mathfrak{a}^{\mathfrak{b}}\cdot\mathfrak{a}^{\mathfrak{c}}, & (\mathfrak{a}\cdot\mathfrak{b})^{\mathfrak{c}}=\mathfrak{a}^{\mathfrak{c}}\cdot\mathfrak{b}^{\mathfrak{c}}, & (\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}}=\mathfrak{a}^{\mathfrak{b}\cdot\mathfrak{c}},\\
\mathfrak{a}\cdot(\mathfrak{b}+\mathfrak{c})=\mathfrak{a}\cdot\mathfrak{b}+\mathfrak{a}\cdot\mathfrak{c}, & 0!=1, & (\mathfrak{a}+1)!=\mathfrak{a}!\cdot(\mathfrak{a}+1).
\end{array}$$

Proof. Most assertions are obvious or follow from Lemma II.4.18 and Lemma II.4.21. We only show the following:

- $\mathfrak{a}^0 = |\{f\colon \varnothing\to\mathfrak{a}\}| = \{\varnothing\} = 1$.
- The map $\mathfrak{a}^{\mathfrak{b}}\cdot\mathfrak{a}^{\mathfrak{c}}\to\mathfrak{a}^{\mathfrak{b}+c}$, $(f,g)\mapsto h$ with

  $$h(x) := \begin{cases} f(x) & \text{if } x\in\mathfrak{b},\\ g(x) & \text{if } x\in\mathfrak{c}\end{cases}$$

  is a bijection.

- The map $\mathfrak{a}^{\mathfrak{c}} \cdot \mathfrak{b}^{\mathfrak{c}} \to (\mathfrak{a} \cdot \mathfrak{b})^{\mathfrak{c}}$, $(f, g) \mapsto h$ with

  $$h(x) := (f(x), g(x))$$

  for $x \in \mathfrak{c}$ is a bijection.
- The map $(\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} \to \mathfrak{a}^{\mathfrak{b} \cdot \mathfrak{c}}$, $f \mapsto g$ with

  $$g(x, y) := (f(y))(x)$$

  is a bijection.
- $0! = |\operatorname{Sym}(\varnothing)| = |\{\varnothing \to \varnothing\}| = 0^0 = 1$.
- Let $A := \mathfrak{a} \cup \{x\}$ with $|A| = \mathfrak{a} + 1$. Then the map $A \times \operatorname{Sym}(\mathfrak{a}) \to \operatorname{Sym}(A)$, $(a, f) \mapsto g$ with

  $$g(y) := \begin{cases} a & \text{if } y = x, \\ f(y) & \text{if } y \neq x \end{cases}$$

  for $y \in A$ is a bijection. □

Remark II.5.10. For $\mathfrak{a} > 0$, it holds that $0^{\mathfrak{a}} = |\{f \colon \mathfrak{a} \to \varnothing\}| = |\varnothing| = 0$. Compare the following theorem with Example II.4.24.

Theorem II.5.11. *For cardinal numbers $\mathfrak{a} \leq \mathfrak{b}$ and $\mathfrak{c} \leq \mathfrak{d}$, it holds that:*

(i) $\mathfrak{a} < 2^{\mathfrak{a}}$,

(ii) $\mathfrak{a} + \mathfrak{c} \leq \mathfrak{b} + \mathfrak{d}$,

(iii) $\mathfrak{a} \cdot \mathfrak{c} \leq \mathfrak{b} \cdot \mathfrak{d}$,

(iv) $\mathfrak{a}^{\mathfrak{c}} \leq \mathfrak{b}^{\mathfrak{d}}$ *if* $\mathfrak{a} + \mathfrak{c} > 0$.

Proof.

(i) The injective map $\mathfrak{a} \to \mathcal{P}(\mathfrak{a})$, $x \mapsto \{x\}$ shows $\mathfrak{a} \leq |\mathcal{P}(\mathfrak{a})| = 2^{\mathfrak{a}}$. Now assume that a bijection $f \colon \mathfrak{a} \to \mathcal{P}(\mathfrak{a})$ exists. Let $A := \{x \in \mathfrak{a} : x \notin f(x)\} \in \mathcal{P}(\mathfrak{a})$. Then there exists an $x \in \mathfrak{a}$ with $f(x) = A$. The contradiction $x \in A = f(x) \Leftrightarrow x \notin f(x)$ follows.

(ii) It holds that $\mathfrak{a} \cup (1 \times \mathfrak{c}) \subseteq \mathfrak{b} \times (1 \times \mathfrak{d})$.

(iii) It holds that $\mathfrak{a} \times \mathfrak{c} \subseteq \mathfrak{b} \times \mathfrak{d}$.

(iv) In the case $\mathfrak{a} = 0$, we have $\mathfrak{c} > 0$ and $\mathfrak{a}^{\mathfrak{c}} = 0 \leq \mathfrak{b}^{\mathfrak{d}}$ according to Remark II.5.10. So let $\mathfrak{a} > 0$ and $x \in \mathfrak{a}$. Then every map $f \colon \mathfrak{c} \to \mathfrak{a}$ can be extended to $\hat{f} \colon \mathfrak{d} \to \mathfrak{b}$ by setting $\hat{f}(y) = x$ for $y \in \mathfrak{d} \setminus \mathfrak{c}$. This yields an injective map $\mathfrak{a}^{\mathfrak{c}} \to \mathfrak{b}^{\mathfrak{d}}$, $f \mapsto \hat{f}$. □

Remark II.5.12.

(i) (Cantor's first antinomy) The totality $\mathcal{M}$ of all cardinal numbers is not a set: Otherwise, $\mathcal{M}' := \bigcup_{\mathfrak{a} \in \mathcal{M}} \mathfrak{a}$ would also be a set and $2^{|\mathcal{M}'|} \subseteq \mathcal{M}'$ in contradiction to $|\mathcal{M}'| < 2^{|\mathcal{M}'|}$.

(ii) (Cantor's second antinomy) The totality $\mathcal{M}$ of all sets is not a set (same argument).

(iii) Every cardinal number $\mathfrak{a}$ has exactly one successor, namely the smallest element from $\{|A| : A \subseteq 2^{\mathfrak{a}},\ |A| > \mathfrak{a}\}$. We avoid the notation $\mathfrak{a}^+$ to exclude confusion with the successor ordinal number (note $|\omega^+| = \mathbb{N}$).

(iv) Traditionally, infinite cardinal numbers are denoted by the Hebrew letter $\aleph$ (*Aleph*), i. e. $\mathbb{N} =: \aleph_0 < \aleph_1 < \ldots < \aleph_{\mathbb{N}} < \ldots$. The second Hebrew letter $\beth$ (*Beth*) is used for the series $\beth_0 := \mathbb{N}$, $\beth_1 := 2^{\mathbb{N}}, \ldots$.

(v) The *continuum hypothesis* states that no cardinal number lies strictly between $\mathbb{N}$ and $2^{\mathbb{N}}$, i. e. $\aleph_1 = \beth_1$. This can be neither proven nor refuted in $\mathcal{ZF}$. The *generalized continuum hypothesis* states more generally $\aleph_\alpha = \beth_\alpha$ for all ordinal numbers α.

(vi) In $\mathcal{ZF}$, one can neither prove nor refute that there are so-called *inaccessible* cardinal numbers $\mathfrak{a}$ with the following properties:

- $\mathfrak{a} > \mathbb{N}$.
- $\mathfrak{a}$ has no predecessor as in (iii).
- For an index set I with $|I| < \mathfrak{a}$ and cardinal numbers $\mathfrak{a}_i < \mathfrak{a}$, it holds that $\sum_{i\in I} \mathfrak{a}_i < \mathfrak{a}$.

Theorem II.5.13 (Cantor). *Let $\mathfrak{a}$ and $\mathfrak{b}$ be cardinal numbers with $\mathfrak{a} \leq \mathfrak{b} \geq \mathbb{N}$. Then*

(i) $\mathfrak{a} + \mathfrak{b} = \mathfrak{b}$,

(ii) $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b}$ *if* $\mathfrak{a} > 0$,

(iii) $\mathfrak{a}^{\mathfrak{b}} = 2^{\mathfrak{b}}$ *if* $\mathfrak{a} > 1$,

(iv) $\mathfrak{b}! = 2^{\mathfrak{b}}$

Proof.

(i) If $\mathfrak{a}$ is finite, then $f\colon \mathfrak{a} \cup (1 \times \mathfrak{b}) \to \mathfrak{b}$ with

$$f(x) := \begin{cases} x & \text{if } x \in \mathfrak{a}, \\ y + \mathfrak{a} & \text{if } x = (0, y) \in 1 \times \mathbb{N}, \\ y & \text{if } x = (0, y) \in 1 \times (\mathfrak{b} \setminus \mathbb{N}) \end{cases}$$

provides the desired bijection (note: $\mathfrak{a} \subseteq \mathbb{N} \subseteq \mathfrak{b}$). Now let $\mathfrak{a}$ be infinite. Because of $\mathfrak{b} \leq \mathfrak{a} + \mathfrak{b} \leq \mathfrak{b} + \mathfrak{b}$ (Theorem II.5.11), we can assume $\mathfrak{a} = \mathfrak{b}$. It suffices to construct a bijection $2 \times \mathfrak{b} \to \mathfrak{b}$. In the case $\mathfrak{b} = \mathbb{N}$, consider $(0, n) \to 2 \cdot n$ and $(1, n) \to 2 \cdot n + 1$ for $n \in \mathbb{N}$. Now let $\mathfrak{b}$ be uncountable and $\mathcal{M}$ be the set of all pairs (B, α), where $B \subseteq \mathfrak{b}$ and $\alpha\colon 2 \times B \to B$ is a bijection. Because of $\mathbb{N} \subseteq \mathfrak{b}$, $\mathcal{M}$ is non-empty and ordered by

$$(B, \alpha) \leq (B', \alpha') \ :\Longleftrightarrow\ B \subseteq B',\ \alpha'_{|2\times B} = \alpha.$$

Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be totally ordered. Then $C := \bigcup_{(B,\alpha)\in\mathcal{N}} B \subseteq \mathfrak{b}$. We define $\beta\colon 2 \times C \to C$ by $\beta(x) = \alpha(x)$ if $x \in 2 \times B$ and $(B, \alpha) \in \mathcal{N}$. Obviously, β is well-defined and bijective. Therefore, $(C, \beta) \in \mathcal{M}$ is an upper bound of $\mathcal{N}$. By Zorn's Lemma, $\mathcal{M}$ has a maximal element (B, α). If $\mathfrak{b} \setminus B$ contains a countable subset C, then there exists a bijection $2 \times C \to C$ as above and we can extend α to $2 \times (B \cup C)$. This contradicts the maximality of (B, α). Thus $\mathfrak{b} \setminus B$ is finite. As above, then $\mathfrak{b} = |B| + |\mathfrak{b} \setminus B| = B$ and we are finished.

(ii) Because of $\mathfrak{b} = 1 \times \mathfrak{b} \leq \mathfrak{a} \times \mathfrak{b} \leq \mathfrak{b} \times \mathfrak{b}$, we can assume $\mathfrak{a} = \mathfrak{b}$. It suffices to construct a bijection $\mathfrak{b} \times \mathfrak{b} \to \mathfrak{b}$. The case $\mathfrak{b} = \mathbb{N}$ was handled in Example II.5.3. Now let $\mathfrak{b}$ be uncountable and $\mathcal{M}$ be the set of all pairs (B, α), where $B \subseteq \mathfrak{b}$ and $\alpha\colon B \times B \to B$ is a bijection. Because of $\mathbb{N} \subseteq \mathfrak{b}$, $\mathcal{M}$ is non-empty and ordered by

$$(B, \alpha) \leq (B', \alpha') \ :\Longleftrightarrow\ B \subseteq B',\ \alpha'_{|B\times B} = \alpha.$$

Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be totally ordered. Then $C := \bigcup_{(B,\alpha)\in\mathcal{N}} B \subseteq \mathfrak{b}$. We define $\beta\colon C \times C \to C$ by $\beta(x) = \alpha(x)$ if $x \in B \times B$ and $(B, \alpha) \in \mathcal{N}$. Obviously, β is well-defined and bijective. Therefore, $(C, \beta) \in \mathcal{M}$ is an upper bound of $\mathcal{N}$. By Zorn's Lemma, $\mathcal{M}$ has a maximal element (B, α). In the case $B < \mathfrak{b}$, then $\mathfrak{b} = |B| + |\mathfrak{b} \setminus B| = |\mathfrak{b} \setminus B|$ by (i). In particular, there exists $C \subseteq \mathfrak{b} \setminus B$ with $|C| = |B|$. Because of $|C \times C| = |B \cdot B| = |B| = |C| = |B \times C| = |C \times B|$ and $|B \cup C| = |B| + |C| = |C| + |C| \overset{\text{(i)}}{=} |C|$, there exists a bijection

$$(B \times C) \cup (C \times B) \cup (C \times C) \to C.$$

Thus α can be extended to

$$(B \cup C) \times (B \cup C) = (B \times B) \cup (B \times C) \cup (C \times B) \cup (C \times C).$$

This contradicts the maximality of (B, α). Therefore $\mathfrak{b} = B$ and we are finished.

(iii) By (ii), it holds that $2^{\mathfrak{b}} \leq \mathfrak{a}^{\mathfrak{b}} \leq \mathfrak{b}^{\mathfrak{b}} \leq (2^{\mathfrak{b}})^{\mathfrak{b}} = 2^{\mathfrak{b}\cdot\mathfrak{b}} = 2^{\mathfrak{b}}$.

(iv) Because of $\mathfrak{b}! = |\operatorname{Sym}(\mathfrak{b})| \leq |\mathcal{P}(\mathfrak{b} \times \mathfrak{b})| = |\mathcal{P}(\mathfrak{b})| = 2^{\mathfrak{b}}$, it suffices to construct an injective map $f\colon \mathcal{P}(\mathfrak{b}) \to \operatorname{Sym}(2 \times \mathfrak{b})$, $B \mapsto f_B$. This is done by

$$f_B(i, x) := \begin{cases} (1, x) & \text{if } i = 0, x \in B, \\ (0, x) & \text{if } i = 1, x \in B, \\ (i, x) & \text{if } x \notin B. \end{cases}$$

□

Theorem II.5.14 (König)**.** *Let $(\mathfrak{a}_i)_{i\in I}$ and $(\mathfrak{b}_i)_{i\in I}$ be families of cardinal numbers with $\mathfrak{a}_i < \mathfrak{b}_i$ for all $i \in I$. Then*

$$\sum_{i\in I} \mathfrak{a}_i < \prod_{i\in I} \mathfrak{b}_i.$$

Proof. By the axiom of choice, there exist $y_i \in \mathfrak{b}_i \setminus \mathfrak{a}_i$ for all $i \in I$. Then the map $\bigcup_{i\in I}\{i\} \times \mathfrak{a}_i \to \bigtimes_{i\in I} \mathfrak{b}_i$, $(j, x) \mapsto f$ with

$$f(i) := \begin{cases} x & \text{if } i = j, \\ y_i & \text{if } i \neq j \end{cases}$$

is injective. This shows $\sum_{i\in I} \mathfrak{a}_i \leq \prod_{i\in I} \mathfrak{b}_i$. Suppose there exists a bijection

$$\alpha\colon \bigcup_{i\in I}\{i\} \times \mathfrak{a}_i \to \bigtimes_{i\in I} \mathfrak{b}_i,$$
$$(i, x) \mapsto \alpha_x.$$

For $i \in I$, we have $|\{\alpha_x(i) : x \in \mathfrak{a}_i\}| \leq \mathfrak{a}_i < \mathfrak{b}_i$. Therefore, there exist $f(i) \in \mathfrak{b}_i \setminus \{\alpha_x(i) : x \in \mathfrak{a}_i\}$ for all $i \in I$. But then $f \in \bigtimes_{i\in I} \mathfrak{b}_i$ would not be in the image of α. □

Theorem II.5.15. *For every infinite set A, it holds that*

$$|\{B \subseteq A : |B| < \infty\}| = |A|,$$
$$\big|\big\{\sigma \in \mathrm{Sym}(A) : |\{a \in A : \sigma(a) \neq a\}| < \infty\big\}\big| = |A|.$$

Proof. It holds that

$$|A| = |\{\{a\} : a \in A\}| \leq |\{B \subseteq A : |B| < \infty\}| \leq \Big|\bigcup_{n\in\mathbb{N}} A^n\Big| \leq \sum_{n\in\mathbb{N}} |A|^n = \sum_{n\in\mathbb{N}} |A| = |\mathbb{N}| \cdot |A| = |A|.$$

From this it follows that

$$\begin{aligned}\big|\big\{\sigma \in \mathrm{Sym}(A) : |\{a \in A : \sigma(a) \neq a\}| < \infty\big\}\big| &\leq \sum_{\substack{B,C\subseteq A,\\ |B|=|C|<\infty}} |\{B \to C\}| \leq \Big(\sum_{\substack{B\subseteq A,\\ |B|<\infty}} |B|^2\Big)^2 \\ &\leq (|A| \cdot |\mathbb{N}|^2)^2 = |A|. \qquad \square\end{aligned}$$

II.6. Construction of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Remark II.6.1. So far, we can only add, multiply, and exponentiate natural numbers. To define corresponding inverse operations, we must replace $\mathbb{N}$ with larger sets. In the following, we will often omit the multiplication symbol $\cdot$ for the sake of clarity.

