

# Mathematische Logik

Heike Mildenberger

Fassung vom 09.07.2024



# Inhaltsverzeichnis

Vorwort . . . . .	5
<b>1 Die Logik der ersten Stufe – Prädikatenlogik</b>	<b>7</b>
1.1 Symbolmengen, Formeln und Strukturen . . . . .	7
1.2 Semantik, das Wahrheitsprädikat $\models$ . . . . .	11
1.3 Allgemeingültige Formeln . . . . .	16
1.3.1 Exkurs über Boole'sche Algebren . . . . .	18
1.4 Der Gödel'sche Vollständigkeitssatz . . . . .	20
1.5 Elementare Äquivalenz . . . . .	30
<b>2 Mengenlehre</b>	<b>33</b>
2.1 Das Axiomensystem von Zermelo und Fraenkel . . . . .	33
2.1.1 Exkurs über definitorische Spracherweiterungen . . . . .	37
2.2 Die ordinale Addition, Multiplikation und Exponentiation . . . . .	49
2.3 Kardinalzahlen . . . . .	50
2.4 Metamathematik von ZFC . . . . .	54
2.5 Rosser-Sätze . . . . .	58
<b>3 Rekursionstheorie</b>	<b>59</b>
3.1 $\mu$ -rekursive Funktionen und Registermaschinen . . . . .	60
3.2 Primitiv rekursive Funktionen und Prädikate . . . . .	66
3.3 Gödelisierung von Registermaschinen . . . . .	69
3.4 Rekursiv aufzählbare Mengen und partielle rekursive Funktionen . . . . .	72
3.4.1 Exkurs über die Ackermannfunktion . . . . .	74
3.5 Gödelnummern von Formeln . . . . .	76
3.6 Ein anderer Aufbau der Menge der rekursiven Funktionen . . . . .	79
<b>4 Arithmetik</b>	<b>83</b>
4.1 Definierbare, rekursiv aufzählbare und rekursive Teilmengen . . . . .	83
4.2 Cobhams unentscheidbare Theorie $Q^*$ , Robinsons Theorie $Q$ . . . . .	86
4.3 Das Entscheidungsproblem . . . . .	88
4.4 Der Fixpunktsatz für $Q^*$ . . . . .	91

4.5	Die Peanoarithmetik . . . . .	92
4.6	Der zweite Gödel'sche Unvollständigkeitssatz für $P$ . . . . .	96
	<b>Literaturverzeichnis</b>	<b>101</b>
	<b>Stichwortverzeichnis</b>	<b>103</b>

## Vorwort

Dies ist das Skript zur Logik-Vorlesung aus dem Sommersemester 2021 von Heike Mildenberger.

Ich danke Herrn Kai Sickinger für eine  $\text{\LaTeX}$ -Datei meiner Vorlesung aus dem Sommersemester 2018 und insbesondere für die zahlreichen tikz-Bilder. Die vorliegende Version ist eine für die Fern-Lehre um etliche Erläuterungen ergänzte Fassung vom Frühjahr 2020, die ich im Frühjahr 2021 nochmals ergänzte. Bitte seien Sie vorsichtig, es können immer noch Fehler im Skript sein. Wenn Sie einen Fehler finden, schreiben Sie mir bitte eine Mail.

### *Empfohlene Literatur*

Der Klassiker unter den Logik-Büchern ist das Buch von Shoenfield, *Mathematical Logic* [5]. Die Vorlesung lehnt sich (außer im Mengenlehre-Kapitel) eng an das Buch von Ziegler [6] an. Alternative Kalküle findet man in den Büchern von Ebbinghaus, Flum und Thomas [1]. Eine langsamer vorgehende Darstellung findet ist in Endertons [2].



# Kapitel 1

## Die Logik der ersten Stufe – Prädikatenlogik

### 1.1 Symbolmengen, Formeln und Strukturen

Wir beginnen mit dem recht engen Strukturbegriff aus der Modelltheorie. Natürlich gibt es auch mathematische Strukturen, zum Beispiel topologische Räume, die keine Strukturen im Sinne dieser Vorlesung sein werden. In allgemeinerem Kontext kann man die Strukturen aus dieser Vorlesung „erststufige Strukturen“ nennen. Die Stufen zählen grob, wo die Interpretation der Variablen (wie z.B.  $x, y, z \dots$ ) liegen. In der ersten Stufe rangieren die Variablen über die Elemente der Trägermenge, in der zweiten Stufe auch über die Potenzmenge, usf. Gängig sind die erste Stufe, die zweite Stufe und dann abzählbar unendlich viele Stufen oder gleich beliebig viele Stufen.

**Definition 1.1.1** (Symbolmenge). Eine Symbolmenge  $L$  oder  $\tau$  besteht aus Konstantensymbolen (z.B.  $e, 0, 1$ ), Funktionssymbolen mit einer Stelligkeit (z.B.  $+, -, S, \cdot$ ), und Relationssymbolen mit einer Stelligkeit (z.B.  $<, \epsilon, \subseteq$ ). Die Menge  $L$  wird auch Sprache — daher das  $L$  von language — oder Signatur genannt. Oft wird auch der Buchstabe  $\tau$  für die Symbolmenge benutzt, da man  $L$  und  $\mathcal{L}$  gerne als Symbole frei halten möchte.

Streng genommen handelt es sich bei der Symbolmenge nicht nur um die Menge, sondern um die Menge mit einer Abbildung, die jedes Element als Konstantensymbol oder als Relationssymbol einer bestimmten Stelligkeit oder als Funktionssymbol einer bestimmten Stelligkeit klassifiziert. Das Funktionssymbol  $S$  soll an successor – Nachfolger erinnern.

*Beispiele 1.1.2.*

$L_\emptyset$	$= \emptyset$	die leere Sprache,
$L_R$	$= \{0, 1, +, -, \cdot\}$	die Ring-Sprache,
$L_G$	$= \{e, \circ, ^{-1}\}$	die Gruppen-Sprache
$L_O$	$= \{<\}$	die Ordnungs-Sprache,
$L_{AK}$	$= \{0, 1, +, -, \cdot, <\}$	die Sprache der angeordneten Körper,
$L_N$	$= \{0, S, +, \cdot, <\}$	die Sprache der natürlichen Zahlen mit Nachfolgerfunktion $S$ ,
$L_{Me}$	$= \{\in\}$	die Mengenlehre-Sprache.

Sei  $L$  eine Menge und sei für  $Z \in L$ ,  $F_Z$  eine Menge. Die Schreibweise  $(F_Z)_{Z \in L}$  ist eine Kurzschreibweise für die Funktion  $\{(Z, F_Z) : Z \in L\}$ . Statt Funktion kann man auch Familie sagen. Im Folgenden schreibt man sogar  $Z^F$  statt  $F_Z$ , und statt  $F$  hat sich ein gothisches oder kalligraphisches  $\mathfrak{A}$  eingebürgert.

**Definition 1.1.3** ( $L$ -Struktur). Eine  $L$ -Struktur ist ein Paar  $\mathfrak{A} = (A, (Z^{\mathfrak{A}})_{Z \in L})$  mit folgenden Eigenschaften:

$A \neq \emptyset$  ist eine Menge, die Träger der Struktur genannt wird.  $(Z^{\mathfrak{A}})_{Z \in L}$  ist eine Familie/Funktion, so dass für

jedes	Konstantensymbol	$Z \in L$ gilt:	$Z^{\mathfrak{A}} \in A$ ;
jedes	$n$ -stellige Funktionssymbol	$Z \in L$ gilt:	$Z^{\mathfrak{A}} : A^n \rightarrow A$ ;
jedes	$n$ -stellige Relationssymbol	$Z \in L$ gilt:	$Z^{\mathfrak{A}} \subseteq A^n$ .

Also  $(R, +, \cdot) \neq (R, \cdot, +)$ , da jede Familie mit einer festen Stellenbestimmung der Argumente einher geht.

Jede Struktur bestimmt eindeutig ihre Signatur. Wir können daher folgendes definieren.

**Definition 1.1.4.** Wenn  $\mathfrak{A}$  eine  $L$ -Struktur ist, so schreiben wir  $L_{\mathfrak{A}} = L$  und sagen  $L$  sei die Sprache (oder Signatur oder Symbolmenge) von  $\mathfrak{A}$ .

*Beispiele 1.1.5.* Folgendes sind Strukturen, Mengen mit Relation, Operationen und Konstanten verschiedenen Typs:

eine Gruppe:	$(G, \circ, e, ^{-1})$	genauer $\mathfrak{G} = (G, \circ^{\mathfrak{G}}, e^{\mathfrak{G}}, ^{-1\mathfrak{G}})$
ein Ring:	$(R, +, \cdot, 0, 1)$	
eine (lineare oder partielle) Ordnung:	$(L, <)$	
eine Menge $\mathfrak{A}$ :	$(M, \in)$	
die natürlichen Zahlen:	$(\mathbb{N}, +, \cdot, 0, 1, <, S)$	

**Definition 1.1.6** (Isomorphe  $L$ -Strukturen). Zwei  $L$ -Strukturen heißen isomorph  $\mathfrak{A} \cong \mathfrak{B}$ , wenn es einen Isomorphismus  $f : \mathfrak{A} \cong \mathfrak{B}$  gibt, das heißt  $f : A \rightarrow B$  ist bijektiv und erfüllt folgende Gesetze

$$\begin{aligned}
 f(Z^{\mathfrak{A}}) &= Z^{\mathfrak{B}} && \text{für jedes Konstantenzeichen } Z \in L, \\
 f(Z^{\mathfrak{A}}(a_0, \dots, a_{n-1})) &= Z^{\mathfrak{B}}(f(a_0), \dots, f(a_{n-1})) && \text{für jedes Operationszeichen } Z \in L, \\
 Z^{\mathfrak{A}}(a_0, \dots, a_{n-1}) &\Leftrightarrow Z^{\mathfrak{B}}(f(a_0), \dots, f(a_{n-1})) && \text{für jedes Relationszeichen } Z \in L.
 \end{aligned}$$



**Definition 1.1.7** (*L*-Term). Die Menge der *L*-Terme ist die kleinste Menge, die durch die folgenden Regeln bestimmt ist

T1 Jede Variable ist ein *L*-Term. Variablen sind  $v_0, v_1, \dots$

T2 Jedes Konstantenzeichen ist ein *L*-Term.

T3 Wenn  $t_0, \dots, t_{n-1}$  *L*-Terme sind und  $f \in L$  ein  $n$ -stelliges Funktionszeichen ist, dann ist  $ft_0 \dots t_{n-1}$  ein *L*-Term.

*Bemerkung 1.1.8.* Hierbei ist  $ft_0 \dots t_{n-1}$  die polnische Notation. Zum Beispiel für die zwei-stelligen Funktionszeichen  $f = +$ ,  $g = \cdot$ , die Konstante 4 und die Variablen  $x, y$  kann den Term  $g4fxy = \cdot 4 + xy$  ohne Klammern schreiben. Da  $+453$  nicht eindeutig lesbar ist, haben unsere gängigen Schreibweisen, z.B.  $4 \cdot (x + y)$ ,  $45 + 3$ , auch Vorteile. Das Lemma unten über die eindeutige Lesbarkeit der Terme braucht als eine Grundvoraussetzung, dass es nicht zwei Symbole  $c_0, c_1$  gibt, so dass  $c_0c_1$  das Zeichen einer weiteres Symbol ist. (Dieses gilt zum Beispiel auch für das deutsche Alphabet.) In unserem Stellenwertsystem können also nicht die Zahlen, sondern nur die Ziffern als Konstanten dienen. Wir verwenden die Termschreibweise nach Regel T3 hier für unsere grundsätzlichen Betrachtungen.

**Definition 1.1.9** (Anfangsstück). Eine Zeichenreihe  $s$  ist ein Anfangsstück einer Zeichenreihe  $t$ ,  $s \triangleleft t$ , wenn es Zeichen  $z_0, \dots, z_{n-1}, z_n, \dots, z_{m-1}$  gibt, so dass  $n \leq m$  und jedes  $z_i$  eine Variable (jede Variable, zB  $v_{100}$ , zählt in dieser Abstraktion als ein Zeichen, nicht etwa als vier Zeichen), Konstante, oder ein Funktionszeichen ist und

$$\begin{aligned} s &= z_0 \dots z_{n-1}; \\ t &= z_0 \dots z_{n-1} z_n \dots z_{m-1}. \end{aligned}$$

$s$  heißt echtes Anfangsstück von  $t$ ,  $s \triangleleft t$ ,  $s \triangleleft t \wedge s \neq t$ .

**Lemma 1.1.10.** *Kein L-Term ist ein echtes Anfangsstück eines anderen L-Terms.*

*Beweis:* Wir zeigen durch Induktion über  $|t|$ , dass für jeden Term  $s \triangleleft t$  die Gleichheit  $s = t$  gilt. Wenn  $t$  eine Variable oder ein Konstantenzeichen ist, so ist  $s = t$ . Sei  $fs_0 \dots s_{n-1} = s$ ,  $gt_0 \dots t_{m-1} = t$ . Da  $s \triangleleft t$  ist  $f = g$  und daher  $n = m$ . Wir nehmen nun  $s \triangleleft t$  an. Dann gibt es ein kleinstes  $i$ , so dass  $s_i \neq t_i$ .

$$\begin{array}{ccccccc} \underline{s_i} & \underline{s_{i+1}} & \dots & \dots & \dots & \dots & \underline{s_{n-1}} \\ \hline \underline{t_i} & \underline{t_{i+1}} & \dots & \dots & \dots & \dots & \underline{t_{n-1}} \end{array}$$

Dann ist  $s_i \triangleleft t_i$  oder  $t_i \triangleleft s_i$ , denn es gilt  $s_{i+1} \dots s_{n-1} \triangleleft t_{i+1} \dots t_{n-1}$ . Da sowohl  $t_i$  als auch  $s_i$  kürzer als  $t$  sind, widerspricht " $s_i \triangleleft t_i$  oder  $t_i \triangleleft s_i$ " der Induktionsvoraussetzung. Also ist für  $i < n$ ,  $s_i = t_i$ .  $\square$

**Lemma 1.1.11.** *Die  $L$ -Terme sind eindeutig lesbar. Das heißt ausführlich: Jeder Term  $t$  ist entweder eine Variable, eine Konstante oder von der Form  $t = ft_0 \dots t_n$ . Im letzteren Fall ist die Zerlegung eindeutig: Ist  $ft_0 \dots t_{n-1} = gs_0 \dots s_{m-1}$ , so folgt schon*

$$f = g \text{ und} \quad n = m \text{ und} \quad \text{für } 0 \leq i < n, t_i = s_i$$

*Beweis:* Man zeigt induktiv über die Länge von  $t$ , dass  $t$  eindeutig lesbar ist.

Anfang:  $t = v_i = s, s = c = t$ .

Induktionsschritt:  $t = ft_0 \dots t_{n-1} = s = gs_0 \dots s_{m-1} \Rightarrow f = g$  und  $n = m$ .

Nach dem vorigen Lemma ist für alle  $0 \leq i < n$   $s_i \triangleleft t_i$  oder  $t_i \triangleleft s_i$  ausgeschlossen. Aus  $t_0 \dots t_{n-1} = s_0 \dots s_{n-1}$  folgt also induktiv über  $i < n, t_i = s_i$ .  $\square$

**Definition 1.1.12.** Die Menge der  $L$ -Formeln ist die kleinste Menge, die den folgenden Regeln genügt.

- Für je zwei  $L$ -Terme ist  $t_0 = t_1$  eine  $L$ -Formel.
- Wenn  $R$  ein  $n$ -stelliges Relationszeichen ist und  $t_0, \dots, t_{n-1}$   $n$   $L$ -Terme sind, dann ist  $Rt_0 \dots t_{n-1}$  eine  $L$ -Formel.
- Wenn  $\varphi$  eine  $L$ -Formel ist, dann ist auch  $\neg\varphi$  eine  $L$ -Formel.
- Wenn  $\varphi, \psi$   $L$ -Formeln sind, dann ist auch  $(\varphi \wedge \psi)$  eine  $L$ -Formel.
- Wenn  $\varphi$  eine  $L$ -Formel und  $x$  eine Variable ist, dann ist auch  $\exists x\varphi$  eine  $L$ -Formel.

Beachten Sie, dass hierdurch der Wirkungsbereich eines Quantors als der kürzestmögliche festgelegt ist. Lesen Sie zum Beispiel  $\exists xx = y \wedge Rxy$ .

Wir verwenden folgende Abkürzungen

$$\begin{aligned} (\varphi \vee \psi) &= \neg(\neg\varphi \wedge \neg\psi) \\ (\varphi \rightarrow \psi) &= (\neg\varphi \vee \psi) \\ (\varphi \leftrightarrow \psi) &= (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi) \\ \forall x\varphi &= \neg\exists x\neg\varphi \\ \bigwedge_{i < n} \varphi_i &= \underbrace{(\dots((\varphi_0 \wedge \varphi_1) \wedge \varphi_2) \wedge \dots \wedge \varphi_{n-1})}_{n-1 \text{ mal}} \\ \bigwedge_{i < 0} \varphi_i &:= \exists v_0 v_0 = v_0 := \text{True} \\ \bigvee_{i < n} \varphi_i &= \underbrace{(\dots((\varphi_0 \vee \varphi_1) \vee \varphi_2) \vee \dots \vee \varphi_{n-1})}_{n-1 \text{ mal}} \\ \bigvee_{i < 0} \varphi_i &:= \neg\exists v_0 v_0 = v_0 := \text{False} \end{aligned}$$

Das äußerste Klammernpaar kann man weglassen und verliert so die eindeutige Lesbarkeit nicht.

*Bindungsregeln:* Außerdem hat sich eingebürgert, dass die Junktoren  $\wedge$  und  $\vee$  stärker binden als  $\rightarrow$  und  $\leftrightarrow$ . Bei einer Mischung aus  $\wedge$  und  $\vee$  würde ich immer Klammern schreiben.

Man kann also statt  $(\varphi \wedge \psi) \rightarrow \chi$  auch  $\varphi \wedge \psi \rightarrow \chi$  schreiben. Nach den Bindungsregeln kann man die Klammern bei letzterem ergänzen, um zur eindeutigen Interpretation zu kommen.

An der Definition der Formeln True und False sieht man, dass wir die leeren Trägermengen bei Strukturen verbieten müssen. In der leeren Struktur ist False richtig und True falsch. Thema dieser Vorlesung ist die Logik der nicht leeren Strukturen.

**Lemma 1.1.13.** *Keine Formel ist ein echtes Anfangsstück einer Formel.*

Dieses Lemma zeigt man wieder induktiv über die Länge von  $\psi$ : Kein echtes Anfangsstück von  $\psi$  ist eine Formel. Beim Induktionsanfang benutzt man im Beweis auch Lemma 1.1.11.

**Lemma 1.1.14.** *Für jede Formel  $\varphi$  gilt genau einer der fünf Fälle, und die Bestandteile sind eindeutig bestimmt.*

- 1  $\varphi = t_0 = t_1$  für  $L$ -Terme  $t_0, t_1$
- 2  $\varphi = Rt_0 \dots t_{n-1}$  für Terme  $t_0, \dots, t_{n-1}$ , und ein  $n$ -stelliges Relationssymbol  $R$
- 3  $\varphi = \neg\psi$  für eine  $L$ -Formel  $\psi$
- 4  $\varphi = (\psi_0 \wedge \psi_1)$  für  $L$ -Formeln  $\psi_0, \psi_1$
- 5  $\varphi = \exists x\psi$  für eine Variable  $x$  und eine  $L$ -Formel  $\psi$ .

*Beweis:* Im 2. und im 4. Fall untersucht man alle möglichen Unterteilungen und beruft sich dabei auf Lemma 1.1.11 und auf Lemma 1.1.13.  $\square$

## 1.2 Semantik, das Wahrheitsprädikat $\models$

**Definition 1.2.1** ( $A$ -Belegung). Sei  $\mathfrak{A}$  eine  $L$ -Struktur. Eine  $A$ -Belegung ist eine Funktion

$$\beta: \{v_0, \dots\} \rightarrow A.$$

**Definition 1.2.2.** Jede  $A$ -Belegung  $\beta$  wird auf die Menge der  $L$ -Terme fortgesetzt zu einer  $\mathfrak{A}$ -Belegung  $\bar{\beta}$ , die aber meistens einfach auch  $\beta$  genannt wird. Man schreibt  $\bar{\beta}(t)$  oder  $t^{\mathfrak{A}}[\beta]$  für den Wert dieser Fortsetzung an der Stelle  $t$ . Die Regeln für die Fortsetzung sind die folgenden:

$$\begin{aligned} \bar{\beta}(v_i) &= v_i^{\mathfrak{A}} = \beta(v_i); \\ \bar{\beta}(c) &= c^{\mathfrak{A}}; \\ (ft_0 \dots t_{n-1})^{\mathfrak{A}}[\beta] &= \bar{\beta}(ft_0 \dots t_{n-1}); \\ &= f^{\mathfrak{A}}(\bar{\beta}(t_0), \dots, \bar{\beta}(t_{n-1})); \\ &= f^{\mathfrak{A}}(t_0^{\mathfrak{A}}[\beta], \dots, t_{n-1}^{\mathfrak{A}}[\beta]). \end{aligned}$$

*Beispiel 1.2.3.* Es sei  $\beta(v_i) = i + 2$  über  $(\mathbb{Q}, +, \cdot)$

$$t = v_0 + v_1 \cdot v_2 \qquad \bar{\beta}(t) = 2 + (3 \cdot 4)$$

**Definition 1.2.4.** Sei  $\mathfrak{A}$  eine  $L$ -Struktur. Induktiv über den Aufbau der Formel  $\varphi$  definieren wir gleichzeitig für alle Belegungen  $\beta$  die Relation  $\mathfrak{A} \models \varphi[\beta]$ .

$$\begin{aligned} \mathfrak{A} \models t_0 = t_1[\beta] & \quad :\Leftrightarrow t_0^{\mathfrak{A}}[\beta] = t_1^{\mathfrak{A}}[\beta] \\ \mathfrak{A} \models R t_0 \dots t_{n-1}[\beta] & \quad :\Leftrightarrow R^{\mathfrak{A}}(t_0^{\mathfrak{A}}[\beta], \dots, t_{n-1}^{\mathfrak{A}}[\beta]) \\ \mathfrak{A} \models \neg \varphi[\beta] & \quad :\Leftrightarrow \mathfrak{A} \not\models \varphi[\beta] \\ \mathfrak{A} \models (\varphi \wedge \psi)[\beta] & \quad :\Leftrightarrow (\mathfrak{A} \models \varphi[\beta] \wedge \mathfrak{A} \models \psi[\beta]) \\ \mathfrak{A} \models \exists x \psi[\beta] & \quad :\Leftrightarrow \exists a \in A : \mathfrak{A} \models \psi \left[ \beta \frac{a}{x} \right] \end{aligned}$$

$$\beta \frac{a}{x}(y) = \begin{cases} a, & \text{falls } y = x, \\ \beta(y), & \text{sonst.} \end{cases}$$

**Sprechweise 1.2.5.** Die Relation  $\mathfrak{A} \models \varphi[\beta]$  wird ausgesprochen als:

- $\varphi$  gilt in  $(\mathfrak{A}, \beta)$ ;
- $\varphi$  gilt in  $\mathfrak{A}$  mit der Belegung  $\beta$ ;
- $\varphi$  ist wahr in  $(\mathfrak{A}, \beta)$ ;
- $\mathfrak{A}$  erfüllt  $\varphi[\beta]$ ;
- $(\mathfrak{A}, \beta)$  ist ein Modell von  $\varphi$ .

**Definition 1.2.6** (freie Variable). Die Variable  $x$  kommt frei in  $\varphi$  vor, wenn  $x$  nicht im Wirkungsbereich eines Quantors liegt.

Hier ist eine äquivalente induktive Definition:

- $x$  frei in  $t_0 = t_1$   $:= x$  ist in  $t_0$  oder in  $t_1$ .
- $x$  frei in  $R t_0 \dots t_{n-1}$   $:= x$  ist in  $t_i$  für mindestens ein  $i$ .
- $x$  frei in  $\neg \varphi$   $:= x$  ist frei in  $\varphi$ .
- $x$  frei in  $(\varphi \wedge \psi)$   $:= x$  ist frei in  $\varphi$  oder  $x$  ist frei in  $\psi$ .
- $x$  frei in  $\exists y \psi$   $:= x$  ist frei in  $\psi$  und  $x \neq y$ .

Nicht freies Vorkommen heißt gebundenes Vorkommen.

*Beispiel 1.2.7.*

$$\forall v_0 \forall v_1 \forall v_2 P v_0 v_1 v_2 \wedge R v_0 v_3$$

Welche Variablen sind frei? Beachten Sie, dass es keine Klammern gibt in der Formel. Welches sind die Wirkungsbereiche der einzelnen Quantoren?

**Lemma 1.2.8** (Koinzidenzlemma). Wenn  $\beta$  und  $\gamma$  auf den freien Variablen von  $\varphi$  übereinstimmen, dann gilt

$$\mathfrak{A} \models \varphi[\beta] \Rightarrow \mathfrak{A} \models \varphi[\gamma].$$

*Beweis:* Dies zeigt man induktiv über den Aufbau der Formel  $\varphi$ . Wir zeigen nur den interessantesten Aufbauschritt: Es sei  $\varphi = \exists x\psi$ .

$$\begin{aligned} \mathfrak{A} \models \varphi[\beta] &\Leftrightarrow \exists a \in A \mathfrak{A} \models \psi \left[ \beta \frac{a}{x} \right] \\ &\stackrel{\text{I.V.}}{\Leftrightarrow} \exists a \in A \mathfrak{A} \models \psi \left[ \gamma \frac{a}{x} \right] \\ &\Leftrightarrow \mathfrak{A} \models \varphi(\gamma). \end{aligned}$$

□

**Schreibweise 1.2.9.**  $\mathfrak{A} \models \varphi[a_0, \dots, a_{n-1}]$  für  $\varphi = \varphi(v_0, \dots, v_{n-1})$  für  $\beta(v_i) = a_i$ ,  $\mathfrak{A} \models \varphi[\beta]$ .

**Definition 1.2.10** (*L*-Satz, *L*-Aussage). Ein *L*-Satz/Aussage ist eine *L*-Formel ohne freie Variablen.

**Definition 1.2.11** (*L*-Theorie). Eine *L*-Theorie ist eine Menge von *L*-Sätzen/*L*-Aussagen.

Nach dem Koinzidenzlemma gilt für Aussagen  $\varphi$ , dass  $\mathfrak{A} \models \varphi[\beta]$  nicht von der *A*-Belegung  $\beta$  abhängt. Wir schreiben kurz  $\mathfrak{A} \models \varphi$ , wenn  $\mathfrak{A} \models \varphi[\beta]$  für alle *A*-Belegungen  $\beta$ .

**Definition 1.2.12** (Modell). Sei *T* eine Theorie. Ein Modell von *T* ist eine *L*-Struktur  $\mathfrak{A}$ , so dass  $\mathfrak{A} \models T$ , das heißt für alle  $\varphi \in T$  gilt  $\mathfrak{A} \models \varphi$ .

**Definition 1.2.13.** Sei *T* eine *L*-Theorie. Wir definieren die Modellklasse von *T* als

$$\text{Mod}(T) = \{\mathfrak{A} : \mathfrak{A} \models T\}.$$

Klassen der Form  $\text{Mod}(T)$  heißen elementare Klassen.

Vorsicht: Jede elementare Klasse ist eine echte Klasse (also keine Menge) oder leer. Im Mengenlehrekapitel werden Sie den Grund dafür lernen. Häufig wird durch eine Menge von *L*-Sätzen eine Klasse von *L*-Strukturen beschrieben. Man nennt solche Klassen erststufig axiomatisierbar. Hier ist ein Beispiel:

*Beispiel 1.2.14.*  $\mathcal{G} = (G, e, \circ, {}^{-1})$  ist eine Gruppe, wenn in  $\mathcal{G}$  die Gruppenaxiome gelten. Diese sind (zum Beispiel)<sup>1</sup>

$$\begin{aligned} \forall x x \circ x^{-1} &= e \\ \forall x x \circ e &= x \\ \forall x e \circ x &= x \\ \forall x \forall y \forall z (x \circ y) \circ z &= x \circ (y \circ z) \end{aligned}$$

<sup>1</sup>Es gibt andere äquivalente Formulierungen. Zum Beispiel genügt es, ein rechtsneutrales Element zu fordern.

**Definition 1.2.15.** Wir sagen „ $\mathfrak{A}$  ist elementar äquivalent zu  $\mathfrak{B}$ “, wenn für alle  $L$ -Sätze  $\varphi$  gilt, dass  $(\mathfrak{A} \models \varphi) \Leftrightarrow (\mathfrak{B} \models \varphi)$ . Wir schreiben dann  $\mathfrak{A} \equiv \mathfrak{B}$

*Beispiel 1.2.16.*  $(\mathbb{Z}, <) \not\equiv (\mathbb{Q}, <)$  und  $(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$ .

Der Begriff der elementaren Klasse hängt mit der elementaren Äquivalenz zusammen: Falls  $K = \text{Mod}(T)$ , so gilt für alle  $\mathfrak{A} \in K$ : Für alle  $\mathfrak{B}$  gilt:  $\mathfrak{B} \in K$ , wenn  $\mathfrak{B} \equiv \mathfrak{A}$ . Falls  $T$  vollständig (Def. 1.4.14) ist, gilt auch die umgekehrte Implikation: Wenn  $\mathfrak{B} \in K$ , dann  $\mathfrak{B} \equiv \mathfrak{A}$ .

## Substitution

Ein wesentlicher Schritt zum Aufstellen eines vollständigen Beweissystems, das bei rekursiven Theorien proof checking durch einen Algorithmus gestattet, ist die korrekte Behandlung unseres abzählbar unendlich großen Variablenvorrats  $\{v_n : n \in \mathbb{N}\}$ . Dieser technische Schritt fehlte in den Syllogismen im alten Griechenland und wurde um 1900 von Hilbert als Regel (B3) in seinen Kalkül (siehe Def. 1.4.1) aufgenommen. Erst 1929 gelang es Kurt Gödel, die Hilbert'sche Vermutung über die Vollständigkeit des Kalküls zu zeigen.

**Definition 1.2.17.** Sei  $x$  eine Variable und sei  $s$  ein Term. Induktiv über den Aufbau der  $L$ -Formeln  $\varphi$  definieren wir, wann  $x$  frei für  $s$  in  $\varphi$  ist, und falls dieses zutrifft, definieren wir  $\varphi \frac{s}{x}$ , gesprochen:  $\varphi$   $x$  ersetzt durch  $s$ .

- 1) Am Anfang betrachten wir  $t \frac{s}{x}$   
Hier wird jedes Vorkommen von  $x$  im Term  $t$  durch den Term  $s$ .
- 2)  $x$  ist frei für  $s$  in  $\varphi$   
 $x$  ist frei für  $s$  in  $\varphi$ , wenn kein freies Vorkommen von  $x$  im Wirkungsbereich eines Quantors ist, der eine Variable in  $s$  bindet. Auf Seite 14 im Ziegler-Buch [6] findet man zusätzlich eine äquivalente rekursive Definition.
- 3) Wir geben alternativ eine äquivalente induktive Definition von „ $x$  ist frei für  $s$  in  $\varphi$ “ und definieren „ $\varphi$   $x$  ersetzt durch  $s$ .“

Wir schreiben nur den schwierigen Induktionsschritt für  $\varphi = \exists y\psi$ . Bei allen anderen Aufbausritten zieht sich die Ersetzung einfach nach innen.

$$(\exists y\psi) \frac{s}{x} = \begin{cases} \exists y\psi \frac{s}{x}, & \text{falls } x \neq y \text{ und } x \text{ frei für } s \text{ in } \psi \text{ und } y \text{ nicht in } s; \\ \exists y\psi, & \text{falls } x = y \text{ und } x, y \text{ in } s \text{ nicht vorkommen;} \\ \text{undefiniert,} & \text{sonst.} \end{cases}$$

$x$  ist frei für  $s$  in  $\exists y\psi$ , wenn  $(\exists y\psi) \frac{s}{x}$  definiert ist.

n 23.4.23 korrigiert

**Lemma 1.2.18** (Substitutionslemma). *Seien  $x$  eine Variable,  $s$  ein Term und  $\beta$  eine Belegung*

1) Dann gilt:

$$\left(t \frac{s}{x}\right)^{\mathfrak{A}}[\beta] = t^{\mathfrak{A}}\left[\beta \frac{s^{\mathfrak{A}}[\beta]}{x}\right]$$

2) Falls  $x$  frei für  $s$  in  $\varphi$ , so gilt

$$\mathfrak{A} \models \varphi \frac{s}{x}[\beta] \Leftrightarrow \mathfrak{A} \models \varphi \left[\beta \frac{s^{\mathfrak{A}}[\beta]}{x}\right].$$

*Beweis:* 1) Per Induktion. Sei  $t = ft_0 \dots t_{n-1}$ .

$$\begin{aligned} \left(t \frac{s}{x}\right)^{\mathfrak{A}}[\beta] &= \bar{\beta} \left(ft_0 \dots t_{n-1} \frac{s}{x}\right) = f^{\mathfrak{A}} \left(\bar{\beta} \left(t_0 \frac{s}{x}\right), \dots, \bar{\beta} \left(t_{n-1} \frac{s}{x}\right)\right) \\ &\stackrel{\text{I.V.}}{=} f^{\mathfrak{A}} \left(\left(\bar{\beta} \frac{\bar{\beta}(s)}{x}\right)(t_0), \dots, \left(\bar{\beta} \frac{\bar{\beta}(s)}{x}\right)(t_{n-1})\right) \\ &= \left(\bar{\beta} \frac{\bar{\beta}(s)}{x}\right) ft_0 \dots t_{n-1} = t^{\mathfrak{A}} \left[\beta \frac{\bar{\beta}(s)}{x}\right] \\ &= t^{\mathfrak{A}} \left[\beta \frac{s^{\mathfrak{A}}[\beta]}{x}\right]. \end{aligned}$$

2) Der Induktionsanfang folgt aus dem ersten Teil des Lemmas. Wir führen nur den schwierigsten Induktionsschritt aus. Sei also  $\varphi = \exists y \psi$  und  $b = s^{\mathfrak{A}}[\beta] = s^{\mathfrak{A}}[\beta \frac{a}{y}]$ . Letzteres gilt, da  $y$  in  $s$  nicht vorkommt, denn  $x$  ist frei für  $s$  in  $\varphi$ .

$$\begin{aligned} \mathfrak{A} \models \varphi \frac{s}{x}[\beta] &\stackrel{\text{Def.}}{\Leftrightarrow} (\text{es gibt ein } a \in A)(\mathfrak{A} \models \psi \frac{s}{x} \left[\beta \frac{a}{y}\right]) \\ &\stackrel{\text{I.V.}}{\Leftrightarrow} (\text{es gibt ein } a \in A)(\mathfrak{A} \models \psi \left[\beta \frac{a}{y} \frac{s^{\mathfrak{A}}[\beta \frac{a}{y}]}{x}\right]) \\ &\stackrel{\text{einsetzen}}{\Leftrightarrow} (\text{es gibt ein } a \in A)(\mathfrak{A} \models \psi \left[\beta \frac{b}{x} \frac{a}{y}\right]) \\ &\stackrel{x \neq y}{\Leftrightarrow} \mathfrak{A} \models \varphi \left[\beta \frac{b}{x}\right] \end{aligned}$$

Beachten Sie, dass die mit  $\mathfrak{A}$  beginnenden Teilformeln der rechten Seiten in der Zeile eins bis drei der Gleichung sogar für jedes feste  $a \in A$  äquivalent sind. □

*Bemerkung 1.2.19.* Auf die Voraussetzung, dass  $x$  frei für  $s$  in  $\varphi$  ist, kann man nicht verzichten. Untersuchen Sie zum Beispiel  $(\exists x x \neq y) \frac{x}{y}$ .

### 1.3 Allgemeingültige Formeln

**Definition 1.3.1** (allgemeingültig). Eine Formel  $\varphi$  heißt allgemeingültig, wenn  $\varphi$  in allen  $L$ -Strukturen  $\mathfrak{A}$  mit allen Belegungen  $\beta$  gilt. Wir schreiben  $\models \varphi$ .

*Beispiel 1.3.2* (Hutformel von Kreisel). Die Hutformel von Kreisel<sup>2</sup> ist allgemeingültig.

$$\exists x(H(x) \rightarrow \forall yH(y))$$

**Definition 1.3.3.** Sei  $\mathfrak{A}$  eine  $L$ -Struktur und sei  $K \subseteq L$ . Dann definieren wir  $\mathfrak{A} \upharpoonright K$  als  $(A, (Z^{\mathfrak{A}})_{Z \in K})$ .

**Lemma 1.3.4.** Sei  $\varphi$  eine  $L$ -Formel und  $K \supseteq L$ . Dann ist  $\varphi$  genau dann in der Gesamtheit der  $L$ -Strukturen allgemeingültig, wenn  $\varphi$  in der Gesamtheit der  $K$ -Strukturen allgemeingültig ist.

*Beweis:* „ $\Rightarrow$ “: Angenommen,  $\mathfrak{A} \models \neg\varphi$ . Dann gilt nach der Definition der  $\models$ -Relation auch  $\mathfrak{A} \upharpoonright L \models \neg\varphi$ .

„ $\Leftarrow$ “: Angenommen  $\varphi$  ist nicht allgemeingültig für  $L$ -Strukturen. Es gibt also eine  $L$ -Struktur  $\mathfrak{A}$ , so dass  $\mathfrak{A} \models \neg\varphi$ . Dann gibt es eine Expansion von  $\mathfrak{A}$  zu einer  $K$ -Struktur  $\mathfrak{A}'$ . Expansion heißt: die Symbole von  $K \setminus L$  werden auf dem Träger  $A$  in beliebiger Weise interpretiert, die Symbole aus  $L$  werden auf  $\mathfrak{A}$  wie in  $\mathfrak{A}$  interpretiert. Man erhält also eine  $K$ -Struktur  $\mathfrak{A}'$ , so dass  $\mathfrak{A}' \upharpoonright L = \mathfrak{A}$ . Dann gilt  $\mathfrak{A}' \models \neg\varphi$ , und  $\varphi$  ist nicht allgemeingültig in der Gesamtheit der  $K$ -Strukturen.  $\square$

**Definition 1.3.5** (Aussagenlogische Formel). Aussagenlogische Formeln bauen sich aus einem unendlichen Vorrat  $M = \{A_n : n \in \omega\}$  von Aussagenvariablen mit den Junktoren  $\neg$  und  $\wedge$  und dem Klammersymbol auf.

**Definition 1.3.6** (Wahrheitsfunktion). Eine Wahrheitsfunktion ist eine Abbildung  $\mu: M \rightarrow \{W, F\}$ .

**Definition 1.3.7.** Eine Wahrheitsfunktion  $\mu$  setzt sich auf die  $M$ -Formeln fort durch

$$\bar{\mu}(p) = \mu(p) \qquad \bar{\mu}(\varphi \wedge \psi) = \bar{\mu}(\varphi) \wedge \bar{\mu}(\psi) \qquad \bar{\mu}(\neg\varphi) = \neg\bar{\mu}(\varphi)$$

Hierbei werden die Werte der Junktoren auf den rechten Seiten durch die folgenden Wahrheitstabellen festgelegt:

$\wedge$	W	F
W	W	F
F	F	F

$\neg$	
W	F
F	W

<sup>2</sup>Georg Kreisel, 1923 – 2015



**Definition 1.3.8** (allgemeingültige aussagenlogische Formel).  $\varphi = \varphi(\rho_1, \dots, \rho_n)$  heißt allgemeingültige aussagenlogische Formel, wenn  $\forall \mu \bar{\mu}(\varphi) = W$ .

Wir schreiben von nun an nur noch  $\mu$  statt  $\bar{\mu}$ .

**Definition 1.3.9** (Tautologie). Eine Tautologie entsteht aus einer allgemeingültigen aussagenlogischen Formel durch Ersetzung der Aussagenvariablen durch  $L$ -Formeln.

Beispiel:  $A_1 \vee \neg A_1$  ergibt die Tautologie  $\varphi \vee \neg \varphi$ .

