Vorlesung über Mathematische Logik[1]

Martin Ziegler

Freiburg
SS 1997, SS 2000, WS 2003, SS 2007

[1] Version 7.10 (22.7.2008) Subversion: 69, 2008-07-22

Inhaltsverzeichnis

Kapitel 1

Prädikatenkalkül

1 Strukturen und Formeln

Eine *Struktur* ist eine nicht–leere Menge mit ausgezeichneten Elementen, Operationen und Relationen. Zum Beispiel

ein Ring:	$(R, 0, 1, +, -, \cdot)$
eine Gruppe:	$(G, e, \circ, ^{-1})$
die reellen Zahlen	$(\mathbb{R}, 0, 1, +, -, \cdot, <)$
die natürlichen Zahlen	$\mathfrak{N} = (\mathbb{N}, 0, \mathrm{S}, +, \cdot, <)$
	(S ist die Nachfolgeroperation $x \mapsto x + 1$.)

In diesen Beispielen sind die Relationen zweistellig und die Operationen ein– oder zweistellig. Im Allgemeinen sind beliebige positive Stelligkeiten erlaubt. Nicht alle Gegenstände der Mathematik sind Strukturen. Zum Beispiel ist die Klasse aller Gruppen mit der Isomorphie als zweistelliger Relation keine Struktur, weil der Grundbereich — die Klasse aller Gruppen — zu groß ist. Eine topologischer Raum ist keine Struktur, auf ihm ist vielmehr eine Menge von (offenen) Teilmengen ausgezeichnet.

Werden wir etwas präziser:

Definition *Eine Struktur ist ein Paar $\mathfrak{A} = (A, J)$, wobei A eine nicht–leere Menge und J eine Familie von Elementen aus A und Operationen und Relationen auf A ist.*

Die Struktur $\mathfrak{Q} = (\mathbb{Q}, 0, 1, +, -, \cdot)$ des Körpers der rationalen Zahlen müssen wir jetzt schreiben als $(\mathbb{Q}, (Z_i)_{i<5})$, wobei $Z_0 = 0$, $Z_1 = 1$, $Z_2 = +$, $Z_3 = -$, $Z_4 = \cdot$. Wenn eine Frage, wie „ist $(\mathbb{Q}, 0, 1, \cdot, -, +)$ ein Körper“ sinnvoll sein soll, muß man festlegen, welche Operation die Addition und welche die Multiplikation sein soll. Der Ausgangspunkt ist also eine *Sprache*:

Definition *Eine Sprache ist eine Menge von Konstantenzeichen*[1]*, Funktionszeichen und Relationszeichen. Funktionszeichen und Relationszeichen haben eine*

[1] Konstantenzeichen nennen wir auch einfach *Konstanten*.

(positive) Stelligkeit.

Gelegentlich nennt man Relationszeichen, aber auch Relationen, *Prädikate*.

Eine Liste von Beispielen:

$L_\emptyset$	$= \emptyset$	Die leere Sprache
L_R	$= \{\underline{0}, \underline{1}, +, -, \cdot\}$	Die Ring–Sprache.
L_G	$= \{\underline{e}, \circ, ^{-1}\}$	Die Gruppen–Sprache.
L_O	$= \{<\}$	Die Ordnungs–Sprache.
L_{AK}	$= L_R \cup L_O$	Die Angeordnete–Körper–Sprache.
L_N	$= \{\underline{0}, \mathrm{S}, +, \cdot, <\}$	Die Sprache der natürlichen Zahlen.
L_{Me}	$= \{\epsilon\}$	Die Mengenlehre-Sprache.

Dabei sind

Konstanten:	$\underline{0}$, $\underline{1}$, $\underline{e}$
einstellige Funktionszeichen:	$-$, $^{-1}$, S
zweistellige Funktionszeichen:	$+$, $\cdot$, $\circ$
zweistellige Relationszeichen:	$<$, ϵ .

Definition *Sei L eine Sprache. Eine L–*Struktur *ist ein Paar*

$$\mathfrak{A} = (A, (Z^{\mathfrak{A}})_{Z \in L}),$$

wobei

A	*eine nicht–leere Menge (die* Grundmenge von $\mathfrak{A}$ *) ist,*
$Z^{\mathfrak{A}} \in A$,	*wenn Z eine Konstante ist,*
$Z^{\mathfrak{A}} : A^n \longrightarrow A$,	*wenn Z ein n–stelliges Funktionszeichen ist und*
$Z^{\mathfrak{A}} \subset A^n$,	*wenn Z ein n–stelliges Relationszeichen ist.*

Definition *Zwei L–Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ heißen* isomorph, $\mathfrak{A} \cong \mathfrak{B}$, *wenn es einen* Isomorphismus $F : \mathfrak{A} \longrightarrow \mathfrak{B}$ *gibt, eine Bijektion $F : A \longrightarrow B$, die mit den Interpretationen der Zeichen aus L kommutiert:*

$F(Z^{\mathfrak{A}})$	$=$	$Z^{\mathfrak{B}}$	*(Z eine Konstante aus L)*
$F(Z^{\mathfrak{A}}(a_1, \ldots, a_n))$	$=$	$Z^{\mathfrak{B}}(F(a_1), \ldots, F(a_n))$	*(Z ein n–stelliges Funktionszeichen aus L, $a_1, \ldots, a_n \in A$)*
$R^{\mathfrak{A}}(a_1, \ldots, a_n)$	$\Leftrightarrow$	$R^{\mathfrak{B}}(F(a_1), \ldots, F(a_n))$	*(Z ein n–stelliges Relationszeichen aus L, $a_1, \ldots, a_n \in A$)*

Das Inverse eines Isomorphismus und die Verknüpfung von zwei Isomorphismen ist wieder ein Isomorphismus. Daraus folgt, daß $\cong$ eine Äquivalenzrelation ist.

Wir fixieren ein Folge von Variablen $v_0, v_1, \ldots$.

Definition *Ein L–*Term *ist eine Zeichenfolge, die nach den folgenden Regeln gebildet ist:*

T1 *Jede Variable ist ein L–Term.*

T2 *Jede Konstante aus L ist ein L–Term.*

T3 *Wenn f ein n–stelliges Funktionszeichen aus L ist und wenn $t_1, \ldots, t_n$ L–Terme sind, dann ist auch $ft_1 \ldots t_n$ ein L–Term.*

Um Terme besser lesbar zu machen, schreiben wir häufig $f(t_1, \ldots, t_n)$ statt $ft_1 \ldots t_n$. Wenn f einstellig ist, auch $t_1 f$, wenn f zweistellig ist, auch $t_1 f t_2$. Zum Beispiel steht $(x + y) \cdot (z + w)$ für $\cdot + xy + zw$ und $(x \circ y)^{-1}$ für ${}^{-1} \circ xy$.

Das folgende Lemma zeigt, weshalb wir auf Klammern verzichten können. Übrigens würde der Gebrauch von Klammern den Beweis nicht einfacher machen.

Lemma 1.1 (Eindeutige Lesbarkeit von Termen) *Für jeden L–Term t tritt genau einer der folgenden drei Fälle ein:*

1. *t ist eine Variable,*
2. *t ist eine Konstante,*
3. *$t = ft_1 \ldots t_n$, wobei f ein n–stelliges Funktionszeichen und $t_1, \ldots, t_n$ L–Terme sind.*

Im letzten Fall sind f und $t_1, \ldots, t_n$ eindeutig bestimmt.

Beweis:

Daß genau einer der drei Fälle eintritt ist klar. Zu zeigen ist die Eindeutigkeit der t_i. Wenn $t = es_1 \ldots s_m$ für ein m–stelliges Funktionszeichen e und Terme s_i, ist klar, daß $e = f$ und $m = n$. Daß $s_i = t_i$, folgt aus dem nächsten Hilfssatz.[2]
□

Hilfssatz
Kein L–Term ist echtes Anfangsstück eines anderen L–Terms.

Beweis:

Sei s Anfangsstück von t. Wir zeigen $s = t$ durch Induktion über die Länge von t. Wenn t eine Variable oder eine Konstante ist, ist die Behauptung klar. Sonst ist $s = fs_1 \ldots s_n$ und $t = ft_1 \ldots t_n$ für ein n–stelliges Funktionszeichen f. Wenn $s \neq t$, gibt es einen kleinsten Index i mit $s_i \neq t_i$. s_i ist dann echtes Anfangsstück von t_i, oder umgekehrt, was nach Induktionsvoraussetzung unmöglich ist. □

L–Formeln sind Zeichenreihen, die aus den Zeichen aus L, den Klammern (und) als Hilfszeichen und den folgenden *logischen* Zeichen gebildet ist:

[2] Oder vielmehr aus seinem Beweis.

Variable	$v_0, v_1, \ldots$
Gleichheitszeichen	$\doteq$
Junktoren	$\neg$ (Negation), $\wedge$ (Konjunktion)
Existenzquantor	$\exists$

Man liest $\doteq$ als „gleich“, $\neg$ als „nicht“, $\wedge$ als „und“ und $\exists$ als „es gibt ein“.

Definition *Eine L–Formel ist*

F1 $t_1 \doteq t_2$ *, wenn t_1, t_2 L–Terme sind,*

F2 $Rt_1 \ldots, t_n$ *, wenn R ein n–stelliges Relationszeichen aus L und $t_1, \ldots, t_n$ L–Terme sind,*

F3 $\neg\,\psi$ *, wenn ψ eine L–Formel ist,*

F4 $(\psi_1 \wedge \psi_2)$ *,wenn ψ_1 und ψ_2 L–Formeln sind,*

F5 $\exists x\ \psi$ *,wenn ψ eine L–Formel und x eine Variable ist.*

Formeln der Form **F1** und **F2** heißen *Primformeln*[3].

Wir verwenden folgende Abkürzungen:

$$\begin{array}{rcl}
(\psi_1 \vee \psi_2) & = & \neg\,(\neg\,\psi_1 \wedge \neg\,\psi_2) \\
(\psi_1 \rightarrow \psi_2) & = & \neg\,(\psi_1 \wedge \neg\,\psi_2) \\
(\psi_1 \leftrightarrow \psi_2) & = & ((\psi_1 \rightarrow \psi_2) \wedge (\psi_2 \rightarrow \psi_1)) \\
\forall x\ \psi & = & \neg\,\exists x \neg\,\psi \\
(\psi_0 \wedge \cdots \wedge \psi_n) & = & \underbrace{(\ldots(}_{n\text{ -mal}}\ \psi_0 \wedge \psi_1) \wedge \ldots \psi_n) \\
(\psi_0 \vee \cdots \vee \psi_n) & = & \underbrace{(\ldots(}_{n\text{ -mal}}\ \psi_0 \vee \psi_1) \vee \ldots \psi_n)
\end{array}$$

Die Disjunktion $\vee$ liest man als „oder“, die Implikation $\rightarrow$ als „impliziert“, die Äquivalenz $\leftrightarrow$ als „genau dann , wenn“ und den Allquantor $\forall$ als „für alle“.

Statt Rt_1t_2 schreiben wir auch t_1Rt_2 und statt $\exists x_1 \ldots \exists x_n$ schreiben wir $\exists x_1 \ldots x_n$ (ebenso für $\forall$). Zur besseren Lesbarkeit der Formeln gebrauchen wir überflüssige Klammern. Wir lassen auch Klammern weg und lesen die Formeln gemäß der *Bindungsstärke* der logischen Zeichen:

Höchste Bindungsstärke:	$\neg\ \exists\ \forall$
	$\wedge$
	$\vee$
Niedrigste Bindungsstärke:	$\rightarrow\ \leftrightarrow$

Zum Beispiel steht $\neg\,\phi \wedge \psi \rightarrow \chi$ für

$$((\neg\,\phi \wedge \psi) \rightarrow \chi) = \neg\,((\neg\,\phi \wedge \psi) \wedge \neg\,\chi).$$

[3] Man nennt Primformeln auch *atomar*.

Als Beispiel schreiben wir in L_R die Körperaxiome auf. Beachte, daß das erste Axiom zum Beispiel voll ausgeschrieben

$$\neg \exists v_0 \neg \neg \exists v_1 \neg + v_0 v_1 \doteq + v_1 v_0$$

ist. x, y, z stehen für die Variablen v_0, v_1, v_2.

Die Körperaxiome.

1. $\forall x, y \;\; x + y \doteq y + x$
2. $\forall x \;\; x + \underline{0} \doteq x$
3. $\forall x \;\; x + (-x) \doteq \underline{0}$
4. $\forall x, y, z \;\; (x + y) + z \doteq x + (y + z)$
5. $\forall x, y \;\; x \cdot y \doteq y \cdot x$
6. $\forall x \;\; x \cdot \underline{1} \doteq x$
7. $\forall x, y, z \;\; (x \cdot y) \cdot z \doteq x \cdot (y \cdot z)$
8. $\forall x, y, z \;\; x \cdot (y + z) \doteq (x \cdot y) + (x \cdot z)$
9. $\forall x \;\; (\neg x \doteq \underline{0} \rightarrow \exists y \; x \cdot y \doteq \underline{1})$
10. $\neg \underline{0} \doteq \underline{1}$

Die ersten acht Axiome drücken aus, daß ein Körper insbesondere ein kommutativer Ring mit Einselement ist. Die ersten vier Axiome sagen, daß einem Ring eine additive geschriebene abelsche Gruppe zugrunde liegt.

Lemma 1.2 *Für jede L–Formel ϕ tritt genau einer der folgenden Fälle ein.*

1. $\phi = t_1 \doteq t_2$	*für L–Terme t_1, t_2*
2. $\phi = R t_1 \ldots t_n$	*für ein n–stelliges Relationszeichen R aus L und L–Terme $t_1, \ldots, t_n$*
3. $\phi = \neg \psi$	*für eine L–Formel ψ*
4. $\phi = (\psi_1 \wedge \psi_2)$	*für L–Formeln ψ_1 und ψ_2*
5. $\phi = \exists x \; \psi$	*für eine L–Formel ψ und eine Variable x*

In jedem der Fälle sind die Terme t_i, das Relationszeichen R, die Formeln ψ, ψ_1, ψ_2 und die Variable x jeweils eindeutig bestimmt.

Beweis:

Daß genau einer der fünf Fälle auftritt ist klar. Sie treten ein je nachdem, ob das erste Zeichen von ϕ eine Variable, Konstante oder Funktionszeichen ist (Fall 1) oder ein Relationszeichen (Fall 2) oder ein Negationszeichen (Fall 3) oder eine aufgehende Klammer (Fall 4) oder ein Existenzquantor (Fall 5). Wir müssen noch in die Eindeutigkeit der Zerlegung in jedem Fall zeigen:

Fall 1: Klar, weil in ϕ nur ein Gleichheitszeichen vorkommt.

Fall 2: R ist als das erste Zeichen von ϕ eindeutig bestimmt. Die Eindeutigkeit der t_i folgt aus dem Hilfssatz im Beweis von 1.1.

Fall 3: Klar.

Fall 5: Klar.

Fall 4: Wenn $(\psi_1 \wedge \psi_2) = (\psi_1' \wedge \psi_2')$, ist ψ_1 Anfangsstück von ψ_1' oder umgekehrt. Aus dem nächsten Hilfsatz folgt $\psi_1 = \psi_1'$ und also auch $\psi_2 = \psi_2'$. □

Hilfssatz *Keine L–Formel ist echtes Anfangsstück einer anderen L–Formel.*

Beweis:

ϕ und ϕ' seien L–Formeln und ϕ ein echtes Anfangsstück von ϕ'. Wir zeigen durch Induktion über die Länge von ϕ', daß das unmöglich ist. Es ist klar, daß für ϕ und ϕ' derselbe Fall auftritt. Wir gehen alle fünf Fälle durch: Wenn $\phi = t_1 \doteq t_2$ und $\phi' = t_1' \doteq t_2'$, ist t_2 ein echtes Anfangsstück von t_2', was nach dem Hilfssatz im Beweis von 1.1 nicht geht. Wenn $\phi = Rt_1 \ldots t_n$ und $\phi' = Rt_1' \ldots t_n'$, gibt es ein kleinstes i mit $t_i \neq t_i'$. t_i ist dann ein echtes Anfangsstück von t_i' oder umgekehrt: unmöglich. Wenn $\phi = \neg\psi$ und $\phi' = \neg\psi'$, ist ψ echtes Anfangsstück von ψ', das ist unmöglich nach Induktionsannahme. $\phi = \exists x \psi$ ist aus demselben Grund unmöglich. Wenn $\phi = (\psi_1 \wedge \psi_2)$ und $\phi' = (\psi_1' \wedge \psi_2')$, ist ψ_1 echtes Anfangsstück von ψ_1' oder umgekehrt. □

2 Semantik

Ein L-Term t hat einen Wert in einer L–Struktur, wenn man die Variablen von t durch Elemente von A belegt.

Definition *Sei $\mathfrak{A}$ eine L–Struktur. Eine* Belegung *ist eine Funktion*

$$\beta : \{v_0, v_1 \ldots\} \longrightarrow A$$

von der Menge der Variablen in die Grundmenge von $\mathfrak{A}$.

Diese Belegung der Variablen läßt sich auf alle Terme fortsetzen. Die folgende rekursive Definition ist sinnvoll wegen 1.1.

Definition *Für L–Terme t, L–Strukturen $\mathfrak{A}$ und Belegungen β definieren wir $t^{\mathfrak{A}}[\beta]$ durch*

$$\begin{array}{lrcl} (1) & v_i^{\mathfrak{A}}[\beta] & = & \beta(v_i) \\ (2) & c^{\mathfrak{A}}[\beta] & = & c^{\mathfrak{A}} \\ (3) & ft_1 \ldots t_n^{\mathfrak{A}}[\beta] & = & f^{\mathfrak{A}}(t_1^{\mathfrak{A}}[\beta], \ldots, t_n^{\mathfrak{A}}[\beta]). \end{array}$$

Sei $\mathfrak{Q}$ der Körper der rationalen Zahlen und $t = \cdot v_0 + v_1 v_2$. Wenn $\beta(v_i) = i+2$, ist $t^{\mathfrak{Q}}[\beta] = 2(3+4) = 14$.

Das folgende Lemma ist klar.

Lemma 2.1 *Wenn die Belegungen β und γ auf den Variablen, die in t vorkommen übereinstimmen, ist $t^{\mathfrak{A}}[\beta] = t^{\mathfrak{A}}[\gamma]$.* □

Wenn wir einen Term in der Form $t(x_1, \ldots, x_n)$ schreiben, meinen wir:

1. daß die x_i paarweise verschiedene Variable sind,
2. daß in t nur Variable aus $\{x_1, \ldots, x_n\}$ vorkommen.

Wenn dann $a_1, \ldots, a_n$ Elemente der Struktur $\mathfrak{A}$ sind, ist wegen 2.1 $t^{\mathfrak{A}}[a_1, \ldots, a_n]$ durch $t^{\mathfrak{A}}[\beta]$ für eine Belegung β mit $\beta(x_i) = a_i$ wohldefiniert.

Die folgende rekursive Definition der Semantik ist sinnvoll, wegen 1.2.

Definition *Sei $\mathfrak{A}$ eine L–Struktur. Wir definieren für Belegungen β und L–Formeln ϕ die Relation*

$$\mathfrak{A} \models \phi[\beta]$$

— ϕ trifft in $\mathfrak{A}$ auf β zu— *durch Rekursion über den Aufbau von ϕ:*

$$\begin{array}{lrcl} (1) & \mathfrak{A} \models t_1 \doteq t_2\,[\beta] & \Leftrightarrow & t_1^{\mathfrak{A}}[\beta] = t_2^{\mathfrak{A}}[\beta] \\ (2) & \mathfrak{A} \models Rt_1 \ldots t_n\,[\beta] & \Leftrightarrow & R^{\mathfrak{A}}(t_1^{\mathfrak{A}}[\beta], \ldots, t_n^{\mathfrak{A}}[\beta]) \end{array}$$

(3)	$\mathfrak{A} \models \neg\,\psi\,[\beta]$	$\Leftrightarrow$	$\mathfrak{A} \not\models \psi\,[\beta]$
(4)	$\mathfrak{A} \models (\psi_1 \wedge \psi_2)\,[\beta]$	$\Leftrightarrow$	$\mathfrak{A} \models \psi_1\,[\beta]$ *und* $\mathfrak{A} \models \psi_2\,[\beta]$
(5)	$\mathfrak{A} \models \exists x\psi\,[\beta]$	$\Leftrightarrow$	*es gibt ein* $a \in A$ *mit* $\mathfrak{A} \models \psi\,[\beta\frac{a}{x}]$.

Dabei ist $\beta\frac{a}{x}(y) = \begin{cases} \beta(y) & ,\textit{wenn} \quad y \neq x \\ a & ,\textit{wenn} \quad y = x. \end{cases}$

Es ist klar, daß unsere Abkürzungen die intendierte Interpretation haben. Also, daß z.B.

$$\mathfrak{A} \models (\psi_1 \rightarrow \psi_2)[\beta] \iff \text{wenn } \mathfrak{A} \models \psi_1[\beta], \text{ dann } \mathfrak{A} \models \psi_2[\beta].$$

Ob ϕ in $\mathfrak{A}$ auf β zutrifft, hängt nur von den freien Variablen von ϕ ab.

