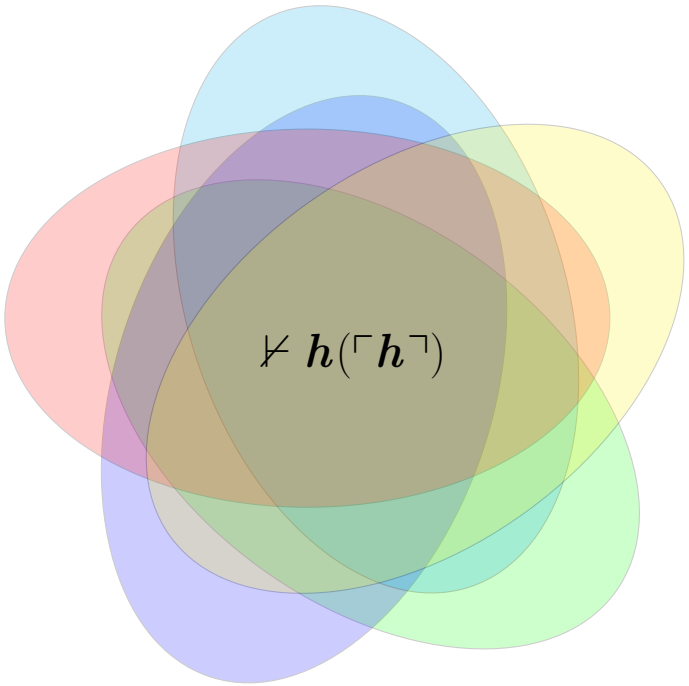
Logik und Mengenlehre

Benjamin Sambale

Version: 28. Juli 2025



Inhaltsverzeichnis

Vorwort

Die zweite Hälfte dieses Skripts (Mengenlehre) entstand im Rahmen eines Seminars im Sommersemester 2019 an der Friedrich-Schiller-Universität Jena. Erst 2025 habe ich die erste Hälfte (Logik) ergänzt (dafür lag keine Lehrveranstaltung zugrunde). Es liegt in der Natur der Sache, dass man nicht ernsthaft über Logik sprechen kann, ohne mengentheoretische Begriffe wie Element, Menge, Funktion und Relation in den Mund zu nehmen. Dieses Henne-Ei-Problem umgeht man üblicherweise dadurch, dass man diese Begriffe nur auf der Metaebene, also umgangssprachlich, verwendet. Zirkelschlüsse sind ausgeschlossen, da die tiefliegenden Ergebnisse der Logik nicht zum mengentheoretischen Aufbau der Mathematik benötigt werden. Man muss sich dennoch vor Augen halten, dass aufgrund der Gödelschen Unvollständigkeitssätze große Teile der Mathematik nicht hundertprozentig fundiert werden können. Es ist in gewisser Weise nur ein großes Gedankenexperiment oder Spiel.

Auch wenn der axiomatische Aufbau der Mathematik Grundlage aller weiteren Theorien sein sollte, eignet sich das Skript nicht für Studienanfänger, denn ich setze eine gewisse Vertrautheit mit Grundbegriffen und Beweisführungen voraus (beispielsweise aus meinem Skript zur linearen Algebra). In der Tat sind die Feinheiten der Logik und Mengenlehre für die meisten anderen Gebiete irrelevant. Dennoch ist die Theorie als solche ein spannendes Themengebiet.

Literatur:

- D. W. Hoffmann, *Grenzen der Mathematik*, 3. Auflage, Springer Spektrum, Wiesbaden, 2018
- E. Mendelson, *Introduction to mathematical logic*, 6. Auflage, CRC Press, Boca Raton, 2015
- C. Celluci, *The theory of Gödel*, Springer, Cham, 2022
- T. Jech, *Set Theory*, 3. Auflage, Springer, Berlin, 2002

I. Logik

I.1. Kalküle

Bemerkung I.1.1. Bevor man überhaupt über Mathematik reden kann, muss man sich auf eine Sprache einigen. Wie für jede Sprache braucht man dafür eine *Syntax* (z. B. lateinisches Alphabet mit Regeln der Zeichensetzung) und eine kontextabhängige *Semantik* (z. B. kann Birne für ein Obst stehen oder eine Abkürzung für Glühbirne sein). Es lässt sich nicht vermeiden, dass man die einfachsten Begriffe nicht weiter auf Bekanntes reduzieren kann, sondern als gegeben hinnehmen muss (so wie ein Kleinkind die Wörter „ja“ oder „Eins“ in der Muttersprache lernt). Wir stellen in diesem Abschnitt eine allgemeine Syntax der Mathematik vor. Formulierungen wie „genau dann, wenn“ und Begriffe wie „Menge“ oder „Funktion“ sind vorerst nur umgangssprachlich, d. h. auf der *Metaebene* zu verstehen (präzise Definitionen folgen in Definition I.2.3 bzw. Abschnitt II.1).

Definition I.1.2. Ein (HILBERT-)*Kalkül* $\mathcal{K}$ besteht aus folgenden Dingen:

- *Alphabet*: Variablen wie $a, b, c, \ldots$ und Symbole wie $(,), \neg, =, \ldots$.
- *Formeln*: Aneinanderreihungen von endlich vielen Zeichen des Alphabets nach bestimmten Regel (z. B. geöffnete Klammern müssen geschlossen werden).
- *Axiome*: Ausgewählte Formeln.
- *Schlussregeln*, die beschreiben wie man aus bekannten Formeln neue Formeln ableiten kann.
- *Beweise*: Aneinanderreihungen von endlich vielen Formeln $f_1, \ldots, f_n$, sodass jedes f_i ein Axiom ist oder sich durch Schlussregeln aus f_j mit $j < i$ ableiten lässt.

Eine Formel f heißt *Satz* oder *beweisbar*, falls sie am Ende eines Beweises auftaucht. Wir schreiben ggf. $\vdash f$. Existiert kein Beweis für f, so schreiben wir $\nvdash f$.

Bemerkung I.1.3.

(i) Da Beweise endlich sind und man durch Aneinanderreihung von Variablen neue Variablen (eigentlich Formeln) konstruieren kann (z. B. $a_1 = a$, $a_2 = aa$ usw.), kommt man mit einem endlichen Alphabet aus. Die Anzahl der Formeln (und Axiome, Schlussregeln) wird in der Regel jedoch unendlich sein.

(ii) Wir werden (formale) Beweise stets so schreiben, dass jede Zeile mit $\vdash$ beginnt und genau eine Formel enthält. Mit zunehmender Übung werden wir später mehrere Beweisschritte in einer Zeile zusammenfassen.

(iii) Schlussregel notieren wir in der Form $\frac{f_1,\ldots,f_n}{g}$ (Die Formel g wird aus den Formeln $f_1, \ldots, f_n$ abgeleitet.

(iv) Wir werden sehen, dass es in der Praxis nicht immer möglich ist zu entscheiden, ob $\vdash f$ oder $\nvdash f$ gilt (siehe Abschnitt I.8).

Beispiel I.1.4. Das Kalkül $\mathcal{K}$ sei gegeben durch:

- Alphabet: Variablen a, b (keine Symbole)
- Formeln: Alle Wörter aus a und b einschließlich des leeren Worts mit 0 Buchstaben.
- Axiome: a
- Schlussregeln: $\frac{f_1 a f_2}{f_1 a b f_2}$, $\frac{f_1 b f_2}{f_1 a a f_2}$, $\frac{f_1 f_2 f_3 f_2 f_4}{f_1 f_3 f_4}$ für beliebige Formeln $f_1, \ldots, f_4$.

Es gilt

$$\begin{aligned} &\vdash a \\ &\vdash ab \\ &\vdash abb \\ &\vdash abaa \\ &\vdash ba \end{aligned}$$

Da die letzte Schlussregel die Länge einer Formel verkürzt, ist es nicht-trivial alle Sätze von $\mathcal{K}$ aufzuzählen. Da in jedem Satz die Anzahl der a ungerade sein muss, ist $\nvdash aa$. (Aufgabe I.2)

Bemerkung I.1.5. Es ist wünschenswert, mit möglichst wenigen Axiomen und Schlussregeln möglichst viele Sätze zu beweisen. Das folgende Kalkül ist die Grundlage fast aller (zweiwertigen) Logiken.

Definition I.1.6 (Łukasiewicz)**.** Das Kalkül $\mathcal{A}$ der *Aussagenlogik* besteht aus:

- Die Variablen heißen *Elementaraussagen* und werden durch Großbuchstaben $A, B, \ldots$ bezeichnet. Die Symbole sind (,), $\neg$, $\Rightarrow$.
- Die Formeln heißen *Aussagen* und werden rekursiv definiert: Alle Elementaraussagen sind Aussagen. Sind f und g Aussagen, so auch $(\neg f)$ und $(f \Rightarrow g)$.
- Für alle Aussagen f, g, h gibt es folgende Axiome:

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

- Für Aussagen f und g ist der *Modus ponens*

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

  die einzige Schlussregel.

Bemerkung I.1.7.

(i) Die Klammersetzung in der rekursiven Definition von Formeln garantiert den eindeutigen Aufbau einer Formel. Um die Lesbarkeit zu erhöhen, werden wir dennoch Klammern einsparen und vereinbaren, dass $\neg$ stärker bindet als $\Rightarrow$. Das äußere Klammerpaar kann generell entfernt werden. Damit vereinfacht sich $((\neg f) \Rightarrow g)$ zu $\neg f \Rightarrow g$.

(ii) Gänzlich ohne Klammern kommt man aus, wenn man die sogenannte *polnische Notation* benutzt (was wir nicht vorhaben), bei der Symbole nicht zwischen Variablen, sondern links davon stehen: aus $(\neg f \Rightarrow g) \Rightarrow \neg h$ wird $\Rightarrow\Rightarrow \neg f g \neg h$.

(iii) Man beachte, dass $\mathcal{A}$ unendlich viele Axiome und Schlussregeln besitzt. Es handelt sich genau genommen um drei *Axiomenschemata*. In der Literatur finden sich verschiedene Versionen, die aber alle zu den gleichen Sätzen führen. Keines der drei Axiomenschemata ist entbehrlich (Aufgabe I.6). Tatsächlich kommt man aber mit nur einem (deutlich komplizierten) Axiomenschema von MEREDITH aus:

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

(iv) Um Beweisführungen zu vereinfachen, leiten wir weitere Schlussregeln ab. Für Aussagen f und g erhält man aus $(\mathcal{A}_1)$ und (MP) die Schlussregel

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

(v) Hat man Beweise für $f \Rightarrow g$ und $g \Rightarrow h$ gefunden, so erhält man einen Beweis für $f \Rightarrow h$:

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

Wir können also die Schlussregel *Modus barbara*

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

benutzen.

Beispiel I.1.8. Für jede Aussage f in $\mathcal{A}$ gilt

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

Definition I.1.9. Seien $f_1, \ldots, f_n$ Formeln eines Kalküls. Wir sagen, f_n kann *unter Annahme* von $f_1, \ldots, f_{n-1}$ bewiesen werden, falls ein Beweis für f_n existiert, in dem $f_1, \ldots, f_{n-1}$ als zusätzliche Axiome benutzt werden dürfen. Ggf. schreiben wir $f_1, \ldots, f_{n-1} \vdash f_n$. Dies verkürzt formale Beweise deutlich und entspricht dem praktischen Vorgehen in allen Teilen der Mathematik (sei $\epsilon > 0 \ldots$).

Lemma I.1.10 (Deduktionslemma)**.** *Für Aussagen $f_1, \ldots, f_{n+1}$ in $\mathcal{A}$ gilt $f_1, \ldots, f_n \vdash f_{n+1}$ genau dann, wenn $f_1, \ldots, f_{n-1} \vdash f_n \Rightarrow f_{n+1}$. Insbesondere ist $f_1 \vdash f_2$ äquivalent zu $\vdash f_1 \Rightarrow f_2$.*

Beweis. Hat man einen Beweis von $f_n \Rightarrow f_{n+1}$ unter Annahme von $f_1, \ldots, f_{n-1}$, so kann man f_n als Axiom hinzunehmen und f_{n+1} mit (MP) ableiten. Nehmen wir umgekehrt an, dass

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

ein Beweis von $f_{n+1} = g_m$ unter Annahme von $f_1, \ldots, f_n$ ist. Wir konstruieren daraus einen Beweis für $f_n \Rightarrow f_{n+1}$, in dem f_n nicht mehr als Axiom vorkommt. Konkret ersetzen wir der Reihe nach jedes g_i durch $f_n \Rightarrow g_i$. Dafür gibt es drei Fälle:

(i) Ist g_i ein Axiom oder eines der $f_1, \ldots, f_{n-1}$, so gilt

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

(ii) Ist $g_i = f_n$, so ersetzen wir g_i durch die nach Beispiel I.1.8 beweisbare Aussage $f_n \Rightarrow f_n$.

(iii) Sei nun g_i aus g_j und $g_j \Rightarrow g_i$ mit $j < i$ mittels (MP) abgeleitet. Wir wissen bereits, dass unser neuer Beweis die Zeilen $\vdash f_n \Rightarrow g_j$ und $\vdash f_n \Rightarrow (g_j \Rightarrow g_i)$ enthält. Wir können daher wie folgt argumentieren:

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

Am Ende erhält man $\vdash f_n \Rightarrow g_m$, d. h. $\vdash f_n \Rightarrow f_{n+1}$ wie gewünscht. Die zweite Aussage ist der Spezialfall $n = 1$. □[1]

Lemma I.1.11. *Für beliebige Aussagen f, g und h in $\mathcal{A}$ gilt:*

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

[1] Dieses Symbol kennzeichnet das Ende eines Beweises (auf der Metaebene).

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

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

Beweis.

(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. Interpretationen

Bemerkung I.2.1. Wir betrachten nun die Semantik von Kalkülen, d. h. wir geben Formeln eine Bedeutung.

Definition I.2.2. Eine *Interpretation* eines Kalküls $\mathcal{K}$ gibt den Formeln von $\mathcal{K}$ eine Bedeutung (z. B. könnte die Variable a für die natürliche Zahl 5 stehen).

Definition I.2.3.

- Die *Standard-Interpretation* der Aussagenlogik weist allen Elementaraussagen den Wert *wahr* (**w**) oder *falsch* (**f**) zu. Die Symbole (und) werden selbstverständlich als Klammern interpretiert. Die Symbole $\neg$ und $\Rightarrow$ stehen für *nicht* bzw. *impliziert*. Natürlich ist $\neg\mathbf{w} = \mathbf{f}$ und $\neg\mathbf{f} = \mathbf{w}$. Die Bedeutung von $\Rightarrow$ lässt sich durch eine *Wahrheitstabelle* präzisieren:

A	B	$A \Rightarrow B$
w	**w**	**w**
w	**f**	**f**
f	**w**	**w**
f	**f**	**w**

- Anstelle von „f impliziert g“ sagen wir auch: „aus f folgt g“ oder „wenn f gilt, dann auch g“. Man nennt $g \Rightarrow f$ die *Umkehrung* von $f \Rightarrow g$.

- Eine Aussage f, die für jede mögliche Belegung seiner Variablen stets wahr ist, nennt man eine *Tautologie*. Ggf. sagen wir f *gilt*[2] und schreiben $\vDash f$. Anderenfalls schreiben wir $\nvDash f$. Wir werden in Satz I.2.13 zeigen, dass die Tautologien genau die in $\mathcal{A}$ beweisbaren Sätze sind.

Bemerkung I.2.4.

(i) Die Idee, Aussagen durch möglichst wenige Axiome abzuleiten, geht auf Euklids Elemente zurück. Er hat darin beispielsweise den Satz des Pythagoras auf einfache Beziehungen zwischen Punkten und Geraden zurückgeführt. Erst viel später hat Hilbert die Axiome der euklidischen Geometrie von ihrer Interpretation gelöst und damit die Grundlage anderer Geometrien geschaffen.[3]

(ii) Um Aussagen übersichtlich darzustellen, führen wir folgende Abkürzungen ein:[4]

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

Die Interpretation ergibt sich wie folgt:

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

Daran kann man die Bedeutung leicht ablesen: $\wedge$, $\vee$, $\Leftrightarrow$ stehen für *und* (*Konjunktion*), *oder* (*Disjunktion*) bzw. *äquivalent*. Anstelle von „f ist äquivalent zu g“ sagen wir auch „f und g sind gleichwertig“ oder „f gilt genau dann, wenn g gilt“. Um Klammern einzusparen, vereinbaren wir, dass $\neg$ stärker bindet als $\wedge$ und $\vee$.

(iii) Man kann das Kalkül alternativ auch mit den Symbolen $\neg$ und $\vee$ (oder $\wedge$) definieren und anschließend $f \Rightarrow g := \neg f \vee g$ (bzw. $f \Rightarrow g := \neg(f \wedge \neg g)$) definieren. Tatsächlich kommt man mit nur einem Symbol (zuzüglich des Klammerpaars) aus:

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

(Aufgabe I.5).

(iv) Im Gegensatz zum alltäglichen Sprachgebrauch ist das mathematische *oder* nicht zum *entweder oder* gleichbedeutend. Das heißt, die Aussage $\mathbf{w} \vee \mathbf{w}$ ist wahr. In der Informatik benutzt man die Bezeichnung XOR für *entweder oder*. Man beachte außerdem, dass $\mathbf{f} \Rightarrow \mathbf{w}$ eine wahre Aussage ist (wenn die Voraussetzung nicht erfüllt ist, muss nichts geprüft werden). Beispiel: Wenn Kurt Gödel noch lebt, ist Gottlob Frege der Kaiser von China.

(v) Oft wird fälschlicherweise angenommen, dass mit einer Implikation auch deren Umkehrung gilt (das Phänomen heißt *Affirmation der Konsequenz*). Beispiel: Die besten Tischtennisspieler sind Chinesen $\not\Rightarrow$ Alle Chinesen sind gut in Tischtennis. Anstelle der fehlenden Kausalität kann aber eine *Korrelation* zwischen diese Aussagen bestehen (siehe Statistik).

[2] Diese Sprechweise haben wir bereits bei der Formulierung von Lemma I.1.11 benutzt.
[3] Siehe Skript zur Synthetischen Geometrie
[4] Das Symbol := auf der Metaebene besagt, dass die linke Seite durch die rechte definiert wird.

(vi) Man kann die Aussagenlogik auch arithmetisch interpretieren, indem man 1 statt **w** und 0 statt **f** benutzt. Man erhält dann $\neg A = 1 - A$, $A \Rightarrow B = \max(1 - A, B)$ (Maximum von $1 - A$ und B), $A \wedge B = \min(A, B) = A \cdot B$ (Minimum von A und B) und $A \vee B = \max(A, B)$. Man spricht in diesem Kontext von der *booleschen Algebra*.

(vii) In der *mehrwertigen* Logik erlaubt man neben **f** und **w** noch weitere Werte. In der *Fuzzylogik* lässt man sogar jede reelle Zahl zwischen 0 und 1 als „Wahrheitswert“ zu. Dies hat Anwendung in der Regelungstechnik und künstlichen Intelligenz.

(viii) Mit den folgenden Tautologien lassen sich Aussagen oft vereinfachen.

Satz I.2.5. *Für beliebige Aussagen f, g und h gilt*

(i) $\vDash \neg\neg f \Leftrightarrow f$ (*doppelte Negation*).

(ii) $\vDash f \vee \neg f$ (*Satz vom ausgeschlossenen Dritten*).

(iii) $\vDash \neg(f \wedge \neg f)$ (*Satz vom Widerspruch*).

(iv) $\vDash (f \wedge f) \Leftrightarrow f$ *und* $\vDash (f \vee f) \Leftrightarrow f$ (*Idempotenz*).

(v) $\vDash (f \Rightarrow g) \Leftrightarrow (\neg g \Rightarrow \neg f)$ (*Kontraposition*).

(vi) $\vDash (f \wedge g) \Leftrightarrow (g \wedge f)$, $\vDash (f \vee g) \Leftrightarrow (g \vee f)$ *und* $\vDash (f \Leftrightarrow g) \Leftrightarrow (g \Leftrightarrow f)$ (*Kommutativität*).

(vii) $\vDash ((f \wedge g) \wedge h) \Leftrightarrow (f \wedge (g \wedge h))$, $\vDash ((f \vee g) \vee h) \Leftrightarrow (f \vee (g \vee h))$, $\vDash ((f \Leftrightarrow g) \Leftrightarrow h) \Leftrightarrow (f \Leftrightarrow (g \Leftrightarrow h))$. (*Assoziativität*)

(viii) $\vDash (f \wedge (g \vee h)) \Leftrightarrow ((f \wedge g) \vee (f \wedge h))$, $\vDash (f \vee (g \wedge h)) \Leftrightarrow ((f \vee g) \wedge (f \vee h))$. (*Distributivität*)

(ix) $\vDash \neg(f \wedge g) \Leftrightarrow (\neg f \vee \neg g)$ *und* $\vDash \neg(f \vee g) \Leftrightarrow (\neg f \wedge \neg g)$ (De Morgan*sche Regeln*).

Beweis. Alle Aussagen lassen sich leicht durch Wahrheitstabellen verifizieren. □

Bemerkung I.2.6.

(i) Eine Abbildung f, die von Elementaraussagen $A_1, \ldots, A_n$ abhängt und den Wert **w** oder **f** annimmt, nennt man *boolesche Funktion*. Die Werte von f kann man mit einer Wahrheitstabelle auflisten, z. B.

A_1	A_2	A_3	f
w	**w**	**w**	**w**
w	**f**	**w**	**f**
f	**w**	**w**	**f**
f	**f**	**w**	**w**
w	**w**	**f**	**f**
w	**f**	**f**	**f**
f	**w**	**f**	**f**
f	**f**	**f**	**w**

Jede Zeile, für die f wahr ist, lässt sich durch eine wahre Aussage der Form $B_1 \wedge \ldots \wedge B_n$ beschreiben, wobei $B_i = A_i$ oder $B_i = \neg A_i$ für jedes i gilt. Verknüpft man diese Aussagen durch $\vee$, so erhält man eine zu f äquivalente Aussage. Im obigen Beispiel:

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

Dies lässt sich nach Satz I.2.5 vereinfachen zu

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

Durch Anwendung der doppelten Negation und der De Morganschen Regeln erhält man eine äquivalente Aussage der Form $(\ldots \vee \ldots \vee \ldots) \wedge (\ldots) \wedge$. Im Beispiel:

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

(ii) Das *Erfüllbarkeitsproblem* (engl. satisfiability, kurz SAT) beschäftigt sich mit der Frage, ob eine gegebene Aussage f bei geeigneter Belegung der Elementaraussagen wahr ist. Hängt f von n Elementaraussagen ab, so müssen dabei im schlechtesten Fall 2^n Fälle betrachtet werden. Das SAT-Problem gehört zur Komplexitätsklasse NP. Das bedeutet, dass der Wert von f für eine gegebene Belegung der Variablen in polynomialer Laufzeit (in n) bestimmt werden kann (zum Beispiel durch eine Rechnung in der booleschen Algebra). Das SAT-Problem ist sogar NP-vollständig (Satz von Cook), d. h. jedes weitere NP-Problem lässt sich in polynomialer Laufzeit auf SAT reduzieren. Eines der größten offenen Probleme der theoretischen Informatik ist, ob die Klassen NP und P übereinstimmen.[5] Findet man einen allgemeinen Algorithmus mit polynomialer Laufzeit, der bestimmt, ob ein beliebiges f erfüllbar ist, so hätte man P=NP bewiesen. Da dies als sehr unwahrscheinlich gilt, ist es wünschenswert, Aussagen auf der syntaktischen Ebene durch Axiome und Schlussregeln zu beweisen (abgesehen davon, dass Aussagen in mächtigeren Kalkülen von unendlich vielen Parametern abhängen können und dann ohnehin nicht mehr durch Wahrheitstabellen verifizierbar sind).

(iii) Im Folgenden nehmen wir an, dass die Symbole der Aussagenlogik und deren Standard-Interpretation in jedem Kalkül vorhanden sind.

Definition I.2.7. Ein Kalkül mit einer Interpretation heißt

- *konsistent* oder *widerspruchsfrei*, falls keine Formel f zusammen mit ihrer Negation bewiesen werden kann ($\nvdash f$ oder $\nvdash \neg f$).
- *negationsvollständig*, falls jede Formel f oder deren Negation bewiesen werden kann ($\vdash f$ oder $\vdash \neg f$).
- *korrekt*, wenn jeder Satz f wahr ist (aus $\vdash f$ folgt $\vDash f$)
- *vollständig*, wenn jede wahre Aussage f beweisbar ist (aus $\vDash f$ folgt $\vdash f$).

Bemerkung I.2.8.

(i) Die Konsistenz und Negationsvollständigkeit sind rein syntaktische Eigenschaften, die nicht von der Bedeutung des Symbols $\neg$ abhängen.

[5] Dies ist eines der sieben *Millennium-Probleme*, für deren Lösung jeweils eine Million Dollar ausgeschrieben sind, siehe `https://www.claymath.org/millennium-problems/`.

(ii) In einem inkonsistenten Kalkül lässt sich jede Aussage g beweisen:

$$\begin{aligned}
&\vdash f && \text{(gegeben aus Inkonsistenz)}\\
&\vdash \neg f && \text{(gegeben aus Inkonsistenz)}\\
&\vdash \neg f \Rightarrow (f \Rightarrow g) && \text{(Lemma I.1.11(v))}\\
&\vdash f \Rightarrow g && \text{(MP)}\\
&\vdash g && \text{(MP)}
\end{aligned}$$

Ein solches System kann nicht korrekt sein, denn sonst wären f und $\neg f$ wahr. Da die Mathematik nicht zuletzt als Grundlage der Naturwissenschaften dient, ist man primär an korrekten Systemen interessiert.

Satz I.2.9. *Die Aussagenlogik mit der Standard-Interpretation ist korrekt und konsistent, aber nicht negationsvollständig.*

Beweis. Für die Korrektheit zeigen wir zunächst, dass die drei Axiome des Kalküls Tautologien sind. Nehmen wir an, dass $(\mathcal{A}_1)$ für gewisse Aussagen f und g falsch ist. Dann muss f wahr sein und $g \Rightarrow f$ falsch. Dies geht aber nur, wenn f falsch ist. Dieser Widerspruch zeigt, dass $(\mathcal{A}_1)$ eine Tautologie ist. Ist $(\mathcal{A}_2)$ falsch, so gilt $\neg f \Rightarrow \neg g$ und $g \Rightarrow f$ ist falsch. Dies impliziert, dass g gilt, aber f nicht. Nun wäre aber $\neg f \Rightarrow \neg g$ falsch. Sei schließlich $(\mathcal{A}_3)$ falsch. Wir führen die Argumentation tabellarisch, wobei der Wert einer Aussage unter dem verbindenden $\Rightarrow$ steht:

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

Damit sind alle Axiome Tautologien. Sind f und $f \Rightarrow g$ wahr, so folgt aus der Interpretation von $\Rightarrow$, dass auch g wahr sein muss. Die Anwendung von (MP) produziert daher nur Tautologien. Dies zeigt die Korrektheit von $\mathcal{A}$. Nach Bemerkung I.2.8 ist $\mathcal{A}$ konsistent.

Da jede Elementaraussage A sowohl wahr als auch falsch sein kann, lässt sich weder A noch $\neg A$ beweisen. Damit kann $\mathcal{A}$ nicht negationsvollständig sein. □

Bemerkung I.2.10.

(i) Man beachte, dass ($\vDash A$ oder $\vDash B$) nicht äquivalent ist zu $\vDash A \vee B$ (wähle $B = \neg A$).

(ii) Um die Vollständigkeit der Aussagenlogik zu beweisen, werden folgende Lemmas benötigt.

Lemma I.2.11. *Seien $f_1, \ldots, f_{n+1}$ Aussagen in $\mathcal{A}$. Gilt $f_1, \ldots, f_n \vdash f_{n+1}$ und $f_1, \ldots, f_{n-1}, \neg f_n \vdash f_{n+1}$, so gilt auch $f_1, \ldots, f_{n-1} \vdash f_{n+1}$.*

[6] Widerspruch-Symbol

Beweis. Nach Lemma I.1.10 gilt

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

□

Lemma I.2.12 (Kalmár)**.** *Sei f eine aus Elementaraussagen $A_1, \dots, A_n$ konstruierte Aussage in $\mathcal{A}$. Seien $x_1, \dots, x_n$ beliebige Wahrheitswerte, d. h. $x_i = \boldsymbol{f}$ oder $x_i = \boldsymbol{w}$ für $i = 1, \dots, n$. Sei $A_i' := A_i$, falls $x_i = \boldsymbol{w}$ und $A_i' := \neg A_i$, falls $x_i = \boldsymbol{f}$ für $i = 1, \dots, n$. Ersetzt man jedes A_i durch x_i in f, so wird f wahr oder falsch. Im ersten Fall setzen wir $f' := f$ und im zweiten $f' := \neg f$. Dann gilt $A_1', \dots, A_n' \vdash f'$.*

Beweis. Wir können annehmen, dass f nur die Symbole (,), $\neg$ und $\Rightarrow$ enthält, d. h. keine Abkürzungen wie $\wedge$ oder $\vee$. Sei $m = m(f)$ die Gesamtzahl aller $\neg$ und $\Rightarrow$ in f. Im Fall $m(f) = 0$ ist $f = A_i$ für ein i. Dann ist $f' = A_i'$ und $A_1', \dots, A_n' \vdash f'$. Sei nun $m > 0$ und die Behauptung für alle Aussagen g mit $m(g) < m$ bereits bewiesen.

Fall 1: $f = \neg g$ mit $m(g) < m$.
Im Fall $f' = f$ ist $g' = \neg g = f = f'$ und $A_1', \dots, A_n' \vdash g'$ nach Induktion. Sei nun $f' = \neg f$. Dann ist $g' = g$. Aus Lemma I.1.11 folgt

$$
\begin{aligned}
A_1', \dots, A_n' &\vdash g \\
A_1', \dots, A_n' &\vdash g \Rightarrow \neg\neg g \\
A_1', \dots, A_n' &\vdash \neg\neg g
\end{aligned}
$$

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

Fall 2: $f = (g \Rightarrow h)$ mit $m(g), m(h) < m$.
Sei zunächst $g' = \neg g$. Dann ist $f' = f$. Nach Induktion gilt

$$
\begin{aligned}
A_1', \dots, A_n' &\vdash \neg g \\
A_1', \dots, A_n' &\vdash \neg g \Rightarrow (g \Rightarrow h) && \text{(Lemma I.1.11(v))} \\
A_1', \dots, A_n' &\vdash g \Rightarrow h
\end{aligned}
$$

Sei nun $g' = g$ und $h' = h$. Dann ist $f' = f$ und es gilt

$$
\begin{aligned}
A_1', \dots, A_n' &\vdash h \\
A_1', \dots, A_n' &\vdash h \Rightarrow (g \Rightarrow h) && (\mathcal{A}_1) \\
A_1', \dots, A_n' &\vdash g \Rightarrow h && \text{(MP)}
\end{aligned}
$$

Sei schließlich $g' = g$ und $h' = \neg h$. Dann ist $f' = \neg f = \neg(g \Rightarrow h)$ und

$$
\begin{aligned}
A_1', \dots, A_n' &\vdash g \\
A_1', \dots, A_n' &\vdash \neg h \\
A_1', \dots, A_n' &\vdash g \Rightarrow (\neg h \Rightarrow \neg(g \Rightarrow h)) && \text{(Lemma I.1.11(viii))} \\
A_1', \dots, A_n' &\vdash \neg h \Rightarrow \neg(g \Rightarrow h) && \text{(MP)} \\
A_1', \dots, A_n' &\vdash \neg(g \Rightarrow h) && \text{(MP)}
\end{aligned}
$$

□

Satz I.2.13. *Die Aussagenlogik mit der Standard-Interpretation ist vollständig.*

Beweis. Sei f eine aus den Elementaraussagen $A_1, \ldots, A_n$ konstruierte Tautologie. Für jede Belegung von $A_1, \ldots, A_n$ ist f wahr. Aus Lemma I.2.12 und Lemma I.2.11 folgt daher

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

□

Bemerkung I.2.14.

(i) Die in Satz I.2.5 gefunden Tautologien können nun wie Axiome im Kalkül benutzt werden. Aus der Assoziativität von $\wedge$, $\vee$ und $\Leftrightarrow$ folgt, dass die Aussagen $f \wedge g \wedge h$, $f \vee g \vee h$ und $f \Leftrightarrow g \Leftrightarrow h$ auch ohne Klammerung Sinn ergeben. Der Satz vom ausgeschlossenen Dritten erlaubt die indirekte Beweisführung durch Widerspruch: Wenn eine Aussage A zum Widerspruch geführt werden kann, muss $\neg A$ gelten.

(ii) Es gibt Situationen, in denen man $A \Rightarrow B$ und $\neg A \Rightarrow B$ beweisen kann. Ohne zu wissen, ob A gilt, kann man in jedem Fall die Gültigkeit von B ableiten (Lemma I.2.11). Man spricht ggf. von einem *nicht-konstruktiven* Beweis. Beispiel: Es gibt irrationale reelle Zahlen x, y, sodass x^y rational ist. Beweis: Bekanntlich ist $\sqrt{2}$ irrational (Satz II.8.14). Ist $\sqrt{2}^{\sqrt{2}}$ rational, so sind wir fertig. Anderenfalls ist $\sqrt{2}^{\sqrt{2}}$ irrational und

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

rational. Ohne zu wissen welcher Fall eintritt, haben wir die Behauptung bewiesen. Die von Brouwer entwickelte Theorie des *Intuitionismus* lehnt solche Beweise ab. Dafür muss ein Kalkül mit schwächeren Axiomen und Schlussregeln benutzt werden, in der der Satz von ausgeschlossenen Dritten unbeweisbar ist. Da in diesem Rahmen viele wichtige Sätze der Mathematik unbeweisbar bleiben, hat sich der Intuitionismus nie durchgesetzt.

(iii) Die Vollständigkeit der Aussagenlogik erlaubt es, Sätze durch mechanisches Ableiten im Kalkül zu verifizieren. Es ist jedoch keineswegs klar, wie man einen solchen Beweis findet (vgl. Beweis von Lemma I.1.11). Genau das macht im Allgemeinen aber den Reiz der Mathematik aus! Mit der Programmiersprache *Prolog* und dem Beweisassistenten *lean* lassen sich logische Ableitung mit dem Computer konstruieren.

I.3. Prädikatenlogik

Bemerkung I.3.1. In der Mathematik spricht man generell nur über Dinge, die man intrinsisch definieren kann (Fragen wie „gibt es einen Gott?“ gehören in die Philosophie). Da die Aussagenlogik offensichtlich viel zu primitiv ist, um einfache Sätze wie $1 + 1 = 2$ auszudrücken, werden wir unser Kalkül schrittweise erweitern. Zur Verbesserung der Lesbarkeit ersetzen wir gelegentlich die Metasprache durch primitive Symbole der Mengenlehre wie $\in$, $\subseteq$ oder $\cup$ (siehe Abschnitt II.1).

Definition I.3.2. Die *Prädikatenlogik* (*erster Stufe*) $\mathcal{P}^1 = \mathcal{P}$ ist ein Kalkül mit folgenden Eigenschaften:

- Alphabet: Variablen und Konstanten $(a, b, \ldots, 0, 1, \ldots)$, Funktionen $(\alpha, \beta, \ldots)$, Prädikate $(A, B, \ldots)$, Symbole $(,)$, $\neg$, $\Rightarrow$, $\forall$ (*Allquantor*). Funktionen und Prädikate hängen von einer endlichen Anzahl an Parametern (auch Argumente genannt) ab. Hängt α bzw. A von $x_1, \ldots, x_n$ ab, so nennt man α bzw. A *n-stellig* und schreibt $\alpha(x_1, \ldots, x_n)$ bzw. $A(x_1, \ldots, x_n)$. Wir nehmen aus technischen Gründen stets an, dass das Alphabet abzählbar ist (siehe Bemerkung II.6.4).
- Als Vorstufe von Formeln definiert *Terme* rekursiv: Variablen und Konstanten sind Terme. Sind $t_1, \ldots, t_n$ Terme und φ eine n-stellige Funktion, so ist auch $\varphi(t_1, \ldots, t_n)$ ein Term.
- Formeln: Sind $t_1, \ldots, t_n$ Terme und P ein n-stelliges Prädikat, so ist $P(t_1, \ldots, t_n)$ eine Formel. Sind f und g Formeln und x eine Variable, so sind auch $(\neg f)$, $(f \Rightarrow g)$ und $(\forall x f)$ Formeln. Dabei ist nicht gefordert, dass x in f vorkommt.
- Wir definieren rekursiv, wann eine Variable x *frei* in einer Formel f vorkommt: Ist f ein Term oder von der Form $P(t_1, \ldots, t_n)$, so ist x frei. Ist x frei in f, so auch in $\neg f$ und in $\forall y f$, wobei y von x verschieden ist. Das Vorkommen von x in $\forall x f$ hingegen nennt man *gebunden*. Hat f die Form $g \Rightarrow h$ und kommt x frei in g oder h vor, so ist x auch frei in f (x kann sowohl frei als auch gebunden in f vorkommen). In f frei vorkommenden Variablen gibt man oft wie bei Funktionen als Argumente an: $f(x_1, \ldots, x_n)$. Eine Formel, in der keine Variable frei vorkommt, nennt man *geschlossen*. Terme ohne Variablen (also Konstruktionen aus Konstanten und Funktionen) nennt man ebenfalls *geschlossen* (Terme enthalten generell keine Allquantoren).
- Man kann jedes freie Vorkommen einer Variable x in einer Formel f durch einen Term t ersetzen. Dafür schreiben wir $f(x \leftarrow t)$ oder kurz $f(t)$, falls Missverständnisse ausgeschlossen sind.[7] Wir setzen dabei stets voraus, dass die Ersetzung *kollisionsfrei* erfolgt, d. h. das keine Variable aus t in f gebunden wird (dies lässt sich oft durch geeignete Umbenennung der Variablen erreichen).
- Axiome: Für alle Formeln f, g, h gelten die Axiome $(\mathcal{A}_1)$, $(\mathcal{A}_2)$ und $(\mathcal{A}_3)$ der Aussagenlogik. Für alle Variablen x und alle Terme t gelten zusätzlich:

$$((\forall x(f \Rightarrow g)) \Rightarrow (f \Rightarrow (\forall x g))) \qquad \text{falls } x \text{ nicht frei in } f \text{ vorkommt} \qquad (\mathcal{P}_1)$$
$$(\forall x f) \Rightarrow (f(x \leftarrow t)) \qquad \text{falls kollisionsfrei} \qquad (\mathcal{P}_2)$$

- Schlussregeln: Modus ponens (MP) und die *Generalisierung*

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

  für jede Formel f und jede Variable x.

Wie in jedem Kalkül definiert man Beweise (unter Annahmen) und $\vdash$.

Beispiel I.3.3. Sei σ eine 1-stellige Funktion und P ein 2-stelliges Prädikat in $\mathcal{P}$. Dann ist

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

eine Formel, in der x nur gebunden und y sowohl frei als auch gebunden auftritt. Ist z eine weitere Variable, so ist

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

eine kollisionsfreie Ersetzung. Die Ersetzung $f(y \leftarrow x)$ wäre jedoch nicht kollisionsfrei.

[7] Das neue Symbol $\leftarrow$ wird hier lediglich als Abkürzung benutzt, um die tatsächliche Ersetzung von x nicht ausschreiben zu müssen.

Bemerkung I.3.4.

(i) Die Symbole $\wedge$, $\vee$ und $\Leftrightarrow$ werden wie üblich als Abkürzungen verwendet. Ergänzend zu den Klammerkonventionen aus Bemerkung I.2.4 vereinbaren wir, dass $\forall$ stärker bindet als $\Rightarrow$ und $\Leftrightarrow$, aber nicht stärker als die übrigen Symbole. Daher steht $\forall x f \Rightarrow g$ für $(\forall x f) \Rightarrow g$.

(ii) Aus der Abzählbarkeit des Alphabets folgt, dass sich alle Formeln in $\mathcal{P}$ abzählen lassen (siehe Beispiel II.6.5). Auf die Konstanten kann man verzichten, wenn man stattdessen 0-stellige Funktionen zulässt.

(iii) Viele der Ergebnisse aus Abschnitt I.1, insbesondere die Schlussregeln (MP') und (MP), bleiben auch in $\mathcal{P}$ gültig. Wegen der neuen Regel (G) gilt das Deduktionslemma im Allgemeinen jedoch nur für geschlossene Formeln (Aufgabe I.10). Da im Beweis von Lemma I.1.11 (G) aber nicht zur Verfügung stand, gilt Lemma I.1.11 uneingeschränkt für Formeln in $\mathcal{P}$ (vgl. Aufgabe I.11).

(iv) Als Ersatz für das Deduktionslemma führen wir die *Deduktion* als neue Schlussregel ein:

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

Sie ist gültig, denn

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

(v) Aus der Kombination von $(\mathcal{P}_2)$ und (G) erhält die *Spezialisierung* als neue Schlussregel

$$\frac{f}{f(x \leftarrow t)} \qquad \text{falls kollisionsfrei.} \tag{S}$$

Dies gilt insbesondere, wenn t geschlossen ist oder f keine Allquantoren enthält. Außerdem gilt

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

denn die „Ersetzung“ $x \leftarrow x$ ist stets kollisionsfrei (nur freie Vorkommen von x werden „ersetzt“). Kommt x nicht frei in f vor, so lässt sich auch die Umkehrung beweisen:

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

Nach den Schlussregeln ist $\vdash f$ im Allgemeinen äquivalent zu $\vdash \forall x f$ (auch wenn x frei in f vorkommt). Durch Anfügen weiterer Allquantoren (für jede freie Variable in f) kann man auf diese Weise f in eine geschlossene Formel umwandeln.

(vi) Werden mehrere Variablen einer Formel ersetzt, so ist die Reihenfolge zu beachten. Um Kollisionen zu vermeiden, kann man neue Variablen kreieren und sie als Zwischenspeicher verwenden:

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

(vii) Nimmt man weitere Axiome hinzu, so spricht man allgemein von einem Kalkül *erster Stufe*.

Definition I.3.5.

(i) Eine *Interpretation* von $\mathcal{P}$ besteht aus einer Menge U (*Universum*) und einer Abbildung I. Jede Konstante c wird als Element in U interpretiert, d. h. $I(c) \in U$. Variablen repräsentieren ebenfalls Elemente in U, aber werden keinem festen Wert zugewiesen. Die Symbole (,), $\neg$, $\Rightarrow$, $\wedge$, $\vee$ und $\Leftrightarrow$ haben die gleiche Bedeutung wie in der Standard-Interpretation der Aussagenlogik. Das neue Symbol $\forall$ bedeutet *für alle* (siehe (iii)).

(ii) Jede n-stellige Funktion φ von $\mathcal{P}$ wird als „gewöhnliche“ Abbildung $I(\varphi)\colon U^n \to U$ interpretiert.[8] Für einen geschlossenen Term t gilt daher $I(t) \in U$. Prädikate sind Eigenschaften oder Beziehungen, die für ihre Parameter gelten oder nicht gelten (ein n-stelliges Prädikat entspricht formal einer Relation, d. h. einer Teilmenge von U^n, siehe Definition II.2.1).

(iii) Eine Formel der Form $P(t_1, \ldots, t_n)$ wird als wahr interpretiert, wenn $t_1, \ldots, t_n$ bzgl. $I(P)$ in Relation stehen. Enthalten die t_i Variablen, so muss die Relation allgemein für jede Belegung dieser Variablen gültig sein. Eine Formel der Form $\forall x f$ ist genau dann wahr, wenn $I(f) = \mathbf{w}$ für jede Belegung von x in U gilt.

(iv) Gilt $I(f)$, so nennt man (U, I) ein *Modell* für f und schreibt $\vDash_{(U,I)} f$. Analog ist (U, I) ein Modell für eine Menge M von Formeln, wenn $I(f)$ für jedes f in M gilt. Ist jede Interpretation von $\mathcal{P}$ ein Modell für f, so nennt man f eine *Tautologie* und schreibt (wie bisher) $\vDash f$ (in der Aussagenlogik haben wir dafür jedoch nur die Standard-Interpretation berücksichtigt). Ist (U, I) ein Modell für jeden Satz in $\mathcal{P}$, so nennt man (U, I) ein *Modell* für $\mathcal{P}$.

Bemerkung I.3.6.

(i) Wie auf der syntaktischen Ebene (Bemerkung I.3.4) sind $\vDash_{(U,I)} f$ und $\vDash_{(U,I)} \forall x f$ für jede Formel f äquivalent. Daher ist (I, U) bereits dann ein Modell für eine Menge M von Formeln, wenn $I(f) = \mathbf{w}$ für jede geschlossene Formel f in M gilt.

(ii) Für geschlossene Formeln f ist f oder $\neg f$ bzgl. einer festen Interpretation wahr. Besitzt f jedoch freie Variablen, so können f und $\neg f$ beide falsch sein (z. B. $f := P(x)$ für ein Prädikat, das für manche x gilt und für andere nicht). In diesem Sinn kann die Prädikatenlogik nicht negationsvollständig sein. Selbst wenn f geschlossen ist, muss weder f noch $\neg f$ eine Tautologie sein, denn f könnte in einer Interpretation falsch sein, während $\neg f$ in einer anderen Interpretation falsch ist.

