

Mathematische Logik

Kurzskript

A. Martin-Pizarro
Albert-Ludwigs-Universität Freiburg
Sommersemester 2025
`pizarro@math.uni-freiburg.de`

16. Juli 2025

Anmerkungen.

Dieses Kurzsript ist während im Wintersemester 2018/19 und 2020/2021 an der Albert-Ludwigs-Universität in Freiburg gehaltenen Vorlesung „Logik für Studierende der Informatik“ sowie der im Sommersemester 2019 gehaltenen Vorlesung „Mathematische Logik“ entstanden und stark geprägt von den Skripten meiner Kollegen Martin Ziegler und Markus Junker. Deren Einflüsse sind nicht zu trennen und können nicht einzeln dargelegt werden.

Zu meinem eigenen Beitrag gehören sicherlich die zahlreichen Fehler, welche es im Skript definitiv geben wird. Ich bin sehr dankbar über die Mitteilung solcher Fehler und Ungenauigkeiten. Insbesondere bedanke ich mich bei Frau Nadja Valentin und bei Herrn Michael Lösch für ihr aufmerksames Korrekturlesen und ihre Geduld, sowie bei Herrn Arnt-Jonas Trabert, Herrn Patrick Meurin und Herrn Sören Andres.

Inhaltsverzeichnis

1	Aussagenlogik	1
1.1	Formeln und Tautologien	1
1.2	Normalformen	3
2	Prädikatenlogik	5
2.1	Sprachen und Strukturen	5
2.2	Theorien und Beweise	10
2.3	Vollständigkeit und Kompaktheit	19
3	Mengenlehre	27
3.1	Das Axiomensystem ZF	27
3.2	Angeordnete Mengen und Ordinalzahlen	33
3.3	Ordinalarithmetik	36
3.4	Auswahlsaxiom und Kardinalität	39
4	Unentscheidbarkeit	43
4.1	Rekursivität	43
4.2	Gödelisierung und rekursiv aufzählbare Mengen	49
4.3	Entscheidbarkeit	53
4.4	Der Gödel'sche Unvollständigkeitssatz	56
4.5	Modelle der Peanoarithmetik	61
	Appendix	65
A	Das Zorn'sche Lemma	66
B	Cantorsche Normalform einer Ordinalzahl	69
C	Ultrafilter und -produkte	71
D	Der chinesische Restsatz	74
	Literaturverzeichnis	75

Kapitel 1

Aussagenlogik

In diesem Abschnitt werden wir die Grundlagen der aristotelischen Aussagenlogik einführen. Dabei gelten das Zweiwertigkeitsprinzip (eine Aussage ist entweder wahr oder falsch) und das Prinzip des ausgeschlossenen Dritten (Beweise ad absurdum oder Widerspruchsbeweise sind gültige Beweise), im Gegensatz zum mathematischen Konstruktivismus bzw. Intuitionismus.

1.1 Formeln und Tautologien

Notation. Wir haben unendlich viele *Aussagenvariablen* (oder *Atome*), welche mit A_1, A_2, \dots bezeichnet werden. Falls wir nur endlich viele Variablen betrachten, werden wir möglicherweise eher A, B, C usw. oder P, Q, R , usw. verwenden.

Definition 1.1. Die Klasse aller *aussagenlogischen Formeln* ist die kleinste Kollektion \mathcal{F} aller Ausdrücke, welche alle Aussagenvariablen enthält und so, dass

- wenn P in \mathcal{F} liegt, so liegt $\neg P$ in \mathcal{F} (*Negation*);
- wenn P und Q in \mathcal{F} liegen, so liegt $(P \vee Q)$ in \mathcal{F} (*Disjunktion*).

Insbesondere haben wir die Eindeutigkeit der Darstellung: Jede aussagenlogische Formel P lässt sich eindeutig schreiben, das heißt, es existieren entweder

- eine eindeutige Aussagenvariable A_i mit $P = A_i$. Wir sagen, dass P der Stufe 0 ist; oder
- eine eindeutige aussagenlogische Formel Q so, dass $P = \neg Q$. Wir sagen, dass P der Stufe $n + 1$ ist, wenn Q der Stufe n ist; oder
- eindeutige aussagenlogischen Formeln Q und R so, dass $P = (Q \vee R)$. Wir sagen, dass P der Stufe $n + 1$ ist, wobei n das Maximum der Stufen von Q und R ist.

Bemerkung 1.2. Mit Hilfe der Stufe einer Formel können wir Eigenschaften der Menge der Formeln zeigen, indem wir sie induktiv über den Aufbau von Formeln zeigen. Insbesondere gelten Eigenschaften, welche für alle Atome gelten und unter Negation und Disjunktion erhalten bleiben, für alle aussagenlogischen Formeln.

Notation. Wir werden folgende Abkürzungen verwenden, wobei wir die Eindeutigkeit der Darstellung dementsprechend verlieren:

- $(P \wedge Q) = \neg(\neg P \vee \neg Q)$ (Konjunktion).
- $(P \rightarrow Q) = (\neg P \vee Q)$ (Implikation).
- $(P \leftrightarrow Q) = ((P \rightarrow Q) \wedge (Q \rightarrow P))$ (Äquivalenz).

Definition 1.3. In aristotelischer Logik ist $\{0, 1\}$ als geordnete Menge (mit $0 < 1$) die Menge der Wahrheitswerte. Eine *Belegung* β ist eine Abbildung

$$\beta : \{A_i\}_{i \in \mathbb{N}} \rightarrow \{0, 1\}.$$

Jede Belegung β lässt sich induktiv nach den folgenden Regeln eindeutig auf die Menge aller aussagenlogischen Formeln fortsetzen:

$$\beta(\neg P) = 1 - \beta(P) \text{ und } \beta((P \vee Q)) = \max\{\beta(P), \beta(Q)\}.$$

Durch Induktion über den Aufbau von Formeln lässt sich folgendes Lemma leicht zeigen:

Lemma 1.4. Wenn zwei Belegungen β_1 und β_2 auf der endlichen Menge der Aussagenvariablen, welche in der aussagenlogischen Formel P vorkommen, übereinstimmen, so gilt $\beta_1(P) = \beta_2(P)$.

Bemerkung 1.5. Eine anschauliche Methode, um zu sehen welche Wahrheitswerte eine aussagenlogische Formel bekommen kann, wird mit Hilfe der Wahrheitstafel gegeben. Zum Beispiel:

A_1	A_2	$\neg A_1$	$(A_1 \vee A_2)$	$(A_1 \wedge A_2)$	$(A_1 \rightarrow A_2)$	$(A_1 \leftrightarrow A_2)$
1	1	0	1	1	1	1
1	0	0	1	0	0	0
0	1	1	1	0	1	0
0	0	1	0	0	1	1

Falls in der aussagenlogischen Formel n Aussagenvariablen vorkommen, steigt die Komplexität der Wahrheitstafel mit Ordnung 2^n . Daher ist es in der Regel praktischer, die *Tableau-Methode* zu verwenden.

Definition 1.6. Eine aussagenlogische Formel P ist eine *Tautologie*, falls $\beta(P) = 1$ für alle Belegungen β .

Zwei aussagenlogische Formeln P und Q sind *logisch äquivalent*, bezeichnet als $P \sim Q$, falls $(P \leftrightarrow Q)$ eine Tautologie ist.

Bemerkung 1.7. Die aussagenlogischen Formeln P und Q sind genau dann logisch äquivalent, wenn $\beta(P) = \beta(Q)$ für alle Belegungen β .

Dass P und Q logisch äquivalent sind bedeutet nicht, dass P und Q als Ausdrücke gleich sind!! Zum Beispiel:

- $((P \vee Q) \vee R)$ ist logisch äquivalent zu $(P \vee (Q \vee R))$, aber die beiden Formeln sind im formellen Sinne verschieden.
- $\neg\neg P \sim P$ aber $\neg\neg P \neq P$ als Aussagenformel.

Bemerkung 1.8. Logische Äquivalenz definiert eine Äquivalenzrelation auf der Klasse der aussagenlogischen Formeln. Mit \top bezeichnen wir die Äquivalenzklasse einer (bzw. jeder) Tautologie und mit \perp die Äquivalenzklasse einer (bzw. jeder) aussagenlogischen Formel, deren Negation eine Tautologie ist, zum Beispiel $(A_1 \wedge \neg A_1)$.

Wir können dementsprechend Ausdrücken der Form $(P \wedge \top)$ oder $(P \vee \top)$ einen Wahrheitswert zuordnen und behandeln diese Symbole formell als aussagenlogische Formeln.

Bemerkung 1.9. Für alle aussagenlogische Formeln P, Q und R gilt:

- $\neg\neg P \sim P$.
- $(P \vee \neg P) \sim \top$ (*Prinzip des ausgeschlossenen Dritten*).
- $(P \wedge \neg P) \sim \perp$ (*Prinzip des ausgeschlossenen Widerspruchs*).
- $\neg(P \wedge Q) \sim (\neg P \vee \neg Q)$ (*Erstes De Morgan'sche Gesetz*)
- $\neg(P \vee Q) \sim (\neg P \wedge \neg Q)$ (*Zweites De Morgan'sche Gesetz*)
- $(P \rightarrow Q) \sim (\neg P \vee Q)$ (*Definition der materialen Implikation*)
- $(P \rightarrow Q) \sim (\neg Q \rightarrow \neg P)$ (*Kontrapositionsgesetz*).
- $(P \leftrightarrow Q) \sim ((P \rightarrow Q) \wedge (Q \rightarrow P))$ (*Definition der materialen Äquivalenz*)
- $(P \wedge (Q \wedge R)) \sim ((P \wedge Q) \wedge R)$ (*Assoziativität der Konjunktion*)
- $(P \vee (Q \vee R)) \sim ((P \vee Q) \vee R)$ (*Assoziativität der Disjunktion*)
- $(P \vee (Q \wedge R)) \sim ((P \vee Q) \wedge (P \vee R))$ (*Distributivgesetz I*)
- $(P \wedge (Q \vee R)) \sim ((P \wedge Q) \vee (P \wedge R))$ (*Distributivgesetz II*)
- $((P \rightarrow Q) \wedge (Q \rightarrow R)) \rightarrow (P \rightarrow R) \sim \top$ (*Inferenz*)
- $((P \wedge (P \rightarrow Q)) \rightarrow Q) \sim \top$ (*Modus Ponens*)

1.2 Normalformen

Notation. Ab jetzt werden wir folgende Abkürzungen verwenden:

- $(P_1 \wedge P_2 \wedge \dots \wedge P_n)$ oder $(\bigwedge_{i=1}^n P_i)$ für die Formel $((\dots (P_1 \wedge P_2) \wedge \dots) \wedge P_n)$.
- $(P_1 \vee P_2 \vee \dots \vee P_n)$ oder $(\bigvee_{i=1}^n P_i)$ für die Formel $((\dots (P_1 \vee P_2) \vee \dots) \vee P_n)$.

Definition 1.10. Eine aussagenlogische Formel ist ein *Literal*, falls sie eine Aussagenvariable oder die Negation davon ist.

Eine aussagenlogische Formel ist in *konjunktiver Normalform* (KNF), falls sie eine endliche Konjunktion $(\bigwedge_{i=1}^n P_i)$ von endlichen Disjunktionen

$$P_i = (L_{i1} \vee \dots \vee L_{in_i})$$

von Literalen L_{ij} ist.

Eine aussagenlogische Formel ist in *disjunktiver Normalform* (DNF), falls sie eine endliche Disjunktion $(\bigvee_{i=1}^n P_i)$ von endlichen Konjunktionen

$$P_i = (L_{i1} \wedge \dots \wedge L_{in_i})$$

von Literalen L_{ij} ist.

Lemma 1.11. *Jede aussagenlogische Formel ist logisch äquivalent zu einer aussagenlogischen Formel in KNF und auch logisch äquivalent zu einer aussagenlogischen Formel in DNF.*

Beweis. Beachte, dass die Negation eines Literales logisch äquivalent zu einem Literal ist. Somit sieht man leicht, dass die Negation einer aussagenlogischen Formel in DNF logisch äquivalent zu einer aussagenlogischen Formel in KNF ist. Weil $P \sim \neg\neg P$, genügt es zu zeigen, dass jede aussagenlogische Formel logisch äquivalent zu einer aussagenlogischen Formel in DNF ist.

Wir beweisen dies durch Induktion über den Aufbau von Formeln. Für Formeln der Stufe 0 ist das trivial. Falls P und Q beide logisch äquivalent zu aussagenlogischen Formeln in DNF sind, so gilt dies klarerweise auch für $(P \vee Q)$. Wir müssen nur zeigen, dass $\neg P$ logisch äquivalent zu einer Formel in DNF ist, falls P logisch äquivalent zu einer Formel in DNF ist.

Falls $P \sim (\bigvee_{i=1}^m P_i)$, wobei jedes $P_i = (L_{i1} \wedge \dots \wedge L_{in_i})$ für Literale L_{ij} , ist

$$\neg P \sim \left(\bigwedge_{i=1}^m (\neg L_{i1} \vee \dots \vee \neg L_{in_i}) \right)$$

Weil die Negation eines Literales logisch äquivalent zu einem Literal ist, können wir mit Hilfe der Distributivitätsgesetze die Konjunktionen mit den Disjunktionen so distributiv umformen, dass $\neg P$ auch logisch äquivalent zu einer Formel in DNF ist. □

Bemerkung 1.12. Wenn wir noch verlangen, dass jedes Literal L_{ij} in jeder endlichen Konjunktion genau einmal vorkommt, bekommen wir eine *kanonische* DNF, welche bis auf Permutation der P_i und innerhalb der P_i bis auf Permutation der Literale eindeutig ist, denn $(L_i \wedge \neg L_i) \sim \perp$.

Kapitel 2

Prädikatenlogik

Nach dem Satz von Lindström ist die Logik erster Stufe die stärkste Logik, in welcher der Kompaktheitssatz (Korollar 2.66) und Löwenheim-Skolem abwärts (Korollar 2.67) gelten. Beide Sätze sind eine Folgerung des *Vollständigkeitssatzes* (Korollar 2.64), welcher besagt, dass *wahr* und *beweisbar* äquivalente Begriffe sind. Wir werden in diesem Abschnitt untersuchen wie mathematische Strukturen als Strukturen erster Stufe betrachtet werden können und den Begriff eines formellen Beweises einführen. Formelle Beweise sind im Kern des *Gödel'schen Unvollständigkeitssatzes*, welcher im nächsten Abschnitt bewiesen wird.

2.1 Sprachen und Strukturen

Definition 2.1. Eine *Sprache* ist eine Menge \mathcal{L} von Konstanten, Funktions- und Relationszeichen.

$$\mathcal{L} = \{c_i\}_{i \in I} \cup \{f_j\}_{j \in J} \cup \{R_k\}_{k \in K}.$$

Jedes Funktionszeichen f_j , bzw. jedes Relationszeichen R_k , hat eine Stelligkeit n_j , bzw. n_k .

Eine *Struktur* \mathcal{A} in der Sprache \mathcal{L} besteht aus einer nicht-leeren Grundmenge A , das *Universum* von \mathcal{A} , zusammen mit Interpretationen der Konstanten-, Funktions- und Relationszeichen der Sprache \mathcal{L} . Dies bedeutet, dass es

- für jedes Konstantenzeichen c_i ein Element aus A gibt, das wir als $c_i^{\mathcal{A}}$ bezeichnen;
- für jedes Funktionszeichen f_j mit Stelligkeit n_j eine Funktion $f_j^{\mathcal{A}} : A^{n_j} \rightarrow A$ gibt;
- für jedes Relationszeichen R_k mit Stelligkeit n_k eine Teilmenge $R_k^{\mathcal{A}}$ von A^{n_k} gibt.

Wir sagen, dass \mathcal{A} eine \mathcal{L} -Struktur ist und schreiben

$$\mathcal{A} = (A, \{c_i^{\mathcal{A}}\}_{i \in I}, \{f_j^{\mathcal{A}}\}_{j \in J}, \{R_k^{\mathcal{A}}\}_{k \in K}).$$

Beispiel 2.2.

- Jede nicht-leere Menge ist eine Struktur in der leeren Sprache.
- Jeder ungerichtete Graph ist eine Struktur in der Graphensprache $\mathcal{L}_{Graph} = \{R\}$ mit Universum die Menge der Knoten und der Interpretation des zweistelligen Relationszeichens R als die Kantenrelation (welche symmetrisch ist).

- Jede Gruppe G ist eine Struktur in der Gruppensprache $\mathcal{L}_{Grp} = \{1, \cdot, ^{-1}\}$.
- Jeder Körper F ist eine Struktur in der Ringsprache $\mathcal{L}_{Ring} = \{0, 1, +, -, \cdot\}$.

Definition 2.3. Eine *Einbettung* der \mathcal{L} -Struktur \mathcal{A} in die \mathcal{L} -Struktur \mathcal{B} ist eine injektive Abbildung $F : A \rightarrow B$, welche mit den Interpretationen kompatibel ist. Dies bedeutet, dass

- für jedes Konstantenzeichen c aus \mathcal{L} ist $F(c^{\mathcal{A}}) = c^{\mathcal{B}}$;
- für jedes Funktionszeichen f aus \mathcal{L} mit Stelligkeit n und Elemente a_1, \dots, a_n aus A gilt

$$F(f^{\mathcal{A}}(a_1, \dots, a_n)) = f^{\mathcal{B}}(F(a_1), \dots, F(a_n));$$

- für jedes Relationszeichen R aus \mathcal{L} mit Stelligkeit m gilt

$$(a_1, \dots, a_m) \text{ liegt genau dann in } R^{\mathcal{A}}, \text{ wenn } (F(a_1), \dots, F(a_m)) \text{ in } R^{\mathcal{B}} \text{ liegt.}$$

Ein *Isomorphismus* ist eine surjektive Einbettung. Falls es einen Isomorphismus von \mathcal{A} nach \mathcal{B} gibt, bezeichnen wir dies mit $\mathcal{A} \simeq \mathcal{B}$.

Bemerkung 2.4. Die Komposition von Einbettungen ist wiederum eine Einbettung. Insbesondere ist die Relation \simeq eine Äquivalenzrelation zwischen \mathcal{L} -Strukturen.

Definition 2.5. Gegeben zwei \mathcal{L} -Strukturen \mathcal{A} und \mathcal{B} , sagen wir, dass \mathcal{A} eine *Unterstruktur* von \mathcal{B} ist, falls $A \subset B$ gilt und die mengentheoretische Inklusion $\text{Id}_A : A \rightarrow B$ eine Einbettung ist. Wir schreiben $\mathcal{A} \subset \mathcal{B}$.

Bemerkung 2.6. Gegeben eine \mathcal{L} -Struktur \mathcal{A} und eine nicht-leere Teilmenge $C \subset A$ derart, dass C alle Interpretationen (in \mathcal{A}) der Konstantenzeichen enthält und unter den (Interpretationen der) Funktionen aus \mathcal{L} abgeschlossen ist, ist C das Universum einer \mathcal{L} -Unterstruktur \mathcal{C} von \mathcal{A} : Setze

$$R^{\mathcal{C}} = C^m \cap R^{\mathcal{A}},$$

für jedes Relationszeichen R der Stelligkeit m aus \mathcal{L} .

Für zwei Unterstrukturen \mathcal{A} und \mathcal{B} einer gemeinsamen Struktur \mathcal{M} in der Sprache \mathcal{L} mit nicht-trivialem Durchschnitt $A \cap B \neq \emptyset$ existiert eine natürliche \mathcal{L} -Unterstruktur mit Universum $A \cap B$, welche wir als $\mathcal{A} \cap \mathcal{B}$ bezeichnen. Insbesondere, gegeben eine nicht-leere Teilmenge $C \subset A$, ist der Durchschnitt aller Unterstrukturen \mathcal{D} von \mathcal{A} , deren Universum D die Menge C enthält, die kleinste Unterstruktur, deren Universum C enthält. Sie ist die von C *erzeugte Unterstruktur* in \mathcal{A} , bezeichnet als $\langle C \rangle_{\mathcal{A}}$. Die Unterstruktur \mathcal{D} von \mathcal{A} ist *endlich erzeugt*, falls es eine endliche Teilmenge C so gibt, dass $\mathcal{D} = \langle C \rangle_{\mathcal{A}}$.

Notation. Im Gegensatz zu den Aussagenvariablen werden die Variablen in der Prädikatenlogik mit den Symbolen x, y, z usw. bezeichnet. Da wir auch in diesem Zusammenhang unendlich viele Variablen besitzen, werden wir abhängig von der Situation die Variablen mit x_1, \dots, x_n, \dots , oder y_1, \dots, y_m, \dots usw. bezeichnen.

Definition 2.7. Die Kollektion von *Termen* einer Sprache \mathcal{L} ist die kleinste Menge TERM von Ausdrücken, welche alle Variablen und Konstantenzeichen enthält, und so, dass

- für jedes n aus \mathbb{N} und Terme t_1, \dots, t_n aus **TERM** sowie jedes n -stellige Funktionszeichen f aus \mathcal{L} , der Ausdruck $f(t_1, \dots, t_n)$ in **TERM** liegt.

Bemerkung 2.8. Die obige Definition impliziert, dass wir die Terme *einstufen* können. Variablen und Konstantenzeichen sind Terme der Stufe 0. Falls t_1, \dots, t_n Terme der Stufe höchstens k sind, ist der Term $f(t_1, \dots, t_n)$ der Stufe höchstens $k + 1$.

Insbesondere hat man die Eindeutigkeit der Darstellung: Jeder Term der Stufe $k > 0$ lässt sich eindeutig schreiben als $f(t_1, \dots, t_n)$ für ein eindeutig bestimmtes Funktionszeichen f und eindeutig bestimmte Terme t_1, \dots, t_n , welche der Stufe höchstens k sind.

Notation. Wie üblich in der Mathematik, werden wir in gewissen Fällen Terme anders darstellen, z. B:

$$t_1 + t_2 \text{ anstatt } +(t_1, t_2).$$

Für einen Term t schreiben wir $t = t[x_1, \dots, x_m]$, wobei die Variablen x_1, \dots, x_m verschieden sind, falls die Variablen, welche in t vorkommen, in der Menge $\{x_1, \dots, x_m\}$ liegen.

ACHTUNG: $t[x_1, \dots, x_n]$ bedeutet nicht, dass jede Variable x_i , für $1 \leq i \leq n$, unbedingt in t vorkommt!!

Somit definiert für jede \mathcal{L} -Struktur \mathcal{A} der Term $t = t[x_1, \dots, x_m]$ eine Funktion

$$t^{\mathcal{A}} : \begin{array}{ccc} A^m & \rightarrow & A \\ (a_1, \dots, a_m) & \mapsto & t^{\mathcal{A}}[a_1, \dots, a_m] \end{array},$$

wobei $t^{\mathcal{A}}[a_1, \dots, a_m]$ der Wert von t evaluiert auf $x_1 = a_1, \dots, x_m = a_m$ ist. Dieser Wert wird induktiv über die Stufe des Termes t definiert:

- Falls $t = c$ für ein Konstantenzeichen c aus \mathcal{L} , ist $t^{\mathcal{A}}$ die konstante Funktion mit Wert $c^{\mathcal{A}}$;
- Falls $t = x_i$ für eine Variable x_i , ist $t^{\mathcal{A}}[a_1, \dots, a_m] = a_i$;
- Falls $t = f(t_1, \dots, t_n)$, ist

$$t^{\mathcal{A}}[a_1, \dots, a_m] = f^{\mathcal{A}}(t_1^{\mathcal{A}}[a_1, \dots, a_m], \dots, t_n^{\mathcal{A}}[a_1, \dots, a_m]).$$

Beispiel 2.9. Sei (G, \cdot, e) eine Gruppe, gesehen als natürliche Struktur in der Gruppensprache $\mathcal{L}_{Gp} = \{1, \cdot, {}^{-1}\}$. Die Terme

$$t_1 = 1 \cdot x \text{ und } t_2 = x$$

definieren die gleichen Funktionen in der Struktur $\mathcal{G} = (G, e, \cdot, x \mapsto x^{-1})$, sind aber verschiedene Terme, gesehen als Ausdrücke in \mathcal{L} (allein schon, weil t_1 der Stufe 1 und t_2 der Stufe 0 ist).

Definition 2.10. *Atomare Formeln* in der Sprache \mathcal{L} sind entweder Ausdrücke der Form

$$(t_1 \doteq t_2),$$

für zwei \mathcal{L} -Terme t_1 und t_2 , oder Ausdrücke der Form

$$R(t_1, \dots, t_n),$$

wobei n aus \mathbb{N} kommt, die Elemente t_1, \dots, t_n Terme aus \mathcal{L} sind und R ein n -stelliges Relationszeichen ist.

Die Kollektion von *Formeln* in der Sprache \mathcal{L} ist die kleinste Menge **FORM** von Ausdrücken, welche alle atomare Formel enthält, und so, dass

- wenn φ in FORM liegt, so liegt $\neg\varphi$ in FORM;
- wenn φ und ψ in FORM liegen, so liegt $(\varphi \vee \psi)$ in FORM;
- wenn φ in FORM liegt und x eine Variable ist, so liegt $\exists x\varphi$ in FORM.

Ebenso wie Terme, können wir nun Formeln einstufen, indem wir sagen, dass atomare Formeln der Stufe 0 sind und wenn wir eine der drei obigen Konstruktionen auf Formeln φ und ψ der Stufe höchstens k anwenden, die neue Formel der Stufe höchstens $k + 1$ ist. Insbesondere lässt sich jede Formel eindeutig schreiben, entweder als

- $(t_1 \doteq t_2)$, für eindeutige Terme t_1 und t_2 ; oder
- $R(t_1, \dots, t_n)$, für eindeutige Terme t_1, \dots, t_n , oder
- $\neg\varphi$, für eine eindeutige Formel φ ; oder
- $(\varphi \vee \psi)$, für eindeutige Formeln φ und ψ ; oder
- $\exists x\varphi$, für eine eindeutige Formel φ und eine eindeutige Variable x .

Bemerkung 2.11. Wie in der Notation 1.1, werden wir folgende Abkürzungen verwenden, wobei wir die Eindeutigkeit der Darstellung von Formeln dementsprechend verlieren:

- $(\varphi \wedge \psi) = \neg(\neg\varphi \vee \neg\psi)$.
- $(\varphi \rightarrow \psi) = (\neg\varphi \vee \psi)$.
- $(\varphi \leftrightarrow \psi) = ((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$.
- $\forall x\varphi = \neg\exists x\neg\varphi$.

Ähnlich wie bei Termen schreiben wir für Formeln $\varphi = \varphi[x_1, \dots, x_n]$, falls die Variablen, welche in φ frei vorkommen, in der Menge $\{x_1, \dots, x_n\}$ liegen. Eine Variable x kommt frei in φ vor, falls x nicht im Wirkungsbereich eines Quantors $\exists x$ liegt. Genauer definieren wir induktiv über den Aufbau von Formeln, dass x in φ frei vorkommt, falls

- φ atomar ist;
- $\varphi = \neg\psi$ und x frei in ψ vorkommt;
- $\varphi = (\psi_1 \vee \psi_2)$ und x frei in ψ_1 oder ψ_2 vorkommt;
- $\varphi = \exists y\psi$ und x frei in ψ vorkommt aber verschieden von y ist.

Das Vorkommen einer Variable x , welche in φ nicht frei vorkommt, ist *gebunden*.

ACHTUNG: Die Schreibweise $\varphi[x_1, \dots, x_n]$ bedeutet nicht, dass jede Variable x_i , für $1 \leq i \leq n$, unbedingt in φ vorkommt!!

Definition 2.12. Sei $\varphi = \varphi[x_1, \dots, x_n]$ eine \mathcal{L} -Formel und a_1, \dots, a_n Elemente aus der Grundmenge einer \mathcal{L} -Struktur \mathcal{A} . Wir sagen, dass *das Tupel* (a_1, \dots, a_n) *die Formel* φ *in* \mathcal{A} *erfüllt*, oder dass φ *von* a_1, \dots, a_n *in* \mathcal{A} *gilt*, wir schreiben $\mathcal{A} \models \varphi[a_1, \dots, a_n]$, falls entweder

- $\varphi = (t_1 \doteq t_2)$ und $t_1^A[a_1, \dots, a_n] = t_2^A[a_1, \dots, a_n]$; oder
- $\varphi = R(t_1, \dots, t_m)$ und $(t_1^A[a_1, \dots, a_n], \dots, t_m^A[a_1, \dots, a_n])$ in R^A liegt; oder
- $\varphi = \neg\psi$ und $\mathcal{A} \not\models \psi[a_1, \dots, a_n]$; oder
- $\varphi = (\psi_1 \vee \psi_2)$ und $\mathcal{A} \models \psi_1[a_1, \dots, a_n]$ oder $\mathcal{A} \models \psi_2[a_1, \dots, a_n]$; oder
- $\varphi = \exists y\psi$, wobei $\psi = \psi[x_1, \dots, x_n, y]$ und es ein Element a aus A derart gibt, dass $\mathcal{A} \models \psi[a_1, \dots, a_n, a]$.

Bemerkung 2.13. Es folgt aus der Definition, dass $\mathcal{A} \not\models \varphi[a_1, \dots, a_n]$ genau dann, wenn $\mathcal{A} \models \neg\varphi[a_1, \dots, a_n]$.

Die obige Definition ist kompatibel mit unserer Intuition bezüglich der eingeführten Abkürzungen 2.11. Zum Beispiel:

$$\mathcal{A} \models (\varphi \rightarrow \psi)[a_1, \dots, a_n]$$

ist äquivalent zu

$$\mathcal{A} \models \varphi[a_1, \dots, a_n] \implies \mathcal{A} \models \psi[a_1, \dots, a_n],$$

Definition 2.14. Sei \mathcal{A} eine \mathcal{L} -Struktur. Eine Teilmenge $X \subset A^n$ ist *definierbar mit Parametern aus der Teilmenge $B \subset A$* , falls es Elemente (oder *Parameter*) b_1, \dots, b_m aus B und eine \mathcal{L} -Formel $\varphi[x_1, \dots, x_n, y_1, \dots, y_m]$ so gibt, dass

$$X = \varphi[\mathcal{A}] = \{(a_1, \dots, a_n) \in A^n \mid \mathcal{A} \models \varphi[a_1, \dots, a_n, b_1, \dots, b_m]\}.$$

Wenn wir X ohne Zusatzparameter definieren können, ist X *0-definierbar*. Die Kollektion aller definierbaren Teilmengen von \mathcal{A} (für n beliebig) ist unter Booleschen Kombinationen und Projektionen abgeschlossen.

Eine Funktion $f : A^n \rightarrow A$ ist *definierbar* in der Struktur \mathcal{A} , falls ihr Graph

$$\text{Graph}(f) = \{(a_1, \dots, a_n, b) \in A^{n+1} \mid b = f(a_1, \dots, a_n)\}$$

eine definierbare Menge ist.

Definition 2.15. Eine *Aussage* ist eine Formel χ ohne freie Variablen. Dennoch ist die Schreibweise $\chi = \chi[x]$ sinnvoll, siehe Bemerkung 2.11. Somit sagen wir, dass die \mathcal{L} -Aussage χ in der \mathcal{L} -Struktur \mathcal{A} *gilt* oder dass \mathcal{A} die Aussage χ *erfüllt*, wir schreiben $\mathcal{A} \models \chi$, falls $\mathcal{A} \models \chi[a]$, für ein (bzw. jedes) Element a aus A .

Definition 2.16. Zwei \mathcal{L} -Strukturen \mathcal{A} und \mathcal{B} sind *elementar äquivalent*, wir schreiben $\mathcal{A} \equiv \mathcal{B}$, falls sie dieselben Aussagen erfüllen. Dies bedeutet, dass für jede Aussage χ ,

$$\text{falls } \mathcal{A} \models \chi, \text{ dann } \mathcal{B} \models \chi.$$

Wir möchten den Zusammenhang und den Unterschied zwischen Isomorphismen und elementar Äquivalenz verstehen. Dafür brauchen wir den Begriff von *Back-&-Forth-Systeme*, manchmal auch *Ehrenfeucht-Fraïssé* Spielen genannt.

Definition 2.17. Seien \mathcal{A} und \mathcal{B} zwei \mathcal{L} -Strukturen. Ein *Back-&-Forth* System zwischen \mathcal{A} und \mathcal{B} ist eine Kollektion \mathcal{S} von \mathcal{L} -Isomorphismen $F : \text{Dom}(F) \rightarrow \text{Im}(F)$ zwischen endlich erzeugten \mathcal{L} -Unterstrukturen $\text{Dom}(F)$ von \mathcal{A} und $\text{Im}(F)$ von \mathcal{B} derart, dass folgende Bedingungen gelten:

Back Für jedes F aus \mathcal{S} und jedes b aus \mathcal{B} existiert eine Fortsetzung G von F in \mathcal{S} derart, dass b im Bildbereich $\text{Im}(G)$ von G liegt.

Forth Für jedes F aus \mathcal{S} und jedes a aus \mathcal{A} existiert eine Fortsetzung H von F in \mathcal{S} derart, dass a im Definitionsbereich $\text{Dom}(H)$ von H liegt.

Bemerkung 2.18. Die triviale Menge $\mathcal{S} = \emptyset$ ist ein Back-&-Forth System zwischen je zwei \mathcal{L} -Strukturen \mathcal{A} und \mathcal{B} .

Jeder Isomorphismus zwischen den \mathcal{L} -Strukturen \mathcal{A} und \mathcal{B} induziert ein nicht-leeres Back-&-Forth System zwischen \mathcal{A} und \mathcal{B} .

Induktiv über den Aufbau von $\varphi[x_1, \dots, x_n]$ beweist man, dass für ein Element F aus einem Back-&-Forth System \mathcal{S} und Elemente a_1, \dots, a_n aus $\text{Dom}(F)$

$$\mathcal{A} \models \varphi[a_1, \dots, a_n] \text{ genau dann gilt, wenn } \mathcal{B} \models \varphi[F(a_1), \dots, F(a_n)].$$

Insbesondere erfüllen \mathcal{A} und \mathcal{B} dieselbe Aussagen falls $\mathcal{S} \neq \emptyset$.