**Lemma 1.3.10.** *Jede Tautologie ist allgemeingültig.*

*Beweis:* Sei  $f$  eine Tautologie. Dann gilt  $\forall \mu \mu(f) = W$  mit  $f = f(\varphi_0, \dots, \varphi_{n-1})$ . Seien  $\mathfrak{A}, \beta$  gegeben. Nun nehmen wir

$$\mu(\varphi_i) = W \Leftrightarrow \mathfrak{A} \models \varphi_i[\beta].$$

dann ist

$$\mu(f) = W.$$

Also gilt

$$\mathfrak{A} \models f(\varphi_0, \dots, \varphi_{n-1})[\beta].$$

□

**Lemma 1.3.11** (Axiome der Gleichheit). *Die folgenden  $L$ -Formeln sind allgemeingültig. Sie heißen Axiome der Gleichheit.*

*Reflexivität:*  $\forall x x = x$ .

*Symmetrie:*  $\forall x \forall y (x = y \rightarrow y = x)$ .

*Transitivität:*  $\forall x y z (x = y \wedge y = z \rightarrow x = z)$ .

*Kongruenz für Funktionszeichen  $f \in L$ :*  $\forall x_0 \dots x_{n-1} y_0 \dots y_{n-1} (\bigwedge_{i < n} x_i = y_i \rightarrow f\bar{x} = f\bar{y})$ .

*Kongruenz für ein Relationszeichen  $R \in L$ :*  $\forall \bar{x} \forall \bar{y} (\bigwedge x_i = y_i \rightarrow (R\bar{x} \leftrightarrow R\bar{y}))$ .

*$L$ :*

*Die Gleichheitsaxiome sagen genau, dass  $=$  eine Kongruenzrelation ist.*

**Lemma 1.3.12** ( $\exists$ -Quantorenaxiom). *Sei  $\varphi$  eine  $L$ -Formel,  $t$  ein  $L$ -Term und  $x$  frei für  $t$  in  $\varphi$ . Dann ist*

$$\varphi \frac{t}{x} \rightarrow \exists x \varphi$$

*allgemeingültig.*

*Beweis:* Sei  $(\mathfrak{A}, \beta)$  eine  $L$ -Interpretation. Dann gilt nach dem Substitutionslemma

$$\mathfrak{A} \models \varphi \frac{t}{x} [\beta] \Leftrightarrow \mathfrak{A} \models \varphi \left[ \beta \frac{t^{\mathfrak{A}}[\beta]}{x} \right] \Rightarrow \mathfrak{A} \models \exists x \varphi [\beta].$$

□

**Lemma 1.3.13** (Modus ponens). *Wenn  $\varphi$  und  $(\varphi \rightarrow \psi)$  allgemeingültig sind, so auch  $\psi$ .*

*Beweis:* Seien  $\mathfrak{A}$  und  $\beta$  gegeben. Lese  $\mathfrak{A} \models \varphi[\beta]$  und  $\mathfrak{A} \models (\varphi \rightarrow \psi)[\beta]$  zusammen.  $\square$

**Lemma 1.3.14** ( $\exists$ -Einführungsregel, auch  $\exists$ -Einführung im Antezedens). *Wenn  $x$  nicht frei in  $\psi$  vorkommt, dann ist mit  $\varphi \rightarrow \psi$  auch  $\exists x\varphi \rightarrow \psi$  allgemeingültig.*

*Beweis:* Sei  $\mathfrak{A}$ ,  $\beta$  gegeben und  $\mathfrak{A} \models \exists x\varphi[\beta]$ . Also gilt  $\mathfrak{A} \models \varphi[\beta \frac{a}{x}]$  für ein  $a \in A$ .  $\mathfrak{A} \models (\varphi \rightarrow \psi)[\beta \frac{a}{x}]$ , da  $\varphi \rightarrow \psi$  allgemeingültig ist, gilt also  $\mathfrak{A} \models \psi[\beta \frac{a}{x}]$ . Aus dem Koinzidenzlemma 1.2.8 folgt nun  $\mathfrak{A} \models \psi[\beta]$ .  $\square$

### 1.3.1 Exkurs über Boole'sche Algebren

**Definition 1.3.15** (Boole'sche Algebra). Eine Boole'sche<sup>3</sup> Algebra  $(\mathcal{B}, 0, 1, \cap, \cup, ^c)$  ist eine nicht leere Menge  $\mathcal{B}$  mit zwei ausgezeichneten Elementen 0 und 1, zwei zweistelligen Operationen  $\cap$  und  $\cup: \mathcal{B}^2 \rightarrow \mathcal{B}$  und einer einstelligen Operation  $^c: \mathcal{B} \rightarrow \mathcal{B}$ , für die die folgenden Gleichungen jeweils für alle  $a, b, c$  gelten:

Idempotenz	$a \cap a = a$	$a \cup a = a$
Kommutativität	$a \cap b = b \cap a$	$a \cup b = b \cup a$
Assoziativität	$(a \cap b) \cap c = a \cap (b \cap c)$	$(a \cup b) \cup c = a \cup (b \cup c)$
Absorption	$a \cap (a \cup b) = a$	$a \cup (a \cap b) = a$
Distributivität	$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$	$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$
Null und Eins	$0 \cap a = 0$	$1 \cup a = 1$
Komplement	$a \cap a^c = 0$	$a \cup a^c = 1$

*Beispiel 1.3.16.* Sei  $X$  eine Menge (es kann auch  $X = \emptyset$  gelten). Die Potenzmengenalgebra  $\mathcal{B}(X) = (\mathcal{P}(X), \emptyset, X, \cap, \cup, ^c)$  mit  $Y^c = X \setminus Y$  für  $Y \subseteq X$  ist eine Boole'sche Algebra.

**Definition 1.3.17.** Sei  $\mathcal{B}$  eine Boole'sche Algebra. Wir schreiben  $x \leq y$  für  $x \cap y = x$ .

**Satz 1.3.18** (Stone'scher Darstellungssatz). *Jede Boole'sche Algebra ist isomorph zu einer Unteralgebra einer Potenzmengenalgebra.<sup>4</sup>*

*Beweis:* Sei  $(\mathcal{B}, 0, 1, \cup, \cap, ^c)$  gegeben.

**Definition 1.3.19** (Ultrafilter).  $U \subseteq \mathcal{B}$  heißt Ultrafilter auf  $\mathcal{B}$ , wenn folgendes gilt:

- $0 \notin U$ ,  $1 \in U$
- $\forall x \in \mathcal{B} \forall y (x \in U \wedge y \geq x \rightarrow y \in U)$
- $\forall x \in \mathcal{B} \forall y (x, y \in U \rightarrow x \cap y \in U)$
- $\forall x \in \mathcal{B} (x \in U \vee x^c \in U)$

<sup>3</sup>George Boole, 1815 – 1864

<sup>4</sup>Marshall Harvey Stone, 1903 – 1989

Die Struktur

$$\mathfrak{S} = (\text{Pot}(\{U : U \text{ Ultrafilter auf } \mathfrak{B}\}), \emptyset, \text{Menge aller Ultrafilter}, \cap, \cup, ^c)$$

ist die Stone-Algebra von  $\mathfrak{B}$ .

Die Abbildung  $b \in \mathfrak{B} \xrightarrow{e} \{U : U \text{ Ultrafilter auf } \mathfrak{B}, b \in U\}$  bettet  $\mathfrak{B}$  in die Stone-Algebra ein. Die Abbildung  $e$  erhält  $0, 1, \sqcup, \sqcap, ^c$  alle in beide Richtungen und ist injektiv, also ist  $e$  ein Isomorphismus auf ihr Bild. Isomorphismen auf Bilder werden auch Einbettungen genannt.  $\square$

**Satz 1.3.20.** *Die Einbettung  $e$  ist genau dann surjektiv, wenn  $\mathfrak{B}$  endlich ist.*

*Bemerkung 1.3.21.* Sei  $\mathfrak{B}$  eine endliche Boole'sche Algebra. Gibt es Ultrafilter auf  $B$ ? Es gibt Hauptultrafilter. Diese sind Ultrafilter der Form

$$\{x : x \geq b\}$$

für ein Atom  $b$  in  $B$ . Ein Element ungleich der Null von  $B$ , das sich in  $B$  nicht in zwei Elemente ungleich Null aufteilen lässt, heißt Atom von  $B$ . Eine Boole'sche Algebra ohne Atome heißt atomlos.

Exkurs: Die Nicht-Hauptultrafilter heißen freie Ultrafilter. Gibt es auf jeder atomlosen Boole'schen Algebra einen Ultrafilter? (Solch ein Ultrafilter ist notwendigerweise frei.) Dazu braucht man das Auswahlaxiom. Einen Beweis findet man in Satz 2.1.47. Jedoch impliziert die Aussage "Auf jeder atomlosen Boole'schen Algebra gibt es einen Ultrafilter" nicht das Auswahlaxiom. Dies wurde 1965 von Halpern und Levy gezeigt, siehe Satz 2.1.48.

*Beispiel 1.3.22* (Lindenbaum-Algebra). Zwei aussagenlogische Formeln  $\varphi$  und  $\psi$  heißen äquivalent wenn für jede Wahrheitsbelegung  $\mu$  der Variablen beider Formeln gilt:

$$\mu(\varphi) = W \leftrightarrow \mu(\psi) = W.$$

Wir schreiben  $\varphi \equiv \psi$ . Die Äquivalenzrelation ist bezüglich der Junktoren eine Kongruenzrelation und daher lassen sich diese auch auf dem Quotienten (also auf der Menge  $L(M)/\equiv$ ) definieren, zum Beispiel:

$$(\varphi/\equiv \vee \equiv \psi/\equiv) := (\varphi \vee \psi)/\equiv$$

Sei  $M$  eine Menge aussagenlogischer Variablen,  $A_0 \in M$ . Dann heißt

$$\mathfrak{L}(M) = (L(M)/\equiv, A_0 \wedge \neg A_0/\equiv, A_0 \vee \neg A_0/\equiv, \wedge_{\equiv}, \vee_{\equiv}, \neg_{\equiv})$$

die Lindenbaumalgebra über  $M$ .<sup>5</sup>

---

<sup>5</sup>Adolf Lindenbaum, 1904 – 1941

## 1.4 Der Gödel'sche Vollständigkeitsatz

Es gibt recht einfache Systematisierungen aller gültiger Beweisregeln, so dass die Allgemeingültigkeit mit der Beweisbarkeit äquivalent ist. Dies ist der Inhalt des Gödel'schen Vollständigkeitsatzes<sup>6</sup>. Wir formulieren und beweisen ihn in diesem Abschnitt für den Hilbert'schen Beweiskalkül. Wir beginnen mit dem Aufstellen der Beweisregeln.

**Definition 1.4.1.** [Der Hilbert-Kalkül,  $T \vdash \varphi$ ] Sei  $T$  eine Menge von Formeln. Induktiv über die Anzahl der Regelanwendungen definieren wir folgendes: Eine  $L$ -Formel  $\varphi$  heißt (im Hilbert-Kalkül)<sup>7</sup> beweisbar aus  $T$ , wenn

B1  $\varphi$  eine Tautologie ist, oder

B2  $\varphi$  ein Gleichheitsaxiom ist, oder

B3  $\varphi$  ein  $\exists$ -Quantoraxiom ist, oder

B4  $\varphi$  sich aus zwei aus  $T$  beweisbaren  $L$ -Formeln  $\psi$  und  $(\psi \rightarrow \varphi)$  mit Hilfe des Modus ponens ergibt, oder

B5  $\varphi = \exists x \chi \rightarrow \psi$  sich aus einer aus  $\emptyset$  beweisbaren Formel  $\chi \rightarrow \psi$ , in der  $x$  in  $\psi$  nicht vorkommt, mit Hilfe der  $\exists$ -Einführung ergibt, oder

B6  $\varphi$  ein Element aus  $T$  ist.

Wir schreiben  $T \vdash_L \varphi$ , wenn  $\varphi$  aus  $T$  beweisbar ist. Ein Beweis besteht aus einer endlich langen Folge von Anwendungen der Beweisregeln. Falls  $T = \emptyset$ , kann man die Regel B6 weglassen und schreibt  $\vdash_L \varphi$ . Falls  $L$  betont werden soll, schreibt man  $\vdash_L$ .<sup>8</sup>

Meistens wendet man den Hilbertkalkül auf Voraussetzungsmengen  $T$  ohne freie Variablen an. Diese heißen Theorien.

**Definition 1.4.2** ( $T \models \varphi$ ). Seien  $T$  eine Menge von  $L$ -Formeln und  $\varphi$  eine  $L$ -Formel. Wir schreiben  $T \models \varphi$  und sagen „ $\varphi$  folgt aus  $T$ “, wenn  $\varphi$  in allen Modellen  $(\mathfrak{A}, \beta)$  von  $T$  gilt.

In den Lemmata 1.3.10 bis 1.3.14 bewiesen wir den folgenden Satz:

**Satz 1.4.3** (Korrektheitsatz). *Seien  $T$  eine Menge von  $L$ -Formeln und  $\varphi$  eine  $L$ -Formel.*

$$T \vdash \varphi \Rightarrow T \models \varphi.$$

Nun gilt auch die umgekehrte Implikation:

**Satz 1.4.4** (Gödel'scher Vollständigkeitsatz). *Sei  $T$  eine  $L$ -Theorie und sei  $\varphi$  eine  $L$ -Formel.*

$$T \models \varphi \Leftrightarrow T \vdash_L \varphi.$$

<sup>6</sup>Kurt Friedrich Gödel, 1906 – 1978

<sup>7</sup>David Hilbert, 1862 – 1943

<sup>8</sup>Da für  $L$ -Formeln  $\varphi$  die Beweisbarkeit  $\vdash_L \varphi$  für jede Obermenge  $L' \supseteq L$  die Beweisbarkeit  $\vdash_{L'} \varphi$  impliziert, führt das Nichtschreiben von  $L$  nicht in Unstimmigkeiten.

Beweis: Nur noch die Vorwärtsrichtung ist zu zeigen.

Der Beweis des Satzes und seiner unten angeführten Varianten wird erst auf Seite 29 zu Ende sein.

Wir ergänzen die Axiome B1, B2, B3, B6 und die Regeln B4, B5 durch eine weitere abgeleitete Regel und ein abgeleitetes Axiom. Diese zusätzlichen Beweisregeln heißen auch abgeleitete Beweisregeln.

**Lemma 1.4.5.** (*Abgeleitete Beweisregeln*)

1) Wenn  $T \vdash \varphi_0, \dots, T \vdash \varphi_{n-1}$  und  $T \vdash ((\bigwedge_{i < n} \varphi_i) \rightarrow \psi)$ , so ist  $T \vdash \psi$ .

2)  $\forall$ -Quantorenaxiome: Wenn  $x$  frei für  $t$  in  $\varphi$  ist, so ist

$$\vdash \forall x \varphi \rightarrow \varphi \frac{t}{x}.$$

3)  $\forall$ -Einführungsregel,  $\forall$ -Einführung im Sukzedens: Wenn  $x$  nicht frei in  $\varphi$  ist und  $\emptyset \vdash (\varphi \rightarrow \psi)$ , dann gilt:

$$T \vdash (\varphi \rightarrow \forall x \psi).$$

Insbesondere folgt im Falle  $\varphi = \exists x x = x$  aus  $T \vdash \psi$  die Aussage  $T \vdash \forall x \psi$ .

*Beweis:* 1) Durch Nachprüfung aller vier Wahrheitsbelegungen sieht man, dass

$$\varphi_0 \rightarrow (\varphi_1 \rightarrow (\varphi_0 \wedge \varphi_1)) \tag{1.4.1}$$

eine Tautologie ist. Man erhält also aus  $T \vdash \varphi_0$  und  $T \vdash \varphi_1$  durch zweimalige Anwendung des Modus ponens

$$T \vdash \varphi_0 \wedge \varphi_1.$$

Diese Überlegung wiederholt man noch  $n - 2$  Mal und erhält so  $T \vdash \bigwedge_{i < n} \varphi_i$ . Nun bringt uns eine weitere Anwendung des Modus ponens zu  $T \vdash \psi$ .

2)  $\neg \varphi \frac{t}{x} \rightarrow \exists x \neg \varphi$  ist ein  $\exists$ -Quantorenaxiom, da  $x$  frei für  $t$  in  $\varphi$  ist.

$$\left( \neg \varphi \frac{t}{x} \rightarrow \exists x \neg \varphi \right) \rightarrow \left( \neg \exists x \neg \varphi \rightarrow \varphi \frac{t}{x} \right)$$

ist eine Tautologie (aus  $(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$ ). Mit dem Modus ponens erhalten wir  $\vdash_L \neg \exists x \neg \varphi \rightarrow \varphi \frac{t}{x}$ .

3) Wenn  $T \vdash \varphi \rightarrow \psi$ , folgt mit Teil 1) von Lemma 1.4.5 die Aussage  $T \vdash_L \neg \psi \rightarrow \neg \varphi$ . Nun ergibt die  $\exists$ -Einführung

$$T \vdash \exists x \neg \psi \rightarrow \neg \varphi.$$

Da  $(\neg \psi \rightarrow \varphi) \rightarrow (\exists x \neg \psi \rightarrow \neg \varphi)$  nach der  $\exists$ -Einführungsregel allgemeingültig ist, gilt auch  $T \vdash (\neg \psi \rightarrow \varphi) \rightarrow (\exists x \neg \psi \rightarrow \neg \varphi)$ . In  $T$  darf  $x$  als freie Variable vorkommen. Erneute Anwendung der Aussagenlogik und Modus ponens liefern

$$T \vdash (\varphi \rightarrow \neg \exists x \neg \psi).$$

Nun zu der „inbesondere“-Bemerkung: Wir können eben Durchgeführtes auch mit einer Tautologie  $\varphi$  anwenden, die  $x$  nicht frei enthält. Wir nehmen also  $\vdash \varphi$  an. Dann impliziert  $\vdash (\varphi \rightarrow \varphi)$  die scheinbar stärkere Aussage  $\varphi \rightarrow \forall x\varphi$  mit dem eben Durchgeführten. Anwendung des Modus ponens auf  $\vdash_L \varphi$  und  $\vdash \varphi \rightarrow \forall x\varphi$  ergibt nun

$$\vdash_L \forall x\varphi.$$

□

*Beispiel 1.4.6.* Wir wollen  $\vdash \exists x\forall yRxy \rightarrow \forall y\exists xRxy$  zeigen. Dazu gehen wir wie folgt vor.

- (1) Es gilt  $\vdash \forall yRxy \rightarrow Rxy$ . Begründung:  $\forall yRxy \rightarrow Rxy$  ist ein  $\forall$ -Quantorenaxiom, denn  $y$  ist frei für  $y$  in  $Rxy$ .
- (2)  $Rxy \rightarrow \exists xRxy$  ist ein  $\exists$ -Quantorenaxiom, denn  $x$  ist frei für  $x$  in  $Rxy$ .
- (3) Wir setzen die beiden Axiome mit dem Modus ponens zusammen und erhalten  $\vdash \forall yRxy \rightarrow \exists xRxy$ .
- (4) Nun kommt  $y$  in der Voraussetzung  $\forall yRxy$  nicht frei vor. Wie nehmen die  $\forall$ -Einführung und erhalten  $\vdash \forall yRxy \rightarrow \forall y\exists xRxy$ .
- (5) Nun kommt  $x$  nicht frei in der Konklusion  $\forall y\exists xRxy$  vor. Wir nehmen die  $\exists$ -Einführung und erhalten  $\vdash \exists x\forall yRxy \rightarrow \forall y\exists xRxy$ .

Beim Beweis des Vollständigkeitssatzes 1.4.4 können wir uns auf Sätze beschränken. Falls  $T$  und/oder  $\varphi$  freie Variablen haben, so ersetzt man sie passend (d.h.  $v_i$  durch  $c_i$  sowohl in  $T$  als auch in  $\varphi$ ) durch neue Konstanten.

**Definition 1.4.7** (*L*-Beweis). Sei  $T$  eine Menge von *L*-Formeln und sei  $\varphi$  eine *L*-Formel. Ein *L*-Beweis von  $\varphi$  aus den Voraussetzungen  $T$  ist eine Folge

$$\langle \alpha_0, \dots, \alpha_n = \varphi \rangle$$

so dass für alle  $i < n$ ,

- 1)  $\alpha_i$  entweder Axiom der Art B1, B2, B3, B6 oder ein  $\forall$ -Quantorenaxiom nach Lemma 1.4.5 Punkt 2 ist,
- 2) es  $m < i$ ,  $\varphi_k$ ,  $k < m$ , gibt, so dass die Formel  $\alpha_i = \psi$  ist, und es  $m < i$ , und für  $k < m$ ,  $j_k < i$  gibt, so dass  $\alpha_{j_k} = \varphi_k$ , und es  $j < i$  gibt, so dass  $\alpha_j = \bigwedge_{k < m} \varphi_k \rightarrow \psi$  (dann ist nach Lemma 1.4.5 Punkt 1  $\alpha_i$  eine korrekte Beweisverlängerung), oder
- 3)  $\alpha_i$  sich aus einer früheren  $\alpha_j$ ,  $j < i$  oder mit Regel B5 oder mit dem dazu dualen Lemma 1.4.5 Punkt 3 ergibt. Beachten Sie hierzu, dass man dazu an der früheren Stelle  $\emptyset$  als Voraussetzung hat.

Ausführlich geschrieben sind die Möglichkeiten im Punkt 3) also wie folgt. Es gibt  $\psi$ ,  $\chi$  mit folgenden Eigenschaften:

3a) B5,  $\exists$ -Antezedens:  $\alpha_i = \exists x\chi \rightarrow \psi$ ,  $x$  nicht frei in  $\psi$ , und es gibt  $j < i$ ,  $\alpha_j = (\chi \rightarrow \psi)$  und  $\emptyset \vdash \alpha_j$ .

3b) dual zu B5,  $\forall$ -Sukzedens:  $\alpha_i = \psi \rightarrow \forall x\chi$ ,  $x$  nicht frei in  $\psi$ , und es gibt  $j < i$ ,  $\alpha_j = (\psi \rightarrow \chi)$  und  $\emptyset \vdash \alpha_j$ .

Falls  $T$  keine freien Variablen enthält, kann man die Anwendungen von B5 und dualem B5 zu  $T \vdash \alpha_j$  abschwächen.

**Lemma 1.4.8.**  $\varphi(\bar{x})$  sei eine  $L$ -Formel und  $T$  eine  $L$ -Theorie,  $C$  eine Menge von neuen Konstanten,  $\bar{c}$  paarweise verschieden, dann gilt

$$T \vdash_{L \cup C} \varphi(\bar{c}) \Leftrightarrow T \vdash_L \varphi(x_0, \dots, x_{n-1})$$

*Beweis:*

„ $\Rightarrow$ “ Sei  $B(c_0, \dots, c_{m-1}) = \langle \alpha_0, \dots, \alpha_n = \varphi \rangle$  ein  $L \cup C$ -Beweis von  $\varphi(\bar{c})$ . Hierbei sollen alle Konstanten aus  $C$ , die im Beweis vorkommen, unter  $c_0, \dots, c_{m-1}$  sein. Nun ersetzen wir alle (freien und gebundenen) Variablen  $x_i$  in  $B(\bar{c})$  durch neue  $y_i$ . Nach der Ersetzung haben wir immer noch einen Beweis. Nun ersetzen wir  $c_i$  durch  $x_i$ . Alle Beweisregeln sind auch nach dieser Ersetzung noch korrekte Regeln. Wir erhalten  $\vdash_L \varphi(\bar{x})$ .

„ $\Leftarrow$ “ Sei  $T \vdash_L \varphi(\bar{x})$ . Dann  $T \vdash_L \forall \bar{x} \varphi(\bar{x})$  nach Lemma 1.4.5 Punkt 3. Dann gilt  $T \vdash_{L \cup C} \forall \bar{x} \varphi(\bar{x})$ . Nun folgt  $T \vdash_{L \cup C} \varphi(\bar{c})$  nach Punkt 2 von Lemma 1.4.5.

□

**Definition 1.4.9** (widerspruchsfrei, konsistent). Eine Menge  $T$  von  $L$ -Formeln heißt widerspruchsfrei, oder konsistent, wenn

$$\text{für alle } n \in \mathbb{N}, \text{ für alle } \varphi_i \in T, i < n, \text{ gilt: } \not\vdash_L \neg(\varphi_0 \wedge \dots \wedge \varphi_{n-1}).$$

Ist die Theorie nicht widerspruchsfrei, so nennen wir  $T$  widerspruchsvoll oder widersprüchlich, contradictory.

*Beispiel 1.4.10.* Zum Beispiel ist für jeden Satz  $\varphi$  die Theorie  $T = \{\varphi \wedge \neg\varphi\}$  widerspruchsvoll.

Nun ist die Untersuchung der Beweisregeln für sich beendet und wir gehen zur semantischen Seite über.

**Satz 1.4.11** (Gödel'scher Satz für die Erfüllbarkeit). *Jede widerspruchsfreie Menge von  $L$ -Formeln hat ein Modell.*

Wir führen die schwere Implikation im Satz 1.4.4 auf den Satz 1.4.11 zurück.

„ $\Rightarrow$ “ Angenommen  $T \not\vdash \varphi$ . Dann ist  $T \cup \{\neg\varphi\}$  widerspruchsfrei. Nach Satz 1.4.11 gibt es ein Modell  $\mathfrak{A} \models T \cup \{\neg\varphi\}$ . Also  $\neg T \models \varphi$ .

Somit haben wir nur noch den Satz 1.4.11 zu zeigen.

Wir zeigen nun Satz 1.4.11 mit einer Methode, die 1949 von Leon Henkin<sup>9</sup> gefunden wurde.

Von nun an sei  $T$  eine Menge von  $L$ -Sätzen. Der Grund für diese Einschränkung ist Lemma 1.4.8. Wenn man den Gödel'schen Satz für eine Formelmenge beweisen möchte, ersetzt man erst jedes  $v_i$  in dieser Formelmenge durch eine neue Konstante, und rechnet dann mit der so entstandenen  $L \cup C$ -Theorie weiter.

**Korollar 1.4.12.** *Es sei  $T$  eine  $L$ -Theorie.  $T$  ist auch als Menge von  $L \cup C$ -Formeln aufgefasst widerspruchsfrei.*

**Definition 1.4.13** (Henkin-Theorie). Eine  $L \cup C$ -Theorie  $T^+$  heißt Henkin-Theorie für  $T$  mit Konstantenmenge  $C$ , wenn  $T^+ \supseteq T$  und es zu jeder  $L \cup C$ -Formel  $\varphi$  mit einer einzigen freien Variable eine Konstante  $c \in C$  gibt, so dass

$$(\exists x\varphi(x) \rightarrow \varphi(c)) \in T^+.$$

**Definition 1.4.14.** [vollständige Theorie]

- 1) Eine  $K$ -Theorie  $T^*$  heißt vollständig im starken Sinne, wenn  $T$  widerspruchsfrei ist und für jeden  $K$ -Satz gilt:

$$\varphi \in T^* \quad \text{oder} \quad \neg\varphi \in T^*.$$

- 2) Eine  $K$ -Theorie  $T^*$  heißt vollständig, wenn  $T$  widerspruchsfrei ist und für jeden  $K$ -Satz gilt:

$$T^* \vdash \varphi \quad \text{oder} \quad T^* \vdash \neg\varphi.$$

Warnung: Die Vollständigkeit hängt von der Sprache ab. Fasst man die  $L$ -Theorie  $T$  als  $K$ -Theorie auf für ein  $K \supseteq L$ , dann ist  $T$  in der  $K$ -Sprache in der Regel meistens nicht vollständig. Streng genommen müsste man "vollständig in der  $L$ -Sprache" sagen.

Normalerweise ist man an der Vollständigkeit einer Theorie interessiert. Nur für die Dauer unseres Beweises ist die starke Vollständigkeit der nützlichere Begriff. Die meisten Theorien sind unvollständig, zum Beispiel die Gruppentheorie.

Nun führen wir den Henkin'schen Beweis durch: Er besteht aus drei Schritten:

1.  $T$  wird zu einer Henkin-Theorie  $T^+$  erweitert. Dabei wird auch die Sprache erweitert von  $L$  zu  $L \cup C$ .

2.  $T^+$  wird in  $L \cup C$  vervollständigt zu  $T^*$ . Dann ist auch  $T^*$  eine Henkin-Theorie.

3. Aus  $T^*$  wird ein Modell von  $T^*$  definiert.

Nun zum ersten Schritt, der sogenannten Henkinisierung.

---

<sup>9</sup>Leon Albert Henkin, 1921 – 2006



**Lemma 1.4.15.** *Sei  $T$  widerspruchsfrei. Es gibt eine Konstantenmenge  $C^{10}$  und eine widerspruchsfreie Theorie  $T^+ \supseteq T$ , so dass  $T^+$  eine Henkintheorie mit Konstantenmenge  $C$  ist.*

*Beweis:* Wir betrachten zuerst einen einzigen Erweiterungsschritt. Sei  $\varphi(x)$  eine  $L$ -Formel und  $c$  eine neue Konstante. Dann ist

$$T \cup \{(\exists x\varphi(x) \rightarrow \varphi(c))\}$$

widerspruchsfrei. Dies wollen wir nun zeigen. Angenommen, dies wäre nicht der Fall. Dann gibt es  $n, \psi_i \in T, i < n$ , so dass

$$\vdash_{L \cup \{c\}} \neg \left( \bigwedge_{i < n} \psi_i \wedge (\exists x\varphi(x) \rightarrow \varphi(c)) \right).$$

Wir schreiben zur Abkürzung  $\psi = \bigwedge_{i < n} \psi_i$ . Dann folgt

$$\vdash_{L \cup \{c\}} \neg\psi \vee (\exists x\varphi(x) \wedge \neg\varphi(c)), \quad \vdash_{L \cup \{c\}} \psi \rightarrow \exists x\varphi(x) \quad \text{und} \quad \vdash_{L \cup \{c\}} \psi \rightarrow \neg\varphi(c).$$

Somit gilt für ein neues  $y$

$$\vdash_L \psi \rightarrow \exists x\varphi(x) \quad \text{und} \quad \vdash_L \psi \rightarrow \neg\varphi(y)$$

also nach der  $\forall$ -Einführungsregel

$$\vdash \psi \rightarrow \forall y\neg\varphi$$

Daraus folgt, dass  $\vdash_L \neg\psi$ . Da aber  $\psi_i \in T$  ist, folgt nun dass  $T$  widerspruchsvoll ist, im Gegensatz zur Annahme.

Nun folgt im abzählbaren Fall induktiv über eine Aufzählung aller  $L$ -Formeln oder im überabzählbaren Fall mit dem Lemma von Zorn<sup>11</sup> oder nach dem Wohlordnungssatz, dass wir für jedes  $\varphi(x) \in L$  eine neue Konstante  $c_\varphi$  einführen können, so dass

$$T_1 = T \cup \{(\exists x\varphi(x) \rightarrow \varphi(c_\varphi)) : \varphi \text{ } L\text{-Formel mit nur einer freien Variablen}\}$$

widerspruchsfrei ist.  $T_1$  ist  $L \cup C_1$ -Theorie mit der Konstantenmenge

$$C_1 = \{c_\varphi : \varphi \text{ } L\text{-Formel mit nur einer freien Variablen}\}$$

und enthält Henkin-Sätze für  $L$ -Formeln.

Wir wiederholen den Schritt von  $T = T_0$  auf  $T_1$ : Sei die widerspruchsfreie Theorie  $T_n$  in der Sprache  $L \cup C_1 \cup \dots \cup C_n$  gegeben. Wir definieren:

$$C_{n+1} = \{c_\varphi : \varphi \text{ } L \cup C_1 \cup \dots \cup C_n\text{-Formel mit nur einer freien Variablen}\},$$

$$T_{n+1} = T_n \cup \{(\exists x\varphi(x) \rightarrow \varphi(c_\varphi)) : \varphi \text{ } L \cup C_1 \cup \dots \cup C_n\text{-Formel mit nur einer freien Variablen}\}.$$

<sup>10</sup>Nach dem Studium des zweiten Kapitel wissen Sie:  $|C| \leq \aleph_0 + |L|$

<sup>11</sup>Max August Zorn, 1906 – 1993

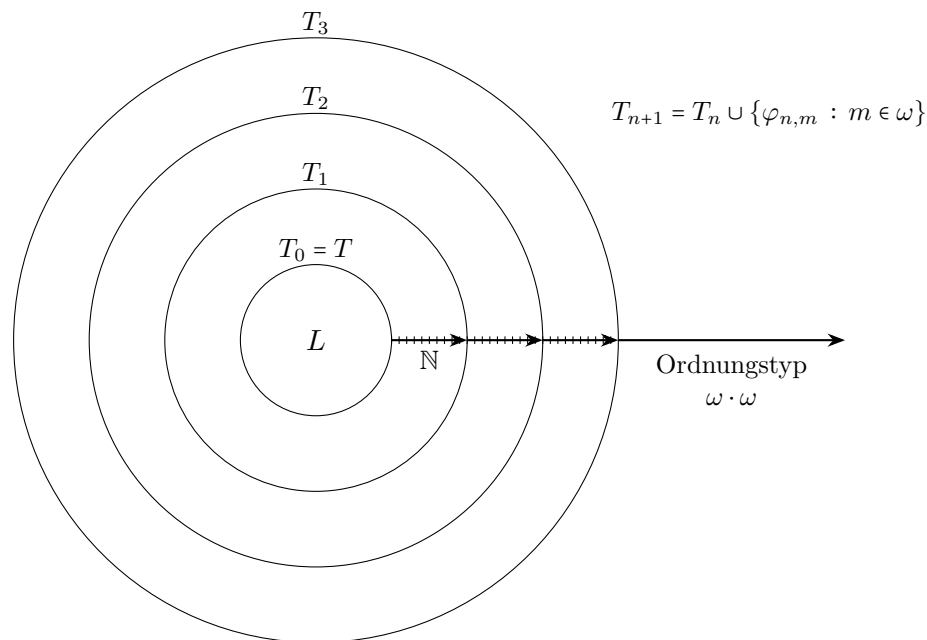
Wenn alle  $T_n, C_n, n \in \mathbb{N}$  definiert sind, setzen wir

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

$$C = \bigcup_{n \in \mathbb{N}} C_n.$$

Aus der Konstruktion folgt, dass  $T^+$  die geforderten Eigenschaften hat.  $\square$

Hier ist ein Bild zur Veranschaulichung der  $\mathbb{N}$  mal  $\mathbb{N}$  vielen Schritte in der Konstruktion der Henkin-Erweiterung für den Fall einer abzählbaren Sprache. Im überabzählbaren Fall muss man das  $\mathbb{N}$  im Bild durch eine geeignete Ordinalzahl ergänzen. Dies lernen Sie im Mengenlehre-Kapitel. Die Bemerkung über den Ordnungstyp werden Sie auch nach dem Studium des Mengenlehre-Kapitels verstehen.



Das folgende Lemma spielt auch in anderem Zusammenhang eine Rolle. Wir wenden es für die Henkin-Konstruktion für die Sprache  $K = L \cup C$  an.

**Lemma 1.4.16.** *Jede widerspruchsfreie  $K$ -Theorie  $T^+$  hat eine im starken Sinne vollständige Obertheorie (in derselben Sprache).*

*Beweis:* Wie im vorigen Beweis betrachten wir zunächst einen einzelnen Erweiterungsschritt. Angenommen  $T^+$  ist widerspruchsfrei und  $T^+ \cup \{\varphi\}$  und  $T^+ \cup \{\neg\varphi\}$  sind widerspruchsvoll. Dann gibt es  $n, m, \psi_i \in T^+, i < n, \chi_j \in T^+, j < m$ , so dass

$$\vdash_K \bigwedge_{i < n} \psi_i \rightarrow \neg\varphi, \quad \vdash_K \bigwedge_{j < m} \chi_j \rightarrow \varphi.$$

Mit der Aussagenlogik folgt

$$\vdash_K \neg \left( \bigwedge_{i < n} \psi_i \wedge \bigwedge_{j < m} \chi_j \right).$$

Also wäre  $T^+$  im Gegensatz zur Voraussetzung widerspruchsvoll.

Im Fall einer höchstens abzählbaren Sprache  $K$  iterieren wir den Einzelschritt. Wir beginnen mit  $T_0^+ = T^+$ . Wir zählen alle  $K$ -Aussagen auf als  $\varphi_n$ ,  $n \in \mathbb{N}$ , und nehmen der Reihe nach jeweils  $\varphi_n$  oder  $\neg\varphi_n$  zu  $T_n^+$  hinzu und setzen  $T_{n+1}^+ = T_n^+ \cup \{(\neg)\varphi\}$ . Am Schluss ist  $T^* = \bigcup_{n \in \mathbb{N}} T_n^+$  wie gewünscht.

Wenn  $K$  überabzählbar ist, nehmen wir das Lemma von Zorn und wenden es an auf die induktive Halbordnung

$$\left( \{ \tilde{T} : \tilde{T} \supseteq T^+, \tilde{T} \text{ widerspruchsfreie } K\text{-Theorie} \}, \subseteq \right)$$

Die Vereinigung jeder  $\subseteq$ -aufsteigenden Kette von widerspruchsfreien Theorien ist widerspruchsfrei. Also gibt es nach Zorn eine maximale widerspruchsfreie Theorie  $T^*$ . Dann ist  $T^* \cup \{\varphi\}$  genau dann widerspruchsfrei, wenn  $\varphi \in T^*$ . Letzteres folgt aus der Maximalität und der Eigenschaft eines einzelnen Erweiterungsschritts. □

**Definition 1.4.17** (deduktiv abgeschlossen). Eine Theorie  $T$  heißt deduktiv abgeschlossen, wenn gilt

$$T \vdash \varphi \Rightarrow \varphi \in T$$

Das folgende Lemma wird bei der Auswertung unserer Konstruktion in Lemma 1.4.21 mehrmals aufgerufen:

**Lemma 1.4.18.** *Jede im starken Sinne vollständige Theorie ist deduktiv abgeschlossen.*

Nicht im Beweis gebraucht wird folgendes Lemma:

**Lemma 1.4.19.** *Jede deduktiv abgeschlossene Theorie ist vollständig genau dann, wenn sie im starken Sinne vollständig ist.*

Da später oft (aber nicht in der Rekursionstheorie!) Theorien mit ihrem deduktiven Abschluss identifiziert werden, arbeitet man dann nur noch mit dem schwächeren Begriff der Vollständigkeit.

**Definition 1.4.20.** Sei  $T^+$  eine vollständige Henkin-Theorie in the Sprache  $L \cup C$ . Wir definieren die Relation  $\sim$  auf den  $L \cup C$ -Termen durch

$$s \sim t \quad :\Leftrightarrow \quad T^+ \vdash s = t.$$

**Lemma 1.4.21.** *Jede vollständige<sup>12</sup> Henkin-Theorie  $T^*$  mit Konstanten  $C$  hat ein (bis auf Isomorphie eindeutig bestimmtes kleinstes) Modell  $\mathfrak{A}^* = (\mathfrak{A}, (c/\sim)_{c \in C})$ . Hierbei ist  $\mathfrak{A}$  eine  $L$ -Struktur.*

*Beweis:* Der Träger von  $\mathfrak{A}$  soll  $A$  sein. Wir setzen

$$A = \{c/\sim : c \in C\}.$$

Wir zeigen zuerst  $A \neq \emptyset$ . Dies folgt aus  $C \neq \emptyset$ . Zum Beispiel  $\varphi = v_0 = v_0$  erhält einen Henkinkonstante.

Mit der Anwendung der Henkinisierung auf die Formel  $\exists v_0 v_0 = t$  folgt:

$$A = \{t/\sim : t \text{ ist } L \cup C\text{-Term ohne freie Variable}\}.$$

Wir setzen nun

$$R^{\mathfrak{A}}(c_0/\sim, \dots, c_{n-1}/\sim) :\Leftrightarrow Rc_0 \dots c_{n-1} \in T^*.$$

Dies ist wohldefiniert, denn es gilt

$$c_i/\sim = d_i/\sim \text{ und } R\bar{c} \in T^* \Rightarrow R\bar{d} \in T^*.$$

Letzteres folgt aus dem Gleichheitsaxiom Lemma 1.3.11 und der deduktiven Abgeschlossenheit von  $T^*$ . Wir definieren weiter:

$$f^{\mathfrak{A}}(c_1/\sim, \dots, c_{n-1}/\sim) = c_0/\sim :\Leftrightarrow f(c_1, \dots, c_n) = c_0 \in T^*.$$

Wiederum folgt aus den Gleichheitsaxiomen und der deduktiven Abgeschlossenheit von  $T^*$ , dass dies woldefiniert ist.

Wir definieren weiter für  $d \in L \cup C$ :

$$d^{\mathfrak{A}} := c/\sim \text{ für ein } c \in C, \text{ so dass } d = c \in T^*.$$

Wiederum folgt aus den Gleichheitsaxiomen und der deduktiven Abgeschlossenheit von  $T^*$ , dass dies woldefiniert ist.