(iii) Formeln der Bauart $\forall x(f \Rightarrow \forall x g)$ sind zwar zugelassen, aber irreführend, da der äußere Allquantor keine Wirkung auf g hat. In solchen Fällen ist es hilfreich g durch $g(x \leftarrow y)$ zu ersetzen und $\forall x(f \Rightarrow \forall y g)$ zu verwenden.

(iv) Neben dem Allquantor führt man als Abkürzung den *Existenzquantor* $\exists$ als neues Symbol mit der Interpretation *es existiert* ein:

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

Die Formel entspricht der De Morganschen Regel in einem beliebigen Universum (Es existiert ein x mit $f(x)$ genau dann, wenn nicht für alle x die $f(x)$ falsch ist.) Für jeden geschlossenen Term t

[8] Genaue Definition in Abschnitt II.3.

gilt

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

Satz I.3.7. *Jede beweisbare Formel in $\mathcal{P}$ ist eine Tautologie.*

Beweis. Die Axiome $(\mathcal{A}_1)$, $(\mathcal{A}_2)$ und $(\mathcal{A}_3)$ sind Tautologien, da wir die Standard-Interpretation von $\mathcal{A}$ voraussetzen. Seien f und g Formeln, sodass x nicht frei in f vorkommt. Um die Gültigkeit von $(\mathcal{P}_1)$ zu verifizieren, können wir nach Satz I.2.5 $\vDash_{(U,I)} \forall x(f \Rightarrow g)$ für eine beliebige Interpretation (I, U) annehmen. Ist $I(f) = \mathbf{f}$, so wird $(\mathcal{P}_1)$ insgesamt wahr. Sei also $I(f) = \mathbf{w}$. Da x nicht frei in f vorkommt, gilt $f(x)$ für alle x in U. Andererseits gilt auch $f(x) \Rightarrow g(x)$ für alle x. Mit (MP) folgt $\vDash_{(U,I)} \forall x g$. Damit ist $(\mathcal{P}_1)$ eine Tautologie. Ist f für alle x bzgl. (I, U) wahr, so auch für $x = t$ für einen speziellen Term t, sofern die Ersetzung kollisionsfrei ist. Dies zeigt, dass auch $(\mathcal{P}_2)$ eine Tautologie ist.

Wie in $\mathcal{A}$ liefert (MP) nur Tautologien. Ist f eine Tautologie, so ist f für jede mögliche Interpretation der Variablen eine wahre Aussage. Insbesondere ist $\forall x f$ eine Tautologie. Dies bestätigt die Gültigkeit von (G). □

Beispiel I.3.8.

(i) Sei $\mathcal{N}$ ein Kalkül erster Stufe mit der Konstanten 0, einer 1-stelligen Funktion σ und einem 2-stelligen Prädikat G. Als neue Axiome ergänzen wir:

$$\begin{aligned}
&\vdash \forall x G(x, \sigma(x))\\
&\vdash \neg\exists x G(x, 0)
\end{aligned}$$

Eine naheliegende Interpretation I erhält man mit dem Universum der natürlichen Zahlen $U = \{0, 1, \ldots\}$,[9] der Nachfolgerfunktion $I(\sigma)(x) := x + 1$ und der Größer-Relation $I(G)(x, y) \Leftrightarrow x < y$. Die Axiome besagen, dass jede Zahl kleiner als ihr Nachfolger ist und keine Zahl kleiner als 0 ist. Also ist (U, I) ein Model für $\mathcal{N}$. Damit ist keinesfalls klar, dass man alle bekannten Eigenschaften von G und σ in $\mathcal{N}$ beweisen kann. So ist zum Beispiel auch (U', I') mit $U' = \{0, 1\}$, $I'(\sigma)(0) = I'(\sigma)(1) = 1$ und $I'(G)(x, y) \Leftrightarrow y = 1$ ein Modell für $\mathcal{N}$. Die in (I, U) gültige Formel

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

wird in (I', U') falsch. Sie kann also nicht in $\mathcal{N}$ bewiesen werden.

(ii) Ein klassisches Beispiel für die Verwendung der Quantoren ist die Stetigkeit einer reellen Funktion f an einem Punkt x_0. Als Universum dient die Menge der reellen Zahlen.[10] Anstelle der üblichen Variablen ϵ und δ verwenden wir nach unserer Konvention die lateinischen Buchstaben e und d. Neben der in (i) eingeführten Konstante 0 und der Größer-Relation G braucht man die 2-stellige Abstandsfunktion δ mit der Interpretation $I(\delta)(x, y) = |x - y|$. Damit erhält man folgende Formel:

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

[9] Die natürlichen Zahlen werden formal in Beispiel II.5.11 definiert.
[10] Definiert in Definition II.8.6.

(iii) In einem Kalkül erster Stufe lässt sich die Gleichheitsrelation $=$ nicht vollständig ausdrücken. Angenommen es gibt ein Prädikat P mit geeigneten Axiomen, sodass bzgl. einer Interpretation (U, I) die Aussage $P(x, y)$ für alle x, y in U genau dann wahr ist, wenn $x = y$ gilt. Man kann jetzt das Universum U vergrößern, indem man zu jedem u in U eine „Kopie“ u' in einem „Paralleluniversum“ hinzunimmt. Jede Variable in einer Formel f kann wahlweise als u oder u' interpretiert werden, ohne die Gültigkeit von f zu verändern. In dieser neuen Interpretation hat P nicht mehr die gewünschte Eigenschaft, denn $P(u, u')$ ist wahr. Es kann also keine Tautologie geben, die P mit der Gleichheitsrelation verknüpft.

Definition I.3.9. In der *Prädikatenlogik mit Gleichheit* $\mathcal{P}^=$ ergänzt man $\mathcal{P}$ um das Symbol $=$, welches als Gleichheitszeichen interpretiert wird. Sind s und t Terme, so sei $s = t$ eine Formel. Für jede Formel f und alle Variablen x und y ergänzen wir die folgenden Axiome:

$$x = x \qquad (\mathcal{P}_1^=)$$
$$(x = y) \Rightarrow (f(y \leftarrow x) \Rightarrow f) \qquad \text{falls kollisionsfrei} \qquad (\mathcal{P}_2^=)$$

Bemerkung I.3.10.

(i) Wir vereinbaren, dass $=$ stärker bindet als $\Rightarrow$. Statt $\neg(x = y)$ schreibt man $x \neq y$.

(ii) In jeder Interpretation ist offensichtlich $x = x$ wahr, d. h. $(\mathcal{P}_1^=)$ ist eine Tautologie. Axiom $(\mathcal{P}_2^=)$ garantiert, dass man Variablen in Formeln durch gleiche Variablen ersetzen kann. Auch dies ist eine Tautologie. Somit überträgt sich Satz I.3.7 auf $\mathcal{P}^=$.

(iii) Mit dem Gleichheitszeichen lässt sich ausdrücken, dass *genau* ein Element mit einer bestimmten Eigenschaft existiert. Dafür benutzt man oft folgende Abkürzung:

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

Beispiel I.3.11. Die Prädikatenlogik mit Gleichheit ist geeignet, um mathematische Gruppen zu definieren. Sei dafür e eine Konstante (für das neutrale Element) und σ eine 2-stellige Funktion (für die Gruppenverknüpfung). Wir erweitern $\mathcal{P}^=$ um die folgenden Axiome:

$$\vdash \sigma(\sigma(x, y), z) = \sigma(x, \sigma(y, z)) \qquad \text{(Assoziativität)}$$
$$\vdash \sigma(x, e) = x \qquad \text{(Neultralität)}$$
$$\vdash \exists y(\sigma(x, y) = e) \qquad \text{(Existenz inverser Elemente)}$$

Sei $\mathcal{G}$ das entstandene Kalkül. Bekanntlich gilt in jeder Gruppe auch die Neutralität von links, d. h. $\sigma(e, x) = x$ ist eine Tautologie.[11] Aus Gödels Vollständigkeitssatz I.4.6 wird folgen, dass $\sigma(e, x) = x$ ein Satz in $\mathcal{G}$ ist. Andererseits ist $\nvdash \sigma(x, y) = \sigma(y, x)$, da nicht jede Gruppe abelsch ist.

Lemma I.3.12. *Für alle Terme t, u, v in $\mathcal{P}^=$ gilt:*

(i) $\vdash t = t$.

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

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

[11] Siehe Gruppentheorie-Skript

Beweis. Da in den Formeln keine Quantoren vorkommen, können wir nach (S) annehmen, dass t, u und v Variablen sind. Nun ist (i) gleich $(\mathcal{P}_1^=)$.

(ii)

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

Aus Symmetriegründen gilt auch $\vdash t = u \Rightarrow u = t$. Die Behauptung folgt aus Aufgabe I.4.

(iii)

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

□

Lemma I.3.13. *Seien $t_1, \ldots, t_n, u_1, \ldots, u_n$ Terme, σ eine n-stellige Funktion und P ein n-stelliges Prädikat in $\mathcal{P}^=$. Dann gilt*

(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) Aus $\vdash t_i = u_i$ *für* $i = 1, \ldots, n$ *folgt* $\vdash P(t_1, \ldots, t_n) \Leftrightarrow P(u_1, \ldots, u_n)$.

Beweis. Da keine Quantoren vorkommen, können wir annehmen, dass $t_1, \ldots, t_n, u_1, \ldots, u_n$ Variablen sind.

(i) Sei $f_k(u_k, \ldots, u_n) := (t_k = u_k \Rightarrow \ldots \Rightarrow (t_n = u_n \Rightarrow \varphi(t_1, \ldots, t_n) = \varphi(t_1, \ldots, t_{k-1}, u_k, \ldots, u_n)) \ldots)$ für $k = 1, \ldots, n$. Wegen

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

gilt $\vdash f_n$. Sei bereits f_{k+1} bewiesen. Dann gilt

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

Schließlich gilt $\vdash f_1$.

(ii) Es gilt

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

Aus Symmetriegründen gilt auch $\vdash P(u_1, \ldots, u_n) \Rightarrow P(t_1, \ldots, t_n)$. Die Behauptung folgt aus Aufgabe I.4. □

I.4. Der Modellexistenzsatz

Bemerkung I.4.1. Wir hatten bisher die Konsistenz eines Kalküls durch Angabe eines Modells bewiesen. Wir zeigen in diesem Abschnitt, dass dies für Kalküle der ersten Stufe stets möglich ist.

Definition I.4.2.

- Sei M eine Menge von Formeln in einem Kalkül $\mathcal{K}$ erster Stufe mit Gleichheit. Wir nennen M *konsistent*, falls keine Formel f mit $M \vdash f$ und $M \vdash \neg f$ existiert. Dies bedeutet, dass man ein konsistentes Kalkül erhält, wenn man die Formeln in M als Axiome zu $\mathcal{K}$ hinzufügt (dafür muss $\mathcal{K}$ selbst konsistent sein).
- Eine konsistente Menge M von Formeln heißt *abgeschlossen*, falls für jede Formel f in $\mathcal{K}$ gilt:
  (i) $\vdash f$ oder $\vdash \neg f$.
  (ii) Ist $\neg\forall x f \in M$, so existiert ein geschlossener Term t mit $\neg f(x \leftarrow t) \in M$.

Lemma I.4.3. *Sei M eine abgeschlossene Menge von Formeln in einem Kalkül $\mathcal{K}$ erster Stufe mit Gleichheit. Sei x eine Variable und f, g Formeln in $\mathcal{K}$. Dann gilt*

(i) Aus $M \vdash f$ folgt $f \in M$.

(ii) Genau dann liegt $f \Rightarrow g$ in M, wenn $\neg f$ oder g in M liegen.

(iii) Genau dann liegt $\forall x f$ in M, wenn $f(x \leftarrow t)$ für jeden geschlossenen Term t in M liegt.

Beweis.

(i) Da M konsistent ist, gilt $M \nvdash \neg f$ und $\neg f$ kann nicht in M liegen. Nach Definition ist $f \in M$.

(ii) Sei $f \Rightarrow g \in M$. Nehmen wir an, dass weder $\neg f$ noch g in M liegen. Dann ist $f, \neg g \in M$ und M wäre inkonsistent:

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

Ist umgekehrt $\neg f \in M$, so gilt

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

Ist $g \in M$, so gilt

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

(iii) Liegt $\forall x f$ in M, so folgt $M \vdash f(t)$ für alle geschlossenen Terme t nach (S). Nach (i) ist $f(t) \in M$ für alle t. Liegt umgekehrt $\forall x f$ nicht in M, so gilt $\neg\forall x f \in M$. Nach Definition existiert ein geschlossener Term t mit $\neg f(t) \in M$, d. h. $f(t)$ liegt nicht in M. □

Lemma I.4.4. *Sei M eine konsistente Menge von Formeln in einem Kalkül $\mathcal{K}$ erster Stufe mit Gleichheit. Dann existiert eine Menge von Formeln $\hat{M}$ in einem Kalkül $\hat{\mathcal{K}}$ erster Stufe mit folgenden Eigenschaften:*

(i) $\hat{\mathcal{K}}$ unterscheidet sich von $\mathcal{K}$ nur durch ein größeres Alphabet.

(ii) $\hat{M}$ enthält M.

(iii) $\hat{M}$ ist abgeschlossen.

Beweis. Wir erhalten $\hat{\mathcal{K}}$ aus $\mathcal{K}$, indem wir neue Konstanten $c_1, c_2, \ldots$ hinzufügen, die noch nicht in $\mathcal{K}$ vorhanden sind. Nach Bemerkung I.3.4 lassen sich die geschlossenen Formeln in $\hat{\mathcal{K}}$ aufzählen: $f_1, f_2, \ldots$. Wir definieren induktiv Formelmengen $M_0, M_1, \ldots$ mit folgenden Eigenschaften:

(a) M_i ist konsistent.

(b) M_{i+1} enthält M_i.

(c) M_i enthält nur endlich viele der c_i.

Offenbar erfüllt $M_0 := M$ diese Eigenschaften. Sei M_i bereits definiert. Wird M_i durch Hinzunahme von f_i inkonsistent, so sei $M_{i+1} := M_i$. Wir nehmen nun an, dass M_i durch Hinzunahme von f_i konsistent ist. Hat f_i nicht die Form $\neg\forall x g$, so erfüllt $M_{i+1} := M_i \cup \{f_i\}$ die Eigenschaften (a)–(c). Sei schließlich $f_i = \neg\forall x g$. Wegen c existiert ein c_j, das weder in M_i noch in f_i vorkommt. Wir setzen $M_{i+1} := M_i \cup \{f_i, \neg g(x \leftarrow c_j)\}$. Angenommen M_{i+1} ist inkonsistent. Da $g(c_j)$ geschlossen ist, darf man das Deduktionslemma anwenden (Aufgabe I.10). Es gilt

$$
\begin{aligned}
&M_i, f_i, \neg g(c_j) \vdash g(c_j) && \\
&\quad M_i, f_i \vdash \neg g(c_j) \Rightarrow g(c_j) && \text{(Lemma I.1.10)} \\
&\quad M_i, f_i \vdash (\neg g(c_j) \Rightarrow g(c_j)) \Rightarrow g(c_j) && \text{(Lemma I.1.11(xi))} \\
&\quad M_i, f_i \vdash g(c_j) && \text{(MP)} \\
&\quad M_i, f_i \vdash \neg\forall x g && \\
&\quad M_i, f_i \vdash \neg g(c_j) && (\mathcal{P}_2^=)
\end{aligned}
$$

Dann wäre aber $M_i \cup \{f_i\}$ inkonsistent. Also muss (a) (und trivialerweise auch (b), (c)) gelten.

Wir zeigen nun, dass $\hat{M} := \bigcup_{i \geq 0} M_i$ abgeschlossen ist. Angenommen $\hat{M}$ ist inkonsistent. Dann könnte man eine widersprüchliche Formel wie $f \wedge \neg f$ aus $\hat{M}$ ableiten. Ein entsprechender Beweis besteht aus nur endlich vielen Formeln, die Axiome sind oder in einem M_i liegen. Dann wäre aber M_i inkonsistent im Widerspruch zu (a). Nehmen wir jetzt an, es gibt eine Formel f in $\hat{\mathcal{K}}$ mit $\hat{M} \nvdash f$ und $\hat{M} \nvdash \neg f$. Nach Bemerkung I.3.6 dürfen wir annehmen, dass f geschlossen ist. Dann existieren i und j mit $f_i = f$ und $f_j = \neg f$. Da f_i nicht in M_{i+1} liegen kann, gilt $M_{i+1} = M_i$ nach Konstruktion. Dies impliziert, dass $M_i \cup \{f\}$ inkonsistent ist. Analog ist auch $M_j \cup \{\neg f\}$ inkonsistent. Es folgt $\hat{M} \vdash f$ und $\hat{M} \vdash \neg f$ im Widerspruch zur Konsistenz von $\hat{M}$. Sei schließlich $f_i := \neg\forall x g$ in $\hat{M}$. Nach Konstruktion ist $M_{i+1} = M_i \cup \{f_i, \neg g(c_j)\}$ für ein j. Insbesondere ist $\neg g(c_f)$ in $\hat{M}$. Damit ist $\hat{M}$ abgeschlossen. □

Satz I.4.5 (Modellexistenzsatz)**.** *Jede konsistente Menge M von Formeln in einem Kalkül $\mathcal{K}$ erster Stufe mit Gleichheit besitzt ein Modell. Insbesondere besitzt jedes konsistente Kalkül erster Stufe ein Modell.*

Beweis (Henkin). Nach Lemma I.4.4 lässt sich M zu einer abgeschlossenen Menge $\hat{M}$ in einem größeren Kalkül $\hat{\mathcal{K}}$ erweitern. Da man ein Modell für $\hat{M}$ auf $\mathcal{K}$ einschränken kann, können wir $\mathcal{K} = \hat{\mathcal{K}}$ und $M = \hat{M}$ annehmen. Für Terme t und u sei $u \sim t$ genau dann, wenn $M \vdash t = u$. Nach Lemma I.3.12 ist $\sim$ eine Äquivalenzrelation. Die Äquivalenzklasse von t bezeichnen wir mit $[t]$. Als Universum U wählen wir die Menge der Äquivalenzklassen $[t]$ für alle geschlossenen Terme t.[12] Für Konstanten c in $\mathcal{K}$ sei $I(c) := [c] \in U$. Variablen stehen für nicht weiter spezifizierte Äquivalenzklassen $[t]$. Für eine n-stellige Funktion φ und $[t_1], \ldots, [t_n] \in U$ sei

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

Dies ist nach Lemma I.3.13 wohldefiniert, d. h. die Definition hängt nicht von der Wahl der Repräsentanten von $[t_i]$ ab. Für ein n-stelliges Prädikat P sei $I(P)([t_1], \ldots, [t_n]) := \mathbf{w}$ genau dann, wenn $P(t_1, \ldots, t_n) \in M$. Dies ist ebenfalls wohldefiniert nach Lemma I.3.13.

Nach Bemerkung I.3.6 genügt es zu zeigen, dass eine geschlossene Formel f genau dann in M liegt, wenn $I(f) = \mathbf{w}$ gilt. Wie im Beweis von Lemma I.2.12 argumentieren wir nach der Anzahl der Symbole $\neg$, $\Rightarrow$ und $\forall$ in f. Angenommen f hat die Form $t = u$ für geschlossene Terme t und u. Dann gilt nach Definition $f \in M$ genau dann, wenn $[t] = [u]$. Also ist $f \in M$ genau dann, wenn $I(f) = \mathbf{w}$. Hat f die Form $P(t_1, \ldots, t_n)$, so gilt $[t_1], \ldots, [t_n] \in U$ und die Behauptung folgt aus der Definition von I. Sei als Nächstes f gleich $\neg g$ für eine geschlossene Formel g. Im Fall $f \in M$ ist $g \notin M$, da M konsistent ist. Nach Induktion ist $I(g) = \mathbf{f}$, d. h. $I(f) = I(\neg g) = \mathbf{w}$. Ist umgekehrt $I(f) = \mathbf{w}$, so folgt $g \notin M$. Da M abgeschlossen ist, gilt $f \in M$. Sei jetzt f gleich $g \Rightarrow h$ für geschlossene Formeln g und h. Im Fall $f \in M$ ist $\neg g \in M$ oder $h \in M$ nach Lemma I.4.3. Nach Induktion ist $I(\neg g) = \mathbf{w}$ oder $I(h) = \mathbf{w}$. Aus Satz I.2.5 folgt $I(f) = I(\neg g \vee h) = \mathbf{w}$. Sei umgekehrt $I(f) = \mathbf{w}$. Da g und h geschlossen sind, folgt $I(\neg g) = \mathbf{w}$ oder $I(h) = \mathbf{w}$. Nach Lemma I.4.3 ist $f \in M$.

Schließlich sei $f = \forall x g$. Im Fall $f \in M$ ist $g(t) \in M$ für jeden geschlossenen Term nach $(\mathcal{P}_2)$. Da U aus den (Äquivalenzklassen der) geschlossenen Termen besteht, ist $I(f) = \mathbf{w}$. Ist umgekehrt $I(f) = \mathbf{w}$, so ist $g(t)$ für jeden geschlossenen Term t wahr. Nach Induktion folgt $g(t) \in M$ für alle t. Aus Lemma I.4.3 erhält man $f \in M$.

Die zweite Behauptung folgt aus der ersten, indem man für M die Menge aller Sätze von $\mathcal{K}$ wählt. □

Satz I.4.6 (Gödels Vollständigkeitssatz)**.** *Jede Tautologie in $\mathcal{P}^=$ ist beweisbar.*

Beweis. Nehmen wir an, es gibt eine nicht-beweisbare Tautologie f in $\mathcal{P}^=$. O. B. d. A. sei f geschlossen. Durch Hinzunahme des Axioms $\neg f$ erhält man das Kalkül $\mathcal{K}$. Nehmen wir an, dass $\mathcal{K}$ inkonsistent ist. Nach Bemerkung I.2.8 lässt sich f in $\mathcal{K}$ beweisen. Bezogen auf $\mathcal{P}^=$ bedeutet das

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

Dieser Widerspruch zeigt, dass $\mathcal{K}$ konsistent ist. Nach dem Modellexistenzsatz existiert ein Modell für $\mathcal{K}$, in dem $\neg f$ wahr und f falsch ist. Dann kann f aber keine Tautologie sein. Also ist $\mathcal{P}^=$ vollständig. □

[12] Man benötigt das Auswahlaxiom, um zu zeigen, dass U wirklich eine Menge ist, siehe Lemma II.2.3.

Bemerkung I.4.7. Achtung: Der Vollständigkeitssatz besagt nicht, dass $\mathcal{P}^=$ bezüglich jeder Interpretation vollständig ist (vgl. Satz I.7.6).

Satz I.4.8 (Kompaktheitssatz[13])**.** *Eine Menge M von Formeln in einem Kalkül erster Stufe mit Gleichheit besitzt ein Modell, wenn jede endliche Teilmenge von M ein Modell besitzt.*

Beweis. Besitzt M kein Modell, so ist M inkonsistent nach dem Modellexistenzsatz. Ein Widerspruch mit Axiomen aus M lässt sich bereits aus endlich vielen solchen Axiomen herleiten. Daher kann auch eine gewisse endliche Teilmenge von M kein Modell besitzen. Widerspruch. □

Folgerung I.4.9. *In $\mathcal{P}^=$ lässt sich nicht ausdrücken, wann ein Universum endlich ist.*

Beweis. Angekommen es gibt eine Formel f in $\mathcal{P}^=$, die in einer beliebigen Interpretation (U, I) genau dann wahr ist, wenn U endlich ist. Wir können $\mathcal{P}$ um 1-stellige Prädikate $P_1, P_2, \ldots$ erweitern, die nicht in f vorkommen. Die Formel

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

ist nur dann wahr in (I, U), wenn U mindestens n Elemente hat. Sei M die (unendliche) Menge der Formeln $f, f_1, f_2, \ldots$. Für jede endliche Teilmenge N von M existiert ein n mit $f_m \notin N$ für alle $m \geq n$. Hat U genau n Elemente, so ist (U, I) ein Modell von N. Nach dem Kompaktheitssatz besitzt auch M ein Modell (U, I). Wegen $I(f) = \mathbf{w}$ ist U endlich. Hat U genau n Elemente, so wäre aber $I(f_{n+1}) = \mathbf{f}$. Widerspruch. □

Bemerkung I.4.10. In der Prädikatenlogik *zweiter* Stufe $\mathcal{P}^2$ (mit Gleichheit) erlaubt man Formeln der Form $\forall P \ldots$ und $\forall \varphi \ldots$ für Prädikate P und Funktionen φ. Sei σ eine 1-stellige Funktion. Die Formeln

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

drücken aus, ob σ injektiv bzw. surjektiv ist.[14] Die Formel $\forall \sigma (f \Rightarrow g)$ ist in einer Interpretation (U, I) genau dann wahr, wenn jede injektive Funktion $U \to U$ surjektiv ist. Bekanntlich ist dies äquivalent zur Endlichkeit von U. Daher kann $\mathcal{P}^2$ mehr ausdrücken als $\mathcal{P}^1$. Der Beweis von Folgerung I.4.9 zeigt außerdem, dass der Modellexistenzsatz in $\mathcal{P}^2$ falsch ist.

I.5. Peano-Arithmetik

Bemerkung I.5.1. Wir haben bereits implizit Gebrauch von den natürlichen Zahlen gemacht, zum Beispiel in der Schreibweise $f_1, \ldots, f_n$. Wir führen in diesem Abschnitt die natürlichen Zahlen und deren Arithmetik axiomatisch ein.

Definition I.5.2.

(i) Die *Peano-Arithmetik* $\mathcal{PA}$ ist eine Prädikatenlogik erster Stufe mit Gleichheit und folgenden Eigenschaften:

- Alphabet: Variablen $a, b, \ldots$, Konstante 0, Symbole (,), $\neg$, $\Rightarrow$, $\forall$, $'$, $+$, $\cdot$ (keine Funktionen oder Prädikate)

[13] auch *Endlichkeitssatz* genannt
[14] Siehe Definition II.3.1

- Terme: Variablen und 0 sind Terme. Sind t, u Terme, so auch (t'), $(t+u)$ und $(t \cdot u)$.
- Formeln: Sind t und u Terme, so ist $t = u$ eine Formel. Für Formeln f, g und jede Variable x sind auch $\neg f$, $f \Rightarrow g$ und $\forall x f$ Formeln.
- Axiome: Für Variablen x, y und Formeln f, g, h gilt:

$f \Rightarrow (g \Rightarrow f)$		$(\mathcal{A}_1)$
$(\neg f \Rightarrow \neg g) \Rightarrow (g \Rightarrow f)$		$(\mathcal{A}_2)$
$(f \Rightarrow (g \Rightarrow h)) \Rightarrow ((f \Rightarrow g) \Rightarrow (f \Rightarrow h))$		$(\mathcal{A}_3)$
$\forall x(f \Rightarrow g) \Rightarrow (f \Rightarrow (\forall x g))$	falls x nicht frei in f vorkommt	$(\mathcal{P}_1)$
$\forall x f \Rightarrow f(x \leftarrow t)$	falls kollisionsfrei	$(\mathcal{P}_2)$
$x = x$		$(\mathcal{P}_1^=)$
$(x = y) \Rightarrow (f(y \leftarrow x) \Rightarrow f)$	falls kollisionsfrei	$(\mathcal{P}_2^=)$
$\neg((x') = 0)$,		(Σ_1)
$(x') = (y') \Rightarrow x = y$,		(Σ_2)
$(x + 0) = x$,		$(+_1)$
$(x + (y')) = ((x + y)')$,		$(+_2)$
$(x \cdot 0) = 0$,		$(\times_1)$
$(x \cdot (y')) = ((x \cdot y) + x)$,		$(\times_2)$
$f(x \leftarrow 0) \Rightarrow \big(\forall x(f(x) \Rightarrow f(x')) \Rightarrow \forall x f\big)$		$(\mathcal{I})$

- Schlussregeln: (MP) und (G).

(ii) Die *Standard-Interpretation* (U, I) benutzt das Universum der natürlichen Zahlen $U = \mathbb{N} = \{0, 1, \ldots\}$. Offensichtlich wird 0 als Null, $+$ als Addition und $\cdot$ als Multiplikation interpretiert. Außerdem sei $x' := x + 1$ die Nachfolgerfunktion wie in Beispiel I.3.8. Wir schreiben $\vDash_{\mathbb{N}} f$, wenn eine Formel f bzgl. $(\mathbb{N}, I)$ wahr ist.

Bemerkung I.5.3.

(i) Anstelle der Symbole $'$, $+$ und $\cdot$ könnte man auch 1- bzw. 2-stelligen Funktionen einführen. Die Symbolschreibweise ist aber ökonomischer. Man sieht leicht, dass der (Beweis von) Lemma I.3.13 für diese „Funktionen“ richtig bleibt. Insbesondere gilt die Umkehrung von (Σ_2), d. h. $\vdash x = y \Rightarrow x' = y'$.

(ii) Wie bisher benutzen wir die Abkürzungen $\wedge$, $\vee$, $\Leftrightarrow$, $\exists$ und $\neq$. Um Klammern zu sparen, vereinbaren wir, dass $'$ stärker bindet als alle anderen Symbole. Zusätzlich soll $\cdot$ stärker binden als $+$ (Punktrechnung geht vor Strichrechnung) und $\cdot$, $+$ stärker binden als $=$ und $\Rightarrow$. Damit hat (Σ_1) die Form $x' \neq 0$ und $((x \cdot y) + (z')) = 0$ verkürzt sich zu $x \cdot y + z' = 0$.

(iii) Das Axiom (Σ_1) besagt, dass 0 keinen Vorgänger hat. Nach (Σ_2) ist die Nachfolgerfunktion injektiv. Die Addition und Multiplikation ist rekursiv für alle natürlichen Zahlen durch $(+_1)$, $(+_2)$, $(\times_1)$ und $(\times_2)$ definiert. Die gewohnten Rechenregeln werden in Lemma I.5.5 bewiesen. Axiom $(\mathcal{I})$ beschreibt das (bereits benutzte) Prinzip der vollständigen Induktion.

(iv) Man sieht leicht, dass die Standard-Interpretation von $\mathcal{PA}$ ein Modell ist. Insbesondere ist $\mathcal{PA}$ konsistent. Möchte man $\mathcal{PA}$ aber nutzen, um $\mathbb{N}$ zu definieren, so steht dieses Modell aber nicht zur Verfügung. Wir kommen darauf in Bemerkung I.7.8 zurück.

(v) Es liegt nahe, die Abkürzungen $1 := 0'$, $2 := 1'$ usw. einzuführen. Um zwischen Variablen und Konstanten unterscheiden zu können, sei $\overline{n}$ die Konstante in $\mathcal{PA}$, die der natürlichen Zahl $n \in \mathbb{N}$ entspricht.

Beispiel I.5.4. Es gilt

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

In der *Principia Mathematica* von Whitehead-Russell wird diese Formel nach über 300 Seiten formaler Argumentation bewiesen.

Lemma I.5.5. *Für alle Terme t, u, v in $\mathcal{PA}$ gilt*

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

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

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

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

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

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

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

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

Beweis. Da keine der Formeln Quantoren enthält, können wir nach (S) annehmen, dass t, u und v Variablen sind.

(i) Für $f := (0 + t = t)$ gilt

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

(ii) Für $f(u) := (t' + u = (t + u)')$ gilt

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

(iii) Für $f(u) := (t + u = u + t)$ gilt

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

(iv) Hier kommt man ohne $(\mathcal{I})$ aus. Für $f(u) := (t + u = t + v)$ gilt

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

(v) Für $f(v) := (t + (u + v) = (t + u) + v)$ gilt

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

(vi),(vii) Aufgabe I.13.

(vi) Für $f(v) := ((t + u) \cdot v = t \cdot v + u \cdot v)$ gilt

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

□

I.6. Repräsentierbarkeit

Bemerkung I.6.1. In der Prädikatenlogik werden Prädikate als Relationen interpretiert. Als Ersatz für die in $\mathcal{PA}$ fehlenden Prädikate werden wir Formeln definieren, die Relationen und Funktionen auf $\mathbb{N}^k$ entsprechen. Ist $R \subseteq \mathbb{N}^k$ eine Relation, so schreiben wir $R(x_1, \ldots, x_n)$ für die Aussage $(x_1, \ldots, x_n) \in R$. Im Fall $k = 2$ definiert man in der Regel ein eigenes Symbol wie $\sim$ und schreibt $x \sim y$, falls $(x, y) \in R$.

Definition I.6.2.

- Eine Relation $R \subseteq \mathbb{N}^n$ wird durch eine Formel f in $\mathcal{PA}$ *repräsentiert*, falls für alle $x_1, \ldots, x_n \in \mathbb{N}$ gilt: $R(x_1, \ldots, x_n)$ genau dann, wenn $\vDash_{\mathbb{N}} f(\overline{x_1}, \ldots, \overline{x_n})$.

- Eine Funktion $\varphi\colon \mathbb{N}^n \to \mathbb{N}$ wird durch eine Formel f *repräsentiert*, falls die dazugehörige Relation durch f repräsentiert wird, d. h. für alle $x_1, \dots, x_n \in \mathbb{N}$ gilt $\varphi(x_1, \dots, x_n) = y$ genau dann, wenn $\vDash_{\mathbb{N}} f(\overline{x_1}, \dots, \overline{x_n}, \overline{y})$.

Interessiert man sich nur für die Existenz von f, so sagt man R bzw. φ sind *repräsentierbar*.

Beispiel I.6.3.

(i) Die Gleichheitsrelation $=$ wird nach Definition durch die Formel $f(x, y) := (x = y)$ repräsentiert. Die Nachfolgerfunktion $x \mapsto x + 1$ wird durch $x' = y$ repräsentiert. Analog werden Addition und Multiplikation durch ihre entsprechenden Symbole repräsentiert.

(ii) In Beispiel I.3.8 hatten wir die Kleiner-Relation als Prädikat definiert. Hier wird sie durch die Formeln

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

repräsentiert.

(iii) Die Teilbarkeitsrelation lässt sich durch

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

repräsentieren.

(iv) Beim Versuch, die Potenzfunktion $\varphi(x, y) := x^y$ zu repräsentieren, stößt man auf das Problem rekursive Aufrufe wie $x^y = x^{y-1} \cdot x$ zu repräsentieren. Dafür benötigen wir Werkzeuge.

Lemma I.6.4 (Gödels $\boldsymbol{\beta}$-Funktion)**.** *Es existiert eine repräsentierbare Funktion $\boldsymbol{\beta}\colon \mathbb{N}^3 \to \mathbb{N}$ mit folgender Eigenschaft: Für $k, n_0, \dots, n_k \in \mathbb{N}$ existieren $a, b \in \mathbb{N}$ mit $\boldsymbol{\beta}(a, b, i) = n_i$ für $i = 0, \dots, k$.*

Beweis. Wir definieren $\boldsymbol{\beta}$ direkt über folgende Formel

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

Die rechte Seite beschreibt y als den kleinsten nicht-negativen Rest bei der Division von a durch $1 + (x + 1)b$. Insbesondere ist $\boldsymbol{\beta}$ wohldefiniert und repräsentierbar.

Um zu zeigen, dass $\boldsymbol{\beta}$ die gewünschte Eigenschaft hat, sei $r := \max(k, n_0, n_1, \dots, n_k)$ und $b := r!$ (Fakultät[15]). Für $i = 0, \dots, k$ sei $d_i := 1 + (i+1)b$. Angenommen es existiert ein gemeinsamer Primteiler p von d_i und d_j mit $i \neq j$. Dann teilt p auch $d_i - d_j = b(i - j)$. Im Fall $p \mid b$ wäre $p \nmid d_i$. Da p eine Primzahl ist, muss also $p \mid i - j$ gelten. Dann wäre aber $p \leq k$ und $p \mid k! \mid r! = b$, was wir bereits ausgeschlossen hatten. Daher sind $d_0, \dots, d_k$ paarweise teilerfremd. Nach dem chinesischen Restsatz[16] existiert ein $a \in \mathbb{N}$ mit $n_i \equiv a \pmod{d_i}$ für $i = 0, \dots, k$. Nach Definition ist $n_i \leq r \leq b < d_i$. Dies zeigt $\boldsymbol{\beta}(a, b, i) = n_i$ für $i = 0, \dots, k$. □

Definition I.6.5. Für $x_1, \dots, x_n \in \mathbb{N}$ schreiben wir $\vec{x} := (x_1, \dots, x_n) \in \mathbb{N}^n$. Eine Funktion $\alpha\colon \mathbb{N}^n \to \mathbb{N}$ heißt (*primitiv*) *rekursiv*, falls sie eine der folgenden Formen hat:

- $n = 1$ und $\alpha = \zeta$ mit $\zeta(x) = 0$ für alle $x \in \mathbb{N}$ (*Nullfunktion*).
- $n = 1$ und $\alpha = \alpha_\prime$ mit $\alpha_\prime(x) = x + 1$ für alle $x \in \mathbb{N}$ (Nachfolgerfunktion).

[15] Siehe Definition II.7.1
[16] Siehe Zahlentheorie-Skript

- $\alpha = \pi_k^n$ mit $\pi_k^n(\vec{x}) = x_k$ für ein festes $1 \leq k \leq n$ (k-te *Projektion*).
- $\alpha(\vec{x}) = \beta\big(\gamma_1(\vec{x}), \ldots, \gamma_k(\vec{x})\big)$ für rekursive Funktionen $\beta\colon \mathbb{N}^k \to \mathbb{N}$ und $\gamma_1, \ldots, \gamma_k\colon \mathbb{N}^n \to \mathbb{N}$ (*Komposition*).
- $n \geq 2$ und
$$\alpha(\vec{x}) = \begin{cases} \beta(x_2, \ldots, x_n) & \text{falls } x_1 = 0 \\ \gamma\big(\alpha(x_1 - 1, x_2, \ldots, x_n), x_1 - 1, x_2, \ldots, x_n\big) & \text{falls } x_1 > 0 \end{cases}$$
mit rekursiven Funktionen $\beta\colon \mathbb{N}^{n-1} \to \mathbb{N}$ und $\gamma\colon \mathbb{N}^{n+1} \to \mathbb{N}$ (*Rekursion*).

Beispiel I.6.6.

(i) Sind $1 \leq i_1, \ldots, i_k \leq n$ beliebige Indizes und $\varphi\colon \mathbb{N}^k \to \mathbb{N}$ rekursiv, so auch
$$\psi(\vec{x}) := \varphi(x_{i_1}, \ldots, x_{i_k}) = \varphi\big(\pi_{i_1}^n(\vec{x}), \ldots \pi_{i_k}^n(\vec{x})\big).$$
Wir können daher Parameter bedenkenlos permutieren, hinzufügen oder entfernen (insbesondere bei der Rekursionsvorschrift).

(ii) Die Nullfunktion ζ^n in n Variablen erhält man rekursiv durch $\zeta^1 := \zeta$ und
$$\zeta^{n+1}(x_0, \ldots, x_n) = \begin{cases} \zeta^n(\vec{x}) & \text{falls } x_0 = 0, \\ \zeta^n(x_0 - 1, x_2, \ldots, x_n) & \text{falls } x_0 > 0 \end{cases}$$
(beachte (i)). Durch Komposition mit der Nachfolgerfunktion erhält man die konstanten Funktionen
$$\kappa_c^n(\vec{x}) := c$$
für ein festes $c \in \mathbb{N}$. Wir werden im Folgenden daher Konstanten direkt anstelle von κ einsetzen.

(iii) Die Identität[17] $\mathbb{N} \to \mathbb{N}$, $x \mapsto x$ wird durch π_1^1 realisiert.

(iv) Die Addition $\alpha_+(x, y) = x + y$ ist rekursiv, denn
$$\alpha_+(x, y) = \begin{cases} y & \text{falls } x = 0, \\ \alpha\prime(\alpha_+(x - 1, y)) & \text{falls } x > 0. \end{cases}$$

(v) Die Multiplikation $\alpha_\times(x, y) = x \cdot y$ ist rekursiv, denn
$$\alpha_\times(x, y) = \begin{cases} 0 & \text{falls } x = 0, \\ \alpha_+\big(\alpha_\times(x - 1, y), y\big) & \text{falls } x > 0. \end{cases}$$

(vi) Die Potenzfunktion $\alpha_\wedge(x, y) = y^x$ ist rekursiv, denn
$$\alpha_\wedge(x, y) = \begin{cases} 1 & \text{falls } x = 0, \\ \alpha_\times\big(\alpha_\wedge(x - 1, y), y\big) & \text{falls } x > 0. \end{cases}$$

[17] Siehe Beispiel II.3.2

(vii) Die Fakultät $\alpha_!(x) = x! = 1 \cdot 2 \cdot \ldots \cdot x$ ist rekursiv, denn

$$\alpha_!(x) = \begin{cases} 1 & \text{falls } x = 0, \\ \alpha_\times(\alpha_!(x-1), x) & \text{falls } x > 0. \end{cases}$$

Zur besseren Lesbarkeit verwenden wir von nun an die Terme $x + y$, $x \cdot y = xy$, x^y und $x!$ in der gewohnten Form.

(viii) Die Vorgängerfunktion $\sigma_-(x) := \begin{cases} x-1 & \text{falls } x > 0 \\ 0 & \text{falls } x = 0 \end{cases}$ ist rekursiv. Dafür definieren wir zuerst

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

und anschließend $\sigma_-(x) = \tau(x, 0)$.

(ix) Die abgeschnittene Subtraktion $\alpha_-(x, y) := \begin{cases} y - x & \text{falls } x < y \\ 0 & \text{sonst} \end{cases}$ ist rekursiv, denn

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

Damit wird auch die Betragsfunktion

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

rekursiv.

(x) Die Funktionen

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

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

sind rekursiv. Man nennt sgn die *Signumfunktion*.

Definition I.6.7. Eine Relation $R \subseteq \mathbb{N}^n$ heißt (*primitiv*) *rekursiv*, falls eine rekursive Funktion $\chi_R \colon \mathbb{N}^n \to \mathbb{N}$ mit

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

existiert.

Bemerkung I.6.8.

(i) Man nennt χ_R eine *charakteristische* Funktion von R. Durch Komposition mit der rekursiven Signumfunktion sgn kann man annehmen, dass χ_R *normiert* ist, also außerhalb von R den Wert 1 annimmt. Dadurch ist χ_R eindeutig bestimmt.

(ii) Sind $R, S \subseteq \mathbb{N}^n$ rekursive Relationen, so auch $\neg R := \mathbb{N}^n \setminus R$, $R \cup S$ und $R \cap S$ mit charakteristischen Funktionen $\overline{\text{sgn}} \circ \chi_R$,[18] $\chi_R \chi_S$ bzw. $\chi_R + \chi_S$.

[18] Siehe Definition II.3.1

(iii) Sind $R \subseteq \mathbb{N}^n$ und $\varphi_1, \ldots, \varphi_n \colon \mathbb{N} \to \mathbb{N}$ rekursiv, so auch die Relation

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

mit charakteristischer Funktion $\chi_S(\vec{x}) = \chi_R\big(\varphi_1(x_1), \ldots, \varphi_n(x_n)\big)$.

(iv) Wir benutzen ab jetzt die in der Mathematik beliebten Abkürzungen

$$\begin{aligned} \forall x < y\, f &:= \forall x(x < y \Rightarrow f), \\ \exists x < y\, f &:= \exists x(x < y \wedge f) \end{aligned}$$

und deren Varianten mit $\leq$, $>$ und $\geq$.

Satz I.6.9. *Jede rekursive Funktion und jede rekursive Relation ist in $\mathcal{PA}$ repräsentierbar.*

Beweis. Die Nullfunktion ζ wird durch die Formel $f(x, y) := (y = 0)$ repräsentiert. Die Nachfolgerfunktion hatten wir bereits in Beispiel I.6.3 repräsentiert. Die k-te Projektion π_k^n wird durch $x_k = y$ repräsentiert. Seien $\beta, \gamma_1, \ldots, \gamma_k$ rekursiv repräsentiert durch Formeln $b, c_1, \ldots, c_k$. Dann wird die Komposition $\alpha(\vec{x}) = \beta(\gamma_1(\vec{x}), \ldots, \gamma_k(\vec{x}))$ repräsentiert durch

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

Schließlich sei α mittels Rekursion aus σ und ρ gewonnen, die durch s bzw. t repräsentiert sind. Die Gödelsche $\boldsymbol{\beta}$-Funktion aus Lemma I.6.4 sei repräsentiert durch die Formel g. Für alle $x_1, \ldots, x_n \in \mathbb{N}$ existieren $a, b \in \mathbb{N}$ mit $\boldsymbol{\beta}(a, b, i) = \alpha(i, x_2, \ldots, x_n)$ für $i = 0, \ldots, x_1$. Damit existieren $y_1, y_2 \in \mathbb{N}$ mit

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

für $x < x_1$. Also wird α repräsentiert durch

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

Induktiv ergibt sich, dass jede primitive rekursive Funktion repräsentierbar ist.