Definition 2.19. Für zwei \mathcal{L} -Strukturen \mathcal{A} und \mathcal{B} und Teilmengen $\emptyset \neq C \subset A$ und $D \subset B$ ist eine partielle Abbildung $F : C \rightarrow D$ *elementar*, falls

$$\mathcal{A} \models \varphi[c_1, \dots, c_n] \text{ genau dann gilt, wenn } \mathcal{B} \models \varphi[F(c_1), \dots, F(c_n)],$$

für alle Elemente c_1, \dots, c_n aus C und jede Formel $\varphi[x_1, \dots, x_n]$.

Die Struktur \mathcal{A} ist eine *elementare Unterstruktur* der Struktur \mathcal{B} , falls $A \subset B$ und die mengentheoretische Inklusion $\text{Id}_A : A \rightarrow B$ elementar ist. Wir schreiben $\mathcal{A} \preceq \mathcal{B}$. Des Weiteren ist \mathcal{B} eine *elementare Erweiterung* der Struktur \mathcal{A} , falls \mathcal{A} sich in \mathcal{B} einbetten lässt.

Bemerkung 2.20. Nach der Bemerkung 2.18 ist jede Abbildung F aus einem Back-&-Forth System \mathcal{S} eine elementare partielle Abbildung von $\text{Dom}(F)$ nach $\text{Im}(F)$ ist. Insbesondere ist jeder Isomorphismus von \mathcal{A} und \mathcal{B} eine elementare Abbildung.

Wenn eine partielle elementare Abbildung von \mathcal{A} nach \mathcal{B} existiert, dann sind \mathcal{A} und \mathcal{B} elementar äquivalent.

Korollar 2.21. Falls ein nicht-leeres Back-&-Forth System \mathcal{S} zwischen den \mathcal{L} -Strukturen \mathcal{A} und \mathcal{B} existiert, sind \mathcal{A} und \mathcal{B} elementar äquivalent. Insbesondere sind isomorphe Strukturen elementar äquivalent.

Die Umkehrung der obigen Bemerkung gilt nicht, wie wir im nächsten Beispiele sehen werden.

Beispiel 2.22. In der Sprache $\mathcal{L} = \{<\}$, wobei $<$ ein zweistelliges Relationszeichen ist, sind die Strukturen $(\mathbb{Q}, <)$ und $(\mathbb{R}, <)$ nicht isomorph (aus Mächtigkeitsgründen) aber elementar äquivalent, weil die Kollektion aller \mathcal{L} -Isomorphismen zwischen endlichen Teilmengen von \mathbb{Q} und \mathbb{R} ein Back-&-Forth System bildet.

2.2 Theorien und Beweise

In diesem Abschnitt fixieren wir eine Sprache \mathcal{L} .

Definition 2.23. Eine \mathcal{L} -Theorie T ist eine Kollektion von Aussagen.

Die \mathcal{L} -Struktur \mathcal{A} ist ein *Modell* von T , falls $\mathcal{A} \models \chi$ für jede Aussage χ aus T . Dies bezeichnen wir mit $\mathcal{A} \models T$.

Die Aussage θ *folgt* aus der Theorie T , bezeichnet mit $T \models \theta$, falls θ in jedem Modell $\mathcal{A} \models T$ gilt.

Wenn eine Theorie Modelle besitzt, heißt sie *konsistent*, ansonsten *inkonsistent*.

Bemerkung 2.24. Jede \mathcal{L} -Struktur ist ein Modell der leeren Theorie, welche keine Aussage enthält.

Jede Aussage ist eine Folgerung einer inkonsistenten Theorie. Falls je zwei Modelle einer konsistenten Theorie T elementar äquivalent sind, gilt für jede Aussage χ entweder $T \models \chi$ oder $T \models \neg\chi$. Beachte, dass diese beiden Fälle nicht gleichzeitig vorkommen können.

Definition 2.25. Eine Klasse \mathcal{C} von \mathcal{L} -Strukturen ist *axiomatisierbar*, falls es eine Theorie gibt, deren Modelle genau die Strukturen aus der Klasse \mathcal{C} sind.

Aufgabe. Ist die Klasse aller Gruppen in der Sprache \mathcal{L}_{Gp} axiomatisierbar? Wenn ja, folgt die Aussage

$$\forall x \forall y (x \cdot y \doteq y \cdot x)$$

(oder die Negation davon) aus der Axiomatisierung?

Bemerkung 2.26. Sei \mathcal{A} eine \mathcal{L} -Struktur mit Grundmenge A . Mit \mathcal{L}_A bezeichnen wir die Sprache $\mathcal{L} \cup \{d_a\}_{a \in A}$, wobei $\{d_a\}_{a \in A}$ eine Menge neuer paarweise verschiedener Konstantenzeichen ist. Beachte, dass \mathcal{A} in natürlicher Weise als \mathcal{L}_A -Struktur gesehen werden kann: Es genügt das Konstantenzeichen d_a als das Element a zu interpretieren.

Sei das *atomare Diagramm* $\text{Diag}^{at}(\mathcal{A})$ von \mathcal{A} die Menge aller quantorenfreien \mathcal{L}_A -Aussagen, welche in \mathcal{A} gelten. Es folgt, dass eine \mathcal{L}_A -Struktur \mathcal{B} genau dann ein Modell von $\text{Diag}^{at}(\mathcal{A})$ ist, wenn die Abbildung

$$\begin{aligned} F : A &\rightarrow B \\ a &\mapsto d_a^{\mathcal{B}} \end{aligned}$$

eine Einbettung bezüglich der Einschränkung zur Sprache \mathcal{L} liefert.

Des Weiteren sei nun das *vollständige Diagramm* $\text{Diag}(\mathcal{A})$ von \mathcal{A} die Menge aller \mathcal{L}_A -Aussagen, welche in \mathcal{A} gelten. Es ist auch leicht zu zeigen, dass eine \mathcal{L}_A -Struktur \mathcal{B} genau dann ein Modell von $\text{Diag}(\mathcal{A})$ ist, wenn die vorige Abbildung $F : A \rightarrow B$ gegeben durch $a \mapsto d_a^{\mathcal{B}}$ elementar bezüglich der Einschränkung zur Sprache \mathcal{L} ist. Insbesondere sind je zwei Modelle von $\text{Diag}(\mathcal{A})$ elementar äquivalent, gesehen als \mathcal{L} -Strukturen.

Induktiv über den Aufbau einer quantorenfreien Formel können wir folgende Bemerkung zeigen:

Bemerkung 2.27. Sei T eine \mathcal{L} -Theorie mit der Eigenschaft, dass es für jede \mathcal{L} -Formel $\varphi[x_1, \dots, x_n]$ eine quantorenfreie \mathcal{L} -Formel $\psi[x_1, \dots, x_n]$ so gibt, dass

$$T \models \forall x_1 \dots \forall x_n (\varphi[x_1, \dots, x_n] \leftrightarrow \psi[x_1, \dots, x_n]).$$

Dann gilt für alle Modelle \mathcal{A} und \mathcal{B} von T , dass $\mathcal{A} \preceq \mathcal{B}$ (siehe Definition 2.19) aus $\mathcal{A} \subset \mathcal{B}$ folgt.

Definition 2.28. Eine \mathcal{L} -Aussage χ ist *allgemeingültig*, falls sie aus der leeren Theorie folgt. Das heißt, dass sie in jeder \mathcal{L} -Struktur \mathcal{A} gilt. Dies bezeichnen wir mit $\models \chi$.

Eine \mathcal{L} -Formel $\varphi[x_1, \dots, x_n]$ ist *allgemeingültig*, falls die Aussage *forall* $x_1 \dots \forall x_n \varphi$ allgemeingültig ist.

Bemerkung 2.29. Sei $P = P(A_1, \dots, A_m)$ eine aussagenlogische Tautologie mit Variablen A_1, \dots, A_m . Gegeben \mathcal{L} -Formeln $\varphi_1[x_1, \dots, x_n], \dots, \varphi_m[x_1, \dots, x_n]$, betrachte die \mathcal{L} -Formel ψ mit freien Variablen x_1, \dots, x_n , welche wir aus $P(A_1, \dots, A_m)$ gewinnen, indem wir jede aussagenlogische Variable A_i durch $\varphi_i[x_1, \dots, x_n]$ ersetzen. Die \mathcal{L} -Formel $\psi[x_1, \dots, x_n]$ ist allgemeingültig.

Wir bezeichnen solche entstandene Formeln wieder als *Tautologien* (trotz der möglichen Verwirrung).

Beweis. Sei \mathcal{B} eine beliebige \mathcal{L} -Struktur und b_1, \dots, b_n Elemente aus B . Definiere folgende Belegung der aussagenlogischen Variablen:

$$\begin{aligned} \beta: \{A_1, \dots, A_m\} &\rightarrow \{0, 1\} \\ A_i &\mapsto \begin{cases} 1, & \text{falls } \mathcal{B} \models \varphi_i[b_1, \dots, b_n] \\ 0, & \text{sonst} \end{cases} \end{aligned}$$

Induktiv über den Aufbau von P sieht man leicht, dass $\beta(P(A_1, \dots, A_m)) = 1$ genau dann, wenn $\mathcal{B} \models \psi[b_1, \dots, b_n]$. Weil $P(A_1, \dots, A_m)$ eine Tautologie ist, folgt somit, dass $\psi[x_1, \dots, x_n]$ allgemeingültig ist. \square

Definition 2.30. Die *Gleichheitsaxiome* sind die folgende Liste von Aussagen:

1. $\forall x(x \doteq x)$
2. $\forall x \forall y((x \doteq y) \rightarrow (y \doteq x))$.
3. $\forall x \forall y \forall z(((x \doteq y) \wedge (y \doteq z)) \rightarrow (x \doteq z))$.
4. $\forall x_1 \dots \forall x_n \forall y_1 \dots \forall y_n \left(\left(\bigwedge_{1 \leq i \leq n} (x_i \doteq y_i) \right) \rightarrow (f(x_1, \dots, x_n) \doteq f(y_1, \dots, y_n)) \right)$ für jedes n -stellige Funktionszeichen f aus \mathcal{L} .
5. $\forall x_1 \dots \forall x_m \forall y_1 \dots \forall y_m \left(\left(\bigwedge_{1 \leq i \leq m} (x_i \doteq y_i) \right) \rightarrow (R(x_1, \dots, x_m) \leftrightarrow R(y_1, \dots, y_m)) \right)$ für jedes m -stellige Relationszeichen R aus \mathcal{L} .

Bemerkung 2.31. Beachte, dass die obige Liste von Axiomen unendlich sein kann, falls die Sprache \mathcal{L} unendlich viele Funktions- oder Relationszeichen enthält.

Jedes Gleichheitsaxiom ist allgemeingültig.

Beweis. Gleichheit ist in der Tat eine Äquivalenzrelation (dies besagen die Axiome (1) – (3)). Ferner ist das Bild von Tupeln, die gleich sind, auch gleich (und dementsprechend für Relationen). \square

Um den Begriff eines formellen Beweises einzuführen, brauchen wir einige Hilfslemmata.

Definition 2.32. Seien t und s Terme aus \mathcal{L} und x eine Variable. Die *Ersetzung* von x durch s in t ist ein neuer Term $t_{s/x}$, der aus t gewonnen wird, indem wir jedes Vorkommen der Variable x durch s ersetzen.

Bemerkung 2.33. Beachte: Falls x in s nicht als Variable vorkommt, dann kommt x nicht mehr in $t_{s/x}$ vor. Allerdings werden die Variablen aus s nun in $t_{s/x}$ vorkommen.

Definition 2.34. Gegeben eine Formel φ , eine Variable x und einen Term s , definieren wir die *Ersetzung* $\varphi_{s/x}$ von x durch s in φ , indem wir alle freien Vorkommen der Variable x in φ durch s ersetzen. Genauer definieren wir rekursiv:

- Falls $\varphi = (t_1 \doteq t_2)$, ist $\varphi_{s/x} = (t_{1s/x} \doteq t_{2s/x})$.
- Falls $\varphi = R(t_1, \dots, t_k)$, ist $\varphi_{s/x} = R(t_{1s/x} \dots, t_{ks/x})$.
- Falls $\varphi = \neg\psi$, ist $\varphi_{s/x} = \neg\psi_{s/x}$.
- Falls $\varphi = (\varphi_1 \vee \varphi_2)$, ist $\varphi_{s/x} = (\varphi_{1s/x} \vee \varphi_{2s/x})$.
- Falls $\varphi = \exists y\psi$, ist $\varphi_{s/x} = \begin{cases} \exists y\psi, & \text{für } y = x \\ \exists y\psi_{s/x}, & \text{für } y \neq x \end{cases}$.

Die Variable x ist *frei* für s in φ , falls keine der Variablen von s in $\varphi_{s/x}$ gebunden wird. Dies bedeutet, dass entweder x nicht frei in φ vorkommt (und somit ist $\varphi_{s/x} = \varphi$), oder

- φ ist quantorenfrei; oder
- $\varphi = \neg\psi$ und x kommt frei für s in ψ vor; oder
- $\varphi = (\varphi_1 \vee \varphi_2)$ und x kommt frei für s sowohl in φ_1 als auch in φ_2 vor; oder
- $\varphi = \exists y\psi$ und $x \neq y$ kommt frei für s in ψ , aber y kommt nicht in s vor.

Beispiel 2.35. Nach dem Ersetzen kann die Erfüllbarkeit einer Formel in einer Struktur höchst verschieden sein. Zum Beispiel, falls $s = y$, kommt x nicht frei für s in $\varphi = \forall y(y \doteq x)$ vor, denn y wird nach dem Ersetzen gebunden. In der Tat ist $\varphi_{s/x} = \forall y(y \doteq y)$ eine allgemeingültige Aussage. Jedoch erfüllt das Element a der Struktur \mathcal{A} die Formel φ genau dann, wenn die Grundmenge A die Einermenge $\{a\}$ ist.

Falls die Variable x frei für s in φ vorkommt, haben wir eine Äquivalenz:

Lemma 2.36 (Substitutionslemma). *Wenn die Variable x frei für $s = s[x_1, \dots, x_n]$ in der Formel $\varphi[x, x_1, \dots, x_n]$ ist, gilt für beliebige Elemente a_1, \dots, a_n in einer Struktur \mathcal{A} ,*

$$\mathcal{A} \models \varphi[s^{\mathcal{A}}[a_1, \dots, a_n], a_1, \dots, a_n] \iff \varphi_{s/x}[a_1, \dots, a_n].$$

Beweis. Mit der obigen Notation zeigen wir zuerst induktiv über den Aufbau eines Termes $t[x, x_1, \dots, x_n]$, dass

$$t_{s/x}^{\mathcal{A}}[a_1, \dots, a_n] = t^{\mathcal{A}}[s^{\mathcal{A}}[a_1, \dots, a_n], a_1, \dots, a_n].$$

Falls t ein Konstantenzeichen ist, ist es trivial. Wenn t eine Variable ist, müssen wir unterscheiden, ob $t = x$ oder $t \neq x$. Und für beliebige Terme folgt es aus der Induktionsannahme.

Nun zeigen wir induktiv über den Aufbau der Formel φ , dass

$$\mathcal{A} \models \varphi[s[a_1, \dots, a_n], a_1, \dots, a_n] \iff \varphi_{s/x}[a_1, \dots, a_n].$$

Für quantorenfreie Formeln folgt es aus dem ersten Teil des Beweises. Daher müssen wir nur den Fall $\varphi = \exists y\psi$ betrachten. Falls x nicht frei in φ vorkommt, so ist $\varphi_{s/x} = \varphi$ und die Äquivalenz folgt klarerweise.

Ansonsten ist $y \neq x$ und wir schreiben $\psi = \psi[x, y, x_1, \dots, x_n]$. Weil x frei für s in φ ist, kommt die Variable y nicht in s vor. Insbesondere ist $s^{\mathcal{A}}[a_1, \dots, a_n] = \tilde{s}^{\mathcal{A}}[a, a_1, \dots, a_n]$ für jedes Element a aus A , wenn wir s als Term \tilde{s} in den Variablen $\{y, x_1, \dots, x_n\}$ schreiben. Ferner ist $\varphi_{s/x} = \exists y\psi_{s/x}[y, x_1, \dots, x_n]$. Nun gilt:

$$\mathcal{A} \models \varphi[s^{\mathcal{A}}[a_1, \dots, a_n], a_1, \dots, a_n] \iff \text{Es gibt ein Element } a \text{ aus } A \text{ mit}$$

$$\mathcal{A} \models \psi[s^{\mathcal{A}}[a_1, \dots, a_n], a, a_1, \dots, a_n] \iff$$

$$\text{Es gibt } a \text{ aus } A \text{ mit } \mathcal{A} \models \psi[\tilde{s}^{\mathcal{A}}[a, a_1, \dots, a_n], a, a_1, \dots, a_n] \stackrel{I.A.}{\iff} \text{Es gibt } a \text{ aus } A \text{ mit}$$

$$\mathcal{A} \models \psi_{\tilde{s}/x}[a, a_1, \dots, a_n] \iff \mathcal{A} \models \varphi_{\tilde{s}/x}[a_1, \dots, a_n] \iff \mathcal{A} \models \varphi_{s/x}[a_1, \dots, a_n]$$

□

Korollar 2.37 (\exists -Quantorenaxiom). *Wenn x frei für $s = s[x_1, \dots, x_n]$ in $\varphi[x, x_1, \dots, x_n]$ ist, dann ist die Formel*

$$(\varphi_{s/x} \rightarrow \exists x\varphi)$$

allgemeingültig.

Insbesondere gilt $\models (\psi(x) \rightarrow \exists x\psi(x))$.

Beweis. Wir müssen zeigen, dass jede Struktur \mathcal{A} die Aussage $\forall x_1 \dots \forall x_n (\varphi_{s/x} \rightarrow \exists x\varphi)$ erfüllt. Gegeben a_1, \dots, a_n aus A so, dass $\mathcal{A} \models \varphi_{s/x}[a_1, \dots, a_n]$ gilt, dann folgt aus dem Lemma 2.36

$$\mathcal{A} \models \varphi[s[a_1, \dots, a_n], a_1, \dots, a_n].$$

Insbesondere bezeugt das Element $s[a_1, \dots, a_n]$ aus A , dass $\mathcal{A} \models \exists x\varphi[x, a_1, \dots, a_n]$, wie gewünscht. Für die letzte Behauptung des Korollars genügt es den Fall $s = x$ zu betrachten. □

Definition 2.38. Eine \mathcal{L} -Formel φ ist in *pränexer Normalform*, wenn

$$\varphi = Q_1 y_1 \dots Q_m y_m \psi,$$

wobei jedes Q_i eines der Quantoren \forall oder \exists ist und ψ eine quantorenfreie Formel ist.

Lemma 2.39. *Für jede Formel $\varphi[x_1, \dots, x_n]$ gibt es eine Formel $\theta[x_1, \dots, x_n]$ in pränexer Normalform derart, dass $(\varphi \leftrightarrow \theta)$ allgemeingültig ist.*

Wir sagen, dass φ und θ logisch äquivalent sind.

Beweis. Es genügt alle Quantoren in φ nach folgenden Regeln nach vorne zu ziehen:

- $\neg\exists \sim \forall\neg$
- $\neg\forall \sim \exists\neg$
- $(\psi_1 \wedge \exists x\psi_2) \sim \exists y(\psi_1 \wedge \psi_{2y/x})$, wobei y nicht in ψ_1 und auch nicht in ψ_2 vorkommt.
- $(\psi_1 \vee \exists x\psi_2) \sim \exists y(\psi_1 \vee \psi_{2y/x})$, wobei y nicht in ψ_1 und auch nicht in ψ_2 vorkommt.
- $(\psi_1 \wedge \forall x\psi_2) \sim \forall y(\psi_1 \wedge \psi_{2y/x})$, wobei y nicht in ψ_1 und auch nicht in ψ_2 vorkommt.
- $(\psi_1 \vee \forall x\psi_2) \sim \forall y(\psi_1 \vee \psi_{2y/x})$, wobei y nicht in ψ_1 und auch nicht in ψ_2 vorkommt.

Jede Reihenfolge dieses Verfahrens liefert möglicherweise eine andere Formel in pränexer Normalform, aber sie sind alle logisch äquivalent zueinander. \square

Der Beweis des folgenden Lemmas ist offensichtlich.

Lemma 2.40 (Modus Ponens). *Falls $\models \varphi$ und $\models (\varphi \rightarrow \psi)$, dann ist ψ auch allgemeingültig.*

Lemma 2.41 (\exists -Einführung). *Falls die Variable x nicht frei in ψ vorkommt und $\models (\varphi \rightarrow \psi)$, dann ist $(\exists x\varphi \rightarrow \psi)$ allgemeingültig.*

Beweis. Schreibe $\varphi = \varphi[x, x_1, \dots, x_n]$ und $\psi = \psi[x, x_1, \dots, x_n] = \psi[x_1, \dots, x_n]$ (weil x nicht frei in ψ vorkommt). Gegeben Elemente a_1, \dots, a_n aus der Grundmenge A einer beliebigen Struktur \mathcal{A} , wollen wir zeigen, dass

$$\mathcal{A} \models (\exists x\varphi \rightarrow \psi)[a_1, \dots, a_n].$$

Angenommen, dass $\mathcal{A} \models \exists x\varphi[x, a_1, \dots, a_n]$, wähle a aus A mit $\mathcal{A} \models \varphi[a, a_1, \dots, a_n]$. Es folgt $\mathcal{A} \models \psi[a, a_1, \dots, a_n]$, weil die Formel $(\varphi \rightarrow \psi)$ allgemeingültig ist. Weil x nicht frei in ψ vorkommt, bedeutet dies, dass $\mathcal{A} \models \psi[a_1, \dots, a_n]$, wie gewünscht. \square

Definition 2.42. Die Formel φ ist aus der Theorie T *beweisbar*, wir schreiben $T \vdash \varphi$, falls ein n aus \mathbb{N} und eine endliche Folge $(\varphi_1, \dots, \varphi_n)$, mit $\varphi_n = \varphi$, derart existieren, dass für jedes $i \leq n$

- die Formel φ_i ein *logisches Axiom* ist, das heißt, entweder eine Tautologie (siehe 2.29) oder ein Gleichheitsaxiom oder eine Instanz $(\psi_{s/x}(x) \rightarrow \exists x\psi(x))$ des \exists -Quantorenaxiomes ist; oder
- die Formel φ_i zu T gehört; oder
- die Formel $\varphi_i = (\exists x\psi_1 \rightarrow \psi_2)$ aus einer vorherigen Formel $\varphi_j = (\psi_1 \rightarrow \psi_2)$ durch \exists -Einführung entsteht (insbesondere kommt x nicht frei in ψ_2 vor); oder
- die Formel φ_i aus zwei vorherigen Formeln φ_j und $\varphi_k = (\varphi_j \rightarrow \varphi_i)$ durch Modus Ponens entsteht.

Die obige Folge $(\varphi_1, \dots, \varphi_n)$ ist ein *Beweis* in T der Formel φ .

Bemerkung 2.43. Falls $(\varphi_1, \dots, \varphi_n)$ ein Beweis in T von φ ist, so ist $(\varphi_1, \dots, \varphi_{n+2})$ ein Beweis von φ , wobei φ_{n+1} die Tautologie $(\varphi_n \rightarrow \varphi_n)$ ist und $\varphi_{n+2} = \varphi_n = \varphi$ mit Anwendung von Modus Ponens entsteht. Insbesondere kann eine Formel mehrere Beweise in T haben.

Falls die Formel φ aus der Theorie $T \cup \{\psi_1, \dots, \psi_n\}$ beweisbar ist, wobei jede Aussage ψ_i auch aus T beweisbar ist, dann ist φ aus T beweisbar: Es genügt die Beweise der ψ_i 's zusammen mit dem Beweis von φ aus $T \cup \{\psi_1, \dots, \psi_n\}$ zu konkatenieren, um einen Beweis von φ aus T zu gewinnen.

Definition 2.44. Eine Formel φ ist *beweisbar*, falls sie aus der leeren Theorie beweisbar ist. Dies bezeichnen wir mit $\vdash \varphi$. Das *Hilbertkalkül* ist die Kollektion aller beweisbaren Formeln (bezüglich der leeren Theorie).

Lemma 2.45.

\forall -Quantorenaxiom Falls x frei für s in φ ist, dann gilt $\vdash (\forall x\varphi \rightarrow \varphi_{s/x})$. Insbesondere ist $(\forall x\varphi \rightarrow \varphi[x])$ beweisbar.

\forall -Einführung Falls x nicht frei in φ vorkommt und $\vdash (\varphi \rightarrow \psi)$, so gilt $\vdash (\varphi \rightarrow \forall x\psi)$. Insbesondere ist $\forall x\psi$ beweisbar, wenn ψ beweisbar ist.

Beweis. Für das \forall -Quantorenaxiom, beachte, dass x auch frei für s in $\neg\varphi$ ist. Insbesondere ist $(\neg\varphi_{s/x} \rightarrow \exists x\neg\varphi)$ eine Instanz des \exists -Quantorenaxiom und daher beweisbar. Die aussagenlogische Tautologie

$$\left((\neg p \rightarrow q) \rightarrow (\neg q \rightarrow p) \right)$$

zusammen mit $\varphi_{s/x}$ als p und $\exists x\neg\varphi$ als q und Modus Ponens liefert, dass

$$\vdash (\neg\exists x\neg\varphi \rightarrow \varphi_{s/x}),$$

das heißt,

$$\vdash (\forall x\varphi \rightarrow \varphi_{s/x}),$$

wie gewünscht.

Wende nun das \forall -Quantorenaxiom mit $s = x$ an und erhalte, dass $(\forall x\varphi \rightarrow \varphi[x])$ beweisbar ist.

Für die \forall -Einführung ist es ähnlich wie oben, weil x nicht frei in $\neg\varphi$ vorkommt, wenn x nicht frei in φ vorkommt. Aus der Tautologie

$$\left((\varphi \rightarrow \psi) \rightarrow (\neg\psi \rightarrow \neg\varphi) \right)$$

und Modus Ponens folgt, dass $(\neg\psi \rightarrow \neg\varphi)$ beweisbar ist und somit auch $(\exists x\neg\psi \rightarrow \neg\varphi)$. Mit Hilfe der entsprechenden Tautologie, Modus Ponens und der Bemerkung 2.43 ist die Formel $(\varphi \rightarrow \forall x\psi)$ beweisbar, wie gewünscht.

Die Formel $\varphi = \forall z(z \doteq z)$ ist ein Gleichheitsaxiom und somit beweisbar. Die aussagenlogische Tautologie

$$\left(p \rightarrow \left(q \rightarrow (p \rightarrow q) \right) \right)$$

und zweimaliges Anwenden von Modus Ponens (mit φ als p und ψ als q) liefern, dass $\vdash (\varphi \rightarrow \psi)$, falls ψ beweisbar ist. Nun kommt x nicht frei in φ vor, so $(\varphi \rightarrow \forall x\psi)$ ist insbesondere mit Anwendung der \exists -Einführung beweisbar. Aus Modus Ponens folgt, dass $\forall x\psi$ auch beweisbar ist. \square

Lemma 2.46. *Sei $\varphi[x_1, \dots, x_n]$ eine \mathcal{L} -Formel und C eine Menge von neuen Konstantenzeichen, welche nicht aus \mathcal{L} kommen. Für Symbole c_1, \dots, c_n aus C , ist die \mathcal{L} -Formel $\varphi[x_1, \dots, x_n]$ genau dann beweisbar, wenn die $\mathcal{L} \cup C$ -Aussage $\varphi[c_1, \dots, c_n]$ beweisbar ist.*

Beweis.

- (\implies) Falls $\vdash \varphi[x_1, \dots, x_n]$, so folgt aus der \forall -Einführung die Beweisbarkeit von der Formel $\forall x_1 \dots \forall x_n \varphi[x_1, \dots, x_n]$. Beachte, dass x_i frei für c_i in $\varphi[x_1, \dots, x_n]$ ist (in der Sprache $\mathcal{L} \cup C$), weil überhaupt keine Variablen im Term c_i vorkommen. Aus dem \forall -Quantorenaxiom folgt induktiv, dass $\varphi[c_1, \dots, c_n]$ beweisbar ist.
- (\impliedby) Sei $\varphi_1, \dots, \varphi_n$ ein Beweis in der Sprache $\mathcal{L} \cup C$. OBdA können wir annehmen, dass alle Konstantenzeichen aus C , welche im Beweis vorkommen, in der Menge $\{c_1, \dots, c_n\}$ enthalten sind. Wenn wir formell jedes Vorkommen von c_i durch eine neue Variable y_i ersetzen, welche im Beweis nicht vorkommen, gewinnen wir einen \mathcal{L} -Beweis von $\varphi[y_1, \dots, y_n]$. Wie oben folgt aus der \forall -Einführung, dass die \mathcal{L} -Aussage

$$(\varphi[y_1, \dots, y_n] \rightarrow \forall y_1 \dots \forall y_n \varphi[y_1, \dots, y_n])$$

beweisbar ist, und somit ist die \mathcal{L} -Aussage $\vdash \forall y_1 \dots \forall y_n \varphi[y_1, \dots, y_n]$ beweisbar. Weil y_i frei für x_i in $\varphi[y_1, \dots, y_n]$ ist, folgt aus dem \forall -Quantorenaxiom und iteriertem Modus Ponens induktiv, dass

$$(\forall y_1 \dots \forall y_n \varphi[y_1, \dots, y_n] \rightarrow \forall y_i \dots \forall y_n \varphi[x_1, \dots, x_{i-1}, y_i, \dots, y_n])$$

beweisbar ist. Insbesondere ist $\varphi[x_1, \dots, x_n]$ beweisbar. \square

Bemerkung 2.47. Eine Formel φ ist genau aus der Theorie T beweisbar, wenn es endlich viele Aussagen χ_1, \dots, χ_k aus T derart gibt, dass $\vdash \left(\bigwedge_{i=1}^k \chi_i \rightarrow \varphi \right)$, wobei die leere Konjunktion mit $k = 0$ die Formel $\forall x(x \doteq x)$ ist (z. B. wenn T die leere Theorie ist).

Beweis.

- (\implies) Wenn $T \vdash \varphi$, gibt es einen Beweis endlicher Länge von φ , welcher die Aussagen χ_1, \dots, χ_k aus T verwendet. Setze nun $\theta = \bigwedge_{i=1}^k \chi_i$. Beachte, dass die Formel

$$\left(\psi \rightarrow (\theta \rightarrow \psi) \right)$$

für jede Formel ψ eine Tautologie ist. Insbesondere folgt aus der Bemerkung 2.43 induktiv über die Länge des Beweises, dass die Formel $\left(\bigwedge_{i=1}^k \chi_i \rightarrow \varphi \right)$ beweisbar ist.

(\Leftarrow) Für $k = 0$, müssen wir nun Modus Ponens und das Gleichheitsaxiom $\forall x(x \doteq x)$ verwenden. Ansonsten folgt diese Richtung aus iteriertem Modus Ponens, denn die Formel

$$\left(\left(\bigwedge_{i=1}^k \chi_i \rightarrow \varphi \right) \rightarrow (\chi_1 \rightarrow (\chi_2 \rightarrow \dots (\chi_k \rightarrow \varphi) \dots)) \right)$$

ist eine Tautologie.

□

Korollar 2.48. *Seien φ eine Formel und ψ eine Aussage. Die Formel φ ist genau aus der Theorie $T \cup \{\psi\}$ beweisbar, wenn die Implikation $(\psi \rightarrow \varphi)$ aus T beweisbar ist. D. h.*

$$T \cup \{\psi\} \vdash \varphi \iff T \vdash (\psi \rightarrow \varphi).$$

Beweis.

(\Rightarrow) Wir unterscheiden zwei Fälle: Zuerst nehmen wir an, dass T bereits die Formel φ beweist. Aus der aussagenlogischen Tautologie

$$(p \rightarrow (q \rightarrow p))$$

folgt (mit $p = \varphi$ und $q = \psi$) mit Hilfe der Bemerkung 2.43, dass $T \vdash (\psi \rightarrow \varphi)$, wie gewünscht.

Im zweiten Fall gibt es keinen Beweis der Formel φ , welcher nur Aussagen aus T verwendet. Wegen der Bemerkung 2.47 gibt es Aussagen $\varphi_1, \dots, \varphi_r$ aus $T \cup \{\psi\}$ derart, dass die Formel $((\bigwedge_{i=1}^r \varphi_i) \rightarrow \varphi)$ beweisbar ist. Nach Umformung können wir annehmen, dass es Aussagen χ_1, \dots, χ_k aus T derart gibt, dass

$$\vdash \left(\left(\bigwedge_{i=1}^k \chi_i \wedge \psi \right) \rightarrow \varphi \right).$$

Nun liefert folgende Tautologie

$$\left(\left(\left(\bigwedge_{i=1}^k \chi_i \wedge \psi \right) \rightarrow \varphi \right) \rightarrow \left(\bigwedge_{i=1}^k \chi_i \rightarrow (\psi \rightarrow \varphi) \right) \right)$$

mit Modus Ponens einen Beweis von $(\psi \rightarrow \varphi)$ aus T , wieder mit der obigen Bemerkung 2.47.

(\Leftarrow) Falls es in T einen Beweis $\varphi_1, \dots, \varphi_n$ der Länge n von der Formel $\varphi_n = (\psi \rightarrow \varphi)$ gibt, dann bekommen wir mit Modus Ponens einen Beweis der Länge $n + 2$ von φ aus $T \cup \{\psi\}$, in dem wir $\varphi_{n+1} = \psi$ und $\varphi_{n+2} = \varphi$ setzen.

□

Korollar 2.49. *Wenn eine Formel beweisbar ist, dann ist sie allgemeingültig. Insbesondere, wenn $T \vdash \varphi$, dann folgt φ aus T , d. h. $T \models \varphi$.*

Beweis. Aus den Bemerkungen 2.31 und 2.29, den Lemmata 2.40 und 2.41 und aus dem Korollar 2.37 folgt, dass jede beweisbare Formel allgemeingültig ist.