Nun zeigen wir, dass  $\mathfrak{A}$  tatsächlich ein Modell von  $T^*$  ist. Wir zeigen: Für alle  $L \cup C$ -Aussagen  $\varphi$

$$\mathfrak{A}^* \models \varphi \Leftrightarrow \varphi \in T^* \tag{1.4.2}$$

Der Beweis wird wieder induktiv über den Aufbau von  $\varphi$  geführt.

Wir beginnen mit den atomaren Formeln. Sei  $\varphi = t_1 = t_2$  mit Termen ohne freie Variablen. Da jeder Term  $t_i$  mit einer Konstanten übereinstimmt, können wir uns auf Gleichungen des Typs  $c_1 = c_2$  beschränken.

$$\begin{aligned} \mathfrak{A} \models \varphi &\Leftrightarrow c_1/\sim = c_2/\sim \\ c_1/\sim = c_2/\sim &\Leftrightarrow c_1 = c_2 \in T^*. \end{aligned}$$

<sup>12</sup>Nach unserer Definition impliziert die Vollständigkeit die Widerspruchsfreiheit.

Nun noch die atomaren Formeln des Typs  $\varphi = R\bar{t}$ . Da jeder Term mit einer geeigneten Konstanten übereinstimmt, können wir uns auf die atomaren Formeln des Typs  $\varphi = R\bar{c}$  beschränken.

$$\begin{aligned} \mathfrak{A} \models \varphi &\Leftrightarrow (c_0/\sim, \dots, c_{n-1}/\sim) \in R^{\mathfrak{A}} \\ (c_0/\sim, \dots, c_{n-1}/\sim) \in R^{\mathfrak{A}} &\Leftrightarrow Rc_0 \dots c_{n-1} \in T^* \\ Rc_0 \dots c_{n-1} \in T^* &\Leftrightarrow \varphi \in T^*. \end{aligned}$$

Nun folgt der Negationsschritt:  $\varphi = \neg\psi$ .

$$\begin{aligned} \mathfrak{A} \models \varphi &\Leftrightarrow \mathfrak{A} \models \neg\psi \\ \mathfrak{A} \models \neg\psi &\stackrel{\text{I.V.}}{\Leftrightarrow} \psi \notin T^* \\ \psi \notin T^* &\Leftrightarrow \varphi \in T^*. \end{aligned}$$

Die letzte Zeile gilt wegen der Vollständigkeit von  $T^*$ .

Nun der Konjunktionsschritt:  $\varphi = (\varphi_0 \wedge \varphi_1)$ .

$$\begin{aligned} \mathfrak{A}^* \models \varphi &\Leftrightarrow \mathfrak{A} \models \varphi_0 \wedge \varphi_1 \\ \mathfrak{A} \models \varphi_0 \wedge \varphi_1 &\Leftrightarrow \mathfrak{A} \models \varphi_0 \wedge \mathfrak{A} \models \varphi_1 \\ \mathfrak{A} \models \varphi_0 \wedge \mathfrak{A} \models \varphi_1 &\stackrel{\text{I.V.}}{\Leftrightarrow} \varphi_0 \in T^* \text{ and } \varphi_1 \in T^* \\ \varphi_0 \in T^* \text{ and } \varphi_1 \in T^* &\Leftrightarrow (\varphi_0 \wedge \varphi_1) \in T^*. \end{aligned}$$

Dabei gilt die letzte Zeile wegen der deduktiven Abgeschlossenheit von  $T^*$ .

Nun kommt der Quantorenschritt. Sei  $\varphi = \exists x\psi$ . Zuerst die Rückwärtsrichtung der Behauptung (1.4.2). Wir nehmen ein  $c/\sim$  in  $A$ , so dass  $\mathfrak{A} \models \psi(c/\sim)$ . Nach der Induktionsvoraussetzung ist  $\psi(c) \in T^*$ . Weil  $T^*$  deduktiv abgeschlossen ist, folgen  $T^* \vdash \exists x\psi$  und  $\exists x\psi \in T^*$ .

Nun die schwierigere Vorwärtsrichtung in (1.4.2).  $T^+ \subseteq T^*$  enthält alle Henkin-Axiome. Also gilt  $T^* \vdash \exists x\psi \Rightarrow T^* \vdash \psi(c)$  für ein  $c$ . Nach der Induktionsvoraussetzung ist  $\mathfrak{A} \models \psi(c/\sim)$ . Dann gilt auch  $\mathfrak{A} \models \varphi$ .  $\square$

Damit ist endlich der Gödel'sche Vollständigkeitssatz 1.4.7 bewiesen.

**Folgerung 1.4.22.** *Der Kompaktheitssatz. Sei  $T$  eine  $L$ -Theorie.  $T$  hat genau dann ein Modell, wenn jede endliche Teilmenge ein Modell hat.*

*Beweis:* Eine Theorie ist widerspruchsfrei genau dann, wenn jede ihrer endlichen Teilmengen widerspruchsfrei ist.  $\square$

**Definition 1.4.23.** Eine Struktur  $\mathfrak{A}$  heißt abzählbar, wenn ihr Träger  $A$  abzählbar ist. Dies heißt, es gibt eine Bijektion von  $\mathbb{N}$  auf  $A$ . Eine Menge heißt höchstens abzählbar, wenn sie endlich oder abzählbar ist.

**Folgerung 1.4.24.** *Der Satz von Löwenheim und Skolem. Jede erfüllbare Theorie in einer höchstens abzählbaren Sprache hat ein höchstens abzählbares Modell.*

*Jede erfüllbare  $L$ -Theorie Sprache hat ein Modell der Mächtigkeit  $\leq |L| + \aleph_0$ .*

*Beweis:* Wir haben im Falle einer abzählbaren Sprache  $L$  abzählbar viele Henkin-Konstanten eingesetzt. Die Trägermenge  $A$  in der Henkin-Konstruktion ist also endlich oder abzählbar. Im allgemeinen Fall ist  $|C| \leq |L| + \aleph_0$ .  $\square$

Wir weisen noch auf eine Besonderheit der Gleichheitsrelation hin.

**Lemma 1.4.25.**  *$T$  ist widerspruchsfrei  $\Leftrightarrow T(\frac{E}{=}) \cup \{E \text{ ist eine } L\text{-Kongruenzrelation}\}$  ist widerspruchsfrei.*

*Beweis:*

„ $\Rightarrow$ “ Wir interpretieren = durch  $E$ .

„ $\Leftarrow$ “ Sei  $\mathfrak{B}$  ein Modell der Theorie auf der rechten Seite. Wir setzen  $\mathfrak{B} = \mathfrak{A}/E^{\mathfrak{A}}$ . Dies ist wohldefiniert, da  $E^{\mathfrak{A}}$  eine Kongruenzrelation ist. Dann ist  $E^{\mathfrak{A}}$  auf  $B$  die Gleichheit und  $\mathfrak{B}$  ist ein Modell von  $T$ .  $\square$

## 1.5 Elementare Äquivalenz

In Definition 1.2.15 definierten wir für jede Sprache  $L$  eine Äquivalenzrelation auf der Klasse der  $L$ -Strukturen. Wir geben eine recht algebraische Charakterisierung dieser Relation.

**Definition 1.5.1.** Es sei  $L$  eine Symbolmenge. Jede  $L$ -Formel ohne Quantoren hat Quantorenrang 0. Falls  $\varphi$  Quantorenrang  $n$  hat, so hat  $\exists x\varphi$  den Quantorenrang  $n + 1$ . Der Quantorenrang von  $\neg\varphi$  ist gleich dem Quantorenrang von  $\varphi$ , und bei  $(\varphi \vee \psi)$  nimmt man das Maximum der beiden einzelnen Quantorenstände.

Wir schreiben  $\mathfrak{A} \equiv_n \mathfrak{B}$ , falls  $\mathfrak{A}$  und  $\mathfrak{B}$  dieselben Sätze vom Quantorenrang  $\leq n$  erfüllen.

**Definition 1.5.2.** Seien  $\mathfrak{A}$  und  $\mathfrak{B}$   $L$ -Strukturen. Eine Folge  $\langle \mathcal{S}_n : n \in \mathbb{N} \rangle$  von Mengen  $\mathcal{S}_n$  partieller Funktionen  $f$  mit folgenden Eigenschaften heißt *Hin- und Her-System für  $\mathfrak{A}$  und  $\mathfrak{B}$*  oder *Ehrenfeucht-Fraïssé-Spiel für  $\mathfrak{A}$  und  $\mathfrak{B}$* .<sup>13 14</sup>

- 1) Für jedes  $n$  für jedes  $f \in \mathcal{S}_n$  gilt: Der Definitionsbereich  $\text{dom}(f) = A_0$  und das Bild  $\text{im}(f) = f[A_0] = \mathfrak{B}_0$  sind endliche erzeugte Substrukturen von  $\mathfrak{A}$  bzw  $\mathfrak{B}$ . Es gibt also eine endliche Menge  $A_1 \subset A$ , so dass  $\mathfrak{A}_0$  die von  $A_1$  in  $\mathfrak{A}$  erzeugte Substruktur, also der mit der Struktur von  $\mathfrak{A}$  ausgestattete Abschluss  $A_0$  von  $A_1$  unter allen in  $\mathfrak{A}$  interpretierten  $L$ -Termen ist. Analoges gilt auf der  $\mathfrak{B}$ -Seite.

<sup>13</sup> Andrzej Ehrenfeucht, \*1932

<sup>14</sup> Roland Fraïssé, 1920 – 2008

- 2)  $f: \mathfrak{A}_0 \rightarrow \mathfrak{B}_0$  ist ein *partieller Isomorphismus* von  $\mathfrak{A}$ ,  $\mathfrak{B}$ . Das heißt: Für Relationen ist  $f$  treu in beide Richtungen und  $f$  kommutiert mit allen  $L$ -Termen. Für  $f \in \mathcal{S}_n$  und  $A_1 = \{a_0, \dots, a_{k-1}\}$  gilt für alle quantorenfreien  $L$ -Formeln  $\varphi$ :

$$\mathfrak{A} \models \varphi[a_0, \dots, a_{k-1}] \Leftrightarrow \mathfrak{B} \models \varphi[f(a_0), \dots, f(a_{k-1})].$$

- 3) Für jedes  $n$  und jedes  $f \in \mathcal{S}_{n+1}$  und  $a \in A \setminus \text{dom}(f)$  gibt es ein  $g \supseteq f$  mit  $g \in \mathcal{S}_n$ ,  $a \in \text{dom}(g)$  und für jedes  $d \in B \setminus \text{im}(f)$  gibt es ein  $g \supseteq f$  mit  $g \in \mathcal{S}_n$ ,  $d \in \text{im}(g)$ . Diese Eigenschaft nennt man auch die Hin- und Her-Eigenschaft oder die back and forth property.

**Theorem 1.5.3** (Der Satz von Ehrenfeucht und Fraïssé). *Es seien  $\mathfrak{A}$  und  $\mathfrak{B}$   $L$ -Strukturen, und  $L$  sei endlich und enthalte nur Relationssymbole. Es sei  $n \in \mathbb{N}$ . Dann gilt  $\mathfrak{A} \equiv_n \mathfrak{B}$  genau dann, wenn es ein Hin- und Her-System für  $\mathfrak{A}$  und  $\mathfrak{B}$  gibt, bei dem  $\mathcal{S}_n \neq \emptyset$  ist.*

*Beweis:* Es sei  $\langle \mathcal{S}_n : n \in \mathbb{N} \rangle$  ein Hin- und Her-System. Für diese Richtung könnte man auch mit beliebigen Sprachen arbeiten. Induktiv über den Aufbau der  $L$ -Formeln zeigt man für jede  $L$ -Formel  $\varphi$  in  $k$  freien Variablen und vom Quantorenrang  $\leq n$  und alle  $f \in \mathcal{S}_n$  mit  $a_0, \dots, a_{k-1} \in \text{dom}(f)$ :

$$\mathfrak{A} \models \varphi[a_0, \dots, a_{k-1}] \Leftrightarrow \mathfrak{B} \models \varphi[f(a_0), \dots, f(a_{k-1})]$$

Umgekehrt, falls  $\mathfrak{A} \equiv_n \mathfrak{B}$ , so erhält man ein Hin- und Her-System, indem man für  $m \leq n$  in  $\mathcal{S}_m$  genau die Funktionen  $f_0 = \{(a_i, b_i) : i < k\}$ , so dass  $(\mathfrak{A}, a_0, \dots, a_{k-1}) \equiv_m (\mathfrak{B}, b_0, \dots, b_{k-1})$ , aufnimmt. Das  $L$  nur Relationen enthält, ist  $A_0 = \text{dom}([A_1]^{\mathfrak{A}}) = A_1$ .

Nun zeigt man zum Beispiel die Hin-Eigenschaft zum Beispiel von  $\mathcal{S}_1$  auf  $\mathcal{S}_0$ ,  $f_1 \in \mathcal{S}_1$ ,  $\text{dom}(f_1)$  von  $a_0, \dots, a_{k-1}$  erzeugt, indem man für ein neues Element  $a$  alle atomaren und alle negierten atomaren Formeln in den Variablen  $a, a_0, \dots, a_{k-1}$  hinschreibt, die in  $\mathfrak{A}$  an der Stelle  $a, a_0, \dots, a_{k-1}$  gelten, und mit und verbindet und dann  $a$  existentiell abquantifiziert. Hier nutzt man, dass  $L$  endlich und relational ist. Daher gibt es die gerade beschriebene Formel vom Quantorenrang 1 überhaupt. Die Existenz-Formel wird nun auch in  $\mathfrak{B}$  erfüllt, und ein Existenzbeispiel liefert ein  $b$  der gewünschten Art.

Bei höheren Quantorenständen muss man sich ein Zählsystem überlegen, so dass alle Schichten endlich sind. Die unendlich vielen  $L$ -Formeln des Quantorenstands  $n$  in den Parametern  $a, a_0, \dots, a_{k-1}$  haben modulo logischer Äquivalenz nur endlich viele Vertreter.  $\square$

*Bemerkung 1.5.4.* Satz 1.5.3 kann in einige Richtungen verstärkt werden.

Falls  $L$  abzählbar unendlich und relational ist, kann man in den Hin- und Her-Eigenschaften mit einem Sprachvergrößerungsschritt arbeiten. Dann gilt eine Version des Satzes.

Falls  $L$  endlich ist und Funktionssymbole enthält, kann man mit unter allen Termen abgeschlossenen Definitionsbereichen der partiellen Isomorphismen arbeiten. Die algebraische

Treue zwischen  $a$  und  $b$  bezieht sich dann in der Regel auf alle Terme  $t$  in  $a, a_0, \dots, a_{n-1}$ , für die man zudem noch  $t^{\mathfrak{A}}(a, a_0, \dots, a_{n-1}) \in A_0 \cup \{a\}$  voraussetzt. Dann soll

$$f(t^{\mathfrak{A}}(a, a_0, \dots, a_{n-1})) = t^{\mathfrak{B}}(f(a), f(a_0), \dots, f(a_{n-1})) \in B_0 \cup \{b\}$$

gelten. Induktiv über geeignet definierte Termränge kann man auch in dieser sprachlichen Situation eine Version des Satzes erarbeiten.

Falls  $L$ -überabzählbar ist, arbeitet man mit allen abzählbaren Teilmengen. Eine abgewandelte Version des Satzes gilt dann noch immer, denn  $\mathfrak{A} \equiv \mathfrak{B}$  ist äquivalent dazu, dass die Verkürzungen von  $\mathfrak{A}$ ,  $\mathfrak{B}$  auf jede endliche Teilmenge der Symbolmenge jeweils elementar äquivalent sind.

*Beispiel 1.5.5.*

- (1) Es sei  $L = \emptyset$ . Dann sind die  $L$ -Strukturen  $\mathbb{N}$  und  $\mathbb{R}$  elementar äquivalent. Man nimmt  $\mathcal{S}_n = \{(n_i, r_i) : i < k, \forall j, i < k (n_i = n_j \leftrightarrow (r_i = r_j))\}$ .
- (2) Es sei  $L = \{<\}$  mit einem zweistelligen Relationssymbol. Es seien  $k, \ell \in \mathbb{N}$ . Dann sind die  $L$ -Strukturen  $(\{0, \dots, k\}, <)_n \equiv_n (\{0, \dots, \ell\}, <)$  genau dann, wenn

$$\begin{aligned} \mathcal{S}_n = & \{(a_i, b_i) : i < k, \forall i, j < k \\ & (d(a_i, a_j) = d(b_i, b_j) \vee d(a_i, a_j), d(b_i, b_j) \geq 2^n \vee d(a_i, a_j), d(b_i, b_j) \leq -2^n)\} \neq \emptyset \end{aligned}$$

Hierbei ist  $d(a_i, a_j) = a_i - a_j$ .

Ähnlich kann man in abstrakteren Ordnungen verfahren, indem man die Anzahl der Elemente zwischen  $a_i$  und  $a_j$  mit Vorzeichen als Abstand definiert. Falls es zwischen je zwei Elementen unendlich viele Elemente gibt, ist  $\mathcal{S}_n$  unabhängig von  $n$ .



# Kapitel 2

## Mengenlehre

### 2.1 Das Axiomensystem von Zermelo und Fraenkel

Die Sprache der Mengenlehre ist  $L_{Me} = \{\epsilon\}$  (oder eine definitorische Erweiterung hiervon). Die atomare Formel  $x \in y$  bedeutet, dass  $x$  ein Element von  $y$  ist. Eine Besonderheit der Mengenlehre ist, dass man auch mit Modellen arbeitet, deren Träger keine Menge, sondern eine Klasse ist.

Zunächst stellen wir uns die Frage, was ist eine Menge? Dazu schauen wir uns zunächst die Definition von Cantor<sup>1</sup> an.

**Definition** (Cantors Definition einer Menge). Unter einer „Menge“  $M$  verstehen wir jede Zusammenfassung von bestimmten wohlunterschiedenen Objekten  $m$  unserer Anschauung oder unseres Denkens (welche „Elemente“ von  $M$  genannte werden) zu einem Ganzen.

Gottlieb Frege<sup>2</sup> versuchte (um 1880), Cantors Definition erststufig zu formalisieren. Sein Axiomensystem sieht wie folgt aus:

**Extensionalitätsaxiom:**

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

**Axiom der vollen Komprehension:** Für alle  $\varphi(x, \bar{y}) \in L(\epsilon)$  gilt

$$\forall \bar{y} \exists x \forall z (z \in x \leftrightarrow \varphi(z, \bar{y}))$$

**Satz 2.1.1** (Satz von Russell). <sup>3</sup> *Das Frege'sche Axiomensystem ist widerspruchsvoll.*

---

<sup>1</sup>Georg Cantor, 1845 – 1918

<sup>2</sup>Friedrich Ludwig Gottlob Frege, 1848 – 1925

<sup>3</sup>Bertrand Arthur William Russell, 1872 – 1970

*Beweis:* Wir nehmen zu

$$\varphi = \neg y \in y$$

nach dem Frege'schen Komprehensionsaxiom  $\exists x \forall y (y \in x \leftrightarrow y \notin y)$  ein solches  $x$ . Dann gilt:

**1. Fall:**  $x \in x \rightarrow x \notin x$ .

**2. Fall:**  $x \notin x \rightarrow x \in x$ .

In jedem Fall führt die Existenz eines solchen  $x$  zu einem Widerspruch. □

Ein Axiomensystem ist eine Theorie, die als unbewiesene, unbeweisbare Grundlage für weitere Folgerungen dient. Lesen Sie im Duden oder auf der Wikipedia die Definition von "Axiom" nach.

**Definition 2.1.2.** Die Axiome von Zermelo<sup>4</sup> und Fraenkel<sup>5</sup> und das Auswahlaxiom bilden das Axiomensystem ZFC, welches aus einzelnen Axiomen und zwei Axiomenschemata besteht. Im einzelnen sind diese

Extensionalitätsaxiom	Ersetzungsschema
Aussonderungsschema	Fundierungsaxiom
Paarmengenaxiom	Unendlichkeitsaxiom
Vereinigungsaxiom	Auswahlaxiom
Potenzmengenaxiom	

Die Axiome werde nun nacheinander erklärt. Wir schreiben für jedes Axiom oder Schema zuerst eine deutsche Formulierung und dann eine  $L_{Me}$ -Formulierung.

**Extensionalitätsaxiom (Ext):** „Jede Menge ist durch ihre Elemente bestimmt.“

$$\forall xy (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

Wir schreiben als Abkürzung

$$x \subseteq y := \forall z (z \in x \rightarrow z \in y).$$

Außerdem können wir schließen, dass gilt

$$\forall xy (x \subseteq y \wedge y \subseteq x \rightarrow x = y).$$

**Aussonderungsschema (Auss):** „Definierbare Teilklassen von Mengen sind Teilmengen.“

Für jede  $L_{Me}$ -Formel  $\varphi$  gilt:

$$\forall y_0 \dots y_{n-1} \forall u \exists x \forall z (z \in x \leftrightarrow (z \in u \wedge \varphi(u, z, \bar{y}))).$$

<sup>4</sup>Ernst Friedrich Ferdinand Zermelo, 1871 – 1953

<sup>5</sup>Abraham Halevi (Adolf) Fraenkel, 1891 – 1965

Bemerkung: Wir schreiben:

$$x = \{z \in u : \varphi(z, \bar{y}, u)\}.$$

Aus diesem Axiom folgt die Existenz des Schnittes  $x \cap y = \{z \in x : z \in y\}$  und des Komplementes  $x \setminus y = \{z \in x : z \notin y\}$  von zwei Mengen, sowie die Existenz der leeren Menge  $\emptyset = \{z \in x : z \neq z\}$ .

**Paarmengenaxiom (Paar):** Zu je zwei Mengen gibt es eine Menge, die mindestens diese beiden als Elemente enthält.

$$\forall x \forall y \exists z (x \in z \wedge y \in z).$$

Wir schreiben als Abkürzung:

$$\{x, y\} \text{ ist ein } z, \text{ so dass } x \in z \text{ und } y \in z \text{ und } \forall u (u \in z \rightarrow u = x \vee u = y).$$

**Vereinigungsaxiom:** „Zu jeder Menge (von Mengen) gibt es eine Obermenge der Vereinigungsmenge.“

$$\forall y \exists x \forall z (z \in y \rightarrow z \subseteq x).$$

Mit der Aussonderung haben wir dann auch die genaue Vereinigungsmenge. Wir schreiben folgende Abkürzungen

$$\bigcup y := \{z : \exists w (w \in y \wedge z \in w)\} = \bigcup_{w \in y} w;$$

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

Somit haben wir alle endlichen Mengen per Induktion über die natürlichen Zahlen auf ihre Elemente zurückgeführt. Falls  $n \in \mathbb{N}$  und die Existenz der Mengen  $y_0, \dots, y_{n-1}$  aus ZFC folgt, so folgt also auch die Existenz von  $\{x_0, \dots, x_{n-1}\}$ . Der Induktionsschritt ist folgender:

$$\{y_0, \dots, y_n\} = \{y_0, \dots, y_{n-1}\} \cup \{y_n\}$$

**Potenzmengenaxiom (Pot):** „Zu jeder Menge gibt es eine Obermenge ihrer Potenzmenge.“

$$\forall y \exists x \forall z (z \subseteq y \rightarrow z \in x).$$

Wir schreiben für die genaue Potenzmenge, die aus einem  $x$  wie im Axiom ausgesondert werden kann,

$$\mathcal{P}(y) = \{z : z \subseteq y\}.$$

**Ersetzungsschema:** „Jede Operation  $\varphi(x, y, \bar{w})$  auf einem mengenkleinen Definitionsbereich  $u$  gibt es eine Obermenge der Bildmenge der Operation“

$$\forall u\bar{w}(\forall x(x \notin u \vee \exists^1 y\varphi(x, y, \bar{w})) \rightarrow \exists b\forall x(x \in u \rightarrow \exists y(y \in b \wedge \varphi(x, y, \bar{w}))).$$

Hierbei verwendeten wir die Abkürzung:

$$\exists^1 y\varphi(y) \equiv \exists(\varphi(y) \wedge \forall y'\varphi(y') \rightarrow y = y').$$

**Fundierungsaxiom (Fund):** „In jeder nicht leeren Menge gibt es mindestens ein  $\epsilon$ -minimales Element.“

$$\forall x(x \neq \emptyset \rightarrow \exists y \in x \ y \cap x = \emptyset).$$

Man sagt  $x$  ist fundiert, wenn  $x = \emptyset$  oder  $\exists y \in x \ y \cap x = \emptyset$ . Man sagt  $x$  ist erblich fundiert, wenn alle  $y \in \text{tcl}(x)$  (siehe Def. 2.1.36) fundiert sind.

Der folgende Satz führt tief in die Grundlagen:

**Satz 2.1.3.** *Wenn ZF  $\setminus$  Fund widerspruchsfrei ist, so auch ZF.*

*Beweis:* Wir nehmen ein Modell  $(N, E)$  von ZF  $\setminus$  Fund. Dann bilden wir

$$M := \{m \in M : (N, E) \models m \text{ ist erblich fundiert}\}.$$

Man rechnet nach, dass  $(M, E \cap M \times M)$  nun ZF erfüllt. Wie das genau geht, steht zum Beispiel in Folgerung 2.1.41.  $\square$

**Unendlichkeitsaxiom:** „Es gibt eine unter der Operation  $x \mapsto x \cup \{x\}$  abgeschlossene Menge.“

$$\exists x(\emptyset \in x \wedge \forall y \in x \ y \cup \{y\} \in x).$$

Hierbei verwendeten wir folgende Abkürzung:

$$\exists x \in y\varphi(x) \text{ für } \exists x(x \in y \wedge \varphi(x)).$$

Man kann ein  $x$  veranschaulichen durch:  $x$  ist Obermenge der „einfachen“ unendlichen Menge  $w$ , wobei

$$w = \{\emptyset, \emptyset \cup \{\emptyset\}, \emptyset \cup \{\emptyset\} \cup \{\emptyset, \{\emptyset\}\}, \dots\}.$$

**Auswahlaxiom (AC):** „Jede Menge nicht leerer Mengen hat eine Auswahlfunktion.“

$$\forall x(\emptyset \notin x \rightarrow \exists f(f: x \rightarrow \bigcup x \wedge \forall z \in x \ f(z) \in z)).$$

Aus den obigen Axiomen des ZFC ergeben sich folgende Definitionen und Erkenntnisse:

**Satz 2.1.4** (aus Auss, Ext). *Die Klasse aller Mengen ist keine Menge.*

*Beweis:* Ansonsten gäbe es eine Menge  $V$ , die Menge aller Mengen wäre. Dann wäre allerdings nach dem Aussonderungsschema auch die

$$\{x \in V : x \notin x\}$$

eine Menge, was nach Satz 2.1.1 zu einem Widerspruch führt.  $\square$

**Definition 2.1.5** (aus Paar). Wir definieren das Kuratowski-Paar<sup>6</sup> aus zwei Mengen wie folgt:

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

**Lemma 2.1.6** (aus Ext, Auss und Paar). *Das Kuratowski-Paar verhält sich wie ein geordnetes Paar, d.h.,*

$$\forall xyx'y' (\langle x, y \rangle = \langle x', y' \rangle \rightarrow (x = x' \wedge y = y')).$$

**Definition 2.1.7.** Das kartesische Produkt aus  $a$  und  $b$  ist

$$a \times b := \{\langle x, y \rangle : x \in a, y \in b\}.$$

**Lemma 2.1.8** (aus Auss, Paar und Pot).  $a \times b$  existiert.

*Beweis:*

$$\{x, y\} \in \mathcal{P}(a \cup b),$$

$$\langle x, y \rangle \in \mathcal{P}(\mathcal{P}(a \cup b)),$$

$$\{\langle x, y \rangle : x \in a, y \in b\} \text{ definiert eine definierbare Teilmenge von } \mathcal{P}(\mathcal{P}(\mathcal{P}(a \cup b))),$$

und existiert also nach dem Paarmengen-, Vereinigungsmengen-, Potenzmengenaxiom und dem Aussonderungsschema.  $\square$

### 2.1.1 Exkurs über definitorische Spracherweiterungen

Wir sagten zu Anfang, dass die Sprache der Mengenlehre  $L_{Me}$  sei. Nun haben wir aber im Laufe der Einführung von ZFC schon etliche zusätzliche Symbole definiert, wie z.B.  $\emptyset$ ,  $\subseteq$ ,  $\cap$ ,  $\cup$ ,  $\cup$ ,  $\mathcal{P}$ ,  $\{\dots\}$ . Wir diskutieren nun die Ausdrucksstärke dieser neuen Zeichen.

**Definition 2.1.9.** (Einführung neuer Relationszeichen)

Sei  $T$  eine  $L$ -Theorie und sei  $\varphi_R(\bar{x})$  eine  $L$ -Formel. Sei  $R$  ein neues  $n$ -stelliges Relationszeichen,  $L' = \{R\} \cup L$  und  $T' = T \cup \{\forall \bar{x} (\varphi_R(\bar{x}) \leftrightarrow R(\bar{x}))\}$ .  $T'$  heißt definitorische Erweiterung von  $T$ .

**Satz 2.1.10.**

---

<sup>6</sup>Kazimierz Kuratowski, 1896 – 1980

- 1) Für jede  $L$ -Formel  $\varphi$  gilt:  $T' \vdash \varphi \Leftrightarrow T \vdash \varphi$ .
- 2) Für jede  $L'$ -Formel  $\psi$  existiert eine  $L$ -Formel  $\varphi$ , so dass  $T' \vdash \psi \leftrightarrow \varphi$ .

*Beweis:*

- 1) Folgt durch Verwendung von  $\vDash$  anstelle von  $\vdash$ . Betrachte zum Beispiel  $\subseteq$ .
- 2) Der Beweis läuft induktiv über  $\psi$ .

□

**Definition 2.1.11.** (Einführung neuer Funktionszeichen)

Sei  $T \vdash \forall \bar{x} \exists^1 y \varphi_f(y, \bar{x})$ , und sei  $f \notin L$ , außerdem sei  $f$   $n$ -stellig,  $L' = L \cup \{f\}$ . Dann heißt die  $L'$ -Theorie  $T \cup \{\forall \bar{x} \varphi_f(f\bar{x}, \bar{x})\}$  definitorische Erweiterung von  $T$ .

Wie zum Beispiel  $\cup, \cap, \{\}, \mathcal{P}, (x, y) \mapsto \langle x, y \rangle, (x, y) \mapsto x \times y, \dots$

**Satz 2.1.12.**

- 1) Für jede  $L$ -Formel  $\varphi$  gilt:  $T' \vdash \varphi \Leftrightarrow T \vdash \varphi$ .
- 2) Für jeden  $L'$ -Term  $t'$  existiert ein  $L$ -Term  $t$ , so dass  $T' \vdash t' = t$ .
- 3) Für jede  $L'$ -Formel  $\psi$  existiert eine  $L$ -Formel  $\varphi$ , so dass  $T' \vdash \psi \leftrightarrow \varphi$ .

*Beweis:* Wir zeigen nur den neuen Punkt 3. Jedes  $T$  Modell  $\mathfrak{A}$  lässt sich zu einem  $T'$  Modell  $\mathfrak{A}'$  erweitern. Sei  $\psi$  zum Beispiel folgende atomare Formel

$$\varphi = R(t_0, t_1), \quad t_0 = s_0(f\bar{s}, \bar{u}),$$

Dann wählen wir

$$\varphi' = \exists x_0 (\varphi_f(x_0, \bar{s}) \wedge (R(s_0(x_0, \bar{u}), t_1)))'.$$

□

**Definition 2.1.13** (Definitorische Erweiterung). Eine Erweiterung einer Theorie durch die Definition neuer Relationszeichen, Funktionszeichen und Konstantenzeichen heißt definitorische Erweiterung.

Wie oben beweist man:

**Satz 2.1.14.** Sei  $L' \supseteq L$  und sei  $T$  eine  $L$ -Theorie und sei  $T'$  die Erweiterung von  $T$  und genau die Definitionen der Symbole in  $L' \setminus L$ .

- 1) Für jede  $L$ -Formel  $\varphi$  gilt:  $T' \vdash \varphi \Leftrightarrow T \vdash \varphi$ .
- 2) Für jeden  $L'$ -Term  $t'$  existiert ein  $L$ -Term  $t$ , so dass  $T' \vdash t' = t$ .
- 3) Für jede  $L'$ -Formel  $\psi$  existiert eine  $L$ -Formel  $\varphi$ , so dass  $T' \vdash \psi \leftrightarrow \varphi$ .

Nicht jede konservative Erweiterung ist definitorisch. Ein Beispiel ist die Obertheorie NBG von ZFC. NBG steht für von Neumann<sup>7</sup>, Bernays<sup>8</sup> und Gödel.

<sup>7</sup>John von Neumann, 1903 – 1957

<sup>8</sup>Paul Isaac Bernays, 1888 – 1977

**Definition 2.1.15.** Das Axiomensystem NBG erhält man, indem man mit Klassenvariablen arbeitet und ein Prädikat

$$M(X) :\Leftrightarrow \exists Y X \in Y$$

für Mengen einführt.  $\exists x\varphi$  steht kurz für  $\exists x(M(x) \wedge \varphi)$ .

Das Extensionalitätsaxiom gilt für Klassen.

Das Komprehensionsschema wird durch ein Klassenschema ersetzt: Für jede Formel  $\varphi$ , in der die Quantoren nur über Mengen rangieren, gibt es eine Klasse  $A$ , so dass

$$A = \{x : \varphi(x, \bar{Z})\}.$$

Hier können in  $\varphi$  Klassen als Parameter  $\bar{Z}$  vorkommen. Dann lautet in NBG das Komprehensionsaxiom:

$$\forall x \forall A (M(x) \rightarrow M(x \cap A)).$$

Im Ersetzungsschema wird die Formel  $\varphi$  durch eine Klassenvariable  $F$  ersetzt und mit  $\forall F$  abquantifiziert. Dann lautet in NBG das Ersetzungsschema:

$$\forall u \forall F ((M(u) \wedge \forall x \in u \exists^1 y F(x) = y) \rightarrow M(F''x)).$$

Die Fundierung, die Extensionalität und alle anderen Mengenexistenz-Axiome von ZFC werden übernommen.

Jedoch gilt: Jede konservative Erweiterung  $T'$  in  $L'$ , in der jede  $L'$ -Formel in  $T'$  beweisbar zu einer  $L$ -Formel äquivalent ist, ist definitorisch.

*Beispiele 2.1.16.* Relationszeichen:  $\subseteq, f : a \rightarrow b$ .

Funktionszeichen:  $\{z \in x : \varphi(z, \bar{y})\}, x \cup y, x \cap y, x \setminus y, \cup x, \mathcal{P}(x), \{x, y\}, \{y_1, \dots, y_n\}, \langle x, y \rangle, x \times y, f(x)$ .

Konstantenzeichen:  $\emptyset$ .

Damit sei die Natur der Spracherweiterungen nun genügend diskutiert. Es werden noch zahlreiche Spracherweiterungen folgen. Wir kehren zur Mengenlehre zurück.

## Natürliche Zahlen und Ordinalzahlen

Von nun an sind alle Sätze so zu lesen: ZFC (mit allen seinen bis jetzt getroffenen definitorischen Erweiterungen) beweist den jeweiligen Satz. Der jeweilige Satz gilt also in jedem ZFC-Modell oder anders gesprochen, in jedem Mengenuniversum. Überlicherweise schreibt man  $(V, \epsilon)$  für ein ZFC-Modell.  $V$  ist hierbei die jeweilige Klasse aller Mengen. Es gibt verschiedene ZFC-Modelle. Um allerdings zwei nicht elementar äquivalente ZFC-Modelle zu konstruieren, muss man schon etliche Wochen Technik studieren, zB Jech [3] oder Kunen [4].

**Definition 2.1.17** (Mengentheoretische natürliche Zahlen). (Diesen sind unendlich viele Definitionen.) Für  $n \in \mathbb{N}$  definieren wir

$$\begin{aligned} \underline{0} &:= \emptyset \\ \underline{1} &:= \{\emptyset\} &&= \{\underline{0}\} \\ \underline{2} &:= \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} &&= \{\underline{0}, \underline{1}\} \\ \underline{3} &:= \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} &&= \{\underline{0}, \underline{1}, \underline{2}\} \\ \underline{n+1} &:= \underline{n} \cup \{\underline{n}\} &&= \{\underline{0}, \dots, \underline{n}\} \end{aligned}$$

$\underline{n}$  heißt von Neumann'sche natürliche Zahl.

**Satz 2.1.18.**

- 1) Ist  $m < n$ , dann gilt  $\text{ZFC} \vdash \underline{m} \in \underline{n}$ .
- 2) Es gilt
  - a)  $\text{ZFC} \vdash \underline{n} = \{\underline{0}, \dots, \underline{n-1}\}$ .
  - b) Für  $m \neq n$  gilt  $\text{ZFC} \vdash \underline{n} \neq \underline{m}$ .
  - c) Für  $m > n$   $\text{ZFC} \vdash \underline{m} \notin \underline{n}$ .

*Beweis per Induktion:*

- 1)  $n = 0$  ✓  
 $n \rightarrow n + 1$  Also  $m < n + 1$ .

$$\text{ZFC} \vdash \begin{cases} \underline{n} \in \underline{n} \cup \{\underline{n}\}, & \text{falls } m = n \\ \underline{m} \in \underline{n} \cup \{\underline{n}\}, & \text{falls } m < n \end{cases}$$

- 2) a)  $n = 0$  ✓  
 $n \rightarrow n + 1$  Dann gilt

$$\text{ZFC} \vdash \underline{n} \cup \{\underline{n}\} = \{\underline{0}, \dots, \underline{n-1}\} \cup \{\underline{n}\}.$$

- b) Wir verwenden 1) und das Fundierungsaxiom wie folgt. Es ist  $m < n$  oder  $n < m$ . Wir nehmen oBdA das erstere an. Dann beweist nach 1)  $\text{ZFC} \vdash \underline{m} \in \underline{n}$ . Nun folgt aus dem Fundierungsaxiom  $\underline{n} \notin \underline{n}$ . Also ist  $\text{ZFC} \vdash \underline{m} \neq \underline{n}$ .
- c) Induktiv über  $n$ .  $n = 0$  folgt aus der Definition von  $\emptyset$ . Sei nun  $n' = n + 1$  und  $m \geq n'$ . Dann ist  $m \geq n$  und daher nach I.V.  $\text{ZFC} \vdash \underline{m} \notin \underline{n}$ . Da  $m \neq n$ , ist nach Aussage b) auch  $\text{ZFC} \vdash \underline{m} \neq \underline{n}$ . Insgesamt haben wir  $\text{ZFC} \vdash \underline{m} \notin \underline{n}'$ .

□

Nun starten wir mit einer alternativen erststufigen Definition.

**Definition 2.1.19.** Eine Menge  $x$  heißt *transitiv*, wenn  $\forall y \in x, y \subseteq x$ .



Beispiele:  $\emptyset$ ,  $\{\emptyset\}$ ,  $\{\emptyset, \{\emptyset\}\}$ , für jedes  $x$  ist  $\bigcup\{\bigcup^{(n)} x : n \in \mathbb{N}\}$  transitiv.  
 Gegenbeispiele:  $\{\{\emptyset\}\}$ , allgemein  $\{x\}$ , falls  $x \neq \emptyset$ .

**Definition 2.1.20** (Wohlordnung). Eine Menge oder Klasse mit einer zweistelligen Relation  $(A, <_A)$  heißt Wohlordnung, wenn gilt:  $A = \emptyset$  oder  $(A, <_A)$  ist eine lineare Ordnung, in der jede nicht leere Teilmenge ein  $<_A$ -kleinstes Element hat.

**Definition 2.1.21** (fundierte Relation). Eine Menge oder Klasse mit einer zweistelligen Relation  $(A, <_A)$  heißt fundiert, wenn gilt: Jede nicht leere Teilmenge ein  $<_A$ -minimales Element.

In Fund gilt für alle Mengen  $A$ :  $(A, \epsilon)$  ist lineare Ordnung impliziert  $(A, \epsilon)$  ist eine Wohlordnung.

Nun folgt eine sagenannte “interne” Definition, d.h. eine erststufige Definition der natürlichen Zahlen.

**Definition 2.1.22** (Natürliche Zahl). Eine Menge  $x$  ist eine natürliche Zahl, wenn gilt:

- (a)  $x$  ist transitiv,
- (b)  $(x, \epsilon)$  ist eine Wohlordnung.
- (c)  $\forall y (y \in x \vee y = x \rightarrow y = \emptyset \vee \exists z y = z \cup \{z\})$ .