Sei nun $R \subseteq \mathbb{N}^n$ eine rekursive Relation mit charakteristischer Funktion χ. Dann existiert eine Formel f mit

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

Also wird R durch die Formel $f(\vec{x}, 0)$ repräsentiert. □

Lemma I.6.10. *Sei $R \subseteq \mathbb{N}^{n+1}$ eine rekursive Relation und $\gamma \colon \mathbb{N} \to \mathbb{N}$ eine rekursive Funktion. Dann sind folgende Relationen bzw. Funktionen rekursiv:*

(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) $\varphi(x_0, \vec{x}) = \begin{cases} 0 & \text{falls } (y, \vec{x}) \notin R \text{ für alle } y \leq \gamma(x_0), \\ \min\limits_{y \leq \gamma(x_0)} R(y, \vec{x}) & \text{sonst} \end{cases}$

Beweis. Sei χ_R eine charakteristische Funktion von R.

(i) Wir nehmen zunächst an, dass $\gamma = \pi_1^1$ die Identität ist. Dann ist

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

eine rekursive charakteristische Funktion von $R_\forall$. Den allgemeinen Fall erhält man durch Komposition $\chi_\forall(x_0, \vec{x}) := \lambda(\gamma(x_0), \vec{x})$.

(ii) Der Beweis verläuft analog mit

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

(iii) Die rekursive Funktion

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

ist genau dann 1, wenn $s = t = 0 < u$ und sonst 0. Damit ist

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

rekursiv. Der Ausdruck $\delta(\tau(y-1, \vec{x}), \chi(y, \vec{x}), \chi_R(y-1, \vec{x}))$ bestimmt das kleinste y, bei dem $R(y, \vec{x})$ erfüllt ist. Der zweite Summand der Formel garantiert, dass sich τ für größere y nicht mehr ändert. Also ist $\varphi(x_0, \vec{x}) = \tau(\gamma(x_0), \vec{x})$ rekursiv. □

Lemma I.6.11. *Die folgenden Relationen und Funktionen sind rekursiv und somit repräsentierbar in $\mathcal{PA}$:*

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

(ii) $\Pr(x) \iff x$ *ist eine Primzahl*

(iii) $\rho(n) = n$*-te Primzahl in* $\mathbb{N}$ ($\rho(0) = 2$, $\rho(1) = 3$ *usw.*)

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

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

(vi) $\mu(x, k, e) = x\rho(k)^{e - \epsilon(k,x)}$ *für* $x > 0$ (*der Exponent von* $\rho(k)$ *in der Primfaktorzerlegung von* x *wird durch* e *ersetzt*)

Beweis.

(i) Obwohl wir nach Beispiel I.6.3 schon wissen, dass diese Relationen repräsentierbar sind, müssen wir für spätere Anwendungen trotzdem die Rekursivität nachweisen. Offenbar ist $|x - y|$ eine rekursive charakteristische Funktion von $x = y$. Als charakteristische Funktion für $x < y$ dient $\overline{\operatorname{sgn}}(\alpha_-(x, y))$. Wegen

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

ist $x \mid y$ nach Lemma I.6.10 rekursiv.[19]

[19] Der Term $z \leq y$ dient lediglich dazu die Voraussetzung von Lemma I.6.10 zu erfüllen.

(ii) Genau dann ist x eine Primzahl, wenn

$$x > 1 \wedge \exists y \leq x(y \mid x).$$

Offenbar ist $x > 1$ eine rekursive Relation. Nach (i) und Lemma I.6.10 ist auch $\exists y \leq x(y \mid x)$ rekursiv. Nach Bemerkung I.6.8 ist die Pr rekursiv.

(iii) Wir definieren zunächst die rekursive Funktion

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

Sicher ist $\rho(0) \leq \gamma(0)$. Sei induktiv bereits $\rho(n) \leq \gamma(n)$ gezeigt. Da $\rho(0)\rho(1)\dots\rho(n)+1$ durch keine der Primzahlen $\rho(0), \dots, \rho(n)$ teilbar ist, gilt $\rho(n+1) \leq \rho(n)! + 1 \leq \gamma(n)! + 1 = \gamma(n+1)$.[20] Nach Lemma I.6.10 ist

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

rekursiv. Daher auch

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

(iv) Für $\rho(k) \mid x$ und $x > 0$ gilt $k \leq \rho(k) \leq x$. Nach (iii), Bemerkung I.6.8 und Lemma I.6.10 ist die Relation

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

rekursiv. Also auch $\lambda(x) = \min_{y \leq x} S(x,y)$ (die Werte $\lambda(0) = \lambda(1) = 0$ sind irrelevant).

(v) Für $x, k \in \mathbb{N}$ gilt $x < 2^x \leq \rho(k)^x$ und daher $\rho(k)^x \nmid x$ sofern $x > 0$. Die Relation

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

ist rekursiv nach Beispiel I.6.6 und Bemerkung I.6.8. Also auch $\epsilon(x,k) = \min_{y \leq x} R(x,y,k)$ (mit $\epsilon(0,k) = 0$).

(vi) Nach den bereits bewiesenen Aussagen ist

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

rekursiv (mit $\mu(0,k,e) = 0$). □

Bemerkung I.6.12. Mit Lemma I.6.11 lassen sich Rekursionen flexibler definieren, indem nicht nur der direkte Vorgänger $\alpha(x_1 - 1, x_2, \dots, x_n)$, sondern mehrere Vorgänger berücksichtigt werden. Wir illustrieren dies anhand der *Fibonacci-Funktion* $\varphi\colon \mathbb{N} \to \mathbb{N}$ mit $\varphi(0) = \varphi(1) = 1$ und $\varphi(n+1) = \varphi(n) + \varphi(n-1)$ für $n > 0$. Nach Lemma I.6.11 ist

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

[20] Nach Bertrands Postulat gilt bereits $\rho(n+1) \leq 2\rho(n)$. Man kommt also mit $\mu(n) = 2^{n+1}$ aus. Siehe Zahlentheorie-Skript.

rekursiv. Wir definieren $\varphi(x) := \epsilon(\tau(x), 0)$. Dann gilt

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

wie gewünscht.

I.7. Gödels Unvollständigkeitssätze

Bemerkung I.7.1. Es gilt klar, dass $\mathcal{PA}$ negationsunvollständig ist, weil man weder $x = 0$ noch $x \neq 0$ beweisen kann (beide Formeln sind in der Standard-Interpretation falsch, vgl. Aufgabe I.14). Gödels erster Unvollständigkeitssatz impliziert, dass es sogar geschlossene Formeln mit dieser Eigenschaft gibt. Insbesondere ist $\mathcal{PA}$ unvollständig. Gödels Idee war es, eine Formel f mit der Bedeutung „f ist nicht beweisbar“ arithmetisch auszudrücken. Wäre f falsch, so könnte man f beweisen und $\mathcal{PA}$ wäre inkonsistent. Folglich muss f wahr und damit unbeweisbar sein. Um arithmetisch über Formeln sprechen zu können, kodiert man sie durch Zahlen wie folgt.

Definition I.7.2. Die Elemente des Alphabets von $\mathcal{PA}$ nennen wir im Folgenden *Zeichen*. Sie werden mit ungeraden Zahlen nummeriert:

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

Seien $p_0, p_1, \ldots = 2, 3, \ldots$ die Primzahlen ($p_i = \rho(i)$ mit der Bezeichnung aus Lemma I.6.11). Für eine beliebige Folge $s = s_0 \ldots s_n$ von Zeichen des Alphabets sei

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

die *Gödelnummer* von s. Besteht ein Beweis B aus Formeln $f_0, \ldots, f_n$, so sei

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

die *Gödelnummer* von B. Wir sagen auch: $\ulcorner s \urcorner$ bzw. $\ulcorner B \urcorner$ *kodiert* s bzw. B.

Beispiel I.7.3. Es gilt

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

Bemerkung I.7.4. Bekanntlich besitzt jede positive natürliche Zahl eine eindeutige Primfaktorzerlegung. Da einzelne Zeichen ungerade Gödelnummern, Zeichenfolgen gerade Gödelnummern mit ungeraden Primzahlexponenten und Beweise Gödelnummern mit geraden Primzahlexponenten haben, ist jedes dieser Objekte durch seine Gödelnummer eindeutig bestimmt. Offensichtlich kodiert nicht jede natürliche Zahl ein solches Objekt (z. B. 18).

Lemma I.7.5. *Die folgenden Funktionen und Relationen sind in $\mathcal{PA}$ repräsentierbar:*

(i) $\varphi(x,y) = \begin{cases} \ulcorner st \urcorner & \text{falls } x \text{ und } y \text{ Zeichenfolgen } s \text{ bzw. } t \text{ kodieren} \\ 0 & \text{sonst} \end{cases}$

(ii) $T(x) \iff$ *x ist Gödelnummer eines Terms*

(iii) $F(x) \iff$ *x ist Gödelnummer einer Formel*

(iv) $V(x,y,k) \iff$ *y kodiert Variable, die frei an Position k in f mit $x = \ulcorner f \urcorner$ vorkommt*

(v) $$\psi(x,y,z) = \begin{cases} \ulcorner f(w \leftarrow t) \urcorner & \text{falls } x = \ulcorner f \urcorner \text{ (Formel), } y = \ulcorner w \urcorner \text{ (Variable)} \\ & \text{und } z = \ulcorner t \urcorner \text{ (geschlossener Term)} \\ 0 & \text{sonst} \end{cases}$$

(vi) $B(x,y) \iff$ *x ist Gödelnummer eines Beweises der Formel mit Gödelnummer y*

Beweis.

(i) Nach Lemma I.6.11 gibt es rekursive Funktionen, die die Primfaktorzerlegung einer Zahl bestimmen. Daher kann man repräsentieren, wann x und y Gödelnummern von Zeichenfolgen s bzw. t sind. Nehmen wir an, dass dies der Fall ist. Es lässt sich außerdem der größte Primteiler $\rho(k)$ von x mit einer rekursiven Funktion bestimmen. Mit Lemma I.6.11 kann man y durch

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

ersetzen. Schließlich berechnet man rekursiv $\varphi(x,y) = x\tilde{y}$. Als rekursive Funktion ist φ nach Satz I.6.9 repräsentierbar.

(ii) Jeder Term t ist aus einer Folge von „Teiltermen“ $t_0, \dots, t_n$ aufgebaut, sodass $t_n = t$ und für jedes i eine der folgenden Aussagen gilt:

- t_i ist 0 oder eine Variable
- t_i ist (t'_j) für ein $j < i$
- t_i ist $(t_j + t_k)$ oder $(t_j \cdot t_k)$ für gewisse $j, k < i$

Es existieren $a, b \in \mathbb{N}$ mit $\boldsymbol{\beta}(a,b,i) = \ulcorner t_i \urcorner$ für $i = 0, \dots, k$ (Lemma I.6.4). Offensichtlich sind

$$\begin{aligned} R_0(x) &\iff x \text{ kodiert } 0 \iff x = 2^{19} \\ R_v(x) &\iff x \text{ kodiert eine Variable} \iff x = 2^r \text{ mit } r \geq 21 \text{ ungerade} \end{aligned}$$

rekursive Relationen. Wegen (i) sind folgende Funktionen repräsentierbar:

$$\varphi_\prime(x) := \begin{cases} \ulcorner (s') \urcorner & \text{falls } x \text{ die Zeichenfolge } s \text{ kodiert} \\ 0 & \text{sonst} \end{cases}$$

$$\varphi_+(x,y) := \begin{cases} \ulcorner (s+t) \urcorner & \text{falls } x, y \text{ die Zeichenfolgen } s \text{ bzw. } t \text{ kodieren} \\ 0 & \text{sonst} \end{cases}$$

$$\varphi_\times(x,y) := \begin{cases} \ulcorner (s \cdot t) \urcorner & \text{falls } x, y \text{ die Zeichenfolgen } s \text{ bzw. } t \text{ kodieren} \\ 0 & \text{sonst} \end{cases}$$

Es gilt

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

Ersetzt man darin R_v, $\boldsymbol{\beta}$ und die verschiedenen φ durch entsprechende Formeln (vgl. Beweis von Satz I.6.9), so erhält man eine Formel, die T repräsentiert.[21]

(iii) Ähnlich wie in (ii) ist jede Formel f aus „Teilformeln“ $f_0, \dots, f_n$ aufgebaut, sodass $f_n = f$ und für jedes i eine der folgenden Aussagen gilt:

- $i < n$ und f_i ist ein Term
- f_i ist $(f_j = f_k)$ für Terme f_j, f_k mit $j, k < i$
- f_i ist $(\neg f_j)$ für ein $j < i$ und f_j ist kein Term
- f_i ist $(f_j \Rightarrow f_k)$ mit $j, k < i$ und f_j, f_k sind keine Terme
- f_i ist $(\forall f_j f_k)$ mit $j, k < i$, f_j ist eine Variable und f_k kein Term

Folgende Funktionen sind nach Lemma I.6.11 repräsentierbar:

$$\varphi_=(x,y) := \begin{cases} \ulcorner (s = t) \urcorner & \text{falls } x \text{ und } y \text{ die Zeichenfolgen } s \text{ und } t \text{ kodieren} \\ 0 & \text{sonst} \end{cases}$$

$$\varphi_\neg(x) := \begin{cases} \ulcorner (\neg s) \urcorner & \text{falls } x \text{ die Zeichenfolge } s \text{ kodiert} \\ 0 & \text{sonst} \end{cases}$$

$$\varphi_\Rightarrow(x,y) := \begin{cases} \ulcorner (s \Rightarrow t) \urcorner & \text{falls } x, y \text{ die Zeichenfolgen } s \text{ bzw. } t \text{ kodieren} \\ 0 & \text{sonst} \end{cases}$$

$$\varphi_\forall(x,y) := \begin{cases} \ulcorner (\forall w s) \urcorner & \text{falls } x \text{ die Variable } w \text{ und } y \text{ die Zeichenfolge } s \text{ kodiert} \\ 0 & \text{sonst} \end{cases}$$

Es gilt

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

Durch Ersetzen von T, R_v und den φ erhält man eine Formel, die F repräsentiert.

(iv) Nach (iii) können wir annehmen, dass x eine Formel f und y eine Variable w kodiert. Mit Lemma I.6.11 sieht man, dass die Relation

$$V_0(x,y,k) \iff w \text{ steht an Position } k \text{ in } f$$

rekursiv ist. Um zu prüfen, ob w tatsächlich frei an Position k vorkommt, betrachten wir $f = s_0 \dots s_n$ als Zeichenfolge. Man muss einerseits prüfen, ob $\forall w$ links von s_k vorkommt und

[21] Man kann mit etwas mehr Aufwand zeigen, dass T rekursiv ist. Dazu muss man gemäß Lemma I.6.10 zeigen, dass n, a und b durch eine rekursive Funktion in x beschränkt sind.

andererseits, ob zwischen $\forall x$ und s_k mindestens so viele öffnende wie schließende Klammern stehen. Wir erinnern daran, dass definitionsgemäß alle Formeln durch Klammern begrenzt sind. Sei

$$\gamma_x(y,i) := \begin{cases} 0 & \text{falls } i = 0 \text{ oder } i > k, \\ \gamma_x(y,i-1)+1 & \text{falls } s_i = (\text{ und } (s_{i-2}s_{i-1} = \forall w \text{ oder } \gamma_x(i-1) > 0), \\ \gamma_x(y,i-1)-1 & \text{falls } s_i =) \text{ und } \gamma_x(i-1) > 0, \\ \gamma_x(y,i-1) & \text{sonst.} \end{cases}$$

Die Fallunterscheidungen lassen sich durch Linearkombinationen geeigneter charakteristischer Funktionen wie im Beweis von Lemma I.6.10 in einem einzigen rekursiven Aufruf bündeln. Daher ist γ_x rekursiv. Es gilt $\gamma_x(k) = 0$ genau dann, wenn x frei an Position k in f vorkommt. Formal ist

$$\gamma(x,y,i) := \begin{cases} \gamma_x(y,i) & \text{falls } x \text{ eine Zeichenfolge kodiert} \\ 0 & \text{sonst} \end{cases}$$

rekursiv. Fasst man alle Bedingungen zusammen, so erhält man

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

(v) Wie bisher können wir prüfen, ob x eine Formel f und y eine Variable w kodiert. Die Relation T aus (ii) lässt sich leicht modifizieren, sodass sie nur für geschlossene Terme t wahr ist. Mit (iv) lassen sich die Positionen aller freien Vorkommen von w in f identifizieren. Mit (i) kann man die Ersetzung $w \leftarrow t$ realisieren. Dabei ist zu beachten, dass neue Primfaktoren hinzukommen, sofern t nicht die Konstante 0 ist. Da t als geschlossen vorausgesetzt ist, gibt es keine Kollisionen zu beachten.

(vi) Wie können annehmen, dass x eine Formel f kodiert. Ein Beweis von f ist eine Folge von Formeln $f_0, \ldots, f_n$, sodass jedes f_i ein Axiom ist oder durch Schlussregeln aus f_j mit $j < i$ gewonnen wurde. Wir können also wie in (iii) argumentieren. Ob ein f_i ein Axiom ist, lässt sich prinzipiell (wenn auch sehr langwierig) durch eine entsprechende Folge von Teilformeln verifizieren. Für $(\mathcal{P}_2^=)$ kann man (v) benutzen. Wir verzichten darauf, die Details niederzuschreiben.[22] Das Überprüfen der beiden Schlussregeln ist hingegen wieder relativ einfach. □

Satz I.7.6 (Gödels erster Unvollständigkeitssatz)**.** *Die Peano-Arithmetik ist bzgl. der Standard-Interpretation unvollständig, d. h. es existieren wahre Aussagen, die man nicht beweisen kann.*

Beweis. Sei $\boldsymbol{b}$ eine Formel, die die Beweis-Relation B aus Lemma I.7.5 repräsentiert. Eine Formel f mit genau einer freien Variable x nennen wir *einstellig* (d. h. x kommt mindestens einmal frei in f vor). Ob f einstellig ist, lässt sich mit Lemma I.7.5 repräsentieren. Wir erinnern, dass $n \in \mathbb{N}$ den geschlossenen Term $\overline{n} = 0''^{\cdots\prime}$ repräsentiert. Nach Lemma I.7.5 wird die sogenannte *Diagonalfunktion*

$$\delta(x) := \begin{cases} \ulcorner f(\overline{x}) \urcorner & \text{falls } x = \ulcorner f \urcorner \text{ für eine einstellige Formel } f \\ 0 & \text{sonst} \end{cases}$$

durch eine Formel $\boldsymbol{d}$ repräsentiert. Die Formel

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

[22] Gödel hat insgesamt 46 Hilfsfunktionen definiert.

repräsentiert die Relation „x ist die Gödelnummer eines Beweises von $f(\overline{y})$ mit $y = \ulcorner f \urcorner$“. Somit repräsentiert die einstellige Formel

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

die Eigenschaft, dass kein Beweis für $f(\overline{y})$ mit $y = \ulcorner f \urcorner$ existiert. Wäre nun $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ beweisbar, so wäre $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ wahr, da $\mathcal{PA}$ bzgl. der Standard-Interpretation korrekt ist. Dann würde aber gerade kein Beweis für $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ existieren. Dieser Widerspruch zeigt, dass $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ unbeweisbar und somit wahr ist. □

Folgerung I.7.7. *Es gibt geschlossene Formeln in $\mathcal{PA}$, die man weder beweisen noch widerlegen kann.*

Beweis. Nach Satz I.7.6 existiert eine wahre geschlossene Formel f mit $\nvdash f$. Da $\mathcal{PA}$ korrekt ist, kann man die falsche Aussage $\neg f$ auch nicht beweisen. □

Bemerkung I.7.8.

(i) Nach Gödels Vollständigkeitssatz kann eine nicht-beweisbare Formel f keine Tautologie sein. Daher muss es sogenannte *Nichtstandard-Modelle* für $\mathcal{PA}$ geben, in denen f tatsächlich falsch ist. Nach dem Satz von Tennenbaum kann man solche Modelle nicht explizit angeben. Sie bilden die Grundlage der *Nichtstandard-Analysis* (siehe Bemerkung II.11.3).

(ii) Gödels Beweis funktioniert auch in dem schwächeren Kalkül der *Robinson-Arithmetik* $\mathcal{R}$. Dabei wird $(\mathcal{I})$ durch

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

ersetzt (jede von Null verschiedene Zahl besitzt einen Vorgänger). Tatsächlich gibt es einfache nicht-beweisbare wahre Aussagen in $\mathcal{R}$. Um das zu sehen, erweitern wir das Universum zu $U := \mathbb{N} \cup \{\infty\}$, wobei ∞ folgende Interpretation hat:

$$\infty' = x + \infty = \infty + x = \infty, \qquad x \cdot \infty = \infty \cdot x = \begin{cases} 0 & \text{falls } x = 0 \\ \infty & \text{falls } x \neq 0 \end{cases} \qquad (\text{für alle } x \in U)$$

Man prüft leicht, dass $\mathcal{R}$ bzgl. dieser Interpretation korrekt ist. Die Formel $x' \neq x$ ist in $\mathbb{N}$ wahr, aber in U falsch. Sie kann also nicht bewiesen werden. Damit hat man mit geringem Aufwand ein konsistentes unvollständiges Kalkül, was für die höhere Mathematik jedoch unzulänglich ist.

(iii) Umgekehrt kann man zeigen, dass $\mathcal{PA}$ bzgl. der Standard-Interpretation vollständig wird, wenn man auf die Multiplikation verzichtet (also die Axiome $(\times_1)$ und $(\times_2)$ streicht).

(iv) Definiert man die Peano-Arithmetik als Prädikatenlogik zweiter Stufe mit dem Induktionsaxiom

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

(wobei P über alle Prädikate läuft), so besagt *Dedekinds Isomorphiesatz*, dass $\mathbb{N}$ bis aus Isomorphie[23] das einzige Modell ist. Auch in dieser Version gilt Satz I.7.6 (ohne Beweis). Damit muss der Vollständigkeitssatz in $\mathcal{P}_2$ wiederum falsch sein (vgl. Bemerkung I.4.10).

(v) Wir hatten bisher die Konsistenz von $\mathcal{PA}$ modelliert durch $\mathbb{N}$ als gegeben angenommen. Dies widerstrebt jedoch dem Bemühen, die Mathematik auf eine axiomatische Grundlage zu stellen. Viel mehr sollte man $\mathbb{N}$ durch $\mathcal{PA}$ definieren. Von diesem Standpunkt muss man die Konsistenz von $\mathcal{PA}$ zusätzlich in Satz I.7.6 voraussetzen (siehe Satz I.7.10). Die Repräsentierbarkeit von

[23] d. h. bis auf Umbenennung der natürlichen Zahlen

Relationen und Funktionen muss dann rein syntaktisch erfolgen. Eine Funktion $\varphi\colon \mathbb{N}^n \to \mathbb{N}$ wird beispielsweise durch eine Formel f *syntaktisch repräsentiert*, falls für alle $\vec{x} \in \mathbb{N}^n$ gilt:

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

Die in Satz I.7.6 konstruierten Formeln $\boldsymbol{b}$ und $\boldsymbol{h}$ müssen außerdem durch

$$\begin{aligned} \tilde{\boldsymbol{b}}(x,y) &:\Longleftrightarrow\ x \text{ ist die Gödelnummer eines Beweises von } \ulcorner \neg f(\overline{y}) \urcorner \text{ mit } y = \ulcorner f \urcorner \\ \tilde{\boldsymbol{h}}(y) &:= \forall x \big(\boldsymbol{b}(x,y) \Rightarrow \exists z < x \tilde{\boldsymbol{b}}(z,y) \big) \end{aligned}$$

ersetzt werden (*Rossers Trick*). Semantisch bedeutet $g := \tilde{\boldsymbol{h}}(\ulcorner \tilde{\boldsymbol{h}} \urcorner)$ so viel wie:

Wenn g beweisbar ist, so existiert ein „kürzerer“ Beweis für $\neg g$.

Man kann nun mit deutlich mehr Aufwand Gödels Beweis durchführen[24] und erhält direkt die Negationsunvollständigkeit von $\mathcal{PA}$. Wir illustrieren in Beispiel I.7.9, wie man die syntaktische Repräsentierbarkeit der Addition beweist.

(vi) Es liegt nahe zu versuchen $\mathcal{PA}$ durch Hinzunahme weiterer Axiome zu „vervollständigen“. Die in (v) skizzierte syntaktische Version des ersten Unvollständigkeitssatzes gilt jedoch allgemeiner in jedem konsistenten Kalkül, das aussagekräftig genug ist, die Peano-Arithmetik zu formalisieren (ein solches Kalkül definieren wir in Definition II.1.6). Diese Erkenntnis zerstörte Hilberts langgehegten Traum, sämtliche wahre Aussagen der Mathematik mit einem Axiomensystem beweisen zu können.

Beispiel I.7.9.

(i) Wir zeigen, dass die Funktion $(x,y) \mapsto x+y$ syntaktisch durch die Formel $f(x,y,z) := (x+y=z)$ repräsentiert wird, d. h. $\vdash \overline{x} + \overline{y} = z \Leftrightarrow z = \overline{x+y}$. Nach Lemma I.3.12 und Aufgabe I.4 genügt es

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

zu beweisen. Für $y = 0$ gilt dies nach $(+_1)$. Sei nun $y > 0$ und $\vdash \overline{x} + \overline{y-1} = \overline{x+y-1}$ bereits gezeigt. Dann gilt

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

Man beachte, dass das Induktionsaxiom $(\mathcal{I})$ nicht gebraucht wird.

(ii) Da die im Beweis von Satz I.7.6 konstruierte nicht-beweisbare Formel $\boldsymbol{h}(\ulcorner \boldsymbol{h} \urcorner)$ sehr esoterisch daherkommt, kann man fragen, ob es greifbare nicht-beweisbare Formeln gibt. Die *Goodstein-Folge* $(g_i(n))_{i \geq 1}$ einer natürlichen Zahl n wird wie folgt definiert: Setze $g_1(n) := n$. Sei $b > 1$. Ist $g_{b-1}(n) = 0$, so sei auch $g_b(n) = 0$. Anderenfalls schreibe man $g_{b-1}(n)$ in der b-adischen Darstellung, z. B.

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

[24] Selbst Gödel verzichtet an dieser Stelle auf Details. Siehe [D. W. Hoffmann, *Die Gödel'schen Unvollständigkeitssätze*, Springer Spektrum, Wiesbaden, 2017].

für $n = 291$ und $b = 2$. Die Exponenten in dieser Darstellung werden iterativ ebenfalls in die b-adische Darstellung gebracht:

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

Nun werden darin alle Vorkommen von b durch $b+1$ ersetzt und anschließend 1 subtrahiert:

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

Für $n = 4$ lauten die ersten Glieder der Folge:

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

Auf den ersten Blick scheint die Folge gegen unendlich zu streben. Überraschenderweise erreicht $(g_i(4))$ aber erstmals für $i = 3 \cdot 2^{402653211} - 1$ den Wert 0 (und bleibt dann dort). Im Allgemeinen kann man die Formel

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

zwar in $\mathcal{PA}$ ausdrücken, aber nicht beweisen. Tatsächlich kann man g in $\mathcal{P}^2$ beweisen. Es ist durchaus denkbar, dass bekannte offene Probleme der Zahlentheorie wie die *Goldbachsche Vermutung* oder die Existenz von unendlich vielen *Primzahlzwillingen* nicht in $\mathcal{PA}$ (oder größeren Kalkülen) beweisbar sind.

Satz I.7.10 (Gödels zweiter Unvollständigkeitssatz)**.** *Die Konsistenz von $\mathcal{PA}$ lässt sich nicht in $\mathcal{PA}$ beweisen.*

Beweisskizze. Mit der Bezeichnung aus dem Beweis von Satz I.7.6 repräsentiert die Formel

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

die Eigenschaft, dass die Formel mit Gödelnummer x beweisbar ist. Bekanntlich lässt sich in einem inkonsistenten System jede Formel beweisen. Die Konsistenz von $\mathcal{PA}$ entspricht daher der Formel $c := \neg \boldsymbol{e}(\overline{\ulcorner 0 \neq 0 \urcorner})$. Wir hatten in Bemerkung I.7.8 skizziert, wie man die syntaktische Version von Satz I.7.6 unter Annahme von c beweisen würde. Ein formalisierter Beweis würde also mit der Zeile

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

enden.[25] Da die Funktion δ aus Satz I.7.6 in diesem Kontext syntaktisch durch $\boldsymbol{d}$ repräsentiert wird (siehe Bemerkung I.7.8), gilt

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

[25] Streng genommen müsste man Rossers Formel $\tilde{\boldsymbol{h}}(\ulcorner \tilde{\boldsymbol{h}} \urcorner)$ benutzen.

Wäre c in $\mathcal{PA}$ beweisbar, so erhält man:

$$\begin{aligned}
&\vdash \neg \boldsymbol{e}(\ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner)^{26} && \\
&\vdash y = \ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner \Rightarrow \big(\neg \boldsymbol{e}(\ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner) \Rightarrow \neg \boldsymbol{e}(y)\big) && (\text{Lemma I.3.12, } (\mathcal{P}_2^=)) \\
&\vdash y = \ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner \Rightarrow \neg \boldsymbol{e}(y) && (\text{D}) \\
&\vdash \boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \Rightarrow y = \ulcorner \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})\urcorner && (*) \\
&\vdash \boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \Rightarrow \neg \boldsymbol{e}(y) && (\text{MB}) \\
&\vdash \boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \Rightarrow \forall x \neg \boldsymbol{b}(x, y) && (\text{Def. } \exists, \text{ Lemma I.1.11}) \\
&\vdash \forall x \neg \boldsymbol{b}(x, y) \Rightarrow \neg \boldsymbol{b}(x, y) && (\mathcal{P}_2') \\
&\vdash \boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \Rightarrow \neg \boldsymbol{b}(x, y) && (\text{MB}) \\
&\vdash \neg\big(\boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \wedge \boldsymbol{b}(x, y)\big) && (\text{Def. } \wedge, \text{ Lemma I.1.11}) \\
&\vdash \forall y \neg\big(\boldsymbol{d}(\overline{\ulcorner \boldsymbol{h} \urcorner}, y) \wedge \boldsymbol{b}(x, y)\big) && (\text{G}) \\
&\vdash \neg \boldsymbol{g}(x, \ulcorner \boldsymbol{h} \urcorner) && (\text{Def. } \boldsymbol{g}) \\
&\vdash \boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner}) && ((\text{G}), \text{ Def. } \boldsymbol{h})
\end{aligned}$$

Das ist ein Widerspruch, denn $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ ist nach dem Beweis von Satz I.7.6 nicht beweisbar. □

Bemerkung I.7.11. Die Konsistenz von $\mathcal{PA}$ lässt sich im Kalkül der Zermelo-Fraenkel-Mengenlehre beweisen, das wir in Definition II.1.6 einführen.

I.8. Berechenbarkeit

Bemerkung I.8.1. Bisher haben wir die in der Praxis wichtige Frage, wie man Beweise findet, außer Acht gelassen. Da wir stets annehmen, dass das Alphabet eines Kalküls $\mathcal{K}$ abzählbar ist, kann man prinzipiell alle Axiome durchlaufen und in jedem Schritt mögliche Schlussregeln anwenden (in $\mathcal{PA}$ kann man alle natürlichen Zahlen durchlaufen und jeweils prüfen, ob sie einen Beweis kodieren). Auf diese Weise wird jeder Satz nach endlich vielen Schritten ausgegeben. Hat man jedoch eine unbeweisbare Formel f gegeben, so wird man vergebens darauf warten, dass f auf diese Weise gefunden wird. Ist $\mathcal{K}$ negationsvollständig, so wird aber $\neg f$ gefunden und man kann an dieser Stelle abbrechen (vorausgesetzt $\mathcal{K}$ ist konsistent). In diesem Fall heißt $\mathcal{K}$ *entscheidbar*. Wir werden zeigen, dass es für $\mathcal{PA}$ keinen Entscheidungsalgorithmus geben kann (Satz I.8.21).

Definition I.8.2. Die ACKERMANN-*Funktion* $\boldsymbol{\alpha}\colon \mathbb{N}^2 \to \mathbb{N}$ ist rekursiv definiert durch

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

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

[26] Bereits diese Aussage ist ein semantisches Paradoxon: Wir haben bewiesen, dass es keinen Beweis für die nicht-beweisbare Formel $\boldsymbol{h}(\overline{\ulcorner \boldsymbol{h} \urcorner})$ gibt.

Beispiel I.8.3. Nach Lemma I.8.4(i) ist $\boldsymbol{\alpha}$ wohldefiniert, auch wenn die explizite Berechnung eine große Zahl rekursiver Aufrufe erfordert. Wir zeigen $\boldsymbol{\alpha}_1(n) = 2^{n+2} - 1$ durch Induktion nach n. Es gilt

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

Lemma I.8.4. *Für alle $x, y, z, k \in \mathbb{N}$ gilt:*

(i) $\boldsymbol{\alpha}_k$ *ist rekursiv.*

(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) Für jede rekursive Funktion $\varphi\colon \mathbb{N}^n \to \mathbb{N}$ existiert ein $k \in \mathbb{N}$ mit $\varphi(\vec{x}) < \boldsymbol{\alpha}_k(\max(\vec{x}))$ für alle $\vec{x} \in \mathbb{N}^n$.

Beweis.

(i) Wegen $\boldsymbol{\alpha}_0(x) = 2x + 1$ ist $\boldsymbol{\alpha}_0$ rekursiv. Sei $k > 0$ und die Behauptung bereits für $k-1$ bewiesen. Dann ist

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

rekursiv.

(ii) Induktion nach x: Offenbar ist $\boldsymbol{\alpha}(0, y+1) = 2y + 3 > 2y + 1 = \boldsymbol{\alpha}(0, y)$ für alle $y \in \mathbb{N}$. Sei $x > 0$ und $\boldsymbol{\alpha}(x-1, y+1) > \boldsymbol{\alpha}(x-1, y)$ für alle y bereits gezeigt. Induktion nach y: Wegen $\boldsymbol{\alpha}(x-1, 1) > \boldsymbol{\alpha}(x-1, 0) \geq 1$ gilt

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

Sei $y > 0$ und $\boldsymbol{\alpha}(x, y) > \boldsymbol{\alpha}(x, y-1)$ bereits gezeigt. Dann gilt

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

(iii) Induktion nach x: Sicher ist $\boldsymbol{\alpha}(1, 0) = 3 > 1 = \boldsymbol{\alpha}(0, 0)$. Für $y > 0$ gilt $\boldsymbol{\alpha}(1, y-1) = 2^{y+1} - 1 > y$ nach Beispiel I.8.3. Es folgt

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

Sei nun $x > 0$ und $\boldsymbol{\alpha}(x, y) > \boldsymbol{\alpha}(x-1, y)$ für alle $y \in \mathbb{N}$ bereits gezeigt. Induktion nach y: Für $y = 0$ ist $\boldsymbol{\alpha}(x+1, 0) = \boldsymbol{\alpha}(x, 1) > \boldsymbol{\alpha}(x-1, 1) = \boldsymbol{\alpha}(x, 0)$. Sei $y > 0$ und $\boldsymbol{\alpha}(x+1, y-1) > \boldsymbol{\alpha}(x, y-1)$ bereits gezeigt. Dann gilt

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

(iv) Induktion nach y: Für $y = 0$ gilt $\boldsymbol{\alpha}(x+1, 0) = \boldsymbol{\alpha}(x, 1)$ nach Definition. Sei $y > 0$ und $\boldsymbol{\alpha}(x+1, y-1) \geq \boldsymbol{\alpha}(x, y)$ für alle $x \in \mathbb{N}$ bereits gezeigt. Dann ist

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

(v) Es gilt

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

(vi) Für die Nullfunktion, die Nachfolgerfunktion und die Projektionen kann man $k = 0$ wählen. Seien $\beta_1, \ldots, \beta_r, \gamma$ rekursiv mit entsprechenden Konstanten $k(\beta_i)$ und $k(\gamma)$. Sei $m := \max(k(\beta_1), \ldots, k(\beta_r))$ und $k := m + k(\gamma) + 1$. Für $\vec{x} \in \mathbb{N}^n$ gilt

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

Schließlich sei

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

mit rekursiven β und γ. Sei $m := k(\beta) + k(\gamma) + 1$. Wir zeigen zunächst

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

durch Induktion nach x_1. Dies gilt für $x_1 = 0$ wegen $k(\beta) < m$. Sei nun $x_1 > 1$ und die Behauptung für $x_1 - 1$ gezeigt. Dann gilt

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

Die Behauptung folgt nun mit $k := m + 1$, denn

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

Satz I.8.5 (Ackermann)**.** *Die Ackermann-Funktion ist nicht rekursiv.*

Beweis. Angenommen $\boldsymbol{\alpha}$ ist rekursiv. Dann existiert nach Lemma I.8.4 ein $k \in \mathbb{N}$ mit $\boldsymbol{\alpha}(x,x) < \boldsymbol{\alpha}_k(x) = \boldsymbol{\alpha}(k,x)$ für alle $x \in \mathbb{N}$. Dies widerspricht Lemma I.8.4 für $x > k$. $\square$

Definition I.8.6. Eine *Turing-Maschine* $T = (A, Z, I)$ besteht aus folgenden Dingen:

- ein endliches Alphabet A mit Sonderzeichen $\triangle \in A$
- eine endliche Menge von Zuständen Z mit Startzustand $\boldsymbol{s} \in Z$
- eine Menge von Instruktionen $I \subseteq Z \times A \times A \times \{\pm 1\} \times Z$

Die Maschine operiert auf einem beidseitig unendlichen Band, das mit Zeichen von A beschrieben ist. Zu Beginn ist eine Bandkonfiguration $(\ldots, a_{-1}, a_0, a_1, \ldots)$ vorgegeben, bei der $a_i = \triangle$ für fast alle i gilt (d. h. bis auf endlich viele Ausnahmen). Außerdem befindet sich T im Zustand $\boldsymbol{s}$ und der Lesekopf an Bandposition 0. Die Instruktionen definieren wie T arbeitet. Angenommen T ist im Zustand z und liest das Zeichen $a \in A$. Existiert eine Instruktion der Form $(z, a, \tilde{a}, r, \tilde{z})$, so ersetzt T das Zeichen a durch $\tilde{a}$ auf der gleichen Position und wechselt in den Zustand $\tilde{z}$. Ist $r = -1$ (bzw. $r = 1$), so rutscht der Lesekopf eine Position nach links (bzw. rechts). Anschließend wird erneut eine passende Instruktion gesucht. Wir setzen stets voraus, dass höchstens eine Instruktion $(z, a, \tilde{a}, r, \tilde{z})$ mit gegebenen z und a existiert (d. h. T ist *deterministisch*). Insbesondere ist $|I| \leq |A||Z|$.[27] Gibt es in einer Situation keine geeignete Instruktion, so hält T an (wir sagen T *terminiert*). Es kann passieren, dass T nie anhält (zum Beispiel wenn $|I| = |A||Z|$).

Bemerkung I.8.7.

(i) Wir nehmen stets an, dass A neben $\triangle$ noch mindestens ein weiteres Zeichen, sagen wir $1 \in A$, enthält. Man kann nun eine natürliche Zahl n als Bandkonfiguration mit n Einsen

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

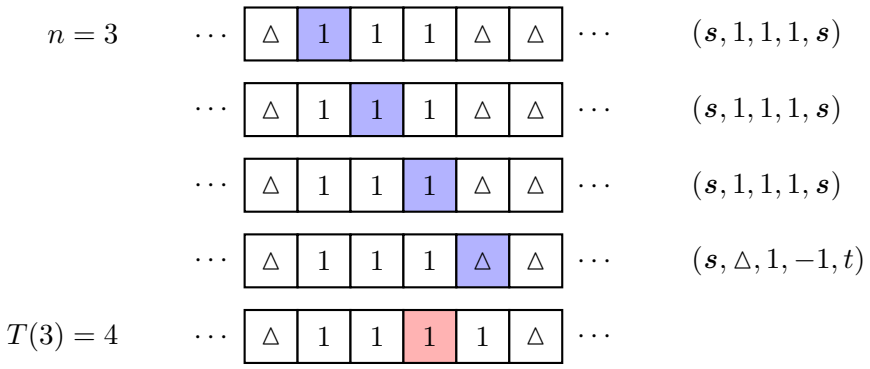
interpretieren (im Fall $0, 1 \in A$ könnte man auch die Binärdarstellung von n benutzen, siehe Aufgabe I.16). Wir nennen n die *Eingabe* von T, wenn dies die Startkonfiguration des Bands ist. Im Fall $n = 0$ sprechen wir vom *leerem* Band. Während der Berechnung kann T das Band mit weiteren Zeichen beschreiben. Terminiert T mit einer (zwangsweise endlichen) Folge von Einsen, so können wir das Ergebnis als $m \in \mathbb{N}$ interpretieren. Wir schreiben in diesem Fall $T(n) := m$. Terminiert T nicht mit einer Einsen-Folge oder gar nicht, so ist $T(n)$ nicht definiert. Auf diese Weise bestimmt T eine *partielle* Funktion $T\colon \mathbb{N} \rightharpoonup \mathbb{N}$.[28]

(ii) Eine Turing-Maschine T ist im Wesentlichen durch die Menge der Instruktionen I eindeutig bestimmt, denn Zeichen des Alphabets oder Zustände, die nicht I vorkommen, haben keinen Einfluss auf die Arbeitsweise von T.

(iii) Im Internet gibt es zahlreiche Simulatoren für Turing-Maschinen, mit denen man experimentieren kann.[29]

Beispiel I.8.8.

(i) Die Turing-Maschine T mit Instruktionen $I = \{(\boldsymbol{s}, 1, 1, 1, \boldsymbol{s}), (\boldsymbol{s}, \triangle, 1, -1, t)\}$ berechnet den Nachfolger $T(n) = n + 1$ für $n \in \mathbb{N}$.

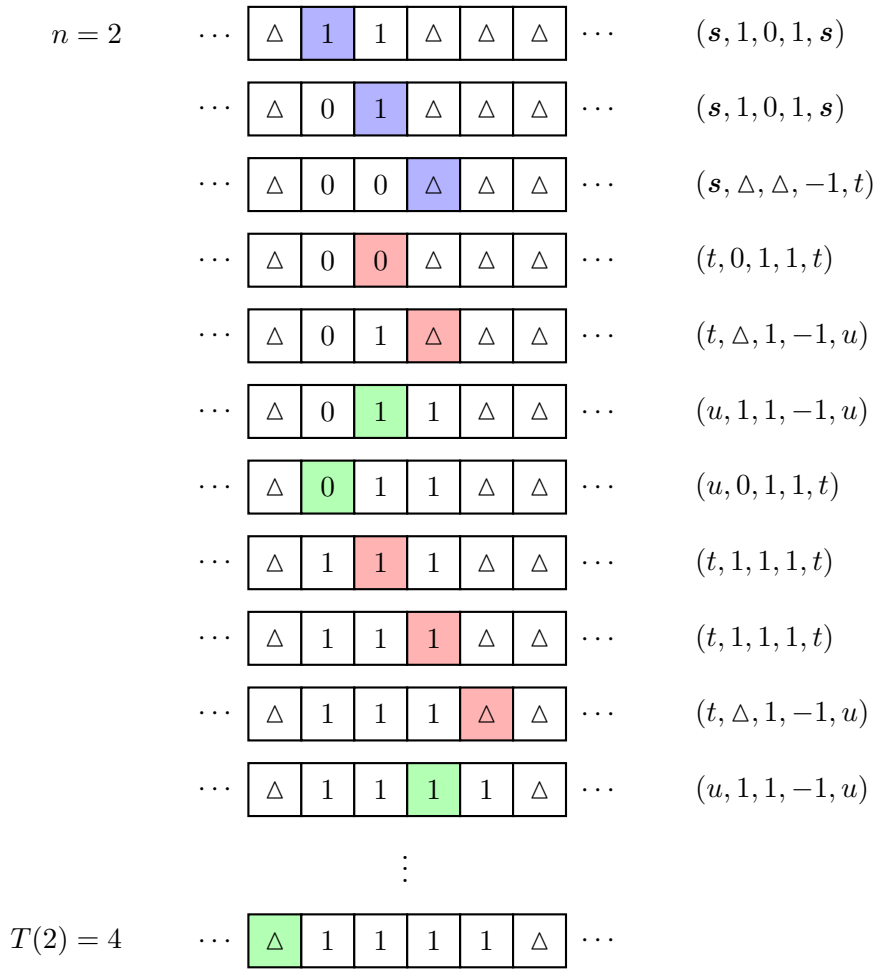


[27] Zur Notation siehe Definition II.1.2.
[28] Siehe Definition II.3.1
[29] Zum Beispiel `http://turingmachine.vassar.edu/` oder `https://turingmachinesimulator.com/`.

(ii) Die Turing-Maschine T mit Instruktionen

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

berechnet $T(n) = 2n$ für $n > 0$.



Bemerkung I.8.9. Obwohl viel komplexere Maschinen (z. B. Quantencomputer) denkbar sind, können diese bislang nicht mehr berechnen als Turing-Maschinen (sie können aber effizienter arbeiten). Daher nimmt man an, dass die *Church-These* gilt:

Alles was intuitiv berechenbar ist, lässt sich durch eine Turing-Maschine berechnen.

Definition I.8.10.

- Eine partielle Funktion $\varphi\colon \mathbb{N} \rightharpoonup \mathbb{N}$ heißt *berechenbar*, falls eine Turing-Maschine T existiert, sodass für alle $n \in \mathbb{N}$ gilt: Ist $\varphi(n)$ definiert, so auch $T(n)$ und $\varphi(n) = T(n)$ wie in Bemerkung I.8.7.
- Eine Funktion in mehreren Argumenten $\varphi\colon \mathbb{N}^n \to \mathbb{N}$ heißt *berechenbar*, falls ihre „Gödelisierung“ (Definition I.7.2)

$$\psi\colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto \begin{cases} \varphi(r_0, \dots, r_n) & \text{falls } n = p_0^{r_0} \dots p_k^{r_k}, \\ 0 & \text{falls } n = 0 \end{cases}$$

berechenbar ist.