Für die letzte Behauptung; falls φ aus T beweisbar ist, dann ist $\vdash (\bigwedge_{i=1}^k \chi_i \rightarrow \varphi)$ für endlich viele Aussagen χ_1, \dots, χ_k aus T . Jedes Modell \mathcal{A} von T erfüllt die Formeln χ_1, \dots, χ_k und somit auch φ . \square

Wir werden im nächsten Abschnitt sehen, dass die Rückrichtung auch gilt: der Vollständigkeitssatz. Insbesondere haben wir eine Äquivalenz zwischen zwei Begriffen: semantische *Wahrheit* und syntaktische Folgerung.

2.3 Vollständigkeit und Kompaktheit

In diesem Abschnitt fixieren wir eine Sprache \mathcal{L} .

Definition 2.50. Eine Theorie T ist *widerspruchsfrei*, falls keine Aussage χ derart existiert, dass $T \vdash \chi$ und $T \vdash \neg\chi$. Ansonsten ist T widersprüchlich.

Eine widerspruchsfreie Theorie ist *vollständig*, falls $T \vdash \chi$ oder $T \vdash \neg\chi$ für jede Aussage χ .

Bemerkung 2.51. Jede konsistente Theorie ist widerspruchsfrei: Wenn \mathcal{A} ein Modell von T ist, dann gilt, siehe Korollar 2.49, in \mathcal{A} jede Aussage, welche aus T beweisbar ist. Aber in einer Struktur kann nicht sowohl χ als auch $\neg\chi$ gelten.

Je zwei Modelle einer vollständigen Theorie sind elementar äquivalent: Falls \mathcal{A} und \mathcal{B} Modelle der vollständigen Theorie sind und χ eine beliebige Aussage ist, gilt

$$\mathcal{A} \models \chi \iff T \vdash \chi \iff \mathcal{B} \models \chi.$$

Bemerkung 2.52. Eine Theorie T ist genau dann widerspruchsfrei, wenn für keine endliche Kollektion von Formeln $\varphi_1, \dots, \varphi_k$ aus T gilt, dass $\vdash \neg(\bigwedge_{i=1}^k \varphi_i)$.

Insbesondere ist T genau dann widerspruchsfrei, wenn jede endliche Teilmenge von T widerspruchsfrei ist.

Beweis. Wenn die Formel $\neg(\bigwedge_{i=1}^k \varphi_i)$ beweisbar wäre, ist sie insbesondere auch aus T beweisbar. Mit Hilfe von iteriertem Modus Ponens und Benutzung der Tautologie

$$\left(\varphi_1 \rightarrow (\varphi_2 \rightarrow \dots \rightarrow (\varphi_k \rightarrow (\bigwedge_{i=1}^k \varphi_i) \dots)) \right).$$

sieht man, dass $(\bigwedge_{i=1}^k \varphi_i)$ aus T beweisbar ist. Somit ist T widersprüchlich.

Für die andere Richtung nehmen wir an, dass T widersprüchlich ist, das heißt wir nehmen an, dass T sowohl χ als auch $\neg\chi$ beweist. Wie in der Bemerkung 2.47 existieren Aussagen $\varphi_1, \dots, \varphi_i$ und $\varphi_{i+1}, \dots, \varphi_k$ aus T mit

$$\vdash \left(\left(\bigwedge_{j=1}^i \varphi_j \right) \rightarrow \chi \right) \text{ und } \vdash \left(\left(\bigwedge_{j=i+1}^k \varphi_j \right) \rightarrow \neg\chi \right).$$

Die aussagenlogische Tautologie

$$\left((p \rightarrow q) \rightarrow \left((r \rightarrow \neg q) \rightarrow \neg(p \wedge r) \right) \right)$$

liefert mit Modus Ponens, dass $\vdash \neg(\bigwedge_{i=1}^k \varphi_i)$, wie gewünscht. \square

Lemma 2.53. *Eine Theorie T ist genau dann widersprüchlich, wenn sich jede Aussage aus T beweisen lässt.*

Beweis. Eine Richtung ist trivial. Für die andere Richtung sei χ eine beliebige Aussage. Falls T widersprüchlich ist, gibt es eine Aussage θ mit $T \vdash \theta$ und $T \vdash \neg\theta$. Die Tautologie

$$\left(\theta \rightarrow (\neg\theta \rightarrow \chi)\right)$$

liefert mit Modus Ponens (zwei Mal) einen Beweis von χ aus T . \square

Korollar 2.54. *Sei T eine Theorie und χ eine Aussage. Die Theorie $T \cup \{\neg\chi\}$ ist genau dann widersprüchlich, wenn $T \vdash \chi$.*

Beweis.

(\implies) Falls $T \cup \{\neg\chi\}$ widersprüchlich ist, dann beweist sie wegen Lemma 2.53 jede Aussage. Insbesondere beweist $T \cup \{\neg\chi\}$ die Aussage χ . Wegen Korollar 2.48 ist $(\neg\chi \rightarrow \chi)$ aus T beweisbar. Die Tautologie

$$\left((\neg\chi \rightarrow \chi) \rightarrow \chi\right)$$

liefert nun mit Modus Ponens einen Beweis aus T von χ , wie gewünscht.

(\impliedby) Wenn $T \vdash \chi$, dann ist χ auch in jeder Obertheorie von T beweisbar, insbesondere in $T \cup \{\neg\chi\}$. Aber $T \cup \{\neg\chi\}$ beweist auch $\neg\chi$, trivialerweise. Daher ist $T \cup \{\neg\chi\}$ widersprüchlich. \square

Satz 2.55. *Die Behauptung*

$$T \models \varphi \iff T \vdash \varphi \text{ für jede Theorie } T \text{ und jede Aussage } \varphi$$

ist äquivalent zur Behauptung

Eine Theorie ist genau dann widerspruchsfrei, wenn sie konsistent ist.

Beweis.

(\implies) Wegen Bemerkung 2.51 müssen wir nur zeigen, dass die widerspruchsfreie Theorie T ein Modell besitzt. Sonst gilt trivialerweise $T \models \varphi$ für jede Aussage φ . Aber unsere Annahme bedeutet, dass $T \vdash \varphi$ für jede Aussage φ , das heißt T wäre widersprüchlich wegen Lemma 2.53.

(\impliedby) Wegen Korollar 2.49 genügt es zu zeigen, dass $T \vdash \varphi$, wenn $T \models \varphi$. Sonst ist die Theorie $T \cup \{\neg\varphi\}$ wegen Korollar 2.54 widerspruchsfrei und es gibt somit ein Modell \mathcal{A} von $T \cup \{\neg\varphi\}$. Insbesondere ist \mathcal{A} ein Modell von T mit $\mathcal{A} \models \neg\varphi$. Aber φ folgt aus T , was den gewünschten Widerspruch liefert. \square

Um den Vollständigkeitssatz zu beweisen, werden wir die äquivalente Umformulierung im Satz 2.55 beweisen. Wir müssen für eine widerspruchsfreien Theorie ein Modell konstruieren. Dafür führen wir neue Konstantenzeichen ein, welche erzwingen, dass die Theorie (in der erweiterten Sprache) genau die Kollektion aller Aussagen ist, welche in einer konkreten Struktur gelten.

Lemma 2.56. *Sei T eine widerspruchsfreie Theorie und χ eine Aussage. Eine der beiden Theorien $T \cup \{\chi\}$ oder $T \cup \{\neg\chi\}$ muss auch widerspruchsfrei sein (eventuell beide).*

Beweis. Ansonsten wären $T \cup \{\chi\}$ und $T \cup \{\neg\chi\}$ beide widersprüchlich. Wir werden nun zeigen, dass T auch widersprüchlich ist, was den gewünschten Widerspruch liefert. Aus dem Lemma 2.53 genügt es zu zeigen, dass T jede Aussage θ beweist. Nun ist $T \cup \{\chi\}$ widersprüchlich, so $T \cup \{\chi\} \vdash \theta$ und somit $T \vdash (\chi \rightarrow \theta)$ aus dem Korollar 2.48. Analog gilt, dass $T \cup \{\neg\chi\} \vdash \theta$, so $T \vdash (\neg\chi \rightarrow \theta)$. Somit folgern wir, dass $T \vdash \theta$, aus der aussagenlogischen Tautologie

$$\left((p \rightarrow q) \rightarrow ((\neg p \rightarrow q) \rightarrow q) \right),$$

indem wir p durch χ und q durch θ ersetzen. □

Proposition 2.57. *Jede widerspruchsfreie Theorie ist in einer vollständigen Theorie enthalten.*

Beweis. Sei T eine widerspruchsfreie Theorie. Wir definieren auf

$$\mathcal{S} = \{T' \text{ widerspruchsfreie } \mathcal{L}\text{-Theorie mit } T \subset T'\}$$

eine partielle Ordnung durch

$$T_1 \leq T_2 \iff T_1 \subset T_2.$$

Wir wollen zeigen, dass \mathcal{S} induktiv ist (siehe A.1). Sei Γ eine linear geordnete Teilmenge von \mathcal{S} . Falls $\Gamma = \emptyset$, dann ist das Element T aus \mathcal{S} eine obere Schranke aus \mathcal{S} . Falls $\Gamma \neq \emptyset$, ist die Kollektion

$$T^* = \bigcup_{T' \in \Gamma} T' = \{\mathcal{L}\text{-Aussagen } \chi \text{ mit } \chi \in T' \text{ für ein } T' \text{ aus } \Gamma\}$$

eine Theorie, welche jedes T' aus Γ enthält. Insbesondere enthält T^* die Theorie T . Es genügt also zu zeigen, dass T^* in \mathcal{S} liegt, das heißt, dass T^* widerspruchsfrei ist. Sonst gäbe es wegen Bemerkung 2.52 χ_1, \dots, χ_n aus T^* derart, dass die Teiltheorie $\{\chi_1, \dots, \chi_n\}$ widersprüchlich ist. Dies bedeutet, dass es T'_1, \dots, T'_n aus Γ mit φ_i in T'_i gibt. Da Γ linear geordnet ist, können wir $T'_1 \leq \dots \leq T'_n$ annehmen. Aber dann ist T'_n widersprüchlich, weil sie alle Aussagen χ_i enthält. Aus dem Zorn'schen Lemma A.3 folgt, dass eine maximale Theorie \widehat{T} in \mathcal{S} existiert. Per Definition ist \widehat{T} widerspruchsfrei und enthält T . Wir müssen nur zeigen, dass \widehat{T} vollständig ist. Sei χ eine beliebige Aussage. Wegen Lemma 2.56 liegt $\widehat{T} \cup \{\chi\}$ oder $\widehat{T} \cup \{\neg\chi\}$ in \mathcal{S} . Aus der Maximalität von \widehat{T} folgt, dass $\widehat{T} = \widehat{T} \cup \{\chi\}$ oder $\widehat{T} = \widehat{T} \cup \{\neg\chi\}$. Dementsprechend beweist \widehat{T} trivialerweise die Aussage χ oder ihre Negation. □

Bemerkung 2.58. Falls die Sprache \mathcal{L} abzählbar ist, kann man eine Vervollständigung der widerspruchsfreien Theorie T direkt konstruieren: Da jede Aussage eine endliche Folge von Symbolen aus der Sprache ist (unter anderem Quantoren und logische Zeichen), ist die Kollektion

aller \mathcal{L} -Aussagen auch abzählbar. Sei $\{\chi_n\}_{1 \leq n \in \mathbb{N}}$ eine Aufzählung aller \mathcal{L} -Aussagen. Definiere rekursiv für jedes n aus \mathbb{N} eine Theorie $T_n \supset T$ in folgender Weise: Setze $T_0 = T$ und

$$T_{n+1} = \begin{cases} T_n \cup \{\chi_n\}, & \text{falls } T_n \cup \{\chi_n\} \text{ widerspruchsfrei ist.} \\ T_n \cup \{\neg\chi_n\}, & \text{sonst.} \end{cases}$$

Die Theorie $\widehat{T} = \bigcup_{n \in \mathbb{N}} T_n$ ist vollständig und enthält T .

Definition 2.59. Eine Theorie T ist eine *Henkintheorie*, falls es zu jeder Formel $\varphi[x]$ ein Konstantenzeichen c_φ derart gibt, dass

$$T \vdash (\exists x \varphi[x] \rightarrow \varphi[c_\varphi]),$$

wobei $\varphi[c_\varphi] = \varphi_{c_\varphi/x}$.

Lemma 2.60. Sei $\varphi[x]$ eine \mathcal{L} -Formel und c ein neues Konstantenzeichen, das nicht aus \mathcal{L} kommt. Falls T widerspruchsfrei ist, so ist die $\mathcal{L} \cup \{c\}$ -Theorie $T \cup \{(\exists x \varphi[x] \rightarrow \varphi[c])\}$ widerspruchsfrei.

Beweis. Sonst wäre in der Sprache $\mathcal{L} \cup \{c\}$ wegen Korollar 2.54 die Aussage $\neg(\exists x \varphi[x] \rightarrow \varphi[c])$ aus T beweisbar. Aus Bemerkung 2.47 folgt, dass es eine endliche Konjunktion θ von Aussagen aus T gibt, sodass

$$\vdash_{\mathcal{L} \cup \{c\}} (\theta \rightarrow \neg(\exists x \varphi[x] \rightarrow \varphi[c])).$$

Insbesondere

$$\vdash_{\mathcal{L} \cup \{c\}} (\neg\theta \vee (\exists x \varphi[x] \wedge \neg\varphi[c]))$$

oder äquivalent dazu (mit Hilfe der entsprechenden aussagenlogischen Tautologien):

$$\vdash_{\mathcal{L} \cup \{c\}} ((\neg\theta \vee \exists x \varphi[x]) \wedge (\neg\theta \vee \neg\varphi[c])).$$

Dies bedeutet, dass sowohl $(\neg\theta \vee \exists x \varphi[x])$ als auch $(\neg\theta \vee \neg\varphi[c])$ in $\mathcal{L} \cup \{c\}$ beweisbar sind. Da $(\neg\theta \vee \exists x \varphi[x])$ eine \mathcal{L} -Aussage ist, heißt das, dass $(\neg\theta \vee \exists x \varphi[x])$ \mathcal{L} -beweisbar ist und somit ist dies auch $(\theta \rightarrow \exists x \varphi[x])$.

Analog ist $(\varphi[c] \rightarrow \neg\theta)$ beweisbar. Weil c nicht aus \mathcal{L} kommt, bedeutet dies, dass $(\varphi[x] \rightarrow \neg\theta)$ als \mathcal{L} -Formel beweisbar ist, wegen Lemma 2.46. Mit \exists -Einführung (weil θ eine Aussage ist, kommt x nicht frei vor), ist die Aussage $(\exists x \varphi[x] \rightarrow \neg\theta)$ auch beweisbar.

Aus der aussagenlogischen Tautologie

$$((p \rightarrow q) \rightarrow ((q \rightarrow \neg p) \rightarrow \neg p))$$

folgt mit Modus Ponens, dass $\neg\theta$ beweisbar ist. Aber θ ist eine endliche Konjunktion von Aussagen aus T , was mit Bemerkung 2.52 den gewünschte Widerspruch liefert. \square

Proposition 2.61. Jede widerspruchsfreie Theorie T in der Sprache \mathcal{L} ist in einer widerspruchsfreien Henkintheorie T^+ in der Sprache $\mathcal{L} \cup C$ enthalten, wobei C eine Menge neuer Konstantenzeichen ist.

Wenn die Sprache \mathcal{L} abzählbar ist, können wir die Menge C neuer Konstantenzeichen abzählbar wählen. Wenn die Sprache \mathcal{L} der Mächtigkeit Kontinuum ist (das heißt, die Mächtigkeit der reellen Zahlen), können wir die Menge C neuer Konstantenzeichen der Mächtigkeit Kontinuum wählen.

Beweis. Sei $(\varphi_i[x])_{i \in I}$ eine Aufzählung aller \mathcal{L} -Formeln in einer freien Variable. Desweiteren sei c_i für jedes i aus I ein neues Konstantenzeichen, das nicht in \mathcal{L} vorkommt, so dass $c_i \neq c_j$ für $i \neq j$. Setze $\mathcal{L}_0 = \mathcal{L}$ und $\mathcal{L}_1 = \mathcal{L} \cup \{c_i\}_{i \in I}$.

Mit iterierter Anwendung von Lemma 2.60 folgt aus der Bemerkung 2.52, dass für jedes i aus I die Theorie

$$T_i = T \cup \bigcup_{j < i} \{(\exists x \varphi_j[x] \rightarrow \varphi_j[c_j])\}_{j \leq i}$$

widerspruchsfrei ist (in der Sprache $\mathcal{L} \cup \{c_j\}_{j \leq i}$). Insbesondere ist die \mathcal{L}_1 -Theorie $T_1 = \bigcup_{i \in I} T_i$ widerspruchsfrei. Sie enthält T und hat die Eigenschaft, dass es für jede \mathcal{L}_0 -Formel $\varphi[x]$ ein Konstantenzeichen c_φ aus \mathcal{L}_1 so gibt, dass

$$T_1 \vdash (\exists x \varphi[x] \rightarrow \varphi[c_\varphi]).$$

Wir iterieren dieses Verfahren und konstruieren so in einer Spracherweiterung \mathcal{L}_2 eine Theorie T_2 aus T_1 mit den obigen Eigenschaften. Und dementsprechend allgemein T_{n+1} aus T_n . Setze

$$T^+ = \bigcup_{n \in \mathbb{N}} T_n$$

in der Sprache $\mathcal{L}^+ = \bigcup_{n \in \mathbb{N}} \mathcal{L}_n$. Jede \mathcal{L}^+ -Formel muss dann für ein n aus \mathbb{N} eine \mathcal{L}_n -Formel sein. Daraus folgt, dass T^+ eine Henkintheorie ist. \square

Bemerkung 2.62. Wenn die \mathcal{L} -Theorie T eine Henkintheorie ist, so ist jede Vervollständigung eine Henkintheorie.

Satz 2.63. Jede vollständige Henkintheorie T in der Sprache \mathcal{L} besitzt ein Modell, welches nur aus Interpretationen der Konstantenzeichen besteht. Ferner ist solch ein Modell bis auf Isomorphie eindeutig bestimmt.

Wenn die Sprache \mathcal{L} abzählbar ist, so ist das obige Modell abzählbar.

Beweis. Die Eindeutigkeit ist leicht zu zeigen. Sei C die Menge der Konstantenzeichen aus \mathcal{L} . Falls $\mathcal{A} = (c^{\mathcal{A}})_{c \in C}$ und $\mathcal{B} = (c^{\mathcal{B}})_{c \in C}$ zwei solche Modelle sind, dann sind sie wegen Bemerkung 2.51 elementar äquivalent. Insbesondere gilt für c und d aus C

$$c^{\mathcal{A}} = d^{\mathcal{A}} \Leftrightarrow T \vdash (c \doteq d) \Leftrightarrow c^{\mathcal{B}} = d^{\mathcal{B}}.$$

Die Funktion

$$\begin{aligned} F : A &\rightarrow B \\ c^{\mathcal{A}} &\mapsto c^{\mathcal{B}} \end{aligned}$$

ist eine Bijektion. Es genügt zu zeigen, dass F einen Isomorphismus zwischen den \mathcal{L} -Strukturen \mathcal{A} und \mathcal{B} definiert, was sofort aus den folgenden Überlegungen für jedes Funktionszeichen f , bzw Relationszeichen R , folgt.

$$c_{n+1}^{\mathcal{A}} = f(c_1^{\mathcal{A}}, \dots, c_n^{\mathcal{A}}) \Leftrightarrow T \vdash (c_{n+1} \doteq f(c_1, \dots, c_n)) \Leftrightarrow c_{n+1}^{\mathcal{B}} = f(c_1^{\mathcal{B}}, \dots, c_n^{\mathcal{B}}) \text{ und}$$

$$(c_1^A, \dots, c_k^A) \in R^A \Leftrightarrow T \vdash R(c_1, \dots, c_k) \Leftrightarrow (c_1^B, \dots, c_k^B) \in R^B.$$

Wir müssen also nur zeigen, dass so ein Model \mathcal{A} existiert. Definiere auf der Menge C der Konstantenzeichen folgende Relation:

$$c \sim d \Leftrightarrow T \vdash c \doteq d.$$

Aus den Gleichheitsaxiomen (mit Hilfe von Modus Ponens und Lemma 2.45) folgt, dass \sim eine Äquivalenzrelation auf C ist. Sei A die Menge der Äquivalenzklassen c/\sim . Wir wollen eine \mathcal{L} -Struktur \mathcal{A} auf der Menge A definieren.

Behauptung. Für jedes n -stellige Funktionszeichen f aus \mathcal{L} und alle c_1, \dots, c_n aus C gibt es ein c aus C derart, dass $T \vdash (f(c_1, \dots, c_n) \doteq c)$.

Beweis der Behauptung. Sei $\varphi[x] = (f(c_1, \dots, c_n) \doteq x)$. Weil T eine Henkintheorie ist, gibt es ein Konstantenzeichen c aus C derart, dass

$$T \vdash (\exists x \varphi[x] \rightarrow \varphi[c]).$$

Aus den Gleichheitsaxiomen und dem Lemma 2.45 folgt, dass $T \vdash (f(c_1, \dots, c_n) \doteq f(c_1, \dots, c_n))$ und somit

$$T \vdash \left((f(c_1, \dots, c_n) \doteq f(c_1, \dots, c_n)) \rightarrow \exists x \varphi \right),$$

weil x frei für $f(c_1, \dots, c_n)$ in $\varphi[x]$ ist. Aus iteriertem Modus Ponens folgt, dass

$$T \vdash (f(c_1, \dots, c_n) \doteq c),$$

wie gewünscht. □ Beh.

Definiere dementsprechend:

- $c^{\mathcal{A}} = c/\sim$;
- $f^{\mathcal{A}}(c_1/\sim, \dots, c_n/\sim) = c/\sim \Leftrightarrow T \vdash (f(c_1, \dots, c_n) \doteq c)$;
- $(c_1/\sim, \dots, c_k/\sim) \in R^{\mathcal{A}} \Leftrightarrow T \vdash R(c_1, \dots, c_k)$.

Beachte, dass diese Interpretationen wohldefiniert sind (dies besagen die Gleichheitsaxiome mit Hilfe von Modus Ponens und Lemma 2.45).

Induktiv über den Aufbau des Termes t ohne freie Variablen können wir leicht zeigen, dass

$$t^{\mathcal{A}} = c^{\mathcal{A}} \Leftrightarrow T \vdash (t \doteq c).$$

Wir wollen nun beweisen, dass \mathcal{A} ein Modell von T ist. Es genügt folgende Äquivalenz induktiv über den Aufbau der \mathcal{L} -Aussage χ zu zeigen:

$$\mathcal{A} \models \chi \Leftrightarrow T \vdash \chi,$$

Für $\chi = (t_1 \doteq t_2)$, wobei t_1 und t_2 Terme ohne freie Variablen sind, existieren c und d aus C mit $t_1^{\mathcal{A}} = c^{\mathcal{A}}$ und $t_2^{\mathcal{A}} = d^{\mathcal{A}}$. Insbesondere gilt $T \vdash ((t_1 \doteq c) \wedge (t_2 \doteq d))$ und

$$\mathcal{A} \models (t_1 \doteq t_2) \Leftrightarrow \mathcal{A} \models (c \doteq d) \Leftrightarrow T \vdash (c \doteq d) \Leftrightarrow T \vdash (t_1 \doteq t_2).$$

Genauso sieht man die Äquivalenz für den Fall $\chi = R(t_1, \dots, t_k)$. Der Fall $\chi = (\chi_1 \vee \chi_2)$ ist trivial. Falls $\chi = \neg\theta$, gilt

$$\mathcal{A} \models \chi \Leftrightarrow \mathcal{A} \not\models \theta \Leftrightarrow T \not\vdash \theta \xLeftrightarrow{T\text{vollst.}} T \vdash \chi.$$

Es ist nur noch der Fall $\chi = \exists x\psi$ übrig. Falls $\mathcal{A} \models \chi$, dann gibt es ein Element a aus \mathcal{A} mit $\mathcal{A} \models \psi[a]$. Aus der Konstruktion des Modells \mathcal{A} folgt, dass $a = d^{\mathcal{A}}$ für ein Konstantenzeichen d aus $\mathcal{L}_{\mathcal{A}}$. Dies bedeutet, dass $\mathcal{A} \models \psi[d]$ und induktiv folgt $T \vdash \psi[d]$. Weil d keine Variablen enthält, ist x frei für d in $\psi[x]$. Insbesondere folgt aus dem \exists -Quantorenaxiom, dass

$$\vdash (\psi[d] \rightarrow \exists x\psi[x]).$$

Insbesondere gilt mit Modus Ponens, dass $T \vdash \exists x\psi[x]$, das heißt, $T \vdash \chi$.

Falls $T \vdash \chi$, beachte, dass T eine Henkintheorie ist. Insbesondere gibt es ein c aus C mit $T \vdash (\exists x\psi[x] \rightarrow \psi[c])$. Mit Modus Ponens folgt also $T \vdash \psi[c]$. Induktiv erfüllt das Element $a = c/\sim$ aus A die Formel $\psi[x]$. Dies bedeutet, dass $\mathcal{A} \models \chi$, wie gewünscht. \square

Aus den Sätzen 2.55 und 2.63, und den Propositionen 2.57 und 2.61 folgt der Vollständigkeitsatz:

Korollar 2.64 (Vollständigkeitsatz). *Gegeben eine Theorie T und eine Aussage χ ,*

$$T \models \chi \Leftrightarrow T \vdash \chi.$$

Zusammen mit der Bemerkung 2.24 bekommen wir:

Korollar 2.65. *Eine widerspruchsfreie Theorie ist genau dann vollständig, wenn je zwei Modelle elementar äquivalent sind.*

Aus der Bemerkung 2.52 folgt nun folgendes:

Korollar 2.66 (Kompaktheitssatz). *Eine Theorie ist genau dann konsistent, wenn jede endliche Teiltheorie konsistent ist.*

Im Appendix C werden wir einen alternativen Beweis des Kompaktheitssatzes mit Hilfe von Ultraprodukten zeigen.

Beweis. Wir müssen nur zeigen, dass T ein Modell besitzt, wenn jede endliche Teiltheorie von T konsistent ist. Sonst wäre T wegen Satz 2.55 widersprüchlich. Aus der Bemerkung 2.52 gibt es endlich viele Aussagen aus T derart, dass diese Teiltheorie widersprüchlich ist und somit kein Modell besitzen. \square

Korollar 2.67 (Abzählbares aufwärts/abwärts Löwenheim-Skolem). *Jede konsistente Theorie in einer abzählbaren Sprache besitzt ein abzählbares Modell. Falls T unendliche Modelle (oder beliebig große endliche Modelle) besitzt, dann hat sie auch ein Modell der Mächtigkeit Kontinuum (das heißt, ein Modell der Mächtigkeit der reellen Zahlen \mathbb{R}).*

Beweis. Beachte, dass die Sprache der zu T gehörigen Henkintheorie wiederum abzählbar ist. Insbesondere ist das Modell, welches aus den Interpretationen der Konstanten besteht, auch abzählbar.

Falls T ein unendliches Modell (oder beliebig große endliche Modelle) besitzt, wähle neue paarweise verschiedene Konstantenzeichen $\{c_r\}_{r \in \mathbb{R}}$ und definiere

$$T' = T \cup \{\neg(c_r \doteq c_s)\}_{r \neq s \in \mathbb{R}}.$$

Diese Theorie ist endlich konsistent, das heißt, jede endliche Teiltheorie ist konsistent. Insbesondere gibt es ein Modell, welche aus Interpretationen der Konstantenzeichen besteht. Wir haben Kontinuum viele Konstantenzeichen und sie liefern verschiedene Elemente. \square

Korollar 2.68. *Sei \mathcal{C} eine Klasse endlicher \mathcal{L} -Strukturen, welche für jedes n aus \mathbb{N} eine Struktur der Mächtigkeit zumindest n enthält. Die Klasse \mathcal{C} ist nicht axiomatisierbar (siehe Definition 2.25).*

Insbesondere ist die Klasse aller endlichen Gruppen (in der Gruppensprache \mathcal{L}_{Gp}) sowie die Klasse aller endlichen vollständigen Graphen (in der Sprache $\mathcal{L}_{Graphen}$) nicht axiomatisierbar.

Mit Hilfe der Bemerkung 2.26 läßt sich folgendes leicht mit Kompaktheit zeigen:

Korollar 2.69. *In der Sprache $\mathcal{L} = \{0, +\}$ gibt es eine nichtstandard Erweiterung \mathcal{M} der Struktur $\mathcal{N} = (\mathbb{N}, 0, +)$, das heißt, die Struktur \mathcal{M} ist eine elementare Erweiterung von \mathcal{N} und besitzt ein Element m aus M , welche sich von jeder Primzahl aus \mathbb{N} teilen läßt.*

Analog besitzt die Struktur $(\mathbb{R}, <)$ elementare Erweiterungen mit nichtstandard Elementen, welche größer als alle reellen Zahlen sind.

Kapitel 3

Mengenlehre

Wir werden in diesem Abschnitt eine Grundaxiomatik einführen, um die naiven mengentheoretischen Konstruktionen aus der Mathematik zu formalisieren. Dieses Axiomensystem, namens ZF für *Ernst Zermelo* und *Abraham Fraenkel*, besteht aus folgenden Axiomen: *Extensionalität*, *Aussonderung*, *Paarmenge*, *Vereinigung*, *Potenzmenge*, *Ersetzung*, *Fundierung* und *Unendlichkeit*, wobei *Aussonderung* und *Ersetzung* keine Aussagen, sondern eher Aussagenschemata sind. Daher ist ZF nicht endlich axiomatisierbar, jedoch rekursiv axiomatisierbar (siehe Definition 4.29 im Abschnitt 4). Das von ZF unabhängige *Auswahlaxiom* bildet zusammen mit ZF die Erweiterung ZFC.

Es wird angenommen, dass ZF (oder eher ZFC) stark genug ist, um jede mathematische Konstruktion und jeden Beweis zu implementieren. Diese Annahme (philosophischer Natur) bedeutet wegen des zweiten Gödel'schen Unvollständigkeitssatzes, dass wir nicht im Rahmen der Axiomatik der Theorie ZF zeigen können, dass diese konsistent ist. Denn ein Beweis in ZF ist eine endliche Menge (eher eine Folge) von Aussagen, die wiederum endliche Mengen (eher Folgen) von Symbolen in der endlichen Sprache $\mathcal{L}_{ZF} = \{\in\}$ sind.

3.1 Das Axiomensystem ZF

Um die Relevanz jedes einzelnen Axiomes zu begreifen, werden wir konsekutiv eines nach dem anderen präsentieren. Wir nehmen an, dass wir in der Sprache \mathcal{L}_{ZF} , die aus einem zweistelligen Relationszeichen \in (für Elementzeichen oder Zugehörigkeit) besteht, innerhalb eines Modelles der Theorie ZF arbeiten, dessen Grunduniversum wir mit \mathbb{V} bezeichnen,

Notation. Die Abkürzung $x \subset y$ bedeutet, dass

$$\mathbb{V} \models \forall z(z \in x \rightarrow z \in y)$$

Elemente aus \mathbb{V} heißen *Mengen*. Der Begriff *Menge* ist somit mehrdeutig: Elemente y aus \mathbb{V} , die in \in -Relation zu einer Menge x aus \mathbb{V} stehen, sind wiederum *Mengen*. Ferner sind Teilkollektionen von \mathbb{V} auch Mengen (extern gesehen). Diese mögliche Verwirrung könnten wir auf verschiedene Weisen lösen, z. B. mit Hilfe von Typentheorie, aber wir hoffen, dass der Leser den Unterschied versteht. Dennoch ist nicht jede Teilkollektion von \mathbb{V} eine Menge (im ersten Sinne), denn die Russel'sche Antomie liefert, dass $\{x \in \mathbb{V} \mid x \notin x\}$ keine Menge (im ersten Sinne) ist, das heißt, es gibt kein Element z aus \mathbb{V} derart, dass

$$\mathbb{V} \models \forall x(x \in z \leftrightarrow x \notin x).$$

Teilkollektionen aus \mathbb{V} , welche in \mathcal{L}_{ZF} definierbar sind, werden häufig *Klassen* genannt. Das Extensionalitätsaxiom besagt, dass jedes Element x aus \mathbb{V} eine definierbare Teilmenge von \mathbb{V} bestimmt, nämlich die Elemente, welche zu x gehören.

Extensionalität

$$\forall x \forall y \left((x \subset y \wedge y \subset x) \rightarrow (x \doteq y) \right)$$

Um die Russel'sche Antinomie zu lösen, entstehen Mengen erst, wenn wir aus einer gegebenen Menge x die Teilmenge der Elemente betrachten, welche eine mit Parametern definierbare konkrete Eigenschaft erfüllen. Für jede \mathcal{L}_{ZF} -Formel $\varphi[z, y_1, \dots, y_n]$ gibt es folgendes Axiom:

Aussonderung

$$\forall x \forall y_1 \dots \forall y_n \exists u \forall z (z \in u \leftrightarrow z \in x \wedge \varphi[z, y_1, \dots, y_n])$$

Aus Extensionalität folgt, dass die obige Menge u eindeutig ist.

Korollar 3.1. $ZF \vdash \neg \exists x \forall z (z \in x)$

Da \mathbb{V} nicht-leer ist, können wir mit Hilfe der Aussonderung bezüglich der Formel $\varphi[z] = \neg(z \doteq z)$ die leere Menge gewinnen.

Korollar 3.2. *Es gibt genau eine Menge in \mathbb{V} , welches kein Element enthält. Wir bezeichnen diese Menge mit \emptyset .*

Paarmenge

$$\forall x \forall y \exists z \forall u \left(u \in z \leftrightarrow ((u \doteq x) \vee (u \doteq y)) \right)$$

Die obige Menge z ist wegen Extensionalität eindeutig bestimmt und wird mit $\{x, y\}$ bezeichnet. Damit definieren wir das (*geordnete*) *Paar* (x, y) als $\{\{x\}, \{x, y\}\}$.