**Definition 2.1.23** (endliche Menge). Eine Menge  $x$  heißt endlich, wenn es es eine von Neumann’sche Zahl  $\underline{n}$  und eine Bijektion von  $\underline{n}$  auf  $x$  gibt.

Überlegen Sie, warum diese Definition tatsächlich erststufig ist.

**Satz 2.1.24.** *Jedes von Neumann’sche  $\underline{n}$  ist eine natürliche Zahl im Sinne von Definition 2.1.22.*

*Beweis:* Induktiv über  $\mathbb{N}$ . □

Nun folgt die nächste erststufige Definition:

**Definition 2.1.25** (Ordinalzahl). Eine Menge  $x$  ist eine Ordinalzahl, wenn gilt:

- (a)  $x$  ist transitiv.
- (b)  $(x, \epsilon)$  ist eine Wohlordnung.

Wir schreiben dann  $x \in \text{On}$ . Gewöhnlich nimmt man kleine griechische Buchstaben als Variablen für Ordinalzahlen.

In Fund gilt für alle Mengen  $A$ :  $(A, \epsilon)$  ist lineare Ordnung impliziert  $(A, \epsilon)$  ist eine Wohlordnung.

Nun definieren wir ein neues Konstantenzeichen:

**Definition 2.1.26.** Sei  $x$  eine Menge wie im Unendlichkeitsaxiom. Wir definieren

$$\omega = \{y \in x : y \text{ ist eine natürliche Zahl}\}.$$

Man überlegt sich, dass diese Definition nicht von der Wahl des  $x$  abhängt.

**Satz 2.1.27.** Jedes  $\underline{n}$ ,  $n \in \mathbb{N}$ , ist eine Ordinalzahl, und  $\omega$  ist eine Ordinalzahl.

**Satz 2.1.28** (Vollständige Induktion in  $\omega$ ).

$$\forall x((x \subseteq \omega \wedge \emptyset \in x \wedge \forall n(n \in x \rightarrow n \cup \{n\} \in x)) \rightarrow x = \omega).$$

Nun gilt  $x$  ist eine von Neumann'sche natürliche Zahl, genau dann wenn

$$\bigvee_{n \in \mathbb{N}} x = \underline{n}.$$

Aber wie kann man das Laufen über die Standard-natürlichen Zahlen  $\mathbb{N}$  erststufig aufschreiben? Das geht nach Kompaktheit nicht.

**Satz 2.1.29.** Es sei nun  $(V, \epsilon) \models \text{ZFC}$  und  $\omega$  sei in  $V$  definiert. Falls  $\omega$  von außen gesehen fundiert ist, gilt:  $\omega$  enthält nur die von Neumann'schen natürlichen Zahlen. Falls  $\omega$  von außen gesehen nicht fundiert ist, dann gibt es Zahlen in  $\omega$ , die keine von Neumann Zahlen sind.

*Beweis:*  $\emptyset$  ist eine von Neumann-Zahl. Wenn  $n$  eine von Neumann-Zahl ist, so auch  $n \cup \{n\}$ . Wenn nun  $X = \{u : u \in \omega \wedge \bigvee_{n \in \mathbb{N}} u = \underline{n}\}$  nicht ganz  $\omega$  ist, dann sieht seine Fortsetzung in  $\omega$  wie  $\mathbb{Z}$  aus und es gibt also eine absteigende Kette, denn jedes Element in  $\omega \setminus \{0\}$  hat einen Vorgänger. Wenn  $X \in V$ , dann ist nach dem Induktionsprinzip  $X = \omega$ .  $X \in V$  gilt genau dann, wenn es keine absteigende Kette oberhalb von  $X$  gibt.

Wir nehmen nun an, dass ZFC konsistent ist. Es gibt nach dem Kompaktheitssatz auch Modelle  $(V, \epsilon) \models \text{ZFC}$ , in denen es in  $\omega$  eine unendliche absteigende  $\epsilon$ -Kette gibt und in denen es also eine nicht-standard Zahl  $\gamma$  gibt, so dass  $(V, \epsilon) \models \gamma \in \omega$ . Die Menge  $X$  der Standard-natürlichen Zahlen  $\{\underline{n} : n \in \mathbb{N}\}$  ist eine echte Teilklasse von  $\omega^V$  in so einem  $V$ . Aber sie ist keine Teilmenge. Denn  $(V, \epsilon)$  erfüllt das Induktionsaxiom, und das  $x$  im Induktionsprinzip läuft über die Teilmengen von  $\omega$ , die es im Modell  $V$  gibt.  $\square$

Der folgende Sätze sind mit Klassenvariablen (großen Buchstaben) formuliert. Durch Beschränkung auf definierbare Klassen kommt man nach ZFC zurück. Wir folgen also nun der Konvention:  $\forall X \subseteq \text{On}$  steht für alle  $\varphi(x, \bar{z})$  und  $X = \{x \in \text{On} : \varphi(x, \bar{z})\}$ . Die folgenden zwei Sätze sind also eigentlich Schemata von Sätzen. Man vergleiche mit NBG in Def. 2.1.15.

**Satz 2.1.30.**

- 1)  $\text{On}$  ist durch  $\in$  linear geordnet.
- 2) Jede transitive Teilmenge  $S \subseteq \text{On}$  ist selbst eine Ordinalzahl.
- 3) Jede nicht leere Teilklasse  $X$  von  $\text{On}$  hat ein  $\in$  kleinstes Element.
- 4) Für alle  $\alpha \in \text{On}$  gilt  $\alpha = \{\beta \in \text{On} : \beta < \alpha\}$
- 5)  $\text{On}$  ist eine echte Klasse, also keine Menge. (Paradoxon von Burali-Forti)

*Beweis:*

- 1) Für die Irreflexivität,  $\forall \alpha \alpha \notin \alpha$  kann man ohne Fundierungsaxiom arbeiten oder einfach das Fundierungsaxiom benutzen. Wir zeigen nun die Vergleichbarkeit. Seien  $\alpha, \beta \in \text{On}$ , dann ist  $\alpha \cap \beta \in \text{On}$ .

1. Fall:  $\alpha \cap \beta = \alpha$ , dann ist  $\alpha \subseteq \beta$ , also  $\alpha = \beta$  oder  $\alpha \in \beta$ .

2. Fall:  $\alpha \cap \beta = \beta$

3. Fall:  $\alpha \cap \beta \in \alpha, \alpha \cap \beta \in \beta \Rightarrow \alpha \cap \beta \in \alpha \cap \beta \not\checkmark$ .

Die Transitivität beweist man mit ähnlichen Mitteln.

- 2)  $(S, \in)$  ist linear geordnet und transitiv.

- 3) Sei  $X \neq \emptyset$  und  $\alpha \in X$ .

1. Fall:  $\alpha = \min(X)$

2. Fall:  $\alpha \neq \min(X) \Rightarrow X \cap \alpha \neq \emptyset$ . Also ist  $X \cap \alpha$  eine Menge und fundiert. Da  $\in$  auf  $\text{On}$  eine transitive Relation ist, ist jedes  $\in$ -Minimum von  $X \cap \alpha$  auch ein  $\in$ -Minimum von  $X$ .<sup>9</sup>

- 4)  $\beta \in \alpha \wedge \alpha \in \text{On} \Rightarrow \beta \in \text{On}$ .

- 5)  $(\text{On}, \in)$  ist linear geordnet. Wenn  $\text{On}$  eine Ordinalzahl wäre, so wäre  $\text{On} \in \text{On}$ , was der Irreflexivität in Teil 1) widerspricht.

□

**Satz 2.1.31** (Der Induktionssatz für  $\text{On}$  (mit Klassenvariablen)).

$$\forall X \subseteq \text{On} ((\forall \alpha \in \text{On} (\alpha \subseteq X \rightarrow \alpha \in X)) \rightarrow X = \text{On}).$$

*Beweis:* sonst wäre  $\alpha = \min(\text{On} \setminus X)$ .  $\alpha \subseteq X \wedge \alpha \notin X \not\checkmark$ .

□

**Definition 2.1.32.** Sei  $\alpha \in \text{On}$

- 1)  $\alpha$  heißt Nachfolger, wenn gilt

$$\exists z \quad z \cup \{z\} = \alpha \quad \text{und} \quad z \in \text{On}.$$

<sup>9</sup>Für nicht notwendig transitive Relationen, braucht man an dieser Stelle vom Schritt von Mengen auf Klassen eine zusätzliche Überlegung, siehe Satz 2.1.39

2)  $\alpha$  heißt Limes-Ordinalzahl, wenn  $\alpha \neq \emptyset$  und  $\alpha$  kein Nachfolger ist.

Wir bleiben auch für den folgenden Satz bei der Abkürzung, dass große Buchstaben für definierbare Klassen stehen. Dann ist es ein Satz von ZFC. Diese können auch definierbare Klassen von Paaren sein. Wir nennen so eine Klasse Operation, falls es zu jedem  $x$  aus dem Definitionsbereich (der auch eine Klasse sein kann) genau ein  $y$  aus dem Zielbereich gibt, so dass das geordnete Paar  $\langle x, y \rangle$  in der Klasse liegt.

**Satz 2.1.33.** *Der Rekursionssatz für On. Sei  $G: V \rightarrow V$  eine Operation. Dann gibt es genau eine Operation  $F: \text{On} \rightarrow V$ , so dass*

$$\forall \alpha \quad F(\alpha) = G(F \upharpoonright \alpha).$$

*Beweis:* Wir zeigen zuerst die Eindeutigkeit. Wir nehmen an, dass es zwei verschiedene Lösungen  $F_1, F_2$  gibt. Sei  $\alpha = \min \{\alpha' : F_1(\alpha') \neq F_2(\alpha')\}$ . Dann gilt

$$F_1(\alpha) = G(F_1 \upharpoonright \alpha) = G(F_2 \upharpoonright \alpha) = F_2(\alpha).$$

Im Widerspruch zu  $F_1(\alpha) \neq F_2(\alpha)$ .

Nun zeigen wir die Existenz: Wir definieren  $f_\alpha : \alpha \rightarrow \text{On}$ .  $f_\emptyset = \emptyset$ .

$$f_{\alpha+1} = f_\alpha \cup \{(\alpha, G(f_\alpha))\}.$$

Nun sei  $\lambda$  limes. Hier folgt die Existenz aus dem Ersetzungsschema. Wir setzen

$$f_\lambda = \bigcup \{f_\alpha : \alpha < \lambda\}.$$

Zum Schluss setzt man  $F = \bigcup_{\alpha \in \text{On}} f_\alpha$ . □

Nun folgt eine typische durch Rekursion über  $(\text{On}, \epsilon)$  gegebene Definition:

**Definition 2.1.34.** Die von Neumann-Hierarchie  $(V_\alpha)_{\alpha \in \text{On}}$  und die fundierte Allklasse  $V_{\text{fund}}$  sind in  $\text{ZFC} \setminus \{\text{Fund}\}$  gegeben durch:

$$\begin{aligned} V_\emptyset &= \emptyset, \\ V_{\alpha+1} &= \mathcal{P}(V_\alpha) = G(F \upharpoonright \alpha + 1) \text{ für } \alpha \in \text{On}, \\ V_\lambda &= \bigcup_{\alpha < \lambda} V_\alpha = G(F \upharpoonright \lambda) \text{ für Limesordinalzahlen } \lambda, \\ V_{\text{fund}} &= \bigcup_{\alpha \in \text{On}} V_\alpha \text{ heißt die fundierte Allklasse oder das von Neumann'sche Universum.} \end{aligned}$$

Sie können die zugrundeliegende definierbare Operation  $G$  selbst definieren.

**Definition 2.1.35.**

- 1) Eine Klasse  $X$  heißt transitiv, wenn  $\forall y \in X y \subseteq X$ .
- 2) Eine zweistellige Relation  $R$  heißt transitiv, wenn  $(\forall x, y, z)(xRy \wedge yRz \rightarrow xRz)$ .

Nun folgt eine Rekursion nur über  $\omega \cup \{\omega\}$ :

**Definition 2.1.36.** [tcl(transitive closure)] Sei  $x$  eine Menge. Wir definieren den transitiven Abschluss von  $x$ ,  $\text{tcl}(x)$  genannt.

$$t_0(x) = \{x\}, \quad t_{n+1}(x) = t_n(x) \cup \bigcup t_n(x), \quad \bigcup_{n \in \omega} t_n(x) = \text{tcl}(x)$$

### Das stärkste Rekursionsgesetz in ZFC

Nun folgt ein ‘‘sportlicher’’ Teil der Vorlesung: Das stärkste Rekursionsgesetz in ZFC. Daraus folgern wir, dass das Fundierungsaxiom nicht zu einem Widerspruch beitragen kann, s. Satz 2.1.3 und Satz 2.1.42.

**Definition 2.1.37** (Mengenähnlich). Sei  $(A, R)$  eine möglicherweise klassengroße Struktur.  $(A, R)$  heißt mengenähnlich<sup>10</sup>, wenn für jedes  $a \in A$ ,

$$\{b \in A : bRa\}$$

eine Menge ist.

**Definition 2.1.38** (transitiver Abschluss einer Relation). Sei  $R$  eine zweistellige mengenähnliche Relation.

$$R_0 = R, \quad R_{n+1} = \{(x, y) : \exists z(xR_n z \wedge zRy)\}, \quad \bigcup_{n \in \omega} R_n = R^{\text{trans}}.$$

**Satz 2.1.39** (von der Induktion über eine fundierte, mengenähnliche Relation  $R$ ). Sei  $(A, R)$  fundiert und mengenähnlich. Sei  $R^{\text{trans}}$  der transitive Abschluss von  $R$ . Dann gilt

- 1) Auch  $R^{\text{trans}}$  ist fundiert und mengenähnlich. Zusätzlich ist  $R^{\text{trans}}$  transitiv.
- 2) Jede nicht leere Teilklasse von  $A$  ein  $R$ -minimales Element. Anders formuliert: Das Induktionsgesetz gilt:

$$\forall X \subseteq A((X \neq \emptyset \wedge \forall x \in A(\forall y(yRx \rightarrow y \in X) \rightarrow x \in X) \rightarrow X = A))$$

- 3) Das Rekursionsgesetz gilt:

$$\forall G : V \rightarrow V \exists^1 F : A \rightarrow V, \quad (\forall a \in A)F(a) = G(F \upharpoonright \{b : bRa\})$$

<sup>10</sup>auch vorgängerklein oder mengenartig genannt

*Beweis:* 1) Folgt aus Definition 2.1.37 der Mengenähnlichkeit und dem Ersetzungsschema.

2) Man zeigt die Behauptung zunächst für  $R^{\text{trans}}$  statt  $R$ . Da  $R^{\text{trans}}$  transitiv ist, kann man den Beweis des Punktes 3 des Satzes 2.1.30 wörtlich übernehmen. Dann überlegt man sich, dass  $R^{\text{trans}}$ -Minima auch  $R$ -Minima sind.

3) Die Existenz wird rekursiv  $R^{\text{trans}}$  gezeigt. Wir definieren für  $s \in \text{dom}(R)$  ein Anfangssück  $f_a$ , so dass

$$\text{dom}(f_a) = \{b : bR^{\text{trans}}a \vee b = a\}.$$

Sei  $f_b$  für alle  $bR^{\text{trans}}a$  definiert. Dann setzen wir

$$f_a = \bigcup \{f_b : bR^{\text{trans}}a\} \cup \{(a, G(\bigcup \{f_b : bR^{\text{trans}}a\} \upharpoonright \{b : bRa\}))\}.$$

Zum Schluss setzt man  $F = \bigcup \{f_a : a \in A\}$ . Einen ausführlichen Beweis findet man in [4, Seite 42 – 53].  $\square$

Als Anwendung zeigen wir einen Satz über  $\epsilon$ -Induktion. Wir wenden also Punkt (2) des Satzes 2.1.39 auf  $R = \epsilon$  an.

**Satz 2.1.40.**

$$\text{ZF} \setminus \text{Fund} \vdash (\text{Fund} \leftrightarrow \forall x \exists \alpha x \in V_\alpha).$$

*Beweis:* Die leichtere Rückwärtsrichtung ergibt sich daraus, dass alle Elemente von  $V_\alpha$  fundierte Mengen sind. Dies zeigt man induktiv über  $\alpha$  (mit dem Induktionssatz für Ordinalzahlen).

Die schwerere Vorwärtsrichtung zeigt man durch  $\epsilon$ -Induktion über das ganze Mengenumversum  $V$ . Annahme  $x$  ist  $\epsilon$ -minimal, so dass es kein  $\alpha$  gibt, so dass  $x \in V_\alpha$ . Dann ist jedes Element  $y \in \text{tcl}(x)$  in einem  $V_{\alpha_y}$ . Man kann das kleinste  $\alpha_y$  nehmen und braucht so nicht auf das Auswahlaxiom zurückzugreifen. Nach dem Ersetzungsschema gibt es eine Ordinalzahl

$$\beta := \bigcup \{\alpha_y : y \in \text{tcl}(x)\}.$$

Aber dann ist  $x \subseteq V_\beta$  und somit  $x \in V_{\beta+1}$ . Widerspruch.  $\square$

**Satz 2.1.41.**

$$\text{ZF} \setminus \text{Fund} \vdash (V_{\text{fund}} \models \text{ZF}).$$

$$\text{ZFC} \setminus \text{Fund} \vdash (V_{\text{fund}} \models \text{ZFC}).$$

Damit ist auch Satz 2.1.3 bewiesen, und es gilt auch

**Theorem 2.1.42.** *Falls  $\text{ZFC} \setminus \text{Fund}$  widerspruchsfrei ist, so auch ZFC.*

Nun endet der extrem sportliche Exkurs. Ab jetzt nehmen wir die Fundierung an und erhalten dann nach Satz 2.1.40

$$V_{\text{fund}} = V.$$

## Der Wohlordnungssatz und das Lemma von Zorn

Wir kehren zur Rekursion über die Ordinalzahlen zurück. In linearen Ordnungen sind die Minima eindeutig.

**Lemma 2.1.43.** *Jede Wohlordnung ist zu genau einer Ordinalzahl isomorph.*

*Beweis:* Sei  $(a, <)$  eine gegebene Wohlordnung, hier gestatten wir auch die leere Struktur  $a = \emptyset$ . Wir definieren  $F: \text{On} \rightarrow a \cup \{a\}$  rekursiv über die Ordinalzahlen. Sei  $F$  auf  $\beta$  schon definiert. Wir schreiben

$$F[\beta] = \{F(\gamma) : \gamma \in \beta\}.$$

Wir setzen

$$F(\beta) := \begin{cases} \text{das } < \text{-minimale Element von } (a \setminus F[\beta]), & \text{falls } F[\beta] \neq a \\ a, & \text{sonst.} \end{cases}$$

Außerdem ist  $a \in \text{Im}(F)$ , da sonst  $F: \text{On} \xrightarrow{\text{inj.}} a$  und dann  $\text{On} = F^{-1}a = F^{-1}[a]$  eine Menge wäre. Also ist

$$\exists \alpha \quad \alpha = \min \{\beta : F(\beta) = a\}$$

wohldefiniert. Wir setzen  $f = F \upharpoonright \alpha$ . Dann gilt

$$f: (\alpha, <) \cong (a, <).$$

Wir zeigen nun, dass  $f$  und  $\alpha$  eindeutig sind. Sei  $f'$  mit  $\alpha'$  eine zweite Lösung, dann folgt per Induktion über  $\beta \in \alpha \cup \{\alpha\}$ , dass  $f'(\beta) = f(\beta)$ .  $\square$

**Satz 2.1.44** (Die Äquivalenz von AC und "Jede Menge hat eine Wohlordnung"<sup>11</sup>).

$$\text{ZF} \vdash (\text{AC} \leftrightarrow \text{jede Menge hat eine Wohlordnung.})$$

*Die Vorwärtsrichtung wird auch der Wohlordnungssatz genannt.*

*Beweis:* Für die leichte Rückwärtsrichtung sei eine Menge  $x$  nicht leerer Mengen gegeben und sei  $<$  eine Wohlordnung der Menge  $\cup x$ . Wir definieren  $f(z)$  als das  $<$ -kleinste Element von  $z$ , für  $z \in x$ . Da  $z \in x$  impliziert  $z \subseteq \cup x$ , gibt es in der Wohlordnung  $(\cup x, <)$  ein  $<$ -kleinstes Element von  $z$ . Also ist  $f$  eine Auswahlfunktion auf  $x$ .

Nun die schwerere Vorwärtsrichtung. Es sei  $a$  eine Menge. Wir nehmen eine Auswahlfunktion  $g$  auf  $\mathcal{P}(a) \setminus \{\emptyset\}$ . Nun definieren wir rekursiv über  $\text{On}$  mithilfe des Parameters  $g$  die folgende Operation  $F: \text{On} \rightarrow a \cup \{a\}$ :

$$F(\alpha) = \begin{cases} g(a \setminus F[\alpha]), & \text{wenn } F[\alpha] \neq a; \\ a, & \text{wenn } F[\alpha] = a. \end{cases}$$

<sup>11</sup>Zermelo 1904

Wie im vorigen Beweis argumentiert man, dass es eine Ordinalzahl  $\alpha$  gibt, so dass  $F[\alpha] = a$ , da  $F$  injektiv ist. Wir nehmen das minimale  $\alpha$ . Dann ist  $F \upharpoonright \alpha: \alpha \xrightarrow{\text{bij.}} a$ . Wir definieren nun eine Wohlordnung  $<$  auf  $a$ , indem wir für  $x, y \in a$

$$x < y := F^{-1}(x) \in F^{-1}(y)$$

setzen. □

**Definition 2.1.45.**

- 1) Sei  $H \in V$ ,  $H \neq \emptyset$ . Eine Struktur  $(H, <_H)$  heißt *Halbordnung*, wenn  $<_H$  eine irreflexive, transitive zweistellige Relation ist.
- 2) Ein Element  $m \in H$  heißt *maximales Element* von  $(H, <_H)$ , falls  $(\forall g \in H)(\neg g >_H m)$ .
- 3) Sei  $G \subseteq H$ .  $s \in H$  heißt  $\leq_H$ -*obere Schranke* von  $G$ , falls für alle  $g \in G$ ,  $g \leq_H s$ . Eine obere Schranke von  $G$ , die kein Element von  $G$  ist, heißt *echte obere Schranke* von  $G$ .

**Satz 2.1.46** (Zorn'sches Lemma). *Sei  $(H, <_H)$  eine partielle Ordnung, in der jede linear geordnete Menge eine  $\leq_H$ -obere Schranke hat. Dann hat  $H$  ein  $<_H$ -maximales Element.*

*Beweis:* Wir nehmen eine Auswahlfunktion  $g$  auf  $\mathcal{P}(H) \setminus \{\emptyset\}$ . Nun definieren wir rekursiv über  $\text{On}$  mithilfe des Parameters  $g$  die folgende Operation  $F: \text{On} \rightarrow H \cup \{H\}$ :

$$F(\alpha) = \begin{cases} g(\text{Menge der echten oberen Schranken von } F[\alpha]), & \text{wenn } F[\alpha] \\ & \text{eine echte obere Schranke hat;} \\ H, & \text{sonst.} \end{cases}$$

Wie im vorigen Beweis argumentiert man, dass es eine Ordinalzahl  $\alpha$  gibt, so dass  $F[\alpha]$  keine echte obere Schranke hat, da  $F$  injektiv ist. Wir nehmen das minimale  $\alpha$ , so dass  $F[\alpha]$  keine echte obere Schranke hat. Dann ist  $\alpha$  eine Nachfolgerzahl. Dies sieht man wie folgt: Nach Konstruktion ist die Menge  $F[\alpha]$  eine  $<_H$ -Kette und müsste daher eine obere Schranke haben. Jede obere Schranke dieser Kette  $F[\alpha]$  von Limeslänge  $\alpha$  wäre aber eine echte obere Schranke, im Widerspruch zur Wahl von  $\alpha$ . Wir haben also  $\alpha = \beta + 1$  und  $F(\beta)$  ist ein maximales Element von  $H$ . □

**Satz 2.1.47** (Ultrafiltertheorem). *Jeder Filter lässt sich zu einem Ultrafilter erweitern.*

*Beweis:* Es sei

$$H = (\{F' : F' \supseteq F, F' \text{ Filter}\}, \subseteq).$$

nach dem Zorn'schen Lemma (Proposition 2.1.46) existiert ein Maximum in  $H$ . □

Der folgende Satz ist weit jenseits dieser Vorlesung.

**Satz 2.1.48.** (Satz von Halpern-Lévy, 1965)<sup>12</sup> (ZF und das Ultrafiltertheorem)  $\neq$  ZFC.

<sup>12</sup>Azriel Lévy, geboren 1934, J. D. Halpern, Daten nicht bekannt



## 2.2 Die ordinale Addition, Multiplikation und Exponentiation

Wie immer schreiben wir  $S(\beta) = \beta + 1 = \beta \cup \{\beta\}$  für  $\beta \in \text{On}$ .

**Definition 2.2.1** (Ordinale Addition). Für jede feste On  $\gamma$  definieren wir induktiv über  $\beta$  die ordinale Summe  $\gamma + \beta$ <sup>13</sup>

$$\begin{aligned}\gamma + 0 &= \gamma; \\ \gamma + S(\beta) &= S(\gamma + \beta) \text{ für } \beta \in \text{On}; \\ \gamma + \lambda &= \bigcup_{\beta < \lambda} \gamma + \beta \quad \text{für } \lambda \text{ Limesordinalzahl.}\end{aligned}$$

**Definition 2.2.2** (Ordinale Multiplikation). Für jedes feste On  $\gamma$  definieren wir induktiv über  $\beta$  das ordinale Produkt  $\gamma \cdot \beta$

$$\begin{aligned}\gamma \cdot 0 &= 0; \\ \gamma \cdot S(\beta) &= \gamma \cdot \beta + \gamma \text{ für } \beta \in \text{On}; \\ \gamma \cdot \lambda &= \bigcup_{\beta < \lambda} \gamma \cdot \beta \quad \text{für } \lambda \text{ Limesordinalzahl.}\end{aligned}$$

**Definition 2.2.3** (Ordinale Exponentiation). Für jedes feste On  $\gamma$  definieren wir induktiv über  $\beta$

$$\begin{aligned}\gamma^0 &= 1; \\ \gamma^{\beta+1} &= \gamma^\beta \cdot \gamma \text{ für } \beta \in \text{On}; \\ \gamma^\lambda &= \bigcup_{\beta < \lambda} \gamma^\beta \quad \text{für } \lambda \text{ Limesordinalzahl.}\end{aligned}$$

**Lemma 2.2.4.**

- 1)  $\alpha + \beta = \alpha + \gamma \rightarrow \beta = \gamma$ .
- 2)  $1 + \omega = 0 + \omega \neq \omega + 1$ .
- 3)  $2 \cdot \omega = \omega \neq \omega \cdot 2$ .
- 4)  $2^\omega = \omega \neq \omega^2$ .

Warnung: Später wird auch die kardinale Exponentiation mit  $x^y$  geschrieben. Dann ist  $2^\omega \neq \omega$ , denn  $2^\omega$  kardinal ist überabzählbar.

<sup>13</sup>Vorsicht: Keine der drei zweistelligen Operationen ist kommutativ.

## 2.3 Kardinalzahlen

**Definition 2.3.1** (Gleichmächtig, schwächtiger als). Seien  $a, b$  Mengen. Wir definieren die folgenden drei Relationen:

$a \sim b$ :  $a$  ist *gleichmächtig wie*  $b$ , wenn es eine Funktion  $f$  gibt, so dass  $f: a \xrightarrow{\text{bij.}} b$ .

$a \leq b$ :  $a$  ist *schwächtiger als oder gleich wie*  $b$ , wenn es eine Funktion  $f$  gibt, so dass  $f: a \xrightarrow{\text{inj.}} b$ .

$a < b$ :  $a$  ist *echt schwächtiger als*  $b$ , wenn  $a \leq b$  und nicht  $a \sim b$ .

**Definition 2.3.2** (Mächtigkeit). Die Mächtigkeit  $|a|$  einer Menge  $a$  ist die kleinste Ordinalzahl, die gleichmächtig zu  $a$  ist.

Das folgende ist eine Folgerung aus dem Wohlordnungssatz 2.1.44.

*Bemerkung 2.3.3.* 1) In ZFC hat jede Menge  $a$  eine Mächtigkeit, denn man kann unter den Wohlordnungen auf  $a$  die kürzesten nehmen.

2)

ZF  $\vdash$  („jede Menge hat eine Mächtigkeit“  $\leftrightarrow$  AC).

**Lemma 2.3.4.**

1)  $a \sim b \Leftrightarrow |a| = |b|$

2)  $a \leq b \Leftrightarrow |a| \leq |b|$

*Beweis:* Beide Richtungen beider Teilbehauptungen folgen aus dem folgenden kommutativen Diagramm:

$$\begin{array}{ccc}
 |a| & \xrightarrow{\text{id}_{|a|}} & |b| \\
 \text{bij. } g \uparrow & & \downarrow \text{bij. } g' \\
 a & \overset{\text{---}}{\xrightarrow{f}} & b
 \end{array}$$

Einmal ist  $f$  gegeben, und einmal ist die Wohldefiniertheit der Identität gegeben. □

**Definition 2.3.5** (Kardinalzahl).  $\alpha \in \text{On}$  heißt eine Kardinalzahl, wenn  $\alpha = |\alpha|$ .

**Lemma 2.3.6.** *Alle von Neumann'schen natürlichen Zahlen und  $\omega$  sind Kardinalzahlen.*

*Beweis:* Wir schreiben statt  $\underline{n}$  nur  $n$ . Sei  $n < m$ , dann folgt

$$\neg \exists f : n \xrightarrow{\text{bij.}} m.$$

Dies zeigt man induktiv über  $n$ . Für  $n = \emptyset$  ist die Behauptung klar. Sei nun  $n < m+1 = m'$ . Dann ist  $n-1 < m$ . Sei  $f : n \rightarrow m'$ . Wenn  $f$  bijektiv wäre, dann gäbe es ein  $n^- < n$ , so dass  $f(n^-) = m$ . Wir können nach einer Permutation  $p$  von  $n$  und Ersetzung von  $f$  durch  $f \circ p$  annehmen, dass  $f \circ p(n-1) = m$ . Dann ist aber

$$(f \circ p) \upharpoonright (n-1) : n-1 \xrightarrow{\text{bij.}} m,$$

im Widerspruch zur Induktionsvoraussetzung. □

**Definition 2.3.7** (Endlich, abzählbar).

Eine Menge  $a$  heißt endlich, wenn  $|a| < \omega$ .

Eine Menge  $a$  heißt abzählbar, wenn  $|a| = \omega$ .

Eine Menge  $a$  heißt höchstens abzählbar, wenn  $|a| \leq \omega$ .

*Bemerkung 2.3.8.*

- $a$  ist genau dann abzählbar, wenn  $a$  unendlich ist und  $a \leq \omega$ .
- $a$  ist genau dann abzählbar, wenn  $a$  unendlich ist und  $\exists f : \omega \xrightarrow{\text{surj.}} a$ .

**Satz 2.3.9** (Satz von Cantor). *Für jede Menge  $a$  gilt in ZF:*

$$(\forall f)(\neg f : a \xrightarrow{\text{surj.}} \mathcal{P}(a)).$$

Da  $a \leq \mathcal{P}(a)$ , hat man

$$a < \mathcal{P}(a).$$

Mit AC hat man:

$$|a| < |\mathcal{P}(a)|$$

*Beweis:*  $x \mapsto \{x\}$  ist eine Injektion von  $a$  in  $\mathcal{P}(a)$ , daher ist  $a \leq \mathcal{P}(a)$ . Angenommen

$$f : a \xrightarrow{\text{surj.}} \mathcal{P}(a).$$

Wir betrachten die Menge

$$b = \{x \in a : x \notin f(x)\}$$

Da  $f$  surjektiv ist, ist  $b \in \text{Bild}(f)$ . Wir halten ein  $x \in a$  fest, so dass  $f(x) = b$ . Dann gilt

$$x \in b \leftrightarrow x \notin f(x) = b.$$

Widerspruch. □

**Folgerung 2.3.10** (Potenzaxiom Pot). *Es existiert keine größte Kardinalzahl.*

**Satz 2.3.11.** *Hartogs-Nachfolger<sup>14</sup>. Zu jeder Kardinalzahl  $|\alpha|$  gibt es eine nächstgrößere  $\alpha^+ = |\alpha|^+$  genannt. Diese sieht wie folgt aus:*

$$\alpha^+ = \sup \left\{ \beta + 1 \in |\mathcal{P}(\alpha)| + 1 : \exists f : \beta \xrightarrow{\text{bij.}} \alpha \right\}$$

*Beweis:* Nach dem Satz von Cantor ist  $\alpha^+ \leq |\mathcal{P}(\alpha)|$ , also  $\alpha^+ \in |\mathcal{P}(\alpha)| + 1$ . Da letzteres eine transitive Menge ist, gilt  $\alpha^+ \subseteq |\mathcal{P}(\alpha)| + 1$ . Nach dem Aussonderungsschema ist  $M = \left\{ \beta + 1 \in |\mathcal{P}(\alpha)| + 1 : \exists f : \beta \xrightarrow{\text{bij.}} \alpha \right\}$  eine Menge.

$\alpha^+$  ist eine Kardinalzahl, denn gäbe es ein  $\gamma < \alpha^+$ , so dass  $\gamma$  gleichmächtig zu  $\alpha^+$  ist, so wäre  $\alpha^+ \in M$  und damit auch  $\alpha^+ + 1 \in M$ . Aber dann könnte  $\alpha^+$  nicht das Supremum von  $M$  sein.  $\square$

Falls  $\alpha$  unendlich ist, gilt auch

$$\alpha^+ = \sup \left\{ \beta \in |\mathcal{P}(\alpha)| + 1 : \exists f : \beta \xrightarrow{\text{bij.}} \alpha \right\}.$$

Denn in diesem Fall ist  $\sup(M)$  eine Limesordinalzahl.

**Satz 2.3.12.** *Sei  $K \subseteq \text{On}$  eine Menge von Kardinalzahlen, dann ist  $\bigcup K$  eine Kardinalzahl.*

*Beweis:* (Skizze) Falls  $K$  ein größtes Element  $\mu$  hat, so ist  $\bigcup K = \mu$  eine Kardinalzahl. Andernfalls ist  $\bigcup K$  die kleinste Kardinalzahl, die größer als jedes Element von  $K$  ist. Dies zeigt man mit einer ähnlichen Überlegung wie im vorigen Beweis.  $\square$

**Definition 2.3.13.** Man schreibt  $\aleph$  und spricht Aleph.

$$\begin{aligned} \aleph_0 &= \omega_0 = \omega \\ \aleph_{\alpha+1} &= (\aleph_\alpha)^+ \\ \aleph_\lambda &= \bigcup_{\alpha < \lambda} \aleph_\alpha \end{aligned}$$

$\{\aleph_\alpha : \alpha \in \text{On}\}$  ist die Klasse der unendlichen Kardinalzahlen.

Es gilt  $|\mathcal{P}(\aleph_0)| \geq \aleph_1$  und allgemein gilt  $|\mathcal{P}(\aleph_\alpha)| \geq \aleph_{\alpha+1}$ .

**Definition 2.3.14.** Die Aussage  $|\mathcal{P}(\aleph_0)| = \aleph_1$  heißt die Kontinuumshypothese und wird oft mit CH abgekürzt.

Mit Forcing kann man zeigen:  $\text{ZFC} \not\vdash \text{CH}$  und  $\text{ZFC} \not\vdash \neg\text{CH}$ . Man sagt: Die Kontinuumshypothese ist von ZFC unabhängig.

<sup>14</sup>Friedrich Moritz Hartogs, 1874 – 1943

**Satz 2.3.15** (Satz von Hessenberg). *Für jede Ordinalzahl  $\delta$  gilt:*

$$|\aleph_\delta \times \aleph_\delta| = \aleph_\delta.$$

*Beweis:* Wir definieren eine Wohlordnung auf  $\aleph_\delta$

$$(\alpha, \beta) <_H (\alpha', \beta') := (\max(\alpha, \beta), \alpha, \beta) <_3 (\max(\alpha', \beta'), \alpha', \beta').$$

Hierbei ist  $<_3$  die folgende Wohlordnung:

$$(\alpha, \beta, \gamma) <_3 (\alpha', \beta', \gamma'),$$

wenn  $\max(\alpha, \beta) < \max(\alpha', \beta')$  oder  
 $(\max(\alpha, \beta) = \max(\alpha', \beta') \text{ und } \alpha < \alpha')$  oder  
 $(\max(\alpha, \beta) = \max(\alpha', \beta') \text{ und } \alpha = \alpha' \text{ und } \beta < \beta')$ .

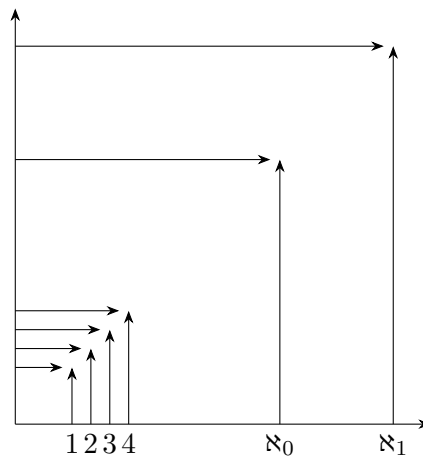
Nun zeigen wir:

$$(\aleph_\delta \times \aleph_\delta, <_H) \cong (\aleph_\delta, \epsilon).$$

Dies sieht man wie folgt: Sei  $(\alpha, \beta) \in \aleph_\alpha \times \aleph_\alpha$ . Dann gilt  $\max(\alpha, \beta) < \aleph_\delta$ . Daher ist

$$|\{(\gamma, \delta) : (\gamma, \delta) <_H (\alpha, \beta)\}| < \aleph_\delta.$$

Jede Wohlordnung, in der alle Vorgängermengen die Mächtigkeit  $< \aleph_\delta$  haben, ist von Länge höchstens  $\aleph_\delta$ .



□

**Frage 2.3.16.** Für Kenner(innen) der normalen (i.e., monoton wachsenden, stetigen) Funktionen auf den Ordinalzahlen fragen wir: Gibt es ein  $\gamma \in (\aleph_0, \aleph_1)$ , so dass

$$(\gamma \times \gamma, <_H) \cong (\gamma, \epsilon)$$

ist?

## 2.4 Metamathematik von ZFC

Wir ordnen jeder  $L_{\text{Me}}$ -Formel  $\varphi$  eine Konstante  $\ulcorner \varphi \urcorner \in \omega$  in einer definitorischen Erweiterung von ZFC zu.

**Definition 2.4.1.** Wir fixieren eine (erststufig beschreibbare) Injektion  $b : \omega \times \omega \rightarrow \omega$ , z.B.  $b(m, n) = \frac{1}{2}(m+n)(m+n+1) + m$ .

$$\begin{array}{llll} \ulcorner v_i \urcorner := b(\underline{1}, \underline{i}) & \ulcorner = \urcorner := b(\underline{0}, \underline{0}) & \ulcorner \epsilon \urcorner := b(\underline{0}, \underline{1}) & \ulcorner \neg \urcorner := b(\underline{0}, \underline{2}) \\ \ulcorner \wedge \urcorner := b(\underline{0}, \underline{3}) & \ulcorner \exists \urcorner := b(\underline{0}, \underline{4}) & \ulcorner ( \urcorner := b(\underline{0}, \underline{5}) & \ulcorner ) \urcorner := b(\underline{0}, \underline{6}) \end{array}$$

Seien  $p_i, i \in \mathbb{N}$ , die Primzahlen in aufsteigender Reihenfolge.

$$\ulcorner \varphi \urcorner = \ulcorner \zeta_0 \dots \zeta_{n-1} \urcorner = \prod_{i < n} p_i^{\ulcorner \zeta_i \urcorner + 1}.$$

**Definition 2.4.2** (Gödelnummer).  $\ulcorner \varphi \urcorner$  heißt Gödelnummer von  $\varphi$ .

Wir kehren zurück zum Substitutionslemma aus dem ersten Kapitel. Sei  $\varphi$  eine  $L$ -Formel mit einer freien Variablen  $v_0$ . Dann bezeichnen wir mit  $\varphi(\underline{n})$  die Ersetzung  $\varphi \frac{\underline{n}}{v_0}$ . Da der Term  $\underline{n}$  keine freien Variablen oder wiederum  $v_0$  als freie Variable hat (wenn  $\underline{n} = \underline{n}(v_0)$  von  $v_0$  aus brechnet wird), ist  $v_0$  frei für  $\underline{n}$  in  $\varphi$ , die Ersetzung also gestattet.