Definition II.6.2.

(i) Obviously,

$$(a,b) \sim (c,d) \ :\Longleftrightarrow\ a + d = b + c$$

defines an equivalence relation on $\mathbb{N} \times \mathbb{N}$. The equivalence classes $[a,b]$ form the set $\mathbb{Z}$ of *integers*. For $[a,b],[c,d] \in \mathbb{Z}$ we define

$$\begin{aligned}[a,b] + [c,d] &:= [a + c, b + d],\\ [a,b] - [c,d] &:= [a + d, b + c],\\ [a,b] \cdot [c,d] &:= [ac + bd, ad + bc],\\ [a,b] \leq [c,d] &:\Leftrightarrow a + d \leq b + c,\end{aligned}$$

One calls $z \in \mathbb{Z}$ *even* (resp. *odd*), if there exists (no) $w \in \mathbb{Z}$ with $z = w + w$.

(ii) Obviously,

$$(a,b) \sim (c,d) \ :\Longleftrightarrow\ ad = bc$$

defines an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. The equivalence classes $[a,b]$ form the set $\mathbb{Q}$ of *rational numbers*. For $[a,b],[c,d] \in \mathbb{Q}$ we define

$$\begin{aligned}[a,b] + [c,d] &:= [ad + bc, bd],\\ [a,b] - [c,d] &:= [ad - bc, bd],\\ [a,b] \cdot [c,d] &:= [ac, bd],\\ [a,b] : [c,d] &:= [ad, bc] \text{ if } c \neq 0,\\ [a,b] \leq [c,d] &:\Leftrightarrow ad \leq bc.\end{aligned}$$

Remark II.6.3.

(i) Through $n \mapsto [n, 0]$ one can consider $\mathbb{N}$ as a subset of $\mathbb{Z}$. Every further element from $\mathbb{Z}$ has the form $-n := [0, n]$ for an $n \in \mathbb{N}$. Then $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ and $m - n = m + (-n)$ for $m, n \in \mathbb{Z}$ holds. In particular, $m - m = 0$.

(ii) Through $z \mapsto [z, 1]$ one can embed $\mathbb{Z}$ into $\mathbb{Q}$. More generally, one writes $[a, b] \in \mathbb{Q}$ in the form a/b or $\frac{a}{b}$. Then $a : b = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ holds. For $q \in \mathbb{Q} \setminus \{0\}$ we also have $q : q = 1$.

(iii) One easily shows that the given arithmetic operations are well-defined and extend the corresponding operations on $\mathbb{N}$. For $a \in \mathbb{Q}$ and $z \in \mathbb{Z}$ one additionally sets

$$a^z := \begin{cases} \prod_{x \in z} a & \text{if } z \geq 0, \\ \prod_{x \in -z} \frac{1}{a} & \text{if } z < 0. \end{cases}$$

The rules formulated in Theorem II.5.9 then also hold in $\mathbb{Q}$ (provided they are defined). The order relation on $\mathbb{Q}$ is total and also compatible with the order on $\mathbb{N}$.

Theorem II.6.4 (CANTOR's first diagonalization[3])**.** *The sets $\mathbb{Z}$ and $\mathbb{Q}$ are countable.*

Proof. By construction, $\mathbb{Z}$ is a set of equivalence classes on $\mathbb{N}\times\mathbb{N}$. By choosing a system of representatives, one can consider $\mathbb{Z}$ as a subset of $\mathbb{N}\times\mathbb{N}$. According to Example II.5.3, $\mathbb{N} \leq |\mathbb{Z}| \leq |\mathbb{N}\times\mathbb{N}| = \mathbb{N}$. Analogously, one can consider $\mathbb{Q}$ as a subset of $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ and it follows that $\mathbb{N} \leq |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = \mathbb{N}$. □

Remark II.6.5.

(i) The mapping

$$\mathbb{N} \to \mathbb{Z}, \qquad n \mapsto \begin{cases} \frac{n}{2} & \text{if } n \text{ is even,} \\ -\frac{n+1}{2} & \text{is } n \text{ is odd} \end{cases}$$

is an explicit bijection. Nevertheless, $(\mathbb{N}, \leq)$ and $(\mathbb{Z}, \leq)$ are not isomorphic, because $\mathbb{N}$ possesses a smallest element, but $\mathbb{Z}$ does not.

(ii) The CALKIN-WILF *sequence* $\mathbb{Q} = \{q_0, q_1, -q_1, q_2, -q_2, \ldots\}$ with $q_0 := 0$ and

$$q_{n+1} := \frac{1}{2\lfloor q_n \rfloor + 1 - q_n}$$

for $n \in \mathbb{N}$ yields an explicit bijection $\mathbb{Z} \to \mathbb{Q}$ (without proof). Here, $\lfloor q \rfloor$ is the largest integer z with $z \leq q$. Nevertheless, $(\mathbb{Q}, \leq)$ is isomorphic neither to $(\mathbb{N}, \leq)$ nor to $(\mathbb{Z}, \leq)$, because if $f \colon \mathbb{Q} \to \mathbb{Z}$ were an isomorphism, then

$$|\{q \in \mathbb{Q} : 0 \leq q \leq 1\}| = |\{z \in \mathbb{Z} : f(0) \leq z \leq f(1)\}| < \infty.$$

Definition II.6.6. A *Dedekind cut* is a subset $D \subseteq \mathbb{Q}$ with the properties:

- $\varnothing \neq D \neq \mathbb{Q}$,
- D possesses no largest element,
- $\forall d \in D : \mathbb{Q}^{<d} \subseteq D$.

[3]The name results from Example II.5.3.

The Dedekind cuts form the set $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$ of *real numbers*. Through $q \mapsto \mathbb{Q}^{<q}$, the rational numbers can be embedded into $\mathbb{R}$. In particular, $0 \in \mathbb{R}$. For Dedekind cuts D and E we define

$$
\begin{aligned}
D \leq E &:\Leftrightarrow D \subseteq E,\\
D + E &:= \{d + e : d \in D,\ e \in E\},\\
-D &:= \{x \in \mathbb{Q} : \forall d \in D : x < -d\},\\
D - E &:= D + (-E),\\
D \cdot E &:= \begin{cases}
\{x \in \mathbb{Q} : \exists d \in D, e \in E : d > 0, e > 0, x < de\} & \text{if } D, E > 0,\\
-((-D) \cdot E) & \text{if } D < 0, E > 0,\\
-(D \cdot (-E)) & \text{if } D > 0, E < 0,\\
(-D) \cdot (-E) & \text{if } D, E < 0,\\
0 & \text{if } D = 0 \vee E = 0,
\end{cases}\\
\frac{1}{D} &:= \begin{cases}
\{x \in \mathbb{Q} : \exists d \in D : d > 0, x < \frac{1}{d}\} & \text{if } D > 0,\\
-\frac{1}{-D} & \text{if } D < 0,
\end{cases}\\
D : E &:= D \cdot \frac{1}{E} \qquad \text{if } E \neq 0.
\end{aligned}
$$

One calls $r \in \mathbb{R}$ *positive* (resp. *negative*), if $r > 0$ (resp. $r < 0$).

Remark II.6.7. The operations on $\mathbb{R}$ extend the operations on $\mathbb{Q}$ and the calculation rules formulated in Theorem II.5.9 hold (as far as defined). The order on $\mathbb{R}$ is total and extends the order on $\mathbb{Q}$. Furthermore,

$$
\begin{aligned}
a \leq b &\implies a + c \leq b + c,\\
a, b \geq 0 &\implies ab \geq 0
\end{aligned}
\tag{II.6.1}
$$

for all $a, b, c \in \mathbb{R}$. Thus $\mathbb{R}$ becomes an *ordered field*.

Lemma II.6.8. *If $\varnothing \neq M \subseteq \mathbb{R}$ possesses an upper bound, then*

$$\sup M := \bigcup_{r \in M} r \in \mathbb{R}$$

is the least upper bound of M. One calls $\sup M$ *the* supremum *of M.*

Proof. If $s \in \mathbb{R}$ is an upper bound of M, then s is also an upper bound of $D := \bigcup_{r \in M} r \subseteq \mathbb{Q}$, i. e. $D \subseteq s$. In particular, $D \neq \mathbb{Q}$. If there existed a largest element x in D, then x would also be a largest element of some $r \in M$. This contradicts the properties of Dedekind cuts. Thus D has no largest element. For all $d \in D$, we have $\mathbb{Q}^{<d} \subseteq D$. Therefore $D \in \mathbb{R}$ is the least upper bound of M. □

Lemma II.6.9. *Every real number is the supremum of rational numbers, i. e. $\mathbb{Q}$ lies* dense *in $\mathbb{R}$.*

Proof. Let $r \in \mathbb{R}$. For $n \in \mathbb{N}$ we choose $q_n \in \mathbb{Q}$ maximal with the properties $n! \cdot q_n \in \mathbb{Z}$ and $q_n \in r$. Then certainly $\sup\{q_n : n \in \mathbb{N}\} \leq r$. Let $x \in r$ be arbitrary. Since r has no largest element, there exists a $y \in r$ with $x < y$. We write $y = \frac{k}{m}$ with $k, m \in \mathbb{Z}$ and $m > 0$. The maximality of q_m shows $y \leq q_m$ and $x \in \mathbb{Q}^{<q_m}$. This shows $r = \sup\{q_n : n \in \mathbb{N}\}$. □

Theorem II.6.10 (CANTOR's second diagonalization)**.** *It holds that* $|\mathbb{R}| = 2^{\mathbb{N}}$*. In particular,* $\mathbb{R}$ *is uncountable.*

Proof. Because of $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = 2^{|\mathbb{Q}|} = 2^{\mathbb{N}}$ it suffices to construct an injective map $2^{\mathbb{N}} \to \mathbb{R}$. For $f \in 2^{\mathbb{N}}$ and $n \in \mathbb{N}$ we consider $f_n := \sum_{k=0}^{n} \frac{f(k)}{3^k} \in \mathbb{Q}$. By induction on n one shows

$$f_n \leq \sum_{k=0}^{n} \frac{1}{3^k} = \frac{3^{n+1}-1}{2 \cdot 3^n} \leq \frac{3}{2}.$$

Therefore $\frac{3}{2}$ is an upper bound of $\{f_n : n \in \mathbb{N}\}$ and by Lemma II.6.8 there exists

$$S_f := \sup\{f_n : n \in \mathbb{N}\} \in \mathbb{R}.$$

Now let $g \in 2^{\mathbb{N}}$ with $S_g = S_f$. In the case $f \neq g$ there exists a smallest $n \in \mathbb{N}$ with $f(n) \neq g(n)$. Wlog. let $f(n) = 0$ and $g(n) = 1$. For all $m \geq n$ it then holds that

$$f_m + \frac{1}{2 \cdot 3^n} \leq f_m + \frac{3^{m-n}+1}{2 \cdot 3^m} = f_m + \frac{1}{3^n} - \sum_{k=n+1}^{m} \frac{1}{3^k} \leq \sum_{k=0}^{n} \frac{g(k)}{3^k} \leq g_m \leq S_g = S_f.$$

Because of $f_0 \leq f_1 \leq \ldots \leq f_n$ then $S_f - \frac{1}{2 \cdot 3^n}$ would also be an upper bound of $\{f_k : k \in \mathbb{N}\}$ in contradiction to the minimality of S_f. Thus the map $2^{\mathbb{N}} \to \mathbb{R}$, $f \to S_f$ is injective. □

Remark II.6.11.

(i) In analysis, one writes

$$\sum_{k=0}^{\infty} \frac{f(k)}{3^n} := \lim_{k \to \infty} f_k := S_f$$

in the situation of the above proof. The constructed mapping $f \mapsto S_f$ maps only into the set $\{r \in \mathbb{R} : 0 \leq r \leq \frac{3}{2}\}$. By scaling, every *interval* $\{r \in \mathbb{R} : a \leq r \leq b\}$ with $a < b$ is therefore already uncountable.

(ii) If one has already proven that real numbers can be written by infinite decimal expansions (or if one defines $\mathbb{R}$ in this way), then there is an intuitive argument for $|\mathbb{R}| > |\mathbb{N}|$: Suppose $\mathbb{R} = \{r_1, r_2, \ldots\}$. Construct $x = x_1{,}x_2x_3\ldots$, such that $x_i - 1$ is the i-th decimal digit of r_i (for $x_i = 0$ let $x_i - 1 = 9$). Example:

$$\begin{aligned} r_1 &= \mathbf{1}{,}0000\ldots, \\ r_2 &= 0{,}\mathbf{0}234\ldots, \\ r_3 &= 11{,}4\mathbf{9}02\ldots \\ r_4 &= 3{,}14\mathbf{1}5\ldots \\ &\vdots \\ x &= 2{,}102\ldots \end{aligned}$$

Because of $x \in \mathbb{R}$, there exists an $n \in \mathbb{N}$ with $x = r_n$. On the other hand, x and r_n differ at the n-th decimal digit. Contradiction. [4]

[4] Compare this argument with the proof of Gödel's first incompleteness theorem I.7.6 or the halting problem Theorem I.8.15.

(iii) The numbers in $\mathbb{R} \setminus \mathbb{Q}$ are called *irrational*. Because of $|\mathbb{R}| = |\mathbb{Q}| + |\mathbb{R} \setminus \mathbb{Q}| = |\mathbb{R} \setminus \mathbb{Q}|$, there are "more" irrational numbers than rational ones. We construct an example.

Lemma II.6.12. *For all $n \in \mathbb{N}_+$ and $r \in \mathbb{R}$ with $r > 0$, there exists exactly one $s \in \mathbb{R}$ with $s > 0$ and $s^n = r$.*

Proof. If one has constructed s, then $1/s > 0$ and $(1/s)^n = 1/r$ holds. We can therefore assume $r \geq 1$ by replacing r with $1/r$ if necessary. For $r = 1$, one chooses $s = 1$. So let $r > 1$. For every $t > r$, it then holds that $t^n > r^n$. Therefore, $s := \sup\{q \in \mathbb{Q} : q^n < r\}$ exists. Let us first assume $s^n < r$. For every $k \in \mathbb{N}$, there exist by Lemma II.6.9 $a, b \in \mathbb{Q}$ with $0 < a < b$, $b - a < \frac{1}{k}$ and $b^n < r$. It then holds that

$$b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \ldots + ba^{n-2} + a^{n-1}) < \frac{1}{k} n b^{n-1} \leq \frac{nr}{k}.$$

Therefore, there exist $a, b \in \mathbb{N}$ with $s^n < \frac{a^n}{b^n} < r$. Then $s < \frac{a}{b}$ in contradiction to the choice of s. In the case $r < s^n$, one analogously finds $a, b \in \mathbb{N}$ with $r < \frac{a^n}{b^n} < s^n$. Then $\frac{a}{b} < s$ would also be an upper bound of $\{q \in \mathbb{Q} : q^n < r\}$. Thus $s^n = r$.

Let also $t > 0$ with $t^n = r$. Then

$$(s-t)(s^{n-1} + s^{n-2}t + \ldots + st^{n-1} + t^{n-1}) = s^n - t^n = 0.$$

Because of $s^{n-1} + s^{n-2}t + \ldots + st^{n-2} + t^{n-1} > 0$, it follows that $s = t$. □

Remark II.6.13. In the situation of Lemma II.6.12, one calls $\sqrt[n]{r} := s$ the n-th *root* of r. For $n = 2$, one calls $\sqrt{r} := \sqrt[2]{r}$ the *square root* of r.

Theorem II.6.14. *The square root of 2 is irrational.*

Proof. In the case $w := \sqrt{2} \in \mathbb{Q}$, there exist $a, b \in \mathbb{Z}$ with $w = \frac{a}{b}$. Here we can assume that $b \in \mathbb{N}$ is as small as possible. It follows that $2b^2 = a^2$. In particular, a^2 is even. If a were odd, say $a = 2k + 1$, then

$$a^2 = (2k+1)(2k+1) = 4k^2 + 4k + 1^2 = 2(2k^2 + 2k) + 1$$

would also be odd. Therefore a is even, say $a = 2c$. Then $2b^2 = 4c^2$ and $b^2 = 2c^2$. Thus b is also even, say $b = 2d$. Finally, $w = \frac{a}{b} = \frac{2c}{2d} = \frac{c}{d}$ in contradiction to the choice of b. □

Remark II.6.15. For all $r \in \mathbb{R}$, $r^2 \geq 0$ holds. Therefore, no $r \in \mathbb{R}$ exists with $r^2 = -1$. We thus extend $\mathbb{R}$ in order to be able to take roots of negative numbers as well.

Definition II.6.16. We define the set of *complex numbers* by $\mathbb{C} := \mathbb{R} \times \mathbb{R}$. For $(a, b), (c, d) \in \mathbb{C}$ we define:

$$\begin{aligned}
(a,b) + (c,d) &:= (a+c, b+d),\\
(a,b) - (c,d) &:= (a-c, b-d),\\
(a,b) \cdot (c,d) &:= (ac - bd, ab + bc),\\
(a,b) : (c,d) &:= \Big(\frac{ac+bd}{c^2+d^2}, \frac{bc-ad}{c^2+d^2}\Big) \qquad (\text{if } (c,d) \neq 0).
\end{aligned}$$

Remark II.6.17.