Korollar 3.3. $ZF \vdash \forall x \forall y \forall z \forall u \left(((x, y) \doteq (z, u)) \leftrightarrow ((x \doteq z) \wedge (y \doteq u)) \right)$

Vereinigung

$$\forall x \exists y \forall z \left(z \in y \leftrightarrow \exists u ((u \in x) \wedge (z \in u)) \right)$$

Die obige Menge y ist wegen Extensionalität eindeutig bestimmt und wird mit $\bigcup x$ bezeichnet. Sie besteht aus den Elementen, welche zu einem Element von x gehören. Insbesondere ist die *Vereinigung* zweier Mengen

$$x \cup y = \bigcup \{x, y\}.$$

Induktiv definieren wir $\{x_1, \dots, x_n\} = \{x_1, \dots, x_{n-1}\} \cup \{x_n\}$.

Ein leerer Durchschnitt ist allgemein nicht wohldefiniert. Wenn $x \neq \emptyset$, gibt es ein y mit $y \in x$. Mit Aussonderung definieren wir den *Durchschnitt* von x als

$$\bigcap x = \{z \in y \mid \forall u (u \in x \rightarrow z \in u)\}.$$

Beachte, dass der Durchschnitt nicht vom Element y abhängt. Setze nun

$$x \cap y = \bigcap \{x, y\}.$$

Aussonderung liefert auch, dass das *relative Komplement*

$$x \setminus y = \{z \in x \mid z \notin y\}$$

eine Menge bildet.

Die Kollektion aller Elemente, welche eine Teilmenge von x sind, soll auch ein Element von \mathbb{V} sein, nämlich die Potenzmenge $\mathcal{P}(x)$.

Potenzmenge

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subset x)$$

Korollar 3.4. Für jedes x und y aus \mathbb{V} gibt es eine Menge $x \times y$ in \mathbb{V} , das kartesische Produkt von x und y , deren Elemente genau die angeordneten Paare (a, b) mit a aus x und b aus y sind.

Beweis. Falls a aus x und b aus y sind, dann liegen $\{a\}$ und $\{a, b\}$ in $\mathcal{P}(x \cup y)$. Somit ist $(a, b) \subset \mathcal{P}(x \cup y)$, das heißt, das Element (a, b) liegt in $\mathcal{P}(\mathcal{P}(x \cup y))$. Mit Hilfe von Aussonderung setze

$$x \times y = \left\{ z \in \mathcal{P}(\mathcal{P}(x \cup y)) \mid \exists a \exists b \left((a \in x \wedge b \in y) \wedge (z \doteq (a, b)) \right) \right\}$$

□

Bemerkung 3.5. Sei R eine Menge derart, dass das angeordnete Paar (x, y) in R liegt. Dann liegt $\{x, y\}$ in $\bigcup R$ und somit liegen x und y beide in $\bigcup \bigcup R$. Insbesondere sind mit Hilfe von Aussonderung folgende Objekte auch Mengen:

$$\begin{aligned} \text{Dom}(R) &= \{x \in \bigcup \bigcup R \mid \exists y ((x, y) \in R)\} \\ \text{Im}(R) &= \{y \in \bigcup \bigcup R \mid \exists x ((x, y) \in R)\} \end{aligned}$$

Die Menge R ist eine *Relation* auf $\text{Dom}(R) \times \text{Im}(R)$, falls jedes Element z aus R von der Form $z = (x, y)$ mit x in $\text{Dom}(R)$ und y in $\text{Im}(R)$ ist.

Eine *Funktion* oder eine *Abbildung* f ist eine Relation derart, dass es für jedes a aus $\text{Dom}(f)$ genau ein y in $\text{Im}(f)$ mit (a, y) in f gibt. Wir bezeichnen das eindeutige Element y mit $f(x)$ und schreiben $f : \text{Dom}(f) \rightarrow \text{Im}(f)$. Somit werden die bekannten Begriffe *Injektivität*, *Surjektivität* und *Bijektion* eingeführt.

Beachte, dass sich die Menge x injektiv in $\mathcal{P}(x)$ durch die Abbildung $a \mapsto \{a\}$ einbetten lässt. Diese Abbildung ist keine Bijektion.

Satz 3.6 (Cantor). *Es gibt keine Surjektion von der Menge x nach $\mathcal{P}(x)$.*

Beweis. Falls die Abbildung $f : x \rightarrow \mathcal{P}(x)$ surjektiv wäre, hätte die Teilmenge

$$z = \{y \in x \mid y \notin f(y)\}$$

ein Urbild u in x . Die Äquivalenz

$$u \in z \iff u \notin z$$

liefert den gewünschten Widerspruch. □

Die Kollektion v der Bilder der Elemente x einer Menge u durch eine mit Parametern definierbare Funktion, welche durch die Formel $\varphi[x_1, y_1, z_1, \dots, z_n]$ gegeben wird, soll auch eine Menge bilden. Wir benutzen die Abkürzung $\exists!y_1\varphi[x_1, y_1, z_1, \dots, z_n]$ für

$$\left(\exists y_1\varphi[x_1, y_1, z_1, \dots, z_n] \wedge \forall y_2(\varphi[x_1, y_2, z_1, \dots, z_n] \rightarrow (y_1 \doteq y_2))\right)$$

Ersetzung

$$\forall u\forall w_1\dots\forall w_n\left(\forall x\exists!y\varphi[x, y, w_1, \dots, w_n] \rightarrow \exists v\forall y_1(y_1 \in v \leftrightarrow \exists x_1(x_1 \in u \wedge \varphi[x_1, y_1, w_1, \dots, w_n]))\right)$$

Korollar 3.7. Für jede Relation R ist R^{-1} eine Relation auf $\text{Im}(R) \times \text{Dom}(R)$, wobei

$$(b, a) \in R^{-1} \iff (a, b) \in R.$$

Das Fundierungsaxiom bedeutet, dass keine unendliche \in -Schleife existiert, obwohl der Begriff der Unendlichkeit noch zu definieren ist. Jeder Menge wird somit eine wohldefinierte Komplexität zugeordnet, welche \in -Rekursion auf \mathbb{V} ermöglicht.

Fundierung

$$\forall x\exists y\left(\neg(x \doteq \emptyset) \rightarrow (y \in x \wedge \neg\exists z(z \in y \wedge z \in x))\right)$$

Korollar 3.8. $ZF \vdash \forall x(x \notin x)$

Beweis. Ansonsten gäbe es ein x in \mathbb{V} mit $x \in x$. Setze

$$y = \{z \in x \mid z \in z\}$$

Da x ein Element von x ist, ist $y \neq \emptyset$. Wegen Fundierung gibt es ein Element z in y mit $z \cap y = \emptyset$. Weil z in y liegt, folgt $z \in z$ und somit liegt z in $z \cap y = \emptyset$, was den gewünschte Widerspruch liefert. \square

Definition 3.9. Eine Menge x ist *transitiv*, falls $\bigcup x \subset x$, oder äquivalent dazu, falls $z \in x$, wenn $z \in y$ für ein $y \in x$.

Typische Beispiele transitiver Menge sind \emptyset oder $\{\emptyset\}$. Allgemeiner gilt:

Lemma 3.10. Wenn x transitiv ist, so ist $x \cup \{x\}$ dies auch.

Beweis. Sei $z \in y$ mit $y \in x \cup \{x\}$. Es folgt, dass $y \in \{x\}$ oder $y \in x$. Dies bedeutet entweder $y = x$ oder $y \in x$. Falls $y = x$, dann liegt z in $x = y$, und somit in $x \cup \{x\}$. Ansonsten liegt y in x , welches transitiv ist, und somit liegt z auch in $x \subset x \cup \{x\}$, wie gewünscht. \square

Definition 3.11. Gegeben eine Menge x , ist ihr *Nachfolger* die Menge $S(x) = x \cup \{x\}$. Wir definieren rekursiv die Menge \underline{n} , für n in \mathbb{N} , folgenderweise:

- $\underline{0} = \emptyset$.
- $\underline{n+1} = S(\underline{n})$.

Beachte, dass \underline{n} transitiv ist, für jedes n aus \mathbb{N} , wegen Lemma 3.10.

Lemma 3.12. Für m und n aus \mathbb{N} gilt:

- $ZF \vdash \left(\underline{m} \in \underline{n} \wedge \neg(\underline{m} \doteq \underline{n}) \right)$, falls $m < n$.
- $ZF \vdash \underline{m} \notin \underline{n}$, falls $n \leq m$.

Beweis. Es genügt zu zeigen, dass $ZF \vdash \underline{m} \in \underline{n}$, für $m < n$. Aus dem Korollar 3.8 folgt dann, dass $\underline{m} \neq \underline{n}$. Analog, falls $\mathbb{V} \models \underline{m} \in \underline{n}$ für $n \leq m$, müssen n und m verschieden sein, also $n < m$ und somit $\underline{n} \in \underline{m}$. Weil die Menge \underline{m} transitiv ist, folgt aus

$$\underline{m} \in \underline{n} \in \underline{m},$$

dass $\underline{m} \in \underline{m}$, was dem Korollar 3.8 widerspricht.

Wir zeigen nun für $m < n$ induktiv über n , dass $ZF \vdash \underline{m} \in \underline{n}$. Für $n = 0$ ist die Aussage trivial. Sei nun $m < n = k + 1$. Wenn $m = k$, liegt $\underline{m} = \underline{k}$ in $\underline{k} \cup \{k\} = \underline{k+1} = \underline{n}$.

Falls $m < k$, dann liegt aus der Induktionsannahme \underline{m} in $\underline{k} \in \underline{k+1} = \underline{n}$. Da \underline{n} transitiv ist, liegt \underline{m} in \underline{n} , wie gewünscht. \square

Die nachfolgenden Begriffe *lineare Ordnung*, *kleinstes* und *größtes Element* werden im Appendix A.1 definiert.

Definition 3.13. Eine Menge x ist eine *natürliche Zahl*, falls x transitiv ist und die Relation \in eingeschränkt auf Elemente von x eine lineare Ordnung so bestimmt, dass jede nicht-leere Teilmenge $y \subset x$ ein \in -kleinstes und ein \in -größtes Element besitzt.

Beachte, dass es eine \mathcal{L}_{ZF} -Formel $\varphi_{\text{Nat.Zahl}}[x]$ derart gibt, dass $\mathbb{V} \models \varphi_{\text{Nat.Zahl}}[a]$ genau dann, wenn die Menge a eine natürliche Zahl ist.

Lemma 3.14.

- (a) $ZF \vdash \forall x \forall y \left((\varphi_{\text{Nat.Zahl}}[x] \wedge y \in x) \rightarrow \varphi_{\text{Nat.Zahl}}[y] \right)$
- (b) $ZF \vdash \forall x \left(\varphi_{\text{Nat.Zahl}}[x] \rightarrow \varphi_{\text{Nat.Zahl}}[S(x)] \right)$
- (c) $ZF \vdash \varphi_{\text{Nat.Zahl}}[\underline{n}]$, für jedes n aus \mathbb{N} .
- (d) $ZF \vdash \forall x \left((\varphi_{\text{Nat.Zahl}}[x] \wedge \neg(x \doteq \underline{0})) \rightarrow \exists y (\varphi_{\text{Nat.Zahl}}[y] \wedge (x \doteq S(y))) \right)$

Beweis. Für (a) sei x eine Menge aus \mathbb{V} , welche die Formel $\varphi_{\text{Nat.Zahl}}$ erfüllt, und y ein Element aus x . Beachte, dass $y \subset x$. Insbesondere ist die Relation \in auf y eine lineare Ordnung und jede nicht-leere Teilmenge aus y besitzt sowohl ein \in -kleinstes als auch ein \in -größtes Element. Es genügt zu zeigen, dass y auch transitiv ist. Falls $u \in z \in y$, ist $z \in x$ und somit liegt u in x , weil x transitiv ist. Da \in linear auf x ist, folgt aus

$$u \in z \in y,$$

dass $u \in y$.

Für (b) beachte, dass wegen Lemma 3.10 die Menge $S(x) = x \cup \{x\}$ transitiv ist, wenn x eine natürliche Zahl ist. Zwei verschiedene Elemente aus $S(x)$ sind entweder beide in x enthalten, und somit bezüglich \in linear geordnet, oder eines von ihnen ist x , welches das andere Element

enthält. Somit ist \in eine lineare Ordnung auf $S(x)$ derart, dass das Element x echt größer als alle Elemente aus x ist. Gegeben $\emptyset \neq y \subset S(x)$, liegt y ganz in x oder enthält das Element x . In beiden Fällen besitzt y ein \in -größtes Element. Analog zeigen wir, dass y ein \in -kleinstes Element besitzt, abhängig davon, ob $y \cap x = \emptyset$.

Wir zeigen (c) induktiv über n in \mathbb{N} . Für $n = 0$ ist $\underline{0} = \emptyset$, welche klarerweise $\varphi_{\text{Nat.Zahl}}$ erfüllt. Falls $n > 0$, ist $n = k + 1$ für eine natürliche Zahl k und somit $\underline{n} = S(\underline{k})$. Aus (b) folgt, dass \underline{n} auch eine natürliche Zahl ist.

Für (d) sei die nicht-leere Menge x eine natürliche Zahl. Insbesondere besitzt x ein \in -größtes Element y . Aus (a) folgt, dass y eine natürliche Zahl ist. Ferner ist

$$x = \{z \in x \mid (z \in y \vee z = y)\} = y \cup \{y\} = S(y),$$

wie gewünscht. □

Das Axiom der Unendlichkeit besagt, dass die Kollektion aller natürliche Zahlen eine Menge bildet.

Unendlichkeit

$$\exists x \left(\emptyset \in x \wedge \forall y (y \in x \rightarrow S(y) \in x) \right)$$

Mit Hilfe der Aussonderung bezüglich der Formel $\varphi_{\text{Nat.Zahl}}$ konstruieren wir die Menge der natürlichen Zahlen.

Korollar 3.15. *Es gibt eine Menge ω , welche genau aus allen natürlichen Zahlen besteht.*

Korollar 3.16 (Induktionsprinzip für ω). *Die einzige Teilmenge von ω , welche $\underline{0}$ enthält und unter Nachfolger abgeschlossen ist, ist ω .*

Beweis. Sei $x \subset \omega$ unter Nachfolger abgeschlossen und $\underline{0}$ in x . Das Komplement $y = \omega \setminus x$ ist wegen Aussonderung eine Menge. Beachte, dass $x \neq \omega$ genau dann, wenn $y \neq \emptyset$, wegen Extensionalität.

Wir nehmen nun $x \neq \omega$ an. Sei $z \in y \neq \emptyset$. Da $z \notin x$, ist $z \neq \underline{0}$ eine natürliche Zahl und somit ist $z = S(u)$ für eine natürliche Zahl u . Insbesondere ist u nicht in x , weil z nicht in x liegt. Wegen Aussonderung bildet

$$v = \{w \in z \mid w \in y\}$$

eine nicht-leere Menge. Sei w ein \in -kleinstes Element in v . Wegen der Eigenschaft (a) des vorigen Lemmas 3.14, ist w eine natürliche Zahl. Da w nicht in x liegt, ist $w \neq \underline{0}$, also gibt es wegen Lemma 3.14 (d) eine natürliche Zahl w' in ω mit $w = S(w')$. Da x unter Nachfolger abgeschlossen ist, kann w' nicht in x liegen. Insbesondere liegt w' in y . Ferner ist $w' \in w \in z$, welche eine transitive Menge ist, also $w' \in z$. Das heißt, dass w' in v liegt. Dies ist ein Widerspruch dazu, dass w das \in -kleinstes Element in v war. □

Falls ZF konsistent ist, finden wir wegen Kompaktheit Modelle mit nichtstandard natürlichen Zahlen.

Korollar 3.17. *Falls ZF konsistent ist, gibt es Modelle \mathcal{M} von ZF mit nichtstandard natürlichen Zahlen, das heißt, natürliche Zahlen x in ω derart, dass $x \neq \underline{n}$ für jedes n aus \mathbb{N} .*

Es gibt keine kleinste nichtstandard natürliche Zahl in \mathcal{M} .

3.2 Angeordnete Mengen und Ordinalzahlen

In diesem Abschnitt werden wir die Konstruktion natürlicher Zahlen verallgemeinern, um die sogenannten *Ordinalzahlen* zu konstruieren, welche eine echte Klasse von \mathbb{V} bilden. Mit Hilfe des Rekursionssatzes definieren wir die Summe und Multiplikation zweier Ordinalzahlen.

Bemerkung 3.18. Seien x und y zwei transitive Mengen. Der Durchschnitt $S = x \cap y$ ist auch transitiv.

Definition 3.19. Eine *Ordinalzahl* ist eine transitive Menge, welche linear angeordnet bezüglich der Relation \in ist.

Natürliche Zahlen sind Ordinalzahlen. Jede Ordinalzahl $x \neq \emptyset$ enthält das Element \emptyset : Wegen Fundierung gibt es $y \in x$ derart, dass $y \cap x = \emptyset$. Es genügt zu zeigen, dass $y = \emptyset$. Sonst gäbe es $z \in y$ und da x transitiv ist, läge z in x und somit in $y \cap x$, was ein Widerspruch wäre.

Die Eigenschaft Ordinalzahl zu sein ist durch eine \mathcal{L}_{ZF} -Formel ausdrückbar. Wir schreiben On für die Klasse der Ordinalzahlen, das heißt, die Erfüllungsmenge dieser Formel im Modell \mathbb{V} . Der Ausdruck $\alpha \in \text{On}$ bedeutet, dass α eine Ordinalzahl ist.

Notation. Wir bezeichnen mit $<$ die Relation \in zwischen Ordinalzahlen und Elementen davon. Beachte, dass jedes Element einer Ordinalzahl wiederum eine Ordinalzahl ist.

Eine Teilmenge S der linear geordnet Menge $(x, <)$ ist ein *Anfangssegment von x* , falls für jedes u aus x und z aus S mit $u < z$, das Element u in S liegt.

Lemma 3.20.

(a) Jedes echte Anfangssegment $S \subsetneq \alpha$ einer Ordinalzahl α bezüglich der Relation \in ist ein Element aus α .

(b) Die Klasse On ist durch \in linear angeordnet, das heißt, gegeben zwei verschiedene Ordinalzahlen α und β , ist $\alpha \in \beta$ oder $\beta \in \alpha$.

(c) $\omega \in \text{On}$.

(d) Für $\alpha \in \text{On}$,

$$\alpha = \{\beta \in \text{On} \mid \beta \in \alpha\}$$

(e) Jede nicht-leere Teilklasse χ von On hat ein \in -kleinstes Element. Insbesondere ist On eine echte Klasse und bildet keine Menge.

Beweis. Für (a) sei $S \subsetneq \alpha$ ein echtes Anfangssegment. Die Menge $\alpha \setminus S$ ist nicht leer und Fundierung liefert ein β in $\alpha \setminus S$ mit $\beta \cap (\alpha \setminus S) = \emptyset$. Da α transitiv ist, folgt $\beta \subset S$. Ferner ist $S \subset \beta$, weil S ein Anfangssegment der linearen Ordnung $(\alpha, <)$ ist. Also $S = \beta \in \alpha$.

Für (b) seien $\alpha \neq \beta$ Ordinalzahlen. Die Menge $S = \alpha \cap \beta$ ist ein Anfangssegment von α und von β , wegen der Transitivität von α und von β . Da $\alpha \neq \beta$, muss die Menge S eine echte Teilmenge von α oder von β sein. Beachte, dass diese zwei Fälle nicht gleichzeitig eintreten können, denn sonst gehört S zu $\alpha \cap \beta = S$, was dem Korollar 3.8 widerspricht. Weil die Situation symmetrisch ist, können wir annehmen, dass $\beta = S \subsetneq \alpha$. Aus dem obigen Teil (a) folgt, dass β in α liegt, wie gewünscht.

Da je zwei natürliche Zahlen Ordinalzahlen sind und wegen (b) vergleichbar sein müssen, folgt aus dem Lemma 3.14 (a), dass ω eine Ordinalzahl ist.

Für (d) sei α in On . Es genügt zu zeigen, dass $\alpha \subset \{\beta \in \text{On} \mid \beta \in \alpha\}$, was sofort aus der obigen Bemerkung folgt, weil jedes Element von α eine Ordinalzahl ist.

Für (e) sei χ eine nicht-leere Teilklasse von On und α in χ . Wegen Aussonderung ist $x = \{\beta \in \alpha \mid \beta \in \chi\}$ eine Menge. Falls $x = \emptyset$, ist α kleinstes Element in χ . Ansonsten gibt es wegen Fundierung ein Element β in $x \subset \alpha$ mit $\beta \cap x = \emptyset$. Weil α transitiv ist, ist β kleinstes Element von χ .

Falls On eine Menge wäre, wäre On wegen (a) und (b) eine Ordinalzahl, weil jedes Element einer Ordinalzahl wiederum in On liegt, was dem Korollar 3.8 widerspricht. \square

Korollar 3.21 (Induktionsprinzip für On). *Sei χ eine Teilklasse Ordinalzahlen derart, dass für jedes α in On ,*

$$\alpha \subset \chi \implies \alpha \in \chi.$$

Dann ist $\chi = \text{On}$.

Beweis. Klarerweise ist \emptyset in χ , weil $\emptyset \subset \chi$. Falls $\text{On} \neq \chi$, gäbe es wegen Lemma 3.20 (e) ein kleinstes Element α in $\text{On} \wedge \neg \chi \neq \emptyset$. Aus der Minimalität folgt, dass

$$\{\beta \in \text{On} \mid \beta \in \alpha\} = \alpha \subset \chi,$$

was widerspricht, dass α nicht in χ liegt. \square

Analog zu Lemma 3.14 (b) zeigen wir, dass $S(\alpha)$ für α in On eine Ordinalzahl ist.

Definition 3.22. Eine Ordinalzahl α ist *Nachfolgerzahl*, falls $\alpha = S(\beta)$ für eine Ordinalzahl β gilt. Beachte, dass $\beta < \alpha$.

Eine Ordinalzahl $\alpha \neq \underline{0}$ ist *Limeszahl*, wenn sie keine Nachfolgerzahl ist.

Die Ordinalzahl ω ist eine Limeszahl.

Bemerkung 3.23. Eine Ordinalzahl $\alpha \neq \emptyset$ ist genau dann eine Limeszahl, wenn es für alle $\beta < \alpha$ ein $\gamma < \alpha$ mit $\beta < \gamma < \alpha$ gibt.

Bemerkung 3.24. Gegeben eine nicht-leere Menge I von Ordinalzahlen, ist die Menge $\alpha = \bigcup I$ transitiv und wiederum eine Ordinalzahl. Ferner ist $\beta \leq \alpha$ für jedes β aus I und α ist die kleinste Ordinalzahl, welche größer oder gleich aller Elemente aus I ist. Das heißt, die Ordinalzahl $\alpha = \sup I$ ist das *Supremum* der Ordinalzahlen aus I .

Wenn das Element α kein Maximum von I ist, so ist α Limeszahl. Die Rückrichtung gilt offensichtlich nicht.

Lemma 3.25. *Für jede streng monoton wachsende Abbildung f von der Ordinalzahl α zu der Ordinalzahl α' ist $f(\beta) \geq \beta$ für alle $\beta < \alpha$. Insbesondere ist $\alpha \leq \alpha'$.*

Falls f ein Isomorphismus ist (von angeordneten Mengen), dann ist $\alpha = \alpha'$ und f muss die Identität sein.

Beweis. Wir nehmen an, dass es ein $\beta < \alpha$ mit $f(\beta) < \beta$ gäbe. Wegen Lemma 3.20 (e) können wir annehmen, dass β kleinstmöglich in α mit dieser Eigenschaft ist. Da α transitiv ist, liegt $f(\beta)$ in α . Weil f streng monoton wachsend ist, folgt, dass $f(f(\beta)) < f(\beta) < \beta$, was der Minimalität von β widerspricht.

Da $\beta \leq f(\beta) < \alpha'$ für jedes β aus α , ist α eine Teilmenge von α' . Falls $\alpha' < \alpha$, hätten wir einen Widerspruch zum Korollar 3.8, da die Ordinalzahlen linear angeordnet sind. Also $\alpha \leq \alpha'$.

Wir nehmen nun an, dass f ein Isomorphismus ist. Dann ist f^{-1} streng monoton wachsend und somit gilt $\alpha' \leq \alpha$, also $\alpha' = \alpha$. Um zu zeigen, dass f die Identität sein muss, genügt es zu zeigen, dass es kein $\beta < \alpha$ mit $f(\beta) \neq \beta$ gibt. Ansonsten können wir annehmen, dass β kleinstmöglich in α mit dieser Eigenschaft ist. Da α linear angeordnet und $f(\beta) \geq \beta$ ist, folgt, dass $\beta < f(\beta)$. Sei γ in $f(\beta) \setminus \beta$. Weil f ein Isomorphismus ist, gibt es ein $\delta < \alpha$ mit $f(\delta) = \gamma$. Insbesondere ist $\delta < \beta$, also muss $\gamma = f(\delta) = \delta$ in β liegen, was den gewünschten Widerspruch liefert. \square

Definition 3.26. Eine *Wohlordnung* $<$ auf der Menge x ist eine *fundierte* lineare Ordnung, das heißt, dass jede nicht-leere Teilmenge y von x ein kleinstes Element besitzt.

Bemerkung 3.27. Jede Ordinalzahl ist wohlgeordnet bezüglich der Relation \in , welche wir weiter mit $<$ bezeichnen.

Beispiel 3.28. Die *angeordnete Summe* $x_1 \dot{+} x_2$ zweier linear geordneter Mengen $(x_1, <_1)$ und $(x_2, <_2)$ ist die Menge

$$x_1 \sqcup x_2 = (x_1 \times \{\underline{1}\}) \cup (x_2 \times \{\underline{2}\})$$

mit der linearen Ordnung

$$(z, i) <_{x_1 \dot{+} x_2} (u, j) \iff \begin{cases} i <_{\text{On}} j \text{ oder} \\ i = j \text{ und } z <_i u \end{cases}$$

Das *angeordnete Produkt* $x \dot{\times} y$ der linear geordneten Mengen $(x, <_x)$ und $(y, <_y)$ ist die Menge $x \times y$ mit der linearen Ordnung

$$(z_1, u_1) <_{x \dot{\times} y} (z_2, u_2) \iff \begin{cases} u_1 <_y u_2 \text{ oder} \\ u_1 =_y u_2 \text{ und } z_1 <_x z_2 \end{cases}$$

Wenn x und y beide wohlgeordnet sind, so sind $x \dot{+} y$ und $x \dot{\times} y$ wohlgeordnet bezüglich der obigen Ordnungen.

Bemerkung 3.29. Für linear geordnete Mengen $(x, <_x)$, $(y, <_y)$ und $(z, <_z)$ gilt:

- $(x \dot{+} y) \dot{+} z \simeq x \dot{+} (y \dot{+} z)$.
- $(x \dot{\times} y) \dot{\times} z \simeq x \dot{\times} (y \dot{\times} z)$.
- $x \dot{\times} (y \dot{+} z) \simeq (x \dot{\times} y) \dot{+} (x \dot{\times} z)$.

Satz 3.30. Jede wohlgeordnete Menge ist isomorph zu einer Ordinalzahl. Diese Ordinalzahl sowie der Isomorphismus sind eindeutig bestimmt.

Beweis. Sei $(x, <)$ eine wohlgeordnete Menge und y in x . Falls das Anfangssegment

$$S_y = \{z \in x \mid z < y\}$$

isomorph zu einer Ordinalzahl α ist, dann ist das Anfangssegment

$$S_{\leq y} = \{z \in x \mid z \leq y\} = S_y \cup \{y\}$$

isomorph zur Ordinalzahl $S(\alpha)$. Wegen Aussonderung bildet

$$\{y \in x \mid \exists \alpha_y \exists f_y (\alpha_y \in \text{On} \wedge (f_y : S_{\leq y} \xrightarrow{\cong} \alpha_y))\}$$

eine Teilmenge u von x . Aus dem Lemma 3.25 folgt, dass α_y und f_y eindeutig bestimmt sind für y aus u . Insbesondere sind $\alpha_y < \alpha_z$ und $f_z \upharpoonright S_{\leq y} = f_y$ für Elemente $y < z$ aus u . Beachte, dass u ein Anfangssegment von x ist.

Die Kollektion von Ordinalzahlen α_y mit y aus u bildet wegen Ersetzung eine Menge I . Setze $\alpha = \sup I$. Die Abbildung $f = \bigcup \{f_y \mid y \in u\}$ ist ein ordnungstreuer Isomorphismus zwischen u und α .

Es genügt zu zeigen, dass $u = x$. Ansonsten gibt es ein kleinstes Element y in $x \setminus u \neq \emptyset$. Wegen der Minimalität von y , ist das Anfangssegment S_y isomorph zu der Ordinalzahl $\beta = \sup\{\alpha_z \mid z < y\}$. Somit ist dann $S_{\leq y}$ isomorph zu der Ordinalzahl $S(\beta)$ im Widerspruch dazu, dass y nicht in u lag. □

3.3 Ordinalarithmetik

Definition 3.31. Die *Summe* zweier Ordinalzahlen α und β ist die einzige Ordinalzahl $\alpha + \beta$ (siehe Satz 3.30), welche zu der wohlgeordneten Summe $\alpha \upharpoonright \beta$ isomorph ist.

Das *Produkt* der Ordinalzahlen α und β ist die einzige Ordinalzahl $\alpha \cdot \beta$, welche zum wohlgeordneten Produkt $\alpha \times \beta$ isomorph ist.

Bemerkung 3.32. Es folgt, dass $\alpha + \underline{0} = \alpha$ und $\alpha \cdot \underline{0} = \underline{0}$, sowie $\alpha + \underline{1} = S(\alpha)$ und $\alpha \cdot \underline{1} = \alpha$. Beachte, dass weder die Summe noch das Produkt kommutativ sind:

$$\begin{aligned} \underline{1} + \omega &= \omega \neq \omega + \underline{1} \\ \underline{2} \cdot \omega &= \omega \neq \omega \cdot \underline{2} \end{aligned}$$

Mit Hilfe des Rekursionssatzes werden wir eine alternative Definition der Summe und des Produktes geben.

Notation. Gegeben Teilklassen X und Y aus \mathbb{V} , welche durch die \mathcal{L}_{ZF} -Formeln φ und ψ definiert werden, schreiben wir $F : X \rightarrow Y$, falls es eine definierbare Funktion von X nach Y gibt (obwohl X oder Y eventuell echte Klassen sind). Das heißt, es gibt eine \mathcal{L}_{ZF} -Formel $\theta[x, y, w_1, \dots, w_n]$ und Mengen z_1, \dots, z_n aus \mathbb{V} derart, dass

$$\mathbb{V} \models \forall x \left(\varphi[x] \rightarrow \exists ! y (\psi[y] \wedge \theta[x, y, z_1, \dots, z_n]) \right).$$

Satz 3.33 (Rekursionssatz). *Für $G : \mathbb{V} \rightarrow \mathbb{V}$ gibt es genau eine Klassenfunktion $F : \text{On} \rightarrow \mathbb{V}$ derart, dass für jede Ordinalzahl α*

$$F(\alpha) = G(F \upharpoonright \alpha),$$

wobei $F \upharpoonright \alpha = \{(\beta, F(\beta)) \mid \beta < \alpha\}$ die Einschränkung von F auf α ist.

Beweis. Es genügt zu zeigen, dass für jede Ordinalzahl α genau eine Abbildung $f_\alpha : \alpha \rightarrow \mathbb{V}$ derart existiert, dass

$$f_\alpha(\beta) = G(f_\alpha \upharpoonright \beta) \quad \forall \beta < \alpha. \quad (\star)$$

Beachte, dass die Eigenschaft (\star) in \mathcal{L}_{ZF} ausdrückbar ist. Definiere nun $F : \text{On} \rightarrow \mathbb{V}$ durch $F(\alpha) = f_{S(\alpha)}(\alpha) = f_\gamma(\alpha)$ für $\alpha < \gamma$ aus On .

Die Eindeutigkeit der Abbildung f_α ist klar: Angenommen es gäbe eine andere Abbildung $f' : \alpha \rightarrow \mathbb{V}$, welche (\star) erfüllt, mit $f' \neq f_\alpha$. Weil α linear geordnet ist, gibt es in α ein kleinstes Element β mit $f'(\beta) \neq f_\alpha(\beta)$. Wegen der Minimalität ist $f' \upharpoonright \beta = f_\alpha \upharpoonright \beta$, aber

$$f'(\beta) = G(f' \upharpoonright \beta) = G(f_\alpha \upharpoonright \beta) = f_\alpha(\beta),$$

was den gewünschten Widerspruch liefert.

Für die Existenz genügt es wegen dem Korollar 3.21 induktiv zu zeigen, dass die Teilklasse χ aller Ordinalzahlen α , für die es genau eine Abbildung f_α mit (\star) gibt, die Bedingung

$$\alpha \subset \chi \implies \alpha \in \chi$$

erfüllt. Klarerweise liegt \emptyset in χ mit $f_\emptyset = \emptyset$. Sei nun $\alpha \neq \emptyset$ in On mit $\alpha \subset \chi$. Falls α Nachfolgerzahl ist, sei $\beta \in \alpha \subset \chi$ mit $\alpha = S(\beta)$. Setze nun

$$f_\alpha = f_\beta \cup \{(\beta, G(f_\beta))\}.$$

Falls α Limeszahl ist, beachte, dass für $\beta < \gamma < \alpha$ die Ordinalzahlen γ und β in χ liegen und somit $f_\gamma \upharpoonright \beta = f_\beta$ wegen der Eindeutigkeit der Bedingung (\star) gilt. Wegen Ersetzung ist $\{f_\beta \mid \beta < \alpha\}$ eine Menge und

$$f_\alpha = \bigcup \{f_\beta \mid \beta < \alpha\}$$

ist eine wohldefinierte Funktion auf α , welche (\star) erfüllt. □

Analog zum vorigen Satz können wir folgendes beweisen:

Korollar 3.34. *Seien $G_{\text{Nachfolger}}$ und G_{Limes} Klassenfunktionen und G_0 eine Menge. Es gibt genau eine Klassenfunktion $F : \text{On} \rightarrow \mathbb{V}$ derart, dass*

- $F(\emptyset) = G_0$.
- $F(\alpha) = G_{\text{Nachfolger}}(F \upharpoonright \alpha)$ für α Nachfolgerzahl.
- $F(\alpha) = G_{\text{Limes}}(\{F(\beta)\}_{\beta < \alpha})$ für α Limeszahl.