- Die Existenz einer berechenbaren Funktion ist äquivalent zur Existenz eines *Algorithmus*. Die Schritte des Algorithmus entsprechen den Instruktionen der Turing-Maschine.

Beispiel I.8.11. Die Nullfunktion ζ wird durch die Turing-Maschine $(\{\triangle, 1\}, \{\boldsymbol{s}\}, \{(\boldsymbol{s}, 1, \triangle, 1, \boldsymbol{s})\})$ berechnet. Nach Beispiel I.8.8 ist die Nachfolgerfunktion berechenbar. Die Projektion π_k^n ist genau dann berechenbar, wenn die rekursive Funktion $\epsilon(x, k)$ aus Lemma I.6.11 berechenbar ist. Nach Aufgabe I.18 ist die Komposition von berechenbaren Funktionen berechenbar. Man kann zeigen, dass tatsächlich jede rekursive Funktion berechenbar ist (ohne Beweis). Der nächste Satz zeigt, dass die Umkehrung falsch ist.

Satz I.8.12. *Die Ackermann-Funktion ist berechenbar.*

Beweisskizze. Idee: Konstruiere eine Turing-Maschine T, die die rekursiven Aufrufe

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

durch geeignete Instruktionen ausführt. Es genügt dabei, die Argumente als Tupel direkt (anstelle der Gödelisierung) an T zu übergeben. Zu Beginn sei (x, y) (zum Beispiel als Einer-Folge getrennt durch $\triangle$) auf das Band geschrieben. In jeder Iteration ist eine Folge $(x_0, \ldots, x_n)$ gegeben. Die Instruktionen lauten

(i) Ist $n = 0$, so halte an.

(ii) Ist $x_{n-1} = 0$, so ersetze (x_{n-1}, x_n) durch $(2x_n + 1)$.

(iii) Ist $x_{n-1} > 0$ und $x_n = 0$, so ersetze (x_{n-1}, x_n) durch $(x_{n-1} - 1, 1)$.

(iv) Ist $x_{n-1} > 0$ und $x_n > 0$, so ersetze (x_{n-1}, x_n) durch $(x_{n-1} - 1, x_{n-1}, x_n - 1)$.

Man muss sich natürlich klarmachen, dass man dies mit einer Turing-Maschine realisieren kann. □

Beispiel I.8.13. Die Berechnung von $\boldsymbol{\alpha}(2, 1)$ durch eine Turing-Maschine läuft wie folgt ab:

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

Bemerkung I.8.14. Man kann zeigen, dass die Klasse der berechenbaren Funktionen mit der Klasse der *μ-rekursiven* Funktionen übereinstimmt. Dies sind partielle Funktionen φ, die durch (iterierte) Anwendung des *μ-Operators*

$$\varphi(x) := \begin{cases} \min\limits_{k \in \mathbb{N}} \Big(\gamma(k, x) = 0 \wedge \forall l < k \big(\gamma(l, x) \text{ ist definiert}\big)\Big) & \text{falls min existiert} \\ \text{undefiniert} & \text{sonst} \end{cases}$$

aus (μ-)rekursiven (partiellen) Funktionen $\gamma\colon \mathbb{N}^2 \to \mathbb{N}$ entstehen. Man beachte, dass im Unterschied zu Lemma I.6.10 die „Suchvariable“ k für das Minimum unbeschränkt ist. Existiert das Minimum nicht, so hält die entsprechende Turing-Maschine nicht an.

Satz I.8.15 (Halteproblem)**.** *Es gibt keinen allgemeinen Algorithmus, der entscheidet, ob eine gegebene Turing-Maschine mit einer gegebenen Eingabe terminiert.*

Beweis. Aufgrund ihrer Endlichkeit lässt sich jede Turing-Maschine T eindeutig durch eine Zahl $t \in \mathbb{N}$ beschreiben. Angenommen die Funktion $\varphi\colon \mathbb{N} \to \mathbb{N}$ mit

$$\varphi(n) = \begin{cases} 1 & \text{falls } n = 2^t 3^e \text{ und } T \text{ mit Eingabe } e \text{ terminiert,} \\ 0 & \text{sonst} \end{cases}$$

ist berechenbar. Dann existiert eine Turing-Maschine M mit $\varphi(n) = M(n)$ für alle $n \in \mathbb{N}$. Durch Ergänzen weiterer Instruktionen erhält man eine Turing-Maschine $\tilde{M}$, die genau dann mit Eingabe e terminiert, wenn $M(e) = 0$. In diesem Fall sei $\tilde{M}(e) = 1$. Wie im Beweis von Satz I.7.6 benutzen wir ein Diagonalargument. Sei $\tilde{M}$ durch $u \in \mathbb{N}$ kodiert und $n = 2^u 3^u$. Im Fall $\varphi(n) = 1$ terminiert $\tilde{M}$ bei Eingabe von u (Definition von f), aber dann wäre $\varphi(n) = M(n) = 0$. Im Fall $\varphi(n) = 0$ hingegen würde $\tilde{M}$ bei Eingabe von u nicht terminieren und $\varphi(n) = M(n) = 1$. Widerspruch. □

Bemerkung I.8.16.

(i) Angenommen es gibt einen Algorithmus, der entscheidet, ob eine Turing-Maschine zumindest auf dem leeren Band terminiert. Der folgende Algorithmus würde dann auch das allgemeine Halteproblem entscheiden: Für eine gegebene Turing-Maschine T und eine Eingabe $e \in \mathbb{N}$ konstruiere die Turing-Maschine $\tilde{T}$, die zuerst e auf das leere Band schreibt (das ist immer möglich, indem man notfalls für jeden Schritt einen eigenen Zustand definiert) und anschließend T ausführt. Nun terminiert T mit Eingabe e genau dann, wenn $\tilde{T}$ auf dem leeren Band terminiert. Daher ist auch das Halteproblem auf dem leeren Band unentscheidbar.

(ii) Das Halteproblem lässt sich noch viel weiter verallgemeinern: Sei E eine nicht-triviale Eigenschaft, die das Verhalten einer Turing-Maschine T betrifft (z. B. ob T an Position 10 eine 1 schreibt oder ob alle Ausgaben kleiner als 100 sind). Nicht-trivial bedeutet hierbei nur, dass E weder für alle noch für keine Turing-Maschine gilt. Der Satz von Rice besagt, dass kein Algorithmus existiert, der entscheidet, ob eine gegebene Turing-Maschine Eigenschaft E besitzt. Daraus folgt, dass auch die besten Compiler nicht jeden Bug in einem Programmcode finden können.

(iii) Es gibt sogenannte *universelle* Turing-Maschinen, die bei entsprechender Eingabe jede Turing-Maschine simulieren können (Vorläufer eines programmierbaren Computers). Dies ist schon mit relativ kleinen Parameter wie $(|A|, |Z|, |I|) = (5, 5, 22)$ möglich.

Definition I.8.17. Für $x, y \in \mathbb{N}$ sei $\boldsymbol{\rho}(x, y)$ die größtmögliche Anzahl an Schritten, die eine terminierende Turing-Maschine $T = (A, Z, I)$ mit $|A| = x$ und $|Z| = y$ auf dem leeren Band ausführen kann (man setze zusätzlich $\boldsymbol{\rho}(0, y) = 0 = \boldsymbol{\rho}(x, 0)$). Da es wegen $|I| \leq xy$ nur endlich viele solche Maschinen gibt, ist $\boldsymbol{\rho}$ wohldefiniert. Man nennt $\boldsymbol{\rho}$ die *Radó-Funktion* oder *fleißiger Biber*.

Satz I.8.18. *Die Radó-Funktion ist unberechenbar.*

Beweis. Ist $\boldsymbol{\rho}$ berechenbar, so erhält man folgenden Algorithmus für das Halteproblem: Man lasse eine Turing-Maschine $T = (A, Z, I)$ für $\boldsymbol{\rho}(|A|, |Z|)$ Schritte auf dem leeren Band laufen. Hat T bis dahin nicht angehalten, so weiß man, dass T nie anhält. Dies widerspricht Bemerkung I.8.16. □

Beispiel I.8.19. Man ist hauptsächlich an den Werten $\boldsymbol{\rho}(2, n)$ interessiert, d. h. Turing-Maschinen mit Alphabet $\{\triangle, 1\}$.[30] Traditionell zählt man auch den letzten Schritt, wenn es keine anwendbare

[30] Die Funktion $\mathbb{N} \to \mathbb{N}$, $n \mapsto \boldsymbol{\rho}(2, n)$ ist ebenfalls unberechenbar. Dafür muss man zeigen, dass sich jede Turing-Maschine durch eine Turing-Maschine mit 2-elementigem Alphabet simulieren lässt.

Instruktion mehr gibt und die Maschine in den „Haltezustand“ wechselt. Mit dieser Konvention erhält man

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

wobei $\boldsymbol{\rho}(2,5)$ erst im Jahr 2024 bestimmt wurde.[31] Die folgenden Instruktionen beschreiben eine entsprechende Maschine mit fünf Zuständen:

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

Die Bestimmung von $\boldsymbol{\rho}(2,6,0)$ ist hoffnungslos, da dieser Wert Größenordnungen erreicht, die nur mit spezieller Notation erfasst werden können.

Lemma I.8.20. *Jede berechenbare Funktion lässt sich auf einer Turing-Maschine simulieren, ohne die negative Bandhälfte zu benutzen (d. h. man arbeitet auf einem* einseitig *unendlichen Band).*

Beweis. Sei $T = (A, Z, I)$ eine Turing-Maschine. Wir definieren eine neue Turing-Maschine $\tilde{T} := (\tilde{A}, \tilde{Z}, \tilde{I})$ mit erweiterten Parametern wie folgt:

(i) Seien $\boldsymbol{s}$ und $\tilde{\boldsymbol{s}}$ die Startzustände von T bzw. $\tilde{T}$. Zu Beginn wird eine „Stoppmarke“ mit neuem Symbol $\|$ auf das Band geschrieben. Dafür dienen die Instruktionen $(\tilde{\boldsymbol{s}}, \triangle, \|, 1, \boldsymbol{s}), (\tilde{\boldsymbol{s}}, a, a, -1, \tilde{\boldsymbol{s}}) \in \tilde{I}$ für alle $a \in A \setminus \{\triangle\}$. Ist das Band anfangs leer, so steht $\|$ an Position 0 und anderenfalls an Position -1.

(ii) Die Instruktionen von T können nahezu unverändert nach $\tilde{T}$ übernommen werden. Wir verhindern lediglich, dass $\tilde{T}$ „Lücken“ auf dem Band hinterlässt, indem wir statt $\triangle$ ein neues Ersatzzeichen $\blacktriangle$ schreiben. Instruktionen der Form $(*, *, \triangle, *, *)$ werden also durch $(*, *, \blacktriangle, *, *)$ ersetzt. Für jede Instruktion der Form $(*, \triangle, *, *, *)$ braucht man zusätzlich die entsprechende Instruktion $(*, \blacktriangle, *, *, *)$ in $\tilde{I}$. Am Ende können diese Zeichen wieder durch $\triangle$ ersetzt werden.

(iii) Rückt der Lesekopf während der Ausführung auf die Stoppmarke, so soll das bisher beschriebene Band um eine Position nach rechts geschoben werden. Die Instruktionen $(z, \|, \|, 1, \tilde{z})$ für alle $z \in Z$ bewirken, dass der Lesekopf von $\|$ nach rechts rutscht und $\tilde{T}$ in einen neuen Zustand $\tilde{z} \in \tilde{Z}$ versetzt. Damit später die Ausführung in Zustand z fortgesetzt werden kann, schreiben wir ein neues Symbol $a_z \in \tilde{A}$ auf das Band: $(\tilde{z}, b, a_z, 1, z_b)$ für alle $z \in Z$ und $b \in A$. Hierbei ist $z_b \in \tilde{Z}$ ein neuer Zustand, der als Zwischenspeicher für das eingelesene Symbol b dient. Das eigentliche Verschieben des Bandinhalts geschieht durch die Instruktionen $(z_a, b, a, 1, z_b)$ für alle $a, b \in A \cup \{\blacktriangle\}$ mit $a \neq \triangle$. Am rechten Ende befindet sich $\tilde{T}$ in Zustand $z_\triangle$.

(iv) Durch die Instruktionen $(z_\triangle, a, a, -1, z_\triangle)$, $(z_\triangle, a_z, \triangle, -1, \tilde{z})$ und $(\tilde{z}, \|, \|, 1, z)$ für alle $a \in A \cup \{\blacktriangle\}$ und $z \in Z$ wird der Lesekopf zurück zur Stoppmarke geführt. Nun kann $\tilde{T}$ mit den Instruktionen aus T weitermachen.

(v) Wenn T nicht terminiert, wird auch $\tilde{T}$ nicht terminieren und der Bandinhalt ist irrelevant. Nehmen wir also an, dass T terminiert. Dann gibt es für ein Paar $(z, a) \in \tilde{Z} \times \tilde{A}$ keine passende Instruktion $(z, a, *, *, *)$. Um die in (ii) eingeführten Symbole $\blacktriangle$ zu entfernen, können wir für jedes solche Paar (z, a) eine neue Instruktion $(z, a, a, -1, q)$ mit einem neuen „Endzustand“ $q \in \tilde{Z}$ einführen. In diesem Zustand läuft $\tilde{T}$ ohne etwas zu verändern nach links zu $\|$. Anschließend läuft $\tilde{T}$ nach rechts unter Anwendung von $(q, \blacktriangle, \triangle, 1, q)$ bis zum ersten Mal $\triangle$ auf dem Band steht. Dort terminiert $\tilde{T}$. □

[31] Siehe Quanta magazine

Satz I.8.21 (Turing)**.** *Es gibt keinen allgemeinen Algorithmus, der entscheidet, ob eine geschlossene Formel der Peano-Arithmetik wahr ist.*

Beweis. Idee: Konstruiere zu jeder Turing-Maschine $T = (A, Z, I)$ eine geschlossene Formel f_T in $\mathcal{PA}$, die genau dann bzgl. der Standard-Interpretation wahr ist, wenn T auf dem leeren Band terminiert. Hat man einen Algorithmus, der entscheidet, ob f_T wahr ist, so hätte man nach Bemerkung I.8.16 auch ein Verfahren, das Halteproblem zu lösen.

Nach Lemma I.8.20 können wir annehmen, dass T nur die durch $\mathbb{N}$ indizierten Bandpositionen beschreibt. O. B. d. A. sei $A := \{0, \ldots, a\}$ und $Z := \{0, \ldots, z\}$, wobei 0 jeweils für $\triangle$ bzw. $\boldsymbol{s}$ steht. Jeder Schritt von T wird durch ein Tupel $t := (z, i, a_0, \ldots, a_n)$ beschrieben, wobei $z \in Z$ der aktuelle Zustand, $i \in \mathbb{N}$ die Position des Lesekopfs und $a_0, \ldots, a_n \in A$ der bisher benutzte Bandinhalt ist. Mittels Gödelisierung lässt sich t in einer Zahl $x \in \mathbb{N}$ kodieren. Es gibt rekursive Funktionen $\alpha(x) = z$, $\beta(x) = i$, $\gamma(x) = n$ und $\delta(x, k) = a_k$, wobei $\delta(x, k) = 0$ für $k > n$. Der Ausgangszustand wird durch die Formel

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

beschrieben. Für jede Instruktion $I_j = (z, a, *, *, *) \in I$ existiert eine Formel

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

die genau dann wahr ist, wenn I_j in der Konfiguration t anwendbar ist. Für $I = \{I_1, \ldots, I_l\}$ gilt

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

genau dann, wenn T in der Konfiguration t nicht anhält. Die Folge der Konfigurationen $x_0, \ldots, x_m$ lässt sich mit Gödels $\boldsymbol{\beta}$-Funktion kodieren, d. h. es existieren $a, b \in \mathbb{N}$ mit $\boldsymbol{\beta}(a, b, i) = x_i$ für $i = 0, \ldots, m$. Der Übergang von $x := x_i$ nach $y := x_{i+1}$ hängt wieder von der Existenz einer Instruktion $I_j = (z, a, b, r, w)$ ab:

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

Die folgende Formel ist genau dann wahr, wenn T (nach n Schritten) terminiert:

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

Da die benutzten Funktionen rekursiv sind, lässt sich f_T nach Satz I.6.9 in $\mathcal{PA}$ repräsentieren. Durch das Einsetzen der Konstanten (Definition I.6.2) wird f_T zu einer geschlossenen Formel. □

Folgerung I.8.22 (=Satz I.7.6)**.** *Die Peano-Arithmetik ist unvollständig.*

Beweis. Nehmen wir an $\mathcal{PA}$ wäre vollständig. Für jede geschlossene Formel f gilt $\vDash_{\mathbb{N}} f$ oder $\vDash_{\mathbb{N}} \neg f$, also auch $\vdash f$ bzw. $\vdash \neg f$. Für jede natürliche Zahl n kann man rekursiv (und damit berechenbar nach Beispiel I.8.11) prüfen, ob n einen Beweis von f oder $\neg f$ kodiert. Nach endlicher Zeit muss einer der beiden Fälle eintreten. Damit hätte man ein Entscheidungsverfahren für $\mathcal{PA}$ im Widerspruch zu Satz I.8.21. □

Bemerkung I.8.23. Für eine Prädikatenlogik erster Stufe $\mathcal{K}$ (mit mindestens einem n-stelligen Prädikat mit $n \geq 2$) kann man auf ähnliche Weise zeigen, dass kein Algorithmus existiert, der entscheidet, ob eine gegebene Formel eine Tautologie ist (*Satz von Church*). Nach dem Vollständigkeitssatz I.4.6 gibt es also auch keinen Algorithmus, der entscheidet, ob eine Formel f beweisbar ist. Im Gegensatz zu Folgerung I.8.22 reicht es nicht, alle Sätze in $\mathcal{K}$ aufzuzählen, denn es kann vorkommen, dass weder f noch $\neg f$ beweisbar sind (Bemerkung I.3.6).

Aufgaben

Aufgabe I.1. Seien $x, y \in \{1, 2, \ldots, 9\}$. Der Logiker (S)iegfried kennt nur die Summe $x + y$, während sein Kollege (P)etrus nur das Produkt xy kennt. Die beiden führen folgendes merkwürdiges Gespräch:

S: „Ich kenne x und y nicht.“
P: „Ich kenne x und y nicht.“
S: „Ich kenne x und y nicht.“
P: „Ich kenne x und y nicht.“
S: „Ich kenne x und y nicht.“
P: „Ich kenne x und y nicht.“
S: „Ich kenne x und y nicht.“
P: „Ich kenne x und y nicht.“
S: „Ich kenne x und y nicht.“
P: „Jetzt kenne ich x und y!“

Bestimmen Sie x und y.
Bemerkung: Man nehme an, dass S und P alle möglichen korrekten logischen Schlüsse ziehen.

Aufgabe I.2. Sei $\mathcal{K}$ das Kalkül aus Beispiel I.1.4. Zeigen Sie, dass ein Wort l genau dann in $\mathcal{K}$ beweisbar ist, wenn l eine ungerade Anzahl an a enthält.

Aufgabe I.3. Konstruieren Sie Kalküle $\mathcal{K}$ mit folgenden Eigenschaften:

(a) $\mathcal{K}$ ist negationsvollständig, aber nicht vollständig.

(b) $\mathcal{K}$ ist konsistent, aber nicht korrekt.

Aufgabe I.4.

(a) Zeigen Sie, dass $\Rightarrow$ in $\mathcal{A}$ nicht assoziativ ist, d. h.

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

(b) Beweisen Sie die Schlussregel $\frac{A \Rightarrow (B \Rightarrow C)}{B \Rightarrow (A \Rightarrow C)}$ in $\mathcal{A}$.
Hinweis: Wegen Satz I.2.13 kann man Satz I.2.5 benutzen.

(c) Beweisen Sie die Schlussregel $\frac{A, B}{A \wedge B}$ in $\mathcal{A}$.

Aufgabe I.5. Zeigen Sie, dass man $\mathcal{A}$ allein mit den Symbolen (,) und $\circledast$ beschreiben kann. Hierbei sei $A \circledast B$ gleichbedeutend mit $\neg(A \vee B)$.

Aufgabe I.6. Wir definieren in $\mathcal{A}$ drei „Wahrheitswerte“ $0, 1, 2$ mit folgender 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

Aussagen mit Wert 0 nennen wir *wahr*. Zeigen Sie:

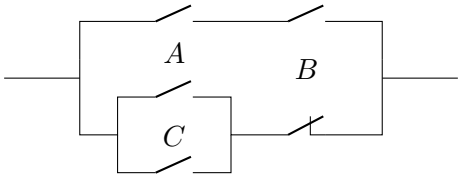
(a) Jede aus $(\mathcal{A}_2)$ und $(\mathcal{A}_3)$ abgeleitete Aussage ist wahr.

(b) Man kann $(\mathcal{A}_1)$ nicht aus $(\mathcal{A}_2)$ und $(\mathcal{A}_3)$ ableiten.

Bemerkung: Auf ähnliche Weise kann man die Unabhängigkeit von $(\mathcal{A}_2)$ und $(\mathcal{A}_3)$ zeigen.

Aufgabe I.7. Sie sind Richter in einem Prozess mit zwei Angeklagten, von denen einer stets die Wahrheit sagt, während der andere immer lügt. Sie wissen aber nicht, wer die Wahrheit sagt. Mit welcher Ja-Nein-Frage an einen der Angeklagten können Sie das Verbrechen aufklären?
Hinweis: Seien A und B die Aussagen „Angeklagter lügt“ und „Angeklagter plädiert auf unschuldig“. Konstruieren Sie die Wahrheitstabelle für die boolesche Funktion „Angeklagter ist schuldig“ und leiten Sie eine äquivalente Formel ab.

Aufgabe I.8. Mit der Aussagenlogik kann man einfache Schaltkreise modellieren. Jede Elementaraussage entspricht einem Schalter, der den Stromfluss durchlässt oder blockiert (z. B. ein Lichtschalter). Die Aussage $(A \wedge B) \vee ((A \vee C) \wedge \neg B)$ ist genau dann wahr, wenn Strom in folgendem Schaltkreis fließt:



(a) Konstruieren Sie einen einfacheren Schaltkreis mit äquivalentem Verhalten.

(b) Eine Lampe in einem Raum soll durch zwei Lichtschalter unabhängig voneinander aus- und eingeschaltet werden können (Betätigen eines Schalters soll den Zustand der Lampe stets ändern). Konstruieren Sie einen entsprechenden Schaltkreis.

Aufgabe I.9. Konstruieren Sie eine Prädikatenlogik erster Stufe, die Graphen modelliert.

Aufgabe I.10. Zeigen Sie:

(a) Das Deduktionslemma I.1.10 gilt für geschlossene Formeln in $\mathcal{P}$.

(b) Im Allgemeinen gilt Lemma I.1.10 nicht in $\mathcal{P}$, d. h. aus $f \vdash g$ folgt nicht unbedingt $\vdash f \Rightarrow g$.

Aufgabe I.11. Seien f, g und h Formeln in $\mathcal{P}$. Beweisen Sie die aus Lemma I.1.11 bekannte Formel

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

ohne Verwendung von Lemma I.1.10.
Bemerkung: Ergänzen Sie die Beweisschritte von Lemma I.1.10 im Beweis von Lemma I.1.11.

Aufgabe I.12. Zeigen Sie, dass jede korrekte Interpretation der Peano-Arithmetik ein unendliches Universum besitzt.

Aufgabe I.13. Beweisen Sie $\vdash t \cdot u = u \cdot t$ und $\vdash t \cdot (u \cdot v) = (t \cdot u) \cdot v$ für Terme t, u, v in $\mathcal{PA}$.

Aufgabe I.14. Wir nehmen an, dass $\mathcal{PA}$ konsistent ist. Beweisen Sie syntaktisch $\nvdash x = 0$ und $\nvdash x \neq 0$ ohne die Korrektheit von $\mathcal{PA}$ zu benutzen.

Aufgabe I.15. Definieren Sie eine Interpretation der Robinson-Arithmetik $\mathcal{R}$ bzgl. der die Addition nicht kommutativ ist.
Hinweis: $U := \mathbb{N} \cup \{a, b\}$.

Aufgabe I.16. Konstruieren Sie Turing-Maschinen T mit Alphabet $\{\triangle, 0, 1\}$ mit

(a) $T(n) = 2n$ für alle $n \in \mathbb{N}$.

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

Die Ein- und Ausgabe soll (im Gegensatz zu Beispiel I.8.8) in Binärdarstellung erfolgen.

Aufgabe I.17. Zeigen Sie, dass jeder Wert der Ackermann-Funktion die Form $2^n - 1$ mit $n \geq 1$ hat.

Aufgabe I.18. Zeigen Sie, dass $\varphi \circ \psi$ berechenbar ist, falls $\varphi, \psi \colon \mathbb{N} \to \mathbb{N}$ berechenbar sind.

Aufgabe I.19. Konstruieren Sie eine Turing-Maschine $T = (A, Z, I)$ mit $|A| = |Z| = 2$, die auf dem leeren Band nach genau fünf Schritten anhält.

II. Mengenlehre

II.1. Mengen

Bemerkung II.1.1. Wir definieren und untersuchen in diesem Kapitel ein Kalkül, das basierend auf dem Mengenbegriff praktisch alle Teile der modernen Mathematik ausdrücken kann. Wir hatten in Kapitel I bereits intuitiv von Mengen gesprochen. Cantor hat folgenden Versuch unternommen, eine Menge umgangssprachlich zu beschreiben.

Definition II.1.2 (Cantor)**.** Eine *Menge* M ist eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten x unserer Anschauung oder unseres Denkens zu einem Ganzen. Man sagt dann: x ist ein *Element* von M und schreibt $x \in M$ sowie $M = \{x : x \in M\}$ (bzw. $x \notin M$ für $\neg(x \in M)$). Die Anzahl $|M|$ der Elemente von M heißt *Kardinalität* oder *Mächtigkeit* von M. Man nennt M *leer*, *endlich* bzw. *unendlich*, falls M keine Elemente, endlich viele bzw. unendlich viele Elemente enthält.

Bemerkung II.1.3 (Russellsche Antinomie)**.** Definition II.1.2 ist ungenau, denn sie lässt Mengen zu, die zu logischen Widersprüchen führen. Sei beispielsweise M die Menge aller Mengen, die sich nicht selbst enthalten. Die Aussage $M \in M$ kann dann weder wahr noch falsch sein. Ebenso ist die Notation $|M|$ für unendliche Mengen ungenau, denn wir werden sehen, dass es mehrere unendliche Mächtigkeiten gibt (Definition II.6.3). Um solche Widersprüche zu verhindern, werden wir in Definition II.1.6 ein Kalkül aufstellen. Im Folgenden definieren wir die dafür benötigten Symbole und deren Bedeutung.

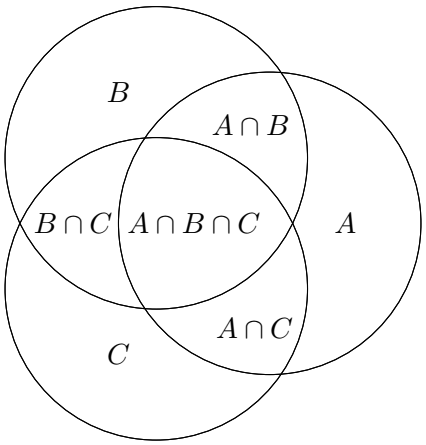
Definition II.1.4. Für Mengen A und B sei

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

Im Fall $A \cup B = B$ ist A eine *Teilmenge* von B. Man schreibt dann $A \subseteq B$ oder $A \subsetneq B$, falls zusätzlich $A \neq B$ (man spricht dann von einer *echten* Teilmenge). Ist A keine Teilmenge von B, so schreibt man $A \not\subseteq B$.

Bemerkung II.1.5. Vereinigungen und Durchschnitte von Mengen lassen sich graphisch durch Venn-

Diagramme darstellen:



Sind mehr als drei Mengen im Spiel, so lässt sich die allgemeine Situation nicht mehr durch Kreise darstellen. Das Coverbild zeigt ein Venn-Diagramm für fünf Mengen mit Hilfe von Ellipsen.

Definition II.1.6 (Zermelo-Fraenkel)**.** Das *Zermelo-Fraenkel-Kalkül* $\mathcal{ZF}$ der Mengenlehre ist eine Prädikatenlogik erster Stufe mit Gleichheit. Für Variablen benutzt man das lateinische Alphabet (Kleinbuchstaben werden in der Regel als Elemente interpretiert und Großbuchstaben als Mengen). Neben den üblichen Symbolen (Definition I.3.9) gibt es $\in$, $:$, $\{$, $\}$, $\cup$, $\cap$ und $\setminus$. Es gelten folgende Axiome:

(1) (Unendlichkeitsaxiom) Es existiert eine unendliche Menge M mit $x \in M \Rightarrow x \cup \{x\} \in M$.

(2) (Extensionalitätsaxiom) Mengen sind genau dann gleich, wenn sie die gleichen Elemente enthalten.

(3) (Fundierungsaxiom) Jede nichtleere Menge M besitzt ein Element $x \in M$, sodass $M \cap x$ leer ist.

(4) (Ersetzungsaxiom) Sei $A(x, y)$ ein Prädikat mit der Eigenschaft $(A(x, y) \wedge A(x, z)) \Rightarrow y = z$. Für jede Menge B existiert dann eine Menge C mit $x \in C \Leftrightarrow (\exists y \in B : A(x, y))$.

(5) (Vereinigungsaxiom) Für jede Menge A existiert eine Menge B mit der Eigenschaft $x \in B \Leftrightarrow (\exists C \in A : x \in C)$. Man schreibt $B = \bigcup_{a \in A} a$.

(6) (Potenzmengenaxiom) Für jede Menge M ist auch $\mathcal{P}(M) := \{N : N \subseteq M\}$ eine Menge, die man *Potenzmenge* von M nennt.

(7) (Auswahlaxiom) Ist A eine Menge von nichtleeren Mengen, so existiert eine Menge B, die zu jeden $C \in A$ genau ein $x \in C$ enthält.

Bemerkung II.1.7.

(i) In der Literatur finden sich weitere (historisch motivierte) Axiome, die man jedoch aus den oben genannten ableiten kann. Beispielsweise impliziert das Ersetzungsaxiom das

Aussonderungsaxiom: Ist $A(x)$ ein Prädikat und B eine Menge, so existiert eine Menge C mit $x \in C \Leftrightarrow (x \in B \wedge A(x))$

(wähle $A(x, y) := (x = y \wedge A(x))$). Man schreibt $C = \{x \in B : A(x)\}$. Aus dem Unendlichkeitsaxiom und dem Aussonderungsaxiom erhält man das

Leermengenaxiom: Es existiert eine leere Menge $\varnothing$.

(wähle $A(x) := \mathbf{f}$). Nach dem Extensionalitätsaxiom ist $\varnothing$ die einzige leere Menge. Schließlich ergibt sich das

Paarmengenaxiom: Für Mengen A und B existiert eine Menge C, die nur A und B als Elemente hat.

Dafür wendet man das Ersetzungsaxiom auf

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

mit dem Prädikat

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

an. Man schreibt $C = \{A, B\}$. Mit dem Vereinigungsaxiom folgt schließlich, dass $A \cup B$ tatsächlich eine Menge ist. Das Aussonderungsaxiom garantiert, dass auch $A \cap B$ und $A \setminus B$ Mengen sind.

(ii) Das Fundierungsaxiom verhindert die Russellsche Antinomie. Wir werden in Beispiel II.5.11 sehen, dass $\mathcal{ZF}$ die Peano-Arithmetik ausdrücken kann. Nach Gödels zweiten Unvollständigkeitssatz I.7.10 kann man daher die Konsistenz von $\mathcal{ZF}$ nicht in $\mathcal{ZF}$ beweisen. Ist $\mathcal{ZF}$ tatsächlich konsistent (wovon die meisten Mathematiker ausgehen), so muss es nach Gödels ersten Unvollständigkeitssatz I.7.6 wahre Aussagen geben, die man nicht beweisen kann. Das bekannteste Beispiel hierfür ist die *Kontinuumshypothese* (siehe Bemerkung II.7.7).

(iii) Manche Mathematiker verzichten auf das Auswahlaxiom, da es die Konstruktion kontraintuitiver Mengen zulässt: Das *Banach-Tarski-Paradoxon* besagt beispielsweise, dass man eine dreidimensionale Kugel in endlich viele Teile zerlegen kann, die anders zusammengesetzt zwei Kugeln vom gleichen Volumen wie die Ausgangskugel ergeben.

(iv) In seltenen Fällen benötigt man Objekte, die zu „groß“ sind um Mengen zu sein. Diese heißen *Klassen*. Zum Beispiel ist die Gesamtheit aller Mengen eine Klasse (Bemerkung II.7.7).

Definition II.1.8. Zwei Mengen A und B heißen *disjunkt*, falls $A \cap B = \varnothing$. Ggf. nennen wir $A \dot\cup B := A \cup B$ eine *disjunkte* Vereinigung.

Lemma II.1.9. *Für Mengen A, B und C gilt:*

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

(ii) $A \cup B = B \cup A$ *und* $A \cap B = B \cap A$ (*Kommutativität*).

(iii) $(A \cup B) \cup C = A \cup (B \cup C)$ *und* $(A \cap B) \cap C = A \cap (B \cap C)$ (*Assoziativität*).

(iv) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ *und* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (*Distributivität*).

(v) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ *und* $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ (*De Morgansche Regeln*).

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

Beweis. Durch logische Deduktion mittels Satz I.2.5 oder mit Venn-Diagrammen. Zum Beispiel

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

□

II.2. Relationen

Definition II.2.1.

(i) Seien A und B Mengen mit $a \in A$ und $b \in B$. Dann heißt $(a, b) := \{\{a\}, \{a, b\}\}$ (*geordnetes*) *Paar* von a und b. Im Gegensatz zur Menge $\{a, b\}$ gilt $(a, b) = (a', b') \Leftrightarrow (a = a' \wedge b = b')$.

(ii) Die Menge
$$A \times B := \{(a, b) : a \in A \wedge b \in B\}$$
heißt *kartesisches Produkt* von A und B.

(iii) Induktiv definiert man *Tripel* $(a, b, c) := (a, (b, c))$ und allgemeiner *n-Tupel* $(a_1, \ldots, a_n) := (a_1, (a_2, \ldots, a_n))$ für $n \geq 2$. Analog ist $A_1 \times \ldots \times A_n := A_1 \times (A_2 \times \ldots \times A_n)$ für Mengen $A_1, \ldots, A_n$. Speziell setzt man $A^n := A \times \ldots \times A$ (n Faktoren).

(iv) Eine *Relation* auf A ist eine Teilmenge $\sim \subseteq A \times A$. Man schreibt dann $a \sim b$, falls $(a, b) \in \sim$. Man nennt $\sim$

- *reflexiv*, falls $\forall a \in A : a \sim a$.
- *symmetrisch*, falls $\forall a, b \in A : (a \sim b \Rightarrow b \sim a)$.
- *antisymmetrisch*, falls $\forall a, b \in A : (a \sim b \sim a \Rightarrow a = b)$.
- *transitiv*, falls $\forall a, b, c \in A : (a \sim b \sim c \Rightarrow a \sim c)$.
- *total*, falls $\forall a, b \in A : (a \sim b \vee b \sim a)$.
- *Äquivalenzrelation*, falls $\sim$ reflexiv, symmetrisch und transitiv ist.
- *Ordnungsrelation*, falls $\sim$ reflexiv, antisymmetrisch und transitiv ist.

(v) Ist $\sim$ eine Äquivalenzrelation auf der Menge A und $a \in A$, so nennt man $[a] := \{b \in A : a \sim b\} \subseteq A$ die *Äquivalenzklasse* von a.

Beispiel II.2.2. Sei M eine Menge.

(i) Die Relation $M \times M$ ist offensichtlich eine (uninteressante) Äquivalenzrelation auf M.

(ii) Die Gleichheitsrelation ist die „kleinste“ reflexive Relation auf M. Außerdem handelt es sich um eine Äquivalenzrelation.

(iii) Die Teilmengenrelation $\subseteq$ ist eine Ordnungsrelation auf $\mathcal{P}(M)$. Im Fall $|M| > 1$ ist $\subseteq$ nicht total, denn $\{a\} \not\subseteq \{b\} \not\subseteq \{a\}$ für verschiedene $a, b \in M$.

(iv) Ist $\sim$ eine Äquivalenzrelation (bzw. Ordnungsrelation) und $A \subseteq M$, so ist $\sim \cap\, A \times A$ eine Äquivalenzrelation (bzw. Ordnungsrelation) auf A.

Lemma II.2.3. *Ist $\sim$ eine Äquivalenzrelation auf einer Menge A, so existiert ein $\mathcal{R} \subseteq A$, sodass A die disjunkte Vereinigung der Äquivalenzklassen $[r]$ mit $r \in \mathcal{R}$ ist.*

Beweis. Seien $a, b \in A$ und $c \in [a] \cap [b]$. Dann gilt $a \sim c$ und $b \sim c$. Da $\sim$ symmetrisch ist, gilt $c \sim b$. Da $\sim$ transitiv ist, gilt $a \sim b$. Für jedes $d \in [b]$ gilt also $a \sim b \sim d$ und $a \sim d$. Dies zeigt $[b] \subseteq [a]$ und analog erhält man $[a] \subseteq [b]$. Es folgt $[a] = [b]$. Somit sind je zwei Äquivalenzklassen entweder gleich oder disjunkt. Die Existenz von $\mathcal{R}$ folgt nun aus dem Auswahlaxiom. □

Bemerkung II.2.4. In der Situation von Lemma II.2.3 nennt man $\mathcal{R}$ ein *Repräsentantensystem* für die Äquivalenzklassen.

II.3. Funktionen

Definition II.3.1.

(i) Seien A und B Mengen. Eine *partielle Funktion* oder *Abbildung* von A nach B ist eine Teilmenge $f \subseteq A \times B$, sodass für jedes $a \in A$ höchstens ein $b \in B$ mit $(a, b) \in f$ existiert. Man schreibt dann $f(a) = b$ und

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

anstatt $(a, b) \in f$. Man nennt $\{a \in A : \exists b : f(a) = b\}$ den *Definitionsbereich* und B *Wertebereich* von f.

(ii) Existiert für jedes a genau ein $b \in B$ mit $(a, b) \in f$, so nennt man f *total* und schreibt $f \colon A \to B$. Wenn nichts anderes gesagt ist, setzen wir stets voraus, dass Funktionen total sind. Die Menge aller Funktionen $A \to B$ wird mit B^A bezeichnet.

(iii) Man nennt $f(a)$ das *Bild* von $a \in A$ unter f und $f(A) := \{f(a) : a \in A\} \subseteq B$ ist das *Bild* von f. Für $C \subseteq B$ ist $f^{-1}(C) := \{a \in A : f(a) \in C\} \subseteq A$ das *Urbild* von C unter f.

(iv) Man nennt f

- *injektiv*, falls $\forall a, a' \in A : (f(a) = f(a') \Rightarrow a = a')$.
- *surjektiv*, falls $\forall b \in B : \exists a \in A : f(a) = b$, d. h. $f(A) = B$.
- *bijektiv* (oder *Bijektion*), falls f injektiv und surjektiv ist. Man nennt dann A und B *gleichmächtig*.
- *Permutation*, falls f bijektiv ist und $A = B$. Die Menge aller Permutationen auf A wird mit $\mathrm{Sym}(A)$ bezeichnet.

(v) Sind $f \colon A \to B$ und $g \colon B \to C$ Funktionen, so auch $g \circ f \colon A \to C$ mit $(g \circ f)(a) := g(f(a))$ für $a \in A$. Man nennt $g \circ f$ die *Komposition* (oder *Hintereinanderausführung*, *Verkettung*) von f und g.

(vi) Ist $f \colon A \to B$ eine Funktion und $C \subseteq A$, so ist auch die *Einschränkung* $f_{|C} \colon C \to B$, $c \mapsto f(c)$ eine Funktion. Jede partielle Funktion wird total, wenn man sie auf ihren Definitionsbereich einschränkt.

Beispiel II.3.2.

(i) Für jede Menge A und $B \subseteq A$ ist $f \colon B \to A$, $b \mapsto b$ eine injektive Funktion, die man *Inklusion*(*sabbildung*) oder *Einbettung* nennt. Im Fall $B = A$ ist f sogar bijektiv und man nennt $\mathrm{id}_A := f$ *Identität* auf A.

(ii) Für Mengen A und B ist $f \colon A \times B \to B \times A$, $(a, b) \mapsto (b, a)$ sicher eine Bijektion.

(iii) Für eine beliebige Indexmenge I und Mengen A_i $(i \in I)$ kann man das kartesische Produkt $\bigtimes_{i \in I} A_i$ als Menge aller Funktionen $I \to \bigcup_{i \in I} A_i$ mit $f(i) \in A_i$ für $i \in I$ definieren. Für endliches I ist dies zu unserer ursprünglichen Definition äquivalent. Man schreibt die Elemente in $\bigtimes_{i \in I} A_i$ daher auch in der Form $(a_i)_{i \in I}$.

(iv) Zwei endliche Mengen A und B sind offenbar genau dann gleichmächtig, wenn $|A| = |B|$ (siehe auch Satz II.6.6).

Lemma II.3.3. *Seien $f\colon A \to B$, $g\colon B \to C$, $h\colon C \to D$ Funktionen mit $A \neq \varnothing$. Dann gilt*

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

(ii) Sind f und g injektiv, so auch $g \circ f$.

(iii) Sind f und g surjektiv, so auch $g \circ f$.

(iv) Ist $g \circ f$ injektiv, so ist f injektiv.

(v) Ist $g \circ f$ surjektiv, so ist g surjektiv.

(vi) Genau dann ist f injektiv, falls eine Funktion $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$ existiert.

(vii) Genau dann ist f surjektiv, falls eine Funktion $g\colon B \to A$ mit $f \circ g = \mathrm{id}_B$ existiert.

(viii) Genau dann ist f bijektiv, falls eine Funktion $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$ existiert. Ggf. ist g eindeutig bestimmt und man nennt $f^{-1} := g$ die Umkehrfunktion *von f.*

Beweis.

(i) Für $a \in A$ ist $((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a))) = h((g \circ f)(a)) = (h \circ (g \circ f))(a)$.

(ii) Für $a, a' \in A$ mit $(g \circ f)(a) = (g \circ f)(a')$ gilt $g(f(a)) = g(f(a'))$, also $f(a) = f(a')$ und $a = a'$.

(iii) Es gilt $(g \circ f)(A) = g(f(A)) = g(B) = C$.

(iv) Sei $f(a) = f(a')$ für $a, a' \in A$. Dann ist $(g \circ f)(a) = g(f(a)) = g(f(a')) = (g \circ f)(a')$. Da $g \circ f$ injektiv ist, folgt $a = a'$. Also ist f injektiv.

(v) Es gilt $C = (g \circ f)(A) = g(f(A)) \subseteq g(B) \subseteq C$, also $g(B) = C$.

(vi) Ist $g \circ f = \mathrm{id}_A$, so ist f injektiv nach (iv). Sei umgekehrt f injektiv und $c \in A$ fest gewählt (beachte: $A \neq \varnothing$). Wir definieren $g\colon B \to A$ wie folgt: ist $b = f(a)$ für ein $a \in A$, so sei $g(b) := a$ und anderenfalls $g(b) := c$. Da f injektiv ist, ist g dadurch wohldefiniert. Außerdem gilt $(g \circ f)(a) = g(f(a)) = a$ für $a \in A$, also $g \circ f = \mathrm{id}_A$.

(vii) Ist $f \circ g = \mathrm{id}_B$, so ist f surjektiv nach (v). Sei umgekehrt f surjektiv, d. h. $f(A) = B$. Nach dem Auswahlaxiom existiert eine Funktion $g\colon B \to A$ mit $g(b) \in f^{-1}(b)$ für alle $b \in B$. Offenbar gilt $(f \circ g)(b) = f(g(b)) = b$, d. h. $f \circ g = \mathrm{id}_B$.

(viii) Ist $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$, so ist f injektiv und surjektiv nach (iv) und (v), also auch bijektiv. Sei umgekehrt f bijektiv. Nach (vi) und (vii) existieren $g\colon B \to A$ und $h\colon B \to A$ mit $g \circ f = \mathrm{id}_A$ und $f \circ h = \mathrm{id}_B$. Dann gilt $g = g \circ \mathrm{id}_B = g \circ (f \circ h) = (g \circ f) \circ h = \mathrm{id}_A \circ h = h$. Dies zeigt auch, dass g eindeutig bestimmt ist. □

Satz II.3.4 (Cantor-Bernstein)**.** *Seien A und B Mengen mit injektiven Abbildungen $f\colon A \to B$ und $g\colon B \to A$. Dann sind A und B gleichmächtig.*

Beweis. Wir definieren $C_0 := A \setminus g(B)$ und $C_n := g(f(C_{n-1}))$ für $n \geq 1$. Weiter sei $C := \bigcup_{n=0}^{\infty} C_n$ und $h\colon A \to B$ mit

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

Im Fall $x \notin C$ ist $x \notin C_0$, d. h. $x \in g(B)$. Folglich ist $g^{-1}(x)$ durch die Injektivität von g eindeutig bestimmt und h ist wohldefiniert. Seien nun $x, y \in A$ mit $h(x) = h(y)$. Nehmen wir $x \in C$ und $y \notin C$ an. Dann ist $f(x) = g^{-1}(y)$ und $g(f(x)) = y$. Sei $x \in C_n$ für ein $n \geq 0$. Dann folgt der Widerspruch $y = g(f(x)) \in g(f(C_n)) = C_{n+1} \subseteq C$. Also gilt $x, y \in C$ oder $x, y \notin C$ und man erhält $x = y$. Somit ist h injektiv.