(i) In algebra and analysis, one writes complex numbers $x := (a, b) \in \mathbb{C}$ in the form $x = a + b\mathrm{i}$. Here, a is called the *real part* and b the *imaginary part* of x.

(ii) Through $a \mapsto (a, 0)$, one can embed $\mathbb{R}$ into $\mathbb{C}$. As usual, this is compatible with the arithmetic operations.

(iii) With the help of the *exponential function* $\exp\colon \mathbb{C} \to \mathbb{C}$, $x \mapsto \sum_{n\in\mathbb{N}} \frac{x^n}{n!}$ and the principal branch of the *natural logarithm* $\log\colon \mathbb{C} \setminus \{0\} \to \mathbb{C}$, one can define $a^b := \exp(b \log(a))$ for arbitrary complex numbers a, b with $a \neq 0$.

(iv) In contrast to $\mathbb{R}$, there is no order relation on $\mathbb{C}$ that is compatible with the arithmetic operations: Suppose $\mathrm{i} > 0$ holds. Then $-1 = \mathrm{i}^2 > 0$ and $1 = (-1)^2 > 0$. Now one obtains the contradiction $0 = 1 - 1 > 0 + 0 = 0$. If, on the other hand, $\mathrm{i} < 0$, then $0 = \mathrm{i} - \mathrm{i} < -\mathrm{i}$ and $-1 = (-\mathrm{i})^2 > 0$. This leads to the same contradiction.

(v) (Fundamental Theorem of Algebra) If $n \in \mathbb{N} \setminus \{0\}$ and $a_0, \ldots, a_n \in \mathbb{C}$ are arbitrary, then there always exists one (or more) $x \in \mathbb{C}$ with

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

(see Algebra-Skript). For example, $\mathrm{i}^2 = -1$. This generalizes Lemma II.6.12.

(vi) If $a_0, \ldots, a_n$ in (v) are rational, then x is called *algebraic*. The set $\overline{\mathbb{Q}}$ of algebraic numbers is countable. The elements of the uncountable set $\mathbb{C} \setminus \overline{\mathbb{Q}}$ are called *transcendental* numbers. For example, the Liouville *constant*

$$\xi := \sum_{n\in\mathbb{N}} \frac{1}{10^{n!}} \in \mathbb{R}$$

is transcendental (see Algebra-Skript).

(vii) Besides the complex numbers, there are at least two alternative extensions of the real numbers, which we will encounter in section II.9.

II.7. Finite Sets

Definition II.7.1.

- For a set M and $k \in \mathbb{N}$, let
$$\binom{M}{k} := \{A \subseteq M : |A| = k\}.$$
- For $k, n \in \mathbb{N}$ with $k \leq n$, one calls
$$\binom{n}{k} := \frac{n!}{k!(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{k!} \in \mathbb{Q}$$
the *binomial coefficient* of n over k. The following theorem shows $\binom{n}{k} \in \mathbb{N}$.

Theorem II.7.2. *Let M be a set with $n \in \mathbb{N}$ elements. For all $k \leq n$, it then holds that*

$$\left|\binom{M}{k}\right| = \binom{n}{k}.$$

Proof. There are $|\operatorname{Sym}(A)| = k!$ possibilities to list the elements of a k-element subset $A = \{b_1, \ldots, b_k\} \subseteq M$. For the choice of b_1, there are n possibilities. After that, there remain $|M \setminus \{b_1\}| = n-1$ possibilities for the choice of b_2 etc. The number of k-element subsets is therefore $\frac{n(n-1)\ldots(n-k+1)}{k!}$. □

Remark II.7.3.

(i) For $0 < k \leq n$, it holds that

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} = \frac{n!k + n!(n-k+1)}{k!(n-k+1)!}$$
$$= \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}.$$

Inductively, it follows that

$$1 = \binom{n}{0} < \binom{n}{1} < \ldots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \ldots > \binom{n}{n} = 1,$$

where $\lceil n/2 \rceil$ denotes the smallest $z \in \mathbb{Z}$ with $n/2 \leq z$ (PASCAL's triangle).

(ii) In the situation of Theorem II.7.2, it holds that

$$2^n = 2^{|M|} = |\mathcal{P}(M)| = \sum_{k=0}^{n} \left| \binom{M}{k} \right| = \sum_{k=0}^{n} \binom{n}{k}.$$

This is a special case of the *binomial formula*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad (a, b \in \mathbb{C}),$$

which can be proven by induction and (i).

Theorem II.7.4 (Inclusion-Exclusion Principle)**.** *For finite sets $A_1, \ldots, A_n$, it holds that*

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leq i_1 < \ldots < i_k \leq n} |A_{i_1} \cap \ldots \cap A_{i_k}|.$$

Proof. We count how often an element $a \in A_1 \cup \ldots \cup A_n$ is taken into account on the right side. For this, let wlog. $a \in A_1 \cap \ldots \cap A_l$ and $a \notin A_i$ for $i > l$. Then a is counted if and only if $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, l\}$ holds. In the k-th summand, a is thus counted $(-1)^{k+1}\binom{l}{k}$ times according to Theorem II.7.2. In total, a is counted on the right side exactly

$$\sum_{k=1}^{n} (-1)^{k+1} \binom{l}{k} = 1 - \sum_{k=0}^{l} (-1)^k \binom{l}{k} \overset{\text{II.7.3}}{=} 1 - (1-1)^l = 1$$

time. This shows the assertion. □

Example II.7.5. Let F be a (finite) set of women and M a set of men. Each woman $f \in F$ finds a set of men $M_f \subseteq M$ attractive. In order for every woman f to find an attractive partner in M_f, it must obviously hold that $|\bigcup_{e \in E} M_e| \geq |E|$ for all $E \subseteq F$ (assuming monogamy). The next theorem shows that this condition is even sufficient.

Theorem II.7.6 (HALL's Marriage Theorem)**.** *Let $(M_i)_{i\in I}$ be a family of subsets of a set M with $|I| < \infty$ or $\forall i \in I : |M_i| < \infty$. Pairwise distinct $x_i \in M_i$ for $i \in I$ exist if and only if $|\bigcup_{i\in J} M_i| \geq |J|$ holds for every finite subset $J \subseteq I$.*

Proof. For $J \subseteq I$ we write $M_J := \bigcup_{i\in J} M_i$. Suppose that pairwise distinct $x_i \in M_i$ exist (one calls $(x_i)_{i\in I}$ a *system of representatives*). Obviously, then $|M_J| \geq |\{x_i : i \in J\}| = |J|$ for every finite subset $J \subseteq I$. Conversely, let the condition

$$|M_J| \geq |J| \qquad (J \subseteq I,\ |J| < \infty) \tag{II.7.1}$$

be satisfied. We distinguish two cases:

Case 1: $|I| < \infty$.
Induction on $n := |I|$: The case $n \leq 1$ is obvious. So let $n > 1$ and wlog. $I = \{1, \ldots, n\}$. A subset $J \subseteq I$ is called *critical* , if $1 \leq |M_J| = |J| < n$ holds.

Suppose first that no critical subsets exist. Because $|M_1| = |M_{\{1\}}| \geq 1$, there exists an $x_1 \in M_1$. For $i \in J := \{2, \ldots, n\}$ let $N_i := M_i \backslash \{x_1\}$. For every subset $K \subseteq J$ it then holds that $|N_K| \geq |M_K| - 1 \geq |K|$, because K is not critical. Thus $(N_i)_{i\in J}$ satisfies condition (II.7.1) and by induction there exists a system of representatives $(x_i)_{i\in J}$ of $(N_i)_{i\in J}$. Then $(x_i)_{i\in I}$ is certainly a system of representatives for $(M_i)_{i\in I}$.

Finally, suppose that a critical subset $J \subseteq I$ exists. Then $1 \leq m := |J| = |M_J| < n$ holds. By induction, $(M_i)_{i\in J}$ has a system of representatives $(x_i)_{i\in J}$. For $i \in I \setminus J$ let $N_i := M_i \setminus M_J$. For every subset $K \subseteq I \setminus J$ it then holds that

$$|N_K| = |M_K \setminus M_J| = |M_{K\cup J}| - |M_J| \geq |K \cup J| - m = |K| + |J| - m = |K|,$$

i. e. $(N_i)_{i\in I\setminus J}$ satisfies (II.7.1). By induction there exists a system of representatives $(x_i)_{i\in I\setminus J}$. By construction, $(x_i)_{i\in I}$ is then a system of representatives for $(M_i)_{i\in I}$.

Case 2: $\forall i \in I : |M_i| < \infty$.
Let $\mathcal{M}$ be the set of all families $(N_i)_{i\in I}$ with $N_i \subseteq M_i$ (for all $i \in I$) for which (II.7.1) holds. Because $(M_i)_{i\in I} \in \mathcal{M}$, $\mathcal{M}$ is non-empty and ordered by

$$(N_i)_{i\in I} \leq (N'_i)_{i\in I} \ :\Longleftrightarrow\ \forall i \in I : N_i \subseteq N'_i.$$

Let $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ be a totally ordered subset and $K_j := \bigcap_{(N_i)_{i\in I}\in\mathcal{N}} N_j$ for $j \in I$. Then $(K_i)_{i\in I} \leq (N_i)_{i\in I}$ for all $(N_i)_{i\in I} \in \mathcal{N}$. Let $J \subseteq I$ be a finite subset and $j \in J$. Because $|M_j| < \infty$, there exists a finite subset $\mathcal{N}_1 \subseteq \mathcal{N}$ with

$$K_j = \bigcap_{(N_i)_{i\in I}\in\mathcal{N}_1} N_j$$

for all $j \in J$. Since $\mathcal{N}$ is totally ordered, $\mathcal{N}_1$ has a smallest element $(N_i)_{i\in I}$. Obviously, then $(K_j)_{j\in J} = (N_j)_{j\in J}$. In particular, $|K_J| = |N_J| \geq |J|$. This shows that $(K_i)_{i\in I}$ satisfies condition (II.7.1) and is thus a lower bound of $\mathcal{N}$ in $\mathcal{M}$. By Zorn's Lemma, there exists a minimal element $(N_i)_{i\in I} \in \mathcal{M}$. Since every system of representatives of $(N_i)_{i\in I}$ is also a system of representatives of $(M_i)_{i\in I}$, we can replace $(M_i)_{i\in I}$ by $(N_i)_{i\in I}$ and assume $\mathcal{M} = \{(M_i)_{i\in I}\}$.

Let $x \in M_I$ and $N_i := M_i \setminus \{x\}$ for $i \in I$. Because $(N_i)_{i\in I} \notin \mathcal{M}$, there exists a finite subset $J \subseteq I$ with $|M_J| - 1 \leq |N_J| < |J| \leq |M_J|$. It follows that $|M_J| = |J|$ and $x \in M_J$. We now define

$$N_i := \begin{cases} M_i & \text{if } i \in J, \\ M_i \setminus M_J & \text{if } i \in I \setminus J. \end{cases}$$

Let $K \subseteq I$ be finite. Then

$$\begin{aligned}|N_K| &= |N_{K\cap J} \cup N_{K\setminus J}| = |M_{K\cap J}| + |M_{K\setminus J} \setminus M_J| \\ &= |M_{K\cap J}| + |M_{K\cup J}| - |M_J| \geq |K \cap J| + |K \cup J| - |J| = |K|.\end{aligned}$$

This shows $(N_i)_{i\in I} \in \mathcal{M} = \{(M_i)_{i\in I}\}$ and $M_i \cap M_J = \varnothing$ for $i \in I \setminus J$. It follows that $M_{I\setminus J} \cap M_J = \varnothing$. According to Case 1, there exist pairwise distinct $x_i \in M_i$ for $i \in J$. If one now sets

$$N_i := \begin{cases} \{x_i\} & \text{if } i \in J, \\ M_i & \text{if } i \in I \setminus J, \end{cases}$$

then $(N_i)_{i\in I}$ again satisfies (II.7.1). Thus $M_i = \{x_i\}$ for $i \in J$. Since x was chosen arbitrarily, it even holds that $|M_i| = 1$ for all $i \in I$. Obviously, the M_i are also pairwise disjoint and the assertion follows. □

Remark II.7.7. Theorem II.7.6 does not hold for $I = \mathbb{N}$ if not all M_i are finite: Choose $M_0 := \mathbb{N}$ and $M_i := \{i - 1\}$ for $i \geq 1$.

Example II.7.8. In the context of Example II.7.5, one can further ask whether "happy" marriages are possible. For this, each woman and each man establishes an "attractiveness ranking" of all persons of the other sex. A set of marriages is called *stable*, if there is no pair $(f, m) \in F \times M$ who would have preferred to marry each other than their actual partners. In the case $|M| = |F|$, one can marry all women and men stably (Exercise II.9).

Definition II.7.9. Every totally ordered subset K of a finite ordered set M has the form $K = \{x_1, \ldots, x_n\}$ with $x_1 < x_2 < \ldots < x_n$. K is therefore also called a *chain*. A chain of M is called *maximal* if it is not contained in any larger chain of M. A subset $A \subseteq M$ is called an *antichain* of M if $x \leq y \Rightarrow x = y$ holds for all $x, y \in A$.

Theorem II.7.10 (Sperner)**.** *Let M be an n-element set and $\mathcal{A}$ a largest possible antichain of $(\mathcal{P}(M), \subseteq)$. Then $\mathcal{A} = \binom{M}{k}$ with $k \in \{\lfloor n/2 \rfloor, \lceil n/2 \rceil\}$ holds. In particular, $|\mathcal{A}| = \binom{n}{\lfloor n/2 \rfloor}$.*

Proof (Lubell). Obviously, every maximal chain in $\mathcal{P}(M)$ has the form $M_0 \subset \ldots \subset M_n$ with $|M_k| = k$ for $k = 0, \ldots, n$. There are n possibilities for M_1. If M_1 is fixed, then $n - 1$ possibilities remain for M_2 and so on. Thus, there are exactly $n!$ maximal chains in $\mathcal{P}(M)$. Now let $N \subseteq M$ be fixed with $|N| = k$. Then there are exactly $k!(n - k)!$ maximal chains containing N (for M_1 there are k possibilities, for M_2 there are $k - 1$ possibilities, ..., for $M_k = N$ there is one possibility, for M_{k+1} there are $n - k$ possibilities and so on). For $A \in \mathcal{A}$, let K_A be the set of all maximal chains containing A. If a (maximal) chain contains both A and B, then $A \leq B$ or $B \leq A$ holds. Therefore, the sets K_A with $A \in \mathcal{A}$ are pairwise disjoint. This shows

$$\sum_{A\in\mathcal{A}} |A|!(n - |A|)! = \sum_{A\in\mathcal{A}} |K_A| = \Big| \bigcup_{A\in\mathcal{A}} K_A \Big| \leq n!. \tag{II.7.2}$$

Division by $n!$ yields

$$|\mathcal{A}| \frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \overset{\text{II.7.3}}{\leq} \sum_{A\in\mathcal{A}} \frac{1}{\binom{n}{|A|}} \leq 1.$$

Thus $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$. Conversely, $\binom{M}{\lfloor n/2 \rfloor}$ is certainly an antichain with $\binom{n}{\lfloor n/2 \rfloor}$ elements (Theorem II.7.2). It follows that $|\mathcal{A}| = \binom{n}{\lfloor n/2 \rfloor}$ and $\binom{n}{|A|} = \binom{n}{\lfloor n/2 \rfloor}$ for all $A \in \mathcal{A}$. Therefore, $\mathcal{A}$ consists only of subsets $N \subseteq M$ with $\lfloor n/2 \rfloor \leq |N| \leq \lceil n/2 \rceil$. If n is even, we are finished.

Now let $n = 2m + 1$ be odd. From (II.7.2) it follows that $\sum_{A \in \mathcal{A}} |K_A| = n!$, which means that all maximal chains contain (exactly) one element from $\mathcal{A}$. Now let us assume indirectly that $S, T \subseteq M$ with $|S| = |T| = m + 1$, $S \in \mathcal{A}$ and $T \notin \mathcal{A}$ exist. With suitable numbering, $S = \{x_1, \ldots, x_{m+1}\}$ and $T = \{x_i, \ldots, x_{m+i}\}$ hold. Because $T \notin \mathcal{A}$, there exists a $j \geq 1$ with $S' := \{x_j, \ldots, x_{m+j}\} \in A$ and $T' := \{x_{j+1}, \ldots, x_{m+j+1}\} \notin \mathcal{A}$. It holds that $|S' \cap T'| = m$. Because $S' \cap T' \subseteq S' \in \mathcal{A}$, $S' \cap T' \notin \mathcal{A}$. Certainly, there exists a chain containing $S' \cap T'$ and T'. Because $\mathcal{A} \subseteq \{N \subseteq M : |N| \in \{m, m + 1\}\}$, one of these sets would have to lie in $\mathcal{A}$. However, this contradicts $T' \notin \mathcal{A}$. □

Theorem II.7.11 (Mirsky). *Let M be a finite ordered set and m the largest cardinality of a chain in M. Then M is a union of m antichains, but not the union of fewer antichains.*

Proof. For $x \in M$ let $f(x) \geq 1$ be the largest cardinality of a chain ending at x. Let $x, y \in M$ with $x \neq y$ and $f(x) = f(y)$. In the case $x < y$, one could extend any chain ending at x by y. But then $f(y) > f(x)$. Therefore $x \not\leq y \not\leq x$. Thus the preimages $A_n := f^{-1}(n)$ for $n \in \mathbb{N}$ are antichains. By assumption $f(x) \leq m$ for all $x \in M$. This shows $M = A_1 \cup \ldots \cup A_m$.