**Lemma 2.4.3.** Es gibt eine in ZFC definierbare Funktion  $\text{Sub}$ , so dass für alle  $L_{\text{Me}}$ -Formeln  $\varphi(x)$  und  $\chi$  gilt

$$\text{ZFC} \vdash \ulcorner \varphi(\ulcorner \chi \urcorner) \urcorner = \text{Sub}(\ulcorner \varphi \urcorner, \ulcorner \chi \urcorner).$$

*Beweis:* (Skizze)

$$\text{Sub}(x, y) = z \leftrightarrow \exists w (w \in V_\omega \wedge \delta(w, x, y, z) \wedge \text{Definition on } x \mapsto \ulcorner x \urcorner)$$

Hierbei ist die Formel  $\delta$  gegeben durch

$$\begin{aligned} (u, v, w) &:= \langle u, \langle v, w \rangle \rangle, \text{ und} \\ \delta(w, x, y, z) &= (\forall (u, v, u') \in w) \forall n \forall \zeta_0 \dots \forall \zeta_{n-1} \in u \\ &\quad (u = \ulcorner \zeta_0 \dots \zeta_{n-1} \urcorner \wedge \zeta_i = \ulcorner v_0 \urcorner \rightarrow u' = \ulcorner \zeta_0 \dots v \dots \zeta_{n-1} \urcorner) \wedge \\ &\quad (x, y, z) \in w \end{aligned}$$

$w$  beschreibt den Graphen einer Ersetzungsfunktion. □

**Satz 2.4.4** (Fixpunktsatz). Zu jeder  $L_{\text{Me}}$ -Formel  $\Sigma(v_0)$  gibt es einen Satz  $\varphi$ , so dass

$$\text{ZFC} \cup \{\text{Definition von } \ulcorner \cdot \urcorner, \text{Sub}\} \vdash \varphi \leftrightarrow \Sigma(\ulcorner \varphi \urcorner).$$

*Beweis:* Wir betrachten die Formel  $\psi(v_0)$ , so dass

$$\text{ZFC} \cup \{\text{Definition von } \ulcorner \urcorner, \text{Sub}\} \vdash \psi(v_0) \leftrightarrow \Sigma(\text{Sub}(v_0, v_0)).$$

Dann gilt

$$\begin{aligned} \text{ZFC} \cup \{\text{Definition von } \ulcorner \urcorner, \text{Sub}\} &\vdash \text{Sub}(\ulcorner \psi \urcorner, \ulcorner \psi \urcorner) = \ulcorner \psi(\ulcorner \psi \urcorner) \urcorner, \text{ und} \\ \text{ZFC} \cup \{\text{Definition von } \ulcorner \urcorner, \text{Sub}\} &\vdash \Sigma(\text{Sub}(\ulcorner \psi \urcorner, \ulcorner \psi \urcorner)) \leftrightarrow \Sigma(\ulcorner \psi(\ulcorner \psi \urcorner) \urcorner). \end{aligned}$$

Der Satz

$$\varphi = \psi(\ulcorner \psi \urcorner)$$

hat also die gesuchten Eigenschaften.  $\square$

**Satz 2.4.5** (Tarskis Satz über die Wahrheitsdefinition). *Wenn ZFC widerspruchsfrei ist, so gibt es keine Formel  $W(v_0)$ , so dass für alle  $L_{Me}$ -Sätze  $\varphi$  gilt*

$$\text{ZFC} \cup \{\text{Definitionen}\} \vdash \varphi \leftrightarrow W(\ulcorner \varphi \urcorner).$$

*Beweis:* Zu  $\Sigma(v_0) = \neg W(v_0)$  existiert nach dem Fixpunktsatz 2.4.4 ein Fixpunkt  $\varphi$ . Dann gilt  $\text{ZFC} \vdash \varphi \leftrightarrow W(\ulcorner \varphi \urcorner)$  und  $\text{ZFC} \vdash \varphi \leftrightarrow \neg W(\ulcorner \varphi \urcorner)$ . Widerspruch.  $\square$

**Definition 2.4.6** (Beweisbarkeitsprädikat).

- 1) Wir zählen alle Beweise in ZFC auf, indem wir folgende Gödelisierung

$$\ulcorner \langle \alpha_0, \dots, \alpha_k \rangle \urcorner = \prod_{0 \leq i \leq k} \frac{p_i^{\ulcorner \alpha_i \urcorner + 1}}{p_i}$$

verwenden. Hierbei ist wieder  $p_i$  die  $i$ -te Primzahl.

- 2)  $\varphi$  ist die Aussage, zu der es einen Beweis  $B = (\alpha_0 \dots, \alpha_m = \varphi)$  aus ZFC im Hilbertkalkül gibt, so dass der Beweis die Nummer  $\ulcorner B \urcorner = n$  hat. Sei  $\text{Bew}(\ulcorner \varphi \urcorner, \underline{n})$  diese Formel. Hier stecken zig Schritte Arbeit, die Formel in  $L_{Me}$  zu schreiben. Wir führen dies nicht aus. Das Studium des Kapitels 3 hilft, diese Schritte zu organisieren. Eine wesentliche Voraussetzung zur Beschreibung der Regel B6 ist, dass

$$\{\ulcorner \varphi \urcorner : \varphi \text{ ZFC-Axiom}\}$$

eine in  $L_{Me}$  beschreibbare Teilmenge von  $\omega$  ist.

$$\varphi = \varphi_n \Rightarrow \text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner, \underline{n}) \quad (2.4.1)$$

$$\varphi \neq \varphi_n \Rightarrow \text{ZFC} \vdash \neg \text{Bew}(\ulcorner \varphi \urcorner, \underline{n}). \quad (2.4.2)$$

- 3)  $\text{Bew}(x) = (\exists n \in \omega) \text{Bew}(x, n)$  ist die Formel „ $x$  ist aus/in ZFC beweisbar“.

Den folgenden Satz können wir im Rahmen der Vorlesung nicht beweisen. Der Beweis wäre zu lang. Ein kleinerer verwandter Satz wird für die Peano-Arithmetik in Satz 4.6.6 bewiesen.

**Satz 2.4.7.** *Das Beweisbarkeitsprädikat 2.4.6 aus dem Hilbertkalkül erfüllt die Löb-Axiome<sup>15</sup>, das heißt für alle  $\varphi$  und  $\psi$  gilt*

$$L1: \text{ZFC} \vdash \varphi \Rightarrow \text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner).$$

$$L2: \text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner) \wedge \text{Bew}(\ulcorner \varphi \rightarrow \psi \urcorner) \rightarrow \text{Bew}(\ulcorner \psi \urcorner).$$

$$L3: \text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner) \rightarrow \text{Bew}(\ulcorner (\text{Bew} \ulcorner \varphi \urcorner) \urcorner).$$

**Folgerung 2.4.8.**

$$1) \text{ZFC} \vdash \varphi \rightarrow \psi \Rightarrow \text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner) \rightarrow \text{Bew}(\ulcorner \psi \urcorner).$$

$$2) \text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \wedge \psi \urcorner) \leftrightarrow (\text{Bew}(\ulcorner \varphi \urcorner) \wedge \text{Bew}(\ulcorner \psi \urcorner)).$$

*Beweis:*

1) L1 angewendet auf  $(\varphi \rightarrow \psi)$  ergibt

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \rightarrow \psi \urcorner).$$

Nun erhalten wir aus L2 (und etwas Boole'scher Rechnung)

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \rightarrow \psi \urcorner) \rightarrow (\text{Bew}(\ulcorner \psi \urcorner) \vee \neg \text{Bew}(\ulcorner \varphi \urcorner)).$$

Nun übersetzen wir "oder nicht" in eine Implikation und erhalten

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \rightarrow \psi \urcorner) \rightarrow (\text{Bew}(\ulcorner \varphi \urcorner) \rightarrow \text{Bew}(\ulcorner \psi \urcorner))$$

2) „ $\rightarrow$ “ Aus den Tautologien  $\varphi \wedge \psi \rightarrow \varphi$  und selbes für  $\psi$  erhalten wir nach L1

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \wedge \psi \urcorner) \rightarrow \text{Bew}(\ulcorner \varphi \urcorner)$$

und selbes für  $\psi$ , Nach der Tautologieregel folgt:

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \wedge \psi \urcorner) \rightarrow \text{Bew}(\ulcorner \varphi \urcorner) \wedge \text{Bew}(\ulcorner \psi \urcorner).$$

„ $\leftarrow$ “ Wir beginnen mit der Tautologie  $\varphi \rightarrow (\psi \rightarrow (\varphi \wedge \psi))$ . L1 liefert

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner) \rightarrow \text{Bew}(\ulcorner \psi \rightarrow \varphi \wedge \psi \urcorner). \quad (2.4.3)$$

Nun wenden wir L2 an

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \psi \urcorner) \wedge \text{Bew}(\ulcorner \psi \rightarrow (\varphi \wedge \psi) \urcorner) \rightarrow \text{Bew}(\ulcorner \varphi \wedge \psi \urcorner). \quad (2.4.4)$$

Nun setzen wir (2.4.3) und (2.4.4) mit dem modus ponens zusammen und erhalten

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner) \wedge \text{Bew}(\ulcorner \psi \urcorner) \rightarrow \text{Bew}(\ulcorner \varphi \wedge \psi \urcorner).$$

<sup>15</sup>Martin Hugo Löb, 1921 – 2006



□

**Definition 2.4.9** ( $\text{Con}_{\text{ZFC}}$ ). Sei  $F$  eine immer falsche Formel wie zum Beispiel  $\neg 0 = 0$  (also eine Formel, deren Negat allgemeingültig ist).

$$\text{Con}_{\text{ZFC}} := \neg \text{Bew}(\ulcorner F \urcorner)$$

drückt die Konsistenz von ZFC aus.

**Satz 2.4.10** (Der zweite Gödel'sche Unvollständigkeitssatz für ZFC). *Wenn ZFC konsistent ist, dann gilt  $\text{ZFC} \not\vdash \text{Con}_{\text{ZFC}}$ .*

(Natürlich gilt auch die umgekehrte Implikation. Aus einer widerspruchsvollen Theorie kann man alles beweisen.)

*Beweis:* Wir beginnen mit irgendeiner Formel  $\varphi$ , so dass

$$\text{ZFC} \vdash \varphi \leftrightarrow \neg \text{Bew}(\ulcorner \varphi \urcorner). \quad (2.4.5)$$

gilt. Nun zeigen wir, dass  $\text{ZFC} \vdash \text{Con}_{\text{ZFC}} \rightarrow \varphi$ . Wir wenden 1) auf (2.4.5) an und erhalten

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner) \rightarrow \text{Bew}(\ulcorner \neg \text{Bew}(\ulcorner \varphi \urcorner) \urcorner). \quad (2.4.6)$$

Aus (2.4.6) und L3 folgt,

$$\text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner) \rightarrow (\text{Bew}(\ulcorner \text{Bew}(\ulcorner \varphi \urcorner) \urcorner) \wedge \text{Bew}(\ulcorner \neg \text{Bew}(\ulcorner \varphi \urcorner) \urcorner)).$$

und weiter mit Folgerung 2.4.8(2)

$$\text{ZFC} \vdash (\text{Bew}(\ulcorner \text{Bew}(\ulcorner \varphi \urcorner) \urcorner) \wedge \neg \text{Bew}(\ulcorner \varphi \urcorner)) \leftrightarrow \text{Bew}(\ulcorner \text{Bew}(\ulcorner \varphi \urcorner) \urcorner) \wedge \text{Bew}(\ulcorner \neg \text{Bew}(\ulcorner \varphi \urcorner) \urcorner)$$

und

$$\text{ZFC} \vdash (\text{Bew}(\ulcorner \text{Bew}(\ulcorner \varphi \urcorner) \urcorner) \wedge \neg \text{Bew}(\ulcorner \varphi \urcorner)) \leftrightarrow \text{Bew}(\ulcorner F \urcorner).$$

Somit erhalten wir

$$\begin{aligned} \text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner) &\rightarrow \neg \text{Con}_{\text{ZFC}}, \\ \text{ZFC} \vdash \text{Con}_{\text{ZFC}} &\rightarrow \neg \text{Bew}(\ulcorner \varphi \urcorner), \\ \text{ZFC} \vdash \text{Con}_{\text{ZFC}} &\rightarrow \varphi. \end{aligned} \quad (2.4.7)$$

Also

$$\text{ZFC} \vdash \text{Con}_{\text{ZFC}} \Rightarrow \text{ZFC} \vdash \varphi \stackrel{\text{L1}}{\Rightarrow} \text{ZFC} \vdash \text{Bew}(\ulcorner \varphi \urcorner).$$

Mit Eq. (2.4.7) folgt, dass ZFC widerspruchsvoll ist. Also gilt

$$\text{ZFC} \not\vdash \text{Con}_{\text{ZFC}}$$

□

**Frage 2.4.11.** Gilt

$$\text{ZFC} \not\vdash \neg \text{Con}_{\text{ZFC}}?$$

Dies würde gelten, wenn wir wüssten, dass alle Aussagen  $\varphi$  mit  $\text{ZFC} \vdash \varphi$  auch wahr sind. Dann wäre  $\text{Con}_{\text{ZFC}}$  eine von ZFC unabhängige Aussage.

## 2.5 Rosser-Sätze

**Definition 2.5.1.**  $\mathcal{R}$  sei ein Satz, der die folgende Fixpunktgleichung erfüllt.  $\mathcal{R}$  heißt Rosser-Satz<sup>16</sup>, falls

$$\text{ZFC} \vdash \mathcal{R} \leftrightarrow \forall y \in \omega (\text{Bew}(\ulcorner \mathcal{R} \urcorner, y) \rightarrow \exists z < y \text{Bew}(\ulcorner \neg \mathcal{R} \urcorner, z))$$

$\mathcal{R}$  gibt es wieder nach dem Fixpunktsatz 2.4.4

**Satz 2.5.2** (Der erste Gödel'sche Unvollständigkeitssatz für ZFC). *Wenn ZFC konsistent ist, dann gilt*

$$\text{ZFC} \not\vdash \mathcal{R} \quad \text{und} \quad \text{ZFC} \not\vdash \neg \mathcal{R}.$$

*Beweis:* Sei  $\varphi$  gegeben

$$\varphi^* = \forall y \text{Bew}(\ulcorner \varphi \urcorner, y) \rightarrow \exists z < y \text{Bew}(\ulcorner \neg \varphi \urcorner, z)$$

Wir zeigen

$$\text{ZFC} \vdash \varphi \Rightarrow \text{ZFC} \vdash \neg \varphi^*. \quad (2.5.1)$$

Wir nehmen den kleinsten Zeugen  $n$ , so dass  $\varphi$  aus ZFC mit Beweis Nummer  $n$  bewiesen wird. ZFC beweist sogar, dass es einen kleinsten Zeugen gibt, und daher  $\text{ZFC} \vdash \neg \mathcal{R}$ .

Wir zeigen

$$\text{ZFC} \vdash \neg \varphi \Rightarrow \text{ZFC} \vdash \varphi^* \quad (2.5.2)$$

Wir nehmen den kleinsten Zeugen  $n$ , so dass  $\varphi$  aus ZFC mit Beweis Nummer  $n$  bewiesen wird. Da nach Annahmen ZFC widerspruchsfrei ist, gibt es keinen Beweis für  $\neg \varphi$ . Außerdem kann ZFC die endlich vielen Beweise mit Nummer  $m < n$  alle durchführen und finden, dass keiner davon  $\text{Bew}(\varphi, m)$  erfüllt. Sei nun  $m > n$ . Ob  $\text{Bew}(\varphi, m)$  spielt für den Rosser-Satz keine Rolle, denn  $\text{Bew}(\neg \varphi, n)$ . (Dies ist gut, denn ZFC kann womöglich nicht beweisen, ob es nicht doch einen größeren Beweis auch für  $\varphi$  gibt.) Insgesamt erhalten wir  $\text{ZFC} \vdash \varphi^*$ . Aus (2.5.1) und (2.5.2) erhalten wir für  $\varphi = \varphi^* = \mathcal{R}$ ,  $\text{ZFC} \not\vdash \mathcal{R}$  und  $\text{ZFC} \not\vdash \neg \mathcal{R}$ .  $\square$

---

<sup>16</sup>John Barkley Rosser Sr., 1907 – 1989

## Kapitel 3

# Rekursionstheorie

Wir betrachten die Menge  $F = \{f : (\exists n \in \mathbb{N} \setminus \{0\})(f: \mathbb{N}^n \rightarrow \mathbb{N})\}$ . Welche Elemente von  $F$  sind mit einem Algorithmus berechenbar? D.h., es soll ein endliches Programm geben, das auf Eingabe jedes Arguments  $(x_1, \dots, x_n) \in \mathbb{N}^n$  nach endlich vielen Arbeitsschritten  $f(x_1, \dots, x_n)$  ausgibt und stoppt.

Wir präzisieren den Begriff der Berechenbarkeit in diesem Kapitel auf zwei äquivalente Weisen:

- Durch einen induktiven zahlentheoretischen Aufbau,  $\mu$ -Rekursivität genannt.
- Durch Registerprogramme und die Registermaschinen-Berechenbarkeit.

Man könnte statt Registermaschinen alternativ auch Turingmaschinen oder jede gängige Programmiersprache in ihrer Idealisierung auf unbegrenzten Speicherplatz und unbegrenzte Rechenschrittzahl verwenden.

Der Zusammenhang zwischen Berechenbarkeit und Beweisbarkeit ist in der Logik interessant. Im vierten Kapitel beantworten wir folgende Fragen.

### Fragen.

- Ist die charakteristische Funktion von

$$\{(\ulcorner \varphi \urcorner, n) : (\text{ZFC} \vdash_{L_{Me}} \varphi) \text{ mit Beweis Nummer } n\}$$

berechenbar?

- Ist die charakteristische Funktion von  $\{\ulcorner \varphi \urcorner : \text{ZFC} \vdash_{L_{Me}} \varphi\}$  berechenbar?
- Ist die charakteristische Funktion  $\{\ulcorner \varphi \urcorner : \emptyset \vdash_L \varphi\}$  berechenbar? Hier spielt die Reichhaltigkeit von  $L$  eine Rolle.

Beachten Sie, dass ZFC (also  $\{\ulcorner \varphi \urcorner : \varphi \in \text{ZFC}\}$ ) berechenbar ist. Die ersten beiden Fragen werden im vierten Kapitel auch für einen berechenbaren Teil der Zahlentheorie, Peano-Arithmetik genannt, beantwortet.

### 3.1 $\mu$ -rekursive Funktionen und Registermaschinen

In diesem Abschnitt führen wir zwei Berechenbarkeitsbegriffe ein und zeigen, dass jede  $\mu$ -rekursive Funktion registermaschinen-berechenbar ist.

**Definition 3.1.1.** Die Menge der ( $\mu$ -)rekursiven Funktionen in  $F$  enthält die in Regel R0 genannten Funktionen und ist die kleinste Teilmenge von  $F$ , die R1, R2 und R3 erfüllt.

(R0): (Die Grundfunktionen)  $S(x) = x + 1$ ,  $I_i^n(x_1, \dots, x_n) = x_i$ ,  $C_0^0 = 0$

(R1): (Die Komposition) Sei für  $0 < i < k$  die Funktion  $g_i$  ist eine  $n$ -stellige  $\mu$ -rekursive Funktion und  $h$  eine  $k$ -stellige  $\mu$ -rekursive Funktion. Dann ist auch die Funktion

$$f(x_1, \dots, x_n) = h(g_0(x_0, \dots, x_{n-1}), \dots, g_{k-1}(\bar{x}))$$

$\mu$ -rekursiv.

(R2): (Die primitive Rekursion) Es seien  $\mu$ -rekursive Funktionen  $g$  und  $h$  gegeben. Dann ist auch die durch folgende Regeln gegebene Funktion  $f$   $\mu$ -rekursiv.

$$f(\bar{x}, 0) = g(\bar{x}) \qquad f(\bar{x}, y + 1) = h(\bar{x}, y, f(\bar{x}, y))$$

(R3): (Die  $\mu$ -Operation) Sei  $g$  eine  $\mu$ -rekursive Funktion, die folgendes erfüllt:

$$\forall \bar{x} \exists y g(\bar{x}, y) = 0$$

Dann ist auch die folgende Funktion  $\mu$ -rekursiv

$$f(\bar{x}) = \mu y (g(\bar{x}, y) = 0) = \min\{y : g(\bar{x}, y) = 0\}.$$

Man sagt:  $f$  entsteht aus  $g$  durch die Anwendung des  $\mu$ -Operators auf  $y$ .

**Definition 3.1.2** (primitiv rekursiv). Verwendet man bei einer Herleitung von  $f \in F$  als  $\mu$ -rekursive Funktion nur die Schritte des Typs R0, R1 und R2, so heißt  $f$  primitiv rekursiv.

Wir stellen nun einen alternativen Berechenbarkeitsbegriff vor. Wir werden zeigen, dass die beiden Begriffe äquivalent sind, und nennen „ $\mu$ -rekursiv“, „registermaschinen-berechenbar“ dann oft nur noch „berechenbar“ oder „rekursiv“. Der bekannte Begriff der Turing-Berechenbarkeit<sup>1</sup> ist ebenfalls zu den genannten äquivalent.

Nach der Church'schen These<sup>2</sup> sind alle Berechenbarkeitsbegriffe äquivalent.

**Definition 3.1.3.** Ein Alphabet  $\mathcal{A}$  ist eine endliche nicht leere Menge von Zeichen.

$$w = a_0 \dots a_{n-1}$$

heißt Wort über  $\mathcal{A}$ , wenn  $n \in \mathbb{N}$  und  $a_i \in \mathcal{A}$ . Für  $n = 0$  schreiben wir  $w = \square$ . Wir bezeichnen mit  $\mathcal{A}^*$  die Menge der Wörter über  $\mathcal{A}$ .

<sup>1</sup>Alan Mathison Turing, 1912 – 1954

<sup>2</sup>Alonzo Church, 1903 – 1995

Im Falle  $\mathcal{A} = \{\}$  können wir das Wort aus  $n$  Strichen mit der Zahl  $n$  identifizieren. Unsere Berechnungen mit Wörtern schließen also die Rechnungen mit natürlichen Zahlen ein.

**Definition 3.1.4.** Ein Tripel

$$\mathcal{M} = ((b_0, \dots, b_N), R, \mathcal{A})$$

heißt Registermaschine, falls folgendes gilt:

- 1)  $\mathcal{A} = \{a_1, \dots, a_L\} \neq \emptyset$  ist ein endliches Alphabet.
- 2)  $R \in \mathbb{N}$  ist die Anzahl der Register, diese heißen  $\mathcal{R}_0, \dots, \mathcal{R}_{R-1}$ . In jedem Register steht zu jedem Arbeitsstadium ein Wort aus  $\mathcal{A}^*$ .
- 3)  $(b_0, \dots, b_N)$  sind die Befehle. Es gibt nun drei Sorten von Befehlen:
  - a)  $b = \text{Push}(r, l)$  für  $r \in R$  und  $l \in \{0, \dots, L\}$  streicht für  $l = 0$  den letzten Buchstaben vom Register  $R_r$  weg, falls  $R_r \neq \square$  (wenn dieses der Fall ist, dann bleibt  $R_r$  unverändert) und fügt für  $l = 1, \dots, L$  den  $l$ -ten Buchstaben des Alphabets in das  $r$ -te Register an der rechten Seite zum dort stehenden Wort hinzu und geht zum nächsten Befehl. Falls  $b = b_n$ , so geht die Maschine also zu  $b_{n+1}$ . Wir schreiben für  $\text{Push}(r, 0)$  in unseren Flussdiagrammen einen Kasten mit Beschriftung  $\mathcal{R}_r \dot{-} 1$ .
  - b)  $b = \text{goto}(r, c_0, \dots, c_L)$  für  $r \in R$  und  $c_i \in \{1, \dots, N\}$ . Falls  $R_r$  leer ist, geht die Maschine als nächstes zu Befehl Nummer  $c_0$ , also zu  $b_{c_0}$ , falls  $i \in L$  und der letzte Buchstabe  $\text{last}(R_r)$  in  $R_r$  der Buchstabe  $a_i$  ist, folgt als nächster Befehl  $b_{c_i}$ .
  - c) Stop. Die Maschine stoppt.

Die Maschine kann also schreiben und lesen und in Abhängigkeit des Gelesenen zu bestimmten Befehlsnummern weiterspringen.

**Definition 3.1.5.** Sei  $\mathcal{M}$  eine Registermaschine. Eine  $\mathcal{M}$ -Berechnung startet mit Registerinhalten  $(\mathcal{R}_i : i < R) \in (\mathcal{A}^*)^R$  und mit Befehl  $b_0$ . Die Maschine arbeitet entweder endlich viele Schritte, bis sie in zu einem Befehl  $b_c = \text{Stop}$  gelangt. Man sagt zu  $c \in \{0, \dots, N\}$  auch Zustand und zu  $c$  mit  $b_c = \text{Stop}$  auch Stoppzustand. Jeder  $R$ -Registermaschine können wir für jedes  $n \in \mathbb{N}$  eine partielle Funktion  $F_{\mathcal{M}}^n$  zuordnen. Hierbei wird  $F_{\mathcal{M}}^n(x_1, \dots, x_n)$  durch die Maschine  $\mathcal{M}$  wie folgt berechnet: Zu Anfang ist die Zeit  $t = 0$ , der Startbefehl ist  $b_0$ , in  $\mathcal{R}_0$  steht das leere Wort und  $\mathcal{R}_r = x_r$  für  $1 \leq r \leq n$ . Man schreibt dieses auch als Konfiguration hin

$$\mathcal{K}_0 := \mathcal{K}_{\mathcal{M},0} = (0, \square, \mathcal{R}_1, \dots, \mathcal{R}_{n-1}, \underbrace{\square, \dots, \square}_{\text{von Stelle } n \text{ bis } R-1}). \quad (3.1.1)$$

Jedes Berechnungsstadium wird in einer Konfiguration

$$\mathcal{K}_s = (c_s, (\mathcal{R}_{r,s})_{0 \leq r < R})$$

niedergeschrieben. Man startet also wie in (3.1.1) mit  $s = 0$ ,  $c_0 = 0$ ,  $\mathcal{R}_{r,0} = \mathcal{R}_r$ ,  $1 \leq r \leq n$ ,  $t = 0$ ,  $c_0 = 0$ ,  $\mathcal{R}_r$  leer für  $r \in R \setminus \{1, \dots, n\}$ . Der Buchstabe  $s$  steht für stage. Wenn  $\mathcal{M}$  in einem einzelnen Befehlsschritt von einer Konfiguration zur nächsten führt, also

$$\mathcal{K} = (c_s, \mathcal{R}_{0,s}, \dots, \mathcal{R}_{R-1,s}) \xrightarrow{\mathcal{M}} (c_{s+1}, \mathcal{R}_{0,s+1}, \dots, \mathcal{R}_{R-1,s+1}) =: \mathcal{M}(\mathcal{K}),$$

dann sagt man auch, dass die rechts stehende Konfiguration  $\mathcal{M}(\mathcal{K})$  die Nachfolgerkonfiguration der linken Konfiguration  $\mathcal{K}$  ist. Die Konfigurationsfolge ist entweder unendlich lang und dann ist  $F_{\mathcal{M}}^n(\mathcal{R}_1, \dots, \mathcal{R}_n)$  nicht definiert, oder die Folge bricht mit dem Stoppbefehl ab. Falls  $\mathcal{K}$  eine Stoppkonfiguration ist, können wir  $\mathcal{M}(\mathcal{K}) = \mathcal{K}$  definieren. Wir setzen

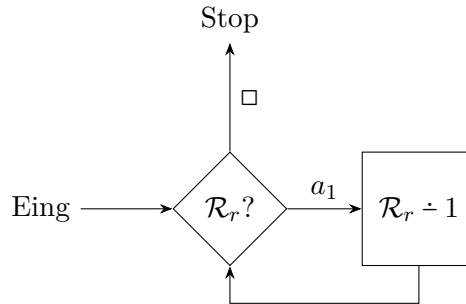
$$F_{\mathcal{M}}^n(x_1, \dots, x_n) = \mathcal{R}_{0,s} \text{ für die Stoppzeit } s.$$

**Definition 3.1.6.** Eine Funktion  $f: (\mathcal{A}^*)^n \rightarrow \mathcal{A}^*$  heißt registermaschinen-berechenbar wenn es eine Registermaschine  $\mathcal{M}$  gibt, so dass  $f = F_{\mathcal{M}}^n$  ist. Beachte: Wir fordern hier, dass  $f$  auf ganz  $(\mathcal{A}^*)^n$  definiert ist. Die Maschine  $\mathcal{M}$ , angesetzt auf einen wie oben normierten  $n$ -stelligen Input, muss also nach endlich vielen Schritten stoppen.

**Definition 3.1.7.** Wir schreiben  $\mathcal{K} \xrightarrow{\mathcal{M}} \mathcal{K}'$ , wenn  $\mathcal{M}$  in endlich vielen Schritten  $\mathcal{K}$  in  $\mathcal{K}'$  überführt und  $\mathcal{K}'$  ein Stoppzustand ist. Oft schreiben wir statt  $\mathcal{K}$  nur die Registerinhalte.

*Beispiel 3.1.8* (Die Löschmaschine  $\mathcal{L}^r$  über  $\mathcal{A} = \{a_1\}$ ).

$$(\mathcal{R}_0, \dots, \mathcal{R}_{R-1}) \rightarrow (\mathcal{R}_0, \dots, \mathcal{R}_{r-1}, \square, \mathcal{R}_{r+1}, \dots, \mathcal{R}_{R-1})$$



$$\mathcal{L}^r = (\underbrace{\text{goto}(r, 3, 1)}_{b_0}, \underbrace{\text{Push}(r, 0)}_{b_1}, \underbrace{\text{goto}(0, 0, 0)}_{b_2}, \underbrace{\text{Stop}}_{b_3})$$

Statt  $\text{goto}(0, 0, 0)$  könnte man auch  $\text{goto}(r, 3, 1)$  als Befehl  $b_2$  nehmen. Jeder dieser zwei Befehle beschreibt die mittlere Raute. Es gibt also mehr als ein Programm, das dieselbe Löschwirkung hat.

Nun identifizieren wir  $x \in \mathbb{N}$  mit  $(a_1, \dots, a_1)$  der Länge  $x$  und erhalten somit eine Bijektion von  $\mathbb{N}$  und  $\mathcal{A}^*$  für  $\mathcal{A} = \{a_1\}$ .

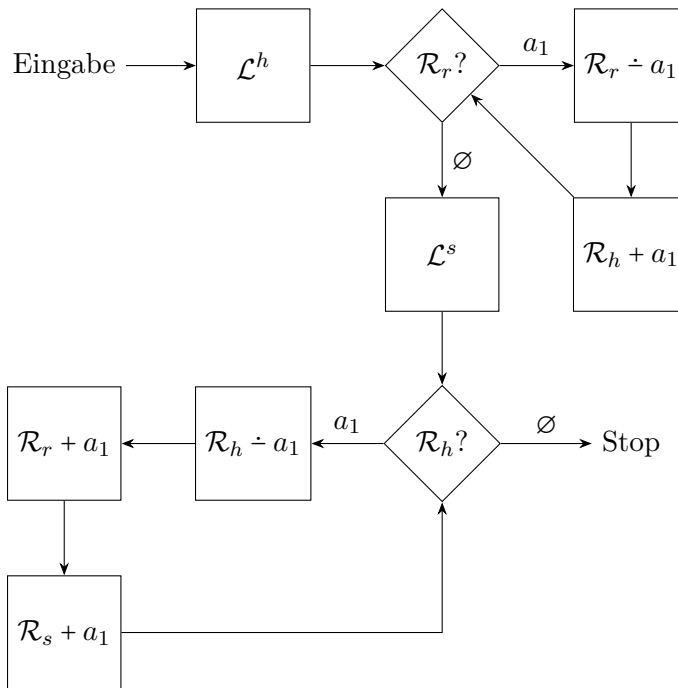
**Satz 3.1.9.** Die  $\mu$ -rekursiven Funktionen stimmen überein mit den registermaschinen-berechenbaren Funktionen über dem einelementigen Alphabet  $\mathcal{A} = \{a_1\}$ .

Nun zeigen wir Schritt für Schritt, dass jede  $\mu$ -rekursive Funktionen registerberechenbar sind. Die umgekehrte Inklusion zeigen wir im kommenden Abschnitt.

*Beweis:* Die Kopiermaschine  $\mathcal{K}_h^{r,s}$

$$(\mathcal{R}_0, \dots, \mathcal{R}_r, \dots, \mathcal{R}_{s-1}, \mathcal{R}_s, \mathcal{R}_{s+1}, \dots, \mathcal{R}_n) \xrightarrow{\mathcal{K}_h^{r,s}} (\mathcal{R}_0, \dots, \mathcal{R}_r, \dots, \mathcal{R}_{s-1}, \mathcal{R}_r, \mathcal{R}_{s+1}, \dots, \mathcal{R}_n)$$

Kopiert  $\mathcal{R}_r$  auf  $\mathcal{R}_s$  mit dem Hilfsregister  $\mathcal{R}_h$   $h \notin \{r, s\}$



Die dazugehörige Formel lautet für das Alphabet  $\{\}$

$$\mathcal{K}_h^{r,s} = ( \text{goto}(h, 3, 1), \quad \text{Push}(h, 0), \quad \text{goto}(0, 0, 0), \quad \text{goto}(r, 7, 4), \\ \text{Push}(r, 0), \quad \text{Push}(h, 1), \quad \text{goto}(0, 3, 3), \quad \text{goto}(5, 10, 8), \\ \text{Push}(5, 0), \quad \text{goto}(0, 7, 7), \quad \text{goto}(h, 15, 11), \quad \text{Push}(h, 0), \\ \text{Push}(r, 1), \quad \text{Push}(5, 1), \quad \text{goto}(0, 10, 10), \quad \text{Stop} \quad )$$

□

**Definition 3.1.10.** Das Hintereinanderausführen der Maschinen  $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3$  (in dieser Reihenfolge) wird als

$$\mathcal{M} = \mathcal{M}_1 \circ \mathcal{M}_2 \circ \mathcal{M}_3$$

notiert. Bei dieser Operation verwandeln sich die Stoppzustände von  $\mathcal{M}_1$  und von  $\mathcal{M}_2$  jeweils in den Anfangszustand von  $\mathcal{M}_2$  beziehungsweise  $\mathcal{M}_3$ .

*Beispiel 3.1.11.* Seien  $r_1, \dots, r_n, s_1, \dots, s_n, h$  paarweise verschiedene Zahlen aus  $\{0, \dots, R-1\}$ . Wir können zum Beispiel die Register  $(r_1, \dots, r_n)$  in die Register  $(s_1, \dots, s_n)$  kopieren mit der folgenden  $R$ -Register-Maschine

$$\mathcal{K}_h^{r_1 \dots r_n; s_1 \dots s_n} = \mathcal{K}_h^{r_1, s_1} \circ \dots \circ \mathcal{K}_h^{r_n, s_n}.$$

Um eine andere Maschine nach einer Maschine  $\mathcal{M}$  richtig zu starten, muss man nach dem Stopp von  $\mathcal{M}$  die Hilfsregister  $\mathcal{R}_0, \mathcal{R}_{n+1}, \dots, \mathcal{R}_{R-1}$  löschen. Wir führen einen Namen ein.

**Definition 3.1.12** (Standardform). Wenn  $\mathcal{M}$  eine  $n$ -stellige Funktion mit  $R$  Registern ist, dann ist

$$\mathcal{M}^* = \mathcal{M}^{*,n,R} = \mathcal{L}^0 \circ \mathcal{L}^{n+1} \circ \dots \circ \mathcal{L}^{R-1} \circ \mathcal{M}$$

die Standardform von  $\mathcal{M}$ .

**Satz 3.1.13.** Die Grundfunktionen sind registermaschinen-berechenbar.

*Beweis:* Die Nachfolgerfunktion  $S$  wird berechnet durch  $\mathcal{K}_2^{1,0} \circ (R_0 + 1)$ .

Die Projektion  $I_i^n$  wird berechnet durch  $\mathcal{K}_{n+1}^{i,0}$ .

Die Nullfunktion  $C_0^0$  wird berechnet durch (Stop). □

**Satz 3.1.14.** Die Menge der registermaschinenberechenbaren Funktionen ist gegen die Hintereinanderausführung abgeschlossen.

*Beweis:* Wir führen die Programmierung am Beispiel zweier einstelliger Funktionen  $f_1, f_2$  und einer zweistelligen Funktion  $g$  durch.  $\mathcal{H}$  berechnet  $h(y_1, y_2)$ ,

$\mathcal{F}_1$  berechnet  $f_1(x)$ ,

$\mathcal{F}_2$  berechnet  $f_2(x)$ .

Wir nehmen an, das  $\mathcal{H}, \mathcal{F}_i$  nur die Register bis  $R-1$  brauchen. Dann wird  $h(f_1(x), f_2(x))$  durch die Hintereinanderausführung folgender Kombinationen berechnet:

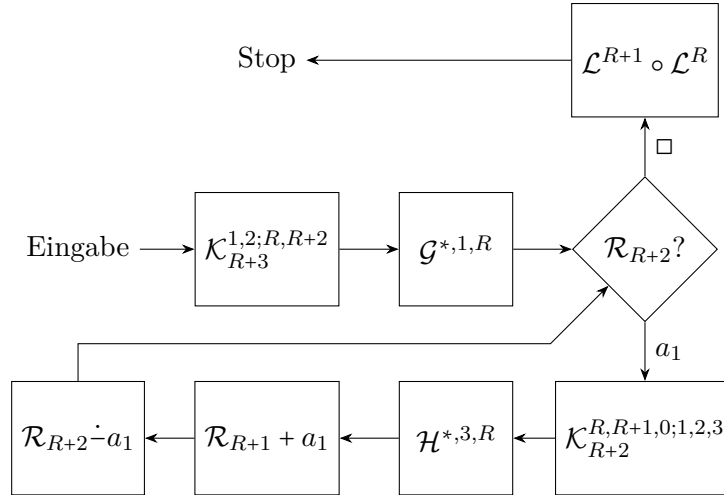
$$\mathcal{K}_{R+2}^{1,R} \circ \mathcal{F}_1^{*,1,R} \circ \mathcal{K}_{R+2}^{0,R+1} \circ \mathcal{K}_{R+2}^{R,1} \circ \mathcal{F}_2^{*,1,R} \circ \mathcal{K}_{R+2}^{0,2} \circ \mathcal{K}_{R+2}^{R+1,1} \circ \mathcal{H}^*.$$

Dieses ist eine  $R+3$ -Registermaschine. Die neuen Register  $\mathcal{R}_R$  und  $\mathcal{R}_{R+1}$  werden benutzt, um Argumente und Zwischenergebnisse an geschützte Plätze zu kopieren.  $\mathcal{R}_{R+2}$  ist das Hilfsregister für die Kopiermaschinen. □

**Satz 3.1.15.** Die registerberechenbaren Funktionen sind abgeschlossen unter  $R2$ .



*Beweis:* Es sei  $\mathcal{A} = \{a_1\}$ . Es seien  $g(x)$  durch  $\mathcal{G}$  berechnet und  $h(x, y, z)$  durch  $\mathcal{H}$  berechnet. Diese benutzen Register  $\mathcal{R}_0, \dots, \mathcal{R}_{R-1}$ . Wir geben nur das Flussdiagramm einer  $(R + 3)$ -Registermaschine zur Berechnung von  $f(x, 0) = g(x)$ ,  $f(x, y + 1) = h(x, y, f(x, y))$  an.