Sei nun $y \in B$ beliebig. Im Fall $g(y) \notin C$ ist $h(g(y)) = g^{-1}(g(y)) = y$. Sei also $g(y) \in C_n$ für ein $n \geq 1$. Es existiert dann ein $x \in C_{n-1}$ mit $g(f(x)) = g(y)$. Aus der Injektivität von g folgt $h(x) = f(x) = y$. Also ist h auch surjektiv und bijektiv. □

Bemerkung II.3.5. Wir geben eine interessante Anwendung des Auswahlaxioms.

Satz II.3.6. *Gegeben sei eine beliebige Menge von Zwergen mit roten oder grünen Hüten. Die Zwerge können die Hüte der anderen Zwerge sehen, aber nicht den eigenen. Sie können sich nicht untereinander verständigen. Dann gilt:*

(i) (Gabay-O'Connor) *Es gibt eine Strategie, mit der alle, bis auf endlich viele, Zwerge ihre Hutfarbe korrekt erraten.*

(ii) (Lenstra) *Es gibt eine Strategie, mit der entweder alle Zwerge ihre Hutfarbe korrekt erraten oder alle Zwerge ihre Hutfarbe falsch erraten.*

(iii) Es gibt eine Strategie, mit der mindestens 50% *alle Zwerge ihre Hutfarbe korrekt erraten.*

Beweis. Sei Z die Menge der Zwerge und $F := \{Z \to \{r, g\}\}$ die Menge aller Hutverteilungen. Für $f, f' \in F$ sei $f \sim f'$, falls sich f und f' nur an endlich vielen Stellen unterscheiden. Offenbar definiert $\sim$ eine Äquivalenzrelation auf F. Nach dem Auswahlaxiom kann man zu jeder Äquivalenzklasse $[f]$ einen Repräsentanten $f_0 \in F$ wählen. Sei nun f die gegebene Hutverteilung. Dann können alle Zwerge f_0 bestimmen.

(i) Zwerg $z \in Z$ rät $f_0(z)$ als seine Hutfarbe. Da sich f nur an endlich vielen Stellen von f_0 unterscheidet, erraten alle, bis auf endliche viele, Zwerge ihre Hutfarbe korrekt.

(ii) Jeder Zwerg $z \in Z$ kann die endliche Mächtigkeit

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

bestimmen. Ist $n(z)$ eine gerade Zahl, so rät z seine Hutfarbe $f_0(z)$ und anderenfalls die von $f_0(z)$ verschiedene Farbe. Unterscheiden sich f und f_0 an einer geraden Anzahl von Stellen, so erraten alle Zwerge ihr Hutfarbe korrekt. Anderenfalls erraten alle Zwerge ihre Hutfarbe falsch.

(iii) Wir nehmen an, dass die Hüte gleichverteilt sind. Sei $z \in Z$ fest und $h \in [f]$. Sei $h' \in [f]$ mit $h'(z) \neq h(z)$ und $h'(z') = h(z')$ für alle $z' \in Z \setminus \{z\}$. Dann ist $h \to h'$ eine Permutation auf $[f]$, sodass sich die Anzahl der Unterschiede zwischen f_0 und h sowie zwischen f_0 und h' um genau 1 unterscheiden. Daher treten die beiden Fälle in (ii) gleich häufig auf. □

Beispiel II.3.7. Angenommen es sind nur endlich viele Zwerge. Dann kann man für f_0 die konstante Funktion mit $f_0(z) = g$ für alle $z \in Z$ wählen. Sieht ein Zwerg eine gerade Anzahl von roten Hüten, so rät er die eigene Hutfarbe als grün und anderenfalls als rot. Gibt es insgesamt eine gerade Anzahl an roten Hüten, so erraten alle Zwerge ihre Hutfarbe korrekt.

II.4. Geordnete Mengen

Definition II.4.1. Sei $\leq$ eine Ordnungsrelation auf einer Menge A und $B \subseteq A$.

(i) Wie üblich benutzen wir die Schreibweisen $a \geq a'$ (falls $a' \leq a$), $a < a'$ (falls $a \leq a' \neq a$) und $a > a'$ (falls $a' \leq a \neq a'$) für $a, a' \in A$.

(ii) Ein $a \in A$ heißt

- *größtes* Element, falls $\forall a' \in A : a' \leq a$.
- *maximales* Element, falls $\forall a' \in A : (a \leq a' \Rightarrow a = a')$.

Analog definiert man *kleinste* und *minimale* Elemente von A.

(iii) Ein $a \in A$ heißt *obere Schranke* von B, falls $\forall b \in B : b \leq a$. Analog definiert man *untere Schranken* von B.

(iv) Man nennt A *wohlgeordnet*, falls jede nichtleere Teilmenge von A ein kleinstes Element enthält.

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

Bemerkung II.4.2.

(i) Im Allgemeinen existieren weder größte Elemente, noch maximale Elemente, noch obere Schranken. Ist $a \in A$ ein größtes Element, so ist a das einzige größte und das einzige maximale Element in A. Man schreibt dann $a = \max M$ (analog $\min M$ für das kleinste Element). In total geordneten Mengen fallen die Begriffe größtes Element und maximales Element zusammen.

(ii) Wohlgeordnete Mengen sind stets total geordnet. Umgekehrt ist eine total geordnete Menge bereits dann wohlgeordnet, wenn es keine unendliche Folge der Form $a_0 > a_1 > \ldots$ gibt. Insbesondere ist jede endliche total geordnete Menge wohlgeordnet.

(iii) Jede Teilmenge einer total (wohl)geordneten Menge ist total (wohl)geordnet.

Beispiel II.4.3. Sei M eine endliche Menge mit $|M| > 1$. Sei $P := \mathcal{P}(M) \setminus \{\varnothing\}$ geordnet durch $\subseteq$. Dann ist jede einelementige Teilmenge von minimales Element von P. Andererseits besitzt P kein kleinstes Element. Offenbar ist $\varnothing$ eine untere Schranke von P in $\mathcal{P}(M)$.

Satz II.4.4 (Transfinite Induktion)**.** *Sei $(A, \leq)$ eine wohlgeordnete Menge. Sei $P(a)$ ein Prädikat, sodass für alle $a \in A$ gilt:*

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

Dann gilt $P(a)$ für alle $a \in A$.

Beweis. Wäre die Menge $\{a \in A : \neg P(a)\}$ nichtleer, so gäbe es ein kleinstes $a \in A$ mit $\neg P(a)$. Für jedes $b < a$ wäre aber $P(b)$ wahr. □

Bemerkung II.4.5. Man beachte, dass diese Formulierung der Induktion keinen Induktionsanfang braucht. Ist a das kleinste Element von A, so ist $A^{<a} = \varnothing$ und $P(a)$ folgt aus der Voraussetzung.

Lemma II.4.6 (Zorn)**.** *Sei M eine geordnete Menge. Besitzt jede total geordnete Teilmenge von M eine obere Schranke, so enthält M ein maximales Element.*

Beweis. [1] Wir nehmen das Gegenteil an. Da $\varnothing \subseteq M$ eine obere Schranke besitzt, ist $M \neq \varnothing$. Sei A eine total geordnete Teilmenge von M und $x \in M$ eine obere Schranke von A. Dann ist x nicht maximal. Daher existiert ein $y \in M$ mit $x < y$. Insbesondere ist $a < y$ für alle $a \in A$. Wir nennen y eine *echte* obere Schranke von A. Nach dem Auswahlaxiom existiert eine Funktion f, die jeder total geordneten Teilmenge $A \subseteq M$ eine echte obere Schranke $f(A)$ zuordnet. Für $a \in A$ ist auch $A^{<a}$ total geordnet. Wir nennen A *zulässig*, falls A wohlgeordnet und $f(A^{<a}) = a$ für jedes $a \in A$ ist. Offenbar ist $\varnothing$ zulässig. Für jede zulässige Teilmenge $A \subseteq M$ ist auch $A \cup \{f(A)\}$ zulässig, denn

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

Seien $A, B \subseteq M$ zulässig mit $A \neq B$, o. B. d. A. $B \nsubseteq A$. Da B wohlgeordnet ist, existiert ein kleinstes Element b in $B \setminus A$. Dann ist $B^{<b} \subseteq A$.

Annahme: $B^{<b} \neq A$.
Da A wohlgeordnet ist, existiert ein kleinstes Element a von $A \setminus B^{<b}$. Dann ist $A^{<a} \subseteq B^{<b}$. Wegen $B \nsubseteq A^{<a}$ existiert ein kleinstes Element c von $B \setminus A^{<a}$. Daher ist $B^{<c} \subseteq A^{<a} \subseteq B^{<b} \subseteq A$. Im Fall $b < c$ wäre $b \in B^{<c} \subseteq A$ im Widerspruch zur Wahl von b. Also ist $c \leq b$. Im Fall $c = b$ ist $A^{<a} = B^{<c}$. Im Fall $c < b$ ist $c \in B^{<b} \subseteq A$. Wegen $c \notin A^{<a}$ ist $c \geq a$, d. h. $A^{<a} \subseteq A^{<c} \cap B \subseteq B^{<c} \subseteq A^{<a}$. Daher ist in jedem Fall $A^{<a} = B^{<c}$. Da A und B zulässig sind, folgt $a = f(A^{<a}) = f(B^{<c}) = c \leq b$. Im Fall $c = b$ wäre $b = c = a \in A$ im Widerspruch zur Wahl von b. Also ist $a = c < b$ und wir haben den Widerspruch $a = c \in B^{<b}$.

Also gilt $A = B^{<b} \subseteq B$. Insbesondere ist die Menge $\mathcal{M}$ aller zulässigen Teilmengen von M total geordnet bzgl. $\subseteq$. Wir zeigen, dass $Z := \bigcup_{A \in \mathcal{M}} A \subseteq M$ total geordnet bzgl. $\leq$ ist. Dazu seien $a, b \in Z$. Dann existieren $A, B \in \mathcal{M}$ mit $a \in A$ und $b \in B$. Da $\mathcal{M}$ bzgl. $\subseteq$ total geordnet ist, gilt o. B. d. A. $A \subseteq B$ und $a, b \in B$. Da B total geordnet ist, gilt $a \leq b$ oder $b \leq a$. Sei nun $a \in A \in \mathcal{M}$. Wegen $A \subseteq Z$ ist $A^{<a} \subseteq Z^{<a}$. Zum Beweis der umgekehrten Inklusion sei $b \in Z^{<a}$, d. h. insbesondere $b < a$.

Annahme: $b \notin A$.
Sei $b \in B \in \mathcal{M}$. Dann ist $B \nsubseteq A$, d. h. $A = B^{<c}$ für ein $c \in B$ nach dem ersten Teil des Beweises. Dann hat man den Widerspruch $b \geq c > a$.

Also ist $A^{<a} = Z^{<a}$. Wir zeigen nun, dass Z wohlgeordnet ist. Sei dafür $\varnothing \neq X \subseteq Z$. Dann existiert ein $A \in \mathcal{M}$ mit $X \cap A \neq \varnothing$ und ein kleinstes Element x in $X \cap A$. Also enthält $Z^x = A^x$ keine Elemente aus X, d. h. x ist das kleinste Element in X. Schließlich zeigen wir $Z \in \mathcal{M}$. Dazu sei $a \in A \in \mathcal{M}$. Dann ist $Z^{<a} = A^{<a}$ und $a = f(A^{<a}) = f(Z^{<a})$. Also ist Z zulässig. Dann ist aber auch $Z \cup \{f(Z)\}$ zulässig im Widerspruch zu $f(Z) \notin Z$. □

Bemerkung II.4.7. Lemma II.4.6 gilt auch in der dualen Version für untere Schranken und minimale Elemente, indem man $\leq$ durch $\geq$ ersetzt.

Satz II.4.8 (Wohlordnungssatz)**.** *Jede Menge kann wohlgeordnet werden.*

[1] Ein etwas kürzerer Beweis steht in meinem Algebra-Skript.

Beweis. Sei M eine Menge und $\mathcal{M}$ die Menge aller Paare $(N, \leq_N)$, wobei $N \subseteq M$ durch $\leq_N$ wohlgeordnet ist. Da die leere Menge wohlgeordnet ist, ist $\mathcal{M} \neq \varnothing$. Durch

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

ist $\mathcal{M}$ geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ total geordnet und $S := \bigcup_{(N,\leq_N)\in\mathcal{N}} N \subseteq M$. Für $x, y \in S$ existieren $(N_1, \leq_1), (N_2, \leq_2) \in \mathcal{N}$ mit $x \in N_1$ und $y \in N_2$. Da $\mathcal{N}$ total geordnet ist, gilt o. B. d. A. $N_1 \subseteq N_2$. Wir definieren

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

Ist auch $(N_3, \leq_3) \in \mathcal{N}$ mit $x, y \in N_3$, so gilt $(N_2, \leq_2) \leq (N_3, \leq_3)$ oder $(N_3, \leq_3) \leq (N_2, \leq_2)$, da $\mathcal{N}$ total geordnet ist. Wegen $\leq_2 \subseteq \leq_3$ oder $\leq_3 \subseteq \leq_2$ gilt dann $x \leq_2 y \Leftrightarrow x \leq_3 y$. Daher hängt $\leq_S$ nicht von der Wahl von N_2 ab. Man zeigt leicht, dass $(S, \leq_S)$ eine geordnete Menge ist. Sei $\varnothing \neq T \subseteq S$ und $(N, \leq_N) \in \mathcal{N}$ mit $T \cap N \neq \varnothing$. Sei x das kleinste Element von $T \cap N$ bzgl. $\leq_N$. Sei $y \in T$ beliebig. Dann existiert $(N_1, \leq_1) \in \mathcal{N}$ mit $y \in N_1$. Im Fall $y \in N$ ist $x \leq_N y$ und $x \leq_S y$. Anderenfalls ist $(N, \leq) < (N_1, \leq_1)$ und $x <_S y$ nach Definition von $\leq$ auf $\mathcal{M}$. Daher ist x das kleinste Element von T und S ist wohlgeordnet. Insgesamt ist $(S, \leq_S) \in \mathcal{M}$ eine obere Schranke von $\mathcal{N}$. Nach Zorns Lemma existiert ein maximales Element $(A, \leq_A) \in \mathcal{M}$. Im Fall $A \neq M$ existiert $b \in M \setminus A$. Dann ist $A \cup \{b\}$ wohlgeordnet, indem man $a < b$ für alle $a \in A$ definiert. Dies widerspricht der Maximalität von $(A, \leq_A)$. Also ist $M = A$ wohlgeordnet. □

Bemerkung II.4.9. Ist $(A_i)_{i\in I}$ eine Familie von nichtleeren Mengen, so lässt sich $\bigcup_{i\in I} A_i$ wohlordnen. Man kann dann für jedes A_i das kleinste Element von A_i auswählen. Auf diese Weise folgt das Auswahlaxiom aus dem Wohlordnungssatz. Daher sind das Auswahlaxiom, Zorns Lemma und der Wohlordnungssatz zueinander äquivalent.

II.5. Ordinalzahlen

Definition II.5.1. Eine Bijektion $f\colon A \to B$ zwischen geordneten Mengen $(A, \leq_A)$ und $(B, \leq_B)$ heißt *Isomorphismus*, falls $a \leq_A a' \iff f(a) \leq_B f(a')$ für alle $a, a' \in A$ gilt. Man nennt A und B dann *isomorph* und schreibt $A \cong B$.

Bemerkung II.5.2. Isomorphe geordnete Mengen haben sicher die gleichen Eigenschaften (total, wohlgeordnet, ...). Jede geordnete Menge ist durch die Identität zu sich selbst isomorph. Außerdem sind Kompositionen und Umkehrabbildungen von Isomorphismen wieder Isomorphismen. Die Isomorphie von geordneten Mengen ist daher eine Äquivalenzrelation. Wir bestimmen im Folgenden ein kanonisches Repräsentantensystem für die entsprechenden Äquivalenzklassen.

Lemma II.5.3. *Zwischen wohlgeordneten Mengen A und B existiert höchstens ein Isomorphismus $A \to B$.*

Beweis. Seien $f, g\colon A \to B$ Isomorphismen und $h := g^{-1} \circ f$. Ist $\{a \in A : h(a) < a\}$ nichtleer, so existiert ein kleinstes Element $a \in A$ mit $h(a) < a$. Da h ein Isomorphismus ist, gilt auch $h(h(a)) < h(a) < a$ im Widerspruch zur Wahl von a. Daher ist $h(a) \geq a$ für alle $a \in A$. Wiederholt man das Argument mit $h^{-1} = f^{-1} \circ g$, so erhält man $h^{-1}(a) \geq a$ also $a \geq h(a) \geq a$ für alle $a \in A$. Dies zeigt $f = g$. □

Definition II.5.4. Eine wohlgeordnete Menge α heißt *Ordinalzahl*, falls $\alpha^{<x} = x$ für alle $x \in \alpha$ gilt.

Bemerkung II.5.5. Sei α eine Ordinalzahl mit Ordnungsrelation $\leq$ und $x, y \in \alpha$. Dann gilt

$$x \leq y \iff \alpha^{<x} \subseteq \alpha^{<y} \iff x \subseteq y,$$

d. h. die Relationen $\leq$ und $\subseteq$ sind identisch. Eine Ordinalzahl ist also bereits durch die Angabe einer Menge eindeutig bestimmt. Außerdem gilt

$$x < y \iff x \in \alpha^{<y} \iff x \in y.$$

Lemma II.5.6. *Für Ordinalzahlen α und β gilt:*

(i) *Jedes $x \in \alpha$ ist eine Ordinalzahl.*

(ii) $\beta \in \alpha \iff \beta \subsetneq \alpha$.

(iii) $\alpha \subseteq \beta$ *oder* $\beta \subseteq \alpha$.

(iv) $\alpha \cong \beta \Longrightarrow \alpha = \beta$.

Beweis.

(i) Wegen $x = \alpha^{<x} \subseteq \alpha$ ist x wohlgeordnet. Für $y \in x$ gilt $x^{<y} = (\alpha^{<x})^{<y} = \alpha^{<y} = y$.

(ii) Für $\beta \in \alpha$ gilt $\beta = \alpha^{<\beta} \subseteq \alpha \setminus \{\beta\} \subsetneq \alpha$. Sei nun umgekehrt $\beta \subsetneq \alpha$. Sei x das kleinste Element von $\alpha \setminus \beta$. Dann gilt $x = \alpha^{<x} \subseteq \beta$. Für $y \in \beta$ gilt umgekehrt $\beta^{<y} = y = \alpha^{<y}$. Im Fall $y > x$ wäre $x \in \alpha^{<y} \subseteq \beta$. Also ist $y \leq x$ und $y < x$ wegen $x \notin \beta$. Dies zeigt $\beta \subseteq \alpha^{<x} = x$. Also ist $\beta = x \in \alpha$.

(iii) O. B. d. A. sei $\alpha \nsubseteq \beta$. Sei x das kleinste Element von $\alpha \setminus \beta$. Dann ist $x = \alpha^{<x} \subseteq \beta$. Im Fall $x \subsetneq \beta$ folgt der Widerspruch $x \in \beta$ aus (i) und (ii). Also ist $\beta = \alpha^{<x} \subseteq \alpha$.

(iv) Sei $f\colon \alpha \to \beta$ ein Isomorphismus und $A := \{x \in \alpha : f(x) \neq x\}$. Angenommen A besitzt ein kleinstes Element x. Dann ergibt sich der Widerspruch

$$f(x) = f(\alpha^{<x}) = \{f(x') : x' < x\} = \{x' : x' < x\} = \alpha^{<x} = x.$$

Also ist $M = \varnothing$. □

Lemma II.5.7. *Sei A eine wohlgeordnete Menge, sodass $A^{<x}$ für alle $x \in A$ zu einer Ordinalzahl isomorph ist. Dann ist A selbst zu einer Ordinalzahl isomorph.*

Beweis. Für $x \in A$ sei α_x die nach Lemma II.5.6 eindeutig bestimmte Ordinalzahl mit $A^{<x} \cong \alpha_x$. Nach Lemma II.5.3 existiert genau ein Isomorphismus $f_x : A^{<x} \to \alpha_x$. Wir zeigen, dass

$$\begin{aligned} f\colon A &\to \{\alpha_x : x \in A\} =: M, \\ x &\mapsto \alpha_x \end{aligned}$$

ein Isomorphismus ist, wobei M durch $\subseteq$ geordnet ist. Für $y < x$ gilt $A^{<y} \subseteq A^{<x}$. Einschränken von f_x liefert einen Isomorphismus

$$A^{<y} \to f_x(A^{<y}) = \alpha_x^{<f_x(y)} = f_x(y) \in \alpha_x.$$

Nach Lemma II.5.6 ist $f_x(y)$ eine Ordinalzahl und es folgt $f_x(y) = \alpha_y$. Dies zeigt $\alpha_y \subsetneq \alpha_x$. Also ist f ein Isomorphismus. Mit A ist auch M wohlgeordnet. Für $\alpha_x \in M$ gilt

$$M^{\alpha_x} = \{\alpha_y : \alpha_y \subsetneq \alpha_x\} = \{f_x(y) : y \in A^{<x}\} = f_x(A^{<x}) = \alpha_x.$$

Also ist M eine Ordinalzahl. □

Satz II.5.8. *Jede wohlgeordnete Menge ist zu genau einer Ordinalzahl isomorph.*

Beweis. Die Eindeutigkeit folgt aus Lemma II.5.6. Nach Lemma II.5.7 genügt es zu zeigen, dass alle $A^{<x}$ ($x \in A$) zu Ordinalzahlen isomorph sind. Sei $x \in A$ minimal, sodass $A^{<x}$ zu keiner Ordinalzahl isomorph ist. Für alle $y \in A^{<y}$ ist $(A^{<x})^{<y} = A^{<y}$ zu einer Ordinalzahl isomorph. Nach Lemma II.5.7 wäre dann aber $A^{<x}$ selbst zu einer Ordinalzahl isomorph. □

Bemerkung II.5.9. Man kann Ordinalzahlen daher als Repräsentanten für die Isomorphieklassen von wohlgeordneten Mengen ansehen.

Lemma II.5.10. *Für jede Ordinalzahl α ist auch der* Nachfolger $\alpha^+ := \alpha \cup \{\alpha\}$ *eine Ordinalzahl.*

Beweis. Wie üblich ist α^+ durch $\subseteq$ geordnet. Sei $\varnothing \neq A \subseteq \alpha'$. Im Fall $A = \{\alpha\}$ ist α das kleinste Element von A. Anderenfalls ist das kleinste Element von $A \cap \alpha$ auch das kleinste Element von A. Also ist α' wohlgeordnet. Für $x \in \alpha$ ist $(\alpha^+)^{<x} = \alpha^{<x} = x$. Für $x = \alpha$ ist $(\alpha^+)^{<x} = \alpha = x$. Somit ist α^+ eine Ordinalzahl. □

Beispiel II.5.11. Die einzigen endlichen Ordinalzahlen sind die *natürlichen Zahlen*

$$0 := \varnothing, \qquad 1 := 0^+ = \{\varnothing\}, \qquad 2 := 1^+ = \{\varnothing, \{\varnothing\}\}, \qquad \ldots.$$

Diese Zahlen stimmen mit ihrer (gewohnten) Mächtigkeit überein. Die kleinste unendliche Ordinalzahl ist die Menge der natürlichen Zahlen $\mathbb{N} := \{0, 1, \ldots\}$ (Unendlichkeitsaxiom). Die transfinite Induktion wird für $\mathbb{N}$ zur *vollständigen Induktion*. Wir setzen $\mathbb{N}_+ := \mathbb{N} \setminus \{0\}$.

II.6. Kardinalzahlen

Satz II.6.1. *Jede Menge von Ordinalzahlen ist wohlgeordnet bzgl. $\subseteq$.*

Beweis. Eine Menge $\mathcal{M}$ von Ordinalzahlen ist nach Lemma II.5.6 total geordnet bzgl. $\subseteq$. Angenommen $\mathcal{M}$ enthält Elemente $\alpha_1 \supsetneq \alpha_2 \supsetneq \ldots$. Aus Lemma II.5.6 folgt $\alpha_2, \alpha_2, \ldots \in \alpha_1$. Dann kann α_1 aber nicht wohlgeordnet (bzgl. $\subseteq$) sein. □

Bemerkung II.6.2 (Burali-Forti-Paradoxon)**.** Die Gesamtheit $\mathcal{M}$ aller Ordinalzahlen ist keine Menge: Anderenfalls wäre $\mathcal{M}$ nach Satz II.6.1 wohlgeordnet. Für $\alpha \in \mathcal{M}$ gilt dann

$$\mathcal{M}^\alpha = \{\beta \in \mathcal{M} : \beta \subsetneq \alpha\} \overset{II.5.6}{=} \{\beta \in \mathcal{M} : \beta \in \alpha\} = \alpha,$$

d. h. $\mathcal{M}$ ist selbst eine Ordinalzahl. Damit hat man den Widerspruch $\mathcal{M} \in \mathcal{M}$, d. h. $\mathcal{M} \subsetneq \mathcal{M}$.

Definition II.6.3. Jede Menge M kann nach dem Wohlordnungssatz wohlgeordnet werden. Nach Satz II.5.8 ist M mit dieser Wohlordnung zu einer Ordinalzahl isomorph. Sei $\mathcal{M}$ die Menge aller Ordinalzahlen, die bzgl. irgendeiner Ordnung zu M isomorph sind. Nach Satz II.6.1 besitzt $\mathcal{M}$ ein kleinstes Element, welches man als *Kardinalzahl* $|M|$ von M bezeichnet. Wir verwenden Frakturbuchstaben wie $\mathfrak{a}$ für Kardinalzahlen, um sie von Ordinalzahlen zu unterscheiden.

Bemerkung II.6.4.

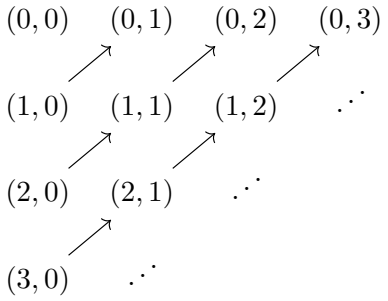
(i) Als Ordinalzahlen lassen sich Kardinalzahlen $\mathfrak{a}$ und $\mathfrak{b}$ stets vergleichen, d. h. es gilt $\mathfrak{a} \subseteq \mathfrak{b}$ oder $\mathfrak{b} \subseteq \mathfrak{a}$. Wir schreiben dann $\mathfrak{a} \leq \mathfrak{b}$ bzw. $\mathfrak{b} \leq \mathfrak{a}$. Für beliebige Mengen A und B ist die Ungleichung $|A| \leq |B|$ äquivalent zur Existenz einer injektiven Abbildung $A \to B$. Der Satz von Cantor-Bernstein ist daher nichts weiter als die Antisymmetrie von $\leq$.

(ii) Für jede Kardinalzahl $\mathfrak{a}$ gilt $|\mathfrak{a}| = \mathfrak{a}$.

(iii) Alle natürlichen Zahlen und $\mathbb{N}$ selbst sind Kardinalzahlen.

(iv) Eine Menge M heißt *abzählbar* (bzw. *überabzählbar*), falls $|M| = \mathbb{N}$ (bzw. $|M| > \mathbb{N}$). Im ersten Fall lassen sich die Elemente von M mit $\mathbb{N}$ indizieren, d. h. $M = \{a_0, a_1, \ldots\}$.

Beispiel II.6.5. Die Abbildung $f\colon \mathbb{N}^+ \to \mathbb{N}$ mit $f(\mathbb{N}) := 0$ und $f(n) := n^+$ für $n \in \mathbb{N}$ ist eine Bijektion. Dies zeigt $|\mathbb{N}^+| = \mathbb{N}$. Insbesondere ist $\mathbb{N}^+$ eine Ordinalzahl, aber keine Kardinalzahl. Die Menge $\mathbb{N} \times \mathbb{N}$ lässt sich „diagonal“ aufzählen, indem man Paare mit konstanter Summe nummeriert:



Die zugrunde liegende Bijektion

$$\mathbb{N}^2 \to \mathbb{N}, \qquad (n, m) \mapsto m + \sum_{k=0}^{n+m} k = m + \frac{(n+m)(n+m+1)}{2}$$

nennt man *Cantorsche Paarungsfunktion*. Eine andere Bijektion findet man in Aufgabe II.5. Insbesondere ist $|\mathbb{N} \times \mathbb{N}| = \mathbb{N}$.

Satz II.6.6. *Zwei Mengen sind genau dann gleichmächtig, wenn sie die gleiche Kardinalzahl besitzen.*

Beweis. Seien A und B Mengen. Gilt $|A| = |B|$, so sind A und B gleichmächtig. Sind umgekehrt A und B gleichmächtig, so sind auch $|A|$ und $|B|$ gleichmächtig. Sei $f\colon |A| \to |B|$ eine Bijektion. Für $x, y \in |A|$ gilt dann

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

Daher ist f ein Isomorphismus. Aus Lemma II.5.6 folgt $|A| = |B|$. □

II.7. Arithmetik von Kardinalzahlen

Definition II.7.1. Für Kardinalzahlen $\mathfrak{a}$ und $\mathfrak{b}$ definieren wir

$$\mathfrak{a} + \mathfrak{b} := |\mathfrak{a} \cup (1 \times \mathfrak{b})|, \qquad \mathfrak{a} \cdot \mathfrak{b} := |\mathfrak{a} \times \mathfrak{b}|,$$
$$\mathfrak{a}^{\mathfrak{b}} := |\{\mathfrak{b} \to \mathfrak{a}\}|, \qquad \mathfrak{a}! := |\operatorname{Sym}(\mathfrak{a})|.$$

Man sagt: $\mathfrak{a}$ *plus* $\mathfrak{b}$, $\mathfrak{a}$ *mal* $\mathfrak{b}$, $\mathfrak{a}$ *hoch* $\mathfrak{b}$ und $\mathfrak{a}$ *Fakultät*.

Bemerkung II.7.2.

(i) Die Konstruktion $1 \times \mathfrak{b}$ bewirkt, dass $\mathfrak{a}$ und $1 \times \mathfrak{b}$ stets disjunkt sind (beachte: $\mathfrak{a} \subseteq \mathfrak{b}$ oder $\mathfrak{b} \subseteq \mathfrak{a}$). Die Notation $\mathfrak{a}^{\mathfrak{b}}$ ist doppeldeutig, denn sie bezeichnet sowohl die Menge aller Abbildungen $\mathfrak{b} \to \mathfrak{a}$ als auch deren Kardinalzahl.

(ii) Für eine beliebige Familie von Kardinalzahlen $(\mathfrak{a}_i)_{i \in I}$ definiert man allgemeiner

$$\sum_{i \in I} \mathfrak{a}_i := \Big|\bigcup_{i \in I} \{i\} \times \mathfrak{a}_i\Big|, \qquad \prod_{i \in I} \mathfrak{a}_i := \Big|\bigtimes_{i \in I} \mathfrak{a}_i\Big|.$$

Sind alle $\mathfrak{a}_i \neq 0$, so zeigt das Auswahlaxiom $\prod_{i \in I} \mathfrak{a}_i \neq 0$. Für Kardinalzahlen $\mathfrak{a}$ und $\mathfrak{b}$ gilt $\sum_{a \in \mathfrak{a}} \mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$ und $\prod_{a \in \mathfrak{a}} \mathfrak{b} = \mathfrak{b}^{\mathfrak{a}}$ (Beispiel II.3.2). Nach Beispiel II.6.5 ist eine abzählbare Vereinigung abzählbarer Mengen abzählbar.

(iii) Um Klammern zu sparen, verabreden wir im Folgenden Punkt- vor Strichrechnung, d. h. $\mathfrak{a} \cdot \mathfrak{b} + \mathfrak{c} := (\mathfrak{a} \cdot \mathfrak{b}) + \mathfrak{c}$.

Satz II.7.3. *Für Mengen A und B gilt*

(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) $|\operatorname{Sym}(A)| = |A|!$.

Beweis. Für die Konstruktion geeigneter Bijektionen (Satz II.6.6) kann man annehmen, dass A und B Kardinalzahlen sind. Dann sind (ii), (iii) und (v) erledigt. Für (i) benutzt man die Bijektion $f\colon (A \cup B) \cup (1 \times (A \cap B)) \to A \cup (1 \times B)$ mit

$$f(x) := \begin{cases} x & \text{falls } x \in A \setminus B, \\ (0, x) & \text{falls } x \in B, \end{cases}$$
$$f(0, x) := x \qquad (x \in A \cap B).$$

Für (iv) benutzt man die Bijektion $f\colon \mathcal{P}(A) \to 2^A$, $B \mapsto f_B$ mit

$$f_B(x) := \begin{cases} 1 & \text{falls } x \in B, \\ 0 & \text{falls } x \notin B. \end{cases}$$

□

Satz II.7.4. *Für Kardinalzahlen* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *gelten folgende Rechenregeln:*

$$\begin{array}{ccc}
\mathfrak{a} + 0 = 0, & \mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}, & (\mathfrak{a} + \mathfrak{b}) + \mathfrak{c} = \mathfrak{a} + (\mathfrak{b} + \mathfrak{c}), \\
\mathfrak{a} \cdot 1 = \mathfrak{a}, & \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a}, & (\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c}), \\
\mathfrak{a}^0 = 1, & \mathfrak{a}^1 = \mathfrak{a}, & 1^{\mathfrak{a}} = 1, \\
\mathfrak{a}^{\mathfrak{b}+\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b}} \cdot \mathfrak{a}^{\mathfrak{c}}, & (\mathfrak{a} \cdot \mathfrak{b})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{c}} \cdot \mathfrak{b}^{\mathfrak{c}}, & (\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} = \mathfrak{a}^{\mathfrak{b} \cdot \mathfrak{c}}, \\
\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}, & 0! = 1, & (\mathfrak{a} + 1)! = \mathfrak{a}! \cdot (\mathfrak{a} + 1).
\end{array}$$

Beweis. Die meisten Behauptungen sind offensichtlich. Wir zeigen nur die Folgenden:

- $\mathfrak{a}^0 = |\{\varnothing \to \mathfrak{a}\}| = \{\varnothing\} = 1$.
- Die Abbildung $\mathfrak{a}^{\mathfrak{b}} \cdot \mathfrak{a}^{\mathfrak{c}} \to \mathfrak{a}^{\mathfrak{b}+c}$, $(f, g) \mapsto h$ mit

  $$h(x) := \begin{cases} f(x) & \text{falls } x \in \mathfrak{b}, \\ g(x) & \text{falls } x \in \mathfrak{c} \end{cases}$$

  ist eine Bijektion.
- Die Abbildung $\mathfrak{a}^{\mathfrak{c}} \cdot \mathfrak{b}^{\mathfrak{c}} \to (\mathfrak{a} \cdot \mathfrak{b})^{\mathfrak{c}}$, $(f, g) \mapsto h$ mit

  $$g(x) := (f(x), g(x))$$

  für $x \in \mathfrak{c}$ ist eine Bijektion.
- Die Abbildung $(\mathfrak{a}^{\mathfrak{b}})^{\mathfrak{c}} \to \mathfrak{a}^{\mathfrak{b} \cdot \mathfrak{c}}$, $f \mapsto g$ mit

  $$g(x, y) := (f(y))(x)$$

  ist eine Bijektion.
- $0! = |\operatorname{Sym}(\varnothing)| = |\{\varnothing \to \varnothing\}| = 0^0 = 1$.
- Sei $A := \mathfrak{a} \cup \{x\}$ mit $|A| = \mathfrak{a} + 1$. Dann ist die Abbildung $A \times \operatorname{Sym}(\mathfrak{a}) \to \operatorname{Sym}(A)$, $(a, f) \mapsto g$ mit

  $$g(y) := \begin{cases} a & \text{falls } y = x, \\ f(y) & \text{falls } y \neq x \end{cases} \qquad (y \in A)$$

  eine Bijektion. □

Bemerkung II.7.5. Für $\mathfrak{a} > 0$ gilt $0^{\mathfrak{a}} = |\{\mathfrak{a} \to \varnothing\}| = |\varnothing| = 0$.

Satz II.7.6. *Für Kardinalzahlen* $\mathfrak{a} \leq \mathfrak{b}$ *und* $\mathfrak{c} \leq \mathfrak{d}$ *gilt:*

(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) $\mathfrak{a}^{\mathfrak{c}} \leq \mathfrak{b}^{\mathfrak{d}}$ *falls* $\mathfrak{a} + \mathfrak{c} > 0$.

Beweis.

(i) Die injektive Abbildung $\mathfrak{a} \to \mathcal{P}(\mathfrak{a})$, $x \mapsto \{x\}$ zeigt $\mathfrak{a} \leq |\mathcal{P}(\mathfrak{a})| = 2^{\mathfrak{a}}$. Nehmen wir nun an, dass eine Bijektion $f\colon \mathfrak{a} \to \mathcal{P}(\mathfrak{a})$ existiert. Sei $A := \{x \in \mathfrak{a} : x \notin f(x)\} \in \mathcal{P}(\mathfrak{a})$. Dann existiert ein $x \in \mathfrak{a}$ mit $f(x) = A$. Es folgt der Widerspruch $x \in A = f(x) \Leftrightarrow x \notin f(x)$.

(ii) Es gilt $\mathfrak{a} \cup (1 \times \mathfrak{c}) \subseteq \mathfrak{b} \times (1 \times \mathfrak{d})$.

(iii) Es gilt $\mathfrak{a} \times \mathfrak{c} \subseteq \mathfrak{b} \times \mathfrak{d}$.

(iv) Im Fall $\mathfrak{a} = 0$ ist $\mathfrak{c} > 0$ und $\mathfrak{a}^{\mathfrak{c}} = 0 \leq \mathfrak{b}^{\mathfrak{d}}$ nach Bemerkung II.7.5. Sei also $\mathfrak{a} > 0$ und $x \in \mathfrak{a}$. Dann lässt sich jede Abbildung $f\colon \mathfrak{c} \to \mathfrak{a}$ zu $\hat{f}\colon \mathfrak{d} \to \mathfrak{b}$ fortsetzen, indem man $\hat{f}(y) = x$ für $y \in \mathfrak{d} \setminus \mathfrak{c}$ setzt. Dies liefert eine injektive Abbildung $\mathfrak{a}^{\mathfrak{c}} \to \mathfrak{b}^{\mathfrak{d}}$, $f \mapsto \hat{f}$. □

Bemerkung II.7.7.

(i) (Cantors erste Antinomie) Die Gesamtheit $\mathcal{M}$ aller Kardinalzahlen ist keine Menge: Anderenfalls wäre auch $\mathcal{M}' := \bigcup_{\mathfrak{a} \in \mathcal{M}} \mathfrak{a}$ eine Menge und $2^{|\mathcal{M}'|} \subseteq \mathcal{M}'$ in Widerspruch zu $|\mathcal{M}'| < 2^{|\mathcal{M}'|}$.

(ii) (Cantors zweite Antinomie) Die Gesamtheit $\mathcal{M}$ aller Mengen ist keine Menge (gleiches Argument).

(iii) Jede Kardinalzahl $\mathfrak{a}$ besitzt genau einen Nachfolger, nämlich das kleinste Element aus $\{|A| : A \subseteq 2^{\mathfrak{a}},\ |A| > \mathfrak{a}\}$. Traditionell bezeichnet man die ersten unendlichen Kardinalzahlen mit dem hebräischen Buchstaben $\aleph$ (*Aleph*), d. h. $\mathbb{N} =: \aleph_0 < \aleph_1 < \ldots < \aleph_{\mathbb{N}} < \ldots$.

(iv) Den zweiten hebräischen Buchstaben $\beth$ (*Beth*) benutzt man für die Reihe $\beta_0 := \mathbb{N}$, $\beta_1 := 2^{\mathbb{N}}, \ldots$.

(v) Die *Kontinuumshypothese* besagt, dass keine Kardinalzahl echt zwischen $\mathbb{N}$ und $2^{\mathbb{N}}$ liegt, d. h. $\aleph_1 = \beth_1$. Dies lässt sich in $\mathcal{ZF}$ weder beweisen noch widerlegen. Die *verallgemeinerte Kontinuumshypothese* besagt allgemeiner $\aleph_\alpha = \beth_\alpha$ für alle Ordinalzahlen α.

(vi) In $\mathcal{ZF}$ kann man weder beweisen noch widerlegen, dass es sogenannte *unerreichbare* Kardinalzahlen $\mathfrak{a}$ mit folgenden Eigenschaften gibt:

- $\mathfrak{a} > \mathbb{N}$.
- $\mathfrak{a}$ hat keinen Vorgänger, d. h. $\mathfrak{b} < \mathfrak{a} \Rightarrow \mathfrak{b}^+ < \mathfrak{a}$.
- Für eine Indexmenge I mit $|I| < \mathfrak{a}$ und Kardinalzahlen $\mathfrak{a}_i < \mathfrak{a}$ ist $\sum_{i \in I} \mathfrak{a}_i < \mathfrak{a}$.

Satz II.7.8 (Cantor). *Seien $\mathfrak{a}$ und $\mathfrak{b}$ Kardinalzahlen mit $\mathfrak{a} \leq \mathfrak{b} \geq \mathbb{N}$. Dann gilt*

(i) $\mathfrak{a} + \mathfrak{b} = \mathfrak{b}$,

(ii) $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b}$ *falls* $\mathfrak{a} > 0$,

(iii) $\mathfrak{a}^{\mathfrak{b}} = 2^{\mathfrak{b}}$ *falls* $\mathfrak{a} > 1$,

(iv) $\mathfrak{b}! = 2^{\mathfrak{b}}$

Beweis.

(i) Ist $\mathfrak{a}$ endlich, so liefert $f\colon \mathfrak{a} \cup (1 \times \mathfrak{b}) \to \mathfrak{b}$ mit

$$f(x) := \begin{cases} x + \mathfrak{a} & \text{falls } x \in \mathbb{N} \setminus \mathfrak{a}, \\ x & \text{sonst} \end{cases}$$

die gewünschte Bijektion (beachte: $\mathfrak{a} \subseteq \mathbb{N} \subseteq \mathfrak{b}$). Sei nun $\mathfrak{a}$ unendlich. Wegen $\mathfrak{b} \leq \mathfrak{a} + \mathfrak{b} \leq \mathfrak{b} + \mathfrak{b}$ (Satz II.7.6) können wir $\mathfrak{a} = \mathfrak{b}$ annehmen. Es genügt, eine Bijektion $2 \times \mathfrak{b} \to \mathfrak{b}$ zu konstruieren. Im Fall $\mathfrak{b} = \mathbb{N}$ betrachte man $(0, n) \to 2 \cdot n$ und $(1, n) \to 2 \cdot n + 1$ für $n \in \mathbb{N}$. Sei nun $\mathfrak{b}$ überabzählbar und $\mathcal{M}$ die Menge aller Paare (B, α), wobei $B \subseteq \mathfrak{b}$ und $\alpha \colon 2 \times B \to B$ eine Bijektion ist. Wegen $\mathbb{N} \subseteq \mathfrak{b}$ ist $\mathcal{M}$ nichtleer und durch

$$(B, \alpha) \leq (B', \alpha') \ :\Longleftrightarrow\ B \subseteq B',\ \alpha'_{|2 \times B} = \alpha$$

geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ total geordnet. Dann ist $C := \bigcup_{(B,\alpha) \in \mathcal{N}} B \subseteq \mathfrak{b}$. Wir definieren $\beta \colon 2 \times C \to C$ durch $\beta(x) = \alpha(x)$ falls $x \in 2 \times B$ und $(B, \alpha) \in \mathcal{N}$. Offenbar ist β wohldefiniert und bijektiv. Daher ist $(C, \beta) \in \mathcal{M}$ eine obere Schranke von $\mathcal{N}$. Nach Zorns Lemma besitzt $\mathcal{M}$ ein maximales Element (B, α). Enthält $\mathfrak{b} \setminus B$ eine abzählbare Teilmenge C, so existiert wie oben eine Bijektion $2 \times C \to C$ und wir können α nach $2 \times (B \cup C)$ fortsetzen. Dies widerspricht der Maximalität von (B, α). Also ist $\mathfrak{b} \setminus B$ endlich. Wie oben ist dann $\mathfrak{b} = |B| + |\mathfrak{b} \setminus B| = B$ und wir sind fertig.