Conversely, let $M = A_1 \cup \ldots \cup A_k$ for antichains $A_1, \ldots, A_k$. Let $K \subseteq M$ be a chain with $|K| = m$. Then $|K \cap A_i| \leq 1$ for $i = 1, \ldots, k$. This shows $k \geq |K| = m$. □

Theorem II.7.12 (Dilworth). *Let M be a finite ordered set and m the largest cardinality of an antichain in M. Then M is a union of m chains, but not the union of fewer chains.*

Proof (Galvin). If M is the union of the chains $K_1, \ldots, K_s$, then $|A \cap K_i| \leq 1$ for every antichain A. This shows $s \geq m$. For the reverse inequality, we argue by induction on $|M|$. For $M = \varnothing$ the claim is clear. So let $M \neq \varnothing$ and let $x \in M$ be a maximal element. If $M' := M \setminus \{x\}$ has no antichain with m elements, then M' is a union of $m - 1$ chains by induction. Then M is certainly a union of m chains. Now let $A \subseteq M'$ be an antichain with $|A| = m$. By induction there exist wlog. disjoint chains $K_1, \ldots, K_m$ with $M' = K_1 \cup \ldots \cup K_m$. In this case $|A \cap K_i| = 1$ for $i = 1, \ldots, m$. Let

$$x_i := \max \bigcup_{\substack{A \subseteq M' \text{ antichain} \\ |A| = m}} K_i \cap A$$

for $i = 1, \ldots, m$. Suppose $x_i \leq x_j$ holds. Let $A \subseteq M'$ be an antichain with $x_j \in A$ and $|A| = m$. Let $x_i' \in A \cap K_i$. Then $x_i' \leq x_i \leq x_j$. Because of $x_i', x_j \in A$ it follows that $x_i' = x_i = x_j$ and $i = j$, since $K_i \cap K_j = \varnothing$. Therefore $A := \{x_1, \ldots, x_m\}$ is an m-element antichain of M'. By assumption $A \cup \{x\}$ is not an antichain. Since x is maximal in M, $x_i < x$ holds for some $i \in \{1, \ldots, m\}$. Thus $K_i' := K_i \cup \{x\}$ is a chain and M is the union of the chains $K_1, \ldots, K_{i-1}, K_i', K_{i+1}, \ldots, K_m$. □

Theorem II.7.13 (Ramsey, infinite version). *Let $n, k \in \mathbb{N}_+$ and M be an infinite set with $\binom{M}{k} = \mathcal{M}_1 \dot\cup \ldots \dot\cup \mathcal{M}_n$. Then there exists an infinite subset $A \subseteq M$ with $\binom{A}{k} \subseteq \mathcal{M}_i$ for some $i \in \{1, \ldots, n\}$.*

Proof. Induction on k: The case $k = 1$ is the (infinite) pigeonhole principle. So let $k \geq 2$. We interpret a given partition of $\binom{M}{k}$ as a mapping $f\colon \binom{M}{k} \to \{1, \ldots, n\}$. We inductively define infinite sets $A_0 \supseteq A_1 \supseteq \ldots$ and elements $a_i \in A_i \setminus A_{i+1}$ for $i \geq 0$, such that

$$f_{a_i} := f(B \cup \{a_i\}) = f(C \cup \{a_i\}) \qquad \forall B, C \in \binom{A_{i+1}}{k-1}. \tag{II.7.3}$$

Let $A_0 := M$ and $a_0 \in A_0$ be arbitrary. Suppose $a_i \in A_i$ are already defined. Let $g\colon \binom{A_i \setminus \{a_i\}}{k-1} \to \{1, \ldots, n\}$, $B \mapsto f(B \cup \{a_i\})$. By induction, there exists an infinite set $A_{i+1} \subseteq A_i \setminus \{a_i\}$ with $|g(\binom{A_{i+1}}{k-1})| = 1$. Thus (II.7.3) holds for A_{i+1}. We choose $a_{i+1} \in A_{i+1}$ arbitrarily.

By the pigeonhole principle, there exists an infinite set $A \subseteq \{a_1, a_2, \ldots\}$ with $f_a = f_b$ for all $a, b \in A$. Thus the claim holds for A. □

Theorem II.7.14 (Ramsey, finite version)**.** *For $r, s, t \in \mathbb{N}_+$, there exists an $n \in \mathbb{N}_+$ with the following property: For every n-element set M and every partition $\binom{M}{r} = \mathcal{M}_1 \dot\cup \ldots \dot\cup \mathcal{M}_s$, there exists a t-element subset $A \subseteq M$ with $\binom{A}{r} \subseteq \mathcal{M}_i$ for some $i \in \{1, \ldots, s\}$.*

Proof. Let us assume indirectly that the claim for r, s, t is false. For each $n \in \mathbb{N}_+$, there exists an n-element set, wlog. $M := \{1, \ldots, n\}$ and a mapping $f\colon \binom{M}{r} \to \{1, \ldots, s\}$ without the desired property. We then say: f is *bad* and write $M_n := \binom{M}{r}$. By the pigeonhole principle, there are infinitely many bad mappings (on arbitrary M_n) that coincide on M_1. Let F_1 be such a set of bad mappings and let $f_1 : M_1 \to \{1, \ldots, s\}$ be the common restriction. In F_1, there are infinitely many mappings that coincide on M_2. Let $F_2 \subseteq F_1$ be such a set and $f_2 : M_2 \to \{1, \ldots, s\}$ the common restriction. In this way, we obtain bad mappings $f_1, f_2, \ldots$ with $(f_{n+1})_{|M_n} = f_n$ for $n \in \mathbb{N}_+$. We now define $f\colon \binom{\mathbb{N}_+}{r} \to \{1, \ldots, s\}$ by $f(B) := f_n(B)$ for $B \subseteq \{1, \ldots, n\}$. By Theorem II.7.13, there exists a t-element subset $A \subseteq \mathbb{N}$ with $|f(\binom{A}{r})| \leq 1$ (in the case $t < r$, $\binom{A}{r} = \varnothing$). But now $A \subseteq M_n$ for some n and f_n is after all not bad. Contradiction. □

Remark II.7.15. The case $r = 2$ can be interpreted graph-theoretically: $\binom{M}{2}$ is the set of edges of the complete graph with vertex set M. The edges in $\mathcal{M}_i$ are colored with "color" i. Theorem II.7.14 states that there is always a monochromatic clique with t vertices, provided M is large enough. In the case $s = 2$, one obtains a statement about arbitrary (not necessarily complete) graphs: Every graph with sufficiently many vertices possesses a complete subgraph with t vertices or a trivial subgraph with t vertices. To determine the exact number of required vertices, one introduces an asymmetric variant: The *Ramsey number* $R(k, l)$ is the smallest natural number such that every graph with at least $R(k, l)$ vertices possesses a complete subgraph with k vertices or a trivial subgraph with l vertices. Obviously, $R(k, l) = R(l, k)$ (consider the complementary graph) and $R(1, l) = 1$. Every graph with l vertices is either complete or possesses a trivial subgraph with two vertices. This shows $R(2, l) = l$.

Lemma II.7.16. *For $k, l \geq 2$, it holds that*

$$R(k, l) \leq R(k-1, l) + R(k, l-1) \leq \binom{k+l-2}{k-1}.$$

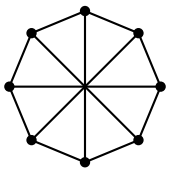
If $R(k-1, l)$ and $R(k, l-1)$ are both even, then $R(k, l) < R(k-1, l) + R(k, l-1)$.

Proof. We first show $R(k,l) \leq R(k-1,l) + R(k,l-1) =: n$. Let G be a graph with n vertices and let $g \in G$ be an arbitrary vertex. Let G_0 (resp. G_1) be the set of all vertices (not) adjacent to g. Then

$$|G_0| + |G_1| = |G_0 \dot\cup G_1| = n - 1 = R(k-1,l) + R(k,l-1) - 1.$$

It follows that $|G_0| \geq R(k-1,l)$ or $|G_1| \geq R(k,l-1)$. Wlog. let $|G_0| \geq R(k-1,l)$. If G_0 possesses a complete subgraph with $k-1$ vertices, then $G_0 \cup \{g\}$ is a complete subgraph of G with k vertices. Otherwise, G_0 (and thus also G) possesses a trivial subgraph with l vertices. This shows the first claim. The second inequality follows inductively from Remark II.7.3. Now assume that $R(k-1,l)$ and $R(k,l-1)$ are even. Let G be a graph with $n-1$ vertices. The above argument only fails if $|G_0| = R(k-1,l) - 1$ and $|G_1| = R(k,l-1) - 1$ holds for every vertex g. In this case, every vertex of G has the same number $R(k-1,l)$ of neighbors. The number of all edges in G is thus $\frac{1}{2}(n-1)(|R(k-1,l)|-1)$. By assumption, however, this is not an integer. Therefore, $R(k,l) \leq n-1$. □

Example II.7.17. From Lemma II.7.16 it follows that $R(3,3) \leq 6$. A 5-gon (as a graph) shows $R(3,3) > 5$ and thus $R(3,3) = 6$. Interpretation: Among six people there are three who all know each other or all do not know each other. Since $R(3,3)$ and $R(2,4) = 4$ are even, $R(3,4) \leq 9$ follows from Lemma II.7.16. The following graph shows conversely $R(3,4) \geq 9$:



Further known values are (without proof):

$$R(3,5) = 14, \qquad R(3,6) = 18, \qquad R(3,7) = 23, \qquad R(3,8) = 28,$$
$$R(3,9) = 36, \qquad R(4,4) = 18, \qquad R(4,5) = 25.$$

Theorem II.7.18 (De Bruijn-Erdős)**.** *Let A be a finite set and $\mathcal{A} \subseteq \mathcal{P}(A)$ with $2 \leq |B| < |A|$ for all $B \in \mathcal{A}$. For every two distinct $x, y \in A$ let there exist exactly one $B \in \mathcal{A}$ with $x, y \in B$. Then $|\mathcal{A}| \geq |A|$ holds.*

Proof (Ivanov). For $a \in A$ let $f(a) := |\{B \in \mathcal{B} : a \in B\}|$. Then

$$\sum_{a \in A} f(a) = |\{(a,B) \in A \times \mathcal{A} : a \in B\}| = \sum_{B \in \mathcal{A}} |B|.$$

For $a \notin B \in \mathcal{A}$ and $b \in B$ there exists exactly one $C_b \in \mathcal{A} \setminus \{B\}$ with $a, b \in C_b$. For $b \neq b'$ we have $C_b \neq C_{b'}$, because otherwise b, b' would be contained in both B and $C_b = C_{b'}$. This shows $|B| \leq f(a)$.

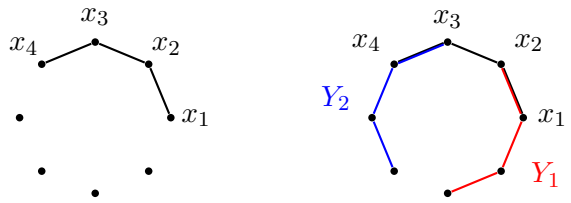
Now assume $|\mathcal{A}| < |A|$. For $B_1, \ldots, B_n \in \mathcal{A}$ we have $|A \setminus B_1| \geq 1$ and $|B_1 \cap B_2| \leq 1$. This shows $|\bigcup_{i=1}^n A \setminus B_i| \geq |A| - 1 \geq |\mathcal{A}| \geq n$ for $n \geq 2$. By Hall's Marriage Theorem there exist pairwise distinct representatives $\alpha(B) \in A \setminus B$ for $B \in \mathcal{A}$. This yields the contradiction

$$\sum_{a \in A} f(a) = \sum_{B \in \mathcal{A}} |B| \leq \sum_{B \in \mathcal{A}} f(\alpha(B)) < \sum_{a \in A} f(a).$$ □

Theorem II.7.19 (Erdős-Ko-Rado). *Let M be a set with $n \geq 2k$ elements. Let $\mathcal{M} \subseteq \binom{M}{k}$ with $A \cap B \neq \varnothing$ for all $A, B \in \mathcal{M}$. Then $|\mathcal{M}| \leq \binom{n-1}{k-1}$ holds. In the case $n > 2k$ and $|\mathcal{M}| = \binom{n-1}{k-1}$ there exists an $x \in M$ with $\mathcal{M} = \{A \in \binom{M}{k} : x \in A\}$.*

Proof (Katona). Wlog. let $M = \{1, \ldots, n\}$.

Case 1: $n \geq 2k$.
There are $(n-1)!$ possibilities to arrange the elements of M in a circle if the position of 1 is fixed. Let Δ be such an arrangement. We count how many connected segments ("circular arcs") of Δ of length k lie in $\mathcal{M}$. Let $X = (x_1, \ldots, x_k)$ be such a segment, numbered in positive direction. Every further segment in $\mathcal{M}$ must intersect X and therefore start or end at some x_i. If a segment Y_1 ends at x_i and segment Y_2 starts at x_{i+1}, then $Y_1 \cap Y_2 = \varnothing$ because of $n \geq 2k$.



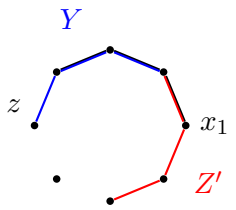
For each $i = 1, \ldots, k-1$, therefore, only one of the two cases can occur. Thus there are at most $k-1$ segments $Y \neq X$ that lie in $\mathcal{M}$. In total, for each Δ, one has at most k segments in $\mathcal{M}$. A given set $A \in \mathcal{M}$ can, however, appear in many arrangements Δ. Specifically, there are $k!$ (resp. $(n-k)!$) possibilities to permute the elements from A (resp. $M \setminus A$). Thus A occurs in $k!(n-k)!$ arrangements Δ. This shows

$$|\mathcal{M}| \leq \frac{k(n-1)!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} = \binom{n-1}{k-1}.$$

Case 2: $n > 2k$ and $|\mathcal{M}| = \binom{n-1}{k-1}$.
We consider, as before, a segment $X = (x_1, \ldots, x_k)$ on a circular arrangement Δ of M. For each i, now either a segment must end with x_i or a segment must start with x_{i+1}. Let i be minimal such that a segment Y_1 ends with i (if necessary $i = n$ with $Y_1 = X$). If a segment Y_2 were to start with x_{i+2}, then $Y_1 \cap Y_2 = \varnothing$ because of $n > 2k$. Therefore, a segment must end with x_{i+1}. This holds for all $j = i, \ldots, k$. We can use the same argument in the reverse direction with $Y_1 = (y_1, \ldots, y_{k-i}, x_1, \ldots, x_i)$ instead of X. By the choice of i, a segment Y_0 must start with x_{i-1}. As before, one obtains segments that start with $x_{i-2}, \ldots, x_1, y_{k-i}, \ldots, y_1$. In total, Δ contains the k segments shifted by one each, starting with y_1.

In particular, all segments contain the element x_i. Wlog. let $i = 1$ from now on. Then the segment $Y = (x_2, x_3, \ldots, x_k, z)$ does not lie in $\mathcal{M}$. Assume indirectly that some $Z \in \mathcal{M}$ does not contain x_1. Because of $n > 2k$, there exists a $Z' \in \binom{M}{k}$ with $x_1 \in Z'$, $z \notin Z'$ and $Z \cap Z' = \varnothing$. In particular, $Z' \notin \mathcal{M}$.

We construct a new arrangement Δ'. First, the elements from $Z' \setminus X$ are listed, then the elements from $X \cap Z'$ starting with x_1, then the elements from $X \setminus Z'$, and finally the element z. All other numbers can be arranged arbitrarily.



As before, Δ' possesses segments from $\mathcal{M}$ shifted by one each. By construction, Z', X and Y are segments of Δ'. Since Y and Z' do not lie in $\mathcal{M}$, however, X cannot be a component of the k shifted segments from $\mathcal{M}$. Contradiction. □

Example II.7.20.

(i) For $|M| = n < 2k$, any two k-element subsets of M intersect. Here,

$$|\mathcal{M}| = \left|\binom{M}{k}\right| = \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} > \binom{n-1}{k-1}$$

is possible.

(ii) Let $n = 2k$, $x \in M$ and $\mathcal{M} = \binom{M\setminus\{x\}}{k}$. For $A, B \in \mathcal{M}$, $A \cap B \neq \varnothing$ holds because of $|A \cup B| \leq 2k-1$. Furthermore, $|\mathcal{M}| = \binom{2k-1}{k} = \binom{n-1}{k-1}$ and $\bigcap_{A\in\mathcal{M}} A = \varnothing$, if $n \geq 4$. The second statement in Theorem II.7.19 thus does not hold for $n = 2k$.