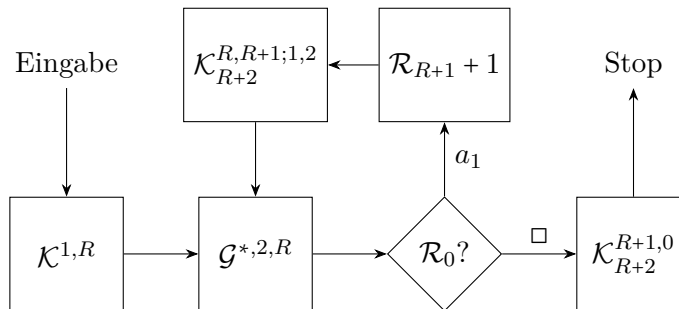
Das Diagramm zeigt eine  $R + 4$ -Registermaschine. Die neuen Register  $\mathcal{R}_R, \mathcal{R}_{R+1}, \mathcal{R}_{R+2}$  werden benutzt, um Argumente und Zwischenergebnisse an geschützte Plätze zu kopieren. Als Hilfsregister für die Kopiermaschinen nehmen wir  $\mathcal{R}_{R+3}$ . In  $\mathcal{R}_{R+2}$  steht  $y, y - 1, \dots, 1$  vor dem Umlauf Nummer  $0, 1, 2, \dots, y - 1$  der unteren Schleife. In  $\mathcal{R}_{R+1}$  steht  $0, \dots, y - 1$  vor dem Umlauf Nummer  $0, 1, 2, \dots, y - 1$ . Die Schleife wird genau  $y$  mal durchlaufen.  $\square$

Die Reihenfolge der Berechnung ist hier für  $y = 3$ :  $f(x, 0)$  im  $\mathcal{R}_0$

$$h(x, 0, f(x, 0)) = f(x, 1) \quad h(x, 1, f(x, 1)) = f(x, 2) \quad h(x, 2, f(x, 2)) = f(x, 3)$$

**Satz 3.1.16.** Die registermaschinen-berechenbaren Funktionen sind unter  $R3$  abgeschlossen.

*Beweis:* Wir schreiben wieder ein Flussdiagramm. Sei die 2-stellige Funktion  $g$  durch die  $R$ -Registermaschine  $\mathcal{G}$  berechnet und gelte  $\forall x \exists y g(x, y) = 0$ .



Das Diagramm zeigt eine  $R + 3$ -Registermaschine. Die neuen Register  $\mathcal{R}_R, \mathcal{R}_{R+1}$  werden benutzt, um Argumente und Zwischenergebnisse an geschützte Plätze zu kopieren. Als Hilfsregister für die Kopiermaschinen nehmen wir  $\mathcal{R}_{R+2}$ .  $\square$

Nun ist Teilbehauptung des Satzes 3.1.9 gezeigt, dass jede  $\mu$ -rekursive Funktion registermaschinenberechenbar ist. Für die umgekehrte Inklusion benutzen wir wieder Gödelisierungen.

## 3.2 Primitiv rekursive Funktionen und Prädikate

**Lemma 3.2.1.** *Für die folgenden Terme ist jeweils die Funktion  $\mapsto \text{term}(x)$  beziehungsweise  $(x, y) \mapsto \text{term}(x, y)$  primitiv rekursiv:*

$$x + y, \quad x \cdot y, \quad x^y, \quad x!, \quad x \dot{-} 1 \quad x \dot{-} y = \begin{cases} x - y, & \text{falls } x - y \geq 0, \\ 0, & \text{sonst} \end{cases}.$$

*Beweis:*

$$\begin{array}{ll} x + 0 = x, & x + (y + 1) = (x + y) + 1 \\ x \cdot 1 = x, & x \cdot (y + 1) = x \cdot y + x \\ x^1 = x & x^{(y+1)} = x^y \cdot x \\ x!, & (x + 1)! = x! \cdot (x + 1) \\ x \dot{-} 1 = \begin{cases} 0, & \text{falls } x = 0, \\ x - 1, & \text{sonst.} \end{cases} & x \dot{-} (y + 1) = (x \dot{-} y) \dot{-} 1 \end{array}$$

Für die Funktion  $f(x) = x \dot{-} 1$  nimmt man Rekursionsregel (R2) auf die Funktion  $f(0) = 0$ ,  $f(1) = 0$ ,  $f(x + 1) = S(f(x))$  für  $x \geq 2$ .  $\square$

**Definition 3.2.2** ((primitiv) rekursive Relation). Eine Relation  $R$  heißt (primitiv) rekursiv, wenn ihre charakteristische Funktion  $K_R$  (primitiv) rekursiv ist. Die charakteristische Funktion ist wie folgt definiert:

$$K_R(x_1, \dots, x_n) = \begin{cases} 0, & \text{wenn } R(x_1, \dots, x_n), \\ 1, & \text{sonst.} \end{cases}$$

*Beispiel 3.2.3.*  $K_R(x, y) = K_{\neq 0}((x + 1) \dot{-} y)$  ist  $x < y$ .

**Lemma 3.2.4.** *Seien  $P$  und  $Q$  primitiv rekursive  $\ell$ -stellige Relationen, sowie  $f_i$  primitiv rekursive  $n$ -stellige Funktion für  $i = 0, \dots, \ell - 1$ . Dann sind*

$$P \wedge Q, \quad P \vee Q, \quad \neg P, \quad P(f_0(\bar{x}), \dots, f_{\ell-1}(\bar{x}))$$

*primitiv rekursiv.*

*Beweis:*

$$\begin{aligned} K_{P \vee Q} &= K_P \cdot K_Q, \\ K_{\neg P} &= 1 \dot{-} K_P, \\ K_{P \wedge Q} &= 1 \dot{-} (1 \dot{-} K_P)(1 \dot{-} K_Q), \\ K_{P(\bar{f})} &= K_P(\bar{f}). \end{aligned}$$

□

**Lemma 3.2.5.** *Seien  $P_i$ ,  $0 \leq i \leq n-1$ , primitiv rekursive  $\ell$ -stellige Relationen, sowie  $f_i$  primitiv rekursive  $\ell$ -stellige Funktion für  $i = 0, \dots, n$ . Wir definieren folgende  $\ell$ -stellige Funktion*

$$f(\bar{x}) = \begin{cases} f_0(\bar{x}), & \text{falls } P_0(\bar{x}), \\ f_1(\bar{x}), & \text{falls } P_1(\bar{x}) \wedge \neg P_0(x), \\ \vdots & \vdots \\ f_{n-1}(\bar{x}), & \text{falls } P_{n-1} \wedge \neg P_{n-2}(x) \wedge \dots \wedge \neg P_0(x), \\ f_n(\bar{x}), & \text{falls } \neg P_{n-1}(x) \wedge \dots \wedge \neg P_0(x). \end{cases}$$

Dann ist  $f$  primitiv rekursiv.

*Beweis:* Wir finden folgende Darstellung für  $f$ :

$$\begin{aligned} Q_i &= P_i \wedge \neg P_{i-1} \wedge \dots \wedge \neg P_0 \text{ für } 0 \leq i < n, \\ Q_n &= \neg P_{n-1} \wedge \dots \wedge \neg P_0, \\ f(\bar{x}) &= \sum_{i=0}^n (1 - K_{Q_i}(\bar{x})) f_i(\bar{x}). \end{aligned}$$

□

**Lemma 3.2.6.** *Seien  $P$  eine primitiv rekursive  $\ell + 1$ -stellige Relation. Die Relationen  $R$  und  $S$  seien gegeben durch*

$$\begin{aligned} R(\bar{x}, z) &\Leftrightarrow \forall y < z \ P(\bar{x}, y), \\ S(\bar{x}, z) &\Leftrightarrow \exists y < z \ P(\bar{x}, y). \end{aligned}$$

Dann sind  $R$  und  $S$  primitiv rekursiv. Sei  $b$  eine primitiv rekursive Funktion. ( $b$  steht für bound Schranke.) Wenn gilt

$$(\forall \bar{x})(\exists y < b(\bar{x}))P(\bar{x}, y),$$

dann ist  $f(\bar{x}) = \mu y P(\bar{x}, y)$  primitiv rekursiv.

*Beweis:*

$$\begin{aligned} R(\bar{x}, 0) &= \text{wahr}, \\ R(\bar{x}, z + 1) &= R(\bar{x}, z) \wedge P(\bar{x}, z). \end{aligned}$$

Dann ist  $R$  also mit Regel R2 hergestellt.

$$S(\bar{x}, z) \leftrightarrow \neg \forall y < z \neg P(\bar{x}, y).$$

Auch die Funktion

$$h(\bar{x}, y) = \mu z (P(\bar{x}, z) \vee z = y)$$

können wir, da der Suchraum primitiv rekursiv beschränkt ist, mit R2 herstellen.

$$\begin{aligned} h(\bar{x}, y) &= 0, \\ h(\bar{x}, y + 1) &= \begin{cases} h(\bar{x}, y), & \text{falls } P(\bar{x}, h(\bar{x}, y)), \\ y + 1, & \text{sonst.} \end{cases} \end{aligned}$$

Die Funktion  $h$  ist primitiv rekursiv. Daher ist mit R1 die Funktion

$$f(\bar{x}) = h(\bar{x}, b(\bar{x}))$$

primitiv rekursiv. □

*Beispiele 3.2.7.*  $x|y$   $\exists z < y (x \cdot z = y \wedge z > 1)$ ,  
 $x$  ist Primzahl  $x \neq 1 \wedge \forall y, z \leq x (y \cdot z = x \rightarrow (y = 1 \vee z = 1))$ ,  
 $p(n)$  ist die  $n$ -te Primzahl  $p(x + 1) = \mu y < p(x)! + 2, (y \text{ prim}, y > p(x))$ .

Also sind die Vorschriften primitiv rekursiv.

**Definition 3.2.8** (Gödelnummer). Die Gödelnummer  $\langle \dots \rangle$  einer Folge  $(x_0, \dots, x_{n-1})$  ist

$$\langle x_0, \dots, x_{n-1} \rangle = p_0^{x_0} \cdot \dots \cdot p_{n-2}^{x_{n-2}} \cdot p_{n-1}^{x_{n-1}+1} - 1$$

Falls  $n = 0$ , so setzen wir  $\langle \square \rangle = 0$ .

**Definition 3.2.9.**

$$\begin{aligned} (x)_i &= \begin{cases} x_i, & \text{falls } x = \langle x_0, \dots, x_{n-1} \rangle \text{ und } i < n, \\ 0, & \text{sonst.} \end{cases} \\ \lg(x) &= \begin{cases} n, & \text{falls } x = \langle x_0, \dots, x_{n-1} \rangle, \\ 0, & \text{sonst.} \end{cases} \end{aligned}$$

**Lemma 3.2.10.**

- 1)  $\langle \cdot \rangle : \cup \{\mathbb{N}^n : n \in \mathbb{N}\} \rightarrow \mathbb{N}$  ist eine Bijektion und primitiv rekursiv.
- 2)  $\lg(x) \leq x$ , wenn  $x > 0$  ist, ist  $(x)_i < x$ .
- 3)  $x \mapsto \lg(x)$  ist primitiv rekursiv.
- 4)  $(x, i) \mapsto (x)_i$  ist primitiv rekursiv.

*Beweis:*

- 1) Sei  $(x_0, \dots, x_{n-1})$  gegeben. Dann sind die  $p(0), \dots, p(n-1)$  primitiv rekursiv berechenbar. Diese Berechnung ist primitiv rekursiv, da nach Lemma 3.2.1 Multiplikation, Exp. und  $\div 1$  primitiv rekursiv sind.
- 2)  $2^n \geq n + 1$ .
- 3)

$$\lg(x) = \mu y (y \leq x \wedge \forall z \in [y, x] p(z) \dagger x + 1).$$

4)

$$(x)_i = \begin{cases} \mu y p(i)^{y+1} \dagger x + 1, & \text{falls } i < \lg(x) - 1, \\ \mu y p(i)^{y+2} \dagger x + 1, & \text{falls } i = \lg(x) - 1, \\ 0, & \text{sonst.} \end{cases}$$

□

*Bemerkung 3.2.11.* Die Umkehrung einer bijektiven rekursiven Funktion ist rekursiv. „Bijektiv“ kann man nicht weglassen. Rekursive monotone Funktion haben immerhin noch eine rekursive Bildmenge und eine rekursive nur auf dieser Bildmenge definierte Umkehrfunktion. Die Umkehrung einer primitiv rekursiven Funktion ist rekursiv.

### 3.3 Gödelisierung von Registermaschinen

**Definition 3.3.1.** Wir ordnen folgende Gödelnummern zu. Sei  $\mathcal{A} = \{a_1, \dots, a_L\}$  ein Alphabet, und sei  $\mathcal{M} = (\mathcal{A}, R, (b_0, \dots, b_N))$  eine  $R$ -Registermaschine über  $\mathcal{A}$ , es sei  $W \in \mathcal{A}^*$ , und  $\mathcal{K}$  eine Konfiguration von  $\mathcal{M}$ . Für  $n \in \mathbb{N}$ ,  $l, i_0, \dots, i_{n-1} \in \{1, \dots, L\}$  und  $r \in \{0, \dots, R-1\}$  setzen wir

$$\begin{aligned} \ulcorner \text{Stop} \urcorner &= 0, & \ulcorner \text{Push}(r, l) \urcorner &= \langle r, l \rangle, \\ \ulcorner \text{goto}(r, c_0, \dots, c_L) \urcorner &= \langle r, c_0, \dots, c_L \rangle, & \ulcorner \mathcal{M} \urcorner &= \langle \ulcorner b_0 \urcorner, \dots, \ulcorner b_N \urcorner, R, L \rangle, \\ \ulcorner W \urcorner = \ulcorner a_{i_0} \dots a_{i_{n-1}} \urcorner &= \langle i_0, \dots, i_{n-1} \rangle, & \ulcorner \mathcal{K} \urcorner &= \langle c, \ulcorner \mathcal{R}_0 \urcorner, \dots, \ulcorner \mathcal{R}_{R-1} \urcorner \rangle. \end{aligned}$$

$R = (m)_{\lg(m)-2}$  ist die Anzahl der Register.

**Lemma 3.3.2.** *Wir führen folgende Funktionen ein.*

$$\text{Ers}(\langle x_0, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_{n-1} \rangle, i, y) := \begin{cases} \langle x_0, \dots, x_{i-1}, y, x_{i+1}, \dots, x_{n-1} \rangle, & \text{falls } i < n; \\ 0, & \text{sonst.} \end{cases}$$

$$\text{Anh}(\langle x_0, \dots, x_{n-1} \rangle, y) := \langle x_0, \dots, x_{n-1}, y \rangle$$

$$\text{Str}(\langle x_0, \dots, x_{n-1} \rangle) := \begin{cases} \langle x_0, \dots, x_{n-2} \rangle, & \text{falls } n > 0; \\ 0, & \text{sonst.} \end{cases}$$

Die drei Funktionen sind primitiv rekursiv.

*Beweis:* Wir setzen  $p(-1) = 1$  (für die obere Abschätzung der  $\mu$ -Operators in the Gleichung fuer Str).

$$\begin{aligned} \text{Ers}(x, i, y) &= \mu z < (x+1) p(i)^{y+1} \left( (\lg(z) = \lg(x)) \right. \\ &\quad \left. \wedge \forall j < \lg(x) (j \neq i \rightarrow (z)_j = (x)_j) \wedge (z)_i = y) \vee (i \geq \lg(x) \wedge z = 0) \right). \\ \text{Anh}(x, y) &= \mu z < (x+1) \cdot p(\lg(x))^{y+2} \left( \lg(z) = \lg(x) + 1 \right. \\ &\quad \left. \wedge \forall j < \lg(x) (z)_j = (x)_j \wedge (z)_{\lg(x)} = y \right). \\ \text{Str}(x) &= \mu z < (x+1) (p(\lg(x) - 1) - 1) \left( (\lg(z) = \lg(x) - 1 \right. \\ &\quad \left. \wedge \forall j < \lg(z) (z)_j = (x)_j) \vee (\lg(x) = 0 \wedge z = 0) \right). \end{aligned}$$

□

**Lemma 3.3.3.** *Es gibt primitiv rekursive  $N : \mathbb{N}^2 \rightarrow \mathbb{N}$ , so dass*

$$\forall \mathcal{K}, \mathcal{M} \quad N(\ulcorner \mathcal{M} \urcorner, \ulcorner \mathcal{K} \urcorner) = \begin{cases} \ulcorner \mathcal{M}(\mathcal{K}) \urcorner, & \text{falls } \mathcal{K} \text{ eine Konfiguration von } \mathcal{M}, \\ 0, & \text{sonst.} \end{cases}$$

*Beweis:* Zur Berechnung von  $N(m, k)$  setzen wir als Abkürzungen ein:  $c = (k)_0$  der aktive Befehlsindex,  $b = (m)_c$  der aktive Befehl,  $r = (b)_0$  das im aktiven Befehl angesprochene Register,  $w = (k)_{r+1}$  der aktuelle Inhalt dieses Registers,  $\ell = \lg(w) - 1$  die Länge des Inhalts des angebrochenen Registers minus 1, und  $a = (w)_\ell$  der letzte Buchstabe in diesem Register oder 0. Dann setzen wir  $N(m, k) = 0$ , falls  $k$  keine Gödelnummer einer Konfiguration von  $\mathcal{M}$  mit  $[\mathcal{M}] = m$  ist, also falls  $\lg(k) \neq R+1 = (m)_{\lg(m)-2} + 1$  oder  $c \geq \lg(m) - 2 = \lg(b_0, \dots, b_N) = N + 1$  (hier hat  $N$  nichts mit der Nachfolgerfunktion zu tun.) Falls  $k$  eine Konfiguration von  $m$  ist, so setzen wir

$$N(m, k) = \begin{cases} k, & \text{falls } (\lg(b) < 2); \\ \text{Ers}(\text{Ers}(k, 0, c+1), r+1, \text{Str}(w)), & \text{falls } (\lg(b) = 2 \wedge (b)_1 = 0); \\ \text{Ers}(\text{Ers}(k, 0, c+1), r+1, \text{Anh}(w, (b)_1)), & \text{falls } (\lg(b) = 2 \wedge (b)_1 > 0); \\ \text{Ers}(k, 0, (b)_{a+1}), & \text{falls } (\lg(b) > 2). \end{cases}$$

□

Nun beenden wir den Beweis des Satzes 3.1.9. Wir zeigen, dass je registermaschinen-berechenbare Funktion  $f(x_1, \dots, x_n)$   $\mu$ -rekursiv ist.

**Definition 3.3.4.** Sei  $\mathcal{M}$  eine  $R$ -Registermaschine, so dass  $f = F_{\mathcal{M}}^n$ . Wir setzen

$$\text{Eingabe}(R, \ulcorner w_1 \urcorner, \dots, \ulcorner w_n \urcorner) = \langle 0, \square, \ulcorner w_1 \urcorner, \dots, \ulcorner w_n \urcorner, \square, \dots, \square \rangle.$$

Der Befehl  $b_0$  soll also der Anfangsbefehl sein. Falls  $\mathcal{M}$  etwas berechnen soll, wird  $N \geq 1$  sein und  $b_0 \neq \text{Stop}$ . Hierbei stehen rechts  $R - n - 1$  leere Register. Dies ist die Gödelnummer der Anfangskonfiguration einer  $R$ -Registermaschine mit Eingabe  $x_1, \dots, x_n$ . Wir setzen weiter

$$\text{Stop}(m, k) :\Leftrightarrow (m)_{(k)_0} = 0.$$

Die Funktion Eingabe ist eine primitiv rekursive Funktion und Stop ist ein primitiv rekursives Prädikat. Die primitiv rekursive Funktion

$$\text{Ausgabe}(k) = (k)_1$$

liefert den Inhalt des Registers  $\mathcal{R}_0$  als Zahl interpretiert. Wir setzen  $N^0(m, k) = k$ ,  $N^{s+1}(m, k) = N(N^s(m, k))$  ( $s$  steht für stage).

**Definition 3.3.5.** [Kleene-Prädikat] Die Relation  $T_n$  heißt *n-stelliges Kleene-Prädikat*<sup>3</sup>.

$$\begin{aligned} T_n(m, \ulcorner w_1 \urcorner, \dots, \ulcorner w_n \urcorner, g) :\Leftrightarrow & N^{(g)_1}(m, \text{Eingabe}((m)_{\lg(m)-2}, \ulcorner w_1 \urcorner, \dots, \ulcorner w_n \urcorner)) = (g)_2 \\ & \wedge \text{Stop}(m, (g)_2) \wedge \text{Ausgabe}((g)_2) = (g)_0. \end{aligned}$$

**Satz 3.3.6.** Sei  $n \geq 1$ . Das Kleene-Prädikat  $T_n \subseteq \mathbb{N}^{n+2}$  ist primitiv rekursiv, und für jede Registermaschine  $\mathcal{M}$  über einem Alphabet  $\mathcal{A} = \{a_0, \dots, a_L\}$  ist die  $n$ -stellige Funktion  $f = F_{\mathcal{M}}^n: (\mathcal{A}^*)^n \rightarrow \mathcal{A}^*$  gegeben durch ihre Kleene-Normalform:

$$\ulcorner f(\bar{w}) \urcorner = (\mu g T_n(\ulcorner M \urcorner, \ulcorner w_1 \urcorner, \dots, \ulcorner w_n \urcorner, g))_0. \quad (3.3.1)$$

**Satz 3.3.7.** Ist  $f$  registermaschinen-berechenbar, so ist  $f$   $\mu$ -rekursiv. Wir zeigten sogar: Jede  $\mu$ -rekursive und jede registermaschinen-berechenbare Funktion ist mit nur einer einzigen unbeschränkten Anwendung des  $\mu$ -Operators als  $\mu$ -rekursive Funktion darstellbar.

Wenn man diese Darstellung zurück in die Programmierung übersetzt, erhält man: Jedes Registerprogramm kann ersetzt werden durch ein äquivalentes, das nur eine einzige Schleife hat, deren Durchlaufzahl nicht durch eine primitiv rekursive Funktionen begrenzt ist.

*Beweis:* Alle Aussagen folgen aus der Darstellung (3.3.5) und der Tatsache, dass das Kleene-Prädikat primitiv rekursiv ist. □

**Korollar 3.3.8** (Church'sche These). Jede durch einen Algorithmus berechenbare Funktionen sind rekursiv.

<sup>3</sup>Stephen Cole Kleene, 1909 – 1994

### 3.4 Rekursiv aufzählbare Mengen und partielle rekursive Funktionen

Nun betrachten wir Mengen, die sich durch einen unbeschränkten Existenzquantor aus rekursiven Mengen ergeben. Viele interessante Mengen sind gerade auf diese Weise „halb“ berechenbar.

**Definition 3.4.1** (rekursiv aufzählbar). Sei  $n \geq 1$ . Eine Relation  $R \subseteq \mathbb{N}^n$  heißt rekursiv aufzählbar, wenn es eine  $n + 1$ -stellige rekursive Relation  $S$  gibt, so dass für all  $\bar{x} \in \mathbb{N}^n$ ,

$$R\bar{x} \leftrightarrow \exists y S(\bar{x}, y).$$

**Definition 3.4.2** (partielle rekursive Funktion). Eine partielle Funktion  $f: \mathbb{N}^n \xrightarrow{\text{partiell}} \mathbb{N}$  heißt partielle rekursive Funktion, wenn es eine Registermaschine  $\mathcal{M}$  gibt, so dass  $f = F_{\mathcal{M}}^n$ . Wenn  $\mathcal{M}$  auf die Eingabe  $\bar{x}$  nicht stoppt, dann ist  $f(\bar{x})$  nicht definiert. Man schreibt auch  $\bar{x} \notin \text{dom}(f)$ . Oft wird statt  $f = F_{\mathcal{M}}^n$  bei partiellen Funktionen auch  $f \simeq F_{\mathcal{M}}^n$  geschrieben.

*Bemerkung 3.4.3.* Jede rekursive Relation ist rekursiv aufzählbar und jede rekursive Funktion ist eine partielle rekursive Funktion.

**Lemma 3.4.4.** Seien  $P \subseteq \mathbb{N}^n$ ,  $R \subseteq \mathbb{N}^n$  rekursiv aufzählbar, sowie für  $1 \leq i \leq n$   $f_i$  eine  $k$ -stellige partielle rekursive Funktion. Dann sind auch die Relationen

- 1)  $P \vee R$ ,
- 2)  $P \wedge R$ ,
- 3)  $\{(x_1, \dots, x_{n-1}) : \exists z R(x_1, \dots, x_{n-1}, z)\}$ ,
- 4)  $T = \{(x_1, \dots, x_{n-1}, w) : \forall z < w R(x_1, \dots, x_{n-1}, z)\}$ ,
- 5)  $\{\bar{x} \in \mathbb{N}^k : R(f_1(\bar{x}), \dots, f_n(\bar{x}))\}$

rekursiv aufzählbar.

*Beweis:* Wir wählen rekursive Relationen  $\bar{P}$  und  $\bar{R}$  such that  $P(\bar{x}) \leftrightarrow \exists z \bar{P}(\bar{x}, z)$  und  $R(\bar{x}) \leftrightarrow \exists z \bar{R}(\bar{x}, z)$ .

- 1)  $P(\bar{x}) \vee R(\bar{x}) \leftrightarrow \exists z (\bar{P}(\bar{x}, z) \vee \bar{R}(\bar{x}, z))$ .
- 2) Wir erinnern an die primitiv rekursive Funktion  $(x, i) \mapsto (x)_i$  aus Lemma 3.2.9.  $P(\bar{x}) \wedge R(\bar{x}) \leftrightarrow \exists z (\bar{P}(\bar{x}, (z)_0) \wedge \bar{R}(\bar{x}, (z)_1))$ .
- 3)  $\exists z R(x_1, \dots, x_{n-1}, z) \leftrightarrow \exists s \bar{R}(x_1, \dots, x_{n-1}, (s)_0, (s)_1)$ .
- 4)  $T(x_1, \dots, x_{n-1}, w) \leftrightarrow \exists s \forall z < w \bar{R}(x_1, \dots, x_{n-1}, z, (s)_z)$ .
- 5) Es sei für  $1 \leq i \leq n$  die  $k$ -stellige Funktion  $f_i$  durch die Registermaschine  $\mathcal{M}_i$  partiell berechnet. Nach dem Satz über die Kleene-Normalform gilt

$$f_i(\bar{x}) = y \leftrightarrow \exists g (T_k(\ulcorner \mathcal{M}_i \urcorner, \bar{x}, g) \wedge (g)_0 = y).$$



Sei  $R(\bar{x}) \leftrightarrow \exists z \bar{R}(\bar{x}, z)$ . Dann gilt

$$R(f_1(\bar{x}), \dots, f_n(\bar{x})) \leftrightarrow \exists z \exists (g_i)_{1 \leq i \leq n} \left( \bigwedge_{1 \leq i \leq n} T_k(\ulcorner \mathcal{M}_i \urcorner, \bar{x}, g_i) \wedge (g_i)_0 = y_i \wedge \bar{R}(\bar{y}, z) \right).$$

Die Relationen hinter den Existenzquantoren sind jeweils rekursiv.  $\square$

**Lemma 3.4.5.** *Sei  $\emptyset \neq A \subseteq \mathbb{N}$ .  $A$  ist genau dann rekursiv aufzählbar, wenn  $A$  die Bildmenge einer rekursiven Funktion ist.*

*Beweis:* Sei  $A$  die Bildmenge einer rekursiven Funktion. Dann gilt

$$A(y) \leftrightarrow \exists x f(x) = y$$

und somit ist  $A$  rekursiv aufzählbar.

Sei  $A$  rekursiv aufzählbar und sei  $a \in A$ . Wir nehmen eine rekursive Relation  $S$ , so dass  $A(y) \leftrightarrow \exists x S(x, y)$ . Dann setzen wir

$$f(z) = \begin{cases} (z)_1, & \text{falls } S((z)_0, (z)_1), \\ a, & \text{sonst.} \end{cases}$$

und erhalten  $A = \text{Im}(f)$ .  $\square$

**Lemma 3.4.6.** *Sei  $A \subseteq \mathbb{N}$ .  $A$  ist genau dann rekursiv aufzählbar, wenn  $A$  der Definitionsbereich einer partiellen rekursiven Funktion ist.*

*Beweis:* Die Umkehrfunktion vom vorigen Lemma bezeugt die Vorwärtsrichtung. Man kann auch  $f(\bar{x}) = \mu z S(\bar{x}, z)$  nehmen.  $\square$

**Definition 3.4.7** (universelle rekursiv aufzählbare Relation). Sei  $U \subseteq \mathbb{N} \times \mathbb{N}$ .  $U$  heißt *universelle rekursiv aufzählbare Relation*, wenn für jedes rekursiv aufzählbare  $R \subseteq \mathbb{N}$  ein Index  $e$  existiert, so dass  $R = \{n : U(e, n)\}$ . Man schreibt auch  $R = U(e, \cdot)$ .

**Satz 3.4.8.** *Es gibt eine universelle rekursiv aufzählbare Relation.*

*Beweis:*

Wir setzen

$$U(e, x) \leftrightarrow \exists g T_1(e, x, g),$$

Man kann sich  $U(e, \cdot)$  als Definitionsbereich der Maschine  $\mathcal{M}$  mit Nummer  $\ulcorner \mathcal{M} \urcorner = e$  vorstellen, also

$$U(e, x) \leftrightarrow \exists y (F_{\mathcal{M}}^1(x) = y \wedge \ulcorner \mathcal{M} \urcorner = e).$$

Sei  $R \subseteq \mathbb{N}^n$  rekursiv aufzählbar. Dann gibt es eine Registermaschine  $\mathcal{M}$ , so dass  $R = \text{dom}(F_{\mathcal{M}}^n)$ . Dann gilt  $R(x) \leftrightarrow U(\ulcorner \mathcal{M} \urcorner, x)$ .  $\square$

**Folgerung 3.4.9.**  $\{x : U(x, x)\}$  ist nicht rekursiv.

*Beweis:* Falls  $U$  rekursiv wäre, so auch  $\neg U$ . Dann ist  $\neg U$  rekursiv aufzählbar und also durch ein  $U(e, \cdot)$  gegeben. Nun erhalten wir

$$\neg U(e, e) \leftrightarrow U(e, e).$$

Widerspruch. □

*Bemerkung 3.4.10.* Es gibt keine universelle rekursive Relation.

**Folgerung 3.4.11.**  $R$  ist rekursiv genau dann, wenn  $R$  und  $\neg R$  rekursiv aufzählbar sind.

*Beweis:* Die Vorwärtsrichtung ist klar, da mit  $R$  auch  $\neg R$  rekursiv ist.

Für die Rückwärtsrichtung wählen wir rekursive Relationen  $V$  und  $W$ , so dass  $R(\bar{x}) \leftrightarrow \exists y V(\bar{x}, y)$  und  $\neg R(\bar{x}) \leftrightarrow \exists y W(\bar{x}, y)$ . Sei

$$g(\bar{x}) := \mu y (V(\bar{x}, y) \vee W(\bar{x}, y)),$$

dann ist  $g$  eine rekursive Funktion und es gilt

$$R(\bar{x}) \leftrightarrow V(\bar{x}, g(\bar{x})).$$

□

### 3.4.1 Exkurs über die Ackermannfunktion

**Definition 3.4.12.** Die Ackermann-Funktion<sup>4</sup> in der einfacheren zweistelligen Version von Péter<sup>5</sup> und Raffael Robinson<sup>6</sup> wird definiert durch:

$$\begin{aligned} \varphi(0, n) &= n + 1 \\ \varphi(m + 1, 0) &= \varphi(m, 1) \\ \varphi(m + 1, n + 1) &= \varphi(m, \varphi(m + 1, n)) \end{aligned}$$

Die ursprüngliche Ackermann-Funktion war dreistellig.

**Satz 3.4.13.**

- 1)  $n \rightarrow \varphi(k, n)$  ist primitiv rekursiv für jedes  $k$ .
- 2)  $(m, n) \mapsto \varphi(m, m)$  ist nicht primitiv rekursiv.

<sup>4</sup>Wilhelm Friedrich Ackermann, 1896 – 1962

<sup>5</sup>Rózsa Péter, geb. Rózsa Politzer, 1905 – 1977

<sup>6</sup>Raphael Robinson, 1911 – 1995

*Beweis:* Wir schreiben  $\varphi_k(n) = \varphi(k, n)$ . 1) Die Funktion  $\varphi_0$  ist die Nachfolgerfunktion  $S$ , die primitiv rekursiv ist. Wir nehmen an, dass  $\varphi_k$  primitiv rekursiv ist, und zeigen dass auch  $\varphi_{k+1}$  primitiv rekursiv ist.

$$\begin{aligned}\varphi_{k+1}(0) &= \varphi_k(1) \\ \varphi_{k+1}(n+1) &= \varphi_k(\varphi_{k+1}(n))\end{aligned}$$

ist die primitiv rekursive Rekursion nach Regel R2, angewandt auf  $h = \varphi_k$ . □

Zum Beweis des Teils 2) zeigen wir erst zwei Lemmata.

**Lemma 3.4.14.** *Es gilt für alle  $m$ , dass  $\forall n \varphi(m, n) > n$  und  $\varphi(m, \cdot)$  monoton ist.*

*Beweis:* Wir führen Induktion über  $m$ . Sei  $m = 0$ . Dann ist

$$\varphi(0, n) = n + 1,$$

und diese Funktion hat die beiden behaupteten Eigenschaften.

$m \mapsto m + 1$ :

$$\varphi(m + 1, n) = \varphi(m, \varphi(m + 1, n - 1)) \geq \max(n + 1, \varphi(m, n), \varphi(m + 1, n - 1)),$$

ist also monoton wachsend und oberhalb der Nachfolgerfunktion. □

**Lemma 3.4.15.**  $\varphi(m + 1, n) \geq \varphi(m, n + 1)$ .

*Beweis:*

$n = 0$ :

$$\varphi(1, 0) = \varphi(0, 1) = 2 \geq \varphi(0, 1).$$

$m = 0$ :

$$\varphi(1, n) = \varphi(0, \varphi(1, n - 1)) \geq \varphi(0, n + 1).$$

$m \mapsto m + 1$ :

$$\varphi(m + 1, n) = \varphi(m, \varphi(m + 1, n - 1)) \geq \varphi(m, \varphi(m, n)) \geq \varphi(m, n + 1).$$

□

Nun folgt der Beweis des zweiten Teils des Satzes 3.4.13 aus dem folgenden Lemma.

**Lemma 3.4.16.** *Für jede primitiv rekursive Funktion  $f$  existiert ein  $k$ , so dass*

$$\forall \bar{x} f(\bar{x}) \leq \varphi\left(k, \sum_i x_i\right).$$

*Beweis:* Wir zeigen die Behauptung induktiv über den Aufbau der primitiv rekursiven Funktion  $f$ . Wir beginnen mit den Grundfunktionen.

$$\begin{aligned} S(x) &\leq \varphi(0, x), \\ C &\leq \varphi(0, 0), \\ I_n^i(x_1, \dots, x_n) &\leq \varphi(0, \sum_i x_i). \end{aligned}$$

Nun betrachten wir die Hintereinanderausführung: Seien  $g_i(\bar{x})$ ,  $i < l$ , jeweils durch  $\varphi(k, \bar{x})$  beschränkt. Sei  $k \geq 1$  und sei  $h(\bar{y})$  durch  $\varphi(k', \sum \bar{y})$  beschränkt. Sei weiter  $k' \geq k$  und  $k' \geq l$ . Sei  $f(\bar{x}) = h(g_0(\bar{x}), \dots, g_{l-1}(\bar{x}))$ . Dann ist

$$\begin{aligned} h(g_0(\bar{x}), \dots, g_{l-1}(\bar{x})) &\leq \varphi(k', l \cdot \varphi(k, \sum \bar{x})) \\ &\leq \varphi(k', \varphi(k+1, \sum \bar{x} + 1)) \quad \text{falls } k+1 \geq 2 \\ &\leq \varphi(k'+1, \sum \bar{x} + 2) \\ &\leq \varphi(k'+3, \sum \bar{x}) \\ &\leq \varphi(k'+3+l, \sum \bar{x}). \end{aligned}$$

Nun betrachten wir die primitive Rekursion. Sei  $k' \geq k \geq 2$  und seien  $g$  und  $h$  gegeben, so dass für alle Argumente

$$\begin{aligned} g(\bar{x}) &\leq \varphi(k, \sum x_j) \\ h(\bar{x}, y, z) &\leq \varphi(k', \sum_j x_j + y + z) \end{aligned}$$

Dann erhalten wir

$$\begin{aligned} f(\bar{x}, 0) &= g(\bar{x}) \leq \varphi(k, \sum \bar{x}), \\ f(\bar{x}, y+1) &= h(\bar{x}, y, f(\bar{x}, y)) \\ &\leq \varphi(k', (\sum \bar{x} + y + f(\bar{x}, y))) \\ &\leq \varphi(k', \sum \bar{x} + y + \varphi(k, (\sum \bar{x} + y))) \\ &\leq \varphi(k', \varphi(k+1, \sum \bar{x} + y)), \quad \text{falls } k \geq 2 \\ &\leq \varphi(k'+1, \sum \bar{x} + y) \\ &\leq \varphi(k'+2, \sum \bar{x} + y). \end{aligned}$$

□

### 3.5 Gödelnummern von Formeln

**Definition 3.5.1.** Sei  $L = \{\lambda_i : i < L \leq \omega\}$  endlich oder primitiv rekursiv oder rekursiv. Das heißt, es gibt eine (primitiv) rekursive Funktion  $g: L \rightarrow \{0, 1, 2\} \times \mathbb{N}$ , so dass  $g(i)$  die Art des

Symbols angibt (0/1/2 für Konstante/Funktion/Relation) und dessen Stelligkeit, hierbei setzen wir die Stelligkeit der Konstantensymbole auf 0. Für endliches  $L$  gibt es natürlich immer so eine primitiv rekursive Funktion  $g$ . Dann ordnen wir folgende Gödelnummern zu

$$\begin{array}{lll} \ulcorner = \urcorner = \langle 0, 0 \rangle & \ulcorner ( \urcorner = \langle 0, 3 \rangle & \ulcorner \lambda_1 \urcorner = \langle 0, 6 \rangle & \ulcorner v_0 \urcorner = \langle 1, 0 \rangle \\ \ulcorner \wedge \urcorner = \langle 0, 1 \rangle & \ulcorner ) \urcorner = \langle 0, 4 \rangle & \vdots & \vdots \\ \ulcorner \neg \urcorner = \langle 0, 2 \rangle & \ulcorner \exists \urcorner = \langle 0, 5 \rangle & \ulcorner \lambda_l \urcorner = \langle 0, l + 6 \rangle, \text{ für } l < L & \\ \ulcorner \varphi \urcorner = \langle \ulcorner \xi_1 \urcorner, \dots, \ulcorner \xi_n \urcorner \rangle \text{ für Formeln } \varphi & & & \\ \ulcorner t \urcorner = \langle \ulcorner \xi_1 \urcorner, \dots, \ulcorner \xi_n \urcorner \rangle \text{ für Terme } t & & & \end{array}$$

**Lemma 3.5.2.** Falls  $g$  wie oben primitiv rekursiv ist, so gilt: Jede der folgenden Mengen

$$\begin{aligned} & \{ \ulcorner t \urcorner : t \text{ } L\text{-Term} \} \\ & \{ \ulcorner \varphi \urcorner : \varphi \text{ } L\text{-Formel} \} \\ & \{ \ulcorner \varphi \urcorner : \varphi \text{ } L\text{-Satz} \} \end{aligned}$$

ist primitiv rekursiv.

*Beweis:* (Skizze) Wir zeigen nur die erste Aussage. Man stellt sich einen Zähler für die Aufbauschritte der Terme oder Formel vor definiert zuerst die (primitiv) rekursive Relation  $\text{Term}(t, n)$  für “ $t$  ist die Gödelnummer eines  $L$ -Term mit  $\leq n$  Aufbauschritten”. Danach kann man die Anzahl der Aufbauschritte durch  $t$  beschränken.

$$\begin{aligned} \text{Term}(t, 0) & \leftrightarrow \exists l \leq t (t = \langle 0, l \rangle \vee (t = \langle 0, l + 6 \rangle \wedge g(l) = 0)), \\ \text{Term}(t, n + 1) & \leftrightarrow \text{Term}(t, n) \vee \exists l, j, s \leq t \left( (t)_0 = \langle 0, l + 6 \rangle \wedge g(l) = \langle 1, j \rangle \wedge \right. \\ & \quad \left. \bigwedge_{e < j} \text{Term}((s)_e, n) \wedge t = \langle (t)_0 \hat{\ } E((s)_0) \hat{\ } \dots \hat{\ } E((s)_{j-1}) \rangle \right). \end{aligned}$$

Hierbei ist  $E(s)$  die Auflistung der einzelnen im Primzahlprodukt  $s$  kodierten Zahlen. Das Lemma 1.1.11 über die eindeutige Lesbarkeit der Terme zeigt, dass dieser rekursive Abbau funktioniert.