Definition 3.35. Gegeben eine Ordinalzahl α , definiere die Funktion

$$\begin{aligned} F : \text{On} &\rightarrow \mathbb{V} \\ \beta &\mapsto \alpha + \beta \end{aligned}$$

induktiv bezüglich der Menge $G_0 = \alpha$ und der Klassenfunktionen

$$G_{\text{Nachfolger}}(x) = \begin{cases} S(x(\beta)), & \text{falls } x \text{ eine Abbildung mit Definitionsbereich } \text{Dom}(x) = S(\beta) \in \text{On} \text{ ist,} \\ x, & \text{sonst.} \end{cases}$$

und $G_{Limes}(x) = \bigcup x$, das heißt:

$$\alpha + \beta = \begin{cases} \alpha, & \text{für } \beta = \underline{0} \\ S(\alpha + \gamma), & \text{für } \beta = S(\gamma) \\ \sup_{\gamma < \beta}(\alpha + \gamma), & \text{für } \beta \text{ Limeszahl} \end{cases}$$

Beachte, dass die Funktionen $\beta \mapsto \alpha + \beta$ durch den Rekursionssatz uniform in α definiert wurden. Das heißt, es gibt eine Formel $\varphi[x, y, z]$ derart, dass für alle Ordinalzahlen α und β die Summe $\alpha + \beta$ die einzige Ordinalzahl ist, welche die Formel $\varphi[x, \alpha, \beta]$ erfüllt. Insbesondere ist $\gamma \mapsto \gamma + \alpha$ auch eine Klassenfunktion.

Für festes α in On, definiere analog $\alpha \cdot \beta$ induktiv bezüglich der Menge $G_0 = \underline{0}$ und der Klassenfunktionen

$$G_{Nachfolger}(x) = \begin{cases} x(\beta) + \alpha, & \text{falls } x \text{ eine Abbildung mit } \text{Dom}(x) = S(\beta) \in \text{On} \text{ und } x(\beta) \text{ in On ist,} \\ x, & \text{sonst.} \end{cases}$$

und $G_{Limes}(x) = \bigcup x$, das heißt:

$$\alpha \cdot \beta = \begin{cases} \underline{0}, & \text{für } \beta = \underline{0} \\ \alpha \cdot \gamma + \alpha, & \text{für } \beta = S(\gamma) \\ \sup_{\gamma < \beta}(\alpha \cdot \gamma), & \text{für } \beta \text{ Limeszahl} \end{cases}$$

Insbesondere sind $\alpha + \beta$ und $\alpha \cdot \beta$ Ordinalzahlen für jedes β aus On.

Induktiv über β ist leicht zu zeigen, dass die obigen Definitionen zu den Definitionen 3.31 äquivalent sind.

Korollar 3.36. *Beide Definition der Summe und des Produktes stimmen überein.*

Korollar 3.37.

- $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
- Wenn $\alpha \leq \beta$, gibt es ein γ mit $\alpha + \gamma = \beta$.
- Wenn $\beta < \gamma$, ist $\alpha + \beta < \alpha + \gamma$. Insbesondere, wenn $\alpha + \beta = \alpha + \gamma$, dann ist $\beta = \gamma$.
- $\underline{1} + \alpha = \alpha$ für alle $\alpha \geq \omega$.
- $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$.
- $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$.
- Falls $\alpha \neq \underline{0}$ und $\beta < \gamma$, dann ist $\alpha \cdot \beta < \alpha \cdot \gamma$. Aus $\alpha \cdot \beta = \alpha \cdot \gamma$ folgt, dass $\alpha = \underline{0}$ oder $\beta = \gamma$.

Proposition 3.38 (Ordinalzahlendivision mit Rest). *Für alle α und β aus On mit $\alpha \neq \underline{0}$ gibt es eindeutig bestimmte γ und δ aus On mit $\beta = \alpha \cdot \gamma + \delta$ und $\delta < \alpha$.*

Beweis. Die Eindeutigkeit läßt sich einfach zeigen: Angenommen $\beta = \alpha \cdot \gamma + \delta = \alpha \cdot \gamma_1 + \delta_1$ mit $\delta_1 < \alpha$. Dann ist $\alpha \cdot \gamma \leq \beta < \alpha \cdot \gamma_1 + \alpha = \alpha \cdot S(\gamma_1)$ und aus dem obigen Korollar folgt $\gamma \leq \gamma_1$, weil $\alpha \neq \underline{0}$. Symmetrisch zeigen wir $\gamma_1 \leq \gamma$ und somit gilt $\gamma = \gamma_1$. Die Gleichung $\alpha \cdot \gamma + \delta = \alpha \cdot \gamma_1 + \delta_1 = \alpha \cdot \gamma + \delta_1$ liefert wie gewünscht $\delta = \delta_1$.

Die Existenz zeigen wir folgendeweise: für $\beta < \alpha$ setze $\gamma = \underline{0}$ und $\delta = \beta$. Für $\beta = \alpha$ setze $\gamma = \underline{1}$ und $\delta = \underline{0}$. Sei nun $\beta > \alpha > \underline{0}$. Die Abbildung

$$\begin{aligned} f : \beta &\rightarrow \alpha \overset{\times}{\times} \beta \\ \mu &\mapsto (\underline{0}, \mu) \end{aligned}$$

ist streng monoton wachsend. Aus dem Lemma 3.25 folgt, dass $\beta \leq \alpha \cdot \beta$. Falls $\beta = \alpha \cdot \beta$, setze $\gamma = \beta$ und $\delta = \underline{0}$. Wir nehmen also nun $\beta < \alpha \cdot \beta$ an.

Mit Hilfe von Lemma 3.20 (e) wähle $\gamma_1 \leq \beta$ in On kleinstmöglich mit $\alpha \cdot \gamma_1 > \beta$. Klarerweise ist $\gamma_1 \neq \underline{0}$.

Die Ordinalzahl γ_1 kann keine Limeszahl sein, denn sonst wäre

$$\alpha \cdot \gamma_1 = \sup_{\mu < \gamma_1} \alpha \cdot \mu \leq \beta$$

wegen der Minimalität von γ_1 . Wähle nun γ in On mit $\gamma_1 = S(\gamma)$. Die Minimalität liefert, dass $\alpha \cdot \gamma \leq \beta$. Aus dem obigen Korollar folgt, dass es ein δ in On gibt mit

$$\beta = \alpha \cdot \gamma + \delta$$

Wir müssen nur zeigen, dass $\delta < \alpha$. Sonst gäbe es ein λ in On mit $\delta = \alpha + \lambda$ und

$$\beta = \alpha \cdot \gamma + \delta = \alpha \cdot \gamma + \alpha + \lambda \geq \alpha \cdot (\gamma + \underline{1}) = \alpha \cdot \gamma_1 > \beta,$$

was den gewünschten Widerspruch liefert. □

3.4 Auswahlaxiom und Kardinalität

Das Auswahlaxiom besagt, dass jede Kollektion nicht-leerer Mengen eine Auswahlfunktion besitzt, das heißt, eine Funktion, welche ein Element aus jeder der Mengen wählt.

Auswahl

$$\forall x \left(\emptyset \notin x \rightarrow \exists f \left((f : x \rightarrow \mathbb{V}) \wedge \forall y (y \in x \rightarrow f(y) \in y) \right) \right)$$

In diesem Abschnitt arbeiten wir in der Theorie ZFC, welche aus ZF zusammen mit dem Auswahlaxiom besteht.

Definition 3.39. Eine *Folge* der Länge α ist eine Funktion f , deren Definitionsbereich eine Ordinalzahl α ist. Wir bezeichnen die Folge mit $(f(\beta))_{\beta < \alpha}$. Wenn die Länge ω ist, sagen wir nur, dass es eine Folge ist.

Eine *endliche Folge* (der Länge n) ist eine Folge, deren Länge die natürliche Zahl \underline{n} ist.

Korollar 3.40 (Abhängiges Auswahlaxiom). *Sei R eine Relation auf einer nicht-leeren Menge S derart, dass es für jedes x aus S ein y aus S mit yRx gibt. Die Relation R besitzt eine unendliche Kette, das heißt, es gibt eine Folge $(x_\gamma)_{\gamma \in \omega}$ aus S mit $x_{\gamma+1}Rx_\gamma$.*

Beweis. Für x aus S , sei R_x die Menge $\{y \in S \mid yRx\}$. Aus der Hypothese folgt $R_x \neq \emptyset$. Wegen Ersetzung ist $u = \{R_x \mid x \in S\}$ eine Menge, welche nicht \emptyset enthält. Auswahl liefert eine Funktion $f : S \rightarrow \mathbb{V}$ derart, dass $f(x)Rx$ für jedes x aus S .

Weil $S \neq \emptyset$, gibt es ein z in S . Definiere nun $x_0 = z$ und $x_{\gamma+1} = f(x_\gamma)$ für $0 < \gamma < \omega$. \square

Definition 3.41. Eine Relation R auf einer Menge S ist *fundiert*, wenn jede nicht-leere Teilmenge von S ein minimales Element bezüglich R besitzt.

Wir können nun die naive Interpretation des Fundierungsaxiomes genau formulieren.

Korollar 3.42. Sei R eine Relation auf der Menge S . Die Relation ist genau dann fundiert, wenn R keine Ketten der Länge ω besitzt.

Beweis. Wenn es eine unendliche Kette $(x_\gamma)_{\gamma \in \omega}$ gibt, hat die Teilmenge $\{x_\gamma \mid \gamma \in \omega\}$ aus S klarerweise kein minimales Element bezüglich R . Für die Rückrichtung sei $u \subset S$ eine nicht-leere Teilmenge ohne R -minimales Element. Für jedes x aus u gibt es ein y aus u mit yRx . Aus dem abhängigen Auswahlaxiom folgt, dass R eine Kette der Länge ω in u (und somit in S) besitzt. \square

Definition 3.43. Zwei Mengen x und y sind *gleichmächtig*, bezeichnet mit $x \sim y$, falls es eine Bijektion zwischen x und y gibt.

Wir schreiben $x \preceq y$, falls es eine injektive Abbildung $f : x \rightarrow y$ gibt.

Bemerkung 3.44. Gleichmächtigkeit ist eine Äquivalenzrelation zwischen Mengen.

Satz 3.45 (Cantor-Bernstein-Schröder-Äquivalenzsatz). Zwei Mengen x und y sind genau dann gleichmächtig, wenn $x \preceq y$ und $y \preceq x$.

Beweis. Eine Richtung ist trivial. Jetzt konstruieren wir aus den beiden injektiven Abbildungen $f : x \rightarrow y$ und $g : y \rightarrow x$ eine Bijektion $h : x \rightarrow y$. Da x in Bijektion mit $f(x) \subset y$ ist, können wir wegen der Bemerkung 3.44 annehmen, dass $x \subset y$ (mit f die Identität auf x). Setze g^0 die Identität auf y und $g^{\gamma+1} = g \circ g^\gamma$ für γ aus ω . Beachte, dass $\text{Im}(g^\gamma) \subset x$ für $\gamma > 0$. Da $y \setminus x$ eine Menge ist, bildet

$$u = \{g^\gamma(z) \mid (z \in (y \setminus x) \wedge \gamma \in \omega)\}$$

eine Menge wegen Ersetzung und Aussonderung. Insbesondere ist $u = (y \setminus x) \cup g(u)$ und $g(u) \cap (y \setminus x) \subset g(y) \cap (y \setminus x) = \emptyset$.

Die Menge $x \setminus u$ ist eine Teilmenge von $y \setminus u$, da $x \subset y$. Aber $y \setminus u \subset x$, also $x \setminus u = y \setminus u$. Insbesondere ist die Abbildung

$$h : y \rightarrow x$$

$$z \mapsto \begin{cases} g(z), & \text{falls } z \in u \\ z, & \text{sonst.} \end{cases}$$

surjektiv. Um zu zeigen, dass h injektiv ist, genügt es zu zeigen, dass $h(u) \cap (y \setminus u) = \emptyset$. Da $h(u) = g(u) \subset u$, sind diese Mengen disjunkt, wie gewünscht. \square

Aus dem Satz A.5 im Appendix A folgt, dass jede Menge gleichmächtig mit einer Ordinalzahl ist.

Korollar 3.46. Jede Menge ist in Bijektion mit einer Ordinalzahl.

Definition 3.47. Die *Mächtigkeit* oder *Kardinalität* einer Menge x ist die kleinste Ordinalzahl $|x|$, welche mit x gleichmächtig ist.

Klarerweise ist $|\alpha| \leq \alpha$, für α aus On. Beachte, dass Gleichheit nicht unbedingt gelten muss: z. B. $\omega + 1 \sim \omega$.

Definition 3.48. Eine Ordinalzahl α ist eine *Kardinalzahl*, falls $|\alpha| = \alpha$, oder äquivalent dazu, wenn es keine Injektion $f : \alpha \rightarrow \beta$ mit $\beta < \alpha$ gibt aus dem Satz 3.45.

Bemerkung 3.49.

- Die Kardinalität einer Menge ist eine Kardinalzahl.
- Jede natürliche Zahl ist eine Kardinalzahl.
- ω ist eine Kardinalzahl.

Beweis. Wenn die natürliche Zahl α keine Kardinalzahl wäre, gäbe es $\beta < \alpha$ derart, dass α sich in β bijektiv einbetten lässt. Insbesondere lässt sich $S(\beta) \leq \alpha$ auch in β injektiv einbetten.

Es genügt also zu zeigen, dass die Teilkollektion aller natürlichen Zahlen α , für welche es keine Injektion $f : S(\alpha) \rightarrow \alpha$ gibt, gleich ω ist. Beachte, dass diese Kollektion natürlicher Zahlen wegen Aussonderung eine Teilmenge x von ω bildet. Mit Hilfe des Induktionsprinzips 3.16 müssen wir nur zeigen, dass x die natürliche Zahl $\underline{0}$ enthält und unter Nachfolger abgeschlossen ist. Klarerweise gibt es keine Injektion von $\underline{1} = \{\emptyset\}$ in die leere Menge. Angenommen nun, dass α in x liegt aber es eine Injektion $f : \alpha + 2 \rightarrow \alpha + 1$ gibt. Wenn α nicht im Bildbereich der Einschränkung $f \upharpoonright \alpha + 1$ liegt, induziert die Einschränkung von f eine Injektion $f \upharpoonright \alpha + 1 : (\alpha + 1) \rightarrow \alpha$, welcher einen Widerspruch liefert, denn α liegt in x .

Sonst besitzt α ein Urbild in $\alpha + 1$, so $\alpha = f(\beta)$ mit $\beta \leq \alpha$. Beachte, dass $f(\alpha + 1) = \delta$ ein Element aus α sein muss, weil die ursprüngliche Abbildung f injektiv ist.

Nun ist die Abbildung

$$g : \alpha + 1 \rightarrow \alpha$$

$$\gamma \mapsto \begin{cases} f(\gamma), & \text{falls } \gamma \neq \beta \\ \delta = f(\alpha + 1), & \text{sonst.} \end{cases}$$

eine Injektion, was den gewünschten Widerspruch liefert.

Falls die Ordinalzahl ω keine Kardinalzahl wäre, gäbe es eine injektive Abbildung von ω in eine natürliche Zahl α . Die Zahl $S(\alpha)$ lässt sich in ω injektiv einbetten und somit gäbe es eine Injektion $S(\alpha) \rightarrow \alpha$, was dem obigen Paragraph widerspricht. \square

Korollar 3.50. Gegeben eine Surjektion $h : x \rightarrow y$, ist $|y| \leq |x|$.

Beweis. Sei $<$ eine Wohlordnung auf x , wegen des Satzes A.5 (oder äquivalent dazu, wähle eine bijektive Abbildungen $f : \alpha \rightarrow x$, für eine Ordinalzahl α). Es genügt zu zeigen, dass $y \preceq x$. Gegeben z aus y , gibt es ein u in x mit $h(u) = z$. Setze nun

$$g : y \rightarrow x$$

$$z \mapsto u \text{ kleinstmöglich bezüglich } < \text{ mit } h(u) = z.$$

Die obige Funktion g ist klarerweise wohldefinierte und injektiv. \square

Notation. Wenn wir ω als Kardinalzahl betrachten, schreiben wir stattdessen \aleph_0 .

Definition 3.51. Eine Menge ist *endlich*, falls ihre Mächtigkeit eine natürliche Zahl ist.
Eine Menge x ist *abzählbar*, falls $|x| \leq \omega$.

Aus dem Korollar 3.6 folgt, dass es keine größte Kardinalzahl gibt.

Definition 3.52. Gegeben eine Kardinalzahl κ , sei κ^+ die kleinste Kardinalzahl, welche echt größer als κ ist.

Die *Kontinuumshypothese* besagt, dass $\aleph_1^+ = |\mathcal{P}(\omega)|$. Die (*allgemeine*) *Kontinuumshypothese* besagt, dass $\kappa^+ = |\mathcal{P}(\kappa)|$.

Kapitel 4

Unentscheidbarkeit

Es gibt mehrere mathematische Modelle, welche die Idee eines Algorithmus formalisieren: Gödel führte *rekursive Funktionen* für seinen Beweis der Unvollständigkeit ein (Satz 4.47), wobei Turing und Church Maschinen bzw. das λ -Kalkül einführten. Diese drei Begriffe der Berechenbarkeit sind äquivalent und somit wurde die Church'sche These eingeführt, welche besagt, dass *alle* Begriffe der Berechenbarkeit äquivalent sein sollen. Selbstverständlich ist diese These nicht beweisbar ohne den Begriff des Algorithmus einführen zu müssen. Der Unvollständigkeitssatz besagt, dass es keinen Algorithmus gibt, der im Voraus entscheiden kann, ob eine Aussage erster Stufe beweisbar ist oder nicht. Konkrete Sätze, die unabhängig vom Axiomensystem sind, sind unter anderem die Kontinuumshypothese (bezüglich des Axiomensystems ZFC der Mengenlehre) oder die Aussage, dass Goodstein'sche Folgen immer aufhören (in jedem Modell der Peanoarithmetik).

4.1 Rekursivität

In diesem gesamten Abschnitt verstehen wir unter *Funktion* eine Abbildung von einem (beliebigen) kartesischen Produkt von \mathbb{N} nach \mathbb{N} .

Definition 4.1. Die Kollektion der *primitiv rekursiven Funktionen* ist die kleinste Menge PREK von Funktionen, welche die *Grundfunktionen*:

Nachfolger $S : \mathbb{N} \rightarrow \mathbb{N}$;
 $x \mapsto x + 1$

Projektion $\pi_i^n : \mathbb{N}^n \rightarrow \mathbb{N}$ und
 $(x_1, \dots, x_n) \mapsto x_i$

Konstanten-
funktion

Null (sogar $0 : \mathbb{N}^n \rightarrow \mathbb{N}$
nullstellig) $(x_1, \dots, x_n) \mapsto 0$

enthält und unter folgenden Operationen abgeschlossen ist:

Komposition Für jede m -stellige Funktion h in PREK und n -stellige Funktionen g_1, \dots, g_m in PREK ist die folgende Funktion in PREK

$$f : \mathbb{N}^n \rightarrow \mathbb{N}$$
$$(x_1, \dots, x_n) \mapsto h(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n))$$

Primitive Rekursion Für jede n -stellige Funktion g und $(n + 2)$ -stellige Funktion h in PREK ist

$$f : \mathbb{N}^{n+1} \rightarrow \mathbb{N}$$

$$(x_1, \dots, x_n, y) \mapsto \begin{cases} g(x_1, \dots, x_n), & \text{für } y = 0 \\ h(x_1, \dots, x_n, z, f(x_1, \dots, x_n, z)), & \text{für } y = z + 1 \end{cases}$$

in PREK.

Beispiel 4.2. Diese Funktionen sind in PREK:

- $+$: $\mathbb{N}^2 \rightarrow \mathbb{N}$
 $(x, y) \mapsto x + y$

- $x \div 1$: $\mathbb{N} \rightarrow \mathbb{N}$
 $x \mapsto \begin{cases} 0, & \text{falls } x = 0 \\ z, & \text{falls } x = z + 1 \end{cases}$

- $x \div y$: $\mathbb{N}^2 \rightarrow \mathbb{N}$
 $(x, y) \mapsto \begin{cases} x, & \text{falls } y = 0 \\ (x \div z) \div 1, & \text{falls } y = z + 1 \end{cases}$

**Beschränkte
Differenz**

- $x \cdot y$: $\mathbb{N}^2 \rightarrow \mathbb{N}$
 $(x, y) \mapsto \begin{cases} 0, & \text{falls } y = 0 \\ x \cdot z + x, & \text{falls } y = z + 1 \end{cases}$

- $!$: $\mathbb{N} \rightarrow \mathbb{N}$
 $x \mapsto \begin{cases} 1 = S(0), & \text{falls } x = 0 \\ x \cdot z!, & \text{falls } x = z + 1 \end{cases}$

Definition 4.3. Die Kollektion der *rekursiven Funktionen* ist die kleinste Menge REK von Funktionen, welche alle Projektionen, die Nachfolger- und die Null-Konstantenfunktion enthält und unter Komposition und primitiver Rekursion sowie der folgenden Operation abgeschlossen ist:

μ -Rekursion Falls für die rekursive Funktion $g : \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ gilt, dass für alle x_1, \dots, x_n ein y aus \mathbb{N} mit $g(x_1, \dots, x_n, y) = 0$ existiert, dann ist die Funktion

$$\mu_y g(x_1, \dots, x_n, y) = 0 : \mathbb{N}^n \rightarrow \mathbb{N}$$

$$(x_1, \dots, x_n) \mapsto \text{kleinstes } z \text{ mit } g(x_1, \dots, x_n, z) = 0$$

auch rekursiv.

Definition 4.4. Eine Teilmenge $A \subset \mathbb{N}^k$ ist (*primitiv*) *rekursiv*, falls ihre charakteristische Funktion

$$\chi_A : \mathbb{N}^k \rightarrow \mathbb{N}$$

$$(x_1, \dots, x_k) \mapsto \begin{cases} 1, & \text{falls } (x_1, \dots, x_k) \in A \\ 0, & \text{sonst.} \end{cases}$$

(primitiv) rekursiv ist.

Beispiel 4.5. Die Relation $<$ ist primitiv rekursiv, das heißt, die Teilmenge $\{(x, y) \in \mathbb{N}^2 \mid x < y\}$ ist primitiv rekursiv, weil

$$\chi_{<}(x, y) = 1 \iff y \dot{-} x \neq 0.$$

Man sieht leicht, dass die einstellige Relation $z \neq 0$ primitiv rekursiv ist.

Lemma 4.6. Falls A und B (primitiv) rekursive Teilmengen von \mathbb{N}^k sind, dann sind

- $A \cup B$;
- $A \cap B$;
- $A \setminus B$;
- $\{(x_1, \dots, x_n) \in \mathbb{N}^n \mid (f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n)) \in A\}$, für alle (primitiv) rekursive Funktionen f_1, \dots, f_k ;

auch (primitiv) rekursiv.

Lemma 4.7. Gegeben (primitiv) rekursive Teilmengen A_1, \dots, A_n von \mathbb{N}^k und k -stellige (primitiv) rekursive Funktionen f_1, \dots, f_{n+1} , ist die Fallunterscheidungsfunktion

$$f : \quad \mathbb{N}^k \quad \rightarrow \quad \mathbb{N}$$

$$(x_1, \dots, x_k) \mapsto \begin{cases} f_1(x_1, \dots, x_k), & \text{falls } (x_1, \dots, x_k) \in A_1 \\ f_2(x_1, \dots, x_k), & \text{falls } (x_1, \dots, x_k) \in A_2 \setminus A_1 \\ \vdots \\ f_n(x_1, \dots, x_k), & \text{falls } (x_1, \dots, x_k) \in A_n \setminus \left(\bigcup_{1 \leq j < n} A_j \right) \\ f_{n+1}(x_1, \dots, x_k), & \text{falls } (x_1, \dots, x_k) \notin \bigcup_{1 \leq j \leq n} A_j \end{cases}$$

auch (primitiv) rekursiv.

Beweis. Aus dem Lemma 4.6 folgt, dass für jedes $i \leq n$ die Teilmenge $B_i = A_i \setminus \left(\bigcup_{1 \leq j < i} A_j \right)$ (primitiv) rekursiv ist. Damit ist auch $B_{n+1} = \mathbb{N}^k \setminus \left(\bigcup_{1 \leq j \leq n} A_j \right)$ (primitiv) rekursiv. Beachte, dass die B_i 's paarweise disjunkt sind und dass

$$f(x_1, \dots, x_k) = f_1(x_1, \dots, x_k)\chi_{B_1}(x_1, \dots, x_k) + \dots + f_{n+1}(x_1, \dots, x_k)\chi_{B_{n+1}}(x_1, \dots, x_k).$$

□

Korollar 4.8. Sind $A \subset B \subset \mathbb{N}^k$ Teilmengen derart, dass $B \setminus A$ endlich und A (primitiv) rekursiv ist, so ist B (primitiv) rekursiv.

Lemma 4.9. Wenn $A \subset \mathbb{N}^{k+1}$ eine (primitiv) rekursive Teilmenge ist, dann sind

- $B = \{(x_1, \dots, x_k, y) \in \mathbb{N}^{k+1} \mid \forall z < y \left((x_1, \dots, x_k, z) \in A \right)\}$

- $C = \{(x_1, \dots, x_k, y) \in \mathbb{N}^{k+1} \mid \exists z < y \left((x_1, \dots, x_k, z) \in A \right)\}$

auch (primitiv) rekursiv.

Beweis. Man sieht leicht, dass

$$\chi_B(x_1, \dots, x_k, y) = \begin{cases} 1, & \text{falls } y = 0 \\ \chi_B(x_1, \dots, x_k, z) \cdot \chi_A(x_1, \dots, x_k, z), & \text{falls } y = z + 1 \end{cases}.$$

Aus Lemma 4.6 und der obigen Überlegung folgt, dass C auch (primitiv) rekursiv ist, weil

$$(x_1, \dots, x_k, y) \in C \iff \neg \forall z < y \left((x_1, \dots, x_k, z) \in \mathbb{N}^k \setminus A \right).$$

□

Lemma 4.10. Seien $A \subset \mathbb{N}^{k+1}$ und $f : \mathbb{N}^k \rightarrow \mathbb{N}$ primitiv rekursiv derart, dass es für jedes (x_1, \dots, x_k) aus \mathbb{N}^k ein y aus \mathbb{N} mit $y \leq f(x_1, \dots, x_k)$ und $(x_1, \dots, x_k, y) \in A$ gibt. Die Funktion $g(x_1, \dots, x_k) = \mu y (x_1, \dots, x_k, y) \in A$ ist primitiv rekursiv.

Wir wissen, dass die Funktion g rekursiv ist, weil sie mit Hilfe der μ -Rekursion aus χ_A gewonnen wird. Da ein mögliches y im Voraus mit Hilfe der Funktion f abgeschätzt werden kann, ist die μ -Rekursion nicht nötig.

Beweis. Definiere $h(x_1, \dots, x_k, y) = \mu z \left((x_1, \dots, x_k, z) \in A \vee z = y \right)$. Weil

$$h(x_1, \dots, x_k, y) = \begin{cases} 0, & \text{falls } y = 0 \\ h(x_1, \dots, x_k, u), & \text{falls } y = u + 1 \text{ und } (x_1, \dots, x_k, h(x_1, \dots, x_k, u)) \in A \\ y, & \text{sonst} \end{cases}$$

ist die Funktion h primitiv rekursiv, denn wie im Beweis vom Lemma 4.7 ist

$$h(x_1, \dots, x_k, u + 1) = h(x_1, \dots, x_k, u) \cdot \chi_A(x_1, \dots, x_k, h(x_1, \dots, x_k, u)) + S(u) \cdot (1 \div \chi_A(x_1, \dots, x_k, h(x_1, \dots, x_k, u))).$$

Beachte, dass $g(x_1, \dots, x_k) = h(x_1, \dots, x_k, S(f(x_1, \dots, x_k)))$ weil es immer ein $y \leq f(x_1, \dots, x_k)$ mit $(x_1, \dots, x_k, y) \in A$ gibt. Insbesondere ist g primitiv rekursiv. □

Lemma 4.11. Folgende Funktionen und Teilmengen sind primitiv rekursiv:

- Das zweistellige Prädikat teilen:

$$x \mid y \iff y = x \cdot z, \text{ für ein } z \in \mathbb{N}.$$

- $\text{PRIM} = \{x \in \mathbb{N} \mid x \text{ Primzahl}\}$ und $p : \mathbb{N} \rightarrow \mathbb{N}$
 $n \mapsto (n + 1)\text{-te Primzahl}$

Beweis. Sei $\text{Rest}(x, y)$ die Funktion, welche den Rest der Division von y durch x gibt, falls es Sinn macht (und Null sonst!). Beachte, dass

$$\text{Rest} : \mathbb{N}^2 \rightarrow \mathbb{N}$$

$$(x, y) \mapsto \begin{cases} 0, & \text{falls } y = 0 \\ \left\{ \begin{array}{l} \text{Rest}(x, z) + 1 \text{ falls } \text{Rest}(x, z) + 1 < x \\ 0, \text{ sonst} \end{array} \right\}, & \text{falls } y = z + 1 \end{cases}$$

Nun gilt $x \mid y$ genau dann, wenn $y = 0$ oder $\text{Rest}(x, y) = 0$ und sowohl x und y beide verschieden von 0.

Ein Element x gehört genau dann zu PRIM , falls $1 < x$ und

$$\forall z < x (z = 1 \vee z \nmid x).$$

Wegen Lemma 4.9 ist PRIM primitiv rekursiv. Induktiv zeigt man, dass die $(n+1)$ -te Primzahl $p(n)$ durch 2^{2^n} beschränkt ist, weil $p(n) \leq 1 + \prod_{k < n} p(k)$. Aus dem Lemma 4.10 folgt, dass

$$p : \mathbb{N} \rightarrow \mathbb{N}$$

$$x \mapsto \begin{cases} 2 = S(S(0)), & \text{falls } x = 0 \\ \mu w (w \in \text{PRIM} \wedge p(z) < w), & \text{falls } x = z + 1 \end{cases}$$

primitiv rekursiv ist. □

Im Folgenden werden wir eine andere Präsentation der rekursiven Funktionen geben.

Lemma 4.12. *Sei \mathcal{F} die Teilkollektion der rekursiven Funktionen, welche die Konstanten-, Nachfolger- und Koordinatenfunktionen sowie $+$, \cdot und $\chi_{<}$ enthält und unter Komposition und μ -Rekursion abgeschlossen ist. Folgende Funktionen sind in \mathcal{F} :*

- $x \dot{-} y$;
- $\chi_{A \cap B}$, $\chi_{A \cup B}$ und $\chi_{\mathbb{N}^k \setminus A}$, falls χ_A und χ_B in \mathcal{F} liegen;
- χ_R , wobei (x, y) in $R \subset \mathbb{N}^2$ genau dann liegt, falls $\exists z < y ((x, z) \in A)$ mit χ_A in \mathcal{F} ;
- $\chi_{=}$;
- χ_{mod} , wobei $\text{mod} = \{(x, y, z) \in \mathbb{N}^3 \mid x \equiv y \pmod{z}\}$;
- *Definition aus Fallunterscheidung (siehe Lemma 4.7), wenn alle Funktionen und Teilmengen in \mathcal{F} liegen.*

Beweis. Beachte, dass $x \dot{-} y = \mu z (x < y + z + 1)$. Der zweite Teil der Behauptung ist trivial. Sei $A \subset \mathbb{N}^2$ mit χ_A in \mathcal{F} . Wir definieren $g(x, y) = \mu z (z = y \vee (x, z) \in A)$. Nun liegt (x, y) genau dann in $R = \exists z < y ((x, z) \in A)$, wenn $g(x, y) < y$. Weil g in \mathcal{F} liegt, ist somit auch χ_R in \mathcal{F} .

Aus der Ordnung $<$ kann man leicht Gleichheit definieren. Falls x und y äquivalent modulo z sind, gibt es ein Element w aus \mathbb{N} mit $|x - y| = z \cdot w$. Für $z = 0$ sind x und y genau dann äquivalent, wenn $\chi_{=}(x, y) = 1$. Ansonsten bedeutet dies, dass $w \leq |x - y| \leq x + y < x + y + 1$. Insbesondere ist

$$\chi_{\text{mod}}(x, y, z) = 1 \iff \left((z = 0 \wedge \chi_{=}(x, y) = 1) \vee \exists w < x + y + 1 (x = y + z \cdot w \vee y = x + z \cdot w) \right),$$

und somit liegt χ_{mod} auch in \mathcal{F} . Letztlich ist eine Definition aus Fallunterscheidung klarerweise in \mathcal{F} , weil \mathcal{F} unter Produkten, Summen und charakteristischen Funktionen von booleschen Kombinationen aus (charakteristischen Funktionen von) Mengen aus \mathcal{F} abgeschlossen ist. \square

Lemma 4.13. *Es existiert eine Funktion $\beta : \mathbb{N}^3 \rightarrow \mathbb{N}$ in \mathcal{F} derart, dass es für jedes n aus \mathbb{N} und c_0, \dots, c_{n-1} aus \mathbb{N} natürliche Zahlen a und b mit $\beta(a, b, i) = c_i$ für $0 \leq i \leq n - 1$ gibt.*

Beweis. Sei b ein Element aus \mathbb{N} , welches durch jede natürliche Zahl zwischen 2 und n teilbar ist und $c_i < b$ für alle $i < n$ erfüllt. Zum Beispiel $b = (\max(c_1, \dots, c_{n-1}) + 1)!$.

Wir zeigen zuerst, dass die Zahlen $1 + b, 1 + 2b, \dots, 1 + nb$ paarweise teilerfremd sind: Falls $i < j$ und die Primzahl p sowohl $1 + ib$ als auch $1 + jb$ teilt, dann teilt p auch die Differenz $(j - i)b$. Aber p kann b nicht teilen, weil p sonst $1 = (1 + ib) - ib$ teilen müsste. Daher teilt p die Zahl $j - i < n$. Weil b von $j - i$ teilbar ist, teilt p die Zahl b , was den gewünschten Widerspruch liefert.