II.8. Topology

Definition II.8.1. Let M be a non-empty set. A family of subsets $\mathcal{F} \subseteq \mathcal{P}(M)$ is called a *filter* of M, if:

- $\varnothing \neq \mathcal{F} \neq \mathcal{P}(M)$.
- $A, B \in \mathcal{F} \Longrightarrow A \cap B \in \mathcal{F}$.
- $A \supseteq B \in \mathcal{F} \Longrightarrow A \in \mathcal{F}$.

If $\mathcal{F}$ is maximal with respect to inclusion, then $\mathcal{F}$ is called an *ultrafilter*.

Remark II.8.2. The first condition in Definition II.8.1 is equivalent to $\varnothing \notin \mathcal{F}$ and $M \in \mathcal{F}$.

Example II.8.3.

(i) For every subset $\varnothing \neq A \subseteq M$,

$$\mathcal{F}(A) := \{B \subseteq M : A \subseteq B\}$$

is a filter. Filters of this type are called *principal filters*. In particular, $\{M\}$ is a filter of M.

(ii) Let $\mathcal{F}$ be a filter of a finite set M. Then there exists a minimal element $A \in \mathcal{F}$. It follows that $\mathcal{F}(A) \subseteq \mathcal{F}$. If there were a $B \in \mathcal{F} \setminus \mathcal{F}(A)$, then $A \cap B \in \mathcal{F}$ would hold, contradicting the choice of A. Therefore, every filter of M is a principal filter. The ultrafilters of M obviously have the form $\mathcal{F}(x) := \mathcal{F}(\{x\})$ for an $x \in M$.

(iii) Now let M be an infinite set and $\mathcal{F}$ the set of all *cofinite* subsets $A \subseteq M$ (i.e., $|M \setminus A| < \infty$). Obviously, $\mathcal{F}$ is a filter, but not a principal filter. $\mathcal{F}$ is called the *Fréchet filter* on M.

(iv) The set Ω of all filters containing a given filter $\mathcal{F}$ is ordered by $\subseteq$. It is easy to see that the union of a totally ordered subset of Ω is again a filter. By Zorn's Lemma, there always exists an ultrafilter containing $\mathcal{F}$.

Lemma II.8.4. *For every filter $\mathcal{F}$ of $M \neq \varnothing$, the following statements are equivalent:*

(1) $\mathcal{F}$ is an ultrafilter.

(2) For all $A \subseteq M$, either $A \in \mathcal{F}$ or $M \setminus A \in \mathcal{F}$ holds.

(3) For all $A_1, \ldots, A_n \subseteq M$ with $A_1 \cup \ldots \cup A_n \in \mathcal{F}$, there exists an i with $A_i \in \mathcal{F}$.

Proof.

(1)⇒(2): Let

$$\mathcal{G} := \big\{B \subseteq M : \exists F \in \mathcal{F} : A \cap F \subseteq B\big\}.$$

If $\varnothing \in \mathcal{G}$, then there exists an $F \in \mathcal{F}$ with $F \subseteq M \setminus A$. Then $M \setminus A \in \mathcal{F}$ also holds. Otherwise, $\mathcal{G}$ is a filter containing $\mathcal{F}$. Since $\mathcal{F}$ is an ultrafilter, $A = A \cap M \in \mathcal{G} = \mathcal{F}$ holds.

(2)⇒(3): Assume $A_i \notin \mathcal{F}$ for $i = 1, \ldots, n$. By (2), $M \setminus A_i \in \mathcal{F}$ holds for $i = 1, \ldots, n$. Since $\mathcal{F}$ is a filter, the contradiction follows:

$$\varnothing = \Big(\bigcup_{i=1}^{n} A_i\Big) \cap \Big(M \setminus \bigcup_{i=1}^{n} A_i\Big) = \Big(\bigcup_{i=1}^{n} A_i\Big) \cap \bigcap_{i=1}^{n} (M \setminus A_i) \in \mathcal{F}.$$

(3)⇒(1): Suppose $\mathcal{F}$ is not an ultrafilter. Then there exists a filter $\mathcal{G} \supsetneq \mathcal{F}$ and an $A \in \mathcal{G} \setminus \mathcal{F}$. Because $A \cup (M \setminus A) \in \mathcal{F}$, it follows from (3) that $M \setminus A \in \mathcal{F} \subseteq \mathcal{G}$. But then $\varnothing = A \cap (M \setminus A) \in \mathcal{G}$ would hold. □

Definition II.8.5. Let M be a non-empty set. A family of subsets $\mathcal{T} \subseteq \mathcal{P}(M)$ is called a *topology* on M if the following hold:

- $\varnothing, M \in \mathcal{T}$.
- $\mathcal{S} \subseteq \mathcal{T} \Longrightarrow \bigcup_{S \in \mathcal{S}} S \in \mathcal{T}$.
- $U, V \in \mathcal{T} \Longrightarrow U \cap V \in \mathcal{T}$.

The sets in $\mathcal{T}$ are called *open*. A set $A \subseteq M$ is called *closed*, if $M \setminus A$ is open. The pair $(M, \mathcal{T})$ is called a *topological space*. If $\mathcal{S} \subseteq \mathcal{T}$ are topologies, then $\mathcal{S}$ (resp. $\mathcal{T}$) is called *coarser* (resp. *finer*) than $\mathcal{T}$ (resp. $\mathcal{S}$).

Remark II.8.6. From De Morgan's laws, it follows that arbitrary intersections and finite unions of closed sets are closed.

Example II.8.7.

(i) One calls $\mathcal{T} = \{\varnothing, M\}$ the *trivial* topology and $\mathcal{T} = \mathcal{P}(M)$ the *discrete* topology on M.

(ii) If $(M, \mathcal{T})$ is a topological space and $\varnothing \neq N \subseteq M$, then $\{N \cap U : U \in \mathcal{T}\}$ defines a topology on N, which is called the *relative topology*. Attention: Open sets in N with respect to the relative topology do not have to be open in M (for example if N itself is not open in M).

(iii) The intersection of any number of topologies on M is again a topology. If $\mathcal{S} \subseteq \mathcal{P}(M)$, then

$$\langle \mathcal{S} \rangle := \bigcap_{\substack{\mathcal{T} \text{ topology} \\ \mathcal{S} \subseteq \mathcal{T}}} \mathcal{T}$$

is the "smallest" topology that contains $\mathcal{S}$. Obviously, $\langle \mathcal{S} \rangle$ consists of arbitrary (including empty) unions of finite intersections of elements from $\mathcal{S}$. If $\mathcal{S}$ is a filter, then obviously $\langle \mathcal{S} \rangle = \mathcal{S} \cup \{\varnothing\}$ holds.

(iv) If $(M_i, \mathcal{T}_i)_{i\in I}$ is a family of disjoint topological spaces, then $M := \bigcup_{i\in I} M_i$ with

$$\mathcal{T} := \Big\{ \bigcup_{i\in I} T_i : T_i \in \mathcal{T}_i \Big\}$$

is also a topological space.

(v) A map $d\colon M \times M \to \mathbb{R}$ is called a *metric*, if for all $x, y, z \in M$ the following holds:

- $d(x, y) \geq 0$ with equality if and only if $x = y$ (positive definite).
- $d(x, y) = d(y, x)$ (symmetric).
- $d(x, z) \leq d(x, y) + d(y, z)$ (triangle inequality).

One calls (M, d) a *metric space*. For $x \in M$ and $\epsilon > 0$ one defines the *ϵ-ball* around x by

$$B_\epsilon(x) := \{y \in M : d(x, y) < \epsilon\}.$$

A subset $U \subseteq M$ is called *open* with respect to d, if for all $x \in U$ there exists an $\epsilon > 0$ with $B_\epsilon(x) \subseteq U$. One easily shows that these open sets form a topology. Topological spaces that arise from a metric are called *metrizable*. The *discrete* metric with $d(x, y) = 1$ for $x \neq y$ leads to the discrete topology (choose $\epsilon = \frac{1}{2}$). Not every topological space is metrizable. Consider for example $M = \{x, y\}$ with the trivial topology. If there were a corresponding metric d, then $\{x\}$ would always be open (choose $\epsilon = \frac{d(x,y)}{2}$).

(vi) Let V be an $\mathbb{R}$-vector space. A map $V \to \mathbb{R}$, $v \mapsto |v|$ is called a *norm* on V, if for all $v, w \in V$ the following holds:

- $|v| \geq 0$ with equality if and only if $v = 0$ (positive definite).
- $|\lambda v| = |\lambda||v|$ for all $\lambda \in \mathbb{R}$ (homogeneous).
- $|v + w| \leq |v| + |w|$ (triangle inequality).

One calls $(V, |.|)$ a *normed space*. One easily shows that $d(v, w) := |v - w|$ defines a metric on V. As is well known, $|v| := \sqrt{v_1^2 + \ldots + v_n^2}$ defines the *Euclidean* norm on $\mathbb{R}^n$. In analysis, one shows that all norms on $\mathbb{R}^n$ lead to the same topology. This is false for infinite-dimensional spaces.

(vii) The set of cofinite subsets together with the empty set forms the *cofinite* topology on every infinite set. It has the special property that the intersection of two non-empty open sets is never empty.

Definition II.8.8. Let $(M, \mathcal{T})$ be a topological space, $A \subseteq M$ and $x \in M$. One calls A a *neighborhood* of x, if an open set U with $x \in U \subseteq A$ exists. One calls x an

- *interior point* of A, if A is a neighborhood of x.
- *boundary point* of A, if neither A nor $M \setminus A$ are neighborhoods of x.

The set of interior points (resp. boundary points) of A is called the *interior* $\mathring{A}$ (resp. the *boundary* ∂A) of A. Finally, one calls $\overline{A} := \mathring{A} \cup \partial A$ the *closure* of A.

Lemma II.8.9. *Let $(M, \mathcal{T})$ be a topological space and $A \subseteq M$. Then:*

(i) $\mathring{A}$ is the union of all open sets in A.

(ii) $\overline{A}$ is the intersection of all closed sets that contain A.

In particular, $\mathring{A} \subseteq A \subseteq \overline{A}$.

Proof.

(i) By definition, every $x \in \mathring{A}$ lies in an open set $U \subseteq A$. Conversely, let $U \subseteq A$ be open. Then A is a neighborhood for all $x \in U$. This shows $U \subseteq \mathring{A}$.

(ii) Obviously, $\mathring{A}$ lies in every closed set that contains A. Let $x \in \partial A$ and B be a closed set that contains A. If $x \in M \setminus B$ were true, then $M \setminus B$ would be a neighborhood of x and x would not be a boundary point. Thus $x \in B$ and $\overline{A}$ lies in the intersection of all closed sets that contain A. Conversely, let $x \in M \setminus \overline{A}$. Then $M \setminus A$ is a neighborhood of x, which means there exists an open set $U \subseteq M \setminus A$ with $x \in U$. Now x is not in the closed set $M \setminus U$, which contains A. This shows the claim. □

Corollary II.8.10. *A subset A of a topological space is open (resp. closed) if and only if $A = \mathring{A}$ (resp. $A = \overline{A}$) holds.*

Example II.8.11. Let $A = (0, 1] \subseteq \mathbb{R}$ be the half-open interval in the Euclidean space $\mathbb{R}$. Then $\mathring{A} = (0, 1)$ is the open interval, $\partial A = \{0, 1\}$ and $\overline{A} = [0, 1]$. Boundary points can therefore lie both inside and outside of A.

Definition II.8.12. A subset K of a topological space M is called *compact*, if for every family of open sets $(U_i)_{i \in I}$ with $K \subseteq \bigcup_{i \in I} U_i$ there exists a finite subset $J \subseteq I$ with $K \subseteq \bigcup_{j \in J} U_j$ (one says: every open cover has a finite subcover). If M itself is compact, one speaks of a *compact* topological space.

Remark II.8.13.

(i) If M has only finitely many open sets, then obviously every subset is compact.

(ii) Every finite subset of a topological space is compact. In the discrete topology, the converse also holds.

(iii) In the cofinite topology on $\mathbb{N}$, every open set is compact.

(iv) If $K \subseteq M$ is compact and $A \subseteq K$ is closed, then A is also compact, because if $A \subseteq \bigcup_{i \in I} U_i$ is an open cover, then $K \subseteq M \setminus A \cup \bigcup_{i \in I} U_i$ is an open cover.

Definition II.8.14. A filter $\mathcal{F}$ of a topological space $(M, \mathcal{T})$ *converges* to $x \in M$, if $\mathcal{F}(x) \cap \mathcal{T} \subseteq \mathcal{F}$ holds.

Lemma II.8.15. *A topological space M is compact if and only if every ultrafilter of M converges to a point.*

Proof. Let M be compact. Suppose an ultrafilter $\mathcal{F}$ of M converges to no point. For all $x \in M$ there then exist $U_x \in \mathcal{T} \setminus \mathcal{F}$ with $x \in U_x$. Since M is compact, there exists a finite set $X \subseteq M$ with $M = \bigcup_{x \in X} U_x$. This contradicts Lemma II.8.4.

Now let us assume that M is not compact. Then there exists an open cover $M = \bigcup_{i \in I} U_i$ without a finite subcover. Consequently,

$$\left\{ A \subseteq M : \exists i_1, \ldots, i_n \in I : M \setminus A \subseteq U_{i_1} \cup \ldots \cup U_{i_n} \right\}$$

is a filter that lies in an ultrafilter $\mathcal{F}$. Suppose $\mathcal{F}$ converges to x. Let $i \in I$ with $x \in U_i$. Then $\varnothing = U_i \cap (M \setminus U_i) \in \mathcal{F}$ would hold. □

Definition II.8.16. Let $(M_i, \mathcal{T}_i)_{i\in I}$ be a family of topological spaces and $M := \bigtimes_{i\in I} M_i$. Let $\pi_i \colon M \to M_i$, $(x_j)_j \mapsto x_i$ be the projection maps for $i \in I$. One calls

$$\langle \pi_i^{-1}(U) : i \in I, U \in \mathcal{T}_i \rangle$$

the *product topology* on M.

Theorem II.8.17 (Tychonoff)**.** *For every family of topological spaces $(M_i)_{i\in I}$, $M := \bigtimes_{i\in I} M_i$ is compact if and only if all M_i are compact.*

Proof. Let M be compact, $i \in I$ and $M_i = \bigcup_{j\in J} U_j$ be an open cover. Then $M = \bigcup_{j\in J} \pi_i^{-1}(U_j)$ is an open cover of M. Since M is compact, there exists a finite subset $J' \subseteq J$ with $M = \bigcup_{j\in J'} \pi_i^{-1}(U_j)$. Therefore $M_i = \bigcup_{j\in J'} U_j$ and M_i is compact.