(ii) Wegen $\mathfrak{b} = 1 \times \mathfrak{b} \leq \mathfrak{a} \times \mathfrak{b} \leq \mathfrak{b} \times \mathfrak{b}$ können wir $\mathfrak{a} = \mathfrak{b}$ annehmen. Es genügt, eine Bijektion $\mathfrak{b} \times \mathfrak{b} \to \mathfrak{b}$ zu konstruieren. Der Fall $\mathfrak{b} = \mathbb{N}$ wurde in Beispiel II.6.5 erledigt. Sei nun $\mathfrak{b}$ überabzählbar und $\mathcal{M}$ die Menge aller Paare (B, α), wobei $B \subseteq \mathfrak{b}$ und $\alpha \colon B \times B \to B$ eine Bijektion ist. Wegen $\mathbb{N} \subseteq \mathfrak{b}$ ist $\mathcal{M}$ nichtleer und durch

$$(B, \alpha) \leq (B', \alpha') \ :\Longleftrightarrow\ B \subseteq B',\ \alpha'_{|B \times B} = \alpha$$

geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ total geordnet. Dann ist $C := \bigcup_{(B,\alpha) \in \mathcal{N}} B \subseteq \mathfrak{b}$. Wir definieren $\beta \colon C \times C \to C$ durch $\beta(x) = \alpha(x)$ falls $x \in B \times B$ und $(B, \alpha) \in \mathcal{N}$. Offenbar ist β wohldefiniert und bijektiv. Daher ist $(C, \beta) \in \mathcal{M}$ eine obere Schranke von $\mathcal{N}$. Nach Zorns Lemma besitzt $\mathcal{M}$ ein maximales Element (B, α). Im Fall $B < \mathfrak{b}$ ist $\mathfrak{b} = |B| + |\mathfrak{b} \setminus B| = |\mathfrak{b} \setminus B|$ nach (i). Insbesondere existiert $C \subseteq \mathfrak{b} \setminus B$ mit $|C| = |B|$. Wegen $|C \times C| = |B \cdot B| = |B| = |C| = |B \times C| = |C \times B|$ und $|B \cup C| = |B| + |C| = |C| + |C| \overset{\text{(i)}}{=} |C|$ existiert eine Bijektion

$$(B \times C) \cup (C \times B) \cup (C \times C) \to C.$$

Also lässt sich α zu

$$(B \cup C) \times (B \cup C) = (B \times B) \cup (B \times C) \cup (C \times B) \cup (C \times C)$$

fortsetzen. Dies widerspricht der Maximalität von (B, α). Also ist $\mathfrak{b} = B$ und wir sind fertig.

(iii) Nach (ii) gilt $2^{\mathfrak{b}} \leq \mathfrak{a}^{\mathfrak{b}} \leq \mathfrak{b}^{\mathfrak{b}} \leq (2^{\mathfrak{b}})^{\mathfrak{b}} = 2^{\mathfrak{b} \cdot \mathfrak{b}} = 2^{\mathfrak{b}}$.

(iv) Wegen $\mathfrak{b}! = |\operatorname{Sym}(\mathfrak{b})| \leq |\mathcal{P}(\mathfrak{b} \times \mathfrak{b})| = |\mathcal{P}(\mathfrak{b})| = 2^{\mathfrak{b}}$ genügt es eine injektive Abbildung $f \colon \mathcal{P}(\mathfrak{b}) \to \operatorname{Sym}(2 \times \mathfrak{b})$, $B \mapsto f_B$ zu konstruieren. Dies ist durch

$$f_B(i, x) := \begin{cases} (1, x) & \text{falls } i = 0, x \in B, \\ (0, x) & \text{falls } i = 1, x \in B, \\ (i, x) & \text{falls } x \notin B \end{cases}$$

getan. □

Bemerkung II.7.9. Die Potenzierung beliebiger Kardinalzahlen lässt sich nicht immer vereinfachen.

Satz II.7.10 (König). *Seien $(\mathfrak{a}_i)_{i\in I}$ und $(\mathfrak{b}_i)_{i\in I}$ Familien von Kardinalzahlen mit $\mathfrak{a}_i < \mathfrak{b}_i$ für alle $i \in I$. Dann gilt*

$$\sum_{i\in I} \mathfrak{a}_i < \prod_{i\in I} \mathfrak{b}_i.$$

Beweis. Nach dem Auswahlaxiom existieren $y_i \in \mathfrak{b}_i \setminus \mathfrak{a}_i$ für alle $i \in I$. Dann ist die Abbildung $\bigcup_{i\in I}\{i\} \times \mathfrak{a}_i \to \bigtimes_{i\in I} \mathfrak{b}_i$, $(j, x) \mapsto f$ mit

$$f(i) := \begin{cases} x & \text{falls } i = j, \\ y_i & \text{falls } i \neq j \end{cases}$$

injektiv. Dies zeigt $\sum_{i\in I} \mathfrak{a}_i \leq \prod_{i\in I} \mathfrak{b}_i$. Nehmen wir an, es existiert eine Bijektion

$$\begin{aligned} \alpha\colon \bigcup_{i\in I}\{i\} \times \mathfrak{a}_i &\to \bigtimes_{i\in I} \mathfrak{b}_i, \\ (i, x) &\mapsto \alpha_x. \end{aligned}$$

Für $i \in I$ ist $|\{\alpha_x(i) : x \in \mathfrak{a}_i\}| \leq \mathfrak{a}_i < \mathfrak{b}_i$. Daher existieren $f(i) \in \mathfrak{b}_i \setminus \{\alpha_x(i) : x \in \mathfrak{a}_i\}$ für alle $i \in I$. Dann wäre aber $f \in \bigtimes_{i\in I} \mathfrak{b}_i$ nicht im Bild von α. □

Definition II.7.11. Für eine Menge A und $\sigma \in \operatorname{Sym}(A)$ sei $\operatorname{supp}\sigma := \{a \in A : \sigma(a) \neq a\} \subseteq A$ der *Träger* von σ.

Satz II.7.12. *Für jede unendliche Menge A gilt*

$$\begin{aligned} |\{B \subseteq A : |B| < \infty\}| &= |A|, \\ |\{\sigma \in \operatorname{Sym}(A) : |\operatorname{supp}\sigma| < \infty\}| &= |A|. \end{aligned}$$

Beweis. Es gilt

$$|A| = |\{\{a\} : a \in A\}| \leq |\{B \subseteq A : |B| < \infty\}| \leq \left|\bigcup_{n\in\mathbb{N}} A^n\right| \leq \sum_{n\in\mathbb{N}} |A|^n = \sum_{n\in\mathbb{N}} |A| = |\mathbb{N}| \cdot |A| = |A|.$$

Daraus folgt

$$|\{\sigma \in \operatorname{Sym}(A) : |\operatorname{supp}\sigma| < \infty\}| \leq \sum_{\substack{B,C\subseteq A,\\ |B|=|C|<\infty}} |\{B \to C\}| \leq \Big(\sum_{\substack{B\subseteq A,\\ |B|<\infty}} |B|^2\Big)^2 \leq (|A| \cdot |\mathbb{N}|^2)^2 = |A|. \quad \square$$

Bemerkung II.7.13.

(i) Man kann auch auf Ordinalzahlen Arithmetik betreiben, indem man geeignete Ordnungsrelationen definiert. Für Ordinalzahlen α und β ist $\alpha + \beta = \alpha \cup (1 \times \beta)$ eine Ordinalzahl mit $(1, b) < (1, b') \iff b < b'$ und $a < (1, b)$ für alle $a \in \alpha$ und $b, b' \in \beta$. Analog wird $\alpha \cdot \beta = \alpha \times \beta$ mit der *anti-lexikografischen* Ordnung

$$(a, b) < (a', b') \ :\iff\ b < b' \vee (b = b' \wedge a < a') \qquad (a, a' \in A,\, b, b' \in B)$$

zu einer Ordinalzahl. Schließlich sei α^β die Menge aller Funktionen $f\colon \beta \to \alpha$ mit $|\{b \in \beta : f(b) \neq 0\}| < \infty$. Für $f, g \in \alpha^\beta$ sei

$$f < g \ :\iff\ \exists b \in \beta\big(f(b) < g(b) \wedge \forall c > b\, f(c) = g(c)\big).$$

Dadurch entsteht in der Regel eine kleinere Ordinalzahl als die entsprechende Potenzierung der Kardinalzahlen (Aufgabe II.6). Satz II.7.4 gilt in dieser Allgemeinheit nicht mehr: $1+\mathbb{N} \cong \mathbb{N} \ncong \mathbb{N}+1$ und $2 \cdot \mathbb{N} \cong \mathbb{N} \ncong \mathbb{N} \cdot 2 \cong \mathbb{N} + \mathbb{N}$.

(ii) Mit den Bezeichnungen aus (i) lässt sich jede Ordinalzahl $\alpha > 0$ in die *Cantorsche Normalform*

$$\alpha \cong \mathbb{N}^{\alpha_0} \cdot a_0 + \mathbb{N}^{\alpha_1} \cdot a_1 + \ldots + \mathbb{N}^{\alpha_n} \cdot a_n$$

bringen, wobei $a_0, \ldots, a_n \in \mathbb{N}_+$ und $\alpha_0 < \ldots < \alpha_n \leq \alpha$ eindeutig bestimmte Ordinalzahlen sind (ohne Beweis). Man kann $\mathbb{N}$ in der Normalform durch eine beliebige Ordinalzahl $\beta > 1$ ersetzen, wenn man $a_0, \ldots, a_n < \beta$ fordert. Im Fall $\beta = b \in \mathbb{N}$ erhält man eine Verallgemeinerung der b-adischen Darstellung von natürlichen Zahlen (dann darf man die a_i wie gewohnt auf der linken Seite der b-Potenzen schreiben).[2]

II.8. Konstruktion von $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$

Bemerkung II.8.1. Bisher können wir natürliche Zahlen nur addieren, multiplizieren und potenzieren. Um entsprechende Umkehroperationen zu definieren, müssen wir $\mathbb{N}$ durch größere Mengen ersetzen. Im Folgenden werden wir das Multiplikationssymbol $\cdot$ der Übersicht halber oft einsparen.

Definition II.8.2.

(i) Offenbar definiert

$$(a,b) \sim (c,d) \iff a + d = b + c$$

eine Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$. Die Äquivalenzklassen $[a,b]$ bilden die Menge $\mathbb{Z}$ der *ganzen Zahlen*. Für $[a,b], [c,d] \in \mathbb{Z}$ definieren wir

$$\begin{aligned}
[a,b] + [c,d] &:= [a+c, b+d], \\
[a,b] - [c,d] &:= [a+d, b+c], \\
[a,b] \cdot [c,d] &:= [ac+bd, ad+bc], \\
[a,b] \leq [c,d] &:\Leftrightarrow a + d \leq b + c,
\end{aligned}$$

Man nennt $z \in \mathbb{Z}$ *gerade* (bzw. *ungerade*), falls (k)ein $w \in \mathbb{Z}$ mit $z = w + w$ existiert.

(ii) Offenbar definiert

$$(a,b) \sim (c,d) \iff ad = bc$$

eine Äquivalenzrelation auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. Die Äquivalenzklassen $[a,b]$ bilden die Menge $\mathbb{Q}$ der *rationalen Zahlen*. Für $[a,b], [c,d] \in \mathbb{Q}$ definieren wir

$$\begin{aligned}
[a,b] + [c,d] &:= [ad+bc, bd], \\
[a,b] - [c,d] &:= [ad-bc, bd], \\
[a,b] \cdot [c,d] &:= [ac, bd], \\
[a,b] : [c,d] &:= [ad, bc] \text{ falls } c \neq 0, \\
[a,b] \leq [c,d] &:\Leftrightarrow ad \leq bc.
\end{aligned}$$

[2] Siehe Zahlentheorie-Skript

Bemerkung II.8.3.

(i) Durch $n \mapsto [n, 0]$ kann man $\mathbb{N}$ als Teilmenge von $\mathbb{Z}$ auffassen. Jedes weitere Element aus $\mathbb{Z}$ hat die Form $-n := [0, n]$ für ein $n \in \mathbb{N}$. Es gilt dann $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ und $m - n = m + (-n)$ für $m, n \in \mathbb{Z}$. Insbesondere ist $m - m = 0$.

(ii) Durch $z \mapsto [z, 1]$ kann man $\mathbb{Z}$ in $\mathbb{Q}$ einbetten. Allgemeiner schreibt man $[a, b] \in \mathbb{Q}$ in der Form a/b oder $\frac{a}{b}$. Es gilt dann $a : b = \frac{a}{b}$ für $a, b \in \mathbb{Z}$. Für $q \in \mathbb{Q} \setminus \{0\}$ ist außerdem $q : q = 1$.

(iii) Man zeigt leicht, dass die angegebenen Rechenoperationen wohldefiniert sind und die entsprechenden Operationen auf $\mathbb{N}$ fortsetzen. Für $a \in \mathbb{Q}$ und $z \in \mathbb{Z}$ setzt man zusätzlich

$$a^z := \begin{cases} \prod_{x \in z} a & \text{falls } z \geq 0, \\ \prod_{x \in -z} \frac{1}{a} & \text{falls } z < 0. \end{cases}$$

Es gelten dann die in Satz II.7.4 formulierten Regeln auch in $\mathbb{Q}$ (sofern definiert). Die Ordnungsrelation auf $\mathbb{Q}$ ist total und ebenfalls mit der Ordnung auf $\mathbb{N}$ kompatibel.

Satz II.8.4 (CANTORs erste Diagonalisierung[3])**.** *Die Mengen $\mathbb{Z}$ und $\mathbb{Q}$ sind abzählbar.*

Beweis. Nach Konstruktion ist $\mathbb{Z}$ eine Menge von Äquivalenzklassen auf $\mathbb{N} \times \mathbb{N}$. Durch Wahl eines Repräsentantensystems kann man $\mathbb{Z}$ als Teilmenge von $\mathbb{N} \times \mathbb{N}$ auffassen. Nach Beispiel II.6.5 ist $\mathbb{N} \leq |\mathbb{Z}| \leq |\mathbb{N} \times \mathbb{N}| = \mathbb{N}$. Analog kann man $\mathbb{Q}$ als Teilmenge von $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ auffassen und es folgt $\mathbb{N} \leq |\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = \mathbb{N}$. □

Bemerkung II.8.5.

(i) Die Abbildung

$$\mathbb{N} \to \mathbb{Z}, \qquad n \mapsto \begin{cases} \frac{n}{2} & \text{falls } n \text{ gerade}, \\ -\frac{n+1}{2} & \text{falls } n \text{ ungerade} \end{cases}$$

ist eine explizite Bijektion. Dennoch sind $(\mathbb{N}, \leq)$ und $(\mathbb{Z}, \leq)$ nicht isomorph, denn $\mathbb{N}$ besitzt ein kleinstes Element, aber $\mathbb{Z}$ nicht.

(ii) Die CALKIN-WILF-*Folge* $\mathbb{Q} = \{q_0, q_1, -q_1, q_2, -q_2, \ldots\}$ mit $q_0 := 0$ und

$$q_{n+1} := \frac{1}{2\lfloor q_n \rfloor + 1 - q_n}$$

für $n \in \mathbb{N}$ liefert eine explizite Bijektion $\mathbb{Z} \to \mathbb{Q}$ (ohne Beweis). Dabei ist $\lfloor q \rfloor$ die größte ganze Zahl z mit $z \leq q$. Dennoch ist $(\mathbb{Q}, \leq)$ weder zu $(\mathbb{N}, \leq)$ noch zu $(\mathbb{Z}, \leq)$ isomorph, denn ist $f \colon \mathbb{Q} \to \mathbb{Z}$ ein Isomorphismus, so wäre

$$|\{q \in \mathbb{Q} : 0 \leq q \leq 1\}| = |\{z \in \mathbb{Z} : f(0) \leq z \leq f(1)\}| < \infty.$$

Definition II.8.6. Ein *Dedekind-Schnitt* ist eine Teilmenge $D \subseteq \mathbb{Q}$ mit den Eigenschaften:

- $\varnothing \neq D \neq \mathbb{Q}$,
- D besitzt kein größtes Element,
- $\forall d \in D : \mathbb{Q}^{<d} \subseteq D$.

[3] Der Name ergibt sich aus Beispiel II.6.5.

Die Dedekind-Schnitte bilden die Menge $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$ der *reellen Zahlen*. Durch $q \mapsto \mathbb{Q}^{<q}$ lassen sich die rationalen Zahlen in $\mathbb{R}$ einbetten. Insbesondere ist $0 \in \mathbb{R}$. Für Dedekind-Schnitte D und E definieren wir

$$
\begin{aligned}
D \leq E &:\Leftrightarrow D \subseteq E,\\
D + E &:= \{d + e : d \in D,\ e \in E\},\\
-D &:= \{x \in \mathbb{Q} : \forall d \in D : x < -d\},\\
D - E &:= D + (-E),\\
D \cdot E &:= \begin{cases}
\{x \in \mathbb{Q} : \exists d \in D, e \in E : d > 0, e > 0, x < de\} & \text{falls } D, E > 0,\\
-((-D) \cdot E) & \text{falls } D < 0, E > 0,\\
-(D \cdot (-E)) & \text{falls } D > 0, E < 0,\\
(-D) \cdot (-E) & \text{falls } D, E < 0,\\
0 & \text{falls } D = 0 \vee E = 0,
\end{cases}\\
\frac{1}{D} &:= \begin{cases}
\{x \in \mathbb{Q} : \exists d \in D : d > 0, x < \frac{1}{d}\} & \text{falls } D > 0,\\
-\frac{1}{-D} & \text{falls } D < 0,
\end{cases}\\
D : E &:= D \cdot \frac{1}{E} \qquad \text{falls } E \neq 0.
\end{aligned}
$$

Man nennt $r \in \mathbb{R}$ *positiv* (bzw. *negativ*), falls $r > 0$ (bzw. $r < 0$).

Bemerkung II.8.7. Die Operationen auf $\mathbb{R}$ setzen die Operationen auf $\mathbb{Q}$ fort und es gelten die in Satz II.7.4 formulierten Rechenregeln (soweit definiert). Die Ordnung auf $\mathbb{R}$ ist total und setzt die Ordnung auf $\mathbb{Q}$ fort. Außerdem gilt

$$
\begin{aligned}
a \leq b &\implies a + c \leq b + c,\\
a, b \geq 0 &\implies ab \geq 0
\end{aligned}
\tag{II.8.1}
$$

für alle $a, b, c \in \mathbb{R}$. Damit wird $\mathbb{R}$ ein *angeordneter Körper*.

Lemma II.8.8. *Besitzt $\varnothing \neq M \subseteq \mathbb{R}$ eine obere Schranke, so ist*

$$\sup M := \bigcup_{r \in M} r \in \mathbb{R}$$

die kleinste obere Schranke von M. Man nennt $\sup M$ *das* Supremum *von M.*

Beweis. Ist $s \in \mathbb{R}$ eine obere Schranke von M, so ist s auch eine obere Schranke von $D := \bigcup_{r \in M} r \subseteq \mathbb{Q}$, d. h. $D \subseteq s$. Insbesondere ist $D \neq \mathbb{Q}$. Existiert ein größtes Element x in D, so wäre x auch ein größtes Element von einem $r \in M$. Dies widerspricht der Eigenschaften von Dedekind-Schnitten. Also besitzt D kein größtes Element. Für alle $d \in D$ ist $\mathbb{Q}^{<d} \subseteq D$. Daher ist $D \in \mathbb{R}$ die kleinste obere Schranke von M. □

Lemma II.8.9. *Jede reelle Zahl ist das Supremum rationaler Zahlen, d. h. $\mathbb{Q}$ liegt* dicht *in $\mathbb{R}$.*

Beweis. Sei $r \in \mathbb{R}$. Für $n \in \mathbb{N}$ wählen wir $q_n \in \mathbb{Q}$ maximal mit den Eigenschaften $n! \cdot q_n \in \mathbb{Z}$ und $q_n \in r$. Sicher ist dann $\sup\{q_n : n \in \mathbb{N}\} \leq r$. Sei $x \in r$ beliebig. Da r kein größtes Element besitzt, existiert ein $y \in r$ mit $x < y$. Wir schreiben $r = \frac{k}{m}$ mit $k, m \in \mathbb{Z}$ und $m > 0$. Die Maximalität von q_m zeigt $y \leq q_m$ und $x \in \mathbb{Q}^{<q_m}$. Dies zeigt $r = \sup\{q_n : n \in \mathbb{N}\}$. □

Satz II.8.10 (CANTORs zweite Diagonalisierung)**.** *Es gilt* $|\mathbb{R}| = 2^{\mathbb{N}}$*. Insbesondere ist* $\mathbb{R}$ *überabzählbar.*

Beweis. Wegen $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = 2^{|\mathbb{Q}|} = 2^{\mathbb{N}}$ genügt es eine injektive Abbildung $2^{\mathbb{N}} \to \mathbb{R}$ zu konstruieren. Für $f \in 2^{\mathbb{N}}$ und $n \in \mathbb{N}$ betrachten wir $f_n := \sum_{k=0}^{n} \frac{f(k)}{3^k} \in \mathbb{Q}$. Durch Induktion nach n zeigt man

$$f_n \leq \sum_{k=0}^{n} \frac{1}{3^k} = \frac{3^{n+1}-1}{2 \cdot 3^n} \leq \frac{3}{2}.$$

Daher ist $\frac{3}{2}$ eine obere Schranke von $\{f_n : n \in \mathbb{N}\}$ und nach Lemma II.8.8 existiert

$$S_f := \sup\{f_n : n \in \mathbb{N}\} \in \mathbb{R}.$$

Sei nun $g \in 2^{\mathbb{N}}$ mit $S_g = S_f$. Im Fall $f \neq g$ existiert ein kleinstes $n \in \mathbb{N}$ mit $f(n) \neq g(n)$. O. B. d. A. sei $f(n) = 0$ und $g(n) = 1$. Für alle $m \geq n$ gilt dann

$$f_m + \frac{1}{2 \cdot 3^n} \leq f_m + \frac{3^{m-n}+1}{2 \cdot 3^m} = f_m + \frac{1}{3^n} - \sum_{k=n+1}^{m} \frac{1}{3^k} \leq \sum_{k=0}^{n} \frac{g(k)}{3^k} \leq g_m \leq S_g = S_f.$$

Wegen $f_0 \leq f_1 \leq \ldots \leq f_n$ wäre dann auch $S_f - \frac{1}{2 \cdot 3^n}$ eine obere Schranke von $\{f_k : k \in \mathbb{N}\}$ im Widerspruch zur Minimalität von S_f. Also ist die Abbildung $2^{\mathbb{N}} \to \mathbb{R}$, $f \to S_f$ injektiv. □

Bemerkung II.8.11.

(i) In der Analysis schreibt man

$$\sum_{k=0}^{\infty} \frac{f(k)}{3^n} := \lim_{k \to \infty} f_k := S_f$$

in der Situation des obigen Beweises. Die konstruierte Abbildung $f \mapsto S_f$ bildet nur in die Menge $\{r \in \mathbb{R} : 0 \leq r \leq \frac{3}{2}\}$ ab. Durch Skalierung ist daher bereits jedes *Intervall* $\{r \in \mathbb{R} : a \leq r \leq b\}$ mit $a < b$ überabzählbar.

(ii) Hat man bereits bewiesen, dass sich reelle Zahlen durch unendliche Dezimalentwicklungen schreiben lassen (oder definiert man $\mathbb{R}$ auf diese Weise), so gibt es ein anschauliches Argument für $|\mathbb{R}| > |\mathbb{N}|$: Angenommen $\mathbb{R} = \{r_1, r_2, \ldots\}$. Konstruiere $x = x_1{,}x_2x_3 \ldots$, sodass $x_i - 1$ die i-te Dezimalziffer von r_i ist (für $x_i = 0$ sei $x_i - 1 = 9$). Beispiel:

$$\begin{aligned} r_1 &= \mathbf{1}{,}0000\ldots, \\ r_2 &= 0{,}\mathbf{0}234\ldots, \\ r_3 &= 11{,}4\mathbf{9}02\ldots \\ r_4 &= 3{,}14\mathbf{1}5\ldots \\ &\vdots \\ x &= 2{,}102\ldots \end{aligned}$$

Wegen $x \in \mathbb{R}$ existiert ein $n \in \mathbb{N}$ mit $x = r_n$. Andererseits unterscheiden sich x und r_n an der n-ten Dezimalziffer. Widerspruch. [4]

(iii) Die Zahlen in $\mathbb{R} \setminus \mathbb{Q}$ nennt man *irrational*. Wegen $|\mathbb{R}| = |\mathbb{Q}| + |\mathbb{R} \setminus \mathbb{Q}| = |\mathbb{R} \setminus \mathbb{Q}|$ gibt es „mehr" irrationale Zahlen als rationale. Wir konstruieren ein Beispiel.

[4] Man vergleiche dieses Argument mit dem Beweis von Gödels ersten Unvollständigkeitssatz I.7.6 oder dem Halteproblem Satz I.8.15.

Lemma II.8.12. *Für alle $n \in \mathbb{N}_+$ und $r \in \mathbb{R}$ mit $r > 0$ existiert genau ein $s \in \mathbb{R}$ mit $s > 0$ und $s^n = r$.*

Beweis. Hat man s konstruiert, so gilt $1/s > 0$ und $(1/s)^n = 1/r$. Wir können also $r \geq 1$ annehmen, indem man notfalls r durch $1/r$ ersetzt. Für $r = 1$ wählt man $s = 1$. Sei also $r > 1$. Für jedes $t > r$ ist dann $t^n > r^n$. Daher existiert $s := \sup\{q \in \mathbb{Q} : q^n < r\}$. Nehmen wir zunächst $s^n < r$ an. Für jedes $k \in \mathbb{N}$ existieren nach Lemma II.8.9 $a, b \in \mathbb{Q}$ mit $0 < a < b$, $b - a < \frac{1}{k}$ und $b^n < r$. Es gilt dann

$$b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \ldots + ba^{n-2} + a^{n-1}) < \frac{1}{k} n b^{n-1} \leq \frac{nr}{k}.$$

Daher gibt es $a, b \in \mathbb{N}$ mit $s^n < \frac{a^n}{b^n} < r$. Dann ist $s < \frac{a}{b}$ im Widerspruch zur Wahl von s. Im Fall $r < s^n$ findet man analog $a, b \in \mathbb{N}$ mit $r < \frac{a^n}{b^n} < s^n$. Dann wäre auch $\frac{a}{b} < s$ eine obere Schranke von $\{q \in \mathbb{Q} : q^n < r\}$. Also ist $s^n = r$.

Sei auch $t > 0$ mit $t^n = r$. Dann ist

$$(s-t)(s^{n-1} + s^{n-2}t + \ldots + st^{n-1} + t^{n-1}) = s^n - t^n = 0.$$

Wegen $s^{n-1} + s^{n-2}t + \ldots + st^{n-2} + t^{n-1} > 0$ folgt $s = t$. □

Bemerkung II.8.13. In der Situation von Lemma II.8.12 nennt man $\sqrt[n]{r} := s$ die n-te *Wurzel* von r. Für $n = 2$ nennt man $\sqrt{r} := \sqrt[2]{r}$ die *Quadratwurzel* von r.

Satz II.8.14. *Die Quadratwurzel von 2 ist irrational.*

Beweis. Im Fall $w := \sqrt{2} \in \mathbb{Q}$ existieren $a, b \in \mathbb{Z}$ mit $w = \frac{a}{b}$. Dabei können wir annehmen, dass $b \in \mathbb{N}$ so klein wie möglich ist. Es folgt $2b^2 = a^2$. Insbesondere ist a^2 gerade. Wäre a ungerade, sagen wir $a = 2k + 1$, so wäre auch

$$a^2 = (2k+1)(2k+1) = 4k^2 + 4k + 1^2 = 2(2k^2 + 2k) + 1$$

ungerade. Daher ist a gerade, sagen wir $a = 2c$. Dann ist $2b^2 = 4c^2$ und $b^2 = 2c^2$. Also ist auch b gerade, sagen wir $b = 2d$. Schließlich ist $w = \frac{a}{b} = \frac{2c}{2d} = \frac{c}{d}$ im Widerspruch zur Wahl von b. □

Bemerkung II.8.15. Für alle $r \in \mathbb{R}$ gilt $r^2 \geq 0$. Daher existiert kein $r \in \mathbb{R}$ mit $r^2 = -1$. Wir erweitern daher $\mathbb{R}$, um auch Wurzeln negativer Zahlen ziehen zu können.

Definition II.8.16. Wir definieren die Menge der *komplexen Zahlen* durch $\mathbb{C} := \mathbb{R} \times \mathbb{R}$. Für $(a, b), (c, d) \in \mathbb{C}$ definieren wir:

$$\begin{aligned}
(a,b) + (c,d) &:= (a+c, b+d),\\
(a,b) - (c,d) &:= (a-c, b-d),\\
(a,b) \cdot (c,d) &:= (ac - bd, ab + bc),\\
(a,b) : (c,d) &:= \Big(\frac{ac+bd}{c^2+d^2}, \frac{ab+bc}{c^2+d^2}\Big) \qquad (\text{falls } (c,d) \neq 0).
\end{aligned}$$

Bemerkung II.8.17.

(i) In der Algebra und Analysis schreibt man komplexe Zahlen $x := (a, b) \in \mathbb{C}$ in der Form $x = a + b\mathrm{i}$. Dabei heißt a *Realteil* und b *Imaginärteil* von x.

(ii) Durch $a \mapsto (a, 0)$ kann man $\mathbb{R}$ in $\mathbb{C}$ einbetten. Wie üblich ist dies mit den Rechenoperationen verträglich.

(iii) Mit Hilfe der *Exponentialfunktion* $\exp\colon \mathbb{C} \to \mathbb{C}, x \mapsto \sum_{n\in\mathbb{N}} \frac{x^n}{n!}$ und dem Hauptzweig des *natürlichen Logarithmus* $\log\colon \mathbb{C} \setminus \{0\} \to \mathbb{C}$, lässt sich $a^b := \exp(b \log(a))$ für beliebige komplexe Zahlen a, b mit $a \neq 0$ definieren.

(iv) Im Gegensatz zu $\mathbb{R}$ gibt es auf $\mathbb{C}$ keine Ordnungsrelation, die mit den Rechenoperationen verträglich ist: Angenommen es gilt $\mathrm{i} > 0$. Dann ist $-1 = \mathrm{i}^2 > 0$ und $1 = (-1)^2 > 0$. Nun erhält man den Widerspruch $0 = 1 - 1 > 0 + 0 = 0$. Ist hingegen $\mathrm{i} < 0$, so wäre $0 = \mathrm{i} - \mathrm{i} < -\mathrm{i}$ und $-1 = (-\mathrm{i})^2 > 0$. Dies führt zum selben Widerspruch.

(v) (Fundamentalsatz der Algebra) Sind $n \in \mathbb{N} \setminus \{0\}$ und $a_0, \ldots, a_n \in \mathbb{C}$ beliebig, so existiert stets ein (oder mehrere) $x \in \mathbb{C}$ mit

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$$

(siehe Algebra-Skript). Beispielsweise ist $\mathrm{i}^2 = -1$. Dies verallgemeinert Lemma II.8.12.

(vi) Sind $a_0, \ldots, a_n$ in (v) rational, so nennt man x *algebraisch*. Die Menge $\overline{\mathbb{Q}}$ der algebraischen Zahlen ist abzählbar. Die Elemente der überabzählbaren Menge $\mathbb{C} \setminus \overline{\mathbb{Q}}$ heißen *transzendente* Zahlen. Zum Beispiel ist die Liouville-*Konstante*

$$\xi := \sum_{n\in\mathbb{N}} \frac{1}{10^{n!}} \in \mathbb{R}$$

transzendent (siehe Algebra-Skript).

(vii) Neben den komplexen Zahlen gibt es mindestens zwei alternative Erweiterungen der reellen Zahlen, die wir im Abschnitt II.11 kennen lernen.

II.9. Endliche Mengen

Definition II.9.1.

- Für eine Menge M und $k \in \mathbb{N}$ sei

$$\binom{M}{k} := \{A \subseteq M : |A| = k\}.$$

- Für $k, n \in \mathbb{N}$ mit $k \leq n$ nennt man

$$\binom{n}{k} := \frac{n!}{k!(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{k!} \in \mathbb{Q}$$

den *Binomialkoeffizienten* von n über k. Der folgende Satz zeigt $\binom{n}{k} \in \mathbb{N}$.

Satz II.9.2. *Sei M eine Menge mit $n \in \mathbb{N}$ Elementen. Für alle $k \leq n$ gilt dann*

$$\left|\binom{M}{k}\right| = \binom{n}{k}.$$

Beweis. Es gibt $|\operatorname{Sym}(A)| = k!$ Möglichkeiten, die Elemente einer k-elementigen Teilmenge $A = \{b_1, \ldots, b_k\} \subseteq M$ aufzulisten. Für die Wahl von b_1 gibt es n Möglichkeiten. Danach bleiben noch $|M \setminus \{b_1\}| = n - 1$ Möglichkeiten für die Wahl von b_2 usw. Die Anzahl der k-elementigen Teilmengen ist daher $\frac{n(n-1)\ldots(n-k+1)}{k!}$. □

Bemerkung II.9.3.

(i) Für $0 < k \leq n$ gilt

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} = \frac{n!k + n!(n-k+1)}{k!(n-k+1)!}$$
$$= \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}.$$

Induktiv folgt

$$1 = \binom{n}{0} < \binom{n}{1} < \ldots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \ldots > \binom{n}{n} = 1,$$

wobei $\lceil n/2 \rceil$ das kleinste $z \in \mathbb{Z}$ mit $n/2 \leq z$ bezeichnet (PASCALsches Dreieck).

(ii) In der Situation von Satz II.9.2 gilt

$$2^n = 2^{|M|} = |\mathcal{P}(M)| = \sum_{k=0}^{n} |\binom{M}{k}| = \sum_{k=0}^{n} \binom{n}{k}.$$

Dies ist ein Spezialfall der *binomischen Formel*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad (a, b \in \mathbb{C}),$$

die man mit vollständiger Induktion und (i) beweisen kann.

Satz II.9.4 (Inklusions-Exklusions-Prinzip)**.** *Für endliche Mengen $A_1, \ldots, A_n$ gilt*

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leq i_1 < \ldots < i_k \leq n} |A_{i_1} \cap \ldots \cap A_{i_k}|.$$

Beweis. Wir zählen, wie oft ein Element $a \in A_1 \cup \ldots \cup A_n$ auf der rechten Seite berücksichtigt wird. Dafür sei o. B. d. A. $a \in A_1 \cap \ldots \cap A_l$ und $a \notin A_i$ für $i > l$. Dann wird a genau dann gezählt, wenn $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, l\}$ gilt. Im k-ten Summanden wird a also $(-1)^{k+1}\binom{l}{k}$-mal gezählt nach Satz II.9.2. Insgesamt wird a auf der rechten Seite genau

$$\sum_{k=1}^{n} (-1)^{k+1} \binom{l}{k} = 1 - \sum_{k=0}^{l} (-1)^k \binom{l}{k} \overset{II.9.3}{=} 1 - (1-1)^l = 1$$

Mal gezählt. Dies zeigt die Behauptung. □

Satz II.9.5 (HALLS Heiratssatz)**.** *Sei $(M_i)_{i \in I}$ eine Familie von Teilmengen einer Menge M mit $|I| < \infty$ oder $\forall i \in I : |M_i| < \infty$. Genau dann existieren paarweise verschiedene $x_i \in M_i$ für $i \in I$, wenn $|\bigcup_{i \in J} M_i| \geq |J|$ für jede endliche Teilmenge $J \subseteq I$ gilt.*

Beweis. Für $J \subseteq I$ schreiben wir $M_J := \bigcup_{i \in J} M_i$. Nehmen wir an, dass paarweise verschiedene $x_i \in M_i$ existieren (man nennt $(x_i)_{i \in I}$ ein *Vertretersystem*). Offenbar ist dann $|M_J| \geq |\{x_i : i \in J\}| = |J|$ für jede endliche Teilmenge $J \subseteq I$. Sei umgekehrt die Bedingung

$$|M_J| \geq |J| \qquad (J \subseteq I,\ |J| < \infty) \tag{II.9.1}$$

erfüllt. Wir unterscheiden zwei Fälle:

Fall 1: $|I| < \infty$.
Induktion nach $n := |I|$: Der Fall $n \leq 1$ ist offensichtlich. Sei also $n > 1$ und o. B. d. A. $I = \{1, \ldots, n\}$. Eine Teilmenge $J \subseteq I$ heißt *kritisch*, falls $1 \leq |M_J| = |J| < n$ gilt.

Nehmen wir zunächst an, dass keine kritischen Teilmengen existieren. Wegen $|M_1| = |M_{\{1\}}| \geq 1$ existiert ein $x_1 \in M_1$. Für $i \in J := \{2, \ldots, n\}$ sei $N_i := M_i \setminus \{x_1\}$. Für jede Teilmenge $K \subseteq J$ gilt dann $|N_K| \geq |M_K| - 1 \geq |K|$, denn K ist nicht kritisch. Also erfüllt $(N_i)_{i \in J}$ Bedingung (II.9.1) und nach Induktion existiert ein Vertretersystem $(x_i)_{i \in J}$ von $(N_i)_{i \in J}$. Sicher ist dann $(x_i)_{i \in I}$ ein Vertretersystem für $(M_i)_{i \in I}$.

Nehmen wir schließlich an, dass eine kritische Teilmenge $J \subseteq I$ existiert. Dann gilt $1 \leq m := |J| = |M_J| < n$. Nach Induktion besitzt $(M_i)_{i \in J}$ ein Vertretersystem $(x_i)_{i \in J}$. Für $i \in I \setminus J$ sei $N_i := M_i \setminus M_J$. Für jede Teilmenge $K \subseteq I \setminus J$ gilt dann

$$|N_K| = |M_K \setminus M_J| = |M_{K \cup J}| - |M_J| \geq |K \cup J| - m = |K| + |J| - m = |K|,$$

d. h. $(N_i)_{i \in I \setminus J}$ erfüllt (II.9.1). Nach Induktion existiert ein Vertretersystem $(x_i)_{i \in I \setminus J}$. Nach Konstruktion ist dann $(x_i)_{i \in I}$ ein Vertretersystem für $(M_i)_{i \in I}$.

Fall 2: $\forall i \in I : |M_i| < \infty$.
Sei $\mathcal{M}$ die Menge aller Familien $(N_i)_{i \in I}$ mit $N_i \subseteq M_i$ (für alle $i \in I$), für die (II.9.1) gilt. Wegen $(M_i)_{i \in I} \in \mathcal{M}$ ist $\mathcal{M}$ nichtleer und durch

$$(N_i)_{i \in I} \leq (N_i')_{i \in I} \ :\Longleftrightarrow\ \forall i \in I : N_i \subseteq N_i'$$

geordnet. Sei $\varnothing \neq \mathcal{N} \subseteq \mathcal{M}$ eine total geordnete Teilmenge und $K_j := \bigcap_{(N_i)_{i \in I} \in \mathcal{N}} N_j$ für $j \in I$. Dann ist $(K_i)_{i \in I} \leq (N_i)_{i \in I}$ für alle $(N_i)_{i \in I} \in \mathcal{N}$. Sei $J \subseteq I$ eine endliche Teilmenge und $j \in J$. Wegen $|M_j| < \infty$ existiert eine endliche Teilmenge $\mathcal{N}_1 \subseteq \mathcal{N}$ mit

$$K_j = \bigcap_{(N_i)_{i \in I} \in \mathcal{N}_1} N_j$$

für alle $j \in J$. Da $\mathcal{N}$ total geordnet ist, besitzt $\mathcal{N}_1$ ein kleinstes Element $(N_i)_{i \in I}$. Offenbar ist dann $(K_j)_{j \in J} = (N_j)_{j \in J}$. Insbesondere ist $|K_J| = |N_J| \geq |J|$. Dies zeigt, dass $(K_i)_{i \in I}$ Bedingung (II.9.1) erfüllt und somit eine untere Schranke von $\mathcal{N}$ in $\mathcal{M}$ ist. Nach Zorns Lemma existiert ein minimales Element $(N_i)_{i \in I} \in \mathcal{M}$. Da jedes Vertretersystem von $(N_i)_{i \in I}$ auch ein Vertretersystem von $(M_i)_{i \in I}$ ist, können wir $(M_i)_{i \in I}$ durch $(N_i)_{i \in I}$ ersetzen und $\mathcal{M} = \{(M_i)_{i \in I}\}$ annehmen.

Sei $x \in M_I$ und $N_i := M_i \setminus \{x\}$ für $i \in I$. Wegen $(N_i)_{i \in I} \notin \mathcal{M}$ existiert eine endliche Teilmenge $J \subseteq I$ mit $|M_J| - 1 \leq |N_J| < |J| \leq |M_J|$. Es folgt $|M_J| = |J|$ und $x \in M_J$. Wir definieren nun

$$N_i := \begin{cases} M_i & \text{falls } i \in J, \\ M_i \setminus M_J & \text{falls } i \in I \setminus J. \end{cases}$$

Sei $K \subseteq I$ endlich. Dann gilt

$$\begin{aligned} |N_K| &= |N_{K \cap J} \cup N_{K \setminus J}| = |M_{K \cap J}| + |M_{K \setminus J} \setminus M_J| \\ &= |M_{K \cap J}| + |M_{K \cup J}| - |M_J| \geq |K \cap J| + |K \cup J| - |J| = |K|. \end{aligned}$$

Dies zeigt $(N_i)_{i \in I} \in \mathcal{M} = \{(M_i)_{i \in I}\}$ und $M_i \cap M_J = \varnothing$ für $i \in I \setminus J$. Es folgt $M_{I \setminus J} \cap M_J = \varnothing$. Nach Fall 1 existieren paarweise verschiedene $x_i \in M_i$ für $i \in J$. Setzt man nun

$$N_i := \begin{cases} \{x_i\} & \text{falls } i \in J, \\ M_i & \text{falls } i \in I \setminus J, \end{cases}$$

so erfüllt $(N_i)_{i\in I}$ wieder (II.9.1). Also gilt $M_i = \{x_i\}$ für $i \in J$. Da x beliebig gewählt war, gilt sogar $|M_i| = 1$ für alle $i \in I$. Offenbar sind die M_i auch paarweise disjunkt und die Behauptung folgt. □

Bemerkung II.9.6. Satz II.9.5 gilt nicht für $I = \mathbb{N}$, wenn nicht alle M_i endlich sind: Wähle $M_0 := \mathbb{N}$ und $M_i := \{i-1\}$ für $i \geq 1$.

Definition II.9.7. Jede total geordnete Teilmenge K einer endlichen geordneten Menge M hat die Form $K = \{x_1, \ldots, x_n\}$ mit $x_1 < x_2 < \ldots < x_n$. Man nennt K daher auch *Kette*. Eine Kette von M heißt *maximal*, wenn sie in keiner größeren Kette von M enthalten ist. Eine Teilmenge $A \subseteq M$ heißt *Antikette* von M, falls $x \leq y \Rightarrow x = y$ für alle $x, y \in A$ gilt.

Satz II.9.8 (Sperner)**.** *Sei M eine n-elementige Menge und A eine größtmögliche Antikette von $(\mathcal{P}(M), \subseteq)$. Dann gilt $A = \binom{M}{k}$ mit $k \in \{\lfloor n/2 \rfloor, \lceil n/2 \rceil\}$. Insbesondere ist $|A| = \binom{n}{\lfloor n/2 \rfloor}$.*

Beweis (Lubell). Offenbar hat jede maximale Kette in $\mathcal{P}(M)$ die Form $M_0 \subset \ldots \subset M_n$ mit $|M_k| = k$ für $k = 0, \ldots, n$. Es gibt n Möglichkeiten für M_1. Ist M_1 fest, so verbleiben noch $n-1$ Möglichkeiten für M_2 usw. Also gibt es genau $n!$ maximale Ketten in $\mathcal{P}(M)$. Sei nun $N \subseteq M$ fest mit $|N| = k$. Dann gibt es genau $k!(n-k)!$ maximale Ketten, die N enthalten (für M_1 gibt es k Möglichkeiten, für M_2 gibt es $k-1$ Möglichkeiten, …, für $M_k = N$ gibt es eine Möglichkeit, für M_{k+1} gibt es $n-k$ Möglichkeiten usw.). Für $x \in A$ sei K_x die Menge aller maximalen Ketten, die x enthalten. Enthält eine (maximale) Kette sowohl x als auch y, so gilt $x \leq y$ oder $y \leq x$. Daher sind die Mengen K_x mit $x \in A$ paarweise disjunkt. Dies zeigt

$$\sum_{x\in A} |x|!(n-|x|)! = \sum_{x\in A} |K_x| = \Big|\bigcup_{x\in A} K_x\Big| \leq n!. \tag{II.9.2}$$

Division durch $n!$ liefert

$$|A| \frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \overset{II.9.3}{\leq} \sum_{x\in A} \frac{1}{\binom{n}{|x|}} \leq 1.$$

Also ist $|A| \leq \binom{n}{\lfloor n/2 \rfloor}$. Umgekehrt ist $\binom{M}{\lfloor n/2 \rfloor}$ sicher eine Antikette mit $\binom{n}{\lfloor n/2 \rfloor}$ Elementen (Satz II.9.2). Es folgt $|A| = \binom{n}{\lfloor n/2 \rfloor}$ und $\binom{n}{|x|} = \binom{n}{\lfloor n/2 \rfloor}$ für alle $x \in A$. Daher besteht A nur aus Teilmengen $N \subseteq M$ mit $\lfloor n/2 \rfloor \leq |N| \lceil n/2 \rceil$. Ist n gerade, so sind wir fertig.