Wegen dem Chinesischen Restsatz D.1, gibt es eine Lösung a in \mathbb{N} (sogar mit $a \leq \prod_{i=1}^n 1 + ib$) für das Kongruenzsystem

$$\left. \begin{array}{l} x \equiv c_0 \pmod{1 + b} \\ \vdots \\ x \equiv c_{n-1} \pmod{1 + nb} \end{array} \right\}$$

Weil $c_i < b < 1 + (i + 1)b$ für $i < n$, ist c_i die kleinste natürliche Zahl, welche zu a kongruent modulo $1 + (i + 1)b$ ist. Die Funktion

$$\beta(x, y, z) = \mu w \left(w \equiv x \pmod{1 + (z + 1)y} \right)$$

liegt in \mathcal{F} wegen Lemma 4.12 und erfüllt, dass $\beta(a, b, i) = c_i$ für $0 \leq i < n$. \square

Satz 4.14. $\mathcal{F} = \text{REK}$.

Beweis. Wir müssen nur zeigen, dass die Teilklasse \mathcal{F} rekursiver Funktionen unter primitiver Rekursion abgeschlossen ist. Seien hierfür g und h aus \mathcal{F} . Betrachte also die Funktion

$$f : \mathbb{N}^{n+1} \rightarrow \mathbb{N} \\ (x_1, \dots, x_n, y) \mapsto \begin{cases} g(x_1, \dots, x_n), & \text{für } y = 0 \\ h(g(x_1, \dots, x_n), z, f(x_1, \dots, x_n, z)), & \text{für } y = z + 1 \end{cases},$$

wobei g und h beide in der Teilklasse \mathcal{F} liegen. Für $\bar{x} = (x_1, \dots, x_n)$ setze $c_0 = g(\bar{x})$ und $c_{i+1} = h(\bar{x}, i, f(\bar{x}, i))$ für $i < k \in \mathbb{N}$. Wegen Lemma 4.13 gibt es für jedes k aus \mathbb{N} natürliche Zahlen a und b mit $\beta(a, b, i) = c_i$. Dies bedeutet, dass

$$\forall 0 \leq i < k \left(\beta(a, b, i + 1) = c_i = h(\bar{x}, i, \beta(a, b, i)) \right).$$

Der Beweis des Lemmas 4.12 zeigt, dass die charakteristische Funktion der Teilmenge $R \subset \mathbb{N}^{n+3}$ mit

$$(\bar{x}, y, a, b) \in R \iff \left((\beta(a, b, 0) = g(\bar{x})) \wedge \forall z < y (\beta(a, b, z + 1) = h(\bar{x}, z, \beta(a, b, z))) \right)$$

in \mathcal{F} ist. Für gegebene \bar{x} und y gibt es nach Konstruktion a und b (und somit ein $s = \max(a, b)$) mit $(\bar{x}, y, a, b) \in R$. Daher ist $H(\bar{x}, y) = \mu s (\exists a \exists b ((a \leq s) \wedge (b \leq s) \wedge (\bar{x}, y, a, b) \in R))$ auch in \mathcal{F} . Es genügt induktiv auf y zu zeigen, dass

$$f(\bar{x}, y) = \mu z (\exists a \exists b ((a \leq H(\bar{x}, y)) \wedge (b \leq H(\bar{x}, y)) \wedge (\bar{x}, y, a, b) \in R) \wedge (z = \beta(a, b, y))),$$

denn die Funktion $\tilde{f}(\bar{x}, y)$ auf der rechten Seite liegt klarerweise in \mathcal{F} . Der Wert $\tilde{f}(\bar{x}, 0)$ ist der kleinste Wert $\beta(a, b, 0)$ derart, dass $(\bar{x}, 0, a, b)$ in R liegt. Aber $\beta(a, b, 0) = g(\bar{x}) = f(\bar{x}, 0)$. Für $y = z + 1$ ist $\tilde{f}(\bar{x}, z + 1)$ der kleinste Wert $\beta(a, b, z + 1)$ sodass $(\bar{x}, z + 1, a, b)$ in R liegt. Also $\tilde{f}(\bar{x}, z + 1) = \beta(a, b, z + 1) = h(\bar{x}, z, \beta(a, b, z))$. Für $z < y + 1$ liegt (\bar{x}, z, a, b) auch in R , also $f(\bar{x}, z) = \tilde{f}(\bar{x}, z) = \beta(a, b, z)$ und somit ist $\tilde{f}(\bar{x}, z + 1) = h(\bar{x}, z, f(\bar{x}, z)) = f(\bar{x}, z + 1)$, wie gewünscht. \square

4.2 Gödelisierung und rekursiv aufzählbare Mengen

Notation. Sei \mathcal{S} die Kollektion aller endlichen Folgen aus \mathbb{N} . Wir definieren folgende Funktion:

$$\begin{aligned} \langle \cdot \rangle : \mathcal{S} &\rightarrow \mathbb{N} \\ s &\mapsto \begin{cases} 0, & \text{falls } s \text{ die leere Folge ist.} \\ p(0)^{x_0} \cdots p(n-2)^{x_{n-2}} p(n-1)^{x_{n-1}+1} - 1 & \text{falls } s = (x_0, \dots, x_{n-1}) \end{cases} \end{aligned}$$

wobei p die Funktion aus Lemma 4.11 ist. Wir schreiben $\langle x_0, \dots, x_{n-1} \rangle$ statt $\langle s \rangle$. Beachte, dass die Funktion $\langle \cdot \rangle$ eine Bijektion ist: Sie ist klarerweise injektiv, wegen der Eindeutigkeit der Faktorisierung in Primzahlen. Ferner, falls $x \neq 0$, ist $x + 1 \geq 2$ und lässt sich faktorisieren, wobei wir immer annehmen können, dass die größte Primzahl in der Faktorisierung nicht trivial vorkommt.

Lemma 4.15. *Mit der obigen Notation sind folgende Funktionen primitiv rekursiv:*

- Die Längenfunktion $\lg : \mathbb{N} \rightarrow \mathbb{N}$

$$m \mapsto \begin{cases} 0, & \text{falls } m = 0 \\ n, & \text{falls } m = \langle x_0, \dots, x_{n-1} \rangle \end{cases}$$

- Die Komponentenfunktion:

$$\begin{aligned} \mathbb{N}^2 &\rightarrow \mathbb{N} \\ (k, m) &\mapsto \begin{cases} x_k, & \text{falls } m = \langle x_0, \dots, x_{n-1} \rangle \text{ und } k < \lg(m) \\ 0, & \text{sonst.} \end{cases} \end{aligned}$$

Insbesondere ist für jedes k aus \mathbb{N} die k -te Komponentenfunktion $(\cdot)_k : \mathbb{N} \rightarrow \mathbb{N}$ primitiv rekursiv.

Beweis. Beachte, dass wegen Lemma 4.9 und Lemma 4.10 die Funktion $\lg(m) = \mu z \left(\forall y \leq m \left((z \leq y) \rightarrow (p(y) \uparrow m + 1) \right) \right)$ primitiv rekursiv ist, weil es immer ein solches $z \leq m + 1$ gibt, da die Funktion $x \mapsto p(x)$ streng monoton ist.

Für die Komponentenfunktion gilt $\mathbb{N} \rightarrow \mathbb{N}$

$$(k, m) \mapsto \begin{cases} \mu y (p(k)^{y+1} \uparrow m + 1), & \text{falls } k < \lg(m) - 1 \\ \mu y (p(k)^{y+2} \uparrow m + 1), & \text{falls } k = \lg(m) - 1 \\ 0, & \text{sonst.} \end{cases}$$

Aus dem Lemma 4.10 ist diese Funktion primitiv rekursiv, da es ein solches $y \leq m$ gibt. □

Korollar 4.16. Die Teilmenge von Elementen aus \mathbb{N} , welche eine Folge aus der Kollektion \mathcal{S}_n aller Folgen der Länge n repräsentieren, ist primitiv rekursiv, für jedes n aus \mathbb{N} . Dementsprechend werden wir sagen, dass \mathcal{S}_n primitiv rekursiv ist.

Korollar 4.17. Mehrfachrekursionen primitiv rekursiver Funktionen $g : \mathbb{N}^2 \rightarrow \mathbb{N}$ sind primitiv rekursiv. Dies bedeutet, dass die Funktion $f : \mathbb{N} \rightarrow \mathbb{N}$ gegeben durch $f(0) = 0$ und $f(x + 1) = g(x, \langle f(0), \dots, f(x) \rangle)$ primitiv rekursiv ist.

Beweis. Setze $h(x) = \langle f(0), \dots, f(x) \rangle$. Weil $f(x) = (h(x))_{x+1}$, genügt es zu zeigen, dass h primitiv rekursiv ist. Aus $h(0) = \langle 0 \rangle = 1 = S(0)$ und

$$\begin{aligned} h(x + 1) &= \langle f(0), \dots, f(x + 1) \rangle = \langle f(0), \dots, f(x), g(x, \langle f(0), \dots, f(x) \rangle) \rangle = \\ &= \langle (h(x))_0, \dots, (h(x))_x, g(x, h(x)) \rangle, \end{aligned}$$

folgt klarerweise, dass h primitiv rekursiv ist. □

Definition 4.18. Eine Teilmenge $A \subset \mathbb{N}^n$ ist *rekursiv aufzählbar*, falls A die Projektion auf die ersten n Koordinaten einer rekursiven Teilmenge $B \subset \mathbb{N}^{n+1}$ ist. Dies bedeutet,

$$(x_1, \dots, x_n) \in A \iff \text{es gibt } y \text{ aus } \mathbb{N} \text{ mit } (x_1, \dots, x_n, y) \in B.$$

Bemerkung 4.19. Jede rekursive Menge ist rekursiv aufzählbar, weil $A \times \mathbb{N} \subset \mathbb{N}^{n+1}$ auch rekursiv ist, wenn $A \subset \mathbb{N}^n$ rekursiv ist.

Wir werden im nächsten Abschnitt sehen, dass nicht jede rekursiv aufzählbare Menge rekursiv ist.

Lemma 4.20.

- Die Projektion einer rekursiv aufzählbaren Menge ist wiederum rekursiv aufzählbar.
- Rekursiv aufzählbare Mengen sind unter endlichen Durchschnitten und Vereinigungen abgeschlossen.
- Falls $A \subset \mathbb{N}^{n+1}$ rekursiv aufzählbar ist, so ist

$$C = \{(x_1, \dots, x_n, w) \in \mathbb{N}^{n+1} \mid \forall z < w \left((x_1, \dots, x_n, z) \in A \right)\}$$

rekursiv aufzählbar.

Beweis.

- Sei $X \subset \mathbb{N}^n$ die Projektion einer rekursiv aufzählbaren Menge $A \subset \mathbb{N}^{n+1}$. Es gibt eine rekursive Menge $B \subset \mathbb{N}^{n+2}$, welche auf A projiziert. Insbesondere liegt (x_1, \dots, x_n) genau dann in X , wenn es eine Folge s in \mathcal{S}_2 der Länge 2 derart gibt, dass $(x_1, \dots, x_n, (s)_0, (s)_1)$ in B liegt. Dies impliziert, dass X auch rekursiv aufzählbar ist, weil \mathcal{S}_2 primitiv rekursiv ist.
- Weil die Vereinigung von Projektionen die Projektion der Vereinigung ist, müssen wir nur den Fall eines Durchschnittes betrachten. Seien A_1 und A_2 rekursiv aufzählbare Teilmengen von \mathbb{N}^n , welche jeweils die Projektion der rekursiven Teilmengen B_1 und B_2 von \mathbb{N}^{n+1} sind. Es folgt, dass ein Tupel (x_1, \dots, x_n) genau dann in $A_1 \cap A_2$ liegt, wenn es eine Folge s in \mathcal{S}_2 der Länge 2 so gibt, dass $(x_1, \dots, x_n, (s)_0)$ in B_1 und $(x_1, \dots, x_n, (s)_1)$ in B_2 liegen.
- Angenommen, dass A die Projektion der rekursiven Teilmenge $B \subset \mathbb{N}^{n+2}$ ist, dann liegt für jedes $z < w$ das Tupel (x_1, \dots, x_n, z) in A , wenn es ein Element $y = y(z)$ so gibt (das von z abhängt), dass $(x_1, \dots, x_n, z, y(z))$ in B liegt. Insbesondere gibt es eine Folge $s = (y(0), \dots, y(w-1))$ der Länge w derart, dass für jedes $z < w$ das Tupel $(x_1, \dots, x_n, z, (s)_z)$ in B liegt:

$$(x_1, \dots, x_n, w) \in C \iff \exists s \left(\text{lg}(s) = w \wedge \forall z < w \left((x_1, \dots, x_n, z, (s)_z) \in B \right) \right).$$

Aus Lemma 4.9 folgt, dass C rekursiv aufzählbar ist.

□

Lemma 4.21. *Eine Teilmenge $A \subset \mathbb{N}^n$ ist genau dann rekursiv, wenn A und ihr Komplement $\mathbb{N}^n \setminus A$ beide rekursiv aufzählbar sind.*

Beweis. Eine Richtung ist wegen Lemma 4.6 und Bemerkung 4.19 trivial. Seien nun A und $\mathbb{N}^n \setminus A$ rekursiv aufzählbar bezüglich der rekursiven Teilmengen B und C von \mathbb{N}^{n+1} . Jedes Tupel (x_1, \dots, x_n) liegt entweder in A oder in ihrem Komplement. Also muss es ein y so geben, dass (x_1, \dots, x_n, y) in B oder in C liegt. Insbesondere ist die Funktion

$$g(x_1, \dots, x_n) = \mu y \left(((x_1, \dots, x_n, y) \in B) \vee ((x_1, \dots, x_n, y) \in C) \right)$$

wohldefiniert und rekursiv. Klarerweise gilt $\chi_A(x_1, \dots, x_n) = \chi_B((x_1, \dots, x_n, g(x_1, \dots, x_n)))$ und somit ist A rekursiv. □

Wir werden nun zeigen, dass Teilmengen von \mathbb{N} (aber nicht allgemein für Teilmengen von \mathbb{N}^n) genau dann rekursiv aufzählbar sind, wenn sie das Bild einer rekursiven Funktion sind. Insbesondere können sie rekursiv aufgezählt werden!

Lemma 4.22. *Eine Teilmenge $A \subset \mathbb{N}$ ist genau dann rekursiv aufzählbar, wenn sie leer oder gleich $f(\mathbb{N})$ ist, für eine rekursive Funktion $f : \mathbb{N} \rightarrow \mathbb{N}$.*

Beweis. Die leere Menge ist klarerweise primitiv rekursiv und somit rekursiv aufzählbar. Falls $A = f(\mathbb{N})$ für eine rekursive Funktion $f : \mathbb{N} \rightarrow \mathbb{N}$, dann ist die Menge $B = \{(x, y) \in \mathbb{N}^2 \mid f(x) = y\}$ rekursiv und $A = \pi_2^2(B)$.

Nun die Rückrichtung. Angenommen, dass die nicht-leere Menge A rekursiv aufzählbar bezüglich der rekursiven Menge $B \subset \mathbb{N}^2$ ist, wählen wir ein a aus A fest (weil $A \neq \emptyset$) und definieren

$$f: \mathbb{N} \rightarrow \mathbb{N}$$

$$z \mapsto \begin{cases} (z)_0, & \text{falls } z = \langle x, y \rangle \text{ mit } (x, y) \in B \\ a, & \text{sonst.} \end{cases}$$

Klarerweise ist f rekursiv und $f(\mathbb{N}) = A$, wie gewünscht. \square

Definition 4.23. Eine Menge $A \subset \mathbb{N}^n$ ist *arithmetisch*, falls sie in der Struktur

$$\mathcal{N}_0 = (\mathbb{N}, 0, S, +, \cdot, <)$$

definierbar ist. Dies bedeutet, falls es eine Formel $\varphi_A[x_1, \dots, x_n]$ in der Sprache $\{0, S, +, \cdot, <\}$ so gibt, dass

$$(a_1, \dots, a_n) \in A \iff \mathcal{N}_0 \models \varphi_A[a_1, \dots, a_n].$$

Eine Funktion ist *arithmetisch*, falls ihr Graph arithmetisch ist.

Für die Struktur \mathcal{N}_0 werden wir zwischen den Symbolen der Sprache $\{0, S, +, \cdot, <\}$ und den kanonischen Interpretationen nicht unterscheiden.

Proposition 4.24. *Rekursive Funktionen und Mengen sind arithmetisch.*

Beweis. Wegen Satz 4.14 genügt es zu zeigen, dass Komposition und μ -Rekursion wiederum definierbar sind, wenn alle Funktionen arithmetisch sind.

- Für die Komposition: Seien die (Graphen der) arithmetischen Funktionen g_1, \dots, g_m, h durch die Formeln $\varphi_{g_1}, \dots, \varphi_{g_m}, \varphi_h$ definiert. Wir setzen $\bar{x} = (x_1, \dots, x_n)$. Die Funktion $y = f(\bar{x}) = h(g_1(\bar{x}), \dots, g_m(\bar{x}))$ ist nun durch die Formel

$$\exists z_1 \dots \exists z_m \left(\varphi_h[z_1, \dots, z_m, y] \wedge \bigwedge_{i=1}^m \varphi_{g_i}[\bar{x}, z_i] \right)$$

definiert.

- Für die μ -Rekursion: Wenn $g(\bar{x}, z)$ durch die Formel $\varphi[\bar{x}, z, u]$ definiert wird, ist $y = f(\bar{x}) = \mu z (g(\bar{x}, z) = 0)$ durch die Formel

$$(\varphi[\bar{x}, y, 0] \wedge \forall u < y \neg \varphi[\bar{x}, u, 0])$$

definiert. \square

Korollar 4.25. *Rekursiv aufzählbare Mengen sind arithmetisch.*

Beweis. Wenn $\varphi[\bar{x}, y]$ die rekursive Menge $B \subset \mathbb{N}^{n+1}$ definiert, wird die Projektion A von B auf die ersten n Koordinaten durch die Formel $\exists y \varphi[\bar{x}, y]$ definiert. \square

4.3 Entscheidbarkeit

In diesem Abschnitt sind alle Sprachen endlich.

Definition 4.26. Sei \mathcal{L} eine endliche Sprache, welche aus den Symbolen $\lambda_0, \dots, \lambda_{l-1}$ besteht. Wir ordnen jeder endlichen Folge aus \mathcal{L} , insbesondere jedem Term und jeder Formel aus \mathcal{L} , nach den folgenden Regeln eine *Gödelnummer* zu:

$$\begin{aligned} \doteq &\mapsto \langle 0, 0 \rangle \\ \vee &\mapsto \langle 0, 1 \rangle \\ \neg &\mapsto \langle 0, 2 \rangle \\ (&\mapsto \langle 0, 3 \rangle \\) &\mapsto \langle 0, 4 \rangle \\ \exists &\mapsto \langle 0, 5 \rangle \\ \lambda_0 &\mapsto \langle 0, 6 \rangle \\ &\vdots \\ \lambda_{l-1} &\mapsto \langle 0, 5 + l \rangle \\ x_i &\mapsto \langle 1, i \rangle \end{aligned}$$

Falls die Formel φ der Folge $\xi_1 \dots \xi_n$ von Zeichen aus \mathcal{L} entspricht, ist ihre *Gödelnummer*

$$\ulcorner \varphi \urcorner = \langle \langle \xi_1 \rangle, \dots, \langle \xi_n \rangle \rangle.$$

Dementsprechend definieren wir die Gödelnummer $\ulcorner t \urcorner$ eines \mathcal{L} -Termes t der Stufe $k > 0$. Beachte, dass Termen der Stufe 0 (das heißt, für Variablen und für Konstantenzeichen aus der Sprache \mathcal{L}) nach dem obigen Vorschrift bereits eine Gödelnummer mit besitzen.

Bemerkung 4.27. Wir hätten eine ähnliche Definition, falls die Sprache \mathcal{L} nicht unbedingt endlich, aber zumindest rekursiv wäre.

Lemma 4.28. *Folgende Teilmengen von \mathbb{N} sind primitiv rekursiv:*

- $\{\ulcorner t \urcorner \mid t \in \text{TERM}\}$;
- $\{\ulcorner \varphi \urcorner \mid \varphi \in \text{FORM}\}$;
- $\{\ulcorner \varphi \urcorner \mid \varphi[x] \in \text{FORM} \text{ mit höchstens einer freien Variable } x\}$;
- $\{\ulcorner \chi \urcorner \mid \chi \text{ Aussage}\}$.

Beweis. Wir werden nur den ersten Teil zeigen, weil sich alle anderen analog beweisen lassen. Es lässt sich leicht zeigen, dass die Menge

$$\begin{aligned} \text{Teilfolge} = \{ (n, r, d) \in \mathbb{N}^3 \mid n = \langle x_0, \dots, x_{\lg(n)-1} \rangle \ \&\ \ r = \langle y_0, \dots, y_{\lg(r)-1} \rangle \ \& \\ d + \lg(r) \leq \lg(n) \ \&\ \ \bigwedge_{i=0}^{\lg(r)-1} (r)_i = (n)_{d+i} \} \end{aligned}$$

primitiv rekursiv ist. Beachte, dass $r \leq n$, wenn das Tripel (n, r, d) in Teilfolge liegt.

Wir sehen zuerst, dass die Menge T_0 der Gödelnummer von Termen t der Stufe 0 primitiv rekursiv ist, denn das Element n ist Gödelnummer von einem Term t der Stufe 0, falls

- $n = \langle 1, i \rangle$, für ein $i < n$ (und somit ist $n = \ulcorner x_i \urcorner$); oder
- $n = \langle 0, 6 + i \rangle = \langle \lambda_i \rangle$, für ein $i < l$, mit λ_i ein Konstantenzeichen aus \mathcal{L} .

Der erste Fall lässt sich mit den Koordinatenfunktionen leicht beschreiben. Der zweite Fall ist primitiv rekursiv, weil die Sprache endlich ist.

Wir müssen also nur noch zeigen, dass die Menge $T_{>0}$ der Gödelnummer von Termen positiver Stufe primitiv rekursiv ist. Das Element n ist $\ulcorner t \urcorner$ für einen Term t positiver Stufe, falls

- $(n)_0 = \langle \lambda_s \rangle$ für ein k -stelliges Funktionszeichen λ_s ; sowie
- die Werte $(n)_1 = \langle 0, 3 \rangle$ und $(n)_{\lg(n)-1} = \langle 0, 4 \rangle$; und
- $t = \lambda_s(t_1, \dots, t_k)$ für Terme t_1, \dots, t_k , welche Teilfolgen von t (an den entsprechenden Stellen) sind. Insbesondere ist jede Gödelnummer $\ulcorner t_i \urcorner$ echt kleiner als n .

Die ersten zwei Bedingungen sind offensichtlich primitiv rekursiv. Für die letzte Bedingung beachte, dass

$$\exists r_1 \dots \exists r_k \left(\sum_{i=1}^k \lg(r_i) + 3 = \lg(n) \wedge \left(\bigwedge_{j=1}^k ((\chi_{T_0}(r_j) = 1 \vee \chi_{T>0}(r_j) = 1) \wedge \right. \right. \\ \left. \left. \wedge (n, r_j, 2 + \sum_{1 \leq i < j} \lg(r_i)) \in \text{Teilfolge}) \right) \right)$$

primitiv rekursiv ist, wegen des Lemmas 4.9 und des Korollars 4.17. Beachte, dass die Termen t_1, \dots, t_k (und somit die Zahlen r_1, \dots, r_k) eindeutig bestimmt sind aufgrund der Eindeutigkeit der Darstellung. \square

Weil jede rekursiv aufzählbare Menge in der Struktur $\mathcal{N}_0 = (\mathbb{N}, 0, S, +, \cdot, <)$ definierbar ist, muss es allein aus Kardinalitätsgründen Teilmengen von \mathbb{N} geben, welche nicht rekursiv aufzählbar sind. Mit Hilfe des Satzes 4.47 können wir explizit Mengen angeben, die nicht rekursiv aufzählbar sind: Es genügt aus dem Lemma 4.21 das Komplement einer Menge zu betrachten, welche rekursiv aufzählbar ist, aber nicht rekursiv.

Definition 4.29. Eine Theorie T in einer endlichen Sprache \mathcal{L} ist *rekursiv axiomatisierbar*, falls $\{\ulcorner \chi \urcorner \mid \chi \in T\}$ rekursiv aufzählbar ist. Die Theorie T ist *entscheidbar*, falls $\{\ulcorner \chi \urcorner \mid T \vdash \chi\}$ rekursiv ist.

Bemerkung 4.30. Das Hilbertkalkül, das heißt die leere Theorie, sowie jede endliche Theorie ist rekursiv axiomatisierbar.

Wenn T entscheidbar und $T' \supset T$ eine Erweiterung mit $T' \setminus T$ endlich ist, so ist wegen Korollar 2.48 T' entscheidbar.

Lemma 4.31. Die Menge $\{\ulcorner \varphi \urcorner \mid \varphi \text{ Tautologie}\}$ ist primitiv rekursiv.

Beweis. Es genügt zu zeigen, dass die Kollektion $\{\ulcorner P \urcorner \mid P \text{ aussagenlogische Tautologie}\}$ primitiv rekursiv, weil die Ersetzungsfunktion klarerweise primitiv rekursiv ist. Dafür genügt es zu zeigen, dass das Komplement $\{\ulcorner P \urcorner \mid P \text{ keine aussagenlogische Tautologie}\}$ primitiv rekursiv

ist. Eine aussagenlogische Formel P ist keine Tautologie, falls es eine Belegung β mit $\beta(P) = 0$. Eine solche Belegung β ist gegeben durch eine Folge von 0 und 1's derart, dass die Menge

$$\{(\ulcorner P \urcorner, n) \mid n \text{ ist eine Belegung } \beta \text{ mit } \beta(P) = 0\}$$

ist primitiv rekursiv. Aus dem Lemma 4.10 folgt, dass eine aussagenlogische Formel P keine Tautologie ist, wenn es eine Belegung β mit $\beta(P) = 0$, deren Länge durch $\ulcorner P \urcorner$ beschränkt ist. \square

Lemma 4.32. *Wenn T rekursiv axiomatisierbar ist, dann ist die Menge $\{\ulcorner \varphi \urcorner \mid T \vdash \varphi\}$ rekursiv aufzählbar.*

Beweis. Weil wegen Lemma 4.20 rekursiv aufzählbare Mengen unter Projektionen abgeschlossen sind, genügt es zu zeigen, dass die Menge $\{(\ulcorner \varphi \urcorner, y) \mid y = \langle \varphi_1, \dots, \varphi_n \rangle \text{ kodiert einen Beweis von } \varphi_n = \varphi \text{ in } T\}$ rekursiv aufzählbar ist. Weil die Menge der Gödel'scher Zahlen der logischen Axiome klarerweise primitiv rekursiv ist, und wir Modus Ponens und \exists -Einführung kodieren können, folgt sofort, dass ein Beweis aus T kodiert werden kann, da wir bestimmen können, wann eine Formel (oder eher ihre Gödel'sche Zahl) zu T gehört, denn T ist rekursiv axiomatisierbar. \square

Aus Lemma 4.21 folgt, dass vollständige rekursiv axiomatisierbare Theorien entscheidbar sind, weil die Funktion

$$\begin{aligned} \mathbb{N} &\rightarrow \mathbb{N} \\ n &\mapsto \begin{cases} \ulcorner \neg \varphi \urcorner, & \text{falls } n = \ulcorner \varphi \urcorner \\ 0, & \text{sonst.} \end{cases} \end{aligned}$$

primitiv rekursiv ist.

Korollar 4.33. *Jede vollständige rekursiv axiomatisierbare Theorie ist entscheidbar.*

Notation. Wenn die Sprache \mathcal{L} die Teilsprache $\{0, S\}$ enthält, bezeichnen wir mit \underline{n} den Term $\underbrace{S \circ \dots \circ S}_n(0)$, wobei $\underline{0} = 0$.

Satz 4.34. *Die Theorie $\text{Th}(\mathcal{N}_0) = \{\chi \text{ Aussage, welche in } \mathcal{N}_0 \text{ gilt, d.h. } \mathcal{N}_0 \models \chi\}$ ist unentscheidbar.*

Beweis. Induktiv über den Aufbau von Formeln sieht man leicht, dass für n aus \mathbb{N} die Funktion

$$\begin{aligned} \mathbb{N}^2 &\rightarrow \mathbb{N} \\ (n, \ulcorner \varphi[x] \urcorner) &\mapsto \ulcorner \neg \varphi[\underline{n}] \urcorner \end{aligned}$$

primitiv rekursiv ist. Wegen Lemma 4.28 gibt es eine rekursive Aufzählung $\{\varphi_n[x]\}$ der Formeln mit einer freien Variable x in der Sprache $\{0, S, +, \cdot, <\}$.

Wenn $\text{Th}(\mathcal{N}_0)$ entscheidbar wäre, wäre die Menge $\{\ulcorner \chi \urcorner \mid \mathcal{N}_0 \models \chi\}$ rekursiv. Insbesondere wäre die Menge $A = \{n \in \mathbb{N} \mid \mathcal{N}_0 \models \neg \varphi_n[\underline{n}]\}$ auch rekursiv und somit arithmetisch wegen Proposition 4.24. Also gibt es eine Formel $\varphi[x]$ in der Sprache $\{0, S, +, \cdot, <\}$, welche in \mathcal{N}_0 die Menge A definiert. Sei n_0 so, dass $\varphi = \varphi_{n_0}$. Aber

$$n_0 \in A \iff \mathcal{N}_0 \models \varphi_{n_0}[n_0] \iff \mathcal{N}_0 \models \varphi_{n_0}[\underline{n}_0] \iff \mathcal{N}_0 \not\models \neg \varphi_{n_0}[\underline{n}_0] \iff n_0 \notin A,$$

was den gewünschten Widerspruch liefert. \square

Korollar 4.35 ((Einfacher) Unvollständigkeitssatz). *Jede rekursiv axiomatisierbare Theorie in der Sprache $\{0, S, +, \cdot, <\}$, welche \mathcal{N}_0 als Modell besitzt, ist unvollständig.*

Beweis. Wenn die rekursiv axiomatisierbare Theorie T vollständig ist, ist sie wegen Korollar 4.33 entscheidbar. Ferner sind wegen Korollar 2.65 alle Modelle von T elementar äquivalent und somit gilt

$$T \vdash \chi \iff \mathcal{N}_0 \models \chi \iff Th(\mathcal{N}_0) \vdash \chi.$$

Insbesondere ist T unentscheidbar. □

Wenn wir eine unentscheidbare Theorie finden, welche rekursiv axiomatisierbar ist (zum Beispiel, weil sie endlich ist), dann haben wir eine Teilmenge von \mathbb{N} , nämlich die Menge Gödel'scher Zahlen der Folgerungen, welche wegen Lemma 4.32 rekursiv aufzählbar aber nicht rekursiv ist. Leider ist $Th(\mathcal{N}_0)$ nicht rekursiv axiomatisierbar, deswegen werden wir im nächsten Abschnitt eine endliche Teiltheorie einführen: das Axiomensystem Q .

4.4 Der Gödel'sche Unvollständigkeitssatz

In diesem Abschnitt fixieren wir die Sprache $\mathcal{L} = \{0, S, +, \cdot, <\}$.

Definition 4.36. Das endliche Axiomensystem Q besteht aus den folgenden Axiomen:

$$Q_1 \quad \forall x(x + 0 \doteq x)$$

$$Q_2 \quad \forall x \forall y(x + S(y) \doteq S(x + y))$$

$$Q_3 \quad \forall x(x \cdot 0 \doteq 0)$$

$$Q_4 \quad \forall x \forall y(x \cdot S(y) \doteq x \cdot y + x)$$

$$Q_5 \quad \forall x \neg(x < 0)$$

$$Q_6 \quad \forall x \forall y(x < S(y) \leftrightarrow ((x < y) \vee (x \doteq y)))$$

Die Struktur \mathcal{N}_0 ist klarerweise ein Modell von Q . Somit ist Q widerspruchsfrei.

Lemma 4.37. *Für alle n und m aus \mathbb{N} sind folgende Axiome Folgerungen aus Q :*

$$Q_1^*(n, m) \quad (\underline{n} + \underline{m} \doteq \underline{n+m})$$

$$Q_2^*(n, m) \quad (\underline{n} \cdot \underline{m} \doteq \underline{n \cdot m})$$

$$Q_3^*(n) \quad \forall x \left((x < \underline{n}) \leftrightarrow \bigvee_{k < n} (x \doteq \underline{k}) \right), \quad \text{wobei } Q_3^*(0) \text{ gleich } \forall x \neg(x < 0) \text{ (Leere Disjunktion!)}$$

Beweis. Wegen dem Vollständigkeitssatz 2.64 genügt es zu zeigen, dass diese Axiome in jedem Modell von Q gelten. Achtung! In einem Modell \mathcal{M} von Q kann es Elemente geben, welche nicht der Form \underline{n} sind. Aber in \mathcal{M} gilt, dass $\underline{n+1} = S(\underline{n})$. Somit lassen sich die ersten beiden Behauptungen leicht induktiv über m zeigen. Die dritte Behauptung zeigt man leicht durch Induktion über n . □

Notation. Wir bezeichnen mit Q^* die Theorie, welche aus den Axiomen $Q_1^*(n, m), Q_2^*(n, m), Q_3^*(n)$ mit n und m aus \mathbb{N} besteht. Beachte, dass Q^* nicht mehr endlich ist, aber dennoch rekursiv axiomatisierbar. Wegen Korollar 4.35 ist weder Q noch Q^* vollständig.

Korollar 4.38. Für alle n und m aus \mathbb{N} gilt:

1. Wenn $n \neq m$, dann $Q^* \vdash \neg(\underline{n} \doteq \underline{m})$.
2. Wenn $n < m$, dann $Q^* \vdash (\underline{n} < \underline{m})$.
3. Wenn $n \not< m$, dann $Q^* \vdash \neg(\underline{n} < \underline{m})$.