Now let all M_i be compact. Let $\mathcal{F}$ be a filter of M. For $i \in I$ let

$$\mathcal{F}_i := \{\pi_i(F) : F \in \mathcal{F}\} \subseteq \mathcal{P}(M_i).$$

Because $\varnothing \notin \mathcal{F}$, we have $\varnothing \notin \mathcal{F}_i$. Let $A \supseteq \pi_i(F) \in \mathcal{F}_i$. Then $F \subseteq \pi_i^{-1}(A) \in \mathcal{F}$ and $A = \pi_i(\pi_i^{-1}(A)) \in \mathcal{F}_i$. For $F_1, F_2 \in \mathcal{F}$ we have $\pi_i(F_1) \cap \pi_i(F_2) \supseteq \pi_i(F_1 \cap F_2) \in \mathcal{F}_i$ and $\pi_i(F_1) \cap \pi_i(F_2) \in \mathcal{F}_i$. This shows that $\mathcal{F}_i$ is a filter of M_i. Let also $\mathcal{G} \supseteq \mathcal{F}_i$ be a filter of M_i. For $F \in \mathcal{F}$ and $G \in \mathcal{G}$ it holds that $\pi_i(F) \cap G \in \mathcal{F}_i$ and $F \cap \pi_i^{-1}(G) \neq \varnothing$. Also the intersection of two sets of the form $F \cap \pi_i^{-1}(G)$ is non-empty, because $\pi_i^{-1}(G_1 \cap G_2) \subseteq \pi_i^{-1}(G_1) \cap \pi_i^{-1}(G_2)$ for $G_1, G_2 \in \mathcal{G}$. Therefore

$$\mathcal{F}' := \left\{A \subseteq M : \exists G \in \mathcal{G}, F \in \mathcal{F} : \pi_i^{-1}(G) \cap F \subseteq A\right\}$$

is a filter of M that contains $\mathcal{F}$. Since $\mathcal{F}$ is an ultrafilter, $\mathcal{F}' = \mathcal{F}$ holds. For $G \in \mathcal{G}$ it thus holds that $\pi_i^{-1}(G) = \pi_i^{-1}(G) \cap M \in \mathcal{F}$ and $G = \pi_i(\pi_i^{-1}(G)) \in \mathcal{F}_i$. Thus $\mathcal{F}_i = \mathcal{G}$ is an ultrafilter of M_i. According to Lemma II.8.15, $\mathcal{F}_i$ converges to an $x_i \in M_i$. Let $x := (x_i)_{i\in I} \in M$. Let $U \subseteq M$ be an open set containing x. According to Lemma II.8.15, it suffices to show $U \in \mathcal{F}$. By the definition of the product topology, we can assume that open sets $U_{i_j} \subseteq M_{i_j}$ for $j = 1, \ldots, n$ exist with

$$U = \pi_{i_1}^{-1}(U_{i_1}) \cap \ldots \cap \pi_{i_n}^{-1}(U_{i_n}).$$

Because $x_{i_j} \in U_{i_j}$, it holds that $U_{i_j} \in \mathcal{F}_{i_j}$ for $j = 1, \ldots, n$. Thus there exist $V_j \in \mathcal{F}$ with $\pi_{i_j}(V_j) = U_{i_j}$. From $V_j \subseteq \pi_{i_j}^{-1}(U_{i_j})$ it follows that $\pi_{i_j}^{-1}(U_{i_j}) \in \mathcal{F}$ and finally $U \in \mathcal{F}$. □

Theorem II.8.18 (Kelley)**.** *Tychonoff's Theorem implies the Axiom of Choice.*

Proof. Let $(M_i)_{i\in I}$ be a family of non-empty sets. Let x be a "new" element which is not contained in any of the M_i. Let $\widehat{M_i} := M_i \cup \{x\}$ be equipped with the cofinite topology, where additionally $\{x\}$ shall be open. According to Remark II.8.13 and Tychonoff, $\widehat{M_i}$ and $\widehat{M} := \bigtimes_{i\in I} \widehat{M_i}$ are compact. The i-th projection $\pi_i \colon \widehat{M} \to \widehat{M_i}$ is continuous. Therefore $\pi_i^{-1}(x)$ is open. Suppose $\bigtimes_{i\in I} M_i = \varnothing$. Then $\widehat{M} = \bigcup_{i\in I} \pi_i^{-1}(x)$ is an open cover. Let $J \subseteq I$ be finite with $\widehat{M} = \bigcup_{j\in J} \pi_j^{-1}(x)$. Obviously, however, there exists an element $m = (m_i)_{i\in I} \in \widehat{M}$ with $m_j \in M_j$ for $j \in J$ and $m_i = x$ for $i \in I \setminus J$. Contradiction. □

Definition II.8.19. A topological space M is called

- *connected*, if M is not the union of two disjoint non-empty open subsets.
- *Hausdorff space*, if for distinct $x, y \in M$ there exist two disjoint open sets $U_x, U_y \subseteq M$ with $x \in U_x$ and $y \in U_y$ (*separation axiom*).

Remark II.8.20. Obviously, a topological space M is connected if and only if $\varnothing$ and M are the only subsets that are both open and closed.

Theorem II.8.21. *Every metric space is a Hausdorff space.*

Proof. Let (M, d) be a metric space and $x, y \in M$ distinct points. Let $\epsilon := \frac{d(x,y)}{2}$. Then $B_\epsilon(x)$ and $B_\epsilon(y)$ are disjoint open sets containing x and y respectively. □

Example II.8.22.

(i) We show that the Euclidean space $\mathbb{R}^n$ is connected. Suppose there exist disjoint non-empty open subsets U, V with $\mathbb{R}^n = U \cup V$. Let $x \in U$ and $y \in V$. Let

$$r := \sup\{s \in [0,1] : x + s(y - x) \in U\}$$

and $z := x + r(y - x)$. If z lies in U, then $B_\epsilon(z) \subseteq U$ for some $\epsilon > 0$. But then $z + \frac{\epsilon}{2|y-x|}(y - z) \in U$ would also hold, in contradiction to the definition of r. Analogously, one obtains a contradiction in the case $z \in V$.

(ii) The trivial topology on M does not yield a Hausdorff space if $|M| > 1$. An infinite set with the cofinite topology is also not a Hausdorff space, because the intersection of two non-empty open sets is never empty.

Lemma II.8.23. *Every compact subset of a Hausdorff space is closed.*

Proof. Let K be compact in the Hausdorff space M. Let $x \in M \setminus K$. For all $a \in K$, there exist disjoint open sets $U_a, V_a \subseteq M$ with $a \in U_a$ and $x \in V_a$. Due to compactness, there exist $a_1, \ldots, a_n \in K$ with $K \subseteq \bigcup_{i=1}^n U_{a_i}$. Now $V_{a_1} \cap \ldots \cap V_{a_n}$ is an open set in $M \setminus K$ containing x. Thus $M \setminus K$ is open and K is closed. □

Example II.8.24. The trivial topology on a finite set shows that compact sets do not have to be closed in general.

Theorem II.8.25. *Let M be a compact Hausdorff space and $U, V \subseteq M$ disjoint closed subsets. Then there exist disjoint open subsets $A, B \subseteq M$ with $U \subseteq A$ and $V \subseteq B$.*

Proof. Let $u \in U$. For each $v \in V$, there exist disjoint open sets U_v, V_v with $u \in U_v$ and $v \in V_v$. The open cover

$$M = (M \setminus V) \cup \bigcup_{v \in V} V_v$$

possesses a finite subcover $M = (M \setminus V) \cup \bigcup_{i=1}^{n} V_{v_i}$. The open sets $A_u := U_{v_1} \cap \ldots \cap U_{v_n}$ and $B_u := V_{v_1} \cup \ldots \cup V_{v_n}$ are disjoint and satisfy $u \in A_u$ and $V \subseteq B_u$. The open cover

$$M = (M \setminus U) \cup \bigcup_{u \in U} A_u$$

likewise possesses a finite subcover $M = (M \setminus U) \cup \bigcup_{i=1}^{m} A_{u_i}$. Now $A := A_{u_1} \cup \ldots \cup A_{u_m}$ and $B := B_{u_1} \cap \ldots \cap B_{u_m}$ satisfy the claim. □

Definition II.8.26. Let (M, d) be a metric space. For $A \subseteq M$, one calls

$$d(A) := \sup\{d(x, y) : x, y \in A\} \in \mathbb{R} \cup \{\infty\}$$

the *diameter* of A. If $d(A) < \infty$, then A is called *bounded*.

Lemma II.8.27. *Every closed interval $[a, b] \subseteq \mathbb{R}$ is compact with respect to the Euclidean metric.*

Proof. Let $[a, b] \subseteq \bigcup_{i \in I} U_i$ be an open cover. Let $S \subseteq [a, b]$ be the set of all points s such that $[a, s]$ possesses a finite subcover. Because of $a \in S$, $S \neq \varnothing$. Since $[a, b]$ is bounded, $s := \sup S$ exists. Suppose $s < b$. Let $[a, s] \subseteq \bigcup_{i=1}^{n} U_i$ be a finite subcover and $1 \leq i \leq n$ with $s \in U_i$. Since U_i is open, there exists an $\epsilon > 0$ with $B_\epsilon(s) \subseteq U_i$. Now $[a, s + \epsilon/2] \subseteq \bigcup_{i=1}^{n} U_i$ also holds, in contradiction to the choice of s. Thus $s = b$ and $[a, b]$ possesses a finite subcover. □

Theorem II.8.28 (Heine-Borel)**.** *Every compact subset of a metric space is bounded and closed. In the Euclidean space $\mathbb{R}^n$, the converse also holds.*

Proof. Let (M, d) be a metric space and $K \subseteq M$ compact. According to Theorem II.8.21 and Lemma II.8.23, K is closed. Since the open cover $K \subseteq \bigcup_{n \in \mathbb{N}} B_n(x)$ for an $x \in M$ has a finite subcover, K is bounded.

Now let $M = \mathbb{R}^n$ and A be bounded and closed. Then there exist $a, b \in \mathbb{R}$ with $A \subseteq [a, b]^n$. If $U_1, \ldots, U_n \subseteq \mathbb{R}$, then also $U_1 \times \ldots \times U_n \subseteq M$. Conversely, for every open set $U \subseteq M$ and $x \in U$, there exist open sets $U_1, \ldots, U_n \subseteq \mathbb{R}$ with $x \in U_1 \times \ldots \times U_n \subseteq U$. This shows that the Euclidean metric on M is exactly the product topology of the Euclidean metric on $\mathbb{R}$. According to Lemma II.8.27, $[a, b]$ is a compact space with respect to the relative topology. According to Tychonoff, $[a, b]^n$ is also compact. According to Remark II.8.13, A is compact. □

Theorem II.8.29 (Lebesgue)**.** *Let (M, d) be a compact metric space and $M = \bigcup_{i \in I} U_i$ an open cover. Then there exists a $\delta > 0$ such that every subset $A \subseteq M$ with $d(A) \leq \delta$ lies in some U_i.*

Proof. For every $x \in M$ there exists an $\epsilon_x > 0$ such that $B_{2\epsilon_x}(x)$ lies in some U_i. Since M is compact, there exist $x_1, \ldots, x_n \in M$ with $M = \bigcup_{i=1}^{n} B_{\epsilon_{x_i}}(x_i)$. Let $\delta := \min\{\epsilon_{x_i} : i = 1, \ldots, n\}$. Let $a \in A \cap B_{\epsilon_{x_i}}(x_i)$. For all $b \in A$ it holds that

$$d(b, x_i) \leq d(b, a) + d(a, x_i) < \delta + \epsilon_{x_i} \leq 2\epsilon_{x_i}$$

and $A \subseteq B_{2\epsilon_{x_i}}(x_i)$. This shows the claim. □

Definition II.8.30. Let $(A, \mathcal{A})$ and $(B, \mathcal{B})$ be topological spaces. A map $f \colon A \to B$ is called *continuous*, if $f^{-1}(C) \in \mathcal{A}$ holds for all $C \in \mathcal{B}$ (preimages of open sets are open). If f is bijective and f, f^{-1} are continuous, then f is called a *homeomorphism*. If applicable, A and B are called *homeomorphic*.

Remark II.8.31.

(i) A map $f\colon A \to B$ is continuous if and only if preimages of closed sets are closed, because $A \setminus f^{-1}(C) = f^{-1}(B \setminus C)$.

(ii) The composition of continuous maps is obviously continuous.

(iii) If $f\colon A \to B$ is continuous and $K \subseteq A$ is compact, then $f(K)$ is also compact, because if $f(K) \subseteq \bigcup_{i\in I} U_i$ is an open cover, then $K \subseteq \bigcup_{i\in I} f^{-1}(U_i)$ is also an open cover.

(iv) The product topology on $X := \bigtimes_{i\in I} X_i$ is the coarsest topology such that the projections $X \to X_i$, $(x_j)_j \mapsto x_i$ are continuous.

Example II.8.32.

(i) Unlike in (linear) algebra, the inverse map of a bijective continuous map is not automatically continuous. Consider for example $A = B = \mathbb{N}$ with the discrete topology on A and the trivial topology on B. Then $f\colon A \to B$, $a \mapsto a$ is continuous, but f^{-1} is not.

(ii) The map $\mathbb{R} \to (0,1)$, $x \mapsto \frac{1}{1+2^x}$ is a homeomorphism with respect to the Euclidean (relative) topology. A bounded space can therefore be homeomorphic to an unbounded space.

Corollary II.8.33. *Let A be a compact space and B a Hausdorff space. Then every continuous bijection $A \to B$ is a homeomorphism.*

Proof. Let $f\colon A \to B$ be a continuous bijection and $U \subseteq A$ closed. According to Remark II.8.13 and Remark II.8.31, U and $f(U)$ are compact. According to Lemma II.8.23, $f(U)$ is closed. Therefore f^{-1} is continuous. □

II.9. Hyperreal and surreal numbers

Remark II.9.1. In analysis, one defines real numbers as equivalence classes of rational Cauchy sequences. Two sequences from $\mathbb{Q}^{\mathbb{N}}$ are considered equivalent if their difference is a null sequence. The same construction applied to $\mathbb{R}$ yields nothing new, since $\mathbb{R}$ is already complete (every Cauchy sequence converges). We therefore define a different equivalence relation on $\mathbb{R}^{\mathbb{N}}$.

Definition II.9.2. Let $\mathcal{F}$ be an ultrafilter on $\mathbb{N}$ that contains all cofinite sets (and therefore, according to Lemma II.8.4, contains no finite set). We define an equivalence relation $\sim$ on $\mathbb{R}^{\mathbb{N}}$ by

$$(a_0, a_1, \ldots) \sim (b_0, b_1, \ldots) \ :\Longleftrightarrow\ \{n \in \mathbb{N} : a_n = b_n\} \in \mathcal{F}.$$

For $a = (a_n)_n \in \mathbb{R}^{\mathbb{N}}$ let $[a]$ be the equivalence class of a. One calls ${}^*\mathbb{R} := \{[a] : a \in \mathbb{R}^{\mathbb{N}}\}$ the set of *hyperreal* numbers. For $a, b \in \mathbb{R}^{\mathbb{N}}$ we define

$$\begin{aligned} [a] + [b] &:= [(a_n + b_n)_n], \\ [a] \cdot [b] &:= [(a_n b_n)_n], \\ [a] < [b] &:\Longleftrightarrow \{n \in \mathbb{N} : a_n < b_n\} \in \mathcal{F}. \end{aligned}$$

Remark II.9.3.

(i) Let $a, b, c \in \mathbb{R}^{\mathbb{N}}$ with $a \sim b \sim c$. Then $S := \{n \in \mathbb{N} : a_n = b_n\}$ and $T := \{n \in \mathbb{N} : b_n = c_n\}$ lie in $\mathcal{F}$. Because of $S \cap T \subseteq \{n \in \mathbb{N} : a_n = c_n\}$, it holds that $a \sim c$. Therefore $\sim$ is indeed an equivalence relation. With the same argument one shows that $+$, $\cdot$ and $<$ are well-defined on ${}^*\mathbb{R}$. Furthermore, the usual calculation rules and (II.6.1) hold.

(ii) Through $r \mapsto [(r, r, \ldots)]$ one can embed $\mathbb{R}$ into ${}^*\mathbb{R}$. On the other hand, $x := [(0, 1, \ldots)] \in {}^*\mathbb{R} \setminus \mathbb{R}$ with $r < x$ for all $r \in \mathbb{R}$. Analogously, $x := [(2^0, 2^{-1}, \ldots)] \in {}^*\mathbb{R}$ with $0 < x < r$ for all positive $r \in \mathbb{R}$. According to Theorem II.5.13 and Theorem II.6.10, $|\mathbb{R}| \leq |{}^*\mathbb{R}| \leq |\mathbb{R}^{\mathbb{N}}| = |2^{\mathbb{N}}| = |\mathbb{R}|$, i. e. $\mathbb{R}$ and ${}^*\mathbb{R}$ have the same cardinality.

(iii) We define $-[a] := [(-a_n)_n]$ and

$$|[a]| := \begin{cases} [a] & \text{if } [a] \geq 0, \\ -[a] & \text{otherwise} \end{cases}$$

for $a \in {}^*\mathbb{R}$. One easily shows $|xy| = |x||y|$ and $|x + y| \leq |x| + |y|$ for $x, y \in {}^*\mathbb{R}$ (since $|.|$ does not map to $\mathbb{R}$, it is formally not a norm).

(iv) Certainly $1 \in \mathbb{R} \subseteq {}^*\mathbb{R}$ is a neutral element of multiplication. Let $a \in {}^*\mathbb{R} \setminus \{0\}$ and

$$b_n := \begin{cases} a_n^{-1} & \text{if } a_n \neq 0, \\ 0 & \text{otherwise} \end{cases}$$

for $n \in \mathbb{N}$. According to Lemma II.8.4, $\{n \in \mathbb{N} : a_n \neq 0\} \in \mathcal{F}$ holds. For $b = (b_n)_n$, it is therefore $[a] \cdot [b] = 1$. This shows that ${}^*\mathbb{R}$ is an ordered field.

(v) Under the assumption of the continuum hypothesis, one can show that ${}^*\mathbb{R}$ does not essentially depend on the choice of the ultrafilter $\mathcal{F}$. If one replaces the real numbers with the hyperreal numbers in analysis, one speaks of *non-standard analysis* (Exercise II.15).

Definition II.9.4. A hyperreal number x is called *finite*, if an $n \in \mathbb{N}$ with $|x| < n$ exists. If applicable, one calls

$$\operatorname{st}(x) := \sup\{r \in \mathbb{R} : r \leq x\} \in \mathbb{R}$$

the *standard part* of x. Let $\mathbb{E} \subseteq {}^*\mathbb{R}$ be the set of finite hyperreal numbers.

Remark II.9.5.

(i) $x \in {}^*\mathbb{R}$ is finite if and only if x is bounded on an index set in $\mathcal{F}$. From this it follows easily that $\mathbb{E}$ is closed under addition and multiplication (but not division).

(ii) From $x < n \in \mathbb{N}$ it follows that the set $\{r \in \mathbb{R} : r \leq x\}$ is bounded and therefore has a supremum.

(iii) Let $a := (a_n)_n \in \mathbb{R}^{\mathbb{N}}$ with $b := \lim_{n\to\infty} a_n \in \mathbb{R}$. For all $r < b$, the cofinite set $\{n \in \mathbb{N} : r < a_n\}$ lies in $\mathcal{F}$. This shows $r \leq [a]$ and $\operatorname{st}(a) \geq b$. For all $r > b$, on the other hand, $[a] < r$. This shows $\operatorname{st}(a) = b$.