Definition *Die Variable x kommt* frei *in der Formel ϕ vor, wenn sie an einer Stelle vorkommt, die nicht im Wirkungsbereich eines Quantors $\exists x$ liegt. Präzis definiert durch Rekursion nach dem Aufbau von ϕ:*

(1)	x *frei in* $t_1 \doteq t_2$	$\Leftrightarrow$	x *kommt in* t_1 *oder in* t_2 *vor.*
(2)	x *frei in* $Rt_1 \ldots t_n$	$\Leftrightarrow$	x *kommt in einem der* t_i *vor.*
(3)	x *frei in* $\neg\,\psi$	$\Leftrightarrow$	x *frei in* ψ
(4)	x *frei in* $(\psi_1 \wedge \psi_2)$	$\Leftrightarrow$	x *frei in* ψ_1 *oder* x *frei in* ψ_2
(5)	x *frei in* $\exists y\,\psi$	$\Leftrightarrow$	$x \neq y$ *und* x *frei in* ψ

Zum Beispiel kommt in $\forall v_0(\exists v_1 R(v_0, v_1) \wedge P(v_1))$ die Variable v_0 nicht frei vor. v_1 kommt gebunden und frei vor.

Satz 2.2 *Wenn β und γ an allen Variablen, die frei in ϕ vorkommen, übereinstimmen, ist*

$$\mathfrak{A} \models \phi[\beta] \Leftrightarrow \mathfrak{A} \models \phi[\gamma].$$

Beweis:

durch Induktion über den Aufbau von ϕ: Wenn ϕ eine Primformel ist, folgt die Behauptung aus 2.1. Wenn ϕ eine Negation oder eine Konjunktion ist, ist der Induktionsschritt einfach. Sei also $\phi = \exists x\psi$. Wenn $\mathfrak{A} \models \phi[\beta]$, gibt es ein a mit $\mathfrak{A} \models \psi[\beta\frac{a}{x}]$. Außer x hat ψ die gleichen freien Variablen wie ϕ. Also ist nach Induktionsvoraussetzung $\mathfrak{A} \models \psi[\gamma\frac{a}{x}]$. Daraus folgt $\mathfrak{A} \models \phi[\gamma]$. $\square$

Wenn wir eine Formel in der Form $\phi(x_1, \ldots, x_n)$ schreiben, meinen wir:

1. daß die x_i paarweise verschiedene Variable sind,
2. daß in ϕ nur Variable aus $\{x_1, \ldots, x_n\}$ frei vorkommen.

Wenn dann $a_1, \ldots, a_n$ Elemente der Struktur $\mathfrak{A}$ sind, ist wegen 2.2 $\mathfrak{A} \models \phi[a_1, \ldots, a_n]$ durch $\mathfrak{A} \models \phi[\beta]$ für eine Belegung β mit $\beta(x_i) = a_i$ wohldefiniert.

Definition *Eine* Aussage ϕ *ist eine Formel ohne freie Variable. Wir schreiben* $\mathfrak{A} \models \phi$, *wenn* $\mathfrak{A} \models \phi[\beta]$ *für ein (alle)* β.

Sprechweisen:

- ϕ gilt in $\mathfrak{A}$.
- ϕ ist wahr in $\mathfrak{A}$.
- $\mathfrak{A}$ ist Modell von ϕ.

Zwei L–Strukturen $\mathfrak{A}$ und $\mathfrak{B}$ heißen *elementar äquivalent*, $\mathfrak{A} \equiv \mathfrak{B}$, wenn in ihnen die gleichen Aussagen gelten.

Übung *Isomorphe Strukturen sind elementar äquivalent.*

Sei x eine Variable und s ein Term.

$t\frac{s}{x}$ entsteht aus t durch Ersetzen aller Vorkommen von x durch s.

$\phi\frac{s}{x}$ entsteht aus ϕ durch Ersetzen aller freien Vorkommen von x durch s.

Man sieht leicht, daß $t\frac{s}{x}$ wieder ein Term und $\phi\frac{s}{x}$ eine Formel ist.

Die rekursive Definition von $\phi\frac{s}{x}$ ist

$$\begin{array}{lrcl}
(1) & (t_1 \doteq t_2)\dfrac{s}{x} & = & t_1\dfrac{s}{x} \doteq t_2\dfrac{s}{x} \\
(2) & (Rt_1 \ldots t_n)\dfrac{s}{x} & = & Rt_1\dfrac{s}{x} \ldots t_n\dfrac{s}{x} \\
(3) & (\neg\,\psi)\dfrac{s}{x} & = & \neg\,(\psi\dfrac{s}{x}) \\
(4) & (\psi_1 \wedge \psi_2)\dfrac{s}{x} & = & (\psi_1\dfrac{s}{x} \wedge \psi_2\dfrac{s}{x}) \\
(5) & (\exists y\psi)\dfrac{s}{x} & = & \exists y(\psi\dfrac{s}{x}),\ \text{wenn } x \neq y \\
 & & = & \exists y\psi,\ \text{wenn } x = y.
\end{array}$$

Definition *x heißt* frei für s in ϕ, *wenn kein freies Vorkommen von x in ϕ im Wirkungsbereich eines Quantors ist, der eine Variable von s bindet.*

Rekursive Definition: x ist frei für s in ϕ, wenn x nicht frei in ϕ ist **oder** wenn x frei in ϕ ist und einer der folgenden Fälle zutrifft

$$\begin{array}{lrcl}
(1) & \phi & = & t_1 \doteq t_n \\
(2) & \phi & = & Rt_1 \ldots t_n \\
(3) & \phi & = & \neg\,\psi \text{ und } x \text{ frei für } s \text{ in } \psi \\
(4) & \phi & = & (\psi_1 \wedge \psi_2) \text{ und } x \text{ frei für } s \text{ in } \psi_1 \text{ und } \psi_2, \\
(5) & \phi & = & \exists y\psi,\ x \text{ frei für } s \text{ in } \psi \text{ und } y \text{ kommt nicht in } s \text{ vor.}
\end{array}$$

Lemma 2.3 (Substitutionslemma) *Sei x eine Variable, s ein Term und β eine Belegung mit Werten in der Struktur $\mathfrak{A}$.*

1. *Für jeden Term t ist*

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

2. *Für jede Formel ϕ ist*

$$\mathfrak{A} \models \phi\frac{s}{x}[\beta] \iff \mathfrak{A} \models \phi[\beta\frac{s^{\mathfrak{A}}[\beta]}{x}],$$

   falls x frei für s in ϕ.

Beweis:

1. Induktion über den Aufbau von t: Wenn $t = x$, sind beide Seiten der behaupteten Gleichung gleich $s^{\mathfrak{A}}[\beta]$. Wenn t eine Variable verschieden von x ist, sind beide Seiten $\beta(t)$. Wenn t eine Konstante ist, steht $t^{\mathfrak{A}}$ links und rechts. Wenn t ein zusammengesetzter Term $ft_1 \ldots t_n$ ist, schließen wir induktiv:

$$(t\frac{s}{x})^{\mathfrak{A}}[\beta] = f^{\mathfrak{A}}\big((t_1\frac{s}{x})^{\mathfrak{A}}[\beta] \ldots\big) = f^{\mathfrak{A}}\big(t_1^{\mathfrak{A}}[\beta\frac{s^{\mathfrak{A}}[\beta]}{x}] \ldots\big) = t^{\mathfrak{A}}\big[\beta\frac{s^{\mathfrak{A}}[\beta]}{x}\big].$$

2. Wenn x nicht frei in ϕ vorkommt, ist $\phi\frac{s}{x} = \phi$ und die Behauptung folgt aus 2.2. Wir nehmen also an, daß x frei in ϕ vorkommt und schließen durch Induktion über den Aufbau von ϕ: Wenn ϕ eine Primformel ist, folgt die Behauptung aus dem ersten Teil. Wenn ϕ eine Negation oder eine Konjunktion ist, ist der Induktionsschritt trivial. Sei schließlich $\phi = \exists y\psi$. Dann ist y verschieden von x und kommt, weil x frei für s in ϕ ist, in s nicht vor. Für $b = s^{\mathfrak{A}}[\beta]$ haben wir dann

$$\begin{array}{rcll}
\mathfrak{A} \models \phi\frac{s}{x}[\beta] & \Leftrightarrow & \mathfrak{A} \models \psi\frac{s}{x}[\beta\frac{a}{y}] & \text{für ein } a \\
& \Leftrightarrow & \mathfrak{A} \models \psi\big[\beta\frac{a}{y}\frac{s^{\mathfrak{A}}[\beta\frac{a}{y}]}{x}\big] & \text{für ein } a \quad \text{(Induktionsvoraussetzung)} \\
& \Leftrightarrow & \mathfrak{A} \models \psi[\beta\frac{a}{y}\frac{b}{x}] & \text{für ein } a \quad (\text{weil } b = s^{\mathfrak{A}}[\beta\frac{a}{y}]) \\
& \Leftrightarrow & \mathfrak{A} \models \psi[\beta\frac{b}{x}\frac{a}{y}] & \text{für ein } a \quad (\text{weil } x \neq y) \\
& \Leftrightarrow & \mathfrak{A} \models \phi[\beta\frac{b}{x}]. &
\end{array}$$

□

Sei $t = t(x_1, \ldots, x_n)$, $\phi = \phi(x_1, \ldots, x_n)$ und $s = s(x_1, \ldots, x_n)$. Dann kann man das Substitutionslemma schreiben als

$$t(s, x_2, \ldots, x_n)^{\mathfrak{A}}[a_1, \ldots, a_n] = t^{\mathfrak{A}}[s^{\mathfrak{A}}[a_1, \ldots, a_n], a_2, \ldots, a_n]$$

und

$$\mathfrak{A} \models \phi(s, x_2, \ldots, x_n)[a_1, \ldots, a_n] \iff \mathfrak{A} \models \phi[s^{\mathfrak{A}}[a_1, \ldots, a_n], a_2, \ldots, a_n].$$

Sei $\phi(x) = \forall y\, y \circ y \doteq x$ und $s = y$. Sei $\mathfrak{A}$ eine L_G–Struktur und β irgendeine Belegung. Dann bedeutet $\mathfrak{A} \models \phi\frac{s}{x}[\beta]$, daß alle Elemente von $\mathfrak{A}$ idempotent sind. $\mathfrak{A} \models \phi[\beta\frac{s^{\mathfrak{A}}[\beta]}{x}]$ bedeutet, daß alle Quadrate gleich $\beta(y)$ sind. Auf die Voraussetzung, daß x frei für s in ϕ, kann man also in 2.3 nicht verzichten.

3 Allgemeingültige Formeln

Definition *Eine L–Formel ϕ heißt* allgemeingültig*, wenn sie für alle*[4] *Belegungen β in allen L–Strukturen gilt. Wir schreiben dafür*

$$\models \phi.$$

$\phi(x_1, \ldots, x_n)$ ist genau dann allgemeingültig, wenn die Aussage $\forall x_1 \ldots x_n \phi(x_1, \ldots, x_n)$ allgemeingültig ist.

Lemma 3.1 *Sei ϕ eine L–Formel und K eine Erweiterung von L. Dann ist ϕ als L–Formel genau dann allgemeingültig, wenn ϕ als K–Formel allgemeingültig ist.*

Beweis:
Wir können annehmen, daß ϕ eine Aussage ist. Wenn $\mathfrak{A} = (A, (Z^{\mathfrak{A}})_{Z \in K})$ eine K-Struktur ist, in der ϕ falsch ist, ist ϕ auch falsch in der *Einschränkung* $\mathfrak{A} \restriction L = (A, (Z^{\mathfrak{A}})_{Z \in L})$ auf L. Wenn ϕ in der L-Struktur $\mathfrak{B}$ falsch ist, wählen wir eine *Expansion* von $\mathfrak{B}$ zu einer K–Struktur $\mathfrak{A}$, für die also $\mathfrak{A} \restriction L = \mathfrak{B}$. (Das ist möglich, weil B nicht leer ist.) Dann ist ϕ auch in $\mathfrak{A}$ falsch. □

Formeln wie zum Beispiel $\phi \vee \neg \phi$ oder $\phi \wedge (\phi \rightarrow \psi) \rightarrow \psi$ sind allgemeingültig, weil sie in einer Struktur immer wahr sind, welchen Wahrheitswert die Teilformeln ϕ und ψ auch haben. Formeln dieser Art heißen Tautologien. Um zu einer präzisen Definition zu kommen, führen wir *Aussagenlogik* ein. Aussagenlogische Formeln bauen sich aus Aussagenvariablen (aus einem Vorrat M von Aussagenvariablen) mit $\neg$ und $\wedge$ auf. $\vee, \rightarrow$ und $\leftrightarrow$ werden wie früher als Abkürzungen verstanden. Eine *Belegung* ist eine Abbildung $\mu : M \longrightarrow \{\mathrm{W}, \mathrm{F}\}$ in die Menge der Wahrheitswerte. μ setzt sich auf die Menge aller Formeln gemäß $\mu(\neg f) = \neg(\mu(f))$ und $\mu(f \wedge g) = \mu(f) \wedge \mu(g)$ fort, wobei $\neg$ und $\wedge$ auf der Menge der Wahrheitswerte durch die Wahrheitstafeln

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

und

$\neg$	
W	F
F	W

definiert sind. Eine aussagenlogische Formel, die bei allen Belegungen den Wahrheitswert W bekommt, heißt allgemeingültig. Zum Beispiel sind für Variable p und q die Formeln $(p \vee \neg p)$ und $(p \wedge (p \rightarrow q) \rightarrow q)$ allgemeingültig.

Wenn wir die Variablen p_i einer aussagenlogischen Formel $f = f(p_1 \ldots, p_n)$ durch L–Formeln ϕ_i ersetzen erhalten wir eine L–Formel $f(\phi_1, \ldots, \phi_n)$.

Definition *Eine* Tautologie *entsteht aus einer allgemeingültigen aussagenlogischen Formel durch Ersetzen der Variablen durch L–Formeln.*

Tautologien sind zum Beispiel $\phi \vee \neg \phi$ und $\phi \wedge (\phi \rightarrow \psi) \rightarrow \psi$.

[4]Weil das leere Universum nicht zugelassen ist, besitzt jede Struktur eine Belegung.

Lemma 3.2 *Tautologien sind allgemeingültig.*

Beweis:
Wenn man die L–Formeln in die aussagenlogische Formel $f = f(p_1, \ldots, p_n)$ einsetzt, ergibt sich für alle Belegungen β:

$$\mathfrak{A} \models f(\phi_1, \ldots, \phi_n)[\beta] \Longleftrightarrow \mu(f) = \mathrm{W},$$

wobei $\mu(p_i) = \mathrm{W} \Leftrightarrow \mathfrak{A} \models \phi_i[\beta]$. □

Lemma 3.3 (Axiome der Gleichheit) *Die folgenden L–Aussagen sind allgemeingültig.*

(1)	*Reflexivität*	$\forall x \;\; x \doteq x$
(2)	*Symmetrie*	$\forall x, y \;\; x \doteq y \rightarrow y \doteq x$
(3)	*Transitivität*	$\forall x, y, z \;\; x \doteq y \wedge y \doteq z \rightarrow x \doteq z$
(4)		$\forall x_1, \ldots, x_n, y_1, \ldots y_n \;\; x_1 \doteq y_1 \wedge \ldots \wedge x_n \doteq y_n \longrightarrow f x_1 \ldots x_n \doteq f y_1 \ldots y_n$
(5)		$\forall x_1, \ldots, x_n, y_1, \ldots y_n \;\; x_1 \doteq y_1 \wedge \ldots \wedge x_n \doteq y_n \longrightarrow (R x_1 \ldots x_n \leftrightarrow R y_1 \ldots y_n)$

Dabei sind die f n–stellige Funktionszeichen und die R n–stellige Relationszeichen aus L.

Beweis:
Klar. □

Die Gleichheitsaxiome drücken aus, daß $=$ eine *Kongruenzrelation*[5] ist.

Lemma 3.4 ($\exists$–Quantorenaxiome) *ϕ sei eine L–Formel, t ein L–Term und x frei für t in ϕ. Dann ist*

$$\phi\frac{t}{x} \longrightarrow \exists x \phi$$

allgemeingültig.

Beweis:
Sei β eine Belegung mit Werten in $\mathfrak{A}$. Dann folgt aus 2.3

$$\mathfrak{A} \models \phi\frac{t}{x}[\beta] \Longrightarrow \mathfrak{A} \models \phi[\beta\frac{t^{\mathfrak{A}}[\beta]}{x}] \Longrightarrow \mathfrak{A} \models \exists x \phi[\beta].$$

□

Daß die Voraussetzung, daß x frei für t in ϕ, notwendig ist, zeigt folgendes Beispiel: Sei $\phi = \forall y \; y \doteq x$ und $t = y$. $\forall y \; y \doteq y \rightarrow \exists x \forall y \; x \doteq y$ ist nicht allgemeingültig.

[5] Eine Kongruenzrelation E auf $\mathfrak{A}$ ist eine Äquivalenzrelation für die $a_1 E b_1, \ldots, a_n E b_n$ impliziert, daß $f^{\mathfrak{A}}(a_1 \ldots a_n) E f^{\mathfrak{A}}(b_1, \ldots, b_n)$, $R^{\mathfrak{A}}(a_1, \ldots, a_n) \Leftrightarrow R^{\mathfrak{A}}(b_1, \ldots, b_n)$.

Lemma 3.5 (Modus Ponens) *Wenn ϕ und $(\phi \to \psi)$ allgemeingültig sind, dann auch ψ.*

Beweis:

Klar. $\square$

Lemma 3.6 ($\exists$–Einführung) *Wenn x nicht frei in ψ vorkommt, dann ist mit $\phi \to \psi$ auch $\exists x\phi \to \psi$ allgemeingültig.*[6]

Beweis:

Wenn $\mathfrak{A} \models \exists x\phi[\beta]$, gibt es ein $a \in A$ mit $\mathfrak{A} \models \phi[\beta\frac{a}{x}]$. Ist $\phi \to \psi$ allgemeingültig, so gilt auch $\mathfrak{A} \models \psi[\beta\frac{a}{x}]$. Aus 2.2 folgt dann $\mathfrak{A} \models \psi[\beta]$. $\square$

[6]Man spricht von *Existenzeinführung.*

4 Der Gödelsche Vollständigkeitssatz

Definition (Der Hilbertkalkül) *L sei eine Sprache. Eine L–Formel ist* beweisbar*, wenn sie*

B1 *eine Tautologie ist,*

B2 *ein Gleichheitsaxiom ist,*

B3 *ein $\exists$–Quantorenaxiom ist,*

B4 *sich mit Hilfe der Modus Ponens Regel aus zwei beweisbaren L–Formeln ergibt,*

B5 *oder wenn sie sich mit der Regel der $\exists$–Einführung aus einer beweisbaren L–Formel ergibt.*

Wir schreiben:

$$\vdash_L \phi$$

Das Ziel dieses Abschnitts ist es, den Gödelschen Vollständigkeitssatz zu beweisen.

Satz 4.1 (Gödelscher Vollständigkeitssatz) *Ein Formel ist genau dann allgemeingültig, wenn sie beweisbar ist:*

$$\models \phi \iff \vdash_L \phi$$

Es folgt, daß $\vdash_L \phi$ von der Sprachumgebung unabhängig ist (vgl. 3.1). Wir verwenden darum später die Notation

$$\vdash \phi.$$

Die eine Richtung ist leicht zu zeigen: Die Menge der allgemeingültigen Sätze hat wegen 3.2, 3.3, 3.4, 3.5 und 3.6 die Eigenschaften **B1**–**B5**. Also sind alle beweisbaren Sätze allgemeingültig.

Der Beweis der Umkehrung macht den Rest des Kapitels aus.

Zuerst ergänzen wir Axiome und Regeln *durch abgeleitete* Axiome und Regeln.

Lemma 4.2

1. **(Aussagenlogik)** *Wenn $\phi_1,\ldots,\phi_n$ beweisbar sind und $(\phi_1 \wedge \ldots \wedge \phi_n) \to \psi$ eine Tautologie ist, ist auch ψ beweisbar.*
2. **($\forall$–Quantorenaxiome)** *Wenn x frei für t in ϕ, ist*
$$\vdash_L \forall x \phi \to \phi\frac{t}{x}.$$
3. **($\forall$–Einführung)** *Wenn x nicht frei in ϕ ist, dann folgt aus der Beweisbarkeit von $\phi \to \psi$ die Beweisbarkeit von $\phi \to \forall x \psi$. Insbesondere folgt aus der Beweisbarkeit von ψ die Beweisbarkeit von $\forall x \psi$.*

Beweis:

1. Die Behauptung gilt auch, wenn wir nur annehmen, daß $(\phi_1 \wedge \ldots \wedge \phi_n) \to \psi$ beweisbar ist. Man sieht leicht, daß

$$((\phi_1 \wedge \ldots \wedge \phi_n) \to \psi) \to (\phi_1 \to (\phi_2 \to (\cdots (\phi_n \to \psi) \cdots)))$$

eine Tautologie ist. Modus Ponens ergibt also die Beweisbarkeit von

$$\phi_1 \to (\phi_2 \to (\cdots (\phi_n \to \psi) \cdots)).$$

Nach n–maliger Anwendung von Modus Ponens sehen wir, daß $\vdash_L \psi$.

2. $\neg \phi \frac{t}{x} \to \exists x \neg \phi$ ist ein $\exists$–Quantorenaxiom.

$$(\neg \phi \frac{t}{x} \to \exists x \neg \phi) \to (\neg \exists x \neg \phi \to \phi \frac{t}{x})$$

ist eine Tautologie (entstanden aus der allgemeingültigen Formel $(\neg p \to q) \to (\neg q \to p)$). Mit Modus Ponens ergibt sich $\vdash_L \neg \exists x \neg \phi \to \phi \frac{t}{x}$.