Beweis. Wegen dem Vollständigkeitsatz 2.64 genügt es induktiv über m zu zeigen, dass diese Axiome in jedem Modell \mathcal{M} von Q^* gelten.

1. Falls $m = 0$, dann ist $n \neq 0$ und somit $n = k + 1$ für ein k aus \mathbb{N} . Aber $\underline{k} < S(\underline{k}) = \underline{n}$ wegen Q_3^* und somit ist \underline{n} verschieden von $0 = \underline{0}$ (nochmal Q_3^*).
Falls $m \neq 0$, aber $n = 0$, ist der Beweis wie oben. Ansonsten gibt es n' und m' aus \mathbb{N} mit $n = n' + 1$ und $m = m' + 1$. Weil $n \neq m$, ist $n' \neq m'$. Wenn $m' < n'$, folgt induktiv, dass \underline{n}' verschieden von \underline{k} ist für alle $k \leq m'$. Weil $\underline{n}' < \underline{n}$, folgt aus Q_3^* , dass \underline{n} und \underline{m} (in \mathcal{M}) verschieden sind.
2. Lässt sich einfach mit Q_3^* induktiv über m zeigen.
3. Falls $m = 0$, folgt dies trivialerweise aus Q_3^* . Wenn $m = m' + 1$, haben wir $n = m$ oder $n > m$ (weil die Ordnung auf \mathbb{N} total ist). Falls $\underline{n} < \underline{m} = S(\underline{m}')$ in \mathcal{M} gilt, dann gibt es ein $k \leq m'$ mit $\underline{n} = \underline{k}$ (in \mathcal{M}). Aber, weil $n \neq k$, ist \underline{n} verschieden von \underline{k} wegen des ersten Teiles.

□

Induktiv über den Aufbau von Formeln sieht man leicht:

Korollar 4.39. Für jede quantorfreie Formel $\varphi[x_1, \dots, x_n]$ und Elemente m_1, \dots, m_n aus \mathbb{N} gilt

$$\mathcal{N}_0 \models \varphi[m_1, \dots, m_n] \iff Q^* \vdash \varphi[\underline{m}_1, \dots, \underline{m}_n].$$

Wir wollen die Äquivalenz von Gültigkeit in \mathcal{N}_0 und Beweisbarkeit aus Q^* auf eine größere Klasse von Formeln erweitern.

Notation. Wir werden die Abkürzung $\forall x < y \varphi$ für die *beschränkte universelle Quantifizierung* $\forall x ((x < y) \wedge \varphi)$ verwenden.

Definition 4.40. Eine Σ_1 -Formel ist eine Formel in der Sprache $\mathcal{L} = \{0, S, +, \cdot, <\}$, welche aus einer quantorfreien Formel durch iteriertes Anwenden von $\wedge, \vee, \exists x$ und *beschränkter universeller Quantifizierung* $\forall x < y$ entsteht, wobei x verschieden von der Variable y sei.

Beispiel 4.41. Die Formel $\exists y(x \doteq y)$ ist Σ_1 , aber ihre Negation $\forall y(x \neq y)$ ist es nicht.

Bemerkung 4.42. Angenommen, dass in der Formel φ nur universelle Quantifizierungen der Form $\forall x < t$ vorkommen, wobei x nicht frei im Term t vorkommt. Weil jeder Term aus $0, S, +, \cdot$ gewonnen wird, können wir dies zu $\forall x < y$ umformen und im Quantorenbereich die quantorenfreie Formel $y = t$ hinzufügen.

Insbesondere hätten wir eine allgemeinere Definition von Σ_1 -Formeln angeben können, welche aber äquivalent ist.

Satz 4.43. Für jede Σ_1 -Formel $\varphi[x_1, \dots, x_n]$ und Elemente m_1, \dots, m_n aus \mathbb{N} gilt

$$\mathcal{N}_0 \models \varphi[m_1, \dots, m_n] \iff Q^* \vdash \varphi[\underline{m}_1, \dots, \underline{m}_n].$$

Beweis. Eine Richtung folgt aus dem Vollständigkeitssatz. Wir müssen nur zeigen, dass Q^* die Aussage $\varphi[\underline{m}_1, \dots, \underline{m}_n]$ beweist, falls $\mathcal{N}_0 \models \varphi[m_1, \dots, m_n]$. Wir beweisen das induktiv über den Aufbau von φ , wobei es für quantorenfreie φ aus Korollar 4.39 folgt. Der Fall einer Konjunktion, bzw. einer Disjunktion, ist trivial. Nur für die Quantifizierung bleibt es zu zeigen:

- Falls $\varphi = \exists y \psi$, dann ist $\psi[x_1, \dots, x_n, y]$ auch eine Σ_1 -Formel. Wenn $\mathcal{N}_0 \models \varphi[m_1, \dots, m_n]$, gibt es ein Element k aus \mathbb{N} mit $\mathcal{N}_0 \models \psi[m_1, \dots, m_n, k]$. Mit der Induktionsannahme folgt, dass $Q^* \vdash \psi[\underline{m}_1, \dots, \underline{m}_n, \underline{k}]$. Aus dem \exists -Quantorenaxiom folgt, dass $Q^* \vdash (\exists y \psi)[\underline{m}_1, \dots, \underline{m}_n]$, das heißt, $Q^* \vdash \varphi[\underline{m}_1, \dots, \underline{m}_n]$.
- Falls $\varphi = \forall y < x_1 \psi[x_1, \dots, x_n, y]$, haben wir $\mathcal{N}_0 \models \psi[m_1, \dots, m_n, k]$ für alle $k < m_1$. Insbesondere beweist Q^* die Aussage $\psi[\underline{m}_1, \dots, \underline{m}_n, \underline{k}]$ für alle $k < m_1$. Aus dem Axiom Q_3^* folgt, dass $Q^* \vdash \forall y < x_1 \psi[\underline{m}_1, \dots, \underline{m}_n]$, wie gewünscht.

□

Proposition 4.44. Jede rekursive Funktion bzw. jede rekursiv aufzählbare Menge wird durch eine Σ_1 -Formel in \mathcal{N} definiert.

Beweis. Aus den Beweisen von Proposition 4.24 und Korollar 4.25 folgt, dass wir nur eine geeignete Definition für die μ -Rekursion angeben müssen, ohne $\neg\varphi$ zu benutzen. Es genügt also, folgende Definition zu betrachten:

$$\left(\varphi[\bar{x}, y, 0] \wedge \forall z < y \exists u (\varphi[\bar{x}, z, u] \wedge u \neq 0) \right),$$

welche eine Σ_1 -Formel ist.

□

Lemma 4.45. Jede rekursive Funktion $f : \mathbb{N}^n \rightarrow \mathbb{N}$ wird von einer Σ_1 -Formel $\varphi[x_1, \dots, x_n, y]$ in Q^* repräsentiert: Für alle m_1, \dots, m_n aus \mathbb{N} gilt

$$Q^* \vdash \forall y \left(\varphi[\underline{m}_1, \dots, \underline{m}_n, y] \leftrightarrow (y \doteq f(m_1, \dots, m_n)) \right)$$

Insbesondere wird jede rekursive Teilmenge $A \subset \mathbb{N}^n$ von einer Σ_1 -Formel $\psi[x_1, \dots, x_n, y]$ in Q^* repräsentiert: Für alle m_1, \dots, m_n aus \mathbb{N} gilt

$$\left. \begin{array}{l} (m_1, \dots, m_n) \in A \implies Q^* \vdash \psi[\underline{m}_1, \dots, \underline{m}_n] \\ (m_1, \dots, m_n) \notin A \implies Q^* \vdash \neg\psi[\underline{m}_1, \dots, \underline{m}_n] \end{array} \right\}$$

Beweis. Wegen Satz 4.14 genügt es zu zeigen, dass die Funktionen aus der Klasse \mathcal{F} durch Σ_1 -Formeln in Q^* repräsentierbar sind. Die Grundfunktionen $\{S, +, \cdot, \chi_{<}\}$ sind klarerweise so repräsentierbar und auch die Konstanten- und Koordinatenfunktionen.

- Für die Komposition: Wir nehmen an, dass die Funktionen g_1, \dots, g_m, h durch die Σ_1 -Formeln $\varphi_{g_1}, \dots, \varphi_{g_m}, \varphi_h$ repräsentiert werden. Setze $\bar{x} = (x_1, \dots, x_n)$. Die Funktion $y = f(\bar{x}) = h(g_1(\bar{x}), \dots, g_m(\bar{x}))$ ist nun durch die Formel

$$\exists z_1 \dots \exists z_m \left(\varphi_h[z_1, \dots, z_m, y] \wedge \bigwedge_{i=1}^m \varphi_{g_i}[\bar{x}, z_i] \right)$$

repräsentiert, welche wieder eine Σ_1 -Formel ist.

- Für die μ -Rekursion: Wir nehmen an, dass $g(\bar{x}, z)$ durch die Σ_1 -Formel $\psi[\bar{x}, z, u]$ repräsentiert wird und machen es so ähnlich wie im Beweis von Proposition 4.44: Wir betrachten die Σ_1 -Formel

$$\varphi[\bar{x}, y] = \left(\psi[\bar{x}, y, 0] \wedge \forall z < y \exists u (\psi[\bar{x}, z, u] \wedge u \neq 0) \wedge ((0 \leq y) \wedge \forall w < y (S(w) \leq y)) \right).$$

Weil $\mathcal{N}_0 \models \varphi[m_1, \dots, m_n, f(m_1, \dots, m_n)]$, folgt aus Satz 4.43

$$Q^* \vdash \varphi[\underline{m}_1, \dots, \underline{m}_n, \underline{f(m_1, \dots, m_n)}].$$

Es genügt nun zu zeigen, dass in jedem Modell \mathcal{M} von Q^* gilt: falls $\mathcal{M} \models \varphi[\underline{m}_1, \dots, \underline{m}_n, b]$ für ein Element b aus M , dann ist $b = \underline{f(m_1, \dots, m_n)}$. Weil

$$\mathcal{M} \models \varphi[\underline{m}_1, \dots, \underline{m}_n, \underline{f(m_1, \dots, m_n)}]$$

folgt, dass weder $b < \underline{f(m_1, \dots, m_n)}$ noch $\underline{f(m_1, \dots, m_n)} < b$ in \mathcal{M} gilt. Wir wissen, dass $b \geq 0$ in \mathcal{M} ist. Entweder ist $b = \underline{0}$ oder $b > 0$ und somit $b \geq \underline{1}$. Dies bedeutet, entweder ist $b = \underline{1}$ oder $b \geq \underline{2}$. Wir iterieren und schließen daraus, dass $b = \underline{f(m_1, \dots, m_n)}$.

Für eine rekursive Teilmenge $A \subset \mathbb{N}^n$, ist ihre Charakteristische Funktion durch eine Σ_1 -Formel $\varphi[x_1, \dots, x_n, y]$ repräsentiert. Setze nun $\psi[x_1, \dots, x_n] = \varphi[x_1, \dots, x_n, \underline{1}]$, weil in jedem Modell von Q^* das Element $\underline{0}$ verschieden von $\underline{1}$ ist. \square

Bemerkung 4.46. Im obigen Beweis für die μ -Rekursion haben wir nicht verwendet, dass die Interpretation von $<$ in einem beliebigen Modell \mathcal{M} von Q^* eine totale Ordnung ist (weil es nämlich nicht stimmt!)

Satz 4.47 (Gödel'scher (erster) Unvollständigkeitssatz). *Jede Teiltheorie $T \subset \text{Th}(\mathcal{N}_0)$ ist unentscheidbar. Insbesondere ist Q unentscheidbar.*

Es gibt Teilmengen aus \mathbb{N} , welche rekursiv aufzählbar aber nicht rekursiv sind.

Beweis. Es genügt zu zeigen, dass jede Teiltheorie $T_1 \subset \text{Th}(\mathcal{N}_0)$, welche alle Aussagen aus Q^* beweist, unentscheidbar ist. Insbesondere ist dann auch Q unentscheidbar. Wenn T eine beliebige Teiltheorie wäre, welche entscheidbar ist, wäre wegen Bemerkung 4.30 auch $T_1 = T \cup \{Q_i\}_{1 \leq i \leq 6}$ entscheidbar, was ein Widerspruch wäre, weil T_1 alle Aussagen aus Q^* beweist.

Sei nun $T_1 \subset \text{Th}(\mathcal{N}_0)$ eine Teiltheorie, welche alle Aussagen aus Q^* beweist. Ferner sei $\{\varphi_n[x]\}$ eine rekursive Aufzählung aller Formeln in einer freien Variable. Falls T_1 entscheidbar wäre, wäre die Menge $A = \{n \in \mathbb{N} \mid T_1 \vdash \neg \varphi_n[\underline{n}]\}$ auch rekursiv und wegen Lemma 4.45 würde A durch eine Σ_1 -Formel repräsentiert werden. Bezeichne diese Formel mit φ_{n_0} .

- Falls n_0 in A liegt, dann gilt $Q^* \vdash \varphi_{n_0}[\underline{n}_0]$, weil A durch $\varphi_{n_0}[x]$ repräsentierbar ist, und deswegen auch $T_1 \vdash \varphi_{n_0}[\underline{n}_0]$. Aber $T_1 \vdash \neg\varphi_{n_0}[\underline{n}_0]$, das heißt T_1 ist widersprüchlich.
- Falls n_0 nicht in A liegt, dann $Q^* \vdash \neg\varphi_{n_0}[\underline{n}_0]$, weil A durch $\varphi_{n_0}[x]$ repräsentierbar ist. Insbesondere beweist T_1 auch $\neg\varphi_{n_0}[\underline{n}_0]$ und somit liegt n_0 in A , was ein Widerspruch ist.

Wegen Lemma 4.32 ist die Menge $\{\ulcorner \chi \urcorner \mid Q \vdash \chi\}$ rekursiv aufzählbar, weil Q endlich ist. Aber diese Menge ist nicht rekursiv, da Q unentscheidbar ist. \square

Wir werden diesen Abschnitt mit einem kleinen Exkurs zur Rekursionstheorie beenden.

Satz 4.48. (Fixpunktssatz) Für jede Formel $\psi[x]$ gibt es eine Aussage χ derart, dass

$$Q^* \vdash (\chi \leftrightarrow \psi[\ulcorner \chi \urcorner]).$$

Falls ψ eine Σ_1 -Formel ist, so ist χ eine Σ_1 -Aussage.

Beweis. Die Funktion

$$f : \quad \mathbb{N}^2 \quad \rightarrow \quad \mathbb{N}$$

$$(\ulcorner \varphi[x] \urcorner, n) \mapsto \ulcorner \varphi[\underline{n}] \urcorner$$

ist primitiv rekursiv und wird durch eine Σ_1 -Formel $\varphi_1[x, y, z]$ repräsentiert: Für

$$Q^* \vdash \forall z (\varphi_1[\ulcorner \varphi[x] \urcorner, \underline{n}, z] \leftrightarrow (z \doteq \ulcorner \varphi[\underline{n}] \urcorner)).$$

Setze nun $\varphi'[x] = \exists y (\psi[y] \wedge \varphi_1[x, x, y])$ und beachte, dass φ' eine Σ_1 -Formel ist, falls ψ es ist. Aus der Konstruktion folgt, dass für jede Formel $\varphi[x]$

$$Q^* \vdash (\varphi'[\ulcorner \varphi[x] \urcorner] \leftrightarrow \psi[\ulcorner \varphi[\ulcorner \varphi[x] \urcorner] \urcorner]).$$

Insbesondere gilt für $\varphi = \varphi'$, dass

$$Q^* \vdash (\varphi'[\ulcorner \varphi'[x] \urcorner] \leftrightarrow \psi[\ulcorner \varphi'[\ulcorner \varphi'[x] \urcorner] \urcorner]).$$

Die gewünschte Aussage χ ist $\varphi'[\ulcorner \varphi'[x] \urcorner]$. \square

Der Fixpunktssatz liefert einen anderen Beweis des Unvollständigkeitssatzes.

Korollar 4.49. Jede Teiltheorie $T \subset \text{Th}(\mathcal{N}_0)$ ist unentscheidbar.

Beweis. Ohne Einschränkung der Allgemeinheit können wir annehmen, dass T alle Aussagen aus Q^* beweist. Falls T entscheidbar wäre, wäre die Menge $A = \{\ulcorner \varphi \urcorner \mid T \vdash \varphi\}$ rekursiv und wegen Lemma 4.45 durch eine Σ_1 -Formel $\psi[x]$ repräsentierbar. Wenden wir den Fixpunktssatz 4.48 auf die Formel $\neg\psi[x]$ an, bekommen wir eine Aussage χ mit

$$Q^* \vdash (\chi \leftrightarrow \neg\psi[\ulcorner \chi \urcorner]),$$

und somit ist auch in T die obige Äquivalenz beweisbar. Beachte, dass $\neg\psi[x]$ nicht unbedingt eine Σ_1 -Formel ist.

- Falls T die Aussage χ beweist, liegt $\ulcorner \chi \urcorner$ in A . Wegen Lemma 4.45 gilt $Q^* \vdash \psi[\ulcorner \chi \urcorner]$ und daher auch $T \vdash \psi[\ulcorner \chi \urcorner]$. Andererseits beweist T aus der Konstruktion von χ auch $\neg\psi[\ulcorner \chi \urcorner]$, was ein Widerspruch ist.
- Falls T die Aussage χ nicht beweist, dann liegt $\ulcorner \chi \urcorner$ nicht in A und es gilt $Q^* \vdash \neg\psi[\ulcorner \chi \urcorner]$. Es folgt $T \vdash \neg\psi[\ulcorner \chi \urcorner]$ und somit beweist T die Aussage χ , was ein Widerspruch ist.

□

4.5 Modelle der Peanoarithmetik

Definition 4.50. *Peanoarithmetik* ist die Theorie PA in der Sprache $\mathcal{L} = \{0, S, +, \cdot, <\}$, welche aus dem Axiomensystem Q zusammen mit folgendem *Induktionsschema*

$$\forall x_1 \dots \forall x_n \left((\varphi[x_1, \dots, x_n, 0] \wedge \forall y (\varphi[x_1, \dots, x_n, y] \rightarrow \varphi[x_1, \dots, x_n, S(y)])) \rightarrow \forall z \varphi[x_1, \dots, x_n, z] \right)$$

für alle \mathcal{L} -Formeln φ besteht.

Die Theorie PA ist rekursiv axiomatisierbar und widerspruchsfrei, da \mathcal{N}_0 ein Modell davon ist.

Lemma 4.51. *In PA sind folgende Aussagen beweisbar:*

- Jedes Element außer 0 besitzt einen Vorgänger.
- Die Nachfolgerfunktion S ist injektiv.
- Die Ordnung $<$ ist linear mit kleinstem Element 0.
- Der Nachfolger $S(x)$ ist das kleinste Element, welches echt größer als x ist.
- Die Summe und das Produkt definieren einen kommutativen Halbring mit neutralen Elementen 0 für $+$ und 1 für \cdot .
- Die Summe und das Produkt sind beide monoton bezüglich der Ordnung:

$$\forall x \forall y \forall z \left((x < y) \rightarrow (x + z < y + z) \right)$$

$$\forall x \forall y \forall z \left(((x < y) \wedge \neg(z \doteq 0)) \rightarrow (x \cdot z < y \cdot z) \right)$$

Beweis. Wir beweisen nur einige der Eigenschaften, weil das Vorgehen jedes Mal ähnlich ist. Für (a) sei $\varphi[x] = (\neg(x \doteq 0) \rightarrow \exists y (S(y) = x))$. Wir wollen zeigen, dass $PA \models \forall x \varphi[x]$. Wir arbeiten in einem beliebigen Modell \mathcal{M} von PA. Wegen dem Induktionsschema für φ genügt es zu zeigen, dass $\mathcal{M} \models \varphi[\underline{0}]$, was trivial ist, und dass $\mathcal{M} \models \varphi[S(a)]$, falls $\mathcal{M} \models \varphi[a]$ für ein Element a aus M . Wenn $\mathcal{M} \models \varphi[a]$, folgt aus Q_6 , dass $a < S(a)$, also $S(a) \neq \underline{0}$ aus Q_5 . Klarerweise gibt es ein Element in M (nämlich a) derart, dass $S(a) = S(a)$, also $\mathcal{M} \models \varphi[S(a)]$.

Wir zeigen nun, dass 0 kleiner als jedes Element ist. Schreibe

$$\psi[x] = (\neg(x \doteq 0) \rightarrow 0 < x).$$

Klarerweise gilt $\mathcal{M} \models \psi[0]$. Wenn $\mathcal{M} \models \psi[a]$, folgt wie oben, dass $S(a) \neq 0$. Wenn $a = 0$, ist $0 < S(0) = S(a)$. Sonst ist $a \neq 0$, also $0 < a$, weil $\mathcal{M} \models \psi[a]$. Somit ist $0 < S(a)$ wegen Q_6 .

Um zu zeigen, dass je zwei Elemente vergleichbar sind, setze

$$\theta[x] = \forall y \left(\neg(y \dot{=} x) \rightarrow (x < y \vee y < x) \right).$$

Aus dem Obigen folgt $\mathcal{M} \models \theta[0]$. Falls $\mathcal{M} \models \theta[a]$, sei nun b mit $b \neq S(a)$. Falls $b = a$, dann ist $b < S(a)$ wegen Q_6 . Falls $b \neq a$, dann ist $b < a$ oder $a < b$. Im ersten Fall ist $b < S(a)$ wegen Q_6 . Falls $a < b$, genügt es zu zeigen, dass $S(a) < S(b)$, weil aus Q_6 dann folgt, dass $S(a) < b$. Dafür setze $\theta_1[x] = \forall y (y < x \rightarrow S(y) < S(x))$. Da $\mathcal{M} \models \theta_1[0]$ trivialerweise gilt, müssen wir nur zeigen, dass $\mathcal{M} \models \theta[S(c)]$, falls $\mathcal{M} \models \theta[c]$. Sei d mit $d < S(c)$. Aus Q_6 folgt, dass $d = c$, also $d < S(c)$ und somit $d < S(S(c))$, oder $d < c$, also $S(d) < S(c)$. Aus Q_6 folgt wieder $S(d) < S(S(c))$, wie gewünscht. \square

Korollar 4.52. *In PA ist das allgemeine Induktionsschema beweisbar:*

$$PA \models \forall x_1 \dots \forall x_n \left(\forall y (\forall z (z < y \rightarrow \varphi[x_1, \dots, x_n, z]) \rightarrow \varphi[x_1, \dots, x_n, y]) \right. \\ \left. \rightarrow \forall u \varphi[x_1, \dots, x_n, u] \right)$$

für alle \mathcal{L} -Formeln φ

Beweis. Sei \mathcal{M} ein beliebiges Modell von PA und \bar{a} ein Tupel aus M^n derart, dass

$$\mathcal{M} \models \forall y (\forall z ((z < y) \rightarrow \varphi[\bar{a}, z]) \rightarrow \varphi[\bar{a}, y]).$$

Setze $\theta[\bar{a}, y] = \forall z (z < y \rightarrow \varphi[\bar{a}, z])$. Klarerweise gilt $\mathcal{M} \models \theta[\bar{a}, 0]$. Angenommen, dass $\mathcal{M} \models \theta[\bar{a}, b]$ für ein b aus M , müssen wir zeigen, dass $\mathcal{M} \models \theta[\bar{a}, S(b)]$. Aus der Hypothese folgt, dass $\mathcal{M} \models \varphi[\bar{a}, b]$.

Sei $c < S(b)$. Aus Q_6 folgt, dass $c = b$, also $\mathcal{M} \models \varphi[\bar{a}, c]$, oder $c < b$ und somit gilt auch $\mathcal{M} \models \varphi[\bar{a}, c]$. Insbesondere erfüllt $S(b)$ die Formel $\theta[\bar{a}, y]$. Daher gilt $\forall y \theta[\bar{a}, y]$ in \mathcal{M} , wie gewünscht, und somit $\mathcal{M} \models \forall u \varphi[\bar{a}, u]$. \square

Bemerkung 4.53. Jede nicht-leere (mit Parametern) definierbare Teilmenge X eines Modells \mathcal{M} der Peanoarithmetik besitzt ein kleinstes Element. Es genügt zu zeigen, dass für die definierbare Menge $Y = \{y \in M \mid \exists x \in X \text{ mit } x < y\}$ die Menge $M \setminus Y$ nicht unter der Nachfolgerfunktion abgeschlossen sein kann.

Bemerkung 4.54. Analog zum Korollar 3.17, ist es leicht zu zeigen, dass es *nichtstandard* Modelle \mathcal{M} von PA gibt. Das heißt, das Modell \mathcal{M} besitzt *nichtstandard natürliche Zahlen* m mit $\underline{n} < m$ für jedes n aus \mathbb{N} . Die Kollektion nichtstandard natürlicher Zahlen in \mathcal{M} besitzt jedoch kein kleinstes Element, also ist diese Kollektion nicht in \mathcal{M} definierbar, wegen der Bemerkung 4.53.

Demnächst werden wir eine konkrete Aussage finden, welche in \mathcal{N}_0 gilt aber nicht in Peanoarithmetik beweisbar ist, nämlich die, dass jede *Goodstein'sche Folge* konstant 0 wird.

Definition 4.55. Sei $2 \leq b$ eine natürliche Zahl. Die *Darstellung der natürlichen Zahl $n \neq 0$ zur Basis b* ist eindeutig bestimmt:

$$n = \sum_{i=0}^k c_i \cdot b^i,$$

mit $0 \leq c_i < b$ für jedes $0 \leq i \leq k$ und $c_0 \neq 0$.

Die *totale Darstellung* von n zur Basis b wird daraus gewonnen, wenn wir die Exponenten auch zur Basis b darstellen, und dann die Exponenten davon usw. z. B für $b = 2$ ist

$$\begin{aligned} 9 &= 2^3 + 1 &= 2^{2+1} + 1 \\ 19 &= 2^4 + 2 + 1 &= 2^{2^2} + 2 + 1 \end{aligned}$$

Bemerkung 4.56. Sowohl die Darstellung $\text{Darst}(\cdot, b)$ zur Basis b als auch die totale Darstellung $\text{totDarst}(\cdot, b)$ zur Basis b sind primitiv rekursive Funktionen, weil $k < n$ mit

$$k = \mu z (b^z > n) \div 1 = \text{Potenz}(n, b)$$

und

$$c_k = \mu z (z \cdot b^{\text{Potenz}(n, b)} = n - \text{Rest}(n, b^{\text{Potenz}(n, b)}).$$

Insbesondere ist die *Basiswechselfunktion* $R_b : \mathbb{N} \rightarrow \mathbb{N}$, welche jedes b durch $b + 1$ in der totalen Darstellung der Zahl n zur Basis b ersetzt, auch primitiv rekursiv, z. B: für

$$266 = 2^{2^{2+1}} + 2^{2+1} + 2$$

ist

$$R_2(266) = 3^{3^{3+1}} + 3^{3+1} + 3 \gg 266.$$

Beachte, dass $R_b(n) = n$, falls $n < b$, weil $n = n \cdot b^0 = n \cdot (b + 1)^0$.

Definition 4.57. Die *Goodstein'sche Folge* $(n_k)_{k \in \mathbb{N}}$ mit Anfangswert n wird folgenderweise definiert:

$$n_k = \begin{cases} n, & \text{falls } k = 0. \\ \text{totDarst}(n, 2), & \text{falls } k = 1 \text{ und } n \neq 0. \\ R_{k+2}(\text{totDarst}(n_k \div 1, k + 1)), & \text{falls } k > 1 \text{ und} \\ & \text{totDarst}(n_k \div 1) \neq 0 \\ 0, & \text{sonst.} \end{cases}$$

Jeder Schritt der Folge ist klarerweise primitiv rekursiv.

Satz 4.58. Für jedes n gibt es ein k mit $n_k = 0$. Insbesondere ist die Goodstein'sche Funktion

$$\begin{aligned} G : \mathbb{N}^n &\rightarrow \mathbb{N} \\ n &\mapsto \mu k (n_k = 0) \end{aligned}$$

wohldefiniert.

Beachte, dass die Goodstein'sche Funktion rekursiv ist und wegen Proposition 4.24 definierbar in der Struktur \mathcal{N}_0 durch eine $\{0, S, +, -, \cdot, <\}$ -Formel.

Wir illustrieren den Beweis mit einem konkreten Beispiel: Sei $n = 16$ der Anfangswert, also $n_1 = 2^{2^2}$. Zu dieser Darstellung ersetzen wir alle 2en durch ω und bekommen die entstprechende Ordinalzahl

$$\alpha_1 = \omega^{\omega^\omega},$$

deren kleinste Potenz von ω die Ordinalzahl ω^ω ist. Nun ist

$$16 - 1 = 2^{2+1} + 2^2 + 2 + 1, \text{ so } n_2 = 3^{3+1} + 3^3 + 3 + 1.$$

Die entsprechende Ordinalzahl, wenn wir alle 3en durch ω ersetzen, ist

$$\alpha_2 = \omega^{\omega+1} + \omega^\omega + \omega + 1.$$

Beachte, dass die kleinste Potenz von ω in α_1 durch kleinere Potenzen in α_1 ersetzt wurde. Beim nächsten Schritt ziehen wir eins ab und auch bei der entsprechenden Ordinalzahl

$$\alpha_3 = \omega^{\omega+1} + \omega^\omega + \omega.$$

Beim nächsten Schritt wird wiederum die kleinste Potenz von ω in α_3 durch kleinere Potenzen von ω ersetzt:

$$\alpha_4 = \omega^{\omega+1} + \omega^\omega + 3.$$

Wir bekommen somit eine absteigende Kette von Ordinalzahlen, welche wegen Lemma 3.20 (e) endlich sein muss. Dies bedeutet, dass der entsprechende Term n_k die natürliche Zahl 0 sein muss (sonst machen wir weiter), wie gewünscht.

Satz 4.59 (Kirby-Paris). $PA \not\vdash \forall x \exists y (G(x) \doteq y)$.

Eine grobe Beweisidee des Satzes von Kirby und Paris ist, dass jede in Peanoarithmetik definierbare Funktion, deren Definitionsbereich das gesamte Universum ist, in einem konkreten Sinne, der für diese Vorlesung nicht geeignet ist, *begrenzt* wachsen muss. Jedoch wächst die Goodstein'sche Funktion zu schnell.

Appendix

A Das Zorn'sche Lemma

Definition A.1. Eine Menge \mathcal{S} ist *partiell angeordnet*, falls sie eine binäre Relation \leq mit den folgenden Eigenschaften besitzt:

Reflexivität $x \leq x$ für alle x aus \mathcal{S} ;

Antisymmetrie Für alle x und y aus \mathcal{S} gelten $x \leq y$ und $y \leq x$ gleichzeitig genau dann, wenn $x = y$;

Transitivität Für alle x, y und z aus \mathcal{S} gilt die Implikation

$$x \leq y \text{ und } y \leq z \implies x \leq z.$$

Wir schreiben $x < y$, falls $x \leq y$ aber $x \neq y$.

Eine partielle Ordnung \leq auf \mathcal{S} ist *total*, oder *linear*, falls $x < y$ oder $y < x$ für alle $x \neq y$ aus \mathcal{S} .

Sei \leq eine partielle Ordnung auf \mathcal{S} .

- Ein Element x ist eine *obere Schranke* für die Teilmenge Γ von \mathcal{S} , falls $\gamma \leq x$ für alle γ aus Γ .
- Ein Element x ist eine *untere Schranke* für die Teilmenge Γ von \mathcal{S} , falls $x \leq \gamma$ für alle γ aus Γ .
- Das Element x aus \mathcal{S} ist *maximal*, falls die einzige obere Schranke der Teilmenge $\{x\}$ von \mathcal{S} das Element x selbst ist. Oder äquivalent dazu, dass kein y aus \mathcal{S} mit $x < y$ existiert. Das Element x ist das größte Element der Teilmenge Γ , falls x in Γ liegt und $y \leq x$ für alle y aus Γ .
- Das Element x aus \mathcal{S} ist *minimal*, falls die einzige untere Schranke der Teilmenge $\{x\}$ von \mathcal{S} das Element x selbst ist. Oder äquivalent dazu, dass kein y aus \mathcal{S} mit $y < x$ existiert. Das Element x ist das kleinste Element der Teilmenge Γ , falls x in Γ liegt und $x \leq y$ für alle y aus Γ .
- Das Element a ist das *Supremum* (oder das *Oberste*) der Teilmenge Γ von \mathcal{S} , falls a die kleinste obere Schranke von Γ ist. Das Element a ist das *Maximum* von Γ , wenn a das Supremum von Γ ist und a in Γ liegt.
- Ein Element a ist das *Infimum* der Teilmenge Γ von \mathcal{S} , falls a die größte untere Schranke von Γ ist. Das Element a ist das *Minimum* von Γ , wenn a das Infimum von Γ ist und a in Γ liegt.
- Die Menge \mathcal{S} ist *induktiv*, falls jede linear geordnete Teilmenge eine obere Schranke in \mathcal{S} besitzt.

Bemerkung A.2. Beachte, dass jede induktive partiell geordnete Menge \mathcal{S} nicht-leer ist, da die leere Menge \emptyset linear geordnet ist und somit eine obere Schranke in \mathcal{S} besitzt (jedes Element aus \mathcal{S} ist eine obere Schranke für \emptyset).

Trotz des folgenden Namens ist das Zorn'sche Lemma eine Aussage der Mengenlehre, welche unabhängig vom Zermelo-Fraenkel-System und äquivalent zum *Auswahlsaxiom* ist.

Lemma A.3 (Zorn'sches Lemma). *Jede induktive partielle geordnete Menge (\mathcal{S}, \leq) besitzt ein maximales Element.*

Das Auswahlsaxiom von ZFC ist äquivalent zum Zorn'schen Lemma, sowie zum Wohlordnungssatz (vom Ernst Zermelo), der besagt, dass jede Menge wohlgeordnet werden kann (und somit ist sie in Bijektion mit einer Ordinalzahl, wegen des Satzes 3.30). Wir werden demnächst die Äquivalenz dieser Axiome zeigen.