Sei nun $n = 2m+1$ ungerade. Aus (II.9.2) folgt $\sum_{x\in A} |K_x| = n!$, das heißt, alle maximalen Ketten enthalten (genau) ein Element aus A. Nehmen wir nun indirekt an, dass $S, T \subseteq M$ mit $|S| = |T| = m+1$, $S \in A$ und $T \notin A$ existieren. Bei geeigneter Nummerierung gilt $S = \{x_1, \ldots, x_{m+1}\}$ und $T = \{x_i, \ldots, x_{m+i}\}$. Wegen $T \notin A$ existiert ein $j \geq 1$ mit $S' := \{x_j, \ldots, x_{m+j}\} \in A$ und $T' := \{x_{j+1}, \ldots, x_{m+j+1}\} \notin A$. Es gilt $|S' \cap T'| = m$. Wegen $S' \cap T' \subseteq S' \in A$ ist $S' \cap T' \notin A$. Sicher existiert eine Kette, die $S' \cap T'$ und T' enthält. Wegen $A \subseteq \{N \subseteq M : |N| \in \{m, m+1\}\}$ müsste eine dieser Mengen in A liegen. Dies widerspricht aber $T' \notin A$. □

Satz II.9.9 (Mirsky)**.** *Sei M eine endliche geordnete Menge und m die größte Mächtigkeit einer Kette in M. Dann ist M eine Vereinigung von m Antiketten, aber nicht die Vereinigung von weniger Antiketten.*

Beweis. Für $x \in M$ sei $f(x) \geq 1$ die größte Mächtigkeit einer Kette, die bei x endet. Seien $x, y \in M$ mit $x \neq y$ und $f(x) = f(y)$. Im Fall $x < y$ könnte man jede Kette, die bei x endet, um y verlängern. Dann wäre aber $f(y) > f(x)$. Daher ist $x \not\leq y \not\leq x$. Also sind die Urbilder $A_n := f^{-1}(n)$ für $n \in \mathbb{N}$ Antiketten. Nach Voraussetzung ist $f(x) \leq m$ für alle $x \in M$. Dies zeigt $M = A_1 \cup \ldots \cup A_m$.

Sei umgekehrt $M = A_1 \cup \ldots \cup A_k$ für Antiketten $A_1, \ldots, A_k$. Sei $K \subseteq M$ eine Kette mit $|K| = m$. Dann gilt $|K \cap A_i| \leq 1$ für $i = 1, \ldots, k$. Dies zeigt $k \geq |K| = m$. □

Satz II.9.10 (Dilworth). *Sei M eine endliche geordnete Menge und m die größte Mächtigkeit einer Antikette in M. Dann ist M eine Vereinigung von m Ketten, aber nicht die Vereinigung von weniger Ketten.*

Beweis (Galvin). Ist M die Vereinigung der Ketten $K_1, \ldots, K_s$, so gilt $|A \cap K_i| \leq 1$ für jede Antikette A. Dies zeigt $s \geq m$. Für die umgekehrte Ungleichung argumentieren wir durch Induktion nach $|M|$. Für $M = \varnothing$ ist die Behauptung klar. Sei also $M \neq \varnothing$ und sei $x \in M$ ein maximales Element. Besitzt $M' := M \setminus \{x\}$ keine Antikette mit m Elementen, so ist M' nach Induktion eine Vereinigung von $m-1$ Ketten. Sicher ist dann M eine Vereinigung von m Ketten. Sei nun $A \subseteq M'$ eine Antikette mit $|A| = m$. Nach Induktion existieren o. B. d. A. disjunkte Ketten $K_1, \ldots, K_m$ mit $M' = K_1 \cup \ldots \cup K_m$. Dabei gilt $|A \cap K_i| = 1$ für $i = 1, \ldots, m$. Sei

$$x_i := \max \bigcup_{\substack{A \subseteq M' \text{ Antikette} \\ |A| = m}} K_i \cap A$$

für $i = 1, \ldots, m$. Angenommen es gilt $x_i \leq x_j$. Sei $A \subseteq M'$ eine Antikette mit $x_j \in A$ und $|A| = m$. Sei $x_i' \in A \cap K_i$. Dann gilt $x_i' \leq x_i \leq x_j$. Wegen $x_i', x_j \in A$ folgt $x_i' = x_i = x_j$ und $i = j$, da $K_i \cap K_j = \varnothing$. Daher ist $A := \{x_1, \ldots, x_m\}$ eine m-elementige Antikette von M'. Nach Voraussetzung ist $A \cup \{x\}$ keine Antikette. Da x maximal in M ist, gilt $x_i < x$ für ein $i \in \{1, \ldots, m\}$. Also ist $K_i' := K_i \cup \{x\}$ eine Kette und M ist die Vereinigung der Ketten $K_1, \ldots, K_{i-1}, K_i', K_{i+1}, \ldots, K_m$. □

Satz II.9.11 (Ramsey, unendliche Version). *Seien $n, k \in \mathbb{N}_+$ und M eine unendliche Menge mit $\binom{M}{k} = \mathcal{M}_1 \dot\cup \ldots \dot\cup \mathcal{M}_n$. Dann existiert eine unendliche Teilmenge $A \subseteq M$ mit $\binom{A}{k} \subseteq \mathcal{M}_i$ für ein $i \in \{1, \ldots, n\}$.*

Beweis. Induktion nach k: Der Fall $k = 1$ ist das (unendliche) Schubfachprinzip. Sei also $k \geq 2$. Eine vorgegebene Partition von $\binom{M}{k}$ interpretieren wir als Abbildung $f\colon \binom{M}{k} \to \{1, \ldots, n\}$. Wir definieren induktiv unendliche Mengen $A_0 \supseteq A_1 \supseteq \ldots$ und Elemente $a_i \in A_i \setminus A_{i+1}$ für $i \geq 0$, sodass

$$f_{a_i} := f(B \cup \{a_i\}) = f(C \cup \{a_i\}) \qquad \forall B, C \in \binom{A_{i+1}}{k-1}. \tag{II.9.3}$$

Sei $A_0 := M$ und $a_0 \in A_0$ beliebig. Seien bereits $a_i \in A_i$ definiert. Sei $g\colon \binom{A_i \setminus \{a_i\}}{k-1} \to \{1, \ldots, n\}$, $B \mapsto f(B \cup \{a_i\})$. Nach Induktion existiert eine unendliche Menge $A_{i+1} \subseteq A_i \setminus \{a_i\}$ mit $|g(\binom{A_{i+1}}{k-1})| = 1$. Somit gilt (II.9.3) für A_{i+1}. Wir wählen $a_{i+1} \in A_{i+1}$ beliebig.

Nach dem Schubfachprinzip existiert eine unendliche Menge $A \subseteq \{a_1, a_2, \ldots\}$ mit $f_a = f_b$ für alle $a, b \in A$. Damit gilt die Behauptung für A. □

Satz II.9.12 (Ramsey, endliche Version). *Für $r, s, t \in \mathbb{N}_+$ existiert ein $n \in \mathbb{N}_+$ mit folgender Eigenschaft: Für jede n-elementige Menge M und jede Partition $\binom{M}{r} = \mathcal{M}_1 \dot\cup \ldots \dot\cup \mathcal{M}_s$ existiert eine t-elementige Teilmenge $A \subseteq M$ mit $\binom{A}{r} \subseteq \mathcal{M}_i$ für ein $i \in \{1, \ldots, s\}$.*

Beweis. Nehmen wir indirekt an, dass die Behauptung für r, s, t falsch ist. Für jedes $n \in \mathbb{N}_+$ existiert eine n-elementige Menge, o. B. d. A. $M := \{1, \dots, n\}$ und eine Abbildung $f\colon \binom{M}{r} \to \{1, \dots, s\}$ ohne die gewünschte Eigenschaft. Wir sagen dann: f ist *schlecht* und schreiben $M_n := \binom{M}{r}$. Nach dem Schubfachprinzip gibt es unendlich viele schlechte Abbildungen (auf beliebigen M_n), die auf M_1 übereinstimmen. Sei F_1 eine solche Menge von schlechten Abbildungen und sei $f_1 : M_1 \to \{1, \dots, s\}$ die gemeinsame Einschränkung. In F_1 gibt es unendlich viele Abbildungen, die auf M_2 übereinstimmen. Sei $F_2 \subseteq F_1$ eine solche Menge und $f_2 : M_2 \to \{1, \dots, s\}$ die gemeinsame Einschränkung. Auf diese Weise erhalten wir schlechte Abbildungen $f_1, f_2, \dots$ mit $(f_{n+1})_{|M_n} = f_n$ für $n \in \mathbb{N}_+$. Wir definieren nun $f\colon \binom{\mathbb{N}_+}{r} \to \{1, \dots, s\}$ durch $f(B) := f_n(B)$ für $B \subseteq \{1, \dots, n\}$. Nach Satz II.9.11 existiert eine t-elementige Teilmenge $A \subseteq \mathbb{N}$ mit $|f(\binom{A}{r})| \leq 1$ (im Fall $t < r$ ist $\binom{A}{r} = \varnothing$). Nun gilt aber $A \subseteq M_n$ für ein n und f_n ist doch nicht schlecht. Widerspruch. □

Bemerkung II.9.13. Der Fall $r = 2$ lässt sich graphentheoretisch interpretieren: $\binom{M}{2}$ ist die Menge der Kanten des vollständigen Graphen mit Eckenmenge M. Die Kanten in $\mathcal{M}_i$ werden mit „Farbe“ i gefärbt. Satz II.9.12 sagt aus, dass es stets eine einfarbige Clique mit t Ecken gibt, sofern M nur groß genug ist. Im Fall $s = 2$ erhält man eine Aussage über beliebige (nicht unbedingt vollständige) Graphen: Jeder Graph mit hinreichend vielen Ecken besitzt einen vollständigen Teilgraphen mit t Ecken oder einen trivialen Teilgraphen mit t Ecken. Um die genaue Anzahl der benötigten Ecken zu bestimmen, führt man eine asymmetrische Variante ein: Die *Ramsey-Zahl* $R(k, l)$ ist die kleinste natürliche Zahl, sodass jeder Graph mit mindestens $R(k, l)$ Ecken einen vollständigen Teilgraphen mit k Ecken oder einen trivialen Teilgraphen mit l Ecken besitzt. Offensichtlich ist $R(k, l) = R(l, k)$ (betrachte komplementären Graphen) und $R(1, l) = 1$. Jeder Graph mit l Ecken ist entweder vollständig oder besitzt einen trivialen Teilgraphen mit zwei Kanten. Dies zeigt $R(2, l) = l$.

Lemma II.9.14. *Für $k, l \geq 2$ gilt*

$$R(k, l) \leq R(k-1, l) + R(k, l-1) \leq \binom{k+l-2}{k-1}.$$

Sind $R(k-1, l)$ und $R(k, l-1)$ beide gerade, so ist $R(k, l) < R(k-1, l) + R(k, l-1)$.

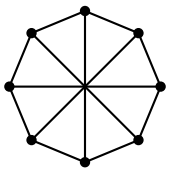
Beweis. Wir zeigen zunächst $R(k, l) \leq R(k-1, l) + R(k, l-1) =: n$. Sei G ein Graph mit n Ecken und sei $g \in G$ eine beliebige Ecke. Sei G_0 (bzw. G_1) die Menge aller zu g (nicht) benachbarten Ecken. Dann ist

$$|G_0| + |G_1| = |G_0 \dot\cup G_1| = n - 1 = R(k-1, l) + R(k, l-1) - 1.$$

Es folgt $|G_0| \geq R(k-1, l)$ oder $|G_1| \geq R(k, l-1)$. O. B. d. A. sei $|G_0| \geq R(k-1, l)$. Besitzt G_0 einen vollständigen Teilgraphen mit $k-1$ Ecken, so ist $G_0 \cup \{g\}$ ein vollständiger Teilgraph von G mit k Ecken. Anderenfalls besitzt G_0 (und damit auch G) einen trivialen Teilgraphen mit l Ecken. Dies zeigt die erste Behauptung. Die zweite Ungleichung folgt induktiv aus Bemerkung II.9.3. Nehmen wir nun an, dass $R(k-1, l)$ und $R(k, l-1)$ gerade sind. Sei G ein Graph mit $n-1$ Ecken. Das obige Argument funktioniert nur dann nicht, wenn $|G_0| = R(k-1, l) - 1$ und $|G_1| = R(k, l-1) - 1$ für jede Ecke g gilt. In diesem Fall besitzt jede Ecke von G die gleiche Anzahl $R(k-1, l)$ an Nachbarn. Die Anzahl aller Kanten in G ist somit $\frac{1}{2}(n-1)(|R(k-1, l)| - 1)$. Nach Voraussetzung ist dies aber keine ganze Zahl. Daher ist $R(k, l) \leq n - 1$. □

Beispiel II.9.15. Aus Lemma II.9.14 folgt $R(3, 3) \leq 6$. Ein 5-Eck (als Graph) zeigt $R(3, 3) > 5$ und damit $R(3, 3) = 6$. Interpretation: Unter sechs Personen gibt es drei, die sich alle kennen oder alle nicht

kennen. Da $R(3,3)$ und $R(2,4) = 4$ gerade sind, folgt $R(3,4) \leq 9$ aus Lemma II.9.14. Der folgende Graph zeigt umgekehrt $R(3,4) \geq 9$:



Weitere bekannte Werte sind (ohne Beweis):

$$R(3,5) = 14, \qquad R(3,6) = 18, \qquad R(3,7) = 23, \qquad R(3,8) = 28,$$
$$R(3,9) = 36, \qquad R(4,4) = 18, \qquad R(4,5) = 25.$$

Satz II.9.16 (De Bruijn-Erdős)**.** *Sei A eine endliche Menge und $\mathcal{A} \subseteq \mathcal{P}(A)$ mit $2 \leq |B| < |A|$ für alle $B \in \mathcal{A}$. Für je zwei verschiedene $x, y \in A$ existiere genau ein $B \in \mathcal{A}$ mit $x, y \in B$. Dann gilt $|\mathcal{A}| \geq |A|$.*

Beweis (Ivanov). Für $a \in A$ sei $f(a) := |\{B \in \mathcal{B} : a \in B\}|$. Dann gilt

$$\sum_{a \in A} f(a) = |\{(a, B) \in A \times \mathcal{A} : a \in B\}| = \sum_{B \in \mathcal{A}} |B|.$$

Für $a \notin B \in \mathcal{A}$ und $b \in B$ existiert genau ein $C_b \in \mathcal{A} \setminus \{B\}$ mit $a, b \in C_b$. Für $b \neq b'$ ist dabei $C_b \neq C_{b'}$, denn anderenfalls wären b, b' sowohl in B als auch in $C_b = C_{b'}$ enthalten. Dies zeigt $|B| \leq f(a)$.

Nehmen wir nun $|\mathcal{A}| < |A|$ an. Für $B_1, \ldots, B_n \in \mathcal{A}$ gilt $|A \setminus B_1| \geq 1$ und $|B_1 \cap B_2| \leq 1$. Dies zeigt $|\bigcup_{i=1}^{n} A \setminus B_i| \geq |A| - 1 \geq |\mathcal{A}| \geq n$ für $n \geq 2$. Nach Halls Heiratssatz existieren paarweise verschiedene Vertreter $\alpha(B) \in A \setminus B$ für $B \in \mathcal{A}$. Dies liefert den Widerspruch

$$\sum_{a \in A} f(a) = \sum_{B \in \mathcal{A}} |B| \leq \sum_{B \in \mathcal{A}} f(\alpha(B)) < \sum_{a \in A} f(a). \qquad \square$$

II.10. Topologie

Definition II.10.1. Sei M eine nichtleere Menge. Eine Familie von Teilmengen $\mathcal{F} \subseteq \mathcal{P}(M)$ heißt *Filter* von M, falls gilt:

- $\varnothing \neq \mathcal{F} \neq \mathcal{P}(M)$.
- $A, B \in \mathcal{F} \Longrightarrow A \cap B \in \mathcal{F}$.
- $A \supseteq B \in \mathcal{F} \Longrightarrow A \in \mathcal{F}$.

Ist $\mathcal{F}$ maximal bzgl. Inklusion, so nennt man $\mathcal{F}$ einen *Ultrafilter*.

Bemerkung II.10.2. Die erste Bedingung in Definition II.10.1 ist äquivalent zu $\varnothing \notin \mathcal{F}$ und $M \in \mathcal{F}$.

Beispiel II.10.3.

(i) Für jede Teilmenge $\varnothing \neq A \subseteq M$ ist

$$\mathcal{F}(A) := \{B \subseteq M : A \subseteq B\}$$

ein Filter. Filter dieser Art heißen *Hauptfilter*. Insbesondere ist $\{M\}$ ein Filter von M.

(ii) Sei $\mathcal{F}$ ein Filter einer endlichen Menge M. Dann existiert ein minimales Element $A \in \mathcal{F}$. Es folgt $\mathcal{F}(A) \subseteq \mathcal{F}$. Gäbe es ein $B \in \mathcal{F} \setminus \mathcal{F}(A)$, so wäre $A \cap B \in \mathcal{F}$ im Widerspruch zur Wahl von A. Daher ist jeder Filter von M ein Hauptfilter. Die Ultrafilter von M haben offenbar die Form $\mathcal{F}(x) := \mathcal{F}(\{x\})$ für ein $x \in M$.

(iii) Sei nun M eine unendliche Menge und $\mathcal{F}$ die Menge aller *koendlichen* Teilmengen $A \subseteq M$ (d. h. $|M \setminus A| < \infty$). Offenbar ist $\mathcal{F}$ ein Filter, aber kein Hauptfilter. Man nennt $\mathcal{F}$ den *Fréchet-Filter* auf M.

(iv) Die Menge Ω aller Filter, die einen gegebenen Filter $\mathcal{F}$ enthalten, ist durch $\subseteq$ geordnet. Man sieht leicht, dass die Vereinigung einer total geordneten Teilmenge von Ω wieder ein Filter ist. Nach Zorns Lemma existiert also stets ein Ultrafilter, der $\mathcal{F}$ enthält.

Lemma II.10.4. *Für jeden Filter $\mathcal{F}$ von $M \neq \varnothing$ sind folgende Aussagen äquivalent:*

(1) $\mathcal{F}$ ist ein Ultrafilter.

(2) Für alle $A \subseteq M$ gilt entweder $A \in \mathcal{F}$ oder $M \setminus A \in \mathcal{F}$.

(3) Für alle $A_1, \ldots, A_n \subseteq M$ mit $A_1 \cup \ldots \cup A_n \in \mathcal{F}$ existiert ein i mit $A_i \in \mathcal{F}$.

Beweis.

(1)⇒(2): Sei

$$\mathcal{G} := \big\{B \subseteq M : \exists F \in \mathcal{F} : A \cap F \subseteq B\big\}.$$

Ist $\varnothing \in \mathcal{G}$, so existiert ein $F \in \mathcal{F}$ mit $F \subseteq M \setminus A$. Dann gilt auch $M \setminus A \in \mathcal{F}$. Anderenfalls ist $\mathcal{G}$ ein Filter, der $\mathcal{F}$ enthält. Da $\mathcal{F}$ ein Ultrafilter ist, gilt $A = A \cap M \in \mathcal{G} = \mathcal{F}$.

(2)⇒(3): Nehmen wir $A_i \notin \mathcal{F}$ für $i = 1, \ldots, n$ an. Nach (2) gilt $M \setminus A_i \in \mathcal{F}$ für $i = 1, \ldots, n$. Da $\mathcal{F}$ ein Filter ist, folgt der Widerspruch

$$\varnothing = \Big(\bigcup_{i=1}^{n} A_i\Big) \cap \Big(M \setminus \bigcup_{i=1}^{n} A_i\Big) = \Big(\bigcup_{i=1}^{n} A_i\Big) \cap \bigcap_{i=1}^{n} (M \setminus A_i) \in \mathcal{F}.$$

(3)⇒(1): Angenommen $\mathcal{F}$ ist kein Ultrafilter. Dann existiert ein Filter $\mathcal{G} \supsetneq \mathcal{F}$ und ein $A \in \mathcal{G} \setminus \mathcal{F}$. Wegen $A \cup (M \setminus A) \in \mathcal{F}$ folgt $M \setminus A \in \mathcal{F} \subseteq \mathcal{G}$ aus (3). Nun wäre aber $\varnothing = A \cap (M \setminus A) \in \mathcal{G}$. □

Definition II.10.5. Sei M eine nichtleere Menge. Eine Familie von Teilmengen $\mathcal{T} \subseteq \mathcal{P}(M)$ heißt *Topologie* auf M, falls gilt:

- $\varnothing, M \in \mathcal{T}$.
- $\mathcal{S} \subseteq \mathcal{T} \Longrightarrow \bigcup_{S \in \mathcal{S}} S \in \mathcal{T}$.
- $U, V \in \mathcal{T} \Longrightarrow U \cap V \in \mathcal{T}$.

Die Mengen in $\mathcal{T}$ nennt man *offen*. Man nennt $A \subseteq M$ *abgeschlossen*, falls $M \setminus A$ offen ist. Das Paar $(M, \mathcal{T})$ heißt *topologischer Raum*. Sind $\mathcal{S} \subseteq \mathcal{T}$ Topologien, so nennt man $\mathcal{S}$ (bzw. $\mathcal{T}$) *gröber* (bzw. *feiner*) als $\mathcal{T}$ (bzw. $\mathcal{S}$).

Bemerkung II.10.6. Aus der De Morganschen Regel folgt, dass beliebige Durchschnitte und endliche Vereinigungen von abgeschlossenen Mengen abgeschlossen sind.

Beispiel II.10.7.

(i) Man nennt $\mathcal{T} = \{\varnothing, M\}$ die *triviale* Topologie und $\mathcal{T} = \mathcal{P}(M)$ die *diskrete* Topologie auf M.

(ii) Ist $(M, \mathcal{T})$ ein topologischer Raum und $\varnothing \neq N \subseteq M$, so definiert $\{N \cap U : U \in \mathcal{T}\}$ eine Topologie auf N, die man *Relativtopologie* nennt. Achtung: Offene Mengen in N bzgl. der Relativtopologie müssen nicht offen in M sein (zum Beispiel wenn N selbst nicht offen in M ist).

(iii) Der Durchschnitt von beliebig vielen Topologien auf M ist wieder eine Topologie. Ist $\mathcal{S} \subseteq \mathcal{P}(M)$, so ist

$$\langle \mathcal{S} \rangle := \bigcap_{\substack{\mathcal{T} \text{ Topologie} \\ \mathcal{S} \subseteq \mathcal{T}}} \mathcal{T}$$

die „kleinste“ Topologie, die $\mathcal{S}$ umfasst. Offenbar besteht $\langle \mathcal{S} \rangle$ aus beliebigen (auch leeren) Vereinigungen von endlichen Durchschnitten von Elementen aus $\mathcal{S}$. Ist $\mathcal{S}$ ein Filter, so gilt offenbar $\langle \mathcal{S} \rangle = \mathcal{S} \cup \{\varnothing\}$.

(iv) Ist $(M_i, \mathcal{T}_i)_{i \in I}$ eine Familie disjunkter topologischer Räume, so ist auch $M := \bigcup_{i \in I} M_i$ mit

$$\mathcal{T} := \Big\{ \bigcup_{i \in I} T_i : T_i \in \mathcal{T}_i \Big\}$$

ein topologischer Raum.

(v) Eine Abbildung $d\colon M \times M \to \mathbb{R}$ heißt *Metrik*, falls für alle $x, y, z \in M$ gilt:

- $d(x, y) \geq 0$ mit Gleichheit genau dann, wenn $x = y$ (positiv definit).
- $d(x, y) = d(y, x)$ (symmetrisch).
- $d(x, z) \leq d(x, y) + d(y, z)$ (Dreiecksungleichung).

Man nennt (M, d) einen *metrischen Raum*. Für $x \in M$ und $\epsilon > 0$ definiert man die *ϵ-Kugel* um x durch

$$B_\epsilon(x) := \{y \in M : d(x, y) < \epsilon\}.$$

Eine Teilmenge $U \subseteq M$ heißt *offen* bzgl. d, falls für alle $x \in U$ ein $\epsilon > 0$ mit $B_\epsilon(x) \subseteq U$ existiert. Man zeigt leicht, dass diese offenen Mengen eine Topologie bilden. Topologische Räume, die durch eine Metrik entstehen, nennt man *metrisierbar*. Die *diskrete* Metrik mit $d(x, y) = 1$ für $x \neq y$ führt zur diskreten Topologie (wähle $\epsilon = \frac{1}{2}$). Nicht jeder metrische Raum ist metrisierbar. Betrachte zum Beispiel $M = \{x, y\}$ mit der trivialen Topologie. Gäbe es eine entsprechende Metrik d, so wäre $\{x\}$ stets offen (wähle $\epsilon = \frac{d(x,y)}{2}$).

(vi) Sei V ein $\mathbb{R}$-Vektorraum. Eine Abbildung $V \to \mathbb{R}$, $v \mapsto |v|$ heißt *Norm* auf V, falls für alle $v, w \in V$ gilt:

- $|v| \geq 0$ mit Gleichheit genau dann, wenn $v = 0$ (positiv definit).
- $|\lambda v| = |\lambda||v|$ für alle $\lambda \in \mathbb{R}$ (homogen).

- $|v + w| \leq |v| + |w|$ (Dreiecksungleichung).

Man nennt $(V, |.|)$ einen *normierten Raum*. Man zeigt leicht, dass $d(v, w) := |v - w|$ eine Metrik auf V definiert. Bekanntlich definiert $|v| := \sqrt{v_1^2 + \ldots + v_n^2}$ die *euklidische* Norm auf $\mathbb{R}^n$. In der Analysis zeigt man, dass alle Normen auf $\mathbb{R}^n$ zur gleichen Topologie führen. Dies ist für unendlich-dimensionale Räume falsch.

(vii) Die Menge der koendlichen Teilmengen zusammen mit der leeren Menge bildet die *koendliche* Topologie auf jeder unendlichen Menge. Sie hat die besondere Eigenschaft, dass der Durchschnitt von zwei nichtleeren offenen Mengen niemals leer ist.

Definition II.10.8. Sei $(M, \mathcal{T})$ ein topologischer Raum, $A \subseteq M$ und $x \in M$. Man nennt A eine *Umgebung* von x, falls eine offene Menge U mit $x \in U \subseteq A$ existiert. Man nennt x einen

- *inneren Punkt* von A, falls A Umgebung von x ist.
- *Randpunkt* von A, falls weder A noch $M \setminus A$ Umgebungen von x sind.

Die Menge der inneren Punkte (bzw. Randpunkte) von A nennt man das *Innere* $\mathring{A}$ (bzw. den *Rand* ∂A) von A. Schließlich nennt man $\overline{A} := \mathring{A} \cup \partial A$ die *abgeschlossene Hülle* von A.

Lemma II.10.9. *Sei $(M, \mathcal{T})$ ein topologischer Raum und $A \subseteq M$. Dann gilt:*

(i) $\mathring{A}$ ist die Vereinigung aller offenen Mengen in A.

(ii) $\overline{A}$ ist der Durchschnitt aller abgeschlossenen Mengen, die A enthalten.

Insbesondere ist $\mathring{A} \subseteq A \subseteq \overline{A}$.

Beweis.

(i) Nach Definition liegt jedes $x \in \mathring{A}$ in einer offenen Menge $U \subseteq A$. Sei umgekehrt $U \subseteq A$ offen. Dann ist A eine Umgebung für alle $x \in U$. Dies zeigt $U \subseteq \mathring{A}$.

(ii) Offensichtlich liegt $\mathring{A}$ in jeder abgeschlossenen Menge, die A enthält. Sei $x \in \partial A$ und B eine abgeschlossene Menge, die A enthält. Wäre $x \in M \setminus B$, so wäre $M \setminus B$ eine Umgebung von x und x kein Randpunkt. Also ist $x \in B$ und $\overline{A}$ liegt im Durchschnitt aller abgeschlossenen Mengen, die A enthalten. Sei umgekehrt $x \in M \setminus \overline{A}$. Dann ist $M \setminus A$ eine Umgebung von x, das heißt es gibt eine offene Menge $U \subseteq M \setminus A$ mit $x \in U$. Nun ist x nicht in der abgeschlossenen Menge $M \setminus U$, die A enthält. Dies zeigt die Behauptung. □

Folgerung II.10.10. *Eine Teilmenge A eines topologischen Raums ist genau dann offen (bzw. abgeschlossen), wenn $A = \mathring{A}$ (bzw. $A = \overline{A}$) gilt.*

Beispiel II.10.11. Sei $A = (0, 1] \subseteq \mathbb{R}$ das halboffene Intervall im euklidischen Raum $\mathbb{R}$. Dann ist $\mathring{A} = (0, 1)$ das offene Intervall, $\partial A = \{0, 1\}$ und $\overline{A} = [0, 1]$. Randpunkte können also sowohl innerhalb als auch außerhalb von A liegen.

Definition II.10.12. Eine Teilmenge K eines topologischen Raums M heißt *kompakt*, wenn für jede Familie offener Mengen $(U_i)_{i \in I}$ mit $K \subseteq \bigcup_{i \in I} U_i$ eine endliche Teilmenge $J \subseteq I$ mit $K \subseteq \bigcup_{j \in J} U_j$ existiert (man sagt: jede offene Überdeckung besitzt eine endliche Teilüberdeckung). Ist M selbst kompakt, so spricht man von einem *kompakten* topologischen Raum.

Bemerkung II.10.13.

(i) Besitzt M nur endlich viele offene Mengen, so ist offenbar jede Teilmenge kompakt.

(ii) Jede endliche Teilmenge eines topologischen Raums ist kompakt. In der diskreten Topologie gilt auch die Umkehrung.

(iii) In der koendlichen Topologie auf $\mathbb{N}$ ist jede offene Menge kompakt.

(iv) Ist $K \subseteq M$ kompakt und $A \subseteq K$ abgeschlossen, so ist auch A kompakt, denn ist $A \subseteq \bigcup_{i\in I} U_i$ eine offene Überdeckung, so ist $K \subseteq M \setminus A \cup \bigcup_{i\in I} U_i$ eine offene Überdeckung.

Definition II.10.14. Ein Filter $\mathcal{F}$ eines topologischen Raums $(M, \mathcal{T})$ *konvergiert* gegen $x \in M$, falls $\mathcal{F}(x) \cap \mathcal{T} \subseteq \mathcal{F}$ gilt.

Lemma II.10.15. *Ein topologischer Raum M ist genau dann kompakt, wenn jeder Ultrafilter von M gegen einen Punkt konvergiert.*

Beweis. Sei M kompakt. Angenommen ein Ultrafilter $\mathcal{F}$ von M konvergiert gegen keinen Punkt. Für alle $x \in M$ existieren dann $U_x \in \mathcal{T} \setminus \mathcal{F}$ mit $x \in U_x$. Da M kompakt ist, existiert eine endliche Menge $X \subseteq M$ mit $M = \bigcup_{x\in X} U_x$. Dies widerspricht Lemma II.10.4.

Nehmen wir nun an, dass M nicht kompakt ist. Dann existiert eine offene Überdeckung $M = \bigcup_{i\in I} U_i$ ohne endliche Teilüberdeckung. Folglich ist

$$\left\{A \subseteq M : \exists i_1, \ldots, i_n \in I : M \setminus A \subseteq U_{i_1} \cup \ldots \cup U_{i_n}\right\}$$

ein Filter, der in einem Ultrafilter $\mathcal{F}$ liegt. Angenommen $\mathcal{F}$ konvergiert gegen x. Sei $i \in I$ mit $x \in U_i$. Dann wäre $\varnothing = U_i \cap (M \setminus U_i) \in \mathcal{F}$. □

Definition II.10.16. Sei $(M_i, \mathcal{T}_i)_{i\in I}$ eine Familie von topologischen Räumen und $M := \bigtimes_{i\in I} M_i$. Seien $\pi_i \colon M \to M_i$, $(x_j)_j \mapsto x_i$ die Projektionsabbildungen für $i \in I$. Man nennt

$$\langle \pi_i^{-1}(U) : i \in I, U \in \mathcal{T}_i \rangle$$

die *Produkt-Topologie* auf M.

Satz II.10.17 (Tychonoff)**.** *Für jede Familie von topologischen Räumen $(M_i)_{i\in I}$ ist $M := \bigtimes_{i\in I} M_i$ genau dann kompakt, wenn alle M_i kompakt sind.*

Beweis. Sei M kompakt, $i \in I$ und $M_i = \bigcup_{j\in J} U_j$ eine offene Überdeckung. Dann ist $M = \bigcup_{j\in J} \pi_i^{-1}(U_j)$ eine offene Überdeckung von M. Da M kompakt ist, existiert eine endliche Teilmenge $J' \subseteq J$ mit $M = \bigcup_{j\in J'} \pi_i^{-1}(U_j)$. Daher ist $M_i = \bigcup_{j\in J'} U_j$ und M_i ist kompakt.

Seien nun alle M_i kompakt. Sei $\mathcal{F}$ ein Filter von M. Für $i \in I$ sei

$$\mathcal{F}_i := \{\pi_i(F) : F \in \mathcal{F}\} \subseteq \mathcal{P}(M_i).$$

Wegen $\varnothing \notin \mathcal{F}$ ist $\varnothing \notin \mathcal{F}_i$. Sei $A \supseteq \pi_i(F) \in \mathcal{F}_i$. Dann ist $F \subseteq \pi_i^{-1}(A) \in \mathcal{F}$ und $A = \pi_i(\pi_i^{-1}(A)) \in \mathcal{F}_i$. Für $F_1, F_2 \in \mathcal{F}$ ist $\pi_i(F_1) \cap \pi_i(F_2) \supseteq \pi_i(F_1 \cap F_2) \in \mathcal{F}_i$ und $\pi_i(F_1) \cap \pi_i(F_2) \in \mathcal{F}_i$. Dies zeigt, dass $\mathcal{F}_i$ ein Filter von M_i ist. Sei auch $\mathcal{G} \supseteq \mathcal{F}_i$ ein Filter von M_i. Für $F \in \mathcal{F}$ und $G \in \mathcal{G}$ gilt $\pi_i(F) \cap G \in \mathcal{F}_i$

und $F \cap \pi_i^{-1}(G) \neq \varnothing$. Auch der Durchschnitt zweier Mengen der Form $F \cap \pi_i^{-1}(G)$ ist nichtleer, denn $\pi_i^{-1}(G_1 \cap G_2) \subseteq \pi_i^{-1}(G_1) \cap \pi_i^{-1}(G_2)$ für $G_1, G_2 \in \mathcal{G}$. Daher ist

$$\mathcal{F}' := \left\{A \subseteq M : \exists G \in \mathcal{G}, F \in \mathcal{F} : \pi_i^{-1}(G) \cap F \subseteq A\right\}$$

ein Filter von M, der $\mathcal{F}$ enthält. Da $\mathcal{F}$ ein Ultrafilter ist, gilt $\mathcal{F}' = \mathcal{F}$. Für $G \in \mathcal{G}$ gilt somit $\pi_i^{-1}(G) = \pi_i^{-1}(G) \cap M \in \mathcal{F}$ und $G = \pi_i(\pi_i^{-1}(G)) \in \mathcal{F}_i$. Also ist $\mathcal{F}_i = \mathcal{G}$ ein Ultrafilter von M_i. Nach Lemma II.10.15 konvergiert $\mathcal{F}_i$ gegen ein $x_i \in M_i$. Sei $x := (x_i)_{i \in I} \in M$. Sei $U \subseteq M$ eine offene Menge, die x enthält. Nach Lemma II.10.15 genügt es $U \in \mathcal{F}$ zu zeigen. Nach Definition der Produkt-Topologie können wir annehmen, dass offene Mengen $U_{i_j} \subseteq M_{i_j}$ für $j = 1, \ldots, n$ mit

$$U = \pi_{i_1}^{-1}(U_{i_1}) \cap \ldots \cap \pi_{i_n}^{-1}(U_{i_n})$$

existieren. Wegen $x_{i_j} \in U_{i_j}$ gilt $U_{i_j} \in \mathcal{F}_{i_j}$ für $j = 1, \ldots, n$. Also existieren $V_j \in \mathcal{F}$ mit $\pi_{i_j}(V_j) = U_{i_j}$. Aus $V_j \subseteq \pi_{i_j}^{-1}(U_{i_j})$ folgt $\pi_{i_j}^{-1}(U_{i_j}) \in \mathcal{F}$ und schließlich $U \in \mathcal{F}$. □

Satz II.10.18 (Kelley)**.** *Der Satz von Tychonoff impliziert das Auswahlaxiom.*

Beweis. Sei $(M_i)_{i \in I}$ eine Familie von nichtleeren Mengen. Sei x ein „neues“ Element, welches in keinem der M_i liegt. Sei $\widehat{M_i} := M_i \cup \{x\}$ ausgestattet mit der koendlichen Topologie, wobei zusätzlich $\{x\}$ offen sein soll. Nach Bemerkung II.10.13 und Tychonoff sind $\widehat{M_i}$ und $\widehat{M} := \bigtimes_{i \in I} \widehat{M_i}$ kompakt. Die i-te Projektion $\pi_i \colon \widehat{M} \to \widehat{M_i}$ ist stetig. Daher ist $\pi_i^{-1}(x)$ offen. Angenommen $\bigtimes_{i \in I} M_i = \varnothing$. Dann ist $\widehat{M} = \bigcup_{i \in I} \pi_i^{-1}(x)$ eine offene Überdeckung. Sei $J \subseteq I$ endlich mit $\widehat{M} = \bigcup_{j \in J} \pi_j^{-1}(x)$. Offenbar existiert jedoch ein Element $m = (m_i)_{i \in I} \in \widehat{M}$ mit $m_j \in M_j$ für $j \in J$ und $m_i = x$ für $i \in I \setminus J$. Widerspruch. □

Definition II.10.19. Ein topologischer Raum M heißt

- *zusammenhängend*, falls M nicht die Vereinigung von zwei disjunkten nichtleeren offenen Teilmengen ist.
- *Hausdorff-Raum*, falls für verschiedene $x, y \in M$ zwei disjunkte offene Mengen $U_x, U_y \subseteq M$ mit $x \in U_x$ und $y \in U_y$ existieren (*Trennungsaxiom*).

Bemerkung II.10.20. Offenbar ist ein topologischer Raum M genau dann zusammenhängend, wenn $\varnothing$ und M die einzigen Teilmengen sind, die zugleich offen und abgeschlossen sind.

Satz II.10.21. *Jeder metrische Raum ist ein Hausdorff-Raum.*

Beweis. Sei (M, d) ein metrischer Raum und $x, y \in M$ verschiedene Punkte. Sei $\epsilon := \frac{d(x,y)}{2}$. Dann sind $B_\epsilon(x)$ und $B_\epsilon(y)$ disjunkte offene Mengen, die x bzw. y enthalten. □

Beispiel II.10.22.

(i) Wir zeigen, dass der euklidische Raum $\mathbb{R}^n$ zusammenhängend ist. Angenommen es existieren disjunkte nichtleere offene Teilmengen U, V mit $\mathbb{R}^n = U \cup V$. Sei $x \in U$ und $y \in V$. Sei

$$r := \sup\{s \in [0,1] : x + s(y - x) \in U\}$$

und $z := x + r(y - x)$. Liegt z in U, so gilt $B_\epsilon(z) \subseteq U$ für ein $\epsilon > 0$. Dann wäre aber auch $z + \frac{\epsilon}{2|y-x|}(y - z) \in U$ im Widerspruch zur Definition von r. Analog erhält man einen Widerspruch im Fall $z \in V$.

(ii) Die triviale Topologie auf M liefert keinen Hausdorff-Raum, falls $|M| > 1$. Eine unendliche Menge mit der koendlichen Topologie ist ebenfalls kein Hausdorff-Raum, denn der Durchschnitt zweier nichtleerer offener Mengen ist nie leer.

Lemma II.10.23. *Jede kompakte Teilmenge eines Hausdorff-Raums ist abgeschlossen.*

Beweis. Sei K kompakt im Hausdorff-Raum M. Sei $x \in M \setminus K$. Für alle $a \in K$ existieren disjunkte offene Mengen $U_a, V_a \subseteq M$ mit $a \in U_a$ und $x \in V_a$. Wegen der Kompaktheit existieren $a_1, \ldots, a_n \in K$ mit $K \subseteq \bigcup_{i=1}^n U_{a_i}$. Nun ist $V_{a_1} \cap \ldots \cap V_{a_n}$ eine offene Menge in $M \setminus K$, die x enthält. Also ist $M \setminus K$ offen und K ist abgeschlossen. □

Beispiel II.10.24. Die triviale Topologie auf einer endlichen Menge zeigt, dass kompakte Mengen im Allgemeinen nicht abgeschlossen sein müssen.

Satz II.10.25. *Sei M ein kompakter Hausdorff-Raum und $U, V \subseteq M$ disjunkte abgeschlossene Teilmengen. Dann existieren disjunkte offenen Teilmengen $A, B \subseteq M$ mit $U \subseteq A$ und $V \subseteq B$.*

Beweis. Sei $u \in U$. Für jedes $v \in V$ existieren disjunkte offene Mengen U_v, V_v mit $u \in U_v$ und $v \in V_v$. Die offene Überdeckung

$$M = (M \setminus V) \cup \bigcup_{v \in V} V_v$$

besitzt eine endliche Teilüberdeckung $M = (M \setminus V) \cup \bigcup_{i=1}^n V_{v_i}$. Die offenen Mengen $A_u := U_{v_1} \cap \ldots \cap U_{v_n}$ und $B_u := V_{v_1} \cup \ldots \cup V_{v_n}$ sind disjunkt und erfüllen $u \in A_u$ und $V \subseteq B_u$. Die offene Überdeckung

$$M = (M \setminus U) \cup \bigcup_{u \in U} A_u$$

besitzt ebenfalls eine endliche Teilüberdeckung $M = (M \setminus U) \cup \bigcup_{i=1}^m A_{u_i}$. Nun erfüllen $A := A_{u_1} \cup \ldots \cup A_{u_m}$ und $B := B_{u_1} \cap \ldots \cap B_{u_m}$ die Behauptung. □

Definition II.10.26. Sei (M, d) ein metrischer Raum. Für $A \subseteq M$ nennt man

$$d(A) := \sup\{d(x, y) : x, y \in A\} \in \mathbb{R} \cup \{\infty\}$$

den *Durchmesser* von A. Ist $d(A) < \infty$, so nennt man A *beschränkt*.

Lemma II.10.27. *Jedes abgeschlossene Intervall $[a, b] \subseteq \mathbb{R}$ ist kompakt bzgl. der euklidischen Metrik.*

Beweis. Sei $[a, b] \subseteq \bigcup_{i \in I} U_i$ eine offene Überdeckung. Sei $S \subseteq [a, b]$ die Menge aller Punkte s, sodass $[a, s]$ eine endliche Teilüberdeckung besitzt. Wegen $a \in S$ ist $S \neq \varnothing$. Da $[a, b]$ beschränkt ist, existiert $s := \sup S$. Angenommen $s < b$. Sei $[a, s] \subseteq \bigcup_{i=1}^n U_i$ eine endliche Teilüberdeckung und $1 \leq i \leq n$ mit $s \in U_i$. Da U_i offen ist, existiert ein $\epsilon > 0$ mit $B_\epsilon(s) \subseteq U_i$. Nun gilt auch $[a, s + \epsilon/2] \subseteq \bigcup_{i=1}^n U_i$ im Widerspruch zur Wahl von s. Also ist $s = b$ und $[a, b]$ besitzt eine endliche Teilüberdeckung. □

Satz II.10.28 (Heine-Borel)**.** *Jede kompakte Teilmenge eines metrischen Raums ist beschränkt und abgeschlossen. Im euklidischen Raum $\mathbb{R}^n$ gilt auch die Umkehrung.*

Beweis. Sei (M, d) ein metrischer Raum und $K \subseteq M$ kompakt. Nach Satz II.10.21 und Lemma II.10.23 ist K abgeschlossen. Da die offene Überdeckung $K \subseteq \bigcup_{n\in\mathbb{N}} B_n(x)$ für ein $x \in M$ eine endliche Teilüberdeckung besitzt, ist K beschränkt.