3. Wenn $\vdash_L \phi \to \psi$, folgt mit einer Anwendung von 4.2.1, daß $\vdash_L \neg \psi \to \neg \phi$. $\exists$–Einführung ergibt $\vdash_L \exists x \neg \psi \to \neg \phi$ und mit Aussagenlogik $\vdash_L \phi \to \neg \exists x \neg \psi$. Um den letzten Teil der Behauptung zu zeigen, nehmen wir an, daß ψ beweisbar ist. Wir nehmen uns dann eine Tautologie ϕ, die x nicht frei enthält. Aussagenlogik ergibt die Beweisbarkeit von $\phi \to \psi$, woraus die Beweisbarkeit von $\phi \to \forall x \psi$ folgt. Mit Modus Ponens ergibt sich $\vdash_L \forall x \psi$. □

Das Lemma erleichtert das Führen von Beweisen sehr. Wir geben als Beispiel einen Beweis[7] der allgemeingültigen Aussage $\exists x \forall y Rxy \to \forall y \exists x Rxy$:

(1)	$\forall y Rxy \to Rxy$	$\forall$–Quantorenaxiom
(2)	$Rxy \to \exists x Rxy$	$\exists$–Quantorenaxiom
(3)	$\forall y Rxy \to \exists x Rxy$	aus (1) und (2) mit Aussagenlogik
(4)	$\forall y Rxy \to \forall y \exists x Rxy$	aus (3) mit $\forall$–Einführung
(5)	$\exists x \forall y Rxy \to \forall y \exists x Rxy$	aus (4) mit $\exists$–Einführung

Das nächste Lemma zeigt, daß wir uns beim Beweis von 4.1 auf Aussagen beschränken können.

Lemma 4.3 *Sei $\phi(x_1, \ldots, x_n)$ eine L–Formel, C eine Menge von neuen Konstanten und $c_1, \ldots, c_n$ eine Folge von paarweise verschiedenen Elementen von C. Dann ist*

$$\vdash_{L \cup C} \phi(c_1, \ldots, c_n) \iff \vdash_L \phi(x_1, \ldots, x_n).$$

Beweis:

Ein *L–Beweis* von ψ ist eine Folge von L–Formeln, die entweder Axiome sind oder mit den beiden Regeln aus früheren Formeln folgen, und die bei ψ endet.

[7] Eigentlich geben wir nur einen Beweis der Beweisbarkeit.

Sei nun $B(c_1, \dots, c_n)$ ein $L \cup C$–Beweis von $\phi(c_1, \dots, c_n)$. (Wir können annehmen, daß alle neuen Konstanten, die im Beweis vorkommen, in der Liste $c_1, \dots, c_n$ aufgeführt sind.) Wenn wir überall im Beweis die Konstanten c_i durch Variable y_i ersetzen, die sonst im Beweis nicht vorkommen, erhalten wir einen L–Beweis $B(y_1, \dots, y_n)$ von $\phi(y_1, \dots, y_n)$. $\forall$–Einführung ergibt (n–mal angewendet) $\forall y_1 \dots y_n\ \phi(y_1, \dots, y_n)$. Zusammen mit dem $\forall$–Quantorenaxiom 4.2.2 $\forall y_1 \dots y_n\ \phi(y_1, \dots, y_n) \to \phi(x_1, \dots, x_n)$ und Modus Ponens ergibt sich $\vdash_L \phi(x_1, \dots, x_n)$.

Wenn umgekehrt $\vdash_L \phi(x_1, \dots, x_n)$, liefert $\forall$–Einführung

$$\vdash_L \forall x_1 \dots x_n\ \phi(x_1, \dots, x_n),$$

woraus $\vdash_{L \cup C} \phi(c_1, \dots, c_n)$ folgt. $\square$

Eine L–*Theorie* ist eine Menge von L–Aussagen. Eine L–Theorie T heißt *widerspruchsfrei* oder *konsistent*, wenn man nicht Aussagen $\phi_1, \dots, \phi_n$ aus T finden kann, die *sich widersprechen*, das heißt, für die $\vdash_L \neg(\phi_1 \wedge \dots \wedge \phi_n)$. (Man beachte, daß es wegen 4.2.1 auf die Klammerung und Reihenfolge der ϕ_i nicht ankommt.) Eine Aussage ϕ ist genau dann nicht beweisbar, wenn $\{\neg \phi\}$ widerspruchsfrei ist. Denn man hat $\vdash \phi \Rightarrow \vdash \neg\neg\phi$ und $\vdash \neg(\neg\phi \wedge \dots \wedge \neg\phi) \Rightarrow \vdash \phi$. Ein *Modell* von T ist eine L–Struktur, in der alle Aussagen aus T gelten. 4.1 folgt also aus dem nächsten Satz, der, weil T auch unendlich sein kann, noch eine wesentliche Verstärkung darstellt.

Sei T eine widerspruchsfreie L–Theorie. Aus dem letzten Lemma folgt, daß T auch als $L \cup C$–Theorie widerspruchsfrei ist. Der nächste Satz hat sogar zur Folge, daß, für jede Erweiterung K von L, T als K–Theorie widerspruchsfrei ist,

Satz 4.4 *Eine Theorie hat genau dann ein Modell, wenn sie widerspruchsfrei ist.*

Beweis:

Eine Theorie, die ein Modell hat, muß natürlich widerspruchsfrei sein.

Für die Umkehrung müssen wir zu einer widerspruchsfreien L–Theorie T ein Modell konstruieren. Wir tun das, indem wir T zuerst zu einer Theorie T^* erweitern, die aussieht wie das *vollständige Diagramm* einer L–Struktur $\mathfrak{A}$: Wir indizieren die Elemente von A mit neuen Konstanten aus einer Menge C

$$A = \{a_c \mid c \in C\}.$$

Das vollständige Diagramm ist dann die Menge aller $L \cup C$–Aussagen, die in der $L \cup C$-Struktur $\mathfrak{A}^* = (\mathfrak{A}, a_c)_{c \in C}$ gelten. Man sieht sofort, daß das vollständige Diagramm eine *vollständige Henkintheorie* ist, im Sinn der folgenden Definition:

Definition

1. *Eine $L \cup C$–Theorie T^+ heißt Henkintheorie mit Konstantenmenge C, wenn es zu jeder $L \cup C$–Formel $\phi(x)$ eine Konstante $c \in C$ mit*

$$\big(\exists x \phi(x) \to \phi(c)\big) \in T^+$$

gibt.

2. *Eine K–Theorie T^* ist vollständig, wenn sie widerspruchsfrei ist und wenn*

$$\phi \in T^* \quad \textit{oder} \quad \neg\,\phi \in T^*$$

für jede K–Aussage ϕ.[8]

Wir werden zuerst zeigen, daß T in einer vollständigen Henkintheorie T^* enthalten ist. Dann beweisen wir, daß T^* das vollständige Diagramm eines Modells ist (das dadurch im wesentlichen eindeutig bestimmt ist.)

Schritt 1
T ist in einer widerspruchsfreien Henkintheorie T^+ enthalten.
Beweis: Sei $\phi(x)$ eine L–Formel und c eine neue Konstante. Dann ist $T \cup \big\{(\exists x\phi(x) \to \phi(c))\big\}$ widerspruchsfrei. Denn wenn für eine L–Aussage ψ

$$\vdash_{L\cup\{c\}} \neg\,\big(\psi \wedge (\exists x\phi(x) \to \phi(c))\big),$$

so folgt (mit Aussagenlogik) $\vdash_{L\cup\{c\}} \neg\,\exists x\phi(x) \to \neg\,\psi$ und $\vdash_{L\cup\{c\}} \phi(c) \to \neg\,\psi$. Aus 4.3 folgt $\vdash_L \neg\,\exists x\phi(x) \to \neg\,\psi$ und $\vdash_L \phi(x) \to \neg\,\psi$. Das letztere hat aber nach der $\exists$–Einführungsregel $\vdash_L \exists x\phi(x) \to \neg\,\psi$ zur Folge und insgesamt ergibt sich (mit Aussagenlogik) $\vdash_L \neg\,\psi$. Daraus ergibt sich: Wenn T widerspruchsfrei ist, dann kann es keine $\psi_1 \ldots \psi_n \in T$ mit $\vdash_{L\cup\{c\}} \neg\,\big(\psi_1 \wedge \ldots \wedge (\exists x\phi(x) \to \phi(c))\big)$ geben.
Daraus folgt (induktiv), daß, wenn wir für jede L–Formel $\phi(x)$ eine eigene Konstante c_ϕ einführen, die Theorie $T_1 = T \cup \{\exists x\phi(x) \to \phi(c_\phi) \mid \phi(x) \text{ L–Formel}\}$ widerspruchsfrei ist (als $L \cup C_1$–Theorie, wobei $C_1 = \{c_\phi \mid \phi(x)\ L\text{–Formel}\}$). Jetzt führen wir für jede $L \cup C_1$–Formel eine neue Konstante ein und erhalten eine $L \cup C_1 \cup C_2$–Theorie T_2. Wenn wir so fortfahren ist $T = \bigcup_{i\in\mathbb{N}} T_i$ eine widerspruchsfreie Henkintheorie T^+ mit Konstantenmenge $C = \bigcup_{i\in\mathbb{N}} C_i$.

Schritt 2
Jede widerspruchsfreie K–Theorie T^+ läßt sich zu einer vollständigen K–Theorie T^* erweitern.
Beweis: Sei ϕ eine K-Aussage. Wenn weder $T^+ \cup \{\phi\}$ noch $T^+ \cup \{\neg\,\phi\}$ widerspruchsfrei wären, gäbe es Aussagen ψ_i und χ_j aus T^+, für die

$$\vdash_K \psi_1 \wedge \ldots \wedge \psi_n \to \phi \qquad \text{und} \qquad \vdash_K \chi_1 \wedge \ldots \wedge \chi_m \to \neg\,\phi.$$

Mit Aussagenlogik ergäbe sich

$$\vdash_K \neg\,(\psi_1 \wedge \ldots \wedge \psi_n \wedge \chi_1 \wedge \ldots \wedge \chi_m),$$

und T^+ wäre nicht widerspruchsfrei.

Es ist also immer $T^+ \cup \{\phi\}$ oder $T^+ \cup \{\neg\,\phi\}$ widerspruchsfrei. Wenn K höchstens abzählbar ist, können wir T^* auf einfache Weise gewinnen: Wir zählen die Menge aller K–Aussagen als $\phi_0, \phi_1 \ldots$ auf und nehmen der Reihe nach jeweils ϕ_i oder $\neg\,\phi_i$ hinzu. Wenn K überabzählbar ist, verwenden wir Zorns Lemma: Weil die Vereinigung jeder Kette von widerspruchsfreien K–Theorien widerspruchsfrei ist, gibt eine maximale widerspruchsfreie K–Theorie T^*, die T^+ enthält. Dann ist $T^* \cup \{\phi\}$ genau dann widerspruchsfrei, wenn $\phi \in T^*$, und T^* ist vollständig. Damit ist die Behauptung bewiesen.

[8] Die offizielle Definition der Vollständigkeit auf Seite 75 ist schwächer.

Wir schreiben $T^+ \vdash_K \phi$, (ϕ *ist aus* T^+ *ableitbar*), wenn es $\psi_1, \ldots, \psi_n \in T^+$ gibt mit

$$\vdash_K \psi_1 \wedge \ldots \wedge \psi_n \to \phi.$$

Wir vermerken, daß eine vollständige Theorie T^* *deduktiv abgeschlossen* ist. Das heißt, daß für alle K–Aussagen ϕ

$$T^* \vdash_K \phi \quad \Leftrightarrow \quad \phi \in T^*.$$

<u>Schritt 3</u>
Eine vollständige Henkintheorie T^* hat ein Modell aus Konstanten. Das heißt ein Modell $\mathfrak{A}^* = (\mathfrak{A}, a_c)_{c\in C}$ mit $A = \{a_c \mid c \in C\}$. $\mathfrak{A}^*$ ist bis auf Isomorphie eindeutig bestimmt.

Beweis der Eindeutigkeit: Sei $\mathfrak{B}^* = (\mathfrak{B}, b_c)_{c\in C}$ ein zweites Modell aus Konstanten. Weil T^* vollständig ist, ist T^* das vollständige Diagramm von $\mathfrak{A}^*$. Es ist also für alle $L \cup C$–Aussagen ϕ

$$\mathfrak{A}^* \models \phi \quad \Leftrightarrow \quad \phi \in T^* \quad \Leftrightarrow \quad \mathfrak{B}^* \models \phi.$$

Weil daher

$$a_c = a_d \quad \Leftrightarrow \quad \mathfrak{A}^* \models c \doteq d \quad \Leftrightarrow \quad \mathfrak{B}^* \models c \doteq d \quad \Leftrightarrow \quad b_c = b_d,$$

liefert $f(a_c) = b_c$ eine Bijektion zwischen A und B. f respektiert die Interpretation der Konstanten aus C nach Konstruktion. Daß die Relationen respektiert werden, folgt aus

$$\begin{aligned} R^{\mathfrak{A}}(a_{c_1}, \ldots, a_{c_n}) \quad &\Leftrightarrow \quad \mathfrak{A}^* \models R(c_1, \ldots, c_n) \quad \Leftrightarrow \quad \mathfrak{B}^* \models R(c_1, \ldots, c_n) \\ &\Leftrightarrow \quad R^{\mathfrak{B}}(b_{c_1}, \ldots, b_{c_n}). \end{aligned}$$

Ebenso schließt man, daß für Funktionszeichen und Konstanten $f \in L$

$$f^{\mathfrak{A}}(a_{c_1}, \ldots, a_{c_n}) = a_{c_0} \quad \Leftrightarrow \quad f^{\mathfrak{B}}(b_{c_1}, \ldots, b_{c_n}) = b_{c_0}.$$

Beweis der Existenz: Um $\mathfrak{A}^*$ zu konstruieren, müssen wir Elemente a_c, $(c \in C)$, finden mit

(1) $$a_c = a_d \quad \Leftrightarrow \quad c \doteq d \in T^*.$$

Das ist genau dann möglich, wenn die Relation

$$c \sim d \quad \Leftrightarrow \quad c \doteq d \in T^*$$

eine Äquivalenzrelation ist. Dann können wir nämlich für a_c die Äquivalenzklasse von c nehmen. Nun folgt aber aus dem ersten Gleichheitsaxiom und dem $\forall$–Quantorenaxiom, daß $\vdash_{L\cup C} c \doteq c$ und, weil T^* deduktiv abgeschlossen ist, $c \doteq c \in T^*$. $\sim$ ist also reflexiv. Aus dem gleichen Grund ist $(c \doteq d \wedge d \doteq e \to c \doteq e) \in T^*$. Wenn nun $c \doteq d \in T^*$ und $d \doteq e \in T^*$, folgt, wegen der deduktiven Abgeschlossenheit, $c \doteq e \in T^*$. Damit ist $\sim$ transitiv. Ebenso folgt die Symmetrie aus dem dritten Gleichheitsaxiom.

Wir setzen $A = \{a_c \mid c \in C\}$.

Jetzt müssen wir für jedes Relationszeichen $R \in L$ eine Relation $R^{\mathfrak{A}}$ auf A finden, sodaß

$$(2) \qquad R^{\mathfrak{A}}(a_{c_1}, \ldots, a_{c_n}) \quad \Leftrightarrow \quad R(c_1, \ldots, c_n) \in T^*.$$

Wir können (2) als Definition nehmen, wenn wir zeigen können, daß

$$a_{c_1} = a_{d_1}, \ldots, a_{c_n} = a_{d_n},\ R(c_1, \ldots, c_n) \quad \Rightarrow \quad R(d_1, \ldots, d_n) \in T^*.$$

Das folgt aber aus dem fünften Gleichheitsaxiom und der deduktiven Abgeschlossenheit von T^*. Sei f ein n–stelliges Funktionszeichen oder eine Konstante (dann setzen wir $n = 0$) aus L. Wir müssen eine Operation $f^{\mathfrak{A}}$ auf A so definieren, daß

$$(3) \qquad f^{\mathfrak{A}}(a_{c_1}, \ldots, a_{c_n}) = a_{c_0} \quad \Leftrightarrow \quad f(c_1, \ldots, c_n) \doteq c_0 \in T^*.$$

Dazu müssen wir erstens für alle $c_1, \ldots, c_n$ ein c_0 finden, für das die rechte Seite von (3) gilt. Aus $\vdash_{L \cup C} f(c_1, \ldots, c_n) \doteq f(c_1, \ldots, c_n)$ folgt aber mit dem $\exists$–Quantorenaxiom $\vdash_{L \cup C} \exists x\ f(c_1, \ldots, c_n) \doteq x$. Weil T^* eine Henkintheorie ist, gibt es ein $c_0 \in C$ mit $(\exists x\ f(c_1, \ldots, c_n) \doteq x \to f(c_1, \ldots, c_n) \doteq c_0) \in T^*$. Aus der deduktiven Abgeschlossenheit folgt die rechte Seite von (3).

Zweitens müssen wir zeigen, daß a_{c_0} durch die rechte Seite von (3) eindeutig bestimmt ist und nur von den $a_{c_1}, \ldots, a_{c_n}$ abhängt. Das heißt, daß $c_0 \doteq d_0$ zu T^* gehört, wenn $c_1 \doteq d_1, \ldots, c_n \doteq d_n$, $f(c_1, \ldots, c_n) \doteq c_0$ und $f(d_1, \ldots, d_n) \doteq d_0$ zu T^* gehören. Das folgt aber aus den Gleichheitsaxiomen und der deduktiven Abgeschlossenheit von T^*.

Konstante Terme (das heißt, Terme ohne Variable) werden in $\mathfrak{A}^*$ so ausgerechnet, wie es T^* sagt:

$$(4) \qquad t^{\mathfrak{A}^*} = a_c \quad \Leftrightarrow \quad t \doteq c \in T^*$$

Wir zeigen das durch Induktion über den Aufbau von t: Wenn t eine Konstante aus C ist, folgt die Behauptung aus (1). Wenn $t = ft_1 \ldots t_n$, und $t_i^{\mathfrak{A}^*} = a_{c_i}$, sind nach Induktionsvoraussetzung die Gleichungen $t_i \doteq c_i$ in T^*. Aus dem vierten Gleichheitsaxiom folgt, daß

$$t \doteq c \in T^* \quad \Leftrightarrow \quad fc_1 \ldots c_n \doteq c \in T^*.$$

Andererseits ist

$$t^{\mathfrak{A}^*} = a_c \quad \Leftrightarrow \quad f^{\mathfrak{A}^*}(a_{c_1}, \ldots, a_{c_n}) = a_c \quad \Leftrightarrow \quad fc_1 \ldots c_n \doteq c \in T^*.$$

Schließlich beweisen wir durch Induktion über den Aufbau der Aussage ϕ, daß

$$\mathfrak{A}^* \models \phi \quad \Leftrightarrow \quad \phi \in T^*.$$

1. Fall: $\phi = t_1 \doteq t_2$

Sei $t_i^{\mathfrak{A}^*} = a_{c_i}$. Dann ist nach (4) $\quad t_i \doteq c_i \in T^*$ für $i = 1, 2$ und daher

$$\mathfrak{A}^* \models \phi \quad \Leftrightarrow \quad a_{c_1} = a_{c_2} \quad \Leftrightarrow \quad c_1 \doteq c_2 \in T^* \quad \Leftrightarrow \quad t_1 \doteq t_2 \in T^*.$$

2. Fall: $\phi = Rt_1 \ldots, t_n$

Sei $t_i^{\mathfrak{A}^*} = a_{c_i}$. Dann ist nach (4) $\quad t_i \doteq c_i \in T^*$ für $i = 1, \ldots, n$ und

$$\mathfrak{A}^* \models \phi \quad \Leftrightarrow \quad Rc_1 \ldots c_n \in T^* \quad \Leftrightarrow \quad \phi \in T^*.$$

Die letzte Äquivalenz folgt aus dem fünften Gleichheitsaxiom.

3. Fall $\phi = \neg \psi$

Weil T^* vollständig ist, gilt

$$\mathfrak{A}^* \models \phi \quad \Leftrightarrow \quad \mathfrak{A}^* \not\models \psi \quad \Leftrightarrow \quad \psi \notin T^* \quad \Leftrightarrow \quad \phi \in T^*.$$

4. Fall $\phi = (\psi_1 \wedge \psi_2)$

Aus der deduktiven Abgeschlossenheit von T^* folgt:

$$\mathfrak{A}^* \models \phi \quad \Leftrightarrow \quad \mathfrak{A}^* \models \psi_i \ (i = 1, 2) \quad \Leftrightarrow \quad \psi_i \in T^* \ (i = 1, 2) \quad \Leftrightarrow \quad \phi \in T^*.$$

5. Fall $\phi = \exists x \ \psi$

Aus der deduktiven Abgeschlossenheit von T^* folgt $\exists x \ \psi \in T^*$, wenn $\psi(c) \in T^*$ für ein $c \in C$. Wenn umgekehrt $\exists x \ \psi \in T^*$, und $\exists x \ \psi \to \psi(c) \in T^*$ folgt $\psi(c) \in T^*$. Also haben wir

$$\mathfrak{A}^* \models \phi \quad \Leftrightarrow \quad \mathfrak{A}^* \models \psi[a_c] \quad \text{für ein } c \in C \quad \Leftrightarrow \quad \mathfrak{A}^* \models \psi(c) \quad \text{für ein } c \in C$$

$$\Leftrightarrow \quad \psi(c) \in T^* \quad \text{für ein } c \in C \quad \Leftrightarrow \quad \phi \in T^*.$$

Damit ist 4.4 bewiesen. □

Definition *Sei T eine L–Theorie und ϕ eine L–Aussage.*

1. *ϕ ist in T* beweisbar,

   $$T \vdash \phi,$$

   wenn es Axiome $\psi_1, \ldots, \psi_n$ aus T gibt für die $\psi_1 \wedge \cdots \wedge \psi_n \to \phi$ beweisbar ist.