Definition A.4. Eine *Familie* von Mengen $(X_i)_{i \in I}$, indiziert nach der nicht-leeren Menge I , ist eine Funktion F mit Definitionsbereich I derart, dass $X_i = F(i)$ für alle i aus I . Beachte, dass

$$\text{Im}(F) = \{X_i \mid i \in I\}$$

eine Menge bildet. Setze

$$\bigcup_{i \in I} X_i = \bigcup \{X_i \mid i \in I\}$$

und definiere das *kartesische Produkt* $\prod_{i \in I} X_i$ als die Menge aller Funktionen

$$f : I \rightarrow \bigcup_{i \in I} X_i$$

derart, dass $f(i)$ in X_i für jedes i aus I liegt.

Die Familie $(X_i)_{i \in I}$ ist eine *Zerlegung* der Menge X , falls

$$X = \bigcup_{i \in I} X_i$$

und $X_i \cap X_j = \emptyset$ für $i \neq j$ aus I .

Satz A.5. *In ZF sind folgende Aussagen äquivalent:*

- (a) *Das Auswahlsaxiom: $\forall x (\emptyset \notin x \rightarrow \exists f ((f : x \rightarrow \mathbb{V}) \wedge \forall y (y \in x \rightarrow f(y) \in y)))$*
- (b) *Für jede Zerlegung der Menge $X = \bigcup_{i \in I} X_i$ in nicht-leeren Mengen X_i gibt es eine Teilmenge Z von X derart, dass $Z \cap X_i$ aus einem einzigen Element für jedes i aus I besteht.*
- (c) *(Tychonoff) Das kartesische Produkt nicht-leerer Mengen ist nicht-leer.*
- (d) *(Zorn) Jede induktive partiell angeordnete Menge besitzt ein maximales Element.*
- (e) *(Wohlordnungssatz) Jede Menge läßt sich wohlordnen.*

Beachte, dass die obigen Aussagen mit Hilfe von \mathcal{L}_{ZF} -Aussagen ausdrückbar sind.

Beweis.

(a) \implies b): Sei $X = \bigcup_{i \in I} X_i$ eine Zerlegung in nicht-leere Mengen und f eine Auswahlfunktion auf $(\mathcal{P}(X) \setminus \{\emptyset\})$. Für jedes i aus I liegt das Element $f(X_i)$ in X_i . Wegen Ersetzung ist $Z = \{f(X_i) \mid i \in I\} \subset X$ eine Menge. Es genügt zu zeigen, dass $f(X_i)$ das einzige Element in $Z \cap X_i$ ist, was klar ist, denn $X_i \cap X_j$ ist leer für $i \neq j$.

(b) \implies c): Sei $\prod_{i \in I} X_i$ ein kartesisches Produkt nicht-leerer Mengen. Für jedes i aus I ist $Y_i = \{i\} \times X_i \neq \emptyset$ eindeutig bestimmt. Sei Z die durch die Zerlegung

$$Y = \bigcup_{i \in I} Y_i$$

gegebene Teilmenge von Y . Da $Z \cap Y_i$ eine Einermenge ist, ist wegen Ersetzung die Funktion $f : I \rightarrow \mathbb{V}$, so dass $f(i)$ die zweite Koordinate des einzigen Elementes von $Z \cap Y_i$ ist, wohldefiniert. Die Funktion f liegt in $\prod_{i \in I} X_i$.

c) \implies (a): Ohne Einschränkung können wir annehmen, dass $x \neq \emptyset$, denn sonst ist die leere Abbildung eine Auswahlfunktion. Die Menge $\prod_{y \in x} y$ ist ein kartesisches Produkt nicht-leerer Mengen, weil $\emptyset \notin x$. Aus dem Satz von Tychonoff folgt, dass es ein Element f in $\prod_{y \in x} y$ gibt, das heißt $f(y)$ ist in y für jedes y aus x , wie gewünscht.

(a) \implies (d): Für die induktive partiell angeordnete Menge (S, \leq) sei f eine Auswahlfunktion auf $(\mathcal{P}(S) \setminus \{\emptyset\})$. Mit Hilfe des Rekursionsatzes 3.33 definiere die Funktion

$$G : \text{On} \rightarrow S \cup \{S\}$$

$$\alpha \mapsto \begin{cases} f(\{x \in S \mid S \neq G(\beta) < x \text{ für alle } \beta < \alpha\}), & \text{falls die Menge} \\ & \{x \in S \mid S \neq G(\beta) < x \text{ für alle } \beta < \alpha\} \neq \emptyset \\ S, & \text{sonst.} \end{cases}$$

Beachte, dass $G(\underline{0}) \in S$. Ferner, falls $G(\alpha) \neq S$ für α aus On, ist $G(\alpha)$ ein Element der Menge $\{x \in S \mid S \neq G(\beta) < x \text{ für alle } \beta < \alpha\}$. Also $G(\alpha) > G(\beta)$ für alle $\beta < \alpha$ und $G(\beta) \neq S$. Weil S eine Menge ist und On eine echte Klasse, kann die Funktion G nicht injektiv sein. Also gibt es ein α in On mit $G(\alpha) = S$. Ohne Einschränkung sei α kleinstmöglich mit $G(\alpha) = S$. Insbesondere ist $\alpha \neq \underline{0}$. Falls α eine Limeszahl wäre, bildet die Teilmenge $\{G(\beta) \mid \beta < \alpha\}$ eine Kette ohne obere Schranke, denn die Menge

$$\{x \in S \mid S \neq G(\beta) < x \text{ für alle } \beta < \alpha\} = \emptyset.$$

Daraus folgt, dass $\alpha = S(\beta)$ für eine Ordinalzahl $\beta < \alpha$. Aus der Minimalität folgt, dass $G(\beta)$ ein Element aus S und echt größer als $G(\gamma)$ für $\gamma < \beta$ ist. Es genügt zu zeigen, dass $G(\beta)$ ein maximales Element aus S ist. Sonst gäbe es x aus S mit $x > G(\beta) > G(\gamma)$ für alle $\gamma < \beta$ und somit gehört x zu der Menge

$$\{y \in S \mid S \neq G(\beta) < y \text{ für alle } \beta < \alpha\} = \emptyset,$$

was den gewünschten Widerspruch liefert.

(d) \implies (e): Sei A eine beliebige Menge. Wenn A leer ist, ist sie trivialerweise wohlgeordnet, also können wir annehmen, dass $A \neq \emptyset$. Setze nun

$$S = \{(B, <_B) \mid (B \subset A \wedge (<_B \text{ ist eine Wohlordnung auf } B))\}.$$

Beachte, dass S eine nicht-leere Menge ist, denn (\emptyset, \emptyset) liegt in S . Wir definieren eine partielle Ordnung \preceq auf S :

$$(B, <_B) \preceq (C, <_C) \iff \begin{cases} B \subset C \text{ mit} \\ b <_C c \text{ f\"ur alle } b \in B \text{ und } c \in C \setminus B \text{ und} \\ <_B = <_C \cap B^2 \end{cases}$$

Die partielle Ordnung (S, \preceq) ist induktiv: Gegeben eine Kette Q aus S , falls Q leer ist, ist jedes Element von S eine obere Schranke. Falls Q nicht leer ist, sei

$$D = \bigcup_{(B, <_B) \in Q} B \text{ und } <_D = \bigcup_{(B, <_B) \in Q} <_B .$$

Die Ordnung $<_D$ ist klarerweise linear. Wir m\u00fcssen nur zeigen, dass $<_D$ fundiert auf D ist und somit $(D, <_D)$ eine obere Schranke der Kette Q ist. F\u00fcr $\emptyset \neq X \subset D$ gibt es ein $(B, <_B)$ aus Q mit $X \cap B \neq \emptyset$. Da $<_B$ eine Wohlordnung auf B ist, gibt es ein $<_B$ -kleinstes Element b in $X \cap B$. Wir m\u00fcssen zeigen, dass b auch $<_D$ -kleinstes Element in X ist. Sei c aus X mit $c \leq_D b$. Es gibt ein $(C, <_C)$ in Q derart, dass c in C liegt. Da Q linear angeordnet ist, sind $(B, <_B)$ und $(C, <_C)$ vergleichbar. Falls $(B, <_B) \preceq (C, <_C)$, folgt $c \leq_C b$ aus der Definition der Ordnung $<_D$. Also liegt c in B , wegen der Definition von \preceq . Da b das $<_B$ -kleinste Element aus $B \cap X$ ist, folgt $c = b$. Falls $(C, <_C) \preceq (B, <_B)$, folgt auch $c \leq_B b$ und somit $c = b$, wie gew\u00fcnscht.

Sei nun $(B, <_B)$ ein maximales Element bez\u00fcglich \preceq in S . Es bleibt noch zu zeigen, dass $B = A$. Ansonsten gibt es ein Element a in $A \setminus B$. Setze $C = B \cup \{a\}$ mit folgender Ordnung $<_C$: F\u00fcr Elemente aus B ist $<_C$ die Ordnung $<_B$ und sonst sind alle Elemente aus B echt kleiner als a bez\u00fcglich $<_C$. Diese Ordnung ist linear und fundiert, so $(B, <_B) \preceq (C, <_C)$, was der Maximalit\u00e4t von B widerspricht.

(e) \implies (b): Sei $X = \bigcup_{i \in I} X_i$ eine Zerlegung in nicht-leere Mengen und $<$ eine Wohlordnung auf X . F\u00fcr jedes i aus I ist das $<$ -kleinste Element x_i aus der nicht-leeren Teilmenge X_i eindeutig bestimmt. Also bildet wegen Ersetzung $\{x_i \mid i \in I\}$ eine Teilmenge Z von X . Da $X_i \cap X_j = \emptyset$ f\u00fcr $i \neq j$, ist $Z \cap X_i = \{x_i\}$.

□

B Cantorsche Normalform einer Ordinalzahl

Mit Hilfe des Rekursionssatzes definieren wir die *Exponentiation zur Basis ω* folgenderweise:

$$\omega^\alpha = \begin{cases} \underline{1}, & \text{f\u00fcr } \alpha = \underline{0} \\ \omega^\beta \cdot \omega, & \text{f\u00fcr } \alpha = S(\beta) \\ \sup_{\beta < \alpha} (\omega^\beta), & \text{f\u00fcr } \alpha \text{ Limeszahl} \end{cases}$$

Beachte, dass $\alpha \leq \omega^\alpha$ f\u00fcr jedes α aus On. Ferner ist die Exponentiation zur Basis ω streng monoton wachsend: f\u00fcr $\alpha < \beta$ ist $\omega^\alpha < \omega^\beta$.

Satz B.6 (Cantorsche Normalform). *Jede Ordinalzahl $\alpha \neq \underline{0}$ l\u00e4\u00dft sich eindeutig schreiben als*

$$\alpha = \omega^{\beta_1} \cdot \gamma_1 + \dots + \omega^{\beta_k} \cdot \gamma_k$$

f\u00fcr ein k aus \mathbb{N} , nat\u00fcrliche Zahlen $\gamma_1, \dots, \gamma_k$, welche alle ungleich $\underline{0}$ sind, und Ordinalzahlen $\beta_1 > \dots > \beta_k$, mit $\alpha \geq \beta_1$. Die Ordinalzahl α ist genau dann eine Limeszahl, wenn $\beta_k \neq \underline{0}$.

Beweis. Wir beweisen die Existenz einer solchen Darstellung induktiv über α . Für $\alpha = \underline{1}$ setze $k = 1$ mit $\beta_1 = \underline{0}$ und $\gamma_1 = \underline{1}$. Sei nun $\alpha > \underline{1}$ beliebig. Da $\alpha \leq \omega^\alpha < \omega^{S(\alpha)}$, sei $\beta \leq S(\alpha)$ die kleinste Ordinalzahl mit $\alpha < \omega^\beta$, welche wegen Lemma 3.20 (e) existiert. Da $\alpha > \underline{0}$, ist $\beta \neq \underline{0}$. Die Ordinalzahl β kann keine Limeszahl sein, denn sonst wäre $\alpha < \sup_{\gamma < \beta} \omega^\gamma$ und somit gäbe es ein $\gamma < \beta$ mit $\alpha < \omega^\gamma$, was der Minimalität von β widerspräche.

Schreibe $\beta = S(\beta_1)$, so $\omega^{\beta_1} \leq \alpha < \omega^{\beta_1} \cdot \omega$. Die Division mit Rest 3.38 liefert Ordinalzahlen γ und $\alpha' < \omega^{\beta_1} \leq \alpha$ mit $\alpha = \omega^{\beta_1} \cdot \gamma + \alpha'$. Um zu zeigen, dass γ eine natürliche Zahl ist, nehmen wir $\gamma \geq \omega$ an. Dann ist

$$\alpha \geq \omega^{\beta_1} \cdot \gamma \geq \omega^{\beta_1} \cdot \omega = \omega^\beta.$$

was ein Widerspruch zu $\alpha < \omega^\beta$ liefert. Das heißt, die Ordinalzahl γ gehört zu ω . Setze $\gamma_1 = \gamma$, also $\alpha = \omega^{\beta_1} \cdot \gamma_1 + \alpha'$ mit $\alpha' < \omega^{\beta_1} \leq \alpha$.

Die Induktionsannahme liefert, dass

$$\alpha' = \omega^{\beta_2} \cdot \gamma_2 + \dots + \omega^{\beta_k} \cdot \gamma_k$$

mit $\beta_2 > \dots > \beta_k$. Wir müssen nur noch zeigen, dass $\beta_1 > \beta_2$. Ansonsten wäre $\beta_1 \leq \beta_2$, was folgenden Widerspruch liefert:

$$\omega^{\beta_1} > \alpha' \geq \omega^{\beta_2} \geq \omega^{\beta_1}.$$

Für die Eindeutigkeit, sei χ die Teilklasse der Ordinalzahlen, welche eine eindeutige Cantorsche Normalform besitzen. Wegen dem Induktionsprinzip 3.21 genügt es zu zeigen, dass α in χ liegt, wenn $\alpha \subset \chi$ ist. Sei

$$\alpha = \omega^{\beta'_1} \cdot \gamma'_1 + \dots + \omega^{\beta'_r} \cdot \gamma'_r$$

eine andere Darstellung für ein r aus \mathbb{N} . Klarerweise ist

$$\omega^{\beta_1} \leq \alpha \leq \omega^{\beta'_1} \cdot \gamma'_1 + \dots + \omega^{\beta'_1} \cdot \gamma'_r = \omega^{\beta'_1} (\gamma'_1 + \dots + \gamma'_r) < \omega^{\beta'_1} \cdot \omega = \omega^{S(\beta'_1)},$$

also $\beta_1 \leq \beta'_1$. Aus symmetrischen Gründen ist $\beta'_1 \leq \beta_1$, also $\beta_1 = \beta'_1$. Aus der Eindeutigkeit bei der Division mit Rest 3.38 ergibt sich nun sofort $\gamma_1 = \gamma'_1$ und

$$\omega^{\beta_2} \cdot \gamma_2 + \dots + \omega^{\beta_k} \cdot \gamma_k = \omega^{\beta'_2} \cdot \gamma'_2 + \dots + \omega^{\beta'_r} \cdot \gamma'_r.$$

Die Ordinalzahl $\delta = \omega^{\beta_2} \cdot \gamma_2 + \dots + \omega^{\beta_k} \cdot \gamma_k$ liegt in α , weil

$$\omega^{\beta_2} \cdot \gamma_2 + \dots + \omega^{\beta_k} \cdot \gamma_k \leq \omega^{\beta_2} (\gamma_2 + \dots + \gamma_k) < \omega^{\beta_2} \cdot \omega = \omega^{S(\beta_2)} \leq \omega^{\beta_1} \leq \alpha.$$

Insbesondere liegt δ in χ und somit sind $\beta_i = \beta'_i$ und $\gamma_i = \gamma'_i$ für jedes $2 \leq i \leq r = k$. □

Definiere nun rekursiv für γ aus ω die Folge

$$\alpha_\gamma = \omega^{\overbrace{\omega^{\dots \omega}^\omega}^\gamma \text{ Mal}}$$

Das heißt,

$$\alpha_\gamma = \begin{cases} \underline{1}, & \text{falls } \gamma = \underline{0}. \\ \omega^{\alpha_{\gamma'}}, & \text{falls } \gamma = S(\gamma') \end{cases}$$

Setze $\epsilon_0 = \sup_{\gamma \in \omega} \alpha_\gamma$ und beachte, dass $\omega^{\epsilon_0} = \epsilon_0$.

Korollar B.7. Jede Ordinalzahl α mit $\underline{0} < \alpha < \epsilon_0$ lässt sich eindeutig schreiben, als

$$\alpha = \omega^{\beta_k} \cdot S(\beta),$$

für eine Ordinalzahl $\beta < \alpha$, wobei β_k die kleinste Potenz von ω in der cantorschen Normalform von α ist.

Beweis. Die Eindeutigkeit lässt sich einfach zeigen. Für die Existenz sei

$$\alpha = \omega^{\beta_1} \cdot \gamma_1 + \dots + \omega^{\beta_k} \cdot \gamma_k,$$

mit $\beta_1 > \dots > \beta_k$ und jedes γ_i ungleich $\underline{0}$. Mit Hilfe des Korollars 3.37 schreibe $\beta_i = \beta_k + \beta'_i$ und $\gamma_k = S(\gamma'_k)$. Also

$$\alpha = \omega^{\beta_k} \cdot (\omega^{\beta'_1} \cdot \gamma_1 + \dots + \omega^{\beta'_{k-1}} \cdot \gamma_{k-1} + S(\gamma'_k)) = \omega^{\beta_k} \cdot S(\beta),$$

für

$$\beta = \omega^{\beta'_1} \cdot \gamma_1 + \dots + \omega^{\beta'_{k-1}} \cdot \gamma_{k-1} + \gamma'_k.$$

Da $\gamma'_k < \gamma_k$ folgt, dass $\beta < \alpha$. □

Die Bedingung $\alpha < \epsilon_0$ ist notwendig, denn $\epsilon_0 \neq \omega^{\epsilon_0} \cdot S(\beta)$ für jede Ordinalzahl $\beta \neq \underline{0}$.

C Ultrafilter und -produkte

In diesem Abschnitt geben wir einen alternative Beweis des Kompaktheitssatzes mit Hilfe von Ultraprodukten.

Sei I eine feste nicht-leere Menge.

Definition C.1. Ein *Filter* \mathcal{F} ist eine nicht-leere Kollektion von Teilmengen von I mit folgenden Eigenschaften:

- (1) $\emptyset \notin \mathcal{F}$.
- (2) Falls X und Y in \mathcal{F} liegen, dann liegt auch $X \cap Y$ in \mathcal{F} .
- (3) Falls X in \mathcal{F} liegt und $X \subset Y \subset I$, dann liegt auch Y in \mathcal{F} .

Beachte, dass wegen (3) die Menge I in \mathcal{F} liegen muss, weil \mathcal{F} nicht-leer ist.

Eine *Filterbasis* \mathcal{B} ist eine nicht-leere Kollektion von Teilmengen von I derart, dass \emptyset nicht in \mathcal{B} enthalten und \mathcal{B} unter endlichen Durschnitten abgeschlossen ist.

Bemerkung C.2. Jede Filterbasis \mathcal{B} bestimmt einen Filter. Setze

$$\mathcal{F}_{\mathcal{B}} = \{X \subset I \mid \exists B \in \mathcal{B} \text{ mit } B \subset X\}.$$

Insbesondere ist für $\emptyset \neq Z \subset I$ die Menge $\{Z\}$ eine Filterbasis. Der entsprechende Filter F_Z ist der von Z erzeugte Filter. Ein Filter, der von einer Menge erzeugt wird ist ein *Hauptfilter*. Sonst ist der Filter *generisch*.

Definition C.3. Ein *Ultrafilter* \mathcal{U} ist ein maximaler Filter bezüglich Inklusion.

Da jeder Filter unter endlichen Durchschnitten abgeschlossen ist, kann es nicht passieren, dass für eine Teilmenge $X \subset I$ sowohl X als auch $I \setminus X$ in \mathcal{U} liegen.

Bemerkung C.4. Ein Filter \mathcal{U} ist genau dann ein Ultrafilter, wenn er zusätzlich folgende Eigenschaft besitzt:

(4) Für $X \subset I$ liegt entweder X oder $I \setminus X$ in \mathcal{U} .

Beweis. Sei \mathcal{U} ein Ultrafilter und $X \subset I$ eine Menge, welche nicht in \mathcal{U} liegt. Setze

$$\mathcal{B} = \{X \cap Z\}_{Z \in \mathcal{U}}.$$

Beachte, dass X in \mathcal{B} liegt, denn I liegt in \mathcal{U} . Ferner, weil \mathcal{U} unter endlichen Durchschnitten abgeschlossen ist, trifft dies auch auf \mathcal{B} zu. Wenn \mathcal{B} eine Filterbasis wäre, würde der Filter $\mathcal{F}_{\mathcal{B}}$ den Filter \mathcal{U} echt enthalten, was der Maximalität von \mathcal{U} widersprechen würde. Es folgt, dass \emptyset in \mathcal{B} liegt. Das heißt, es gibt eine Menge Z aus \mathcal{U} mit $Z \cap X = \emptyset$, also $Z \subset I \setminus X$. Aus der Eigenschaft (3) folgt, dass $I \setminus X$ in \mathcal{U} liegt.

Angenommen, dass \mathcal{U} ein Filter mit der Zusatzeigenschaft (4) ist, müssen wir zeigen, dass \mathcal{U} maximal ist. Falls \mathcal{F} ein Filter wäre, der \mathcal{U} echt enthält, gäbe es eine Teilmenge X in $\mathcal{F} \setminus \mathcal{U}$. Dann liegt $I \setminus X$ in \mathcal{U} und somit in \mathcal{F} . Weil $\emptyset = X \cap I \setminus X$, kann \mathcal{F} kein Filter sein. \square

Bemerkung C.5. Falls $X \cup Y$ in einem Ultrafilter \mathcal{U} liegt, dann liegt X oder Y in \mathcal{U} .

Wir können \mathcal{U} als ein endlich additives Maß auf I betrachten, welches nur die Werte 0 und 1 annimmt. Die Elemente aus \mathcal{U} sind genau die Teilmengen von I mit Maß 1.

Bemerkung C.6. Jeder Hauptultrafilter wird von einer Einermenge erzeugt: Angenommen, dass der Ultrafilter \mathcal{U} von der Menge Z erzeugt ist, folgt, dass jede Teilmenge X aus I genau dann in \mathcal{U} liegt, wenn $Z \subset X$. Weil $Z \neq \emptyset$, gibt es ein Element x aus Z . Beachte, dass $I \setminus \{x\}$ nicht in \mathcal{U} liegen kann, denn $Z \not\subset I \setminus \{x\}$. Also liegt $\{x\}$ in \mathcal{U} und $Z = \{x\}$, wie gewünscht.

Falls I unendlich ist, ist der *Fréchetfilter*

$$\mathcal{F}_{\text{Fréchet}} = \{X \subset I \mid I \setminus X \text{ endlich}\}.$$

Jeder Ultrafilter, der $\mathcal{F}_{\text{Fréchet}}$ enthält muss generisch sein.

Aus dem Zorn'schen Lemma (siehe Appendix A) folgt die Existenz von Ultrafiltern.

Lemma C.7. Die Vereinigung einer steigenden Kette von Filtern ist wiederum ein Filter. Insbesondere gibt es Ultrafilter auf jeder nicht-leeren Menge.

Wenn die Menge I unendlich ist, gibt es generische Ultrafilter auf I .

Sei nun $(A_i)_{i \in I}$ eine Kollektion nicht-leerer Mengen A_i . Jeder Filter \mathcal{F} auf I definiert auf folgende Weise eine Äquivalenzrelation $\sim_{\mathcal{F}}$ auf $\prod_{i \in I} A_i$:

$$(a_i)_{i \in I} \sim_{\mathcal{F}} (b_i)_{i \in I} \iff \{i \in I \mid a_i = b_i\} \in \mathcal{F}.$$

Wir bezeichnen mit $[(a)_{i \in I}]_{\mathcal{F}}$ die $\sim_{\mathcal{F}}$ -Äquivalenzklasse der Folge $(a_i)_{i \in I}$ und mit $\prod_{\mathcal{F}} A_i$ die Kollektion der $\sim_{\mathcal{F}}$ -Äquivalenzklassen aus $\prod_{i \in I} A_i$.

Sei n aus \mathbb{N} . Wenn wir für jedes i aus I eine n -stellige Funktionen $f_i : A_i^n \rightarrow A_i$ haben, bekommen wir wie folgt eine wohldefinierte Funktion:

$$(f)_{\mathcal{F}}^I : \prod_{\mathcal{F}} A_i \times \dots \times \prod_{\mathcal{F}} A_i \rightarrow \prod_{\mathcal{F}} A_i, \\ (([a^1]_{i \in I}]_{\mathcal{F}}, \dots, [(a^n]_{i \in I}]_{\mathcal{F}}) \mapsto [(f_i(a_i^1, \dots, a_i^n))]_{i \in I}]_{\mathcal{F}}$$

Definition C.8. Sei \mathcal{L} eine Sprache und $(\mathcal{A}_i)_{i \in I}$ eine Kollektion von \mathcal{L} -Strukturen indiziert durch die Menge I . Gegeben einen Ultrafilter \mathcal{U} auf I , ist das *Ultraprodukt* $\prod_{\mathcal{U}} \mathcal{A}_i$ von $(\mathcal{A}_i)_{i \in I}$ die \mathcal{L} -Struktur mit Universum $\prod_{\mathcal{U}} A_i$, wobei A_i das Universum der \mathcal{L} -Struktur \mathcal{A}_i ist, und folgenden Interpretationen:

- Für jedes Konstantenzeiche c aus \mathcal{L} setze $c^{\prod_{\mathcal{U}} \mathcal{A}_i} = [(c^{\mathcal{A}_i})_I]_{\mathcal{U}}$.
- Für jedes n -stellige Funktionszeichen f aus \mathcal{L} setze $f^{\prod_{\mathcal{U}} \mathcal{A}_i} = (f^{\mathcal{A}_i})_{\mathcal{U}}^I$.
- Für jedes m -stellige Relationszeichen R aus \mathcal{L} definiere

$$([(a^1)_I]_{\mathcal{U}}, \dots, [(a^m)_I]_{\mathcal{U}}) \in R^{\prod_{\mathcal{U}} \mathcal{A}_i} \iff \{i \in I \mid (a_i^1, \dots, a_i^m) \in R^{\mathcal{A}_i}\} \in \mathcal{U}.$$

Beachte, dass die obige Interpretationen wohldefiniert sind.

Die *Ultrapotenz* $\mathcal{A}^{\mathcal{U}}$ einer \mathcal{L} -Struktur \mathcal{A} ist das Ultraprodukt $\prod_{\mathcal{U}} \mathcal{A}$ der konstanten Kollektion $(\mathcal{A})_{i \in I}$.

Satz C.9 (Łoś). Sei $\prod_{\mathcal{U}} \mathcal{A}_i$ das Ultraprodukt der \mathcal{L} -Strukturen $(\mathcal{A}_i)_{i \in I}$ bezüglich des Ultrafilters \mathcal{U} auf I . Für jede Formel $\varphi[x_1, \dots, x_n]$ und Elemente $[(a^1)_I]_{\mathcal{U}}, \dots, [(a^n)_I]_{\mathcal{U}}$ aus $\prod_{\mathcal{U}} \mathcal{A}_i$,

$$\prod_{\mathcal{U}} \mathcal{A}_i \models \varphi([(a^1)_I]_{\mathcal{U}}, \dots, [(a^n)_I]_{\mathcal{U}}) \iff \{i \in I \mid \mathcal{A}_i \models \varphi[a_i^1, \dots, a_i^n]\} \in \mathcal{U}.$$

Insbesondere ist die Ultrapotenz $\mathcal{A}^{\mathcal{U}}$ eine elementare Erweiterung von \mathcal{A} bezüglich der konstanten Einbettung

$$\begin{aligned} A &\rightarrow \prod_{\mathcal{U}} A, \\ a &\rightarrow [(a)_I]_{\mathcal{U}} \end{aligned}$$

Beweis. Für atomare Formeln folgt die Behauptung aus der Definition der \mathcal{L} -Struktur $\prod_{\mathcal{U}} \mathcal{A}_i$. Der Falls $\varphi = \neg\psi$ folgt induktiv aus der folgenden Bemerkung:

$$\{i \in I \mid \mathcal{A}_i \models \psi[a_i^1, \dots, a_i^n]\} \notin \mathcal{U} \iff \{i \in I \mid \mathcal{A}_i \models \neg\psi[a_i^1, \dots, a_i^n]\} \in \mathcal{U}$$

weil \mathcal{U} ein Ultrafilter ist. Dementsprechend zeigt man den Fall, wenn φ eine Disjunktion zweier Formeln ist.

Falls $\varphi[x_1, \dots, x_n] = \exists y \psi[x_1, \dots, x_n, y]$, folgt eine Richtung sofort aus der Induktionsannahme für ψ . Für die andere Richtung, angenommen dass die Menge

$$X = \{i \in I \mid \mathcal{A}_i \models \exists y \psi[a_i^1, \dots, a_i^n, y]\}$$

in \mathcal{U} liegt, gibt es für i aus X ein Element b_i aus A_i mit $\mathcal{A}_i \models \psi[a_i^1, \dots, a_i^n, b_i]$. Für j nicht in X , sei b_j ein beliebiges Element aus A_j . Für das Element $[(b)_I]_{\mathcal{U}}$ gilt nun, dass

$$\{i \in I \mid \mathcal{A}_i \models \psi[a_i^1, \dots, a_i^n, b_i]\} \in \mathcal{U},$$

denn es ist eine Obermenge von X . Damit haben wir $\prod_{\mathcal{U}} \mathcal{A}_i \models \psi([(a^1)_I]_{\mathcal{U}}, \dots, [(a^n)_I]_{\mathcal{U}}, [(b)_I]_{\mathcal{U}})$ und somit $\prod_{\mathcal{U}} \mathcal{A}_i \models \varphi([(a^1)_I]_{\mathcal{U}}, \dots, [(a^n)_I]_{\mathcal{U}})$.

Die letzte Behauptung folgt, weil I in \mathcal{U} liegt und jede Menge aus \mathcal{U} nicht-leer ist. \square

Korollar C.10. Falls \mathcal{U} ein Hauptultrafilter ist, welcher vom Element i_0 aus I erzeugt wird, ist $\prod_{\mathcal{U}} \mathcal{A}_i$ isomorph zu \mathcal{A}_{i_0} .

Der Satz von Łoś liefert einen alternativen Beweis des Kompaktheitssatzes 2.66.

Korollar C.11 (Kompaktheitssatz). *Eine Theorie T in der Sprache \mathcal{L} ist genau dann konsistent, wenn jede endliche Teilmenge von T konsistent ist.*

Beweis. Wir müssen nur eine Richtung zeigen. Sei I die Kollektion aller nicht-leeren endlichen Teilmengen von T . Jedes s aus I besitzt ein Modell, das heißt, es gibt eine \mathcal{L} -Struktur \mathcal{A}_s mit $\mathcal{A}_s \models \bigwedge_{\chi \in s} \chi$.

Setze $B_s = \{t \in I \mid \mathcal{A}_t \models \bigwedge_{\chi \in s} \chi\}$. Klarerweise ist $s \in B_s \neq \emptyset$. Ferner ist $B_s \cap B_t = B_{s \cup t}$, also ist $\mathcal{B} = (B_s)_{s \in I}$ eine Filterbasis. Wegen Lemma C.7 gibt es einen Ultrafilter \mathcal{U} , welcher alle Teilmengen B_s enthält. Setze $\mathcal{A} = \prod_{\mathcal{U}} \mathcal{A}_s$. Wir müssen nur zeigen, dass \mathcal{A} ein Modell von T ist. Gegeben eine Aussage χ aus T , ist

$$B_\chi = \{s \in I \mid \mathcal{A}_s \models \chi\} \in \mathcal{U},$$

also $\mathcal{A} \models \chi$, wegen des Satzes C.9, wie gewünscht. □

D Der chinesische Restsatz

Sei $\mathbb{Z}/n\mathbb{Z}$ die endliche abelsche Gruppe der Restklassen modulo $n \geq 0$ mit kanonischen Repräsentanten $\{\bar{0}, \dots, \overline{n-1}\}$.

Satz D.1. *Gegeben paarweise teilerfremde natürliche Zahlen n_1, \dots, n_k , gilt*

$$\mathbb{Z}/N\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z},$$

wobei $N = \prod_{i=1}^k n_i$.

Beweis. Weil N von jedem n_i geteilt wird, ist die Abbildung

$$\begin{aligned} \varphi: \mathbb{Z}/N\mathbb{Z} &\rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z} \\ x + N\mathbb{Z} &\mapsto (x + n_1\mathbb{Z}, \dots, x + n_k\mathbb{Z}) \end{aligned}$$

wohldefiniert. Ferner ist φ ein Gruppenhomomorphismus. Um zu beweisen, dass φ ein Isomorphismus ist, genügt es zu zeigen, dass die Abbildung injektiv ist, weil beide Gruppen die gleiche Kardinalität N haben. Sei x eine Zahl mit $\varphi(x) = (\bar{0}, \dots, \bar{0})$. Dies bedeutet $x \equiv \bar{0} \pmod{n_i}$ für jedes $i \leq k$, das heißt, n_i teilt x . Da die Zahlen n_1, \dots, n_k paarweise teilerfremd sind, folgt, dass $N = \prod_{i=1}^k n_i$ das Element x teilt und somit $\bar{x} = \bar{0}$ in $\mathbb{Z}/N\mathbb{Z}$ ist, wie gewünscht. □

Literaturverzeichnis

- [1] M. Junker, *Logik fr Studierende der Informatik*, Skript, (2017), <http://home.mathematik.uni-freiburg.de/junker/skripte/InfoLogik.pdf>
- [2] K. Tent, M. Ziegler, *A course in model theory*, Lecture Notes in Logic **40**, (2012), pp. x+248, ISBN 978-0-521-76324-0.
- [3] M. Ziegler, *Logik fr Informatiker*, Skript, (2013), <http://home.mathematik.uni-freiburg.de/ziegler/skripte/lfi.pdf>