Sei nun $M = \mathbb{R}^n$ und A beschränkt und abgeschlossen. Dann existieren $a, b \in \mathbb{R}$ mit $A \subseteq [a, b]^n$. Sind $U_1, \ldots, U_n \subseteq \mathbb{R}$, so auch $U_1 \times \ldots \times U_n \subseteq M$. Für jede offene Menge $U \subseteq M$ und $x \in U$ existieren umgekehrt offene Mengen $U_1, \ldots, U_n \subseteq \mathbb{R}$ mit $x \in U_1 \times \ldots \times U_n \subseteq U$. Dies zeigt, dass die euklidische Metrik auf M genau die Produkt-Topologie der euklidischen Metrik auf $\mathbb{R}$ ist. Nach Lemma II.10.27 $[a, b]$ ein kompakter Raum bezüglich der Relativtopologie. Nach Tychonoff ist auch $[a, b]^n$ kompakt. Nach Bemerkung II.10.13 ist A kompakt. □

Satz II.10.29 (Lebesgue)**.** *Sei (M, d) ein kompakter metrischer Raum und $M = \bigcup_{i\in I} U_i$ eine offene Überdeckung. Dann existiert ein $\delta > 0$, sodass jede Teilmenge $A \subseteq M$ mit $d(A) \leq \delta$ in einem U_i liegt.*

Beweis. Für jedes $x \in M$ existiert ein $\epsilon_x > 0$, sodass $B_{2\epsilon_x}(x)$ in einem U_i liegt. Da M kompakt ist, existieren $x_1, \ldots, x_n \in M$ mit $M = \bigcup_{i=1}^n B_{\epsilon_{x_i}}(x_i)$. Sei $\delta := \min\{\epsilon_{x_i} : i = 1, \ldots, n\}$. Sei $a \in A \cap B_{\epsilon_{x_i}}(x_i)$. Für alle $b \in A$ gilt

$$d(b, x_i) \leq d(b, a) + d(a, x_i) < \delta + \epsilon_{x_i} \leq 2\epsilon_{x_i}$$

und $A \subseteq B_{2\epsilon_{x_i}}(x_i)$. Dies zeigt die Behauptung. □

Definition II.10.30. Seien $(A, \mathcal{A})$ und $(B, \mathcal{B})$ topologische Räume. Eine Abbildung $f\colon A \to B$ heißt *stetig*, falls $f^{-1}(C) \in \mathcal{A}$ für alle $C \in \mathcal{B}$ gilt (Urbilder offener Mengen sind offen). Ist f bijektiv und f, f^{-1} stetig, so nennt man f einen *Homöomorphismus*. Ggf. nennt man A und B *homöomorph*.

Bemerkung II.10.31.

(i) Eine Abbildung $f\colon A \to B$ ist genau dann stetig, wenn Urbilder abgeschlossener Mengen abgeschlossen sind, denn $A \setminus f^{-1}(C) = f^{-1}(B \setminus C)$.

(ii) Die Komposition von stetigen Abbildungen ist offensichtlich stetig.

(iii) Ist $f\colon A \to B$ stetig und $K \subseteq A$ kompakt, so ist auch $f(K)$ kompakt, denn ist $f(K) \subseteq \bigcup_{i\in I} U_i$ eine offene Überdeckung, so ist auch $K \subseteq \bigcup_{i\in I} f^{-1}(U_i)$ eine offene Überdeckung.

(iv) Die Produkt-Topologie auf $X := \bigtimes_{i\in I} X_i$ ist die gröbste Topologie, sodass die Projektionen $X \to X_i$, $(x_j)_j \mapsto x_i$ stetig sind.

Beispiel II.10.32.

(i) Anders als in der (linearen) Algebra ist die Umkehrabbildung einer bijektiven stetigen Abbildung nicht automatisch stetig. Betrachte zum Beispiel $A = B = \mathbb{N}$ mit der diskreten Topologie auf A und der trivialen Topologie auf B. Dann ist $f\colon A \to B$, $a \mapsto a$ stetig, aber f^{-1} nicht.

(ii) Die Abbildung $\mathbb{R} \to (0, 1)$, $x \mapsto \frac{1}{1+2^x}$ ist ein Homöomorphismus bzgl. der euklidischen (Relativ)topologie. Ein beschränkter Raum kann also zu einem unbeschränkten Raum homöomorph sein.

Folgerung II.10.33. *Sei A ein kompakter Raum und B ein Hausdorff-Raum. Dann ist jede stetige Bijektion $A \to B$ ein Homöomorphismus.*

Beweis. Sei $f\colon A \to B$ eine stetige Bijektion und $U \subseteq A$ abgeschlossen. Nach Bemerkung II.10.13 und Bemerkung II.10.31 sind U und $f(U)$ kompakt. Nach Lemma II.10.23 ist $f(U)$ abgeschlossen. Daher ist f^{-1} stetig. □

II.11. Hyperreelle und surreale Zahlen

Bemerkung II.11.1. In der Analysis definiert man reelle Zahlen als Äquivalenzklassen von rationalen Cauchyfolgen. Zwei Folgen aus $\mathbb{Q}^{\mathbb{N}}$ betrachtet man dabei als äquivalent, wenn ihre Differenz eine Nullfolge ist. Die gleiche Konstruktion auf $\mathbb{R}$ angewendet bringt nichts Neues, da $\mathbb{R}$ bereits vollständig ist (jede Cauchyfolge konvergiert). Wir definieren daher eine andere Äquivalenzrelation auf $\mathbb{R}^{\mathbb{N}}$.

Definition II.11.2. Sei $\mathcal{F}$ ein Ultrafilter auf $\mathbb{N}$, der alle koendlichen Mengen enthält (und daher nach Lemma II.10.4 keine endliche Menge enthält). Wir definieren eine Äquivalenzrelation $\sim$ auf $\mathbb{R}^{\mathbb{N}}$ durch

$$(a_0, a_1, \ldots) \sim (b_0, b_1, \ldots) \ :\Longleftrightarrow\ \{n \in \mathbb{N} : a_n = b_n\} \in \mathcal{F}.$$

Für $a = (a_n)_n \in \mathbb{R}^{\mathbb{N}}$ sei $[a]$ die Äquivalenzklasse von a. Man nennt ${}^*\mathbb{R} := \{[a] : a \in \mathbb{R}^{\mathbb{N}}\}$ die Menge der *hyperreellen* Zahlen. Für $a, b \in \mathbb{R}^{\mathbb{N}}$ definieren wir

$$\begin{aligned}
[a] + [b] &:= [(a_n + b_n)_n],\\
[a] \cdot [b] &:= [(a_n b_n)_n],\\
[a] < [b] &:\Longleftrightarrow \{n \in \mathbb{N} : a_n < b_n\} \in \mathcal{F}.
\end{aligned}$$

Bemerkung II.11.3.

(i) Seien $a, b, c \in \mathbb{R}^{\mathbb{N}}$ mit $a \sim b \sim c$. Dann liegen $S := \{n \in \mathbb{N} : a_n = b_n\}$ und $T := \{n \in \mathbb{N} : b_n = c_n\}$ in $\mathcal{F}$. Wegen $S \cap T \subseteq \{n \in \mathbb{N} : a_n = c_n\}$ gilt $a \sim c$. Daher ist $\sim$ tatsächlich eine Äquivalenzrelation. Mit dem gleichen Argument zeigt man, dass $+$, $\cdot$ und $<$ auf ${}^*\mathbb{R}$ wohldefiniert sind. Außerdem gelten die üblichen Rechenregeln und (II.8.1). Wir definieren zusätzlich $-[a] := [(-a_n)_n]$ und

$$|[a]| := \begin{cases} [a] & \text{falls } [a] \geq 0,\\ -[a] & \text{sonst} \end{cases}$$

für $a \in {}^*\mathbb{R}$. Man zeigt leicht $|xy| = |x||y|$ und $|x + y| \leq |x| + |y|$ für $x, y \in {}^*\mathbb{R}$ (da $|.|$ nicht nach $\mathbb{R}$ abbildet, handelt es sich formal nicht um eine Norm).

(ii) Durch $r \mapsto [(r, r, \ldots)]$ kann man $\mathbb{R}$ in ${}^*\mathbb{R}$ einbetten. Andererseits ist $x := [(0, 1, \ldots)] \in {}^*\mathbb{R} \setminus \mathbb{R}$ mit $r < x$ für alle $r \in \mathbb{R}$. Anlog ist $x := [(2^0, 2^{-1}, \ldots)] \in {}^*\mathbb{R}$ mit $0 < x < r$ für alle positiven $r \in \mathbb{R}$. Nach Satz II.7.8 und Satz II.8.10 ist $|\mathbb{R}| \leq |{}^*\mathbb{R}| \leq |\mathbb{R}^{\mathbb{N}}| = |2^{\mathbb{N}}| = |\mathbb{R}|$, d. h. $\mathbb{R}$ und ${}^*\mathbb{R}$ sind gleichmächtig.

(iii) Sicher ist $1 \in \mathbb{R} \subseteq {}^*\mathbb{R}$ ein neutrales Element der Multiplikation. Sei $a \in {}^*\mathbb{R} \setminus \{0\}$ und

$$b_n := \begin{cases} a_n^{-1} & \text{falls } a_n \neq 0,\\ 0 & \text{sonst} \end{cases}$$

für $n \in \mathbb{N}$. Nach Lemma II.10.4 gilt $\{n \in \mathbb{N} : a_n \neq 0\} \in \mathcal{F}$. Für $b = (b_n)_n$ ist daher $[a] \cdot [b] = 1$. Dies zeigt, dass ${}^*\mathbb{R}$ ein angeordneter Körper ist.

(iv) Unter Annahme der Kontinuumshypothese kann man zeigen, dass ${}^*\mathbb{R}$ nicht wesentlich von der Wahl des Ultrafilters $\mathcal{F}$ abhängt. Ersetzt man in der Analysis die reellen Zahlen durch die hyperreellen Zahlen, so spricht man von *Nichtstandard-Analysis*.

Definition II.11.4. Eine hyperreelle Zahl x heißt *endlich*, falls ein $n \in \mathbb{N}$ mit $|x| < n$ existiert. Ggf. nennt man

$$\operatorname{st}(x) := \sup\{r \in \mathbb{R} : r \leq x\} \in \mathbb{R}$$

Standardteil von x. Sei $\mathbb{E} \subseteq {}^*\mathbb{R}$ die Menge der endlichen hyperreellen Zahlen.

Bemerkung II.11.5.

(i) Genau dann ist $x \in {}^*\mathbb{R}$ endlich, wenn x auf einer Indexmenge in $\mathcal{F}$ beschränkt ist. Daraus folgt leicht, dass $\mathbb{E}$ unter Addition und Multiplikation (aber nicht Division) abgeschlossen ist.

(ii) Aus $x < n \in \mathbb{N}$ folgt, dass die Menge $\{r \in \mathbb{R} : r \leq x\}$ beschränkt ist und daher ein Supremum besitzt.

Satz II.11.6.

(i) Für $x \in \mathbb{E}$ ist $\operatorname{st}(x)$ die einzige reelle Zahl mit $|x - \operatorname{st}(x)| < r$ für alle positiven $r \in \mathbb{R}$, d. h. $\operatorname{st}(x)$ liegt „beliebig nah“ bei x. Insbesondere ist $\operatorname{st}(x) = x$ genau dann, wenn $x \in \mathbb{R}$.

(ii) Für $x, y \in \mathbb{E}$ gilt

$$\operatorname{st}(x+y) = \operatorname{st}(x) + \operatorname{st}(y), \qquad \operatorname{st}(xy) = \operatorname{st}(x)\operatorname{st}(y), \qquad x \leq y \implies \operatorname{st}(x) \leq \operatorname{st}(y).$$

Beweis.

(i) Im Fall $r + \operatorname{st}(x) \leq x$ wäre $\operatorname{st}(x)$ keine obere Schranke von $M := \{s \in \mathbb{R} : s \leq x\}$. Also gilt $x - \operatorname{st}(x) < r$. Da $\operatorname{st}(x)$ die kleinste obere Schranke von M ist, existiert ein $s \in \mathbb{R}$ mit $\operatorname{st}(x) - r < s < x$. Daraus folgt $\operatorname{st}(x) - x < r$. Insgesamt ist $|x - \operatorname{st}(x)| < r$ für alle positiven $r \in \mathbb{R}$. Angenommen $t \in \mathbb{R}$ erfüllt die gleiche Abschätzung. Dann gilt nach der Dreiecksungleichung $|\operatorname{st}(x) - t| \leq |\operatorname{st}(x) - x| + |x - t| < 2r$ für alle $r \in \mathbb{R}$. Es folgt $t = \operatorname{st}(x)$.

(ii) Nach (i) gilt $|x + y - \operatorname{st}(x) - \operatorname{st}(y)| \leq |x - \operatorname{st}(x)| + |y - \operatorname{st}(y)| \leq r$ für alle positiven $r \in \mathbb{R}$. Aus der Eindeutigkeit in (i) folgt $\operatorname{st}(x+y) = \operatorname{st}(x) + \operatorname{st}(y)$. Analog erhält man $\operatorname{st}(xy) = \operatorname{st}(x)\operatorname{st}(y)$ aus

$$|xy - \operatorname{st}(x)\operatorname{st}(y)| \leq |x(y - \operatorname{st}(y)) + (x - \operatorname{st}(x))\operatorname{st}(y)| \leq |x||y - \operatorname{st}(y)| + |x - \operatorname{st}(x)||\operatorname{st}(y)|.$$

Sei nun $x \leq y$. Dann ist $\operatorname{st}(y)$ eine obere Schranke von $\{r \in \mathbb{R} : r \leq x\}$. Dies zeigt $\operatorname{st}(x) \leq \operatorname{st}(y)$. □

Bemerkung II.11.7. Wir verallgemeinern die Konstruktion der Dedekind-Schnitte, um eine deutlich größere Klasse von Zahlen zu definieren.

Definition II.11.8 (Conway)**.** Sei $\mathbb{S}_0 := \varnothing$. Rekursiv definieren wir für jede Kardinalzahl $\mathfrak{a} > 0$ die Menge $\mathbb{S}_\mathfrak{a}$ aller Paare der Form $\{L, R\}$ mit folgenden Eigenschaften:

- $L, R \subseteq \bigcup_{\mathfrak{b}<\mathfrak{a}} \mathbb{S}_\mathfrak{b}$.
- $\forall l \in L, r \in R : r \not\leq l$.

Die Relation $\leq$ ist dabei ebenfalls rekursiv definiert durch

$$\{L, R\} \leq \{L', R'\} \ :\Longleftrightarrow\ \forall l \in L, r' \in R' : \{L', R'\} \not\leq l,\ r' \not\leq \{L, R\}.$$

Wir werden sehen, dass

$$\{L, R\} \sim \{L', R'\} \ :\Longleftrightarrow\ \{L, R\} \leq \{L', R'\} \leq \{L, R\}$$

eine Äquivalenzrelation definiert. Die Äquivalenzklasse von $\{L, R\}$ sei $(L|R)$. Wir werden $\mathbb{S}_\mathfrak{a}$ oft mit der entsprechenden Menge von Äquivalenzklassen identifizieren und die Definition von $\leq$ auf Äquivalenzklassen übertragen. Man nennt dann $\mathbb{S} := \bigcup_\mathfrak{a} \mathbb{S}_\mathfrak{a}$ die Klasse der *surrealen* Zahlen.

Bemerkung II.11.9. Im Folgenden beweisen wir Eigenschaften der surrealen Zahlen mittels transfiniter Induktion. Der Induktionsanfang ist in der Regel trivial, weil es für $\mathbb{S}_0 = \varnothing$ nichts zu zeigen gibt. Wir prüfen zunächst, dass $\leq$ reflexiv und transitiv ist. Sei $(L|R) \in \mathbb{S}$ gegeben mit $L \subseteq \mathbb{S}_\mathfrak{a}$ und $R \subseteq \mathbb{S}_\mathfrak{b}$. Sei $l \in L$ und $r \in R$. Durch Induktion nach $(\mathfrak{a}, \mathfrak{b})$ können wir $l \leq l$ und $r \leq r$ annehmen. Im Fall $(L|R) \leq l$ wäre $l \not\leq l$ und im Fall $r \leq (L|R)$ wäre $r \not\leq r$. Dies zeigt $(L|R) \leq (L|R)$, d. h. $\leq$ und $\sim$ sind reflexiv. Sei nun $(L|R) \leq (L'|R') \leq (L''|R'')$. Angenommen es existiert ein $l \in L$ mit $(L''|R'') \leq l$. Induktiv gilt dann $(L'|R') \leq l$ und $(L|R) \leq l$. Dies widerspricht $l \leq l$. Analog zeigt man $r'' \not\leq (L|R)$ für alle $r'' \in R''$. Damit ist $(L|R) \leq (L''|R'')$ und $\leq$ ist transitiv. Nach Definition ist $\sim$ eine Äquivalenzrelation und $\leq$ eine Ordnungsrelation auf $\mathbb{S}$.

Lemma II.11.10. *Sei $(L|R) \in \mathbb{S}$. Dann gilt $l < (L|R) < r$ für alle $l \in L$ und $r \in R$. Außerdem ist $\leq$ total.*

Beweis. Nach Definition von $(L|R)$ gilt $r \not\leq l$. Sei $l = (L_l|R_l)$. Induktiv gilt $l' < l$ für alle $l' \in L_l$. Im Fall $(L|R) \leq l'$ wäre $(L|R) \leq l$ und $l \not\leq l$. Also ist $(L|R) \not\leq l'$ für alle $l' \in L$. Dies zeigt $l < (L|R)$. Sei nun $r = (L_r, R_r)$. Induktiv gilt $r < r'$ für alle $r' \in R_r$. Im Fall $r' \leq (L|R)$ wäre $r \leq (L|R)$ im Widerspruch zu $r \leq r$. Daher gilt $(L|R) < r$. Für die zweite Behauptung sei $(L'|R') \in \mathbb{S}$ mit $(L|R) \not\leq (L'|R')$. Dann existiert ein $l \in L$ mit $(L'|R') \leq l$ oder ein $r' \in R'$ mit $r' \leq (L|R)$. In beiden Fällen folgt $(L'|R') \leq (L|R)$. Dies zeigt die Totalität von $\leq$. □

Bemerkung II.11.11. Nach Lemma II.11.10 gilt $(L|R) \in \mathbb{S}$ genau dann, wenn $l < r$ für alle $l \in L$ und $r \in R$. Außerdem gilt

$$(L|R) \leq (L'|R') \iff \forall l \in L, r' \in R' : l < (L'|R'),\ (L|R) < r'.$$

Dies werden wir ab jetzt benutzen.

Beispiel II.11.12. Um Klammern zu sparen, schreiben wir $(x, y, \ldots|a, b, \ldots) := (\{x, y, \ldots\}|\{a, b, \ldots\})$.

(i) Offenbar besteht $\mathbb{S}_1$ nur aus $0 := (\varnothing|\varnothing)$. Man macht sich klar, dass $1 := (0|\varnothing)$ und $-1 := (\varnothing|0)$ in $\mathbb{S}_2$ liegen, während $(0|0)$ wegen $0 \leq 0$ nicht zugelassen ist. Nach Lemma II.11.10 gilt $-1 < 0 < 1$.

(ii) Genau dann gilt $(L|R) = 0$, falls $l < 0$ und $r > 0$ für alle $l \in L$ und $r \in R$.

(iii) Aus $0 < (-1, 0|\varnothing)$ folgt $(-1, 0|\varnothing) \leq 1 \leq (-1, 0|\varnothing)$, d. h. $(-1, 0|\varnothing) = 1$. Dies lässt sich verallgemeinern.

Lemma II.11.13. *Besitzt L ein größtes Element, so gilt $(L|R) = (\max(L)|R)$. Besitzt R ein kleinstes Element, so gilt $(L|R) = (L|\min(R))$.*

Beweis. Für alle $l \in L$ gilt $l \leq \max L < (\max(L)|R)$ nach Lemma II.11.10. Für alle $r \in R$ ist $(L|R) < r$. Dies zeigt $(L|R) \leq (\max(L)|R)$. Nach Lemma II.11.10 ist außerdem $\max L < (L|R)$ und $(\max(L)|R) < r$. Es folgt $(\max(L)|R) = (L|R)$. Die zweite Aussage ist analog. □

Definition II.11.14. Für $x := (L|R) \in \mathbb{S}$ und $y := (L'|R') \in \mathbb{S}$ definieren wir rekursiv:

$$\begin{aligned} x + y &:= \big((L + y) \cup (x + L') \mid (R + y) \cup (x + R')\big), \\ -x &:= (-R \mid -L), \end{aligned}$$

wobei $x + L = \{x + l : l \in L\}$.

Bemerkung II.11.15. Es ist keineswegs trivial, dass die Addition mit $\sim$ verträglich ist und tatsächlich surreale Zahlen produziert. Im ersten Schritt können wir die Definition gedanklich zunächst nur auf die ursprünglichen Elemente $\{L, R\}$ anwenden und die Forderung $l < r$ für $l \in L$ und $r \in R$ ignorieren. Der nächste Schritt zur Wohldefiniertheit ist das folgende Lemma.

Lemma II.11.16. *Für alle $x, y, z \in \mathbb{S}$ gilt*

$$x \leq y \iff x + z \leq y + z.$$

Beweis. Sei $x = (L|R) \in \mathbb{S}_{\mathfrak{a}}$, $y = (L'|R') \in \mathbb{S}_{\mathfrak{b}}$ und $z = (L''|R'') \in \mathbb{S}_{\mathfrak{c}}$. Wie üblich seien $l, r, l', \ldots$ Elemente aus $L, R, L', \ldots$. Wir wählen Kardinalzahlen $\bar{\mathfrak{a}} \leq \bar{\mathfrak{b}} \leq \bar{\mathfrak{c}}$ mit $\{\mathfrak{a}, \mathfrak{b}, \mathfrak{c}\} = \{\bar{\mathfrak{a}}, \bar{\mathfrak{b}}, \bar{\mathfrak{c}}\}$. Sei $x+z \leq y+z$, aber $x > y$. Dann existiert ein l mit $l \geq y$ oder ein r' mit $r' \leq x$. Durch Induktion nach $(\bar{\mathfrak{a}}, \bar{\mathfrak{b}}, \bar{\mathfrak{c}})$ folgt $l + z \geq y + z$ oder $r' + z \leq x + z$ (der Induktionsanfang folgt aus der einfachen Gleichung $0 + 0 = 0$). Beides widerspricht $x + z \leq y + z$. Daher gilt $x \leq y$.

Sei nun $x \leq y$, aber $x + z > y + z$. Dann gilt eine der folgenden Aussagen:

$$l + z \geq y + z, \qquad x + l'' \geq y + z, \qquad x + z \geq r' + z, \qquad x + z \geq y + r''.$$

Induktiv gilt $y + l'' \geq x + l''$ und $y + r'' \geq x + r''$. Nach dem ersten Teil des Beweises folgt eine der Aussagen:

$$l \geq y, \qquad l'' \geq z, \qquad x \geq r', \qquad z \geq r''.$$

Alle Aussagen widersprechen $x \leq y$ oder Lemma II.11.10. □

Bemerkung II.11.17. Aus Lemma II.11.16 folgt

$$\begin{aligned} x < y &\iff x + z < y + z, \\ x \leq x',\ y \leq y' &\implies x + y \leq x' + y'. \end{aligned}$$

Mit den üblichen Bezeichnungen gilt $l + y < r + y$, $l + y < x + r'$, $x + l' < r + y$ und $x + l' < x + r'$. Dies zeigt $x + y \in \mathbb{S}$. Ist $x = x'$ und $y = y'$, so ergibt sich $x + y = x' + y'$, d. h. die Addition ist wohldefiniert. Ähnlich zeigt man

$$x \leq y \iff -y \leq -x.$$

Aus $l < r$ folgt insbesondere $-r < -l$. Also ist auch $-x \in \mathbb{S}$.

Lemma II.11.18. *Für alle $x, y, z \in \mathbb{S}$ gilt:*

(i) $x + y = y + x$ *und* $(x + y) + z = x + (y + z)$.

(ii) $x + 0 = x$ *und* $x + (-x) = 0$.

Beweis. Wie üblich sei $x = (L|R)$, $y = (L'|R')$ und $z = (L''|R'')$.

(i) Die Gleichung $x + y = y + x$ ist trivial. Es gilt

$$\begin{aligned}(x+y)+z &= (L + y \cup x + L' \mid R + y, x + R') + z \\ &= \big((L+y)+z \cup (x+L')+z \cup (x+y)+L'' \mid \\ &\qquad (R+y)+z \cup (x+R')+z \cup (x+y)+R''\big) \\ &= \big(L+(y+z) \cup x+(L'+z) \cup x+(y+L'') \mid \\ &\qquad R+(y+z) \cup x+(R'+z) \cup x+(y+R'')\big) \\ &= x + (L' + z \cup y + L'' \mid R' + z \cup y + R'') \\ &= x + (y+z)\end{aligned}$$

(ii) Offenbar gilt $0 + 0 = (\varnothing|\varnothing) = 0$. Induktiv folgt $x + 0 = (L + 0 \mid R + 0) = (L, R) = x$. Außerdem ist $x + (-x) = (L + (-x) \cup x + (-R) \mid R + (-x) \cup x + (-L))$. Aus Lemma II.11.16 folgt induktiv $l + (-x) < l + (-l) = 0$ und $x + (-r) < r + (-r) = 0$. Dies zeigt $x + (-x) \leq 0$. Analog ist $0 = r + (-r) < r + (-x)$ und $0 = l + (-l) < x + (-l)$. Damit ist $0 \leq x + (-x)$ bewiesen. □

Bemerkung II.11.19. Lemma II.11.18 zeigt, dass die surrealen Zahlen bzgl. Addition eine abelsche Gruppe bilden. Wir können nun wie gewohnt $x - y$ anstelle von $x + (-y)$ schreiben.

Beispiel II.11.20.

(i) Wir haben bereits $1 = (0|\varnothing)$ definiert. Für $n \in \mathbb{N}_+$ setzen wir induktiv $n := (n-1|\varnothing)$. Dann gilt

$$n + m = (n-1 \mid \varnothing) + (m-1 \mid \varnothing) = (n-1+m,\ n+m-1 \mid \varnothing) = (n+m-1 \mid \varnothing).$$

Auf diese Weise kann man alle ganzen Zahlen als surreale Zahlen auffassen. Allgemeiner kann man jede Kardinalzahl $\mathfrak{a}$ mit $(\{\mathfrak{b} : \mathfrak{b} < \mathfrak{a}\} \mid \varnothing)$ identifizieren.

(ii) Sei $x := (0|1) \in \mathbb{S}$. Nach Lemma II.11.10 gilt $0 < x < 1$ und $x + x = (x|x+1)$. Es folgt $x + x \leq 1 \leq x + x$. Man kann also $\frac{1}{2} := (0|1)$ definieren. Analog zeigt man $\frac{1}{4} = (0|\frac{1}{2})$ usw. Auf diese Weise lassen sich alle rationalen Zahlen der Form $\frac{a}{2^n}$ mit $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ als surreale Zahlen realisieren. Für jede weitere reelle Zahl $r \in \mathbb{R}$ existieren $a_n \in \mathbb{Z}$ mit $a_n 2^{-n} < r < (a_n + 1)2^{-n}$ für alle $n \in \mathbb{N}$. Es folgt

$$r = \big(\{a_n 2^{-n} : n \in \mathbb{N}\} \mid \{(a_n+1)2^{-n} : n \in \mathbb{N}\}\big) \in \mathbb{S}.$$

Definition II.11.21. Für surreale Zahlen $x = (L|R)$ und $y = (L'|R')$ definieren wir

$$x \cdot y := xy := (ly + xl' - ll',\ ry + xr' - rr' \mid ly + xr' - lr',\ ry + xl' - rl' : l, l', r, r'),$$

wobei jeder Term wie $ly + xl' - ll'$ zu einem Tupel von Parametern wie $(l, l') \in L \times L'$ gehört.

Lemma II.11.22. *Für alle* $x, x_1, x_2, y, y_1, y_2 \in \mathbb{S}$ *gilt:*

(i) $xy \in \mathbb{S}$.

(ii) Aus $x = y$ *folgt* $xz = yz$.

(iii) *Aus* $x_1 \leq x_2$ *und* $y_1 \leq y_2$ *folgt* $x_1y_2 + x_2y_1 \leq x_1y_1 + x_2y_2$. *Die Ungleichung ist strikt, falls* $x_1 < x_2$ *und* $y_1 < y_2$.

(iv) $x, y > 0 \implies xy > 0$.

Beweis. Wir beweisen die ersten drei Aussagen simultan durch Induktion.

(i) Die Bestandteile von xy sind induktiv surreale Zahlen. Wir müssen

$$\begin{aligned} l_1y + xl' - l_1l' &< l_2y + xr' - l_2r', & ly + xl'_1 - ll'_1 &< ry + xl'_2 - rl'_2, \\ ry + xr'_1 - rr'_1 &< ly + xr'_2 - lr'_2, & r_1y + xr' - r_1r' &< r_1y + xl' - r_1l' \end{aligned}$$

zeigen. Nehmen wir $l_1 \leq l_2$ an. Dann folgt $l_1y + l_2l' \leq l_1l' + l_2y$ und $l_2r' + xl' < l_2l' + xr'$ aus (iii). Insgesamt ist

$$l_1y + xl' - l_1l' \leq l_2y + xl' - l_2l' < l_2y + xr' - l_2r'.$$

Gilt hingegen $l_2 \leq l_1$, so hat man $l_1r' + xl' < l_1l' + xr'$, $l_2r' + l_1y \leq l_2y + l_1r'$ und

$$l_1y + xl' - l_1l' < l_1y + xr' - l_1r' \leq l_2y + xr' - l_2r'.$$

Damit ist die erste der vier Ungleichungen bewiesen. Die anderen drei sparen wir uns.

(ii) Induktiv gilt bereits $xl'' = yl''$ und $xr'' = yr''$. Mit (iii) folgt $lz + xl'' - ll'' < yz$ und $rz + xr'' - rr'' < yz$. Analog zeigt man $xz < l'z + yr'' - l'r''$ und $xz < r'z + yl'' - r'l''$. Also gilt $xz \leq yz$. Aus Symmetriegründen folgt $yz \leq xz$.

(iii) Nach (ii) können wir $x_1 < x_2$ und $y_1 < y_2$ annehmen (man beachte, dass wir im Beweis von (ii) nur die strikte Ungleichung für (iii) benutzt haben). Wir bezeichnen die zu beweisende Ungleichung mit $U(x_1, x_2, y_1, y_2)$. Wir benutzen Induktion nach $(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d})$, wobei $y_1 \in \mathbb{S}_\mathfrak{a}$, $y_2 \in \mathbb{S}_\mathfrak{b}$, $x_1 \in \mathbb{S}_\mathfrak{c}$, $x_2 \in \mathbb{S}_\mathfrak{d}$. Wäre $l_2 < x_1$ und $x_2 < r_1$ für alle l_2 und r_1, so hätten wir $x_2 < x_1$. Also gilt $x_1 < r_1 \leq x_2$ für ein l_2 oder $x_1 \leq l_2 < x_2$ für ein r_1. Nehmen wir den ersten Fall an (der zweite Fall ist analog). Induktiv gilt $U(r_1, x_2, y_1, y_2)$. Es genügt, $U(x_1, r_1, y_1, y_2)$ mit strikter Ungleichung zu zeigen, denn dann wäre

$$\begin{aligned} (x_1y_2 + r_1y_1) + x_2y_1 < x_1y_1 + (r_1y_2 + x_2y_1) &\leq x_1y_1 + r_1y_1 + x_2y_2, \\ x_1y_2 + x_2y_1 &< x_1y_1 + x_2y_2 \end{aligned}$$

nach Bemerkung II.11.17. Wir können nun analog $y_1 < r'_1 \leq y_2$ annehmen. Dann gilt $U(x_1, r_1, r'_1, y_2)$ und es verbleibt $U(x_1, r_1, y_1, r'_1) = U(x, r, y, r')$ mit strikter Ungleichung zu beweisen. Das bedeutet $ry + xr' - rr' < xy$ und gilt nach (i) (im Beweis von (i) haben wir (iii) nur für eine niedrigere Induktionsstufe benutzt).

(iv) Folgt aus (iii) mit $(x_1, x_2, y_1, y_2) = (0, x, 0, y)$. □

Lemma II.11.23. *Für alle* $x, y, z \in \mathbb{S}$ *gilt:*

(i) $xy = yx$ *und* $(x + y)z = xz + yz$.

(ii) $(xy)z = x(yz)$.

(iii) $1x = x$.

Beweis.

(i) Vertauscht man x und y, so bleiben die Terme auf der linken Hälfte von xy invariant, während die Terme auf der rechten Hälfte vertauscht werden. Dies zeigt $xy = yx$. Sei $x + y = (S|T)$ und $s \in S$ sowie $t \in T$. Der erste Term der linken Hälfte von $(x+y)z$ besteht aus Elementen der Form

$$\begin{aligned}\{sz + (x+y)l'' - sl''\} &= \{(l+y)z + (x+y)l'' - (l+y)l'',\ (x+l')z + (x+y)l'' - (x+l')l''\} \\ &= \{(lz + xl'' - ll'') + yz,\ xz + (l'z + yl'' - l'l'')\}.\end{aligned}$$

Dies sind Bestandteile der linken Hälfte von $xz + yz$. Die anderen Terme behandelt man analog.

(ii) Die linke Hälfte von $(xy)z$ besteht nach (i) und Induktion aus Elementen der Form

$$\begin{aligned}(ly + xl' - ll')z + (xy)l'' - (ly + xl' - ll')l'' &= l(yz) + x(l'z + yl'' - l'l'') - l(l'z + yl'' - l'l''), \\ (ry + xr' - rr')z + (xy)l'' - (ry + xr' - rr')l'' &= r(yz) + x(r'z + yl'' - r'l'') - r(r'z + yl'' - r'l''), \\ (ly + xr' - lr')z + (xy)r'' - (ly + xr' - lr')r'' &= l(yz) + x(r'z + yr'' - r'r'') - l(r'z + yr'' - r'r''), \\ (ry + xl' - rl')z + (xy)r'' - (ry + xl' - rl')r'' &= r(yz) + x(l'z + yr'' - l'r') - r(l'z + yr'' - l'r').\end{aligned}$$

Das stimmt mit der linken Hälfte von $x(yz)$ überein. Analog behandelt man die jeweils rechten Hälften.

(iii) Es gilt

$$\begin{aligned}x \cdot 0 &= x \cdot (\varnothing|\varnothing) = (\varnothing|\varnothing) = 0, \\ x \cdot 1 &= x \cdot (0|\varnothing) = (l1 + x0 - l0 \mid r1 + x0 - r0) = (L|R) = x.\end{aligned}$$ □

Beispiel II.11.24. Für $n, m \in \mathbb{N}_+$ gilt

$$nm = \big((n-1)m + n(m-1) - (n-1)(m-1) \mid \varnothing\big) = (nm - 1 \mid \varnothing)$$

wie zu erwarten. Außerdem ist

$$2 \cdot \frac{1}{2} = (1|\varnothing) \cdot (0|1) = \Big(\frac{1}{2} + 2 \cdot 0 - 1 \cdot 0 \;\Big|\; \frac{1}{2} + 2 \cdot 1 - 1 \cdot 1\Big) = \Big(\frac{1}{2} \;\Big|\; \frac{3}{2}\Big) = 1.$$

Bemerkung II.11.25.

(i) Die Definition von xy lässt sich durch folgende Ungleichungen motivieren:

$$(x-l)(y-l') > 0, \qquad (r-x)(r'-y) > 0, \qquad (x-l)(r'-y) > 0, \qquad (r-x)(y-l') > 0.$$

(ii) Aus Lemma II.11.23 folgt, dass $(\mathbb{S}, +, \cdot)$ ein kommutativer Ring ist (sofern man darauf verzichtet, dass Ringe Mengen sein müssen). Man kann weiter zeigen, dass $\mathbb{S}$ sogar ein (angeordneter) Körper ist, d. h. jedes $x \in \mathbb{S} \setminus \{0\}$ besitzt ein multiplikatives Inverses. Die rekursive Definition von x^{-1} ist jedoch aufwendig, wie man bereits an

$$\frac{1}{3} = (2|\varnothing)^{-1} = \Big(\sum_{k=1}^{n} \frac{1}{4^k} \;\Big|\; \frac{1}{4^n} + \sum_{k=1}^{n} \frac{1}{4^k} : n \in \mathbb{N}\Big)$$

sieht. Wir haben bereits nachgerechnet, dass Addition und Multiplikation von natürlichen Zahlen mit den entsprechenden Operationen in $\mathbb{S}$ übereinstimmen. Daraus folgt leicht, dass $\mathbb{Q}$ ein Teilkörper

von $\mathbb{S}$ ist. Dies lässt sich auf $\mathbb{R}$ erweitern. Sei dazu $r = (a_n | b_n : n \in \mathbb{N}) \in \mathbb{R}$ mit $a_n, b_n \in \mathbb{Q}$ wie in Beispiel II.11.20. Für $m \in \mathbb{N}_+$ gilt zunächst

$$\begin{aligned} mr &= \big((m-1)r + ma_n - (m-1)a_n \mid (m-1)r + mb_n - (m-1)b_n\big) \\ &= \big((m-1)r + a_n \mid (m-1)r + b_n\big), \end{aligned}$$

wobei beide Seiten im Reellen gegen mr konvergieren. Sei nun $s = (a'_n | b'_n)$ mit $a'_n, b'_n \in \mathbb{Q}$. Dann gilt

$$rs = (a_n s + r a'_m - a_n a'_m,\ b_n s + r b'_m - b_n b'_m \mid a_n s + r b'_m - a_n b'_m,\ b_n s + r a'_m - b_n a'_m),$$

wobei wieder beide Seiten gegen rs konvergieren. Somit ist auch $\mathbb{R}$ ein Teilkörper von $\mathbb{S}$ mit der gleichen Ordnungsrelation. Man kann allgemeiner zeigen, dass jeder angeordnete Körper ein Teilkörper von $\mathbb{S}$ ist.

(iii) Im Gegensatz zu $\mathbb{R}$ stimmt die Arithmetik beliebiger Kardinalzahlen nicht mit den Operationen in $\mathbb{S}$ überein. Nach Satz II.7.8 gilt beispielsweise $\mathbb{N} + \mathbb{N} = \mathbb{N}$. Dies bedeutet umgekehrt, dass man surreale Zahlen mit überraschenden Eigenschaften konstruieren kann. Sei dafür $\mathfrak{a} = (\mathbb{N} | \varnothing) \cong \mathbb{N}$. Dann erhält man mit $x := (\mathbb{N} | \mathfrak{a})$ eine surreale Zahl, die größer als jede reelle Zahl, aber kleiner als $\mathfrak{a}$ ist. Genauer gilt

$$x + 1 = (\mathbb{N} + 1, x \mid \mathfrak{a} + 1) = (x \mid \mathfrak{a} + 1) = \mathfrak{a},$$

wie man leicht nachrechnet. Sei nun $y := (\mathbb{N} \mid \mathfrak{a} - n : n \in \mathbb{N})$. Dann gilt

$$y + y = (\mathbb{N} + y \mid \mathfrak{a} - \mathbb{N} + y) = \mathfrak{a},$$

denn $n + y < \mathfrak{a}$, $n < n + y$ und $\mathfrak{a} < \mathfrak{a} - n + y$. Man kann also $y = \frac{\mathfrak{a}}{2}$ definieren. Sei schließlich $z := (\mathbb{N} \mid 2^{-n}\mathfrak{a} : n \in \mathbb{N})$. Aus Lemma II.11.10 folgt $nz < \mathfrak{a}$ und $(2^{-n} + 2^{-m})z < 2^{-n-m}\mathfrak{a}$ für alle $n, m \in \mathbb{N}$. Damit ergibt sich

$$z^2 = \big(nz + zm - nm,\ 2^{-n}\mathfrak{a}z + 2^{-m}\mathfrak{a}z - 2^{-n-m}\mathfrak{a}^2 \mid nz + z2^{-m}\mathfrak{a} - n2^{-m}\mathfrak{a}\big) \leq \mathfrak{a}.$$

Umgekehrt ist $\mathfrak{a} \leq z^2$, denn $n < z^2$ und $\mathfrak{a} < nz + z2^{-m}\mathfrak{a} - n2^{-m}\mathfrak{a}$. Dies zeigt $y^2 = \mathfrak{a}$ und $y = \sqrt{\mathfrak{a}}$. Man kann allgemeiner zeigen, dass jede positive surreale Zahl für jedes $n \in \mathbb{N}_+$ eine n-te Wurzel besitzt. Analog zur Konstruktion von $\mathbb{C}$ aus $\mathbb{R}$, erhält man durch Adjunktion einer Quadratwurzel von -1 zu $\mathbb{S}$ einen algebraisch abgeschlossenen Körper.

Aufgaben

Aufgabe II.1. Sei M eine Menge. Zeigen Sie, dass $\mathcal{P}(M)$ bzgl. der *symmetrischen Differenz*

$$A \ominus B := (A \cup B) \setminus (B \cap A)$$

eine Gruppe ist.

Aufgabe II.2. Sei $T(n) \subseteq \mathbb{N}$ die Menge aller positiven Teiler einer Zahl $n \in \mathbb{N}_+$. Untersuchen Sie, wann $T(n)$ bzgl. der Teilbarkeitsrelation total geordnet ist.

Aufgabe II.3. Beweisen oder widerlegen Sie: Zwei total geordnete Mengen sind genau dann isomorph, wenn sie gleichmächtig sind.

Aufgabe II.4.

(a) Konstruieren Sie eine Wohlordnung auf $\mathbb{Z}$.

(b) Für gekürzte Brüche $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}_+$ sei

$$\frac{a}{b} \prec \frac{c}{d} \iff a < c \vee (a = c \wedge b < d).$$

Zeigen Sie, dass $(\mathbb{Q}_+, \prec)$ eine wohlgeordnete Menge ist.

(c) Konstruieren Sie eine Wohlordnung auf $\mathbb{Q}$.

Aufgabe II.5. Zeigen Sie, dass $\mathbb{N}^2 \to \mathbb{N}$, $(x, y) \mapsto 2^x(2y + 1) - 1$ eine Bijektion ist.

Aufgabe II.6. Eine Ordinalzahl $\alpha > 0$, die keinen Nachfolger besitzt, nennt man *Limeszahl*. Zum Beispiel ist $\mathbb{N}$ eine Limeszahl. Für Ordinalzahlen α, β, γ definiert man induktiv

$$\alpha + \beta := \begin{cases} \alpha & \text{falls } \beta = 0, \\ (\alpha + \gamma)^+ & \text{falls } \beta = \gamma^+, \\ \bigcup\limits_{\gamma \in \beta} \alpha + \gamma & \text{falls } \beta \text{ eine Limeszahl ist,} \end{cases}$$

$$\alpha \cdot \beta := \begin{cases} 0 & \text{falls } \beta = 0, \\ \alpha \cdot \gamma + \alpha & \text{falls } \beta = \gamma^+, \\ \bigcup\limits_{\gamma \in \beta} \alpha \cdot \gamma & \text{falls } \beta \text{ eine Limeszahl ist,} \end{cases}$$

$$\alpha^\beta := \begin{cases} 1 & \text{falls } \beta = 0, \\ \alpha^\gamma \cdot \alpha & \text{falls } \beta = \gamma^+, \\ \bigcup\limits_{\gamma \in \beta} \alpha^\gamma & \text{falls } \beta \text{ eine Limeszahl ist.} \end{cases}$$

Wie üblich benutzen wir Punkt- vor Strichrechnung. Zeigen Sie:

(a) Für jede Limeszahl α gilt $\alpha = \bigcup_{\beta \in \alpha} \beta$.

(b) Sei β eine Limeszahl. Dann ist $\alpha + \beta$ eine Limeszahl. Ist $\alpha > 0$ (bzw. $\alpha > 1$), so ist auch $\alpha \cdot \beta$ (bzw. α^β) eine Limeszahl.

(c) Es gilt $\alpha + \beta \cong \alpha \cup 1 \times \beta$, $\alpha \cdot \beta \cong \alpha \times \beta$ und $\alpha^\beta \cong \left\{ f \colon \beta \to \alpha : |b \in \beta : f(b) \neq 0| < \infty \right\}$ mit der Definition aus Bemerkung II.7.13.

(d) Es gilt $(\alpha + \beta) + \gamma \cong \alpha + (\beta + \gamma)$ und $(\alpha \cdot \beta) \cdot \gamma \cong \alpha \cdot (\beta \cdot \gamma)$.

(e) Es gilt $\alpha \cdot (\beta + \gamma) \cong \alpha \cdot \beta + \alpha \cdot \gamma$, aber im Allgemeinen $(\alpha + \beta) \cdot \gamma \ncong \alpha \cdot \gamma + \beta \cdot \gamma$.

(f) Es gilt $\alpha^{\beta+\gamma} \cong \alpha^\beta \cdot \alpha^\gamma$ und $(\alpha^\beta)^\gamma \cong \alpha^{\beta \cdot \gamma}$, aber im Allgemeinen $(\alpha \cdot \beta)^\gamma \ncong \alpha^\gamma \cdot \beta^\gamma$.

(g) Sind α und β abzählbar, so auch $\alpha + \beta$, $\alpha \cdot \beta$ und α^β.
Bemerkung: Als Kardinalzahl ist $\mathbb{N}^\mathbb{N} \geq 2^\mathbb{N} > \mathbb{N}$ überabzählbar.

Aufgabe II.7. Sei G ein vollständiger Graph mit mindestens 17 Ecken, sodass jede Kante rot, gelb oder blau gefärbt ist. Zeigen Sie, dass G ein einfarbiges Dreieck besitzt.
Hinweis: Benutzen Sie die Ramsey-Zahl $R(3, 3) = 6$.

Aufgabe II.8. Zehn Kinder stehen beim Sportunterricht in einer Reihe. Zeigen Sie, dass es drei Jungen oder drei Mädchen gibt, die in gleichen Abständen voneinander stehen (z. B. an Position $3, 5, 7$ oder $1, 5, 9$). Geht das auch noch, wenn einer fehlt?
Bemerkung: Der Satz von VAN DER WAERDEN besagt allgemeiner: Werden die natürlichen Zahlen in zwei Klassen eingeteilt, so existieren für jedes k Zahlen a, d, sodass $a, a + d, a + 2d, \ldots, a + kd$ in einer Klasse liegen.

Stichwortverzeichnis