Die zweite Aussage basiert auf Lemma 1.1.14. Für die dritte Aussage zieht man die induktive Definition des freien Vorkommens einer Variablen in einer Formel heran.  $\square$

**Definition 3.5.3** (effektiv axiomatisierbar). Sei  $T$  eine Menge von  $L$ -Sätzen.  $T$  heißt effektiv axiomatisierbar, wenn

$$\{ \ulcorner \varphi \urcorner : \varphi \in T \}$$

rekursiv ist.

*Beispiele 3.5.4.* ZFC, die Gruppentheorie, die Körpertheorie, die Theorie der linearen Ordnungen.

**Definition 3.5.5.** Sei  $T$  eine Theorie. Für den deduktiven Abschluss von  $T$  schreiben wir

$$T^+ = \{\varphi : \varphi \text{ L-Satz und } T \vdash \varphi\}.$$

Erinnerung: Der deduktive Abschluss einer Theorie ist die Menge aller ihrer Folgerungen.

**Satz 3.5.6.**

- 1) Ist  $T$  effektiv axiomatisierbar, dann ist  $\{\ulcorner \varphi \urcorner : T \vdash \varphi\}$  rekursiv aufzählbar.
- 2) Ist  $\{\ulcorner \varphi \urcorner : T \vdash \varphi\}$  rekursiv aufzählbar, dann ist  $T^+$  effektiv axiomatisierbar, hat also eine rekursive Axiomatisierung.

*Beweis von Satz 3.5.6:* 1) Es sei

$$T^* = \{\ulcorner \varphi \urcorner : \varphi \in T\}$$

rekursiv. Dann gilt

$$(T \vdash \varphi) \Leftrightarrow (\exists n)(n \text{ ist die Gödelnummer eines Beweises von } \varphi \text{ aus der Voraussetzung } T).$$

Bei festem rekursivem  $T$  ist die Menge der  $(n, \varphi)$  wie oben rekursiv. Man kodiert die endlich vielen Möglichkeiten die durch die Regeln B1 bis B5 gegeben sind, und für Regel B6 nutzt man, dass  $T$  rekursiv ist.

2) Sei  $T^+$  rekursiv aufzählbar, also  $x \in T^+ \Leftrightarrow \exists n R(x, n)$ . Seien  $n_m, m \in \mathbb{N}$ , die  $n$ , so dass es ein  $x$  gibt, so dass  $R(x, n)$  und  $x = \ulcorner \varphi \urcorner$  für ein  $\varphi$ . Wir nehmen jeweils das kleinst  $x$  zu  $n_m$  und nennen dieses  $x = \ulcorner \varphi_m \urcorner$ . Dann nehmen wir

$$T' = \{\ulcorner \varphi_0 \wedge \dots \wedge \varphi_m \urcorner : m \in \mathbb{N}\}.$$

$T'$  ist rekursiv aufzählbar, da  $R$  rekursiv ist.  $T'$  ist sogar rekursiv, denn es gilt  $\varphi \notin T'$  wenn im Aufbau ein  $\varphi^*$ , das länger ist als  $\varphi$ , vorkommt und  $\varphi$  noch nicht da war. Es gilt  $(T')^+ = T^+$ .  $\square$

*Beispiel 3.5.7.* Sei  $L$  eine rekursive Symbolmenge. Dann ist

$$\{\ulcorner \varphi \urcorner : \varphi \text{ L-Formel und } \emptyset \vdash_L \varphi\}$$

rekursiv aufzählbar.

Wir erinnern an den Begriff vollständige Theorie, Def. 1.4.14. Sei  $T$  eine widerspruchsfreie  $L$ -Theorie.  $T$  heißt vollständig, wenn für alle  $L$ -Sätze  $\varphi$  gilt

$$T \vdash \varphi \text{ oder } T \vdash \neg \varphi.$$

**Folgerung 3.5.8.** Wenn  $T$  effektiv axiomatisierbar und vollständig ist, so ist  $T^+$  rekursiv.<sup>7</sup>

<sup>7</sup>In Zieglers Buch heißt  $T$  entscheidbar, wenn  $T^+$  rekursiv ist. Verwechseln Sie nicht  $T$  und  $T^+$ .

*Beweis:*  $T^+$  ist r.a. Wir zeigen, dass auch das Komplement r.a. ist.

$$f(\ulcorner \varphi \urcorner) = \ulcorner \neg \varphi \urcorner \text{ ist berechenbar}$$

Wir zählen  $\ulcorner \varphi \urcorner$  in  $(T^+)^c$  auf, wenn  $\ulcorner \neg \varphi \urcorner \in T^+$ .

Da  $T^+$  rekursiv aufzählbar ist, ist also auch  $(T^+)^c$  rekursiv aufzählbar. Nach Folgerung 3.4.11 ist  $T^+$  rekursiv.  $\square$

### 3.6 Ein anderer Aufbau der Menge der rekursiven Funktionen

**Definition 3.6.1** (\*-rekursiv). Wir nennen eine Funktion, die sich nur aus

$$S, \quad I_i^m, \quad C_0^0, \quad +, \quad \cdot, \quad K_<$$

sowie R1 und R3 gewinnen lassen, \*-rekursiv.

**Satz 3.6.2.** *Alle rekursiven Funktionen sind \*-rekursiv.*

**Lemma 3.6.3.**

- 1)  $x \div y$  ist \*-rekursiv.
- 2) Die Klasse der \*-rekursiven Relationen ist abgeschlossen unter booleschen Kombinationen und beschränkter Quantifizierung. (Siehe Lemma 3.2.4)
- 3)  $x = y$  ist \*-rekursiv.
- 4)  $x \equiv y \pmod{z}$  ist \*-rekursiv.
- 5) Die Klasse der \*-rekursiven Funktionen ist abgeschlossen unter Definition durch \*-rekursive Fallunterscheidung. (Siehe Lemma 3.2.4)

*Beweis:*

- 1)  $x \div y = \mu z \ x < (y + z) + 1$
- 2) Die Abgeschlossenheit unter Boole'schen Kombinationen sieht man wie in Lemma 3.2.4. Wenn  $P(x, y)$  \*-rekursiv ist, definieren wir

$$g(x, z) = \mu y (P(x, y) \vee y = z).$$

Dann ist

$$\exists y < z \ P(x, y) \Leftrightarrow g(x, z) < z$$

\*-rekursiv.

- 3)  $x = y \Leftrightarrow (\neg x < y \wedge \neg y < x)$
- 4)  $x \equiv y \pmod{z} \Leftrightarrow \exists w < (x + y + 1)(x = y + wz \vee y = x + wz)$

5) Wie Lemma 3.2.4

□

**Lemma 3.6.4** (Die Gödel'sche  $\beta$ -Funktion). *Es existiert eine  $*$ -rekursive Funktion  $\beta(a, b, i)$  mit folgender Eigenschaft. Für jede endliche Folge  $c_0, c_1, \dots, c_{n-1}$  gibt es ein  $a$  und  $b$ , so dass für  $i = 0, \dots, n-1$*

$$\beta(a, b, i) = c_i.$$

*Beweis:*

$$\beta(a, b, i) = \mu z \ z \equiv a \pmod{b(i+1)+1}$$

ist  $*$ -rekursiv. Seien  $c_0, c_1, \dots, c_{n-1}$  gegeben. Wir wählen für  $b$  eine Zahl, die durch alle Zahlen zwischen 1 und  $n$  teilbar ist und die größer ist als alle  $c_i$ , z.B.  $b = n! \cdot (\sum_{j=0}^{n-1} c_j + 1)$ . Dann sind die  $b \cdot 1 + 1, b \cdot 2 + 1, \dots, b \cdot n + 1$  paarweise teilerfremd. Wenn nämlich  $p$  ein Primteiler von  $bi + 1$  ist, teilt  $p$  nicht  $b$ . Würde  $p$  auch  $bj + 1$  teilen, für ein  $j \neq i$ , wäre  $p$  Teiler von  $b(j - i)$  und daher auch von  $j - i$ . Da  $p \nmid b$ , kann  $p$  nicht den Teiler  $j - i$  von  $b$  teilen. Widerspruch.

$a$  sei eine gemeinsame Lösung der Kongruenzen

$$\begin{aligned} a &\equiv c_0 \pmod{b \cdot 1 + 1} \\ a &\equiv c_1 \pmod{b \cdot 2 + 1} \\ &\vdots \\ a &\equiv c_{n-1} \pmod{b \cdot n + 1} \end{aligned}$$

Weil  $c_i < b(i+1) + 1$ , ist  $c_i$  jeweils die kleinste natürliche Zahl, die zu  $a$  kongruent modulo  $b(i+1) + 1$  ist. □

**Lemma 3.6.5.** *Die  $*$ -rekursiven Funktionen sind unter der Aufbauregel R2 abgeschlossen.*

*Beweis:* Seien  $g$  und  $h$   $*$ -rekursiv.  $f$  entstehe aus  $g$  und  $h$  durch die Regel R2.

$$\begin{aligned} f(x, 0) &= g(x), \\ f(x, y + 1) &= h(x, y, f(x, y)). \end{aligned}$$

Wir definieren

$$R(x, y, a, b) \Leftrightarrow \beta(a, b, 0) = g(x) \wedge \forall i < y \underbrace{\beta(a, b, i + 1) = h(x, i, \beta(a, b, i))}_{* \text{-rekursiv}}.$$

Dann ist  $R$   $*$ -rekursiv. Es gilt

$$\forall x, y \exists a, b \ R((a, b), x, y).$$



Wir setzen

$$S(x, y) = \mu s \underbrace{\exists a, b < s R(x, y, a, b)}_{*-\text{rekursiv}}.$$

Nun können wir  $f$  als  $*$ -rekursive Funktion schreiben wie folgt

$$f(x, y) = \mu z \underbrace{\exists a, b < S(x, y) (R(x, y, a, b) \wedge z = \beta(a, b, y))}_{*-\text{rekursiv}}.$$

□

**Folgerung 3.6.6.** *Die  $*$ -rekursiven Funktionen stimmen mit den rekursiven Funktionen überein.*



# Kapitel 4

## Arithmetik

Die erststufige Zahlentheorie ist die Theorie der Struktur

$$\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1, <, S).$$

Diese Theorie wird auch die Arithmetik genannt. In diesem Kapitel befassen wir uns mit dieser Theorie und einigen ihrer rekursiv axiomatisierten Teiltheorien:  $Q^*$ ,  $Q$ ,  $P$ . Da  $<^{\mathfrak{N}}$  und  $S^{\mathfrak{N}}$  in  $(\mathbb{N}, +, \cdot, 0, 1)$  definierbar sind, werden sie auch oft weggelassen. Die im Vergleich zu  $(\mathbb{N}, +, \cdot, 0, 1)$  definitorisch erweiterte Struktur  $\mathfrak{N}$  gestattet bessere Lesbarkeit der Formeln.

### 4.1 Definierbare, rekursiv aufzählbare und rekursive Teilmengen

Wir werden sehen, dass  $\{\ulcorner \varphi \urcorner : \mathfrak{N} \models \varphi\}$  nicht rekursiv aufzählbar und sogar nicht arithmetisch ist.

Wir erinnern an  $L_N = \{0, 1, S, +, \cdot, <\}$ , die Sprache der Arithmetik.

**Definition 4.1.1** (arithmetisch). Eine Menge  $R \subseteq \mathbb{N}^n$  heißt arithmetisch, wenn es eine  $L_N$ -Formel  $\varphi$  gibt, so dass

$$R = \{\bar{a} \in \mathbb{N}^n : \mathfrak{N} \models \varphi[\bar{a}]\}.$$

Eine Funktion ist arithmetisch, wenn ihr Graph es ist.

Vorgriff (siehe weiter unten): Falls die definierende Formel eine  $\Sigma_1$ -Formel ist, so sagt man die Menge sei arithmetisch mit einer  $\Sigma_1$  Formel.

*Bemerkung 4.1.2.* Parameter ändern die Ausdrucksstärke nicht.

*Beweis:*

$$R = \{\bar{a} : \mathfrak{N} \models \varphi[\bar{a}, \bar{b}]\} = \{\bar{a} : \mathfrak{N} \models \varphi[\bar{a}, S^{(b_0)}(0), \dots, S^{(b_{n-1})}(n)]\}.$$

□

Im Allgemeinen können Parameter sehr wohl die Ausdrucksstärke erhöhen. Kenner(innen) mögen an  $V = L$  denken.  $L$  ohne Parameter wäre abzählbar.

**Definition 4.1.3** ( $\Sigma_1$ -Formeln). Eine  $\Sigma_1$ -Formel entsteht aus quantorenfreien Formeln durch Anwenden von  $\wedge$ ,  $\vee$ ,  $\exists x$  und beschränkten Allquantoren  $\forall x < t$ . Hierbei ist  $t$  ein Term. Die abkürzende Schreibweise  $\forall x < t \varphi$  steht für  $\forall x (x < t \rightarrow \varphi)$ .

**Satz 4.1.4.** *Jede rekursive Funktion ist arithmetisch mit einer  $\Sigma_1$ -Formel.*

*Beweis:* Wir nehmen zunächst nur die  $*$ -rekursiven Funktionen

$$K_{<}(a_1, a_2) = a_0 \leftrightarrow \mathfrak{N} \models (a_0 = 0 \wedge a_1 < a_2) \vee (a_0 = S(0) \wedge a_2 \leq a_1).$$

Für die anderen Grundfunktionen ist es noch einfacher.

**R1:** Sei  $g_i$  durch die  $\Sigma_1$ -Formel  $\varphi_i$  beschrieben und sei  $h$  durch die Formel  $\varphi_h$  beschrieben. Dann gilt in  $\mathfrak{N}$

$$h(g_1(x_1), g_2(x_1)) = y \leftrightarrow$$

$$\exists y_1 y_2 (\varphi_1(x_1, y_1) \wedge \varphi_2(x_1, y_2) \wedge \varphi_h(y_1, y_2, y)).$$

**R3:** Sei  $g(x_1, x_2) = x_0$  durch die Formel  $\varphi(x_0, x_1, x_2)$  beschrieben. Dann gilt

$$\mu x_2 g(x_1, x_2) = 0 = x_0 \leftrightarrow \varphi(\underline{0}, x_1, x_0) \wedge \forall x_2 < x_0 \neg \varphi(\underline{0}, x_1, x_2).$$

Da

$$\neg \varphi(\underline{0}, x_1, x_2) \leftrightarrow \exists y (y \neq \underline{0} \wedge \varphi(y, x_1, x_2)),$$

verlässt man die Menge der  $\Sigma_1$ -Formeln nicht. □

**Satz 4.1.5.** *Alle rekursiv aufzählbaren Relationen sind arithmetisch, sogar mit  $\Sigma_1$ -Formeln definierbar.*

*Beweis:* Sei  $R$  rekursiv aufzählbar und sei  $\bar{R}$  rekursiv und durch die  $\Sigma_1$ -Formel  $\varphi$  beschrieben. Es gilt also  $(\mathfrak{N} \models \varphi(\bar{a}, b)) \Leftrightarrow R(\bar{a}, b)$ . Dann ist  $R(x)$  durch

$$\exists y \varphi(0, \bar{x}, y)$$

beschrieben, und letzteres ist eine  $\Sigma_1$ -Formel. □

**Satz 4.1.6.**

$$\text{Th}(\mathfrak{N}) = \{ \ulcorner \varphi \urcorner : \varphi \text{ } L_N\text{-Aussage und } \mathfrak{N} \models \varphi \}$$

ist nicht arithmetisch.

*Beweis:* Wir setzen für  $a \in \mathbb{N}$ ,  $\Delta(a) = \Delta_a$  für den Term  $S^{(a)}(0)$ . Wir definieren ein universelles Prädikat  $U$  durch

$$U(e, a) :\Leftrightarrow \ulcorner \varphi \urcorner = e \wedge \mathfrak{N} \models \varphi(\Delta_a).$$

Angenommen  $\text{Th}(\mathfrak{N}) = \{a : \mathfrak{N} \models \varphi(\Delta_{\ulcorner a \urcorner})\}$  für ein  $\varphi$  mit einer freien Variable.  $\varphi_e$  ist die Formel, so dass  $\ulcorner \varphi \urcorner_e = e$ . Wenn  $\text{Th}(\mathfrak{N})$  arithmetisch ist, so auch

$$U = \{(e, a) : \mathfrak{N} \models \varphi(\Delta(\ulcorner \varphi_e(\Delta_a) \urcorner))\}.$$

Hier geht die primitiv rekursive Substitutionsfunktion

$$(e, a) \mapsto \ulcorner \varphi_e(\Delta_a) \urcorner$$

ein. Gelte  $\neg U(e, e)$  genau dann, wenn  $\mathfrak{N} \models \psi(\Delta_e)$ . Sei  $\ulcorner \psi \urcorner = d$ . Dann gilt

$$\mathfrak{N} \models \psi(\Delta_d) \Leftrightarrow \neg U(d, d).$$

Da aber  $\psi(d)$  dasselbe wie  $\varphi_d(\Delta_d)$  ist, gilt auch und

$$\mathfrak{N} \models \neg \psi(\Delta_d) \Leftrightarrow \neg(U(d, d)),$$

ein Widerspruch.  $\text{Th}(\mathfrak{N})$  und  $U$  (und auch die Diagonale von  $U$ ) sind nicht arithmetisch.  $\square$

**Satz 4.1.7** (Erster Gödel'scher Unvollständigkeitssatz für  $\text{Th}(\mathfrak{N})$ ). *Jede arithmetische Teiltheorie von  $\text{Th}(\mathfrak{N})$  ist unvollständig.*

*Beweis:* Sei  $T \subseteq \text{Th}(\mathfrak{N})$  arithmetisch via  $\varphi(\cdot)$ . Dann ist auch  $T^+$  arithmetisch und  $T^+ \subseteq \text{Th}(\mathfrak{N})$ .

$$\mathfrak{N} \models \ulcorner \varphi \urcorner \in T^+ \Leftrightarrow \exists n \text{Bew}_T(\ulcorner \varphi \urcorner, \underline{n})$$

Die Relation  $\{(n, m) : \text{Bew}_T(m, n)\}$  ist rekursiv aufzählbar, falls  $T$  rekursiv aufzählbar ist. Die Relation ist arithmetisch, falls  $T$  arithmetisch ist (man denke an B6). Wenn nun  $T^+ \subseteq \text{Th}(\mathfrak{N})$  vollständig wäre, so wäre  $T^+ = \text{Th}(\mathfrak{N})$ , also nach dem vorigen Satz nicht arithmetisch.  $\square$

**Satz 4.1.8.**  *$\text{Th}(\mathfrak{N})$  ist nicht rekursiv aufzählbar und nicht rekursiv.*

*Beweis:* Dieser Satz ist zwar im Satz 4.1.6 enthalten, hat aber für sich einen einfacheren Beweis (ohne Rückgriff auf das Substitutionslemma). Man kann jede rekursiv aufzählbare Teilmenge von  $\mathbb{N}$  in  $\mathfrak{N}$  repräsentieren. (Genauer zum Begriff des Repräsentierens findet man weiter unten.) In einer vollständigen r.a. Theorie kann man auch das Negat repräsentieren und hätte so die Relation als rekursiv erwiesen. Dann wäre aber jede r.a. Relation rekursiv.  $\square$

## 4.2 Cobhams unentscheidbare Theorie $Q^*$ , Robinsons Theorie $Q$

**Definition 4.2.1.** Die Axiome von (Raffael Robinsons)  $Q$  sind:

- $Q1 \quad \forall x \ x + 0 = x.$
- $Q2 \quad \forall x \forall y \ x + (y + 1) = (x + y) + 1.$
- $Q3 \quad \forall x \ x \cdot 0 = 0.$
- $Q4 \quad \forall x \forall y \ x \cdot (y + 1) = x \cdot y + x.$
- $Q5 \quad \forall x \ \neg x < 0.$
- $Q6 \quad \forall x \forall y \ (x < Sy \leftrightarrow (x = y \vee x < y)).$

Für jedes  $a, b \in \mathbb{N}$  sind die folgenden Aussagen in  $Q$  ableitbar

- $Q_1^* \quad \Delta_a + \Delta_b = \Delta_{a+b}.$
- $Q_2^* \quad \Delta_a \cdot \Delta_b = \Delta_{a \cdot b}.$
- $Q_3^* \quad \forall x \ (x < \Delta_a \leftrightarrow (x = \Delta_0 \vee \dots \vee x = \Delta_{a-1})).$

Wobei  $\Delta_a = S^a(\underline{0})$  der kanonische  $L_N$ -Term sei, der die Zahl  $a$  in  $\mathfrak{N}$  darstellt.

**Definition 4.2.2** (Die Cobham Theorie). Cobhams<sup>1</sup> Theorie ist die Theorie  $Q^*$ , die aus allen Instanzen von  $Q_1^*$ ,  $Q_2^*$  und  $Q_3^*$  besteht.

Es gilt  $Q^* \subseteq Q^+$ .

**Folgerung 4.2.3** (Per Induktion aus  $Q^*$ ). Für alle natürlichen  $a, b$  gilt

- 1)  $a \neq b \Rightarrow Q^* \vdash \neg \Delta_a = \Delta_b.$
- 2)  $a < b \Rightarrow Q^* \vdash \Delta_a < \Delta_b.$
- 3)  $a \not< b \Rightarrow Q^* \vdash \neg \Delta_a < \Delta_b.$

*Beweis per Induktion über  $b$ :*

- 2) Für  $b = 1$  haben wir  $Q^* \vdash 0 < 1$ . Im Schritt  $b \mapsto b + 1$  erhalten wir

$$\begin{array}{ll} Q^* \vdash b < b + 1 & \text{nach } Q_3^*, \\ Q^* \vdash a < b + 1 & \text{nach } Q_3^* \text{ für } a < b. \end{array}$$

- 3) Für  $b = 0$  folgt  $Q^* \vdash \neg \Delta_a < \Delta_0$ . Im Schritt  $b \mapsto b + 1$  folgt die Aussage aus

$$Q^* \vdash \Delta_a < \Delta_{b+1} \Rightarrow \Delta_a < \Delta_b \vee \Delta_a = \Delta_b.$$

- 1) Falls  $a \neq b$ , ordnen wir die beiden oBdA  $a < b$ . Dann ist nach Teil 2)  $Q^* \vdash \Delta_a < \Delta_b$ .  
Nun lesen wir  $Q_3^*$ .

---

<sup>1</sup>Alan Cobham

□

**Folgerung 4.2.4.** *Alle wahren quantorfreien  $L_N$ -Aussagen sind in  $Q^*$  beweisbar.*

**Definition 4.2.5.**  $\Sigma_1$ -Formeln im engen Sinne entstehen aus Formeln der Form

$$0 = x, \quad S(x) = y, \quad x + y = z, \quad x \cdot y = z, \quad x = y, \quad \neg x = y, \quad x < y, \quad \neg x < y$$

durch Anwenden von  $\vee, \wedge, \exists x, \forall x < y$ .

**Lemma 4.2.6.** *Jede  $\Sigma_1$ -Formel ist zu einer  $\Sigma_1$ -Formel im engen Sinne äquivalent.*

*Beweis:*

$$ft_0 \dots t_n = x \leftrightarrow (\exists y_0 \dots y_n (t_i = y_i \wedge f\bar{y} = x)).$$

Dies lässt sich weiter führen mit der Formel  $f\bar{y} = x$ , bis man zu den in Def. 4.2.5 genannten Grundrelationen gelangt. Für die negierten Gleichungen

$$\neg ft_0 \dots t_n = x$$

benutzt man folgende äquivalente Form

$$\exists y (ft_0 \dots t_n = x \wedge y \neq x).$$

□

*Bemerkung 4.2.7.* Beachten Sie, dass der folgende Satz 4.2.8 nur über  $\Sigma_1$ -Formeln spricht.

**Satz 4.2.8.** *Alle in  $\mathfrak{N}$  wahren  $\Sigma_1$ -Aussagen sind in  $Q^*$  beweisbar.*

*Beweis:* Wir zeigen für jede  $\Sigma_1$ -Formel  $\varphi$  im engen Sinne.

$$\mathfrak{N} \models \varphi[\bar{a}] \Rightarrow Q^* \vdash \varphi(\Delta_{a_1}, \dots, \Delta_{a_n}).$$

Die Richtung  $\Leftarrow$  gilt auch, aber da wie nicht mit der Negation an beliebiger Stelle als Formel-Aufbauschritt arbeiten können, schreiben wir sie lieber nicht hin.

Sei  $\varphi$  die Primformel, dann gilt

$$Q^* \vdash \varphi \vee Q^* \vdash \psi \Rightarrow Q^* \vdash \varphi \vee \psi.$$

$$Q^* \vdash \varphi \wedge Q^* \vdash \psi \Rightarrow Q^* \vdash \varphi \wedge \psi.$$

Zu beachten ist, dass  $\neg$  kein Aufbauschritt ist. Alle  $\neg$  stehen ganz innen

$$\mathfrak{N} \models \exists x \varphi(x, \bar{a}) \Rightarrow \mathfrak{N} \models \varphi(a_0, \bar{a}) \stackrel{\text{Satz 4.2.8}}{\Rightarrow} Q^* \vdash \varphi(\Delta_a, \Delta_{\bar{a}}) \Rightarrow Q^* \vdash \exists x \varphi(\Delta_{\bar{a}}).$$

$$(\forall a_0 \leq a_1 Q^* \vdash \varphi(\Delta_{a_0}, \Delta_{a_1})) \stackrel{Q_3^*}{\Rightarrow} Q^* \vdash \forall x < a_1 \varphi(x, \Delta_a).$$

□

**Folgerung 4.2.9.** *Sei  $T$  eine wahre Erweiterung von  $Q^*$ . Dann ist  $T^\perp$  unentscheidbar.*

*Beweis:* Sei  $R$  rekursiv aufzählbar und nicht rekursiv, und sei  $\varphi$  eine  $\Sigma_1$ -Definition von  $R$  nach Satz 4.1.5. Außerdem sei  $T \supseteq Q^{*\perp}$  und  $T$  sei wahr, d.h.  $T \subseteq \text{Th}(\mathfrak{N})$ . Dann haben wir folgende Implikationsketten:

$$\begin{aligned} R(a) \Rightarrow \mathfrak{N} \models \varphi[\Delta_a] &\stackrel{\text{Satz 4.2.8}}{\Rightarrow} Q^* \vdash \varphi(\Delta_a) \Rightarrow T \vdash \varphi(\Delta_a), \\ \neg R(a) \Rightarrow \mathfrak{N} \models \neg\varphi[\Delta_a] &\Rightarrow T \not\vdash \varphi(\Delta_a). \end{aligned}$$

Die letzte Implikation folgt aus der Wahrheit von  $T$ . Wir erhalten also, dass  $T^\perp$  mindestens so kompliziert wie  $R$  ist, also nicht rekursiv.  $\square$

### 4.3 Das Entscheidungsproblem

**Satz 4.3.1** (Satz von Church). *Die Menge*

$$E = \{\varphi : \emptyset \vdash \varphi, \varphi \text{ } L_N\text{-Satz}\}$$

*ist nicht entscheidbar.*

*Beweis:* Wenn  $E$  entscheidbar wäre, so auch  $Q^\perp$ , denn

$$\varphi \in Q^\perp \Leftrightarrow (\bigwedge Q \rightarrow \varphi) \in E.$$

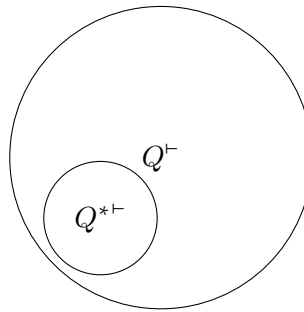
Da  $(Q^*)^\perp \subseteq Q^\perp$ , kann nach der Folgerung 4.2.9  $Q^\perp$  nicht entscheidbar sein.  $\square$

**Definition 4.3.2** (Repräsentieren).

Sei  $T$  eine  $L_N$ -Theorie und  $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$  eine partielle Funktion. Wir sagen „ $\varphi(v_0, \bar{v})$  repräsentiert  $f$  in  $T$ “, für alle  $a_0 = f(\bar{a})$  gilt

$$T \vdash \forall x (x = \Delta_{a_0} \leftrightarrow \varphi(x, \Delta_{a_1}, \dots, \Delta_{a_n}))$$

Je stärker eine Teiltheorie von  $\text{Th}(\mathfrak{N})$  ist, desto mehr Funktionen kann sie repräsentieren.





*Beispiel 4.3.3.* Für  $T = \text{Th}(\mathfrak{N})$  gilt, dass jede definierbare Funktion repräsentierbar ist.

**Lemma 4.3.4.** Sei  $f: \mathbb{N}^n \rightarrow \mathbb{N}$  durch eine Formel  $\varphi$  in  $\text{Th}(\mathfrak{N})$  definierbar. Es sei  $T \subseteq \text{Th}(\mathfrak{N})$  so stark, dass

$$\begin{aligned} T &\vdash \forall \bar{x} \exists y \varphi(y, \bar{x}) \text{ und} \\ T &\vdash \forall \bar{x} \forall y \forall y' (\varphi(y, \bar{x}) \wedge \varphi(y', \bar{x}) \rightarrow y = y'). \end{aligned}$$

Dann wird die Funktion  $f$  durch  $\varphi$  auch in  $T$  repräsentiert.

*Beispiel 4.3.5.* Man kann auch mit dem etwas schwächeren  $T'$  und partiellen  $f: \mathbb{N}^n \rhd \rightarrow \mathbb{N}$  arbeiten, wenn für jedes  $\bar{a} \in \text{dom}(f)$  gilt

$$\forall \bar{a} \ T' \vdash \exists y \ \varphi(y, \Delta_{\bar{a}}) \wedge \forall y y' (\varphi(y, \Delta_{\bar{a}}) \wedge \varphi(y', \Delta_{\bar{a}}) \rightarrow y = y').$$

*Bemerkung 4.3.6.* Jede in einer effektiv axiomatisierbaren Theorie  $T$  repräsentierte Funktion  $f: \mathbb{N}^n \rhd \rightarrow \mathbb{N}$  ist partiell rekursiv. Sei  $\varphi_f$  eine repräsentierende Formel. Dann ist  $f(\bar{a}) = a_0$  gdw  $T \vdash \varphi(\Delta_{a_0}, \Delta_{a_1}, \dots, \Delta_{a_n})$ . Die Menge der  $(a_0, \bar{a})$  auf der rechten Seite sind rek. aufzählbar.

Falls  $f$  total ist, so ist auch  $\{(a_0, \bar{a}) : f(\bar{a}) \neq a_0\}$  rekursiv aufzählbar. Denn es gilt  $\{(a_0, \bar{a}) : f(\bar{a}) \neq a_0\} = \{(a_0, \bar{a}) : \exists b (b \neq a_0 \wedge f(\bar{a}) = b)\}$ .

**Lemma 4.3.7.** Jede rekursive Funktion lässt sich in  $Q^*$  durch eine  $\Sigma_1$ -Formel repräsentieren.

*Beweis:* Man nimmt eine  $\Sigma_1$ -Formel  $\varphi$  aus dem Beweis des Satzes 4.1.4. Doch wir wiederholen dessen Beweis noch einmal sorgfältiger, da wir ja nur  $Q^*$  statt  $\text{Th}(\mathfrak{N})$  als Voraussetzungsmenge benutzen möchten. Wir zeigen induktiv über den Aufbau der  $*$ -rekursiven Funktion  $f$ , dass es eine  $\Sigma_1$ -Formel  $\varphi$  gibt, so dass

$$a_0 = f(\bar{a}) \Rightarrow T \vdash \forall x (x = \Delta_{a_0} \leftrightarrow \varphi(x, \Delta_{a_1}, \dots, \Delta_{a_n})).$$

Die Ausgangsfunktionen

$$S(x), \quad I_i^n, \quad C_0^0, \quad +, \quad \cdot, \quad \text{und} \quad K_<$$

sind in  $\mathfrak{N}$  quantorenfrei definierbar, also gilt nach Folgerung 4.2.4

$$\mathfrak{N} \models \varphi \text{ gdw. } Q^* \vdash \varphi$$

für jede dieser Definitionen.

Zu **(R1)**. Sei  $h$  durch  $\varphi_h$  in  $Q^*$  repräsentiert, und seien  $g_i$  durch  $\varphi_{g_i}$  repräsentiert. Dann gilt für alle  $a_1, a_2$

$$Q^* \vdash \forall x_0 (h(g_1(a_1), g_2(a_1)) = x_0 \leftrightarrow \exists y_1 \exists y_2 (\varphi_{g_1}(y_1, \Delta_{a_1}) \wedge \varphi_{g_2}(y_2, \Delta_{a_1}) \wedge \varphi_h(x_0, y_1, y_2)).$$

Bis jetzt gingen wir wie im Beweis des Satzes 4.1.4 vor. Für die Regel **(R3)** verstärken wir die in  $\text{Th}(\mathfrak{N})$  repräsentierende Formel um einen wahren Zusatz  $\gamma$ , der sichert, dass  $Q^*$  das Geforderte beweist. Dies geht wie folgt. Sei  $g(x_1, x_2)$  in  $Q^*$  repräsentiert durch  $\varphi_g(x_0, x_1, x_2)$  und gelte  $\mathfrak{N} \models \forall x_1 \exists x_2 g(x_1, x_2) = 0$ . Wir repräsentieren die Funktion

$$f(x_1) = \mu x_2 (g(x_1, x_2) = 0)$$

durch die Formel

$$\psi(x_0, x_1) = \alpha(x_0, x_1) \wedge \beta(x_0, x_1) \wedge \gamma(x_0).$$

Die Bestandteile sind gegeben durch

$$\begin{aligned} \alpha(x_0, x_1) &= \varphi(0, x_1, x_0), \\ \beta(x_0, x_1) &= \forall x_2 < x_0 \exists y (-0 = y \wedge \varphi_g(y, x_1, x_2)), \\ \gamma(x_0) &= 0 \leq x_0 \wedge \forall z < x_0 Sz \leq x_0. \end{aligned}$$

Dann ist

$$\forall x_2 < x_0 \neg \varphi(0, x_1, x_2) \text{ äquivalent zu } \forall x_2 < x_0 \exists y (-y = 0 \wedge \varphi(y, x_1, x_2)).$$

In  $\mathfrak{N}$  wird  $f$  durch  $\psi$  definiert. Sei nun  $a_0 = f(a_1)$ . Dann ist dies eine wahre  $\Sigma_1$ -Aussage und  $Q^* \vdash \psi(\Delta_{a_0}, \Delta_{a_1})$ . Noch zu zeigen ist

$$Q^* \vdash \forall x_0 (\psi(x_0, \Delta_{a_1}) \rightarrow x_0 = \Delta_{a_0}).$$

Für  $a_2 \in \mathbb{N}$  gilt

$$\mathfrak{N} \models \exists y (-0 = y \wedge \varphi(y, a_1, a_2) \leftrightarrow \neg \varphi(0, a_1, a_2)).$$

Allerdings gilt dies nur für  $a_2$  aus den natürlichen Zahlen. Wir zeigen induktiv über  $x_0$ :

$$Q^* \vdash \forall x_2 < x_0 (\exists y (-0 = y \wedge \varphi_g(y, a_1, x_2) \leftrightarrow \neg \varphi_g(0, a_1, x_2))).$$

Sei dazu  $f(a_1) = a_0$  und  $Q^* \vdash \psi(x_0, a_1)$ . Wir haben in  $Q^*$  zu zeigen, dass  $x_0 = a_0$  ist. Aus  $\gamma(a_0)$  folgt, dass  $x_0 = 0 \vee \dots \vee x_0 = a_0$  gilt oder  $x_0 > a_0$ . Der Fall  $x_0 = 0$  oder  $\dots$  oder  $x_0 = a_0 - 1$  ist durch die Formel  $\alpha \wedge \beta$  ausgeschlossen. Der Fall  $x_0 > a_0$  ist durch  $\alpha \wedge \beta$  verboten, denn dieses sorgt dafür, dass dann  $x_0$  nicht die kleinste Nullstelle von  $\varphi$  wäre.  $\square$

**Definition 4.3.8.** Eine Relation  $R$  wird in  $T$  repräsentiert durch eine Formel  $\varphi$ , falls für alle  $\bar{a}$  gilt

$$\begin{aligned} R(\bar{a}) &\Rightarrow T \vdash \varphi(\Delta_{a_0}, \dots, \Delta_{a_{n-1}}) \\ \neg R(\bar{a}) &\Rightarrow T \vdash \neg \varphi(\Delta_{a_0}, \dots, \Delta_{a_{n-1}}). \end{aligned}$$

**Folgerung 4.3.9.** Jede rekursive Relation  $R$  wird in  $Q^*$  durch eine  $\Sigma_1$ -Formel repräsentiert.

*Beweis:* Die Funktion  $K_R$  ist rekursiv und wird durch eine Formel  $\varphi(x_0, \bar{x})$  repräsentiert. Dann wird  $R$  durch  $\varphi(0, \bar{x})$  repräsentiert.  $\square$

## 4.4 Der Fixpunktsatz für $Q^*$

**Lemma 4.4.1** (Fixpunktsatz). *Zu jeder  $L_N$ -Formel  $\psi(v_0)$  gibt es einen  $L_N$ -Satz  $\varphi$ , so dass*

$$Q^* \vdash \varphi \leftrightarrow \psi(\Delta_{\ulcorner \varphi \urcorner}).$$

Wenn  $\psi \Sigma_1$  ist, gibt es ein  $\Sigma_1$   $\varphi$ .

*Beweis:* Wir definieren  $\text{Sub}: \mathbb{N}^2 \rightarrow \mathbb{N}$  wie folgt.

$$\text{Sub}(b, a) := \begin{cases} \ulcorner \chi(\Delta_a) \urcorner & \text{falls } b = \ulcorner \chi(v_0) \urcorner \wedge \text{fr}(\chi) = \{v_0\}, \\ 0 & \text{sonst.} \end{cases}$$

Sub ist eine primitiv rekursive Funktion. Es sei Sub im  $Q^*$  repräsentiert durch die  $\Sigma_1$ -Formel  $\sigma$ . Dann gilt für alle  $\chi$  in der freien Variablen  $v_0$

$$Q^* \vdash \forall x_0 \left( x_0 = \Delta_{\ulcorner \chi(\Delta_a) \urcorner} \leftrightarrow \sigma(x_0, \Delta_{\ulcorner \chi(v_0) \urcorner}, \Delta_a) \right). \quad (4.4.1)$$

Wir setzen nun

$$\rho(v_0) := \exists x_0 (\psi(x_0) \wedge \sigma(x_0, v_0, v_0)).$$

Wir setzen den Term  $\Delta_{\ulcorner \chi(v_0) \urcorner}$  für  $v_0$  ein und erhalten

$$\rho(\Delta_{\ulcorner \chi(v_0) \urcorner}) = \exists x_0 (\psi(x_0) \wedge \sigma(x_0, \Delta_{\ulcorner \chi(v_0) \urcorner}, \Delta_{\ulcorner \chi(v_0) \urcorner})).$$

Daraus erhalten aus Gleichung (4.4.1) wir für  $\chi = \rho$

$$Q^* \vdash \rho(\Delta_{\ulcorner \rho(v_0) \urcorner}) \leftrightarrow \psi(\Delta_{\ulcorner \rho(\Delta_{\ulcorner \rho(v_0) \urcorner}) \urcorner}).$$

Nun ist  $\varphi = \chi(\Delta_{\ulcorner \rho(v_0) \urcorner})$  der gewünschte Fixpunkt. □

**Folgerung 4.4.2.** *Sei  $T$  eine konsistente Erweiterung von  $Q^*$ . Dann ist  $T^\perp$  unentscheidbar.*

*Beweis:* Angenommen, für  $T \supseteq Q^{*\perp}$  sei  $T^\perp$  konsistent und entscheidbar. Dann folgt, dass eine Formel  $\tau$  den Abschluss  $T^\perp$  in  $Q^*$  repräsentiert, d.h.

$$\begin{aligned} T \vdash \varphi &\rightarrow Q^* \vdash \tau(\Delta_{\ulcorner \varphi \urcorner}), \\ T \not\vdash \varphi &\rightarrow Q^* \vdash \neg \tau(\Delta_{\ulcorner \varphi \urcorner}). \end{aligned}$$

Der Fixpunktsatz Satz 2.4.4 liefert nun die Existenz eines  $\delta$ , so dass

$$Q^* \vdash \delta \leftrightarrow \neg \tau(\Delta_{\ulcorner \delta \urcorner}).$$

Somit folgt

$$\begin{aligned} T \not\vdash \delta &\Rightarrow Q^* \vdash \neg\tau(\Delta_{\tau\delta}) \Rightarrow Q^* \vdash \delta \Rightarrow T \vdash \delta, \\ T \vdash \delta &\Rightarrow Q^* \vdash \tau(\Delta_{\tau\delta}) \Rightarrow Q^* \vdash \neg\delta \Rightarrow T \vdash \neg\delta \stackrel{T \text{ wfr}}{\Rightarrow} T \not\vdash \delta. \end{aligned}$$

□

**Folgerung 4.4.3.** Für jede Theorie  $T$ , so dass  $T \cup Q$  konsistent ist, ist  $T^+$  unentscheidbar.

## 4.5 Die Peanoarithmetik

**Definition 4.5.1.** Die Axiome der Peanoarithmetik<sup>2</sup>  $P$  sind die Axiome  $Q1$  to  $Q6$ , sowie das Induktionsschema  $\{I_\varphi : \varphi \in L_N\}$ . Die Formel  $I_\varphi$  heißt das Induktions-Axiom für  $\varphi$  und sieht wie folgt aus.

$$I_\varphi := \forall \bar{x} (\varphi(\bar{x}, 0) \wedge \forall y (\varphi(\bar{x}, y) \rightarrow \varphi(\bar{x}, y + 1)) \rightarrow \forall x \varphi(\bar{x}, x)).$$

**Lemma 4.5.2.**

$$\begin{aligned} P &\vdash \forall x \forall y (Sx = Sy \rightarrow x = y). \\ P &\vdash \forall x (x \neq 0 \rightarrow \exists y Sy = x). \\ P &\vdash < \text{ ist eine lineare Ordnung.} \\ P &\vdash \text{ Es gibt kein Element zwischen } x \text{ und } Sx. \\ P &\vdash +, \cdot \text{ definiert einen kommutativen Halbring mit Null und } 1. \\ P &\vdash +, \cdot \text{ sind monoton.} \\ P &\vdash \forall xy (x \leq y \rightarrow \exists z x + z = y). \end{aligned}$$

*Beweis:* Wir beweisen den zweiten Punkt.  $P$  beweist  $1 = S0$  und  $\exists y Sy = x \rightarrow \exists y' Sy' = Sx$  nämlich  $y' = Sy$ . Nun wenden wir das Induktionsaxiom für diese Aussage an und erhalten  $\forall x(x \neq 0 \rightarrow \exists y Sy = x)$ . Die anderen Punkte werden ähnlich bewiesen. □

Die Peanoarithmetik ist rekursiv axiomatisierbar, und somit ist  $P^+$  rek. aufzählbar. Also ist  $P$  eine echte Teiltheorie von  $\text{Th}(\mathfrak{N})$ . Noch stärker sind die sogenannten Peano-Axiome (s.u. nicht verwechseln mit  $P$ ). Diese sind zweitstufig und charakterisieren die natürlichen Zahlen  $(\mathbb{N}, 0, S, <)$  bis auf Isomorphie.