(iv) Conversely, if $a = [(a_n)_n] \in {}^*\mathbb{R}$ is finite, the sequence $(a_n)_n$ needs to be neither convergent nor bounded. According to Lemma II.8.4, for example, $(n(1 + (-1)^n)_n \sim 0$ or $(n(1 - (-1)^n))_n \sim 0$ holds.

Theorem II.9.6.

(i) For $x \in \mathbb{E}$, $\operatorname{st}(x)$ is the unique real number with $|x - \operatorname{st}(x)| < r$ for all positive $r \in \mathbb{R}$, i. e. $\operatorname{st}(x)$ lies "arbitrarily close" to x. In particular, $\operatorname{st}(x) = x$ if and only if $x \in \mathbb{R}$.

(ii) For $x, y \in \mathbb{E}$ we have

$$\operatorname{st}(x+y) = \operatorname{st}(x) + \operatorname{st}(y), \qquad \operatorname{st}(xy) = \operatorname{st}(x)\operatorname{st}(y), \qquad x \leq y \implies \operatorname{st}(x) \leq \operatorname{st}(y).$$

Proof.

(i) In the case $r + \operatorname{st}(x) \leq x$, $\operatorname{st}(x)$ would not be an upper bound of $M := \{s \in \mathbb{R} : s \leq x\}$. Thus $x - \operatorname{st}(x) < r$ holds. Since $\operatorname{st}(x)$ is the least upper bound of M, there exists an $s \in \mathbb{R}$ with $\operatorname{st}(x) - r < s < x$. From this it follows that $\operatorname{st}(x) - x < r$. Overall, $|x - \operatorname{st}(x)| < r$ for all positive $r \in \mathbb{R}$. Suppose $t \in \mathbb{R}$ satisfies the same estimate. Then by the triangle inequality $|\operatorname{st}(x) - t| \leq |\operatorname{st}(x) - x| + |x - t| < 2r$ for all $r \in \mathbb{R}$. It follows that $t = \operatorname{st}(x)$.

(ii) According to (i), $|x + y - \operatorname{st}(x) - \operatorname{st}(y)| \leq |x - \operatorname{st}(x)| + |y - \operatorname{st}(y)| \leq r$ holds for all positive $r \in \mathbb{R}$. From the uniqueness in (i) it follows that $\operatorname{st}(x+y) = \operatorname{st}(x) + \operatorname{st}(y)$. Analogously, one obtains $\operatorname{st}(xy) = \operatorname{st}(x)\operatorname{st}(y)$ from

$$|xy - \operatorname{st}(x)\operatorname{st}(y)| \leq |x(y - \operatorname{st}(y)) + (x - \operatorname{st}(x))\operatorname{st}(y)| \leq |x||y - \operatorname{st}(y)| + |x - \operatorname{st}(x)||\operatorname{st}(y)|.$$

Now let $x \leq y$. Then $\operatorname{st}(y)$ is an upper bound of $\{r \in \mathbb{R} : r \leq x\}$. This shows $\operatorname{st}(x) \leq \operatorname{st}(y)$. □

Remark II.9.7. We generalize the construction of Dedekind cuts to define a significantly larger class of numbers.

Definition II.9.8 (Conway)**.** Let $\mathbb{S}_0 := \varnothing$. Recursively we define for every cardinal number $\mathfrak{a} > 0$ the set $\mathbb{S}_\mathfrak{a}$ of all pairs of the form $\{L, R\}$ with the following properties:

- $L, R \subseteq \bigcup_{\mathfrak{b}<\mathfrak{a}} \mathbb{S}_\mathfrak{b}$.
- $\forall l \in L, r \in R : r \not\leq l$.

The relation $\leq$ is thereby also recursively defined by

$$\{L, R\} \leq \{L', R'\} \ :\Longleftrightarrow\ \forall l \in L, r' \in R' : \{L', R'\} \not\leq l,\ r' \not\leq \{L, R\}.$$

We will see that

$$\{L, R\} \sim \{L', R'\} \ :\Longleftrightarrow\ \{L, R\} \leq \{L', R'\} \leq \{L, R\}$$

defines an equivalence relation. Let the equivalence class of $\{L, R\}$ be $(L|R)$. We will often identify $\mathbb{S}_\mathfrak{a}$ with the corresponding set of equivalence classes and transfer the definition of $\leq$ to equivalence classes. One then calls $\mathbb{S} := \bigcup_\mathfrak{a} \mathbb{S}_\mathfrak{a}$ the class of *surreal* numbers.

Remark II.9.9. In the following, we prove properties of the surreal numbers using transfinite induction. The base case is usually trivial because there is nothing to show for $\mathbb{S}_0 = \varnothing$. We first check that $\leq$ is reflexive and transitive. Let $(L|R) \in \mathbb{S}$ be given with $L \subseteq \mathbb{S}_\mathfrak{a}$ and $R \subseteq \mathbb{S}_\mathfrak{b}$. Let $l \in L$ and $r \in R$. By induction on $(\mathfrak{a}, \mathfrak{b})$ we can assume $l \leq l$ and $r \leq r$. In the case $(L|R) \leq l$ it would follow that $l \not\leq l$ and in the case $r \leq (L|R)$ it would follow that $r \not\leq r$. This shows $(L|R) \leq (L|R)$, i. e. $\leq$ and $\sim$ are reflexive. Now let $(L|R) \leq (L'|R') \leq (L''|R'')$. Suppose there exists an $l \in L$ with $(L''|R'') \leq l$. Inductively it then holds that $(L'|R') \leq l$ and $(L|R) \leq l$. This contradicts $l \leq l$. Analogously one shows $r'' \not\leq (L|R)$ for all $r'' \in R''$. Thus $(L|R) \leq (L''|R'')$ and $\leq$ is transitive. By definition, $\sim$ is an equivalence relation and $\leq$ is an ordering relation on $\mathbb{S}$.

Lemma II.9.10. *Let $(L|R) \in \mathbb{S}$. Then $l < (L|R) < r$ holds for all $l \in L$ and $r \in R$. Furthermore, $\leq$ is total.*

Proof. By definition of $(L|R)$ it holds that $r \not\leq l$. Let $l = (L_l|R_l)$. Inductively it holds that $l' < l$ for all $l' \in L_l$. In the case $(L|R) \leq l'$ it would follow that $(L|R) \leq l$ and $l \not\leq l$. Thus $(L|R) \not\leq l'$ for all $l' \in L$. This shows $l < (L|R)$. Now let $r = (L_r, R_r)$. Inductively it holds that $r < r'$ for all $r' \in R_r$. In the case $r' \leq (L|R)$ it would follow that $r \leq (L|R)$ in contradiction to $r \leq r$. Therefore $(L|R) < r$ holds. For the second assertion let $(L'|R') \in \mathbb{S}$ with $(L|R) \not\leq (L'|R')$. Then there exists an $l \in L$ with $(L'|R') \leq l$ or an $r' \in R'$ with $r' \leq (L|R)$. In both cases it follows that $(L'|R') \leq (L|R)$. This shows the totality of $\leq$. □

Remark II.9.11. According to Lemma II.9.10, $(L|R) \in \mathbb{S}$ holds if and only if $l < r$ for all $l \in L$ and $r \in R$. Furthermore,

$$(L|R) \leq (L'|R') \iff \forall l \in L, r' \in R' : l < (L'|R'),\ (L|R) < r'.$$

We will use this from now on.

Example II.9.12. To save parentheses, we write $(x, y, \ldots|a, b, \ldots) := (\{x, y, \ldots\}|\{a, b, \ldots\})$.

(i) Apparently $\mathbb{S}_1$ consists only of $0 := (\varnothing|\varnothing)$. One can see that $1 := (0|\varnothing)$ and $-1 := (\varnothing|0)$ lie in $\mathbb{S}_2$, while $(0|0)$ is not allowed because of $0 \leq 0$. According to Lemma II.9.10, $-1 < 0 < 1$ holds.

(ii) $(L|R) = 0$ holds if and only if $l < 0$ and $r > 0$ for all $l \in L$ and $r \in R$.

(iii) From $0 < (-1, 0|\varnothing)$ it follows that $(-1, 0|\varnothing) \leq 1 \leq (-1, 0|\varnothing)$, i. e. $(-1, 0|\varnothing) = 1$. This can be generalized.

Lemma II.9.13. *If L has a greatest element, then $(L|R) = (\max(L)|R)$. If R has a smallest element, then $(L|R) = (L|\min(R))$.*

Proof. For all $l \in L$, $l \leq \max L < (\max(L)|R)$ holds according to Lemma II.9.10. For all $r \in R$, $(L|R) < r$ holds. This shows $(L|R) \leq (\max(L)|R)$. According to Lemma II.9.10, $\max L < (L|R)$ and $(\max(L)|R) < r$ also hold. It follows that $(\max(L)|R) = (L|R)$. The second statement is analogous. □

Definition II.9.14. For $x := (L|R) \in \mathbb{S}$ and $y := (L'|R') \in \mathbb{S}$ we define recursively:

$$\begin{aligned} x + y &:= \big((L + y) \cup (x + L') \mid (R + y) \cup (x + R')\big), \\ -x &:= (-R \mid -L), \end{aligned}$$

where $x + L = \{x + l : l \in L\}$.

Remark II.9.15. It is by no means trivial that addition is compatible with $\sim$ and actually produces surreal numbers. In the first step, we can mentally apply the definition only to the original elements $\{L, R\}$ and ignore the requirement $l < r$ for $l \in L$ and $r \in R$. The next step towards well-definedness is the following lemma.

Lemma II.9.16. *For all $x, y, z \in \mathbb{S}$ holds*

$$x \leq y \iff x + z \leq y + z.$$

Proof. Let $x = (L|R) \in \mathbb{S}_{\mathfrak{a}}$, $y = (L'|R') \in \mathbb{S}_{\mathfrak{b}}$ and $z = (L''|R'') \in \mathbb{S}_{\mathfrak{c}}$. As usual, let $l, r, l', \ldots$ be elements from $L, R, L', \ldots$. We choose cardinal numbers $\bar{\mathfrak{a}} \leq \bar{\mathfrak{b}} \leq \bar{\mathfrak{c}}$ with $\{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}\} = \{\bar{\mathfrak{a}}, \bar{\mathfrak{b}}, \bar{\mathfrak{c}}\}$. Let $x + z \leq y + z$, but $x > y$. Then there exists an l with $l \geq y$ or an r' with $r' \leq x$. By induction on $(\bar{\mathfrak{a}}, \bar{\mathfrak{b}}, \bar{\mathfrak{c}})$ it follows that $l + z \geq y + z$ or $r' + z \leq x + z$ (the base case of the induction follows from the simple equation $0 + 0 = 0$). Both contradict $x + z \leq y + z$. Therefore $x \leq y$ holds.

Now let $x \leq y$, but $x + z > y + z$. Then one of the following statements holds:

$$l + z \geq y + z, \qquad x + l'' \geq y + z, \qquad x + z \geq r' + z, \qquad x + z \geq y + r''.$$

Inductively, $y + l'' \geq x + l''$ and $y + r'' \geq x + r''$ hold. According to the first part of the proof, one of the statements follows:

$$l \geq y, \qquad l'' \geq z, \qquad x \geq r', \qquad z \geq r''.$$

All statements contradict $x \leq y$ or Lemma II.9.10. □

Remark II.9.17. From Lemma II.9.16 it follows that

$$\begin{aligned} x < y &\iff x + z < y + z, \\ x \leq x',\ y \leq y' &\implies x + y \leq x' + y'. \end{aligned}$$

With the usual notation, $l + y < r + y$, $l + y < x + r'$, $x + l' < r + y$ and $x + l' < x + r'$ hold. This shows $x + y \in \mathbb{S}$. If $x = x'$ and $y = y'$, then $x + y = x' + y'$ results, i. e. the addition is well-defined. Similarly, one shows

$$x \leq y \iff -y \leq -x.$$

From $l < r$ it follows in particular that $-r < -l$. Thus $-x \in \mathbb{S}$ also holds.

Lemma II.9.18. *For all $x, y, z \in \mathbb{S}$ the following hold:*

(i) $x + y = y + x$ *and* $(x + y) + z = x + (y + z)$.

(ii) $x + 0 = x$ *and* $x + (-x) = 0$.

Proof. As usual, let $x = (L|R)$, $y = (L'|R')$ and $z = (L''|R'')$.

(i) The equation $x + y = y + x$ is trivial. It holds that

$$\begin{aligned} (x + y) + z &= (L + y \cup x + L' \mid R + y, x + R') + z \\ &= \big((L + y) + z \cup (x + L') + z \cup (x + y) + L'' \mid \\ &\qquad (R + y) + z \cup (x + R') + z \cup (x + y) + R''\big) \\ &= \big(L + (y + z) \cup x + (L' + z) \cup x + (y + L'') \mid \\ &\qquad R + (y + z) \cup x + (R' + z) \cup x + (y + R'')\big) \\ &= x + (L' + z \cup y + L'' \mid R' + z \cup y + R'') \\ &= x + (y + z) \end{aligned}$$

(ii) Obviously $0 + 0 = (\varnothing|\varnothing) = 0$ holds. Inductively it follows that $x + 0 = (L + 0 \mid R + 0) = (L, R) = x$. Furthermore, $x + (-x) = (L + (-x) \cup x + (-R) \mid R + (-x) \cup x + (-L))$. From Lemma II.9.16 it follows inductively that $l + (-x) < l + (-l) = 0$ and $x + (-r) < r + (-r) = 0$. This shows $x + (-x) \leq 0$. Analogously, $0 = r + (-r) < r + (-x)$ and $0 = l + (-l) < x + (-l)$. Thus $0 \leq x + (-x)$ is proven. □

Remark II.9.19. Lemma II.9.18 shows that the surreal numbers form an abelian group with respect to addition. We can now write $x - y$ instead of $x + (-y)$ as usual.

Example II.9.20.

(i) We have already defined $1 = (0|\varnothing)$. For $n \in \mathbb{N}_+$, we set inductively $n := (n-1|\varnothing)$. Then

$$n + m = (n-1 \mid \varnothing) + (m-1 \mid \varnothing) = (n-1+m,\ n+m-1 \mid \varnothing) = (n+m-1 \mid \varnothing).$$

In this way, one can interpret all integers as surreal numbers. More generally, one can identify every cardinal number $\mathfrak{a}$ with $(\{\mathfrak{b} : \mathfrak{b} < \mathfrak{a}\} \mid \varnothing)$.

(ii) Let $x := (0|1) \in \mathbb{S}$. According to Lemma II.9.10, $0 < x < 1$ and $x + x = (x|x+1)$ holds. It follows that $x + x \leq 1 \leq x + x$. Thus, one can define $\frac{1}{2} := (0|1)$. Analogously, one shows $\frac{1}{4} = (0|\frac{1}{2})$ etc. In this way, all rational numbers of the form $\frac{a}{2^n}$ with $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ can be realized as surreal numbers. For every other real number $r \in \mathbb{R}$, there exist $a_n \in \mathbb{Z}$ with $a_n 2^{-n} < r < (a_n + 1)2^{-n}$ for all $n \in \mathbb{N}$. It follows that

$$r = \big(\{a_n 2^{-n} : n \in \mathbb{N}\} \mid \{(a_n + 1)2^{-n} : n \in \mathbb{N}\}\big) \in \mathbb{S}.$$

Definition II.9.21. For surreal numbers $x = (L|R)$ and $y = (L'|R')$, we define

$$x \cdot y := xy := (ly + xl' - ll',\ ry + xr' - rr' \mid ly + xr' - lr',\ ry + xl' - rl' : l, l', r, r'),$$

where each term such as $ly + xl' - ll'$ belongs to a tuple of parameters such as $(l, l') \in L \times L'$.

Lemma II.9.22. *For all $x, x_1, x_2, y, y_1, y_2 \in \mathbb{S}$, the following holds:*

(i) $xy \in \mathbb{S}$.

(ii) From $x = y$ follows $xz = yz$.

(iii) From $x_1 \leq x_2$ and $y_1 \leq y_2$ follows $x_1y_2 + x_2y_1 \leq x_1y_1 + x_2y_2$. The inequality is strict if $x_1 < x_2$ and $y_1 < y_2$.

(iv) $x, y > 0 \implies xy > 0$.

Proof. We prove the first three statements simultaneously by induction.

(i) The components of xy are inductively surreal numbers. We must show

$$\begin{aligned} l_1y + xl' - l_1l' &< l_2y + xr' - l_2r', & ly + xl_1' - ll_1' &< ry + xl_2' - rl_2', \\ ry + xr_1' - rr_1' &< ly + xr_2' - lr_2', & r_1y + xr' - r_1r' &< r_1y + xl' - r_1l'. \end{aligned}$$

Assume $l_1 \leq l_2$. Then $l_1y + l_2l' \leq l_1l' + l_2y$ and $l_2r' + xl' < l_2l' + xr'$ follow from (iii). In total,

$$l_1y + xl' - l_1l' \leq l_2y + xl' - l_2l' < l_2y + xr' - l_2r'.$$

If, on the other hand, $l_2 \leq l_1$ holds, then one has $l_1r' + xl' < l_1l' + xr'$, $l_2r' + l_1y \leq l_2y + l_1r'$ and

$$l_1y + xl' - l_1l' < l_1y + xr' - l_1r' \leq l_2y + xr' - l_2r'.$$

Thus the first of the four inequalities is proven. We omit the other three.