2. *ϕ* folgt logisch *aus T,*

   $$T \models \phi,$$

   wenn ϕ in allen Modellen von T gilt

Folgerung 4.5

$$T \vdash \phi \quad \Leftrightarrow \quad T \models \phi$$

Beweis:

ϕ ist in T genau dann nicht beweisbar, wenn $T \cup \{\neg\, \phi\}$ widerspruchsfrei ist. Andererseits folgt ϕ genau dann nicht logisch aus T, wenn $T \cup \{\neg\, \phi\}$ ein Modell hat. □

Folgerung 4.6 (Kompaktheitssatz) *Eine Theorie hat genau dann ein Modell, wenn jede endliche Teilmenge ein Modell hat.*

Den Kompaktheitssatz könnte man den ersten Hauptsatz der Modelltheorie nennen. Der zweite Hauptsatz wäre der Satz von Löwenheim-Skolem.

Folgerung 4.7 (Löwenheim-Skolem) *Wenn eine Theorie mit höchstens abzählbarer Sprache eine Modell hat, hat sie ein höchstens abzählbares Modell.*

Beweis:

Im Beweis von 4.4 wurde die Sprache durch eine Konstantenmenge C erweitert. Zu jeder L–Formel wurde eine Konstante eingeführt und dieser Prozeß abzählbar oft wiederholt. Wenn L höchstens abzählbar ist, ist also auch C höchstens abzählbar. Das im Beweis konstruierte Modell hat aber höchstens so viele Elemente wie C. □

Am Schluß dieses Abschnitts bemerken wir noch, daß man sich in vielen Fällen auf Formeln ohne Gleichheitszeichen zurückziehen kann. Sei T eine L–Theorie und E ein neues zweistelliges Relationszeichen. Wir bezeichnen mit

- $T(\doteq/E)$ die $L \cup \{E\}$–Theorie, die aus T entsteht, indem man in den Axiomen alle Teilformeln $t_1 \doteq t_2$ durch Et_1t_2 ersetzt,
- Kong_L Axiome, die ausdrücken, daß E eine Kongruenzrelation ist.

Dann gilt:

Lemma 4.8 *T ist genau dann konsistent, wenn $T(\doteq/E) \cup \mathrm{Kong}_L$ konsistent ist.*

Beweis:

Ein Modell von T wird ein Modell von $T(\doteq/E) \cup \mathrm{Kong}_L$, wenn man E durch die Gleichheit interpretiert. Sei umgekehrt $(\mathfrak{A}, E^{\mathfrak{A}})$ ein Modell von $T(\doteq/E) \cup \mathrm{Kong}_L$. Dann ist E eine Kongruenzrelation auf $\mathfrak{A}$. Definiere die L–Struktur $\mathfrak{B}$ auf der Grundmenge $A/E^{\mathfrak{A}}$ durch

$$\begin{array}{rcl} c^{\mathfrak{B}} & = & c^{\mathfrak{A}}E \\ f^{\mathfrak{B}}(a_1E,\ldots,a_nE) & = & f^{\mathfrak{A}}(a_1,\ldots,a_n)E \\ R^{\mathfrak{B}}(a_1E,\ldots,a_nE) & \Leftrightarrow & R^{\mathfrak{A}}(a_1,\ldots,a_n) \end{array}$$

$\mathfrak{B}$ ist ein Modell von T. □

Bemerkung *Der Beweis von 4.1 zeigt, daß eine allgemeingültige Formel ohne Gleichheitszeichen einen Beweis hat, in dem keine Gleichheitszeichen vorkommen.*

5 Der Sequenzenkalkül

Der von Gentzen aufgestellte Sequenzenkalkül hat gegenüber dem Hilbertschen Kalkül Vorteile

1. Axiome und Regeln entsprechen den Regeln des Formelaufbaus.
2. Die Beweise sind näher am natürlichen Schließen.
3. Der Beweis des Vollständigkeitssatzes ist einfach.
4. Die Beweise lassen sich analysieren.

aber den Nachteil, daß man Sequenzen (und nicht Formeln) herleitet.

Sei L eine Sprache und C eine abzählbare Menge von neuen Konstanten. Eine *Sequenz* ist ein Paar

$$\Delta \quad \succ \quad \Gamma$$

von endlichen Mengen von $L \cup C$–Aussagen. Eine Sequenz $\Delta \succ \Gamma$ gilt in der $L \cup C$–Struktur $\mathfrak{A}^*$, wenn in $\mathfrak{A}^*$ eine der Aussagen aus Δ falsch ist oder eine der Aussagen aus Γ wahr. $\{\delta_1, \dots, \delta_m\} \succ \{\gamma_1, \dots, \gamma_n\}$ hat also die Bedeutung

$$(\delta_1 \wedge \ldots \wedge \delta_m) \longrightarrow (\gamma_1 \vee \ldots \vee \gamma_n).$$

Eine Sequenz ist *allgemeingültig*, wenn sie in allen $L \cup C$–Strukturen gilt.

Wir beschreiben die Axiome und Regeln des Sequenzenkalküls in der Form $\dfrac{\mathfrak{S}_1, \dots, \mathfrak{S}_n}{\mathfrak{S}_0}$ mit der Bedeutung: *Wenn die Sequenzen* $\mathfrak{S}_1, \dots, \mathfrak{S}_n$ *ableitbar sind, dann auch die Sequenz* $\mathfrak{S}_0$. Wir lassen die Regeln für Gleichheit, Konstanten und Funktionszeichen weg, um die Darstellung zu vereinfachen.[9]

Axiome	$\dfrac{}{\Delta \cup \{\phi\} \succ \Gamma \cup \{\phi\}}$	
$\neg$–links–Regel	$\dfrac{\Delta \succ \Gamma \cup \{\phi\}}{\Delta \cup \{\neg\,\phi\} \succ \Gamma}$	
$\neg$–rechts–Regel	$\dfrac{\Delta \cup \{\phi\} \succ \Gamma}{\Delta \succ \Gamma \cup \{\neg\,\phi\}}$	
$\wedge$–links–Regeln	$\dfrac{\Delta \cup \{\phi_i\} \succ \Gamma}{\Delta \cup \{(\phi_1 \wedge \phi_2)\} \succ \Gamma}$	für $i = 1, 2$
$\wedge$–rechts–Regel	$\dfrac{\Delta \succ \Gamma \cup \{\phi_1\} \quad , \quad \Delta \succ \Gamma \cup \{\phi_2\}}{\Delta \succ \Gamma \cup \{(\phi_1 \wedge \phi_2)\}}$	
$\exists$–links–Regel	$\dfrac{\Delta \cup \{\phi(c)\} \succ \Gamma}{\Delta \cup \{\exists x\, \phi(x)\} \succ \Gamma}$	wenn c nicht in Δ, Γ und ϕ vorkommt.
$\exists$–rechts–Regel	$\dfrac{\Delta \succ \Gamma \cup \{\phi(c)\}}{\Delta \succ \Gamma \cup \{\exists x\, \phi(x)\}}$	

Wenn man will, kann man in den Axiomen voraussetzen, daß ϕ eine Primformel ist.

[9] $n \geq 0$-stellige Funktionen könnte man durch $n+1$ stellige Relationen ersetzen. Für Gleichheitszeichen siehe Lemma 4.8.

Satz 5.1 *Eine Sequenz (ohne Gleichheit, Konstanten und Funktionszeichen aus L) ist genau dann allgemeingültig, wenn sie im Sequenzenkalkül ableitbar ist.*

Beweis:

Es ist klar, daß die Axiome des Kalküls allgemeingültig sind und daß die Regeln von allgemeingültigen Sequenzen wieder zu allgemeingültige Sequenzen führen: In den $\neg$–Regeln und der $\wedge$–rechts–Regel ist die Konklusion logisch äquivalent zu der (Konjunktion der) Hypothese(n). In den $\wedge$–links–Regeln und in der $\exists$–rechts–Regel folgt die Konklusion (wegen 3.4) aus der Hypothese. Die $\exists$–links–Regel ist eine Form der $\exists$–Einführung.

Bevor wir die Umkehrung beweisen, zeigen wir noch wie die Allgemeingültigkeit der Formel $\phi = \exists x \forall y Rxy \rightarrow \forall y \exists x Rxy$ im Sequenzenkalkül abgeleitet wird: (Wir lassen dabei auf beiden Seiten einer Sequenz Mengenklammern weg.)

$Rcd \succ Rcd$	Axiom
$Rcd \succ \exists x Rxd$	$\exists$–rechts–Regel
$\succ \neg Rcd, \exists x Rxd$	$\neg$–rechts–Regel
$\succ \exists y \neg Rcy, \exists x Rxd$	$\exists$–rechts–Regel
$\neg \exists x Rxd \succ \exists y \neg Rcy$	$\neg$–links–Regel
$\neg \exists y \neg Rcy, \neg \exists x Rxd \succ$	$\neg$–links–Regel
$\neg \exists y \neg Rcy, \exists y \neg \exists x Rxy \succ$	$\exists$–links–Regel
$\exists x \neg \exists y \neg Rxy, \exists y \neg \exists x Rxy \succ$	$\exists$–links–Regel
$\exists x \neg \exists y \neg Rxy \succ \neg \exists y \neg \exists x Rxy$	$\neg$–rechts–Regel
$\exists x \neg \exists y \neg Rxy, \neg \neg \exists y \neg \exists x Rxy \succ$	$\neg$–links–Regel
$(\exists x \neg \exists y \neg Rxy \wedge \neg \neg \exists y \neg \exists x Rxy), \exists x \neg \exists y \neg Rxy \succ$	$\wedge$–links–Regel
$(\exists x \neg \exists y \neg Rxy \wedge \neg \neg \exists y \neg \exists x Rxy) \succ$	$\wedge$–links–Regel
$\succ \neg (\exists x \neg \exists y \neg Rxy \wedge \neg \neg \exists y \neg \exists x Rxy)$	$\neg$–rechts–Regel

Die rechte Seite der letzten Sequenz ist ϕ.

Sei $\Delta \succ \Gamma$ eine Sequenz, die nicht ableitbar ist. L sei eine endliche (oder abzählbare) Sprache, zu der diese Sequenz gehört. Wir konstruieren eine Folge $\Delta_i \succ \Gamma_i$, $(i = 0, 1, 2 \ldots)$ von nicht–ableitbaren Sequenzen. Dabei werden die Δ_i und die Γ_i zwei aufsteigende Folgen bilden, die bei $\Delta = \Delta_0$ und bei $\Gamma = \Gamma_0$ beginnen. Wir fixieren eine Aufzählung $(\epsilon_i, \phi_i, c_i)$, in der jedes Tripel (ϵ, ϕ, c), bestehend aus $\epsilon \in \{links, rechts\}$, einer $L \cup C$–Formel ϕ_i und einer Konstanten c, unendlich oft vorkommt. Dann definieren wir die gesuchte Folge rekursiv. Sei $\Delta_i \succ \Gamma_i$ schon konstruiert und nicht ableitbar:

1. Fall: $\phi_i = \neg \psi \in \Delta_i$ und $\epsilon_i = links$. Dann ist wegen der $\neg$–links–Regel die Sequenz $\Delta_{i+1} = \Delta_i \succ \Gamma_{i+1} = \Gamma_i \cup \{\psi\}$ nicht ableitbar.

2. Fall: $\phi_i = \neg \psi \in \Gamma_i$ und $\epsilon_i = rechts$. Dann ist wegen der $\neg$–rechts–Regel die Sequenz $\Delta_{i+1} = \Delta_i \cup \{\psi\} \succ \Gamma_{i+1} = \Gamma_i$ nicht ableitbar.

3. Fall: $\phi = (\psi_1 \wedge \psi_2) \in \Delta_i$ und $\epsilon_i = links$. Wir setzen $\Delta_{i+1} = \Delta_i \cup \{\psi_1, \psi_2\}$ und $\Gamma_{i+1} = \Gamma_i$. Durch Anwenden der beiden $\wedge$–links–Regeln könnte man $\Delta_i \succ \Gamma_i$ aus $\Delta_{i+1} \succ \Gamma_{i+1}$ gewinnen. Also ist $\Delta_{i+1} \succ \Gamma_{i+1}$ nicht ableitbar.

4. Fall: $\phi = (\psi_1 \wedge \psi_2) \in \Gamma_i$ und $\epsilon_i = rechts$. Wegen der $\wedge$–rechts–Regel können nicht beide Sequenzen $\Delta_i \succ \Gamma_i \cup \{\psi_1\}$ und $\Delta_i \succ \Gamma_i \cup \{\psi_2\}$ ableitbar

sein. Wir wählen j so daß $\Delta_{i+1} = \Delta_i \succ \Gamma_{i+1} = \Gamma_i \cup \{\psi_j\}$ nicht ableitbar ist.

5. Fall: $\phi_i = \exists x \psi(x) \in \Delta_i$ und $\epsilon_i = links$. Wähle ein c, daß in Δ_i und Γ_i nicht vorkommt. Dann ist wegen der $\exists$–links–Regel die Sequenz $\Delta_{i+1} = \Delta_i \cup \{\psi(c)\} \succ \Gamma_{i+1} = \Gamma_i$ nicht ableitbar.

6. Fall: $\phi_i = \exists x \psi(x) \in \Gamma_i$ und $\epsilon_i = rechts$. Wir setzen dann $\Delta_{i+1} = \Delta_i$ und $\Gamma_{i+1} = \Gamma_i \cup \{\psi(c_i)\}$. Die neue Sequenz ist nicht ableitbar wegen der $\exists$–rechts–Regel.

Wenn keiner dieser sechs Fälle auftritt, setzen wir $\Delta_{i+1} = \Delta_i$ und $\Gamma_{i+1} = \Gamma_i$. Weil die $\Delta_i \succ \Gamma_i$ keine Axiome sind, sind die Δ_i und die Γ_i disjunkt.

Die Mengen $\Delta^* = \bigcup_{i\in\mathbb{N}} \Delta_i$ und $\Gamma^* = \bigcup_{i\in\mathbb{N}} \Gamma_i$ haben offensichtlich die folgenden Eigenschaften

0. Δ^* und Γ^* sind disjunkt.
1. Wenn $\neg\psi \in \Delta^*$, ist $\psi \in \Gamma^*$.
2. Wenn $\neg\psi \in \Gamma^*$, ist $\psi \in \Delta^*$.
3. Wenn $(\psi_1 \wedge \psi_2) \in \Delta^*$, gehören ψ_1 und ψ_2 zu Δ^*.
4. Wenn $(\psi_1 \wedge \psi_2) \in \Gamma^*$, dann gehört ψ_1 oder ψ_2 zu Γ^*.
5. Wenn $\exists x \psi(x) \in \Delta^*$, gibt es ein $c \in C$ mit $\psi(c) \in \Delta^*$.
6. Wenn $\exists x \psi(x) \in \Gamma^*$, ist $\psi(c) \in \Gamma^*$ für alle $c \in C$.

Sei nun $A = \{a_c \mid c \in C\}$ eine Menge, die durch $(a_c)_{c\in C}$ injektiv aufgezählt ist (man kann z.B. $a_c = c$ nehmen). Wir machen A zu einer L–Struktur $\mathfrak{A}$, indem wir die Relationszeichen $R \in L$ durch $R^{\mathfrak{A}}(a_{c_1}, \ldots, a_{c_n}) \Leftrightarrow R(c_1, \ldots, c_n) \in \Delta^*$ interpretieren. $\mathfrak{A}^* = (\mathfrak{A}, a_c)_{c\in C}$ ist eine $L \cup C$–Struktur, in der $\Delta \succ \Gamma$ nicht gilt. Um das einzusehen, zeigen wir durch Induktion über den Aufbau von ϕ, daß $\phi \in \Delta^* \Rightarrow \mathfrak{A}^* \models \phi$ und $\phi \in \Gamma^* \Rightarrow \mathfrak{A}^* \not\models \phi$:

0. Fall: $\phi = R(c_1, \ldots, c_n)$.
   Wenn $R(c_1, \ldots, c_n) \in \Delta^*$, ist $\mathfrak{A}^* \models R(c_1, \ldots, c_n)$ nach Konstruktion. Wenn $R(c_1, \ldots, c_n) \in \Gamma^*$, ist nach Eigenschaft (0) $R(c_1, \ldots, c_n) \notin \Delta^*$, also $\mathfrak{A}^* \not\models R(c_1, \ldots, c_n)$.

1. Fall: $\phi = \neg\psi \in \Delta^*$.
   Dann ist nach Eigenschaft (1) $\psi \in \Gamma^*$. Nach Induktionsvoraussetzung ist $\mathfrak{A}^* \not\models \psi$. Also $\mathfrak{A}^* \models \phi$.

2. Fall: $\phi = \neg\psi \in \Gamma^*$.
   Dann ist nach Eigenschaft (2) $\psi \in \Delta^*$. Die Induktionsvoraussetzung liefert $\mathfrak{A}^* \models \psi$. Also $\mathfrak{A}^* \not\models \phi$.

3. Fall: Wenn $\phi = (\psi_1 \wedge \psi_2) \in \Delta^*$,
   sind wegen (3) ψ_1 und ψ_2 in Δ^*. Nach Induktionsvoraussetzung gelten ψ_1 und ψ_2 in $\mathfrak{A}^*$, also gilt auch ϕ.

4. Fall: Aus $\phi = (\psi_1 \wedge \psi_2) \in \Gamma^*$
folgt aus (4), daß zum Beispiel $\psi_1 \in \Gamma^*$. Die Induktionsvoraussetzung liefert $\mathfrak{A}^* \not\models \psi_1$, also $\mathfrak{A}^* \not\models \phi$.

5. Fall: Wenn $\exists x \psi(x) \in \Delta^*$,
gibt es wegen (5) ein $c \in C$ mit $\psi(c) \in \Delta^*$. Dann ist $\mathfrak{A}^* \models \psi(c)$ nach Induktionsvoraussetzung, also $\mathfrak{A}^* \models \phi$.

6. Fall: $\phi = \exists x \psi(x) \in \Gamma^*$.
Eigenschaft (6) sagt, daß alle $\phi(c)$ für $c \in C$ zu Γ^* gehören. Also gilt nach Induktionsvoraussetzung keines der $\phi(c)$ in $\mathfrak{A}^*$. Weil $A = \{c^{\mathfrak{A}^*} \mid c \in C\}$ ist $\mathfrak{A}^* \not\models \phi$.

□

Als ein Anwendungsbeispiel beweisen wir den *Interpolationssatz*. Allerdings nur für Aussagen ϕ_i ohne Gleichheit, Konstanten und Funktionszeichen. Man kann sich aber leicht überzeugen, daß der Satz in seiner Allgemeinheit leicht aus diesem Spezialfall folgt.

Satz 5.2 *Sei ϕ_1 eine L_1–Aussage und ϕ_2 eine L_2–Aussage. Wenn*

$$\phi_1 \rightarrow \phi_2$$

allgemeingültig ist, gibt es eine interpolierende *$L_1 \cap L_2$–Aussage δ, für die*

$$\phi_1 \rightarrow \delta \quad \textit{und} \quad \delta \rightarrow \phi_2$$

allgemeingültig sind.

Beweis:

Wenn $\phi_1 \rightarrow \phi_2$ allgemeingültig ist, ist die Sequenz $\phi_1 \succ \phi_2$ ableitbar. Wir zeigen die Existenz von δ durch Induktion über die Länge des Beweises. Weil aber in einem Beweis von $\phi_1 \rightarrow \phi_2$ Sequenzen vorkommen werden, in denen L_1–Aussagen auch rechts und L_2–Aussagen auch links stehen können, beweisen wir durch Induktion über die Beweislänge:

Wenn Δ_i und Γ_i endliche Mengen von $L_i \cup C$–Aussagen sind und

$$\Delta_1 \cup \Delta_2 \succ \Gamma_1 \cup \Gamma_2$$

ableitbar ist, gibt es eine $(L_1 \cap L_2) \cup C$–Aussage β, für die $\Delta_1 \succ \Gamma_1 \cup \{\beta\}$ und $\{\beta\} \cup \Delta_2 \succ \Gamma_2$ allgemeingültig sind.

Daraus folgt dann die Behauptung. Denn wenn $\phi \succ \beta(c_1, \ldots, c_n)$ und $\beta(c_1, \ldots, c_n) \succ \psi$ allgemeingültig sind, leistet $\delta = \exists x_1 \ldots x_n \; \beta(x_1, \ldots x_n)$ das Verlangte.

Sei nun $\mathfrak{S} = \Delta_1 \cup \Delta_2 \succ \Gamma_1 \cup \Gamma_2$ ableitbar. Dann ist $\mathfrak{S}$ ein Axiom oder folgt nach einer der sechs Regeln aus Sequenzen mit kürzeren Ableitungen. Jeder dieser Fälle zerfällt in zwei Unterfälle, je nachdem, ob die Formel im Axiom zu Δ_1 oder Δ_2, oder ob die in der Regel betrachtete Formel zu $\Delta_1 \cup \Gamma_1$ oder $\Delta_2 \cup \Gamma_2$

gehört. Wir brauchen aber immer nur den ersten dieser Fälle zu betrachten. Die Induktionsbehauptung impliziert nämlich die Allgemeingültigkeit von $\Delta_2 \succ \Gamma_2 \cup \{\neg\beta\}$ und $\{\neg\beta\} \cup \Delta_1 \succ \Gamma_1$ und ist daher symmetrisch in L_1 und L_2.

0. Fall: $\mathfrak{S}$ ist ein Axiom, weil es ein $\phi \in \Delta_1$ mit $\phi \in \Gamma_1 \cup \Gamma_2$ gibt. Wenn $\phi \in \Gamma_1$ ist, können wir $\beta = \neg c \doteq c$ setzen[10], und $\beta = \phi$, wenn $\phi \in \Gamma_2$.

1. Fall: Es ist $\Delta_1 = \Delta_1' \cup \{\neg\phi\}$ und $\mathfrak{S}$ folgt mit der $\neg$–links–Regel aus $\Delta_1' \cup \Delta_2 \succ (\Gamma_1 \cup \{\phi\}) \cup \Gamma_2$. Nach Induktionsvoraussetzung gibt es eine $(L_1 \cap L_2) \cup C$–Formel β', für die $\Delta_1' \succ (\Gamma_1 \cup \{\phi\}) \cup \{\beta'\}$ und $\{\beta'\} \cup \Delta_2 \succ \Gamma_2$ allgemeingültig sind. Wir setzen $\beta = \beta'$.

2. Fall: Es ist $\Gamma_1 = \Gamma_1' \cup \{\neg\phi\}$ und $\mathfrak{S}$ folgt mit der $\neg$–rechts–Regel aus $(\Delta_1 \cup \{\phi\}) \cup \Delta_2 \succ \Gamma_1' \cup \Gamma_2$. Wir wählen wieder β', sodaß $\Delta_1 \cup \{\phi\} \succ (\Gamma_1') \cup \{\beta'\}$ und $\{\beta'\} \cup \Delta_2 \succ \Gamma_2$ allgemeingültig sind, und setzen $\beta = \beta'$.

3. Fall: Es ist $\Delta_1 = \Delta_1' \cup \{\phi_1 \wedge \phi_2\}$ und für ein $i = 1, 2$ folgt $\mathfrak{S}$ mit der $\wedge$–rechts–Regel aus $(\Delta_1' \cup \{\phi_i\}) \cup \Delta_2 \succ \Gamma_1 \cup \Gamma_2$. Wenn $(\Delta_1' \cup \{\phi_i\}) \succ \Gamma_1 \cup \{\beta'\}$ und $\{\beta'\} \cup \Delta_2 \succ \Gamma_2$ allgemeingültig sind, können wir $\beta = \beta'$ nehmen.

4. Fall: Es ist $\Gamma_1 = \Gamma_1' \cup \{\phi_1 \wedge \phi_2\}$ und $\mathfrak{S}$ folgt aus den beiden Sequenzen $\Delta_1 \cup \Delta_2 \succ (\Gamma_1 \cup \{\phi_i\}) \cup \Gamma_2$ $(i = 1, 2)$ mit der $\wedge$–rechts–Regel. Wenn dann für $i = 1, 2$ $\Delta_1 \succ (\Gamma_1' \cup \{\phi_i\}) \cup \{\beta_i\}$ und $\{\beta_i\} \cup \Delta_2 \succ \Gamma_2$ allgemeingültig sind, setzen wir $\beta = \beta_1 \vee \beta_2$.

5. Fall: Es ist $\Delta_1 = \Delta_1' \cup \{\exists x\ \phi(x)\}$ und $\mathfrak{S}$ folgt aus $(\Delta_1' \cup \{\phi(c)\}) \cup \Delta_2 \succ \Gamma_1 \cup \Gamma_2$ mit der $\exists$–links–Regel. c kommt also in $\mathfrak{S}$ nicht vor. Wenn nun für ein $\beta(x)$, das c nicht enthält, die Sequenzen $(\Delta_1' \cup \{\phi(c)\}) \succ \Gamma_1 \cup \{\beta'(c)\}$ und $\{\beta'(c)\} \cup \Delta_2 \succ \Gamma_2$ allgemeingültig sind, setzen wir $\beta = \exists x\ \beta'(x)$.

6. Fall: Es ist $\Gamma_1 = \Gamma_1' \cup \{\exists x\ \phi(x)\}$ und $\mathfrak{S}$ folgt mit der $\exists$–rechts–Regel aus $\Delta_1 \cup \Delta_2 \succ (\Gamma_1' \cup \{\phi(c)\}) \cup \Gamma_2$. Wenn $\Delta_1 \succ (\Gamma_1' \cup \{\phi(c)\}) \cup \{\beta'\}$ und $\{\beta'\} \cup \Delta_2 \succ \Gamma_2$ allgemeingültig sind, setzen wir $\beta = \beta'$.

□

[10] Statt $\neg c \doteq c$ können wir irgendeine $(L_1 \cap L_2) \cup C$–Aussage nehmen, deren Negation allgemeingültig ist.

6 Der Herbrandsche Satz und automatisches Beweisen

Definition *Eine universelle Formel hat die Form*

$$\forall x_1 \dots \forall x_n \psi,$$

wobei ψ eine quantorenfreie Formel ist. Existentielle Formeln beginnen mit Existenzquantoren.

Satz 6.1 (Skolem–Normalform) *Zu jeder L–Aussage ϕ kann man eine Spracherweiterung L^* und einen universellen L^*–Satz ϕ^* angeben, derart, daß ϕ in einer L–Struktur $\mathfrak{A}$ genau dann gilt, wenn sich $\mathfrak{A}$ zu einem Modell von ϕ^* expandieren läßt.*
ϕ ist also genau dann erfüllbar, wenn ϕ^* erfüllbar ist.

Beweis:
Eine Formel ist in *pränexer* Normalform, wenn alle Quantoren am Anfang der Formel stehen, wenn also die Formel die Gestalt

$$Q_1 x_1 Q_2 x_2 \dots Q_n x_n \psi$$

hat, mit quantorenfreiem ψ und $Q_i \in \{\exists, \forall\}$.

Man sieht leicht, daß sich in jeder Formel die Quantoren so nach vorn ziehen lassen, daß eine äquivalente Formel[11] in pränexer Normalform entsteht. Man verwendet dabei die Umformungen

$$\begin{array}{rcl} \neg\exists & \rightsquigarrow & \forall\neg \\ \neg\forall & \rightsquigarrow & \exists\neg \\ (\phi \wedge \exists x \psi) & \rightsquigarrow & \exists y\, (\phi \wedge \psi \frac{x}{y}) \\ (\phi \wedge \forall x \psi) & \rightsquigarrow & \forall y\, (\phi \wedge \psi \frac{x}{y}) \end{array}$$

Die Variable y soll dabei in ϕ und ψ nicht vorkommen.

Wir können also annehmen, daß ϕ pränex ist. ϕ^* konstruieren wir durch Rekursion über die Zahl der Quantorenwechsel von ϕ. Sei

$$\phi = \forall x_1 \dots \forall x_m \exists y_1 \dots \exists y_n \chi(x_1, \dots, y_n),$$

wobei χ (höchstens) mit einem $\forall$–Quantor beginnt. Wir führen jetzt neue m–stellige Funktionszeichen $f_1, \dots, f_n$ ein und sehen, daß ϕ genau in den Strukturen gilt, die sich zu einem Modell von

$$\phi' = \forall x_1 \dots \forall x_m\, \chi\big(x_1, \dots, x_m, f_1(x_1, \dots, x_m), \dots, f_n(x_1, \dots, x_m)\big)$$

expandieren lassen.[12]. ϕ' hat zwei Quantorenwechsel weniger als ϕ. Jetzt verfahren wir mit ϕ' ebenso und erhalten schließlich die Skolem–Normalform. $\square$

[11] ϕ und ψ heißen äquivalent, wenn $\phi \leftrightarrow \psi$ allgemeingültig ist.
[12] Wenn $m = 0$, führen wir neue Konstanten ein.

Man nennt die neu eingeführten Funktionszeichen in L^* *Skolemfunktionen*.

Beispiel: Sei
$$\phi = \forall x\, \big(\exists y\, R(x,y) \wedge \forall z\, \exists w\, S(x,z,w)\big).$$
Die pränexe Normalform ist (z.B.)
$$\forall x\, \exists y\, \forall z\, \exists w\, \big(R(x,y) \wedge S(x,z,w)\big).$$
Der erste Umformungsschritt liefert
$$\forall x, z\, \exists w\, \big(R(x,f(x)) \wedge S(x,z,w)\big)$$
und der zweite
$$\phi^* = \forall x, z, w\, \big(R(x,f(x)) \wedge S(x,z,g(x,z))\big).$$

Folgerung 6.2 (Herbrand–Normalform) *Zu jeder L–Aussage ϕ kann man eine Spracherweiterung L^* und einen existentiellen L^*–Satz ϕ_* angeben, der genau dann allgemeingültig ist, wenn ϕ allgemeingültig ist.*

Wichtig ist, daß man ϕ_* explizit angeben kann. Die reine Existenz ist trivial. Man nimmt für ϕ_* entweder $\exists x\, x \doteq x$ oder $\exists x \neg\, x \doteq x$, jenachdem ob ϕ erfüllbar ist oder nicht.

Beweis:

ϕ ist genau dann allgemeingültig, wenn $\neg\, \phi$ nicht erfüllbar ist. Man setzt also $\phi_* = \neg\, (\neg\, \phi)^*$. □

Bemerkung *Wir finden immer ein ϕ_* ohne Gleichheitszeichen.*

Beweis:

Wegen Lemma 4.8 können wir annehmen, daß ϕ kein Gleichheitszeichen enthält. Im eben konstruierten ϕ^* gibt es dann ebenfalls kein Gleichheitszeichen. □

Für die Allgemeingültigkeit existentieller Aussagen gibt es ein einfaches Kriterium.

Satz 6.3 (Satz von Herbrand) *Sei*
$$\phi = \exists x_1 \ldots \exists x_n \psi(x_1, \ldots, x_n)$$
eine existentielle Aussage für eine Sprache L, die mindestens eine Konstante enthält. Dann ist ϕ genau dann allgemeingültig, wenn es konstante Terme
$$t_1^1, t_2^1, \ldots t_n^1 \ldots t_1^N, t_2^N, \ldots t_n^N$$
gibt, für die die quantorenfreie Aussage
$$\bigvee_{i=1}^{N} \psi(t^i) = \psi(t_1^1, t_2^1, \ldots t_n^1) \vee \ldots \vee \psi(t_1^N, t_2^N, \ldots t_n^N)$$
allgemeingültig ist.

Beweis:
Weil ϕ aus $\bigvee_{i=1}^{N} \psi(t^i)$ folgt, ist ϕ allgemeingültig,wenn $\bigvee_{i=1}^{N} \psi(t^i)$ allgemeingültig ist.
Nehmen wir umgekehrt an, an, daß $\bigwedge_{i=1}^{N} \neg\, \psi(t^i)$ für jede beliebige Wahl der t_j^i erfüllbar ist. Dann ist die Theorie

$$T = \big\{ \neg\, \psi(t_1, \ldots, t_n) \bigm| t_1, \ldots, t_n \text{ konstante Terme} \big\}$$

endlich erfüllbar. T hat nach dem Kompaktheitssatz ein Modell $\mathfrak{A}$. Sei $A_0 = \big\{ t^{\mathfrak{A}} \bigm| t \text{ konstanter Term} \big\}$ die Menge der Elemente von A, die von konstanten Termen dargestellt werden. A_0 ist nicht–leer und unter den auf $\mathfrak{A}$ definierten Operationen abgeschlossen. Wenn wir die Interpretation von L in $\mathfrak{A}$ auf A_0 einschränken, erhalten wir also eine *Unterstruktur* $\mathfrak{A}_0$, in der $\forall x_1 \ldots x_n \neg\, \psi(x_1 \ldots x_n)$ gilt und ϕ daher falsch ist. □

Beispiel: Wir betrachten die Aussage $\phi = \exists w \forall x\, R(w, x) \to \forall z \exists y\, R(y, z)$. Eine pränexe Normalform ist $\forall w \exists x \forall z \exists y\, (\neg\, R(w, x) \vee R(y, z))$ und die Herbrand–Normalform $\phi_* = \exists x \exists y\, (\neg\, R(c, x) \vee R(y, f(x))$. Wenn wir x, y zum einen durch c, c und zu anderen durch $f(c), c$ ersetzen, erhalten wir die allgemeingültige Disjunktion

$$\big(\neg\, R(c, c) \vee R(c, f(c)\big) \vee \big(\neg\, R(c, f(c)) \vee R(c, f(f(c))\big).$$

Also ist ϕ_* und daher auch ϕ allgemeingültig.

Wenn in ψ das Gleichheitszeichen nicht vorkommt, ist die Allgemeingültigkeit von $\bigvee_{i=1}^{N} \psi(t^i)$ ein reines Problem der Aussagenlogik. Eine quantorenfreie Aussage ϕ ohne Gleichheitszeichen ist genau dann allgemeingültig, wenn sie eine aussagenlogische Tautologie ist. Anders ausgedrückt: Man ersetzt jede in ϕ enthaltene Primformel $R(s_1, \ldots, s_m)$ durch eine Aussagenvariable $p_{R(s_1, \ldots, s_m)}$. Die resultierende aussagenlogische Formel ist genau dann allgemeingültig, wenn ϕ allgemeingültig ist.

Es gibt drei Methoden, von einer aussagenlogischen Formel f festzustellen, ob sie allgemeingültig oder –dual– erfüllbar ist:

1. <u>Wahrheitstafeln</u> Sei M die Menge aller in f vorkommenden Variablen und (μ_i) eine Liste aller Belegungen $\mu \to \{\mathrm{W}, \mathrm{F}\}$. Dann ist f genau dann erfüllbar, wenn man ein μ_i findet mit $\mu_i(f) = \mathrm{W}$.

2. <u>Disjunktive Normalform</u> Man bringt f in disjunktive Normalform

   $$\bigvee_{i=1}^{N} g_i,$$

   (wobei die g_i Konjunktionen von Variablen und negierten Variablen sind.). Dann ist f genau dann erfüllbar, wenn eines der g_i erfüllbar ist. g_i ist erfüllbar, wenn in g_i nicht eine Variable zusammen mir ihrer Negation vorkommt.

3. Konjunktive Normalform Man bringt f in konjunktive Normalform

$$\bigwedge_{i=1}^{N} c_i,$$

wobei die c_i Disjunktionen von (negierten) Variablen sind, sogenannte *Klauseln*. Dann verwendet man die unten beschrieben *Resolutionsmethode*: Wir schließen die Menge $\mathcal{C} = \{c_i \mid i = 1, \ldots, N\}$ der Klauseln unter Resolutionen ab. Wenn die leere Klausel (die leere Disjunktion) nicht in der resultierendem Menge $\mathcal{C}'$ vorkommt, ist ϕ erfüllbar, sonst nicht.

Definition *Nehmen wir an, daß in der Klausel c^+ die Variable p positiv und in der Klausel c^- negativ vorkommt. Daß also bis auf die Reihenfolge $c^+ = p \vee c_0^+$ und $c^- = \neg\, p \vee c_0^-$. Dann sagen wir, daß*

$$c_0^+ \vee c_0^-$$

eine Resolution von c^+ und c^- ist.

Die Resolution der beiden Klauseln p und $\neg\, p$ ist die (immer falsche) leere Klausel F.

Lemma 6.4 *Sei $\mathcal{C}$ eine erfüllbare Menge von Klauseln und c eine Resolution von zwei Klauseln c^+ und c^- aus $\mathcal{C}$. Dann ist auch $\mathcal{C} \cup \{c\}$ erfüllbar.*

Beweis:

Sei μ eine Belegung der Variablen, die alle Klauseln aus $\mathcal{C}$ wahr macht. Wenn $\mu(p) = \mathrm{W}$, ist $\mu(c^+) = \mathrm{W}$, sonst ist $\mu(c^-) = \mathrm{W}$. In beiden Fällen folgt $\mu(c) = \mathrm{W}$. $\square$

Satz 6.5 (Resolutionsmethode) *Eine unter Resolutionen abgeschlossene Menge von Klauseln ist genau dann erfüllbar, wenn sie die leere Klausel nicht enthält.*

Beweis:

Sei p eine der in $\mathcal{C}$ vorkommenden Variablen. Sei $\mathcal{C}^+$ die Menge der $c \in \mathcal{C}$, in denen $\neg\, p$ nicht als Konjunktionsglied vorkommt und $\mathcal{C}^-$ die Menge der $c \in \mathcal{C}$, in denen p nicht vorkommt. Wir bilden $\mathcal{C}_0^+$ und $\mathcal{C}_0^-$, indem wir p und $\neg\, p$ aus den Klauseln von $\mathcal{C}^+$ und $\mathcal{C}^-$ entfernen. Beide Mengen sind wieder unter Resolutionen abgeschlossen. Weil $\mathcal{C}$ nicht die leere Klausel enthält, kann nicht sowohl $\mathcal{C}^+$ die Klausel p als auch $\mathcal{C}^-$ die Klausel $\neg\, p$ enthalten. Also können nicht beide Mengen $\mathcal{C}_0^+$ und $\mathcal{C}_0^-$ die leere Klausel enthalten. Wenn wir unseren Beweis induktiv über die Zahl der vorkommenden Variablen führen, wissen wir, daß $\mathcal{C}_0^+$ oder $\mathcal{C}_0^-$ erfüllbar ist. Im ersten Fall belegen wir zusätzlich p mit dem Wert F, im zweiten Fall mit W und erhalten jedesmal ein Modell von $\mathcal{C}$.
Wir haben hier angenommen, daß $\mathcal{C}$ nur endlich viele Variable enthält. Was zu der intendierten Anwendung des Satzes paßt. Wenn $\mathcal{C}$ unendlich viele Variablen

enthält verwenden wir den Kompaktheitssatz. □

Wenn man eine endliche Menge von Klauseln unter Resolutionen abschließt, erhält man im allgemeinen unendlich viele neue Klauseln, weil wir Klauseln, in denen eine Variable mehrere Male vorkommt, nicht ausgeschlossen haben. Wir nennen eine Klausel *reduziert*, wenn in ihr keine Variable doppelt vorkommt. Man erhält aus einer Menge von Klauseln eine äquivalente Menge von reduzierten Klauseln, indem man Klauseln, in denen eine Variable positiv und negativ vorkommt, wegläßt und in allen Klauseln doppelte Vorkommen von Variablen mit dem gleichen Vorzeichen streicht.

Eine Menge $\mathcal{C}$ von reduzierten Klauseln nennen wir *reduziert abgeschlossen*, wenn jede reduzierte Klausel, die aus der einer Resolution zweier Klauseln aus $\mathcal{C}$ durch Streichen doppelter Vorkommen von Variablen mit dem gleichen Vorzeichen entsteht, wieder zu $\mathcal{C}$ gehört. Man sieht nun leicht:

Bemerkung *Sei $\mathcal{C}$ reduziert abgeschlossen. Wenn $\mathcal{C}$ die leere Klausel nicht enthält, enthält der Abschluß von $\mathcal{C}$ unter Resolutionen ebenfalls nicht die leere Klausel.*

Beweis:

$\mathcal{C}'$ sei die Menge aller Klauseln in den Variablen von $\mathcal{C}$, die eine Klausel aus $\mathcal{C}$ als Teilklausel enthalten oder in denen eine Variable positiv und negativ vorkommt. $\mathcal{C}'$ ist unter Resolutionen abgeschlossen. □

Die Resolutionsmethode liefert dual eine Kriterium für die Allgemeingültigkeit von aussagenlogischen Formeln in disjunktiver Normalform: Sei $\mathcal{C}$ eine Menge von Konjunktionen von (eventuell negierten) Aussagenvariablen. Wir sagen, daß $\mathcal{C}$ unter Resolutionen abgeschlossen ist, wenn $\mathcal{C}$ mit zwei Konjunktionen $p \wedge c^+$ und $\neg\, p \wedge c^-$ auch die Konjunktion $c^+ \wedge c^-$ enthält.

Folgerung 6.6 *Die Menge $\mathcal{C}$ sei unter Resolutionen abgeschlossen. Dann ist $\bigvee \mathcal{C}$ genau dann allgemeingültig, wenn $\mathcal{C}$ die leere Konjunktion* W *enthält.*

Wenn man den Satz von Herbrand (6.3) verwenden will, um die Allgemeingültigkeit einer Aussage $\phi = \exists x_1 \ldots \exists x_n \psi(x_1, \ldots, x_n)$ ohne Gleichheitszeichen zu zeigen, bringt man ψ in disjunktive Normalform und wählt dann Terme t^i_j, für die man die letzte Folgerung auf $\bigvee_{i=1}^N \psi(t^i)$ anwenden kann. Die Terme wählt man so, daß genügend viele Formelpaare

$$R(s^1_1(x_1, \ldots, x_n), \ldots, s^1_k(x_1, \ldots, x_n))$$

und

$$R(s^2_1(x_1, \ldots, x_n), \ldots, s^2_k(x_1, \ldots, x_n)),$$

in den Disjunktionsgliedern von ψ *gleich* werden, wenn man die x_j durch die t^1_j bzw. t^2_j ersetzt.

Man verwendet dazu die *Unifikationsmethode*. Seien

$$S^1(x_1, \ldots, x_n) = \big(s^1_1(x_1, \ldots, x_n), \ldots, s^1_k(x_1, \ldots, x_n)\big)$$

und

$$S^2(x_1,\dots,x_n) = \big(s^2_1(x_1,\dots,x_n),\dots,s^2_k(x_1,\dots,x_n)\big)$$

zwei gleichlange Folgen von Termen. Eine Termfolge $T = (t_1,\dots,t_n)$ *unifiziert* S^1 und S^2, wenn

$$S^1(t_1,\dots,t_n) = S^2(t_1,\dots,t_n).$$

Satz 6.7 (Unifikation) *Wenn S^1 und S^2 unifizierbar sind, gibt es eine* universelle *unifizierende Termfolge $U(y_1,\dots,y_m)$. Das heißt, daß eine Termfolge T genau dann S^1 und S^2 unifiziert, wenn es Terme $t_1,\dots,t_m$ gibt, sodaß*

$$T = U(t_1,\dots,t_m).$$

Man kann U durch ein einfaches Verfahren finden, das gleichzeitig entscheidet, ob S^1 und S^2 unifizierbar sind.

Beweis:

Wir fassen das Paar S^1, S^2 als eine Menge

$$S(x_1,\dots,x_n) = \{s^1_1 \doteq s^2_1,\dots,s^1_k \doteq s^2_k\}$$

von Gleichungen auf. T unifiziert S, wenn alle Gleichungen aus $S(T)$ allgemeingültig sind. Unser Unifikationsverfahren formt S in äquivalente Gleichungssysteme um. Dabei wenden wir, solange es geht, die folgenden Schritte A und B an.

Schritt A:
Wenn S eine Gleichung $f^1(t^1_1,\dots,t^1_{l^1}) \doteq f^2(t^2_1,\dots,t^2_{l^2})$ enthält, gibt es zwei Möglichkeiten:

- Wenn $f^1 \neq f^2$, ist S nicht unifizierbar und das Verfahren bricht ab.
- Wenn $f^1 = f^2$ (und daher $l^1 = l^2 = l$), ersetzen wir die Gleichung durch die Gleichungen $t^1_1 \doteq t^2_1$, ..., $t^1_l \doteq t^2_l$.

Schritt B:
Wenn S eine Gleichung $x_i \doteq s$ enthält[13], gibt es drei Möglichkeiten:

- $s = x_i$. Dann streichen wir die Gleichung einfach.
- s ist ein zusammengesetzter Term, in dem x_i vorkommt. Dann ist S nicht unifizierbar und das Verfahren bricht ab.
- x_i kommt in s nicht vor. Dann ersetzen wir in allen *anderen* Gleichungen die Variable x_i durch s.

[13] Wir unterscheiden diese Gleichung nicht von $s \doteq x_i$.

Wenn das Verfahren nicht mit dem Ergebnis, daß eine Unifikation unmöglich sei, abbricht, hat das Gleichungssystem – nach Umnumerierung der Variablen – die Form

$$x_m \doteq u_m(x_1, \ldots, x_{m-1}), \ldots,\ x_n \doteq u_n(x_1, \ldots, x_{m-1})$$

für ein $1 \leq m \leq n+1$. Die gesuchte universelle unifizierende Termfolge ist dann

$$x_1, \ldots, x_{m-1}, u_m, \ldots, u_n.$$

$\square$

Beispiel:
Wir wollen die beiden Terme

$$k(x_1, x_1, x_4) \text{ und } k(f(c, g(x_2, x_3)), f(c, g(x_3, x_2)), k(x_3, x_2, x_1))$$

unifizieren. Wir beginnen also mit der Gleichung

$$k(x_1, x_1, x_4) \doteq k(f(c, g(x_2, x_3), f(c, g(x_3, x_2)), k(x_3, x_2, x_1)).$$

Schritt A:

$$\begin{array}{rcl} x_1 & \doteq & f(c, g(x_2, x_3)) \\ x_1 & \doteq & f(c, g(x_3, x_2)) \\ x_4 & \doteq & k(x_3, x_2, x_1) \end{array}$$

Schritt B (ersetze x_1 durch $f(c, g(x_2, x_3))$):

$$\begin{array}{rcl} x_1 & \doteq & f(c, g(x_2, x_3)) \\ f(c, g(x_2, x_3)) & \doteq & f(c, g(x_3, x_2)) \\ x_4 & \doteq & k(x_3, x_2, f(c, g(x_2, x_3))) \end{array}$$

Schritt A:

$$\begin{array}{rcl} x_1 & \doteq & f(c, g(x_2, x_3)) \\ x_2 & \doteq & x_3 \\ x_3 & \doteq & x_2 \\ x_4 & \doteq & k(x_3, x_2, f(c, g(x_2, x_3))) \end{array}$$

Schritt B (ersetze x_2 durch x_3):

$$\begin{array}{rcl} x_1 & \doteq & f(c, g(x_2, x_3)) \\ x_2 & \doteq & x_3 \\ x_4 & \doteq & k(x_3, x_3, f(c, g(x_3, x_3))) \end{array}$$

Es ergibt sich die universelle Lösung

$$f(c, g(x_3, x_3)),\ x_3,\ x_3,\ k(x_3, x_3, f(c, g(x_3, x_3))).$$

Folgerung 6.8 *Sei $\psi(x_1, \ldots, x_n)$ eine quantorenfreie L–Formel ohne Gleichheitszeichen und N eine natürliche Zahl*[14]*. Man kann effektiv entscheiden, ob es konstante Terme*

$$t_1^1, t_2^1, \ldots t_n^1 \ldots t_1^N, t_2^N, \ldots t_n^N$$

gibt, für die

$$\bigvee_{i=1}^{N} \psi(t^i) = \psi(t_1^1, t_2^1, \ldots t_n^1) \vee \ldots \vee \psi(t_1^N, t_2^N, \ldots t_n^N)$$

allgemeingültig ist. □

[14] Der Fall $N = 1$ impliziert sofort die Folgerung für beliebiges N. Wir haben diese Fomulierung gewählt, wegen des Zusammenhangs mit Satz 6.3.

Kapitel 2

Mengenlehre

7 Die Axiome

Die Sprache der Mengenlehre ist $L_{Me} = \{\epsilon\}$. Man liest „$x \epsilon y$" als *x ist Element von y*.

Die Axiome der *Naiven Mengenlehre* sind das Extensionalitätsaxiom: Zwei Mengen sind gleich, wenn sie die gleichen Elemente haben. Und das Schema der vollen Komprehension: Jede definierbare Klasse von Mengen ist die Klasse der Elemente einer Menge. In Formeln:

Axiom (Extensionalität)

$$\forall x, y \left(\forall z \ (z \epsilon x \leftrightarrow z \epsilon y) \to x \doteq y\right)$$

Axiom (Volle Komprehension) *Für alle Formeln $\phi(x, y_1, \ldots, y_n)$*

$$\forall y_1 \ldots y_n \exists x \forall z \ (z \epsilon x \leftrightarrow \phi(z, y_1, \ldots, y_n))$$

(Um genau zu sein: Das Komprehensionsaxiom ist nicht ein einzelnes Axiom, sondern ein Axiomenschema)

Das volle Komprehensionsaxiom sagt, daß für jede Formel $\phi(z, y_1, \ldots, y_n)$ und fixierte Parameter $y_1, \ldots, y_n$ die Klasse

$$\left\{z \mid \phi(z, y_1, \ldots, y_n)\right\}$$

eine Menge ist.

Das System aller Mengen, wie wir sie uns vorstellen, scheint tatsächlich diese Axiome zu erfüllen. Es gilt aber die *Russellsche Antinomie*:

Satz 7.1 (Bertrand Russell) *Die naive Mengenlehre ist inkonsistent.*

Beweis:

Betrachte die Formel $\phi(x) = \neg\, x \in x$. Das Komprehensionsschema liefert dann das Axiom

$$\exists x \forall z\ (z \in x \leftrightarrow \neg\, z \in z).$$

Wenn aber x eine Menge mit $\forall z\ (z \in x \leftrightarrow \neg\, z \in z)$ ist, also

$$x = \{z \mid \neg\, z \in z\},$$

liefert die Einsetzung von x für z den Widerspruch $x \in x \leftrightarrow \neg\, x \in x$. □

Es sind verschiedene Modifikationen der Mengenlehre vorgeschlagen worden (z.B. von Quine: *New Foundation*). Durchgesetzt hat sich

ZFC,

die nach ihren Erfindern Zermelo und Fränkel und nach „choice", dem Auswahlaxiom benannt ist.

Hier ist die Liste der Axiome, die wir im folgenden diskutieren:

- Extensionalität
- Aussonderung
- Paarmenge
- Vereinigung
- Potenzmenge
- Ersetzung
- Fundierung
- Unendlichkeit
- Auswahl

ZFC enthält natürlich das Extensionalitätsaxiom:

Axiom (Extensionalität)

$$\forall x, y\, \big(\forall z\ (z \in x \leftrightarrow z \in y) \to x \doteq y\big)$$

Wir führen als „$x \subset y$" als Abkürzung für die Formel $\forall z\ (z \in x \to z \in y)$ ein, gelesen als „x ist Teilmenge von y". Das Extensionalitätsaxiom ist dann gleichbedeutend mit

$$\forall x, y (x \subset y \land y \subset x) \to x \doteq y.$$

Dann folgen fünf Spezialfälle der vollen Komprehension.

Axiom (Aussonderung)

$$\forall y_0 \dots y_n \exists x \forall z \left(z \in x \leftrightarrow (z \in y_0 \wedge \phi(z, y_1, \dots, y_n)) \right)$$

Das Aussonderungsaxiom erlaubt es zum Beispiel den Durchschnitt

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

und die Differenz

$$x \setminus y = \{z \in x \mid \neg\, z \in y\}$$

von zwei Mengen zu bilden. Es ergibt sich auch die Existenz der leeren Menge.

$$\emptyset = \{z \mid \neg\, z \doteq z\}$$

Für eine beliebige Menge x ist nämlich $\emptyset = \{z \in x \mid \neg\, z \doteq z\}$.

Die Russellsche Antinomie wird jetzt ein Theorem von ZFC:

Bemerkung *In* ZFC *ist beweisbar, daß die Klasse* V *aller Mengen keine Menge ist. Formal:*

$$\mathrm{ZFC} \vdash \neg \exists x \forall z\; z \in x$$

Beweis:
Sonst wäre nach dem Aussonderungsaxiom die Russellsche Klasse

$$\{z \mid \neg\, z \in z\} = \{z \in V \mid \neg\, z \in z\}$$

ebenfalls eine Menge, was sofort zu einem Widerspruch führt. □

Das Paarmengenaxiom

Axiom (Paarmenge)

$$\forall y_1, y_2 \exists x \forall z\; z \in x \leftrightarrow (z \doteq y_1 \vee z \doteq y_2)$$

besagt, daß

$$\{x, y\} = \{z \mid z \doteq x \vee z \doteq y\}$$

eine Menge ist, die aus x und y gebildete *Paarmenge*.

Definition *Das geordnete Paar von zwei Mengen x und y ist die Menge*

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

(x, y) heißt *Kuratowski Paar.*

Lemma 7.2 (ZFC)

$$\mathrm{ZFC} \vdash \forall x, y, x', y' \;\; (x, y) \doteq (x', y') \;\rightarrow\; x \doteq x' \wedge y \doteq y'$$

□

Das Vereinigungsmengenaxiom ist

Axiom (Vereinigung)

$$\forall y \exists x \forall z \;\; z \,\epsilon\, x \;\leftrightarrow\; \exists w \, (z \,\epsilon\, w \wedge w \,\epsilon\, y).$$

Wir schreiben

$$\bigcup y = \big\{ z \mid \exists w \, (z \,\epsilon\, w \wedge w \,\epsilon\, y) \big\}.$$

$\bigcup y$ ist die Vereinigung der Elemente von y. Aus dem Paarmengenaxiom und dem Vereinigungsmengenaxiom folgt die Existenz der Vereinigung von zwei Mengen:

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

Man definiert rekursiv über n

$$\{y_1, y_2, \ldots, y_{n+1}\} = \{y_1, \ldots, y_n\} \cup \{y_{n+1}\}.$$

Das Potenzmengenaxiom

Axiom (Potenzmenge)

$$\forall y \exists x \forall z \;\; z \,\epsilon\, x \;\leftrightarrow\; z \subset y$$

postuliert die Existenz der *Potenzmenge*

$$\mathfrak{P}(y) = \{z \mid z \subset y\}.$$

Lemma 7.3 (ZFC) *Aus den Axiomen von* ZFC *folgt für alle a und b die Existenz des direkten Produktes*

$$a \times b = \big\{ (x, y) \mid x \in a \wedge y \in b \big\}.$$

Beweis:

Wenn $x \in a$ und $y \in b$, sind $\{x\}$ und $\{x, y\}$ Elemente von $\mathfrak{P}(a \cup b)$. Dann ist $(x, y) = \{\{x\}, \{x, y\}\}$ ein Element von $\mathfrak{P}(\mathfrak{P}(a \cup b))$. Es folgt, daß $\big\{(x, y) \mid x \in a \wedge y \in b\big\}$ eine definierbare Teilklasse von $\mathfrak{P}(\mathfrak{P}(a \cup b))$ ist. Also eine Menge nach dem Aussonderungsaxiom. □

Wir definieren Tripel durch

$$(x, y, z) = ((x, y), z)$$

und $a \times b \times c = \{(x, y, z) \mid x \in a,\ y \in b,\ z \in c\}$. Entsprechend Viertupel usw.

Eine *Relation* ist nun eine Menge von Paaren. Der Definitionsbereich von R ist

$$\mathrm{dom}(R) = \{x \mid \exists y \, (x, y) \in R\},$$

der Bildbereich

$$\mathrm{Im}(R) = \{y \mid \exists x\, (x, y) \in R\}.$$

Definitions– und Bildbereich sind Mengen, weil sie Teilklassen von $\bigcup\bigcup R$ sind. Denn

$$\{\{x\}, \{x, y\}\} \in R \;\Rightarrow\; \{x, y\} \in \bigcup R \;\Rightarrow\; x, y \in \bigcup\bigcup R.$$

Eine *Funktion* f ist eine rechtseindeutige Relation[1]:

$$\forall x, y_1, y_2 \;\; (x, y_1) \in f \wedge (x, y_2) \in f \;\rightarrow\; y_1 = y_2.$$

Man schreibt dann

$$f(x) = y \;\; (^2)$$

für $(x, y) \in f$. Die Schreibweise

$$f : a \rightarrow b$$

bedeutet $\mathrm{dom}(f) = a$ und $\mathrm{Im}(f) \subset b$. Wenn wir b nicht spezifizieren wollen, schreiben wir $f : a \rightarrow \mathrm{V}$.

$$f \restriction c = f \cap (c \times b)$$

ist die Einschränkung von f auf c.

$$f[c] = \{f(x) \mid x \in c\}$$

ist der Bildbereich von $f \restriction c$.

Axiom (Ersetzung)

$$\forall y, \overline{w} \Big(\forall u \exists !\, z\, \phi(u, z, \overline{w}) \;\;\rightarrow\;\; \exists x \forall z\, \big(z \,\epsilon\, x \leftrightarrow \exists u (u \,\epsilon\, y \wedge \phi(u, z, \overline{w}))\big)\Big)$$

$\overline{w}$ steht hier für ein Tupel von Variablen. $\exists !\; \phi(x)$, *es gibt genau ein* x ..., steht für $\exists x\big(\phi(x) \wedge \forall x'(\phi(x') \rightarrow x \doteq x')\big)$.

Als ein Beispiel überlegen wir, wie wir ohne Verwendung des Potenzmengenaxioms die Existenz von $a \times b$ aus dem Ersetzungsaxiom schließen können: Wir halten zunächst x fest. Dann gilt offenbar

$$\forall u \exists !\, z\; z \doteq (x, u).$$

Also gibt es eine Menge die genau aus den (x, u) mit $u \in b$ besteht. Diese Menge ist natürlich $\{x\} \times b$. Eine zweite Anwendung des Ersetzungsaxioms liefert die Existenz von $c = \big\{\{x\} \times b \mid x \in a\big\}$. Schließlich ist $a \times b = \bigcup c$.

Ein zweites Beispiel: Mit Hilfe des Ersetzungsaxiom sieht man leicht, daß die *inverse* Relation

$$R^{-1} = \big\{(y, x) \;\big|\; (x, y) \in R\big\}$$

eine Menge ist.

Eine Funktion $f : a \rightarrow b$ heißt

[1] Wir identifizieren also eine Funktion mit ihrem Graphen.

[2] Wenn $x \notin \mathrm{dom}(f)$, setzen wir $f(x) = \emptyset$.

surjektiv, wenn $\mathrm{Im}(f) = b$,[3]

injektiv, wenn f^{-1} eine Funktion ist,

bijektiv, wenn f injektiv und surjektiv ist.

Exkurs über definitorische Erweiterungen: Die Einführung von neuen Relations– und Funktionszeichen

Sei T eine L–Theorie und $\phi(x_1, \dots, x_n)$ eine Formel. Wenn wir für ϕ ein neues (n–stelliges) Relationszeichen R einführen, erweitern wir L zu $L' = L \cup \{R\}$ und T zu $T' = T \cup \{\forall x_1, \dots, x_n\ R(x_1, \dots, x_n) \leftrightarrow \phi(x_1, \dots, x_n)\}$. Es ist klar, daß T' sich nicht wesentlich von T unterscheidet. Erstens ist T' eine *konservative Erweiterung* von T, das heißt, daß jede L–Aussage, die in T' beweisbar ist, auch in T beweisbar ist. Zweitens ist jede L'–Formel zu einer L–Formel T'–beweisbar äquivalent.

Die Einführung neuer Funktionszeichen beschreiben wir in einem Satz.

Satz 7.4 *Sei die Funktionalität von ϕ in T beweisbar, also*

$$T \vdash \forall x_1, \dots, x_n \exists!\, x_0 \phi(x_0, \dots, x_n).$$

Sei f ein neues n–stelliges Funktionszeichen und $L' = L \cup \{f\}$. Dann ist die L'–Theorie

$$T' = T \cup \big\{\forall x_1, \dots, x_n \phi(f(x_1, \dots, x_n), x_1, \dots, x_n)\big\}$$

eine konservative Erweiterung von T. Darüberhinaus gibt es zu jeder L'–Formel ψ eine L–Formel ψ^* mit $T' \vdash \psi \leftrightarrow \psi^*$.

Beweis:

Ein T–Modell $\mathfrak{A}$ läßt sich (in genau einer Weise) zu einem T'–Modell expandieren, indem man f durch die Funktion interpretiert, die $a_1, \dots, a_n$ das a_0 zuordnet, für das $\mathfrak{A} \models \phi[a_0, \dots, a_n]$. Daraus folgt, daß T' eine konservative Erweiterung ist.

Die Übersetzung ψ^* definiert man leicht rekursiv über den Aufbau von ψ. Etwas schwerer ist nur der Fall, daß ψ eine Primformel ist. Sei also zum Beispiel $\psi = R(t_1, t_2)$. Wenn f zum Beispiel in t_1 vorkommt, schreiben wir

$$t_1 = s_0(f(s_1, \dots, s_n))$$

für L'–Terme $s_0, \dots, s_n$ und setzen

$$\psi^* = \exists x_0 \big(\phi(x_0, s_1, \dots, s_n) \wedge R(s_0(x_0), t_2)^*\big).$$

$\square$

Satz 7.4 ist auch sinnvoll für $n = 0$. Wir führen dann allerdings kein Funktionszeichen sondern eine neue Konstante ein.

[3] Surjektivität und Bijektivität sind nicht Eigenschaften von f allein, sondern Eigenschaften des Paares f, b.

Definition *Eine Erweiterung einer Theorie durch definierte Relationszeichen, Funktionszeichen und Konstanten heißt definitorische Erweiterung.*

Man kann leicht zeigen, daß konservative Erweiterungen T', für die jede L'–Formel zu einer L–Formel T'–beweisbar äquivalent ist, definitorisch sind.

Beispiele:

Relationszeichen:	$x \subset y$	$f : a \to b$	
Funktionszeichen:	$\{z \in x \mid \phi(z, y_1, \ldots, y_n)\}$	$x \cup y$	$x \cap y$
	$x \setminus y$	$\bigcup y$	$\mathfrak{P}(y)$
	$\{x, y\}$	$\{y_1, \ldots, y_n\}$	(x, y)
	$x \times y$	$\mathrm{dom}(R)$	$\mathrm{Im}(R)$
	R^{-1}	$f(x)$	$f[x]$
	$f \restriction y$		
Konstantenzeichen:	$\emptyset$		

Folgerung 7.5 *Aussonderungsaxiom und Ersetzungsaxiom bleiben gültig, wenn ϕ neu eingeführte Relationszeichen, Funktionszeichen und Konstanten enthält.*

In unserer Mengenlehre sind die Elemente von Mengen wieder Mengen. Demgemäß sind die einzigen Mengen, die wir konkret angeben können, letztlich aus der leeren Mengen aufgebaut: $\emptyset$, $\{\emptyset, \{\emptyset\}\}$, usw. Wir nennen eine aus der leeren Menge aufgebaute Menge *fundiert*. Die folgende Definition ist noch unpräzise, weil wir den Begriff der unendlichen Folge noch nicht eingeführt haben.

Definition (informell) *Eine Menge x heißt fundiert, wenn jede bei x anfangende absteigende $\in$–Kette*

$$x \ni y_0 \ni y_1 \ni \ldots$$

nach endlich vielen Schritten abbricht.

Das Fundierungsaxiom drückt aus, daß jede Menge fundiert ist:

Axiom (Fundierung)

$$\forall x(\neg\, x \doteq \emptyset \;\to\; \exists z \,\epsilon\, x \; z \cap x \doteq \emptyset)$$

Das läßt sich (informell[4]) folgendermaßen einsehen: Wenn x das Axiom nicht erfüllt, hat jedes Element von x ein Element, das wieder zu x gehört. Man findet also (mit dem Auswahlaxiom) eine unendliche $\in$–Kette von Elementen von x. Wenn umgekehrt $y_0 \ni y_1 \ldots$ eine unendliche $\in$–Kette ist, verletzt $x = \{y_0, y_1, \ldots\}$ das Fundierungsaxiom.

Folgerung 7.6 *Eine Menge kann sich nicht selbst als Element enthalten.*

[4]Man kann diese Schlußweise erst präzise machen, wenn die natürlichen Zahlen eingeführt sind.

Daraus ergibt sich ein zweiter Beweis dafür, daß V keine Menge ist. Sonst wäre nämlich $V \in V$.

Es gibt drei Rechtfertigungen für die Annahme des Fundierungsaxioms:

1. Unheimliche Mengen, wie solche, die nur sich selbst als Element enthalten (!!!), werden ausgeschlossen.
2. Man kann mit Hilfe der übrigen Axiome zeigen, daß es zu jeder Menge eine Bijektion mit einer fundierten Menge gibt. Fundierte Mengen genügen also, um Mathematik zu betreiben.
3. Sei (M, E) ein Modell aller Axiome von ZFC bis auf das Fundierungsaxiom. Setze $N = \{m \in M \mid (M, E) \models m \text{ ist fundiert}\}$. Dann ist $(N, E \cap N^2)$ ein Modell von ZFC, das zusätzlich das Fundierungsaxiom erfüllt.

Die letzten beiden Axiome diskutieren wir in den nächsten Abschnitten.

Axiom (Unendlichkeit)

$$\exists x \big(\emptyset \mathrel{\epsilon} x \ \wedge \ \forall z \mathrel{\epsilon} x \ z \cup \{z\} \mathrel{\epsilon} x\big)$$

Axiom (Auswahl)

$$\forall x \big(\neg\, \emptyset \mathrel{\epsilon} x \rightarrow \ \exists f : x \rightarrow \mathrm{V} \ \ \forall z \mathrel{\epsilon} x \ f(z) \mathrel{\epsilon} z\big)$$

8 Die natürlichen Zahlen

Die rekursive Definition

$$\underline{n} = \{\underline{0}, \underline{1}, \ldots, \underline{n-1}\}$$

ordnet jeder natürlichen Zahl n eine Menge $\underline{n}$ zu. Es ist zum Beispiel

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

Wir schreiben im folgenden $\mathrm{s}(x)$ für die *Nachfolgeroperation* $x \cup \{x\}$. In ZFC ist dann für alle n beweisbar, daß

$$\underline{n+1} = \mathrm{s}(\underline{n}).$$

Man zeigt leicht durch Induktion:

Lemma 8.1 *Wenn $m < n$ ist*

$$\mathrm{ZFC} \vdash \neg\, \underline{m} \doteq \underline{n}.$$

□

Folgerung 8.2 *Für alle n, m ist*

$$\begin{aligned} m < n &\implies \mathrm{ZFC} \vdash \underline{m} \in \underline{n} \\ m \geq n &\implies \mathrm{ZFC} \vdash \neg\, \underline{m} \in \underline{n} \end{aligned}$$

Weil wir noch nicht wissen, wie man rekursive Definitionen in ZFC ausdrückt, ist dadurch der formale Begriff *natürliche Zahl* noch nicht definiert. Wir brauchen dazu:

Definition (ZFC) *Sei $<$ eine Relation auf*[5] *a.*

1. *$<$ ist eine partielle Ordnung , wenn*
   a) *$<$ irreflexiv ist: $\neg\, x < x$ für alle $x \in a$.*
   b) *$<$ transitiv ist: $x < y \wedge y < z \rightarrow x < z$ für alle $x, y, z \in a$.*
2. *Eine partielle Ordnung $<$ auf a heißt linear, wenn für alle $x, y \in a$*

$$x < y \vee x \doteq y \vee y < x.$$

Definition (ZFC) *Eine Menge x heißt transitiv, wenn alle ihre Element auch Teilmengen sind:*

$$z \in y \in x \;\rightarrow\; z \in x.$$

[5]Eine Relation auf a ist eine Teilmenge von $a \times a$.

x ist genau dann transitiv, wenn $\bigcup x \subset x$.

Definition (ZFC) *x heißt natürliche Zahl, wenn*

1. *x transitiv ist,*
2. *$\in$ eine lineare Ordnung auf x definiert*
3. *und jede nicht–leere Teilmenge von x bezüglich dieser Ordnung ein kleinstes und ein größtes Element besitzt.*

Daß jede nicht–leere Teilmenge von x ein bezüglich $\in$ minimales Element hat, folgt schon aus dem Fundierungsaxiom und brauchte in der Definition nicht eigens gefordert zu werden. Wir haben diese Bedingung einerseits aufgenommen, weil eine Menge mit einer linearen Ordnung genau dann endlich (siehe S.54) ist, wenn jede nicht–leere Teilmenge ein kleinstes und ein größtes Element hat. Anderseits hat man so auch in Abwesenheit des Fundierungsaxioms die richtige Definition.

$\in$ ist schon eine lineare Ordnung von x, wenn die Elemente von x bezüglich $\in$ vergleichbar sind. Denn $\in$ ist irreflexiv nach dem Fundierungsaxiom. $\in$ ist transitiv auf x, weil $a \in b \in c \in x$ zur Folge hat, daß $a \neq c$ und $c \notin a$ und daher $a \in c$.

Lemma 8.3 (ZFC)

1. *Eine natürliche Zahl besteht aus natürlichen Zahlen.*
2. *$\underline{0}$ ist eine natürliche Zahl. Wenn x eine natürliche Zahl ist, ist auch* $\mathrm{s}(x)$ *eine natürliche Zahl.*
3. *Jede natürliche Zahl $\neq \underline{0}$ hat die Form* $\mathrm{s}(y)$ *für eine natürliche Zahl y.*

2. impliziert, daß alle $\underline{n}$ natürliche Zahlen sind. Aus 3. folgt (informell), daß man jede natürliche Zahl aus $\emptyset$ mit endlichen vielen Anwendungen der Operation s gewinnen kann.

Beweis:

1: Sei x eine natürliche Zahl und y ein Element von x. $\in$ ordnet y ebenfalls linear und jede nicht–leere Teilmenge von y hat bezüglich $\in$ ein kleinstes und ein größtes Element. Zu zeigen bleibt, daß y transitiv ist. Das folgt aber sofort aus der Transitivität von $\in$ auf x.

2: Leicht.

3: Wenn die natürliche Zahl x nicht leer ist, hat x ein $\in$–größtes Element y. Es ist also

$$x = \{z \mid z \in y \vee z \doteq y\} = \mathrm{s}(y).$$

□

Wir bezeichnen mit ω die Klasse der natürlichen Zahlen.

Lemma 8.4 (ZFC) *ω ist eine Menge.*

Beweis:

Sei x eine Menge wie im Unendlichkeitsaxiom. Wir zeigen, daß ω eine Teilmenge von x ist. Die Behauptung folgt dann aus dem Aussonderungsaxiom. Nehmen wir an, es gäbe ein a aus $\omega \setminus x$. Sei b das kleinste Element von $\mathrm{s}(a)$, das nicht zu x gehört. Dann sind alle Elemente von b (die ja selbst wieder zu ω gehören) Elemente von x. Weil $b \notin x$, ist b nicht leer. Also hat b die Form $\mathrm{s}(c)$. Dann ist $c \in x$, woraus aber auch $b \in x$ folgt. Ein Widerspruch. □

Aus dem Beweis folgt:

Folgerung 8.5 (ZFC, **Induktion**) *Eine Menge von natürlichen Zahlen, die $\underline{0}$ enthält und unter s abgeschlossen ist, besteht aus allen natürlichen Zahlen.*

Wir schreiben $<$ für die $\in$–Relation zwischen natürlichen Zahlen.

Lemma 8.6

1. *$<$ ist eine lineare Ordnung auf ω. Jede nicht–leere Teilmenge von ω hat ein kleinstes Element.*
2. *Für alle $n \in \omega$ ist $\mathrm{s}(n)$ der unmittelbare Nachfolger[6] von n.*
3. *Alle $n > \underline{0}$ haben einen unmittelbaren Vorgänger.*

1. sagt, daß $<$ eine *Wohlordnung* auf ω ist.

Beweis:

Alle Aussagen sind leicht zu beweisen, außer der Vergleichbarkeit von je zwei natürlichen Zahlen. Sei also $m \in \omega$ festgehalten. Wir zeigen durch Induktion, daß alle $n \in \omega$ mit m vergleichbar sind.
Zuerst müssen wir zeigen, daß $\underline{0}$ mit m vergleichbar ist. Wenn $m \neq \underline{0}$, hat m ein kleinstes Element m_0. Weil die Elemente von m_0 auch Elemente von m sind, muß $m_0 = \underline{0}$ sein.
Jetzt nehmen wir an, daß n mit m vergleichbar ist, und zeigen, daß auch $\mathrm{s}(n)$ mit m vergleichbar ist. Das ist klar, wenn $m \leq n$[7]. Wenn $n < m$, sei n_0 der unmittelbare Nachfolger von n in der linearen Ordnung von $\mathrm{s}(m)$. Es ist also $n_0 \leq m$ und die Elemente von n_0 sind genau die Elemente von n und n selbst. Das heißt aber $n_0 = \mathrm{s}(n)$ und daher $\mathrm{s}(n) \leq m$. □

Um $+$ und $\cdot$ definieren zu können, brauchen wir den Rekursionssatz für ω.

Satz 8.7 (ZFC, **Rekursionssatz**) *Seien zwei Funktionen $g : A \to B$ und $h : A \times \omega \times B \to B$ gegeben. Dann existiert ein, eindeutig bestimmtes, $f : A \times \omega \to B$ mit*

$$\begin{aligned} f(a, \underline{0}) &= g(a) \\ f(a, \mathrm{s}(n)) &= h(a, n, f(a, n)) \end{aligned}$$

für alle $a \in A$ und $n \in \omega$

[6] d.h. $\mathrm{s}(n)$ ist die kleinste Zahl, die größer als n ist.
[7] Hier und später ist $x \leq y$ eine Abkürzung für $x < y \vee x \doteq y$.

Beweis:
Wir halten $a \in A$ fest. Man zeigt leicht durch Induktion über m, daß es für alle $m \in \omega$ genau ein $f' : s(m) \to B$ gibt mit $\phi(a, m, f')$, wobei

$$\phi(a, m, f') \;=\; \big(f'(\underline{0}) \doteq g(a) \;\wedge\; \forall n < m \; f'(\mathrm{s}(n)) \doteq h(a, n, f'(n))\big).$$

Wir definieren jetzt

$$f = \big\{(a, m, b) \in (A \times \omega \times B) \;\big|\; \exists f' \; \phi(a, m, f') \wedge f'(m) \doteq b\big\}.$$

$\square$

Definition *Addition* $+ : \omega \times \omega \to \omega$ *und Multiplikation* $\cdot : \omega \times \omega \to \omega$ *werden definiert durch die Rekursionsgleichungen*

$$\begin{aligned} a + \underline{0} &= a \\ a + \mathrm{s}(n) &= \mathrm{s}(a + n) \\ a \cdot \underline{0} &= \underline{0} \\ a \cdot \mathrm{s}(n) &= (a \cdot n) + a. \end{aligned}$$

Rechenregeln wie

$$m + n = n + m$$

beweist man leicht durch Induktion.

9 Ordinalzahlen und Kardinalzahlen

Definition *Eine Ordinalzahl ist eine transitive Menge, die durch $\in$ linear geordnet wird.*

Alle natürlichen Zahlen und ω sind Ordinalzahlen. Wir bezeichnen mit On die Klasse der Ordinalzahlen.

Lemma 9.1

1. On *wird durch $\in$ linear geordnet. (Wir nennen diese lineare Ordnung $<$.)*
2. *Jede nicht–leere Teilklasse von* On *hat ein minimales Element.*
3. *Jede Ordinalzahl α ist die Menge ihrer Vorgänger:*

$$\alpha = \{\beta \in \mathrm{On} \mid \beta < \alpha\}$$

4. On *ist keine Menge.*

Beweis:

Sei $S \subsetneq \alpha$ ein echtes Anfangsstück (d.h. $x < y \in S \rightarrow y \in S$) von α und $\beta \in \alpha$ das kleinste Element von $\alpha \setminus S$. Dann ist offensichtlich $\beta = S$. Wenn nun α und β zwei Ordinalzahlen sind, ist $S = \alpha \cap \beta$ ein Anfangsstück von α und β. S kann nicht sowohl von α als auch von β verschieden sein, weil sonst S selbst ein Element von α und β sein müßte. Wenn aber $S = \alpha$, ist $\alpha \leq \beta$, und wenn $S = \beta$, ist $\beta \leq \alpha$. Daraus folgt, daß alle Ordinalzahlen vergleichbar sind. Wie auf Seite 47 folgt, daß $\in$ die Klasse aller Ordinalzahlen linear ordnet.
Daß jede nicht–leere Teilklasse von On ein minimales Element hat, folgt sofort aus dem Fundierungsaxiom.
3. bedeutet lediglich, daß Ordinalzahlen aus Ordinalzahlen bestehen. Das zeigt man aber wie Lemma 8.3 (1).
Wenn On ein Menge wäre, wäre On selbst eine Ordinalzahl und müßte sich selbst als Element enthalten. □

Aus 2. folgt ein Induktionsprinzip: Eine Teilklasse U von On enthält alle Ordinalzahlen, wenn für alle α

$$\alpha \subset U \rightarrow \alpha \in U.$$

Eine Ordinalzahl der Form $\mathrm{s}(\alpha)$ heißt *Nachfolgerzahl*. Man schreibt auch $\alpha + 1$ für den Nachfolger von α. Eine Ordinalzahl $> \underline{0}$, die keine Nachfolgerzahl ist, heißt *Limeszahl*.

Eine *Klasse A* ist ein System $\{x \mid \phi(x, \overline{a})\}$ von Mengen, die eine Formel $\phi(x, \overline{a})$, mit festgehaltenen Parametern $\overline{a} = a_1, \ldots, a_n$, erfüllen. Das Aussonderungsaxiom besagt, daß der Durchschnitt einer Menge mit einer Klasse wieder eine Menge ist.

Ein Funktional $F : A \to \mathrm{V}$ ist eine funktionale Klasse von Paaren aus $A \times \mathrm{V}$. Es ist also $\forall x \in A\ \exists!\, y\ (x,y) \in F$. Das Ersetzungsaxiom läßt sich so formulieren: Wenn a eine Menge ist und $F : \mathrm{V} \to \mathrm{V}$ ein Funktional, ist $F[a]$ eine Menge.

Satz 9.2 (ZFC**, Rekursionssatz)** *Zu jedem Funktional* $G : \mathrm{V} \to \mathrm{V}$ *kann man ein Funktional* $F : \mathrm{On} \to \mathrm{V}$ *angeben, sodaß für alle* $\alpha \in \mathrm{On}$

$$F(\alpha) = G(F \restriction \alpha).$$

Beweis:

Wir zeigen zuerst, daß es für alle β genau eine Funktion $f : \beta \to \mathrm{V}$ gibt, die für alle $\alpha \in \beta$ die Rekursionsgleichung erfüllt.

Zuerst die Eindeutigkeit: Wenn es ein anderes $f' : \beta \to \mathrm{V}$ gibt, gibt es ein kleinstes $\alpha < \beta$ mit $f(\alpha) \neq f'(\alpha)$. Aus $f \restriction \alpha = f' \restriction \alpha$ folgt aber $f(\alpha) = f'(\alpha)$.

Wir zeigen die Existenz durch Induktion über β. Nehmen wir also an, daß die Behauptung schon für alle $\beta' < \beta$ gezeigt ist. Es gibt drei Fälle:

1. $\beta = \underline{0}$. Wir setzen $f = \emptyset$
2. $\beta = \beta' + 1$. Wir wählen ein $f' : \beta' \to \mathrm{V}$, das die Rekursionsgleichung erfüllt und setzen $f = f' \cup \big\{(\beta', G(f'))\big\}$.
3. β ist eine Limeszahl. Nach dem Ersetzungsaxiom ist

$$X = \{f' : \beta' \to V \mid \beta' < \beta,\ f' \text{ erfüllt die Rekursionsgleichung.}\}$$

eine Menge, weil die f' eindeutig durch β' bestimmt sind. Aus demselben Grund ist $f = \bigcup X$ ein Funktion.

Schließlich setzen wir

$$F = \bigcup \{f : \beta \to V \mid \beta \in \mathrm{On},\ f \text{ erfüllt die Rekursionsgleichung.}\}$$

$\square$

Wenn wir V_α definieren durch

$$\begin{aligned} \mathrm{V}_{\underline{0}} &= \emptyset \\ \mathrm{V}_{\alpha+1} &= \mathfrak{P}(\mathrm{V}_\alpha) \\ \mathrm{V}_\lambda &= \bigcup_{\alpha<\lambda} \mathrm{V}_\alpha,\ \lambda \text{ Limeszahl} \end{aligned}$$

erhalten wir die *von Neumann Hierarchie*. Man zeigt leicht, daß

$$\mathrm{V} = \bigcup_{\alpha \in \mathrm{On}} \mathrm{V}_\alpha.$$

V_ω besteht aus den *erblich endlichen Mengen*. Eine Menge heißt erblich endlich, wenn sie in einer endlichen (siehe S.54) transitiven Menge enthalten ist.

Ordinalzahlen werden durch $<$ wohlgeordnet. Das folgende Lemma besagt, daß Ordinalzahlen Wohlordnungstypen sind.

Lemma 9.3 *Jede Wohlordnung ist zu genau einer Ordinalzahl isomorph.*

Beweis:
Sei $(a, <)$ eine Wohlordnung. Wir suchen eine Ordinalzahl α und eine Bijektion $f : \alpha \to a$, die *ordnungstreu* ist:

$$x < y \Leftrightarrow f(x) < f(y)$$

Sei $*$ eine Menge, die nicht zu a gehört[8]. Wir definieren

$$F : \mathrm{On} \to a \cup \{*\}$$

durch

$$F(\beta) = \begin{cases} \min(a \setminus F[\beta]) & \text{wenn } a \not\subset F[\beta] \\ * & \text{sonst} \end{cases}$$

Wenn $*$ nicht im Bild von F vorkäme, wäre F eine ordnungstreu (also injektive) Abbildung von On nach a. Dann wäre aber $\mathrm{On} = F^{-1}[a]$ eine Menge nach dem Ersetzungsaxiom.
Sei α die kleinste Ordinalzahl, für die $F(\alpha) = *$. Dann ist $f = F \upharpoonright \alpha$ die gesuchte Bijektion.
α ist eindeutig bestimmt. Denn sei $f' : \alpha' \to a$ ein zweiter Isomorphismus. Dann erfüllt $F' = f' \cup \{(\beta, *) \mid \alpha \leq \beta\}$ die gleiche Rekursionsgleichung und es folgt $F' = F$ und $\alpha' = \alpha$. □

Aus dem Beweis folgt, daß nicht nur α sondern auch der Isomorphismus zwischen a und α eindeutig bestimmt ist.

Eine Funktion $f : x \to \mathrm{V}$ mit $f(z) \in z$ für alle $z \in x$ heißt *Auswahlfunktion*. Das Auswahlaxiom sagt, daß jede Menge x von nicht–leeren Mengen eine Auswahlfunktion besitzt. Wenn $\bigcup x$ eine Wohlordnung besitzt, existiert eine Auswahlfunktion, ohne daß man das Auswahlaxiom annehmen muß. Man setzt einfach $f(z) = \min(z)$. Umgekehrt folgt aus dem Auswahlaxiom

Satz 9.4 (Wohlordnungssatz) *Jede Menge hat eine Wohlordnung.*

Beweis:
Sei a eine Menge und $* \notin a$. Man wählt eine Auswahlfunktion $g : \mathfrak{P}(a) \setminus \{\emptyset\} \to a$. Definiere

$$F : \mathrm{On} \to a \cup \{*\}$$

durch

$$F(\beta) = \begin{cases} g(a \setminus F[\beta]) & \text{wenn } a \not\subset F[\beta] \\ * & \text{sonst} \end{cases}$$

Wie im Beweis von 9.3 sieht man, daß es ein α gibt, für das $f = F \upharpoonright \alpha$ eine Bijektion zwischen α und a ist. Diese Bijektion transportiert die Wohlordnung von α auf a: Wir setzen

$$x < y \Leftrightarrow f^{-1}(x) < f^{-1}(y).$$

[8] z.B. $* = a$

□

Aus dem Auswahlaxiom folgt auch das *Zornsche Lemma*, das wie der Wohlordnungssatz zum Auswahlaxiom äquivalent ist.

Satz 9.5 (Zornsches Lemma) *Sei $(A, <)$ eine partielle Ordnung, in der jede linear geordnete Teilmenge K eine obere Schranke s besitzt. Dann besitzt A ein maximales Element m.*

Eine (echte) obere Schranke von K ist ein Element s mit $a \leq s$ $(a < s)$ für alle $a \in K$. m ist ein maximales Element von A, wenn A keine Elemente hat, die größer als m sind.

Beweis:

Das Auswahlaxiom liefert uns ein Funktional G, das jeder Teilmenge von A, die eine echte obere Schranke hat, eine echte obere Schranke zuordnet und das sonst den Wert $*$ hat. Wir definieren

$$F : \mathrm{On} \to A \cup \{*\}$$

durch

$$F(\beta) = G(F[\beta]).$$

Wenn F den Wert $*$ nicht annehmen würde, wäre F eine ordnungstreue Abbildung von On nach A, was nicht geht. Sei α minimal mit $F(\alpha) = *$. Dann ist $K = F[\alpha]$ eine linear geordnete Teilmenge von A, die keine echte obere Schranke hat. Sei m eine obere Schranke (und damit größtes Element) von K. Dann ist m maximal in A. □

Definition *Zwei Mengen a und b heißen gleichmächtig (in Zeichen $a \sim b$), wenn es eine Bijektion zwischen a und b gibt.*
Mit der Schreibweise $a \preceq b$ drücken wir aus, daß es eine Injektion $f : a \to b$ gibt.

$a \preceq b$ bedeutet, daß a gleichmächtig mit einer Teilmenge von b ist. Man überlegt leicht, daß $a \preceq b$ genau dann gilt, wenn a leer ist oder wenn es eine surjektive Abbildung von b nach a gibt.

Aus dem Wohlordnungssatz folgt, daß jede Menge gleichmächtig zu einer Ordinalzahl ist.

Definition *Die Mächtigkeit $|a|$ einer Menge a ist die kleinste Ordinalzahl, die gleichmächtig zu a ist:*

$$|a| = \min\{\alpha \in \mathrm{On} \mid \alpha \sim a\}$$

Lemma 9.6

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

(2) $$a \preceq b \quad \Leftrightarrow \quad |a| \leq |b|$$

Beweis:

(1) folgt sofort aus der Tatsache, daß $\sim$ eine Äquivalenzrelation ist. Die Richtung „$\Leftarrow$" von (2) folgt aus $\beta \leq \alpha \Rightarrow \beta \subset \alpha$. Die Umkehrung folgt aus dem nächsten Hilfssatz. $\square$

Hilfssatz *Sei α eine Ordinalzahl und S eine Teilmenge von α. Dann ist der Ordnungstyp von S (mit der induzierten Wohlordnung) nicht größer als α.*

Beweis:

Wir zeigen durch Induktion über β: Wenn es eine ordnungstreue Funktion $f : \beta \to \alpha$ (z.B. mit Bildbereich S) gibt, ist $\beta \leq \alpha$:
Sei die Behauptung für alle $\beta' < \beta$ bewiesen. Dann folgt $\beta' \leq f(\beta') < \alpha$ für alle $\beta' < \beta$. Daraus folgt $\beta \leq \alpha$. $\square$

Wir nennen α eine *Kardinalzahl*, wenn $\alpha = |\alpha|$. Die Mächtigkeit einer Menge ist immer eine Kardinalzahl.

Lemma 9.7 *Alle natürlichen Zahlen und ω sind Kardinalzahlen.*

Beweis:

Wir zeigen durch Induktion über n, daß $n \sim m \Rightarrow n = m$ für alle $m \in \omega$. Das ist klar für $n = \underline{0}$. Sei $f : n + 1 \to m'$ eine Bijektion. Weil m' nicht $\underline{0}$ sein kann, ist $m' = m + 1$. Wenn $f(n) = m$, ist $f \restriction n$ eine Bijektion zwischen n und m. Wir schließen $n = m$ und daraus $n + 1 = m'$. Sonst sei $f(x) = m$ für ein $x < n$. Dann ist die Funktion

$$g(z) = \begin{cases} f(n) & \text{wenn } z = x \\ z & \text{sonst} \end{cases}$$

eine Bijektion zwischen n und m.

Aus $n \preceq \omega$ folgt $n = |n| \leq |\omega|$. Also ist $|\omega|$ größer als alle $n < \omega$. Es folgt $|\omega| = \omega$. $\square$

Eine Menge a heißt *endlich*, wenn $|a| < \omega$. Wenn $|a| = \omega$, heißt a *abzählbar*.

Satz 9.8 (Cantor)

$$\big|a\big| < \big|\mathfrak{P}(a)\big|$$

Beweis:

Sei $f : a \to \mathfrak{P}(a)$ eine Abbildung. Die Menge

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

kann nicht im Bild von f liegen. Es gibt also keine Surjektion von a nach $\mathfrak{P}(a)$. $\square$

Es folgt, daß es keine größte Kardinalzahl gibt. Man bezeichnet mit κ^+ die kleinste Kardinalzahl, die größer als κ ist. Es ist $\omega^+ \leq \left|\mathfrak{P}(\omega)\right|$. Die Aussage

$$\omega^+ = \left|\mathfrak{P}(\omega)\right|$$

ist die *Kontinuumshypothese* (CH). Wenn ZFC widerspruchsfrei ist, kann CH weder bewiesen noch widerlegt werden.

Man zeigt leicht durch Induktion, daß für disjunkte endliche Mengen

$$\left|a \cup b\right| = \left|a\right| + \left|b\right|.$$

Daraus folgt (wiederum durch Induktion), daß

$$\left|m \times n\right| = m \cdot n$$

für alle $m, n \in \omega$.

Satz 9.9 *Wenn a unendlich ist, ist*

$$\left|a \times a\right| = \left|a\right|$$

Beweis:

Wir führen den Beweis nur für abzählbare a. Den allgemeinen Fall beweist man ähnlich[9].

Die lexikographische Ordnung

$$(l, m, n) < (l', m', n') \Longleftrightarrow \begin{cases} l < l' & & \text{oder} \\ l = l', & m < m' & \text{oder} \\ l = l, & m = m', & n < n' \end{cases}$$

auf $\omega \times \omega \times \omega$ ist eine Wohlordnung. Wir definieren eine Wohlordnung von $\omega \times \omega$ durch

$$(m, n) < (m', n') \Longleftrightarrow \big(\max(m, n), m, n\big) < \big(\max(m', n'), m', n'\big).$$

Sei $l = \max(m, n) + 1$. Dann sind alle Vorgänger von (m, n) in $l \times l$ enthalten. Es gibt also nur endlich viele (nämlich höchstens $l \cdot l$) Vorgänger. Daraus folgt, daß der Ordnungstyp von $\big(\omega \times \omega, <\big)$ nicht größer als ω sein kann. Also ist $\left|\omega \times \omega\right| = \omega$. $\square$

[9] Durch Induktion über $|a|$

10 Metamathematik von ZFC

Wir ordnen jeder L_{Me}–Formel ψ eine Konstante $\ulcorner\psi\urcorner$ in einer definitorischen Erweiterung von ZFC zu[10] (siehe 7.4). Zunächst ordnen wir allen Zeichen einen Term zu:

$$\begin{array}{rcl}
\ulcorner\doteq\urcorner & = & (\underline{0},\underline{0}) \\
\ulcorner\wedge\urcorner & = & (\underline{0},\underline{1}) \\
\ulcorner\neg\urcorner & = & (\underline{0},\underline{2}) \\
\ulcorner(\urcorner & = & (\underline{0},\underline{3}) \\
\ulcorner)\urcorner & = & (\underline{0},\underline{4}) \\
\ulcorner\exists\urcorner & = & (\underline{0},\underline{5}) \\
\ulcorner\epsilon\urcorner & = & (\underline{0},\underline{6}) \\
\ulcorner v_0\urcorner & = & (\underline{1},\underline{0}) \\
\ulcorner v_1\urcorner & = & (\underline{1},\underline{1}) \\
\ldots & = & \ldots
\end{array}$$

Für eine Formel $\psi = \zeta_0\,\zeta_1 \ldots \zeta_{n-1}$ der Länge n setzen wir

$$\ulcorner\psi\urcorner = \Big\{\big(\underline{0},\ulcorner\zeta_0\urcorner\big),\ldots,\big(\underline{n-1},\ulcorner\zeta_{n-1}\urcorner\big)\Big\}.$$

Satz 10.1 (Fixpunktsatz) *Für jede L_{Me}–Formel $\Sigma(x)$ gibt es eine Aussage ϕ mit*

$$\mathrm{ZFC} \vdash \phi \longleftrightarrow \Sigma(\ulcorner\phi\urcorner).$$

Beweis:
Wir meinen mit $\psi(\ulcorner\chi\urcorner)$ eigentlich die L_{Me}–Aussage, die in der definitorischen Erweiterung von ZFC zu $\psi(\ulcorner\chi\urcorner)$ äquivalent ist (siehe 7.4). Wir brauchen das folgende Lemma:

Lemma 10.2 *Es gibt eine in* ZFC *definierbare Funktion* Sub *mit*

$$\mathrm{ZFC} \vdash \ulcorner\psi(\ulcorner\chi\urcorner)\urcorner \doteq \mathrm{Sub}(\ulcorner\psi\urcorner,\ulcorner\chi\urcorner)$$

für alle L_{Me}–Formeln $\psi(x)$ und χ.

Beweis: Sub beschreibt einfach die Einsetzung in Formeln. □

Sei nun $\psi(v_0)$ die L_{Me}–Formel die zu $\Sigma(\mathrm{Sub}(v_0, v_0))$ äquivalent ist. Dann sind in ZFC die folgenden Aussagen äquivalent:

$$\psi(\ulcorner\psi\urcorner) \sim \Sigma(\mathrm{Sub}(\ulcorner\psi\urcorner,\ulcorner\psi\urcorner)) \sim \Sigma(\ulcorner\psi(\ulcorner\psi\urcorner)\urcorner)$$

Wenn man jetzt $\phi = \psi(\ulcorner\psi\urcorner)$ setzt, ergibt sich die Behauptung. □

Der folgende Satz von Tarski behauptet die Unmöglichkeit einer Wahrheitsdefinition in ZFC.

[10] In Abschnitt 14 werden wir mit $\ulcorner\psi\urcorner$ die Gödelnummer von ψ bezeichnen.

Folgerung 10.3 (Tarski) *Wenn* ZFC *widerspruchsfrei ist, gibt es keine Formel* $\mathcal{W}(x)$*, so daß für alle Aussagen* ϕ

$$\mathrm{ZFC} \vdash \phi \longleftrightarrow \mathcal{W}(\ulcorner\phi\urcorner)$$

Beweis:
Wähle ein ϕ mit $\mathrm{ZFC} \vdash \phi \longleftrightarrow \neg\,\mathcal{W}(\ulcorner\phi\urcorner)$. □

Das Beweisbarkeitsprädikat

Sei $\mathrm{Bew}(x)$ die Formel, die (in ZFC) ausdrückt, daß x eine in ZFC beweisbare Aussage ist. Es sollte klar[11] sein, daß $\mathrm{Bew}(x)$ die folgenden **Loeb–Axiome** erfüllt: (Man beachte, daß **L3** gilt, weil **L1** in ZFC beweisbar ist.)

L1 $\mathrm{ZFC} \vdash \phi \implies \mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\phi\urcorner)$

L2 $\mathrm{ZFC} \ \vdash\ \mathrm{Bew}(\ulcorner\phi\urcorner) \wedge \mathrm{Bew}(\ulcorner\phi \to \psi\urcorner) \ \to\ \mathrm{Bew}(\ulcorner\psi\urcorner)$

L3 $\mathrm{ZFC} \ \vdash\ \mathrm{Bew}(\ulcorner\phi\urcorner) \ \to\ \mathrm{Bew}\big(\ulcorner\mathrm{Bew}(\ulcorner\phi\urcorner)\urcorner\big)$

Folgerung 10.4

(1) $\qquad \mathrm{ZFC} \vdash \phi \to \psi \implies \mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\phi\urcorner) \to \mathrm{Bew}(\ulcorner\psi\urcorner)$

(2) $\qquad \mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\phi \wedge \psi\urcorner) \longleftrightarrow (\mathrm{Bew}(\ulcorner\phi\urcorner) \wedge \mathrm{Bew}(\ulcorner\psi\urcorner))$

Beweis:

(1) : Aus $\mathrm{ZFC} \vdash \phi \to \psi$ folgt $\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\phi \to \psi\urcorner)$ wegen **L1**, und daraus, mit **L2**, die Behauptung $\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\phi\urcorner) \to \mathrm{Bew}(\ulcorner\psi\urcorner)$.

(2) $\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\phi\wedge\psi\urcorner) \to \mathrm{Bew}(\ulcorner\phi\urcorner)$ und $\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\phi\wedge\psi\urcorner) \to \mathrm{Bew}(\ulcorner\psi\urcorner)$ folgen sofort aus (1). Aus (1) folgt auch

$$\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\phi\urcorner) \to \mathrm{Bew}(\ulcorner\psi \to (\phi \wedge \psi)\urcorner).$$

Wegen **L2** ist

$$\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\psi\urcorner) \wedge \mathrm{Bew}(\ulcorner\psi \to (\phi \wedge \psi)\urcorner) \to \mathrm{Bew}(\ulcorner\phi \wedge \psi\urcorner).$$

Daraus folgt $(\mathrm{Bew}(\ulcorner\phi\urcorner) \wedge \mathrm{Bew}(\ulcorner\psi\urcorner)) \to \mathrm{Bew}(\ulcorner\phi \wedge \psi\urcorner)$.

□

Sei F eine Formel, deren Negation allgemeingültig ist, z.B. $\neg\,\underline{0} \doteq \underline{0}$. Die Aussage

$$\mathrm{CON}_{\mathrm{ZFC}} = \neg\,\mathrm{Bew}(\ulcorner\mathrm{F}\urcorner)$$

drückt dann die Konsistenz von ZFC aus.

[11] Im Abschnitt 19 werden wir uns mit dem Beweisbarkeitsprädikat der Peanoarithmetik etwas mehr Mühe geben.

Satz 10.5 (Zweiter Gödelscher Unvollständigkeitssatz für ZFC) *Wenn ZFC konsistent ist, ist $\mathrm{CON}_{\mathrm{ZFC}}$ in ZFC unbeweisbar.*

Beweis:

Natürlich folgt aus der Unbeweisbarkeit von $\mathrm{CON}_{\mathrm{ZFC}}$ die Konsistenz von ZFC. Wenn wir den Satz (natürlich in ZFC) bewiesen haben, haben wir gezeigt, daß

$$\mathrm{ZFC} \vdash \mathrm{CON}_{\mathrm{ZFC}} \longleftrightarrow \neg\,\mathrm{Bew}(\ulcorner \mathrm{CON}_{\mathrm{ZFC}} \urcorner).$$

Wir beginnen daher mit einer Formel ϕ, die

$$\mathrm{ZFC} \vdash \phi \longleftrightarrow \neg\,\mathrm{Bew}(\ulcorner \phi \urcorner) \tag{3}$$

erfüllt. Wir zeigen zuerst, daß tatsächlich[12]

$$\mathrm{ZFC} \vdash \phi \longleftrightarrow \mathrm{CON}_{\mathrm{ZFC}} \tag{4}$$

Zunächst folgt aus $\mathrm{ZFC} \vdash \mathrm{F} \rightarrow \phi$ und (1), daß $\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner \mathrm{F} \urcorner) \rightarrow \mathrm{Bew}(\ulcorner \phi \urcorner)$. Also ist $\mathrm{ZFC} \vdash \phi \rightarrow \mathrm{CON}_{\mathrm{ZFC}}$.

Dann folgt aus $\mathrm{ZFC} \vdash \phi \rightarrow \neg\,\mathrm{Bew}(\ulcorner \phi \urcorner)$, daß

$$\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner \phi \urcorner) \rightarrow \mathrm{Bew}(\ulcorner \neg\,\mathrm{Bew}(\ulcorner \phi \urcorner) \urcorner).$$

Zusammen mit **L3** ergibt das

$$\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner \phi \urcorner) \rightarrow (\mathrm{Bew}(\ulcorner \neg\,\mathrm{Bew}(\ulcorner \phi \urcorner) \urcorner) \wedge \mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner \phi \urcorner) \urcorner)).$$

Weil aber wegen 10.4

$$\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner \neg\,\mathrm{Bew}(\ulcorner \phi \urcorner) \urcorner) \wedge \mathrm{Bew}(\ulcorner \mathrm{Bew}(\ulcorner \phi \urcorner) \urcorner) \;\rightarrow\; \mathrm{Bew}(\ulcorner \mathrm{F} \urcorner),$$

folgt $\mathrm{Bew}(\ulcorner \phi \urcorner) \rightarrow \neg\,\mathrm{CON}_{\mathrm{ZFC}}$, das heißt $\mathrm{ZFC} \vdash \mathrm{CON}_{\mathrm{ZFC}} \rightarrow \phi$. Damit ist (4) bewiesen.

Nehmen wir an, daß $\mathrm{ZFC} \vdash \mathrm{CON}_{\mathrm{ZFC}}$. Dann ist $\mathrm{ZFC} \vdash \phi$ wegen (4). Daraus folgt mit **L1** $\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner \phi \urcorner)$ und mit (3) $\mathrm{ZFC} \vdash \neg\,\mathrm{Bew}(\ulcorner \phi \urcorner)$. ZFC wäre also inkonsistent. □

Wenn wir wüßten, daß alle Aussagen, die in ZFC beweisbar sind, auch wahr wären, wäre $\mathrm{CON}_{\mathrm{ZFC}}$ *unabhängig* von ZFC: Weder $\mathrm{CON}_{\mathrm{ZFC}}$ noch $\neg\,\mathrm{CON}_{\mathrm{ZFC}}$ sind dann aus ZFC beweisbar. Es ist aber denkbar[13], daß ZFC zwar konsistent ist, aber $\mathrm{ZFC} \vdash \neg\,\mathrm{CON}_{\mathrm{ZFC}}$. Um (unter der Voraussetzung der Konsistenz) eine von ZFC unabhängige Aussage zu finden, müssen wir anders vorgehen.

Man kann leicht eine Liste $\phi_0, \phi_1, \ldots$ aller in ZFC beweisbaren Aussagen angeben. Wenn man es vernünftig gemacht hat, läßt sich

$$\phi \textit{ ist die } n\textit{-te beweisbare Aussage}$$

[12] Wir verwenden nur „$\leftarrow$“.

[13] Nehmen wir an, daß $\mathrm{ZFC} \not\vdash \neg\,\mathrm{CON}_{\mathrm{ZFC}}$. Dann ist $\mathrm{ZFC}^+ = \mathrm{ZFC} + \mathrm{CON}_{\mathrm{ZFC}}$ konsistent. Aus dem zweiten Gödelschen Unvollständigkeitssatz (für ZFC^+) folgt, daß man in ZFC^+ die Konsistenz von ZFC^+ nicht beweisen kann. Man kann also nicht beweisen, daß $\mathrm{ZFC} \not\vdash \neg\,\mathrm{CON}_{\mathrm{ZFC}}$.

mit einer L_{Me}–Formel $\mathrm{Bew}(x, y)$ ausdrücken, die die folgenden Eigenschaft hat:

Für alle $n = 0, 1, \ldots$ und alle Aussagen ϕ ist

$$\phi = \phi_n \implies \mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\phi\urcorner, \underline{n}) \tag{5}$$

$$\phi \neq \phi_n \implies \mathrm{ZFC} \vdash \neg\,\mathrm{Bew}(\ulcorner\phi\urcorner, \underline{n}). \tag{6}$$

Sei $\mathcal{R}$ eine Aussage mit

$$\mathrm{ZFC} \vdash \mathcal{R} \longleftrightarrow \forall\, y \in \omega\ \big(\mathrm{Bew}(\ulcorner\mathcal{R}\urcorner, y) \to \exists z < y\ \mathrm{Bew}(\ulcorner\neg\,\mathcal{R}\urcorner, z)\big).$$ [14]

Man nennt $\mathcal{R}$ einen *Rossersatz*.

Satz 10.6 (Erster Gödelscher Unvollständigkeitssatz für ZFC**)**
Wenn ZFC *konsistent ist, ist* $\mathcal{R}$ *unabhängig von* ZFC.

Beweis:
Für beliebiges ψ sei ψ^* die Aussage

$$\forall\, y \in \omega\ \big(\mathrm{Bew}(\ulcorner\psi\urcorner, y) \to \exists z < y\ \mathrm{Bew}(\ulcorner\neg\,\psi\urcorner, z)\big).$$

Wir zeigen zuerst

$$\mathrm{ZFC} \vdash \psi \implies \mathrm{ZFC} \vdash \neg\,\psi^* \tag{7}$$

$$\mathrm{ZFC} \vdash \neg\,\psi \implies \mathrm{ZFC} \vdash \psi^*. \tag{8}$$

Daraus folgt $\mathrm{ZFC} \vdash \mathcal{R} \iff \mathrm{ZFC} \vdash \neg\,\mathcal{R}$ und damit die Behauptung des Satzes.

Beweis von (7): Wenn $\mathrm{ZFC} \vdash \psi$, gibt es nach (5) ein n mit $\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\psi\urcorner, \underline{n})$. Weil ZFC konsistent ist[15], ist wegen (6) $\mathrm{ZFC} \vdash \neg\,\mathrm{Bew}(\ulcorner\neg\,\psi\urcorner, \underline{m})$ für alle m. Daraus folgt $\mathrm{ZFC} \vdash \neg\,\exists z < \underline{n}\ \mathrm{Bew}(\ulcorner\neg\,\psi\urcorner, z)$ und schließlich $\mathrm{ZFC} \vdash \neg\,\psi^*$.

Beweis von (8): Wenn $\mathrm{ZFC} \vdash \neg\,\psi$, gibt es ein m mit $\mathrm{ZFC} \vdash \mathrm{Bew}(\ulcorner\neg\,\psi\urcorner, \underline{m})$ und es ist $\mathrm{ZFC} \vdash \neg\,\mathrm{Bew}(\ulcorner\psi\urcorner, \underline{n})$ für alle n. Daraus folgt

$$\mathrm{ZFC} \vdash \forall\, y \in \omega\ \big(\mathrm{Bew}(\ulcorner\psi\urcorner, y) \to \underline{m} < y\big)$$

und schließlich $\mathrm{ZFC} \vdash \psi^*$. □

[14] Eigentlich müßte man statt $\mathrm{Bew}(\ulcorner\neg\,\mathcal{R}\urcorner, z)$ die Formel $\mathrm{Bew}(\mathrm{Neg}(\ulcorner\neg\,\mathcal{R}\urcorner), z)$ nehmen, für eine definierbare Funktion Neg mit $\mathrm{ZFC} \vdash \ulcorner\neg\,\phi\urcorner \doteq \mathrm{Neg}(\ulcorner\phi\urcorner)$ für alle ϕ.

[15] (7) und 8) gelten natürlich auch, wenn ZFC inkosistent ist.