**Definition 4.5.3.** Die Peano-Axiome sind in der Sprache der zweiten Stufe formuliert und lauten wie folgt:

$$1) \quad \forall x \neg Sx = 0.$$

---

<sup>2</sup>Giuseppe Peano, 1851–1932

- 2)  $\forall xy(Sx = Sy \rightarrow x = y)$ .  
 3)  $\forall X(0 \in X \wedge \forall y(y \in X \rightarrow Sy \in X) \rightarrow \forall y y \in X)$ . Hierbei rangiert  $X$  über die Teilmengen des Trägers der Struktur.

Diese Axiome sind nicht Gegenstand unserer Vorlesung. Man kann sie um  $Q$  erweitern und erhält so ein Axiomensystem, das  $\mathfrak{N}$  bis auf Isomorphie charakterisiert.

**Lemma 4.5.4.** *Sei  $\varphi$  eine  $L_N$ -Formel.*

$$P \vdash \forall \bar{x} ((\forall y \forall z < y \varphi(\bar{x}, z) \rightarrow \varphi(\bar{x}, y)) \rightarrow \forall y \varphi(x, y))$$

*Beweis:* Wir setzen

$$\psi(y) := \forall z < y \varphi(z),$$

und vereinfachen  $I_\psi$  nach den Regeln für Tautologien. □

**Definition 4.5.5.** Sei  $T$  eine Theorie und  $\varphi$  eine  $\Sigma_1$ -Formel. Wir sagen, dass  $\varphi$  in  $T$  eine Funktion definiert, falls

$$T \vdash \forall \bar{x} \exists^=1 y \varphi(y, \bar{x}).$$

Wir erweitern in diesem Fall  $L$  um ein neues  $n$ -stelliges Funktionszeichen  $F_\varphi$ . Wir setzen

$$P^* = P \cup \{\forall \bar{x} \varphi(F_\varphi(\bar{x}), \bar{x}) : \varphi \text{ ist eine } \Sigma_1\text{-Formel und definiert eine Funktion in } P\}.$$

Falls es eine  $\Sigma_1$ -Formel  $\varphi$  gibt, die eine Funktion definiert und gilt  $P \vdash \forall \bar{x} \varphi(F(\bar{x}), \bar{x})$ , so sagen wir  $F$  ist  $\Sigma_1^P$ .

Da  $P^*$  eine definitorische Erweiterung von  $P$  ist, ist  $P^*$  eine konservative Erweiterung von  $P$ . Das gilt  $P^{**} = P^*$ , brauchen wir die  $*$ -Bildung nicht schrittweise zu wiederholen. Erinnern Sie sich an den Exkurs über definitorische Erweiterungen im ersten Kapitel.

**Satz 4.5.6.** *Jede primitiv rekursive Funktion  $F$  ist durch eine  $\Sigma_1$ -Formel in  $P$  definierbar.*

Zuerst zeigen wir ein Lemma:

**Lemma 4.5.7.**

1) *Die Gödelsche  $\beta$ -Funktion ist durch eine  $\Sigma_1^P$ -Funktion definierbar.*

2)

$$P^* \vdash \forall a, b, c, i \exists a', b' \forall j < i \beta(a, b, j) = \beta(a', b', j) \wedge c = \beta(a', b', i).$$

*Beweis:* 1) Die dreistellige Gödel'sche  $\beta$ -Funktion  $\beta(a, b, i) = c$  ist  $\Sigma_1^P$  mit der folgenden bezeugenden Formel.

$$\beta(a, b, i) = c_i \leftrightarrow (c_i < b \cdot (i + 1) + 1 \wedge \exists y a = c_i + y(b(i + 1) + 1)).$$

2) Die im  $P^*$  zu beweisende Eigenschaft ist in  $\mathfrak{N}$  wahr. Seien  $a, b, c, i$  gegeben, so dass  $\beta(a, b, i) = c$ . Dann setzen wir

$$c_0 = \beta(a, b, 0), \dots, c_{i-1} = \beta(a, b, i-1), c_i = c.$$

Nach dem Lemma über die Existenz der  $\beta$ -Funktion gibt es  $a'$  und  $b'$  mit

$$c_0 = \beta(a', b', 0), \dots, c_{i-1} = \beta(a', b', i-1), c_i = \beta(a', b', i).$$

Nun lassen wir viele Beweisschritte aus. Man prüft nach, dass das ganze Herleitung der  $\beta$ -Funktion in  $P^*$  funktioniert.  $\square$

Nun beweisen wir den Satz.

*Beweis:* Die Ausgangsfunktionen  $S, I_1^n, C_0^0$ , sind jeweils  $\Sigma_1^P$ . Die Einsetzung gemäß Regel R1, gibt, angewandt auf zwei  $\Sigma_1^P$ -Funktionen, wieder eine  $\Sigma_1^P$ -Funktion. Die Formel ist in Beweis von Satz 4.1.4 gegeben. Nun zeigen wir, dass die Anwendung der Rekursionsregel R2 auf zwei  $\Sigma_1$ -Funktionen  $g, h$  wieder zu einer  $\Sigma_1$ -Funktion führt. Sei

$$\begin{aligned} f(x, 0) &= g(x), \\ f(x, y+1) &= h(x, y, f(x, y)), \end{aligned}$$

mit Funktionen  $g, h$ , so dass  $g$  durch die  $\Sigma_1$ -Formel  $G(v_1) = v_0$  und  $h$  durch die  $\Sigma_1$ -Formel  $H(v_1, v_2, v_3) = v_0$  beschrieben wird. Die Funktion  $F$ , die aus  $G$  und  $H$  durch R2 entsteht, wird durch folgende  $\Sigma_1$ -Formel  $\varphi$  in  $\mathfrak{N}$  definiert.

$$\begin{aligned} \varphi(v_0, v_1, v_2) &= \exists ab \psi(v_0, v_1, v_2, a, b), \text{ wobei} \\ \psi(v_0, v_1, v_2, a, b) &= (\beta(a, b, 0) = G(v_1) \wedge v_0 = \beta(a, b, v_2) \\ &\quad \wedge \forall x < v_2 \beta(a, b, x+1) = H(v_1, x, \beta(a, b, x))). \end{aligned}$$

Nun zeigen wir mit einer Induktion über  $v_2$ , dass

$$P^* \vdash \forall v_1 v_2 \exists^{-1} v_0 \varphi(v_0, v_1, v_2).$$

$v_2 = 0$ :

$$\psi(v_0, v_1, 0, a, b) = G(v_1) = \beta(a, b, 0) = v_0.$$

$v_2 \rightarrow v_2 + 1$ : Seien  $y, a', b'$  so gewählt, dass  $P^*$  folgendes beweist:  $\varphi(y, v_1, v_2)$  und  $\psi(y, v_1, v_2, a', b')$ .

Nun liefert Punkt 2 aus Lemma 4.5.7 Elemente  $a, b$ , so dass

$$\forall x \leq v_2 \beta(a', b', x) = \beta(a, b, x) \quad \text{und} \quad \beta(a, b, v_2 + 1) = H(v_1, v_2, y) = v_0.$$

Die bezeugen

$$\psi(v_0, v_1, v_2 + 1, a, b) \text{ und } \varphi(v_0, v_1, v_2 + 1).$$

Nun zur Eindeutigkeit. Wir argumentieren in  $P^*$ . Die Folgerungen „also“ ergeben sich aus der Anwendung der Hilbertregeln auf  $P^* \vdash \dots$ . Sei  $v'_0$ , so dass

$$\varphi(v'_0, v_1, v_2 + 1).$$

Also ist für ein Paar  $a, b$

$$\psi(v'_0, v_1, v_2 + 1, a, b),$$

und mit  $y' := \beta(a, b, v_2)$

$$\psi(y', v_1, v_2, a, b).$$

Sei nun  $\varphi(y, v_1, v_2)$ . Dann gilt mit der Induktionsvoraussetzung  $y = y'$

$$v'_0 = H(v_1, v_2, y') = H(v_1, v_2, y).$$

□

*Bemerkung 4.5.8.* Wir zeigten also auch:

$$P^* \vdash \forall x (F(x, 0) = G(x) \wedge \forall y F(x, y + 1) = H(x, y, F(x, y))).$$

**Definition 4.5.9.** Wir könnten  $P$  auch nur um die  $\Delta_1^P$ -Funktionen (s.u.) erweitern oder gar nur um die primitiv rekursiven Funktionen und dies  $P^{\text{primitiv rekursiv}}$  nennen.

Es gilt

$$P^* \supseteq P^{\text{primitiv rekursiv}} \supseteq P.$$

**Definition 4.5.10** ( $\Delta_1^P$ ). Eine  $L_N$ -Formel  $\varphi$  heißt  $\Delta_1^P$ , wenn  $\varphi$  eine  $\Sigma_1$ -Formel ist und es ein  $\psi$  in  $\Sigma_1$  gibt, so dass

$$P \vdash \varphi \leftrightarrow \neg\psi.$$

**Folgerung 4.5.11.** Jede primitiv rekursive Funktion/Relation ist definierbar durch eine  $\Delta_1^P$ -Formel.

*Beweis:* Sei  $f$  durch die  $\Sigma_1$  Formel  $\varphi_f$  definiert. Dann gilt

$$P \vdash \varphi(v_0, v_1) \leftrightarrow \exists v_2 (\varphi(v_2, v_1) \wedge \neg v_2 = v_0).$$

Auf der rechten Seite steht wieder eine  $\Sigma_1$ -Formel. □

**Frage 4.5.12.** Nun stellt sich die Frage, ob aus  $R \in \Delta_1^P$  folgt, dass  $R$  primitiv rekursiv ist.

**Definition 4.5.13.**

$$F(a, b) = (a + b + 1) \frac{(a + b)}{2} + a$$

$F$  ist eine primitiv rekursive Bijektion von  $\mathbb{N}^2$  auf  $\mathbb{N}$ . Als nächstes stellt sich die Frage, ob die Umkehrfunktion der Funktion primitiv rekursiv ist. Dazu sei

$$\begin{aligned} F_0(c) &= a + b = \mu x < c \exists r \leq x \ c = x \frac{(x+1)}{2} + r, \\ F_1(c) &= c - F_0(c), \\ F_2(c) &= F_0(c) - F_1(c). \end{aligned}$$

Dann sind auch  $F_0$ ,  $F_1$ , und  $F_2$  primitiv rekursiv, und es gilt

$$F^{-1}(F(a, b)) = (a, b) = (F_1(F(a, b)), F_2(F(a, b))).$$

**Lemma 4.5.14.** *Die Funktion*

$$\beta'(a, i) = \beta(F_1(a), F_2(a), i)$$

ist  $\Sigma_1^P$  und primitiv rekursiv.

*Beweis:*

$$\beta'(a, i) = c \leftrightarrow \exists b \exists d (\beta(b, d, i) = c \wedge F_1(a) = b \wedge F_2(a) = d).$$

□

## 4.6 Der zweite Gödel'sche Unvollständigkeitssatz für $P$

Wir erinnern an den Vollständigkeitssatz:  $P \models \varphi$  gdw  $P \vdash \varphi$ . Nun wollen wir die Beweisbarkeit nach den Hilbertregeln in einer Kodierung in der Theorie  $P$  beschreiben, so dass  $P$  nach einer Anwendung einer Regel beweisen kann, dass es sich um eine Beweisverlängerung um einen gültigen Schritt handelt. Hier machen die Existenzführung im Antecedens und die  $\exists$ -Regel Zusatzüberlegungen nötig: Die unendlich vielen Möglichkeiten der Wahl eines Terms müssen in eine  $\Sigma_1^P$ -Suche gefasst werden. Wir arbeiten daher in  $P^*$ .

**Lemma 4.6.1.** *Die Relationen*

$$\begin{aligned} \text{Auss} &= \{ \ulcorner \varphi \urcorner : \varphi \text{ ist } L_N\text{-Satz} \}, \\ \text{Ax} &= \{ \ulcorner \varphi \urcorner : \text{ist } L_N\text{-Formel, die Axiom des Hilbertkalküls oder Axiom von } P \text{ ist} \}, \\ \text{Reg} &= \{ (\ulcorner \varphi \urcorner, \ulcorner \psi \urcorner, \ulcorner \chi \urcorner) : \varphi, \psi, \chi \text{ sind } L_N\text{-Formeln,} \\ &\quad \varphi \text{ folgt aus } \psi \text{ und } \chi \text{ mit einer Regel des Hilbertkalküls} \} \end{aligned}$$

und die Beweisbarkeitsprädikate

$$\begin{aligned} B'(s, n) &= \forall i < n (\text{Ax}(\beta'(s, i)) \vee \exists j, k < i \text{Reg}(\beta'(s, i), \beta'(s, j), \beta'(s, k))) \\ \text{Bew}'(f) &= \text{Auss}(f) \wedge \exists n, s (\beta'(s, n) = f \wedge B'(s, n+1)) \end{aligned}$$

sind jeweils  $\Sigma_1$  und definieren in  $\mathfrak{N}$  die Beweisbarkeit aus  $P$ .



Nun stellt sich die Frage, ob diese Formeln auch in  $P$  das Beweisbarkeitspädikat definieren. Dafür sind Ax und Reg nicht sorgfältig genug gewählt für den Beweis des dritten Loeb-Axioms L3. Wir erläutern die mögliche Schwierigkeiten.

*Beispiel 4.6.2.* Es gelte

$$\varphi \frac{t}{x} \rightarrow \exists x \varphi$$

also eine unbegrenzte Suche nach  $t$ . Dies lässt sich alternativ auch als

$$\forall x \varphi x \rightarrow \varphi \frac{t}{x}$$

ausdrücken.

Im nächsten Schritt wollen wir die Menge der Axiome von  $P$  erweitern. Wir fügen alle wahren  $\Sigma_1$ -Aussagen hinzu. Da nach Satz 4.2.8 alle wahren  $\Sigma_1$ -Aussagen schon in  $Q^*$  beweisbar sind, sind diese natürlich erst recht in  $P$  beweisbar.

Beachten Sie, dass das folgende Lemma sich nicht auf Fixpunkte der Formel  $\psi \leftrightarrow \neg \text{Bew}(\Delta_{\neg\psi})$  erstreckt.

**Lemma 4.6.3.** *Das Lemma von einer Wahrheitsdefinition für  $\Sigma_1$ -Formeln. Es gibt eine  $\Sigma_1$ -Relation  $W_1(x)$ , so dass für jede  $\Sigma_1$ -Formel  $\varphi$  gilt*

$$\begin{aligned} \mathfrak{N} \models \varphi &\leftrightarrow P \vdash \varphi \text{ und} \\ P \vdash \varphi &\leftrightarrow W_1(\Delta_{\neg\varphi}). \end{aligned}$$

*Beweis:* Wir suchen eine  $\Sigma_1$ -Eigenschaft  $W'$  so dass für alle  $\Sigma_1$ -Formeln  $\varphi(\bar{v})$  gilt

$$P^* \vdash \forall a(\varphi(\beta'(a, \Delta_0), \dots, \beta'(a, \Delta_{|\sigma|-1}))) \leftrightarrow W'_1(\Delta_{\neg\varphi}, a).$$

Es genügt zu zeigen, dass  $W'_1$  eine Wahrheitsdefinition für  $\Sigma_1$ -Formeln im engen Sinne ist, denn jede  $\Sigma_1$ -Formel lässt sich wiederum mit einer  $\Sigma_1^P$ -Funktion in eine  $\Sigma_1$ -Formel im engen Sinne übersetzen.

Alle  $\Sigma_1$ -Formeln im Beweis von  $\varphi(v_0, \dots, v_{s-1})$  aus  $P$  seien nun  $\Sigma_1$ -Formeln im engen Sinne.

Wir beschreiben die Erfüllt-Relation für  $\Sigma_1$ -Formeln im engen Sinne mit einer Belegung  $\sigma$  induktiv. Die  $\varphi_i$  bezeugen den Abbau der Formel bis hin zu Primformeln und die  $\sigma_i$  sind längere Belegungen, die man zum Abbau der Quantoren braucht.

Wir schreiben  $\beta'(a, i) = (a)_i$ . Dies weicht von der früheren Def. 3.2.9 ab. Ebenso definieren wir  $|\sigma|$  für  $\sigma \in \mathbb{N}$  durch das größte  $n$ , so dass für alle  $i < n$ ,

$$\beta(F_1(\sigma), F_2(\sigma), i) = \beta'(\sigma, i)$$

definiert ist. Dieses  $n$  berechnet sich aus  $F_2(\sigma)$  ( $F_2$  aus Def. 4.5.13) und der Bedingung, dass alle  $F_2(\sigma) \cdot i + 1$ ,  $i < n$ , teilerfremd sein müssen gemäß dem Beweis des Lemmas über die  $\beta$ -Funktion.

$$\mathfrak{N} \models \varphi(v_0, \dots, v_{r-1})[\sigma] \leftrightarrow \exists \varphi_0, \dots, \varphi_N \exists \sigma_0, \dots, \sigma_N (\varphi = \varphi_N \wedge \sigma = \sigma_N \wedge \forall n \leq N :$$

- $s_n = |\sigma_n|$  impliziert, dass höchstens  $v_0, \dots, v_{s_n-1}$  frei sind in  $\varphi_n$ . Außerdem ist  $|\sigma_N| \geq r$ .
- $\varphi_n = \Delta_0 = v_i \rightarrow 0 = (\sigma_n)_i$
- $\varphi_n = S(v_i) = v_j \rightarrow (\sigma_n)_i + 1 = (\sigma_n)_j$
- $\varphi_n = v_i + v_j = v_k \rightarrow (\sigma_n)_i + (\sigma_n)_j = (\sigma_n)_k$
- $\varphi_n = v_i \cdot v_j = v_k \rightarrow (\sigma_n)_i \cdot (\sigma_n)_j = (\sigma_n)_k$
- $\varphi_n = v_i = v_j \rightarrow (\sigma_n)_i = (\sigma_n)_j$
- $\varphi_n = \neg v_i = v_j \rightarrow \neg(\sigma_n)_i = (\sigma_n)_j$
- $\varphi_n = v_i < v_j \rightarrow (\sigma_n)_i < (\sigma_n)_j$
- $\varphi_n = \neg v_i < v_j \rightarrow \neg(\sigma_n)_i < (\sigma_n)_j$
- $\varphi_n = \varphi' \wedge \varphi'' \rightarrow \exists n', n'' < n ((\varphi_{n'} = \varphi') \wedge (\varphi_{n''} = \varphi'') \wedge \sigma_{n'} = \sigma_{n''} = \sigma_n)$
- $\varphi_n = \varphi' \vee \varphi'' \rightarrow \exists n' < n ((\varphi_{n'} = \varphi' \wedge \sigma_{n'} = \sigma_n) \vee (\varphi_{n'} = \varphi'' \wedge \sigma_{n'} = \sigma_n))$
- $\varphi_n = \exists v_i \varphi' \rightarrow \exists n' < n \exists a \varphi_{n'}(a) \wedge (\sigma_{n'})_k = (\sigma_n)_k$  für  $k$  mit  $k \neq i$  und  $k < \min\{s_n, s_{n'}\}$ .
- $\varphi_n = \forall v_i < v_j \varphi' \rightarrow \forall a < (\sigma_n)_j \exists n' < n (\varphi_{n'} = \varphi' \wedge (\sigma_{n'})_i = a \wedge (\sigma_{n'})_k = (\sigma_n)_k$  für  $k \neq i$ ,  $k < \min\{s_n, s_{n'}\}$

Die verwendeten Zerlegungen von Formeln in ihre Bestandteile sind primitiv rekursiv.

*Beispiel 4.6.4.*

$$\begin{array}{ll} \{\ulcorner \exists v_i \varphi' \urcorner : i \in N, \varphi' \Sigma_1\text{-Formel}\} & \text{ist primitiv rekursiv} \\ f(\ulcorner \exists v_i \varphi' \urcorner) = i & \text{ist primitiv rekursiv} \\ g(\ulcorner \exists v_i \varphi' \urcorner) = \ulcorner \varphi' \urcorner & \text{ist primitiv rekursiv} \end{array}$$

Die endlichen Folgen werden durch die  $\beta'$ -Funktion beschrieben und so erhalten wir eine  $\Sigma_1$ -Formel  $W_1'(f, a)$ . Nun gilt nach Wahl von  $W'$  für jede  $\Sigma_1$ -Formeln  $\varphi(\bar{v})$

$$P^* \vdash \forall a (\varphi(\beta'(a, \Delta_0), \dots, \beta'(a, \Delta_{|\sigma|-1})) \leftrightarrow W_1'(\Delta_{\ulcorner \varphi \urcorner}, a)). \quad (4.6.1)$$

Letzteres zeigt man induktiv über den Aufbau der  $\Sigma_1$ -Formeln in engen Sinne. Bei festem  $\varphi$  braucht man für den Quantor  $\forall a$  gerade die Stärke von  $P$  gegenüber der von  $Q^*$ . Wir können in  $P$  arbeiten, falls wir  $\beta'$  wieder durch seine definierende  $\Sigma_1$ -Formel ersetzen. Zum Schluss setzen wir  $W_1(x) = W_1'(x, \Delta_0)$ . □

**Definition 4.6.5.** Nun definieren wir das revidierte Beweisbarkeitsprädikat

$$B(s, n) := \forall i < n (W_1(\beta'(s, i)) \vee \text{Ax}(\beta'(s, i)) \vee \exists j, k < i \text{Reg}(\beta'(s, i), \beta'(s, j), \beta'(s, k)))$$

$$\text{Bew}(f) = \text{Auss}(f) \wedge \exists n \exists s (\beta'(s, n) = f \wedge B(s, n+1)). \quad (4.6.2)$$

Auch diese Formeln sind jeweils  $\Sigma_1$  und definieren in  $\mathfrak{N}$  die Beweisbarkeit aus  $P$ .

**Satz 4.6.6.**  $\text{Bew}(x)$  erfüllt die Löb-Axiome

$$L1 : P \vdash \varphi \Rightarrow P \vdash \text{Bew}(\Delta_{\ulcorner \varphi \urcorner}).$$

$$L2 : P \vdash \text{Bew}(\Delta_{\ulcorner \varphi \urcorner}) \wedge \text{Bew}(\Delta_{\ulcorner \varphi \rightarrow \psi \urcorner}) \rightarrow \text{Bew}(\Delta_{\ulcorner \varphi \urcorner}).$$

$$L3 : P \vdash \text{Bew}(\Delta_{\ulcorner \varphi \urcorner}) \rightarrow \text{Bew}(\Delta_{\ulcorner \text{Bew}(\Delta_{\ulcorner \varphi \urcorner}) \urcorner}).$$

*Beweis:*

L1: Gelte  $P \vdash \varphi$ . Letzteres heißt anders geschrieben  $\mathfrak{N} \models \text{Bew}(\Delta_{\ulcorner \varphi \urcorner})$ . Da die Formel  $\text{Bew}(\Delta_{\ulcorner \varphi \urcorner})$  eine  $\Sigma_1$ -Formel ist und  $P$  wahre  $\Sigma_1$ -Formeln beweist, gilt  $P \vdash \text{Bew}(\Delta_{\ulcorner \varphi \urcorner})$ .

L2: Sei  $\text{Bew}(\Delta_{\ulcorner \varphi \urcorner})$  durch  $s$  und  $m$  bezeugt und sei  $\text{Bew}(\Delta_{\ulcorner \varphi \rightarrow \psi \urcorner})$  durch  $t$  und  $n$  bezeugt gemäß Gleichung (4.6.2). Sei  $u$  so gewählt, dass

$$\beta'(u, i) = \begin{cases} \beta'(s, i), & \text{falls } i \leq m, \\ \beta'(t, i - m - 1), & \text{falls } m + 1 \leq i \leq m + n + 1, \\ \ulcorner \psi \urcorner, & \text{falls } i = m + n + 2. \end{cases}$$

Dann bezeugt  $u$  und  $m + n + 3$  die Relation  $\text{Bew}(\Delta_{\ulcorner \psi \urcorner})$ .

L3: Wir wenden das folgende Lemma auf die  $\Sigma_1$ -Formel an  $\text{Bew}(\Delta_{\ulcorner \varphi \urcorner})$  an. □

**Lemma 4.6.7.** Für jede  $\Sigma_1$ -Formel  $\psi$  gilt

$$P \vdash \psi \rightarrow \text{Bew}(\Delta_{\ulcorner \psi \urcorner}).$$

*Beweis:* Wir können  $s$  mit  $\beta'(s, 0) = \ulcorner \psi \urcorner$  wählen, denn  $W_1(\Delta_{\ulcorner \psi \urcorner})$  gilt. Sei  $f$  die Gödelnummer einer  $\Sigma_1$ -Formel. Weil  $\text{Auss}(f)$  eine  $\Sigma_1$ -Formel ist, folgt  $P \vdash \text{Auss}(\Delta_{\ulcorner \psi \urcorner})$ . Wir argumentieren in  $P$ . Aus Lemma 4.6.3 erhalten wir, dass  $P$  die Formel  $\psi \leftrightarrow W_1(\Delta_{\ulcorner \psi \urcorner})$  beweist. Wir wählen  $s$ , so dass  $\beta'(s, 0) = \ulcorner \psi \urcorner$ . Dann gilt  $B(s, 1)$ .  $P$  beweist  $\text{Auss}(\Delta_{\ulcorner \psi \urcorner}) \wedge B(s, 1) \rightarrow \text{Bew}(\Delta_{\ulcorner \psi \urcorner})$ . □

**Satz 4.6.8** (Satz von Löb). Für jede  $L_N$ -Aussage  $\psi$  ist

$$P \vdash \text{Bew}(\Delta_{\ulcorner \text{Bew}(\Delta_{\ulcorner \psi \urcorner}) \rightarrow \psi \urcorner}) \rightarrow \text{Bew}(\Delta_{\ulcorner \psi \urcorner}).$$

*Beweis:* Sei  $\Box\varphi := \text{Bew}(\Delta_{\ulcorner \varphi \urcorner})$ . L1 and L2 liefern

$$P \vdash \varphi \rightarrow \psi \Rightarrow P \vdash \Box\varphi \rightarrow \Box\psi \tag{4.6.3}$$

erneut mit L1 and L2

$$P \vdash \Box(\varphi \wedge \psi) \Leftrightarrow P \vdash \Box\varphi \wedge \Box\psi. \tag{4.6.4}$$

Nun wählen wir  $\varphi$  mithilfe des Fixpunktsatzes Satz 2.4.4

$$P \vdash \varphi \leftrightarrow (\Box\varphi \rightarrow \psi). \quad (4.6.5)$$

Daraus folgt mit einer Implikation wie in Gleichung (4.6.3), die in beide Richtungen angewandt wird,

$$P \vdash \Box\varphi \leftrightarrow \Box(\Box\varphi \rightarrow \psi). \quad (4.6.6)$$

Und schließlich mit L3

$$P \vdash \Box\varphi \rightarrow \Box\Box\varphi. \quad (4.6.7)$$

Aus Gleichungen (4.6.3) und (4.6.4)

$$P \vdash (\Box(\Box\varphi \rightarrow \psi) \wedge \Box\Box\varphi) \rightarrow \Box\psi. \quad (4.6.8)$$

Aus den Gleichungen (4.6.7), (4.6.8), (4.6.6) ergibt sich mit der Modus ponens Regel

$$P \vdash \Box\varphi \rightarrow \Box\psi, \quad (4.6.9)$$

und daraus folgt nach Wahl des Fixpunktes  $\varphi$  gemäß (4.6.5) und nochmaliger Anwendung des Modus ponens auf (4.6.9)

$$P \vdash ((\Box\psi \rightarrow \psi) \rightarrow (\Box\varphi \rightarrow \psi)) \quad (4.6.10)$$

also nach Gleichung (4.6.5)

$$P \vdash (\Box\psi \rightarrow \psi) \rightarrow \varphi. \quad (4.6.11)$$

Weiter folgt mit L1 and L2

$$P \vdash \Box(\Box\psi \rightarrow \psi) \rightarrow \Box\varphi, \quad (4.6.12)$$

und schließlich mit Eq. (4.6.9)

$$P \vdash \Box(\Box\psi \rightarrow \psi) \rightarrow \Box\psi. \quad (4.6.13)$$

□

Da der Beweis des Satzes  $\text{Bew}(\Delta_{\text{Bew}(\Delta_{\psi^*}) \rightarrow \psi^*}) \rightarrow \text{Bew}(\Delta_{\psi^*})$  natürlich statt in  $P$  erst recht in  $\mathfrak{N}$  geführt werden kann, erhalten wir das folgende Korollar.

**Folgerung 4.6.9.** *Es gilt für jede  $L_N$ -Formel  $\psi$*

$$(P \vdash \text{Bew}(\Delta_{\psi^*}) \rightarrow \psi) \Rightarrow P \vdash \psi.$$

**Definition 4.6.10** ( $\text{Con}_P$ ). Wir definieren  $\text{Con}_P$  als  $\neg \text{Bew}(\Delta_{\ulcorner 0=1 \urcorner})$ .

**Folgerung 4.6.11.** *Der zweite Gödel'sche Unvollständigkeitssatz für  $P$ . Es gilt*

$$(P \vdash \neg \text{Bew}(\Delta_{\ulcorner 0=1 \urcorner})) \Rightarrow P \vdash 0 = 1.$$

*In anderen Worten: Falls  $P$  widerspruchsfrei ist, so  $P \not\vdash \text{Con}_P$ . Da ZFC beweist, dass  $P$  ein Modell hat, also widerspruchsfrei ist, kann man auch in ZFC schreiben*

$$P \not\vdash \text{Con}_P$$

*Beweis:* Wir wenden die erste Folgerung an auf  $\psi = 0 = 1$ . Die Voraussetzung der ersten Folgerung folgt aus der Annahme  $P \vdash \neg \text{Bew}(\Delta_{\ulcorner 0=1 \urcorner})$ . □



# Literaturverzeichnis

- [1] Heinz-Dieter Ebbinghaus, Jörg Flum, and Wolfgang Thomas. *Einführung in die Mathematische Logik*. Hochschultaschenbuch, 4 edition, 1996.
- [2] Herbert Enderton. *A Mathematical Introduction to Logic*. Academic Press, 3 edition, 2001.
- [3] Thomas Jech. *Set Theory. The Third Millenium Edition, revised and expanded*. Springer, 2003.
- [4] Kenneth Kunen. *Set theory*, volume 34 of *Studies in Logic (London)*. College Publications, London, 2nd edition, 2013.
- [5] Joseph Shoenfield. *Mathematical Logic, Reprint of the 1973 second printing*. Association for Symbolic Logic, Urbana, IL; A K Peters, Ltd., Natick, MA, 2001.
- [6] Martin Ziegler. *Mathematische Logik, 2. Auflage*. Mathematik kompakt. Birkhäuser, 2017.





# Stichwortverzeichnis

- A-Belegung, 11
- L-Beweis, 22
- L-Satz, L-Aussage, 13
- L-Struktur, 8
- L-Term, 9
- L-Theorie, 13
- $P$ , 92
- $Q^*$ , 86
- $T \models \varphi$ , 20
- $T \vdash \varphi$ , 20
- $V$ , 44
- $V_{\text{fund}}$ , 44
- $\mathcal{A}^*$ , 60
- $\text{Con}_P$ , 101
- $\text{Con}_{\text{ZFC}}$ , 57
- $\Delta_1^P$ , 95
- $\Sigma_1$ -Formeln, 84
- $\Sigma_1^P$ , 93
- $\aleph_\alpha$ , 52
- \*-rekursiv, 79
- $\equiv_n$ , 30
- $\exists$ -Einführungsregel, 18
- $\exists$ -Quantorenaxiom, 17
- $\forall$ -Einführungsregel, 21
- $\forall$ -Quantorenaxiome, 21
- $\omega$ , 42
- tcl, 45
- $\text{Mod}_T$ , 13
- T1 to T3, 9
- B1 to B6, 20
- L1 to L3, 56
- L1 to L3 (Löb-Axiome), 99
- Q1 to Q6, 86
- $Q_1^*$  to  $Q_3^*$ , 86
- R0 to R3, 60
- allgemeingültig, 16
- allgemeingültige aussagenlogische Formel, 17
- Allklasse, 44
- Alphabeth, 60
- Anfangsstück, 9
- arithmetisch, 83
- Atom (Boole'sche Algebra), 19
- atomlos, 19
- Aussagenlogische Formel, 16
- Aussonderungsschema, 34
- Auswahlaxiom, 36
- Axiome der Gleichheit, 17
- back and forth, 31
- Beweisbarkeitsprädikat, 55
- Boole'sche Algebra, 18
- CH, 52
- Church'sche These, 71
- Cobham Theorie, 86
- deduktiv abgeschlossen, 27
- deduktiver Abschluss, 78
- Definitorische Erweiterung, 38

- Der Hilbert-Kalkül, 20  
 Die Löschmaschine  $\mathcal{L}^r$ , 62  
 effektiv axiomatisierbar, 77  
 Ehrenfeucht-Fraïssé-Spiel, 30  
 Einbettung, 19  
 elementar äquivalent, 14  
 elementare Klasse, 13  
 endliche Menge, 41  
 Ersetzungsschema, 36  
 Erster Gödel'scher  
     Unvollständigkeitssatz für  
      $\text{Th}(\mathfrak{N})$ , 85  
 Erster Gödel'scher  
     Unvollständigkeitssatz für ZFC,  
     58  
 erststufig axiomatisierbar, 13  
 erzeugte Substruktur, 30  
 Extensionalitätsaxiom, 34  
 Fixpunktsatz, 54, 91  
 freie Ultrafilter, 19  
 freie Variable, 12  
 fundierte Allklasse, 44  
 fundierte Relation, 41  
 Fundierungsaxiom, 36  
 Funktionssymbol, 7  
 Gödel'scher Vollständigkeitssatz, 20  
 gebundene Variable, 12  
 Gödel'sche  $\beta$ -Funktion, 80  
 Gödel'scher Satz für die Erfüllbarkeit, 23  
 Gödelnummer, 54, 68  
 Halbordnung, 48  
 Hauptultrafilter, 19  
 Henkin-Theorie, 24  
 Hin- und Her-System, 30  
 Hutformel von Kreisel, 16  
 immer falsche Formel, 57  
 Induktion über eine fundierte,  
     mengenähnliche Relation, 45  
 Induktions-Axiom für  $\varphi$ , 92  
 Induktionssatz für On, 43  
 Induktionsschema, 92  
 Isomorphe  $L$ -Strukturen, 8  
 Kardinalzahl, 50  
 Kardinalzahlen  
     gleichmächtig, 50  
     schmächtiger als, 50  
 kartesisches Produkt, 37  
 Kleene-Normalform, 71  
 Kleene-Prädikat, 71  
 Koinzidenzlemma, 12  
 Kompaktheitssatz, 29  
 Konfiguration, 62  
 konsistent, 23  
 Konstantensymbol, 7  
 Kontinuumshypothese, 52  
 Korrektheitssatz, 20  
 Kuratowski-Paar, 37  
 Limes-Ordinalzahl, 44  
 Lindenbaum-Algebra, 19  
 Löb-Axiome, 56  
 maximales Element, 48  
 Menge  
     abzählbar, 51  
     endlich, 51  
 Mengentheoretische natürliche Zahlen,  
     40  
 Mengenähnlich, 45  
 Modell, 13  
 Modellklasse, 13  
 Modus ponens, 18  
 Mächtigkeit, 50  
 Nachfolger, 43  
 Nachfolgerkonfiguration, 62  
 Natürliche Zahl, 41  
 NBG, 39  
 Operation, 44

- Ordinale Addition, 49
- Ordinale Exponentiation, 49
- Ordinale Multiplikation, 49
- Ordinalzahl, 41
  
- Paarmengenaxiom, 35
- Paradoxon von Burali-Forti, 43
- partielle rekursive Funktion, 72
- partieller Isomorphismus, 31
- Peano-Axiome, 92
- Peanoarithmetik, 92
- Potenzmengenalgebra, 18
- Potenzmengenaxiom, 35
- primitiv rekursiv, 60
- primitiv rekursive Relation, 66
  
- Quantorenrang, 30
  
- Registermaschine, 61
- Registermaschinen-Befehle, 61
- registermaschinen-berechenbar, 62
- Rekursionssatz für On, 44
- rekursiv, 66
- rekursiv aufzählbar, 72
- Relationssymbol, 7
- repräsentieren (Relation), 90
- Repräsentieren, 88
  
- Satz von Cantor, 51
- Satz von Church, 88
- Satz von Ehrenfeucht-Fraïssé, 31
- Satz von Halpern-Lévy, 48
- Satz von Hessenberg, 53
- Satz von Löb, 99
- Satz von Löwenheim und Skolem, 30
- Satz von Russell, 33
- Signatur, 7
- Sprache, 7
  
- Standardform, 64
- Stone'scher Darstellungssatz, 18
- Stone-Algebra, 19
- Substitutionslemma, 14
- Symbolmenge, 7
  
- Tarskis Satz über die  
    Wahrheitsdefinition, 55
- Tautologie, 17
- transitive Klasse, 45
- transitive Menge, 40
- transitive Relation, 45
- transitiver Abschluss einer Relation, 45
  
- Ultrafilter, 18
- Ultrafiltertheorem, 48
- Unendlichkeitsaxiom, 36
- universelle rekursiv aufzählbare Relation,  
    73
  
- Vereinigungsaxiom, 35
- Vollständige Induktion in  $\omega$ , 42
- vollständige Theorie, 24
- von Neumann'sche natürliche Zahl, 40
- von Neumann-Hierarchie, 44
  
- Wahrheitsfunktion, 16
- widerspruchsfrei, 23
- widerspruchsvoll, 23
- Wohlordnung, 41
  
- ZFC, 34
- Zorn'sches Lemma, 48
- Zweiter Gödel'scher  
    Unvollständigkeitssatz für ZFC,  
    57
- Zweiter Unvollständigkeitssatz für  $P$ , 101