(ii) Inductively, $xl'' = yl''$ and $xr'' = yr''$ already hold. With (iii) it follows that $lz + xl'' - ll'' < yz$ and $rz + xr'' - rr'' < yz$. Analogously, one shows $xz < l'z + yr'' - l'r''$ and $xz < r'z + yl'' - r'l''$. Thus $xz \leq yz$ holds. For reasons of symmetry, $yz \leq xz$ follows.

(iii) According to (ii), we can assume $x_1 < x_2$ and $y_1 < y_2$ (note that in the proof of (ii) we only used the strict inequality for (iii)). We denote the inequality to be proven by $U(x_1, x_2, y_1, y_2)$. We use induction on $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d})$, where $y_1 \in \mathbb{S}_\mathfrak{a}$, $y_2 \in \mathbb{S}_\mathfrak{b}$, $x_1 \in \mathbb{S}_\mathfrak{c}$, $x_2 \in \mathbb{S}_\mathfrak{d}$. If $l_2 < x_1$ and $x_2 < r_1$ were true for all l_2 and r_1, then we would have $x_2 < x_1$. Thus $x_1 < r_1 \leq x_2$ holds for some l_2 or $x_1 \leq l_2 < x_2$ for some r_1. Let us assume the first case (the second case is analogous). Inductively, $U(r_1, x_2, y_1, y_2)$ holds. It suffices to show $U(x_1, r_1, y_1, y_2)$ with strict inequality, because then

$$\begin{aligned}(x_1y_2 + r_1y_1) + x_2y_1 < x_1y_1 + (r_1y_2 + x_2y_1) \leq x_1y_1 + r_1y_1 + x_2y_2,\\ x_1y_2 + x_2y_1 < x_1y_1 + x_2y_2\end{aligned}$$

according to Remark II.9.17. We can now analogously assume $y_1 < r_1' \leq y_2$. Then $U(x_1, r_1, r_1', y_2)$ holds and it remains to prove $U(x_1, r_1, y_1, r_1') = U(x, r, y, r')$ with strict inequality. This means $ry + xr' - rr' < xy$ and holds according to (i) (in the proof of (i) we used (iii) only for a lower induction stage).

(iv) Follows from (iii) with $(x_1, x_2, y_1, y_2) = (0, x, 0, y)$. □

Lemma II.9.23. *For all $x, y, z \in \mathbb{S}$ the following hold:*

(i) $xy = yx$ *and* $(x + y)z = xz + yz$.

(ii) $(xy)z = x(yz)$.

(iii) $1x = x$.

Proof.

(i) If one swaps x and y, the terms on the left half of xy remain invariant, while the terms on the right half are swapped. This shows $xy = yx$. Let $x + y = (S|T)$ and $s \in S$ as well as $t \in T$. The first term of the left half of $(x + y)z$ consists of elements of the form

$$\begin{aligned}\{sz + (x + y)l'' - sl''\} &= \{(l + y)z + (x + y)l'' - (l + y)l'',\ (x + l')z + (x + y)l'' - (x + l')l''\}\\ &= \{(lz + xl'' - ll'') + yz,\ xz + (l'z + yl'' - l'l'')\}.\end{aligned}$$

These are components of the left half of $xz + yz$. The other terms are treated analogously.

(ii) The left half of $(xy)z$ consists, according to (i) and induction, of elements of the form

$$\begin{aligned}(ly + xl' - ll')z + (xy)l'' - (ly + xl' - ll')l'' &= l(yz) + x(l'z + yl'' - l'l'') - l(l'z + yl'' - l'l''),\\ (ry + xr' - rr')z + (xy)l'' - (ry + xr' - rr')l'' &= r(yz) + x(r'z + yl'' - r'l'') - r(r'z + yl'' - r'l''),\\ (ly + xr' - lr')z + (xy)r'' - (ly + xr' - lr')r'' &= l(yz) + x(r'z + yr'' - r'r'') - l(r'z + yr'' - r'r''),\\ (ry + xl' - rl')z + (xy)r'' - (ry + xl' - rl')r'' &= r(yz) + x(l'z + yr'' - l'r') - r(l'z + yr'' - l'r').\end{aligned}$$

This matches the left half of $x(yz)$. The respective right halves are treated analogously.

(iii) It holds that

$$\begin{aligned}x \cdot 0 &= x \cdot (\varnothing|\varnothing) = (\varnothing|\varnothing) = 0,\\ x \cdot 1 &= x \cdot (0|\varnothing) = (l1 + x0 - l0 \mid r1 + x0 - r0) = (L|R) = x.\end{aligned}$$ □

Example II.9.24. For $n, m \in \mathbb{N}_+$ it holds that

$$nm = \big((n-1)m + n(m-1) - (n-1)(m-1) \mid \varnothing\big) = (nm - 1 \mid \varnothing)$$

as expected. Furthermore,

$$2 \cdot \frac{1}{2} = (1|\varnothing) \cdot (0|1) = \Big(\frac{1}{2} + 2 \cdot 0 - 1 \cdot 0 \;\Big|\; \frac{1}{2} + 2 \cdot 1 - 1 \cdot 1\Big) = \Big(\frac{1}{2} \;\Big|\; \frac{3}{2}\Big) = 1.$$

Remark II.9.25.

(i) The definition of xy can be motivated by the following inequalities:

$$(x-l)(y-l') > 0, \qquad (r-x)(r'-y) > 0, \qquad (x-l)(r'-y) > 0, \qquad (r-x)(y-l') > 0.$$

(ii) It follows from Lemma II.9.23 that $(\mathbb{S}, +, \cdot)$ is a commutative ring (provided one waives the requirement that rings must be sets). One can further show that $\mathbb{S}$ is even an (ordered) field, i. e. every $x \in \mathbb{S} \setminus \{0\}$ possesses a multiplicative inverse. The recursive definition of x^{-1} is however laborious, as can already be seen from

$$\frac{1}{3} = (2|\varnothing)^{-1} = \Big(\sum_{k=1}^{n} \frac{1}{4^k} \;\Big|\; \frac{1}{4^n} + \sum_{k=1}^{n} \frac{1}{4^k} : n \in \mathbb{N}\Big).$$

We have already verified that addition and multiplication of natural numbers coincide with the corresponding operations in $\mathbb{S}$. From this it follows easily that $\mathbb{Q}$ is a subfield of $\mathbb{S}$. This can be extended to $\mathbb{R}$. To this end, let $r = (a_n|b_n : n \in \mathbb{N}) \in \mathbb{R}$ with $a_n, b_n \in \mathbb{Q}$ as in Example II.9.20. For $m \in \mathbb{N}_+$ it first holds that

$$\begin{aligned} mr &= \big((m-1)r + ma_n - (m-1)a_n \mid (m-1)r + mb_n - (m-1)b_n\big) \\ &= \big((m-1)r + a_n \mid (m-1)r + b_n\big), \end{aligned}$$

where both sides converge in the reals to mr. Now let $s = (a'_n|b'_n)$ with $a'_n, b'_n \in \mathbb{Q}$. Then

$$rs = (a_n s + r a'_m - a_n a'_m,\ b_n s + r b'_m - b_n b'_m \mid a_n s + r b'_m - a_n b'_m,\ b_n s + r a'_m - b_n a'_m),$$

where again both sides converge to rs. Thus $\mathbb{R}$ is also a subfield of $\mathbb{S}$ with the same order relation. One can show more generally that every ordered field is a subfield of $\mathbb{S}$.

(iii) In contrast to $\mathbb{R}$, the arithmetic of arbitrary cardinal numbers does not coincide with the operations in $\mathbb{S}$. According to Theorem II.5.13, for example, $\mathbb{N} + \mathbb{N} = \mathbb{N}$ holds. Conversely, this means that one can construct surreal numbers with surprising properties. For this, let $\mathfrak{a} = (\mathbb{N}|\varnothing) \cong \mathbb{N}$. Then with $x := (\mathbb{N}|\mathfrak{a})$ one obtains a surreal number that is larger than every real number, but smaller than $\mathfrak{a}$. More precisely,

$$x + 1 = (\mathbb{N} + 1, x \mid \mathfrak{a} + 1) = (x \mid \mathfrak{a} + 1) = \mathfrak{a},$$

as one easily verifies. Now let $y := (\mathbb{N} \mid \mathfrak{a} - n : n \in \mathbb{N})$. Then

$$y + y = (\mathbb{N} + y \mid \mathfrak{a} - \mathbb{N} + y) = \mathfrak{a},$$

since $n + y < \mathfrak{a}$, $n < n + y$ and $\mathfrak{a} < \mathfrak{a} - n + y$. One can therefore define $y = \frac{\mathfrak{a}}{2}$. Finally, let $z := (\mathbb{N} \mid 2^{-n}\mathfrak{a} : n \in \mathbb{N})$. From Lemma II.9.10 it follows that $nz < \mathfrak{a}$ and $(2^{-n} + 2^{-m})z < 2^{-n-m}\mathfrak{a}$ for all $n, m \in \mathbb{N}$. This yields

$$z^2 = \big(nz + zm - nm,\ 2^{-n}\mathfrak{a}z + 2^{-m}\mathfrak{a}z - 2^{-n-m}\mathfrak{a}^2 \mid nz + z2^{-m}\mathfrak{a} - n2^{-m}\mathfrak{a}\big) \leq \mathfrak{a}.$$

Conversely, $\mathfrak{a} \leq z^2$, since $n < z^2$ and $\mathfrak{a} < nz + z2^{-m}\mathfrak{a} - n2^{-m}\mathfrak{a}$. This shows $y^2 = \mathfrak{a}$ and $y = \sqrt{\mathfrak{a}}$. One can show more generally that every positive surreal number possesses an n-th root for every $n \in \mathbb{N}_+$. Analogously to the construction of $\mathbb{C}$ from $\mathbb{R}$, one obtains an algebraically closed field by adjoining a square root of -1 to $\mathbb{S}$.

Exercises

Exercise II.1. Let M be a set. Show that $\mathcal{P}(M)$ is a group with respect to the *symmetric difference*

$$A \ominus B := (A \cup B) \setminus (B \cap A).$$

Exercise II.2. Let $T(n) \subseteq \mathbb{N}$ be the set of all positive divisors of a number $n \in \mathbb{N}_+$. Investigate when $T(n)$ is totally ordered with respect to the divisibility relation.

Exercise II.3. Prove or disprove: Two totally ordered sets are isomorphic if and only if they have the same cardinality.

Exercise II.4.

(a) Construct a well-ordering on $\mathbb{Z}$.

(b) For reduced fractions $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}_+$, let

$$\frac{a}{b} \prec \frac{c}{d} \;:\Longleftrightarrow\; a < c \vee (a = c \wedge b < d).$$

Show that $(\mathbb{Q}_+, \prec)$ is a well-ordered set.

(c) Construct a well-ordering on $\mathbb{Q}$.

Exercise II.5. Show that $\mathbb{N}^2 \to \mathbb{N}$, $(x, y) \mapsto 2^x(2y + 1) - 1$ is a bijection.

Exercise II.6. Let α, β and γ be ordinal numbers with $\alpha < \beta$. Show:

(a) $\alpha + \gamma \leq \beta + \gamma$.

(b) $\alpha \cdot \gamma \leq \beta \cdot \gamma$.

(c) $\alpha^\gamma \leq \beta^\gamma$.

Show that in all three cases equality can occur (even if $\gamma > 0$).

Exercise II.7. Let $\alpha_0 := \omega$ and $\alpha_{n+1} := \alpha_n^\omega$ for $n \in \mathbb{N}$. Show that $\epsilon := \bigcup_{n\in\mathbb{N}} \alpha_n$ is a countable limit ordinal with $\omega^\epsilon = \epsilon$.

Exercise II.8. A limit ordinal $\alpha > 0$ is called *decomposable*, if there exist ordinal numbers $\beta, \gamma < \alpha$ with $\alpha = \beta + \gamma$. Otherwise α is called *indecomposable* Show:

(a) If α is indecomposable, then $\beta + \gamma < \alpha$ for all $\beta, \gamma < \alpha$.

(b) The following statements are equivalent:

(1) α is indecomposable.

(2) $\beta + \alpha = \alpha$ for all $\beta < \alpha$

(3) $\alpha = \omega^\beta$ for an ordinal number β.

Exercise II.9 (Stable Marriage Theorem)**.** Let F and M be finite sets of women and men of the same cardinality. Each woman and each man ranks the persons of the respective other gender according to attractiveness (total order). The GALE-SHAPLEY *algorithm* consists of the following steps:

(1) Each man makes a marriage proposal to the woman who is most attractive from his perspective.

(2) Each woman who has received proposals becomes engaged to the most attractive applicant for her. She rejects other applicants.

(3) The rejected (still unengaged) men make proposals to their second-most attractive women.

(4) If an engaged woman receives a proposal from a more attractive man, she rejects her fiancé and becomes engaged to the new applicant.

(5) This game is repeated until everyone is engaged (and marries).

Show:

(a) The algorithm terminates, whereby at the end all women and men are monogamously married.

(b) There is no pair $(f, m) \in F \times M$ such that f and m would rather be married to each other than to their actual partners.

Note: This algorithm is used in practice to distribute visitors on the internet to the nearest possible web servers.

Exercise II.10. Let G be a complete graph with at least 17 vertices, such that each edge is colored red, yellow, or blue. Show that G possesses a monochromatic triangle.
Note: Use the Ramsey number $R(3,3) = 6$.

Exercise II.11. Let M be a set with $n = 2k$ elements. Show that there are exactly $2^{\binom{n-1}{k-1}}$ systems $\mathcal{M} \subseteq \binom{M}{k}$ with $|\mathcal{M}| = \binom{n-1}{k-1}$ and $A \cap B \neq \varnothing$ for all $A, B \in \mathcal{M}$.
Note: $\binom{n-1}{k-1} = \frac{1}{2}\binom{n}{k}$.

Exercise II.12 (Universal Property of the Product Topology)**.** Let $(T_i)_{i \in I}$ be a family of topological spaces of $T := \bigtimes_{i \in I} T_i$. For every topological space M and continuous maps $f_i \colon M \to T_i$, there exists exactly one continuous map $f \colon M \to T$ with $\pi_i \circ f = f_i$ for all $i \in I$.

Exercise II.13. A topological space $(T, \mathcal{T})$ is called *path-connected*, if for every two points $x, y \in T$ there exists a continuous mapping $f \colon [0,1] \to T$ with $f(0) = x$ and $f(1) = y$ (w.r.t. $[0,1]$ with the Euclidean metric). Show:

(a) Every path-connected space is connected.

(b) The so-called *comb space*

$$T := \{(0,1)\} \cup \left(\left\{ \frac{1}{n} : n \in \mathbb{N}_+ \right\} \times [0,1] \right) \cup \left([0,1] \times \{0\} \right)$$

is connected w.r.t. the Euclidean metric, but not path-connected.

(c) Topological spaces T_1 and T_2 are (path-)connected if and only if $T_1 \times T_2$ is (path-)connected.

Exercise II.14. Check which of the following topological spaces are homeomorphic to each other w.r.t. the Euclidean norm: $\mathbb{R}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{R}^2$, $\mathbb{R}^2 \setminus \{0\}$.
Hint: Investigate the property: For every compact subset A of a topological space T there exists a compact subset $B \supseteq A$, such that $T \setminus B$ is connected.

Exercise II.15. For $f\colon \mathbb{R} \to \mathbb{R}$ and $[a] \in {}^*\mathbb{R}$ let ${}^*f([a]) = [(f(a_n) : n \in \mathbb{N})] \in {}^*\mathbb{R}$. Show:

(a) ${}^*f\colon {}^*\mathbb{R} \to {}^*\mathbb{R}$ is well-defined with ${}^*f(r) = f(r)$ for all $r \in \mathbb{R}$.

(b) For $f, g\colon \mathbb{R} \to \mathbb{R}$ it holds that ${}^*(f+g) = {}^*f + {}^*g$, ${}^*(f \cdot g) = {}^*f \cdot {}^*g$ and ${}^*(f \circ g) = {}^*f \circ {}^*g$.

For $x, y \in {}^*\mathbb{R}$ we write $x \approx y$, if $x - y \in \mathbb{E}$ and $\mathrm{st}(x-y) = 0$. Show:

(c) f is continuous at $x_0 \in \mathbb{R}$ if and only if for all $x \approx x_0$ it holds: ${}^*f(x) \approx f(x_0)$.

(d) f is uniformly continuous if and only if for all $x, y \in {}^*\mathbb{R}$ it holds: $x \approx y \Rightarrow {}^*f(x) \approx {}^*f(y)$.

(e) f is differentiable at $x_0 \in \mathbb{R}$ if and only if there exists a $y \in \mathbb{R}$ with $\frac{{}^*f(x_0+h)-f(x_0)}{h} \approx y$ for all $0 \neq h \approx 0$. If applicable, $f'(x_0) = y$.

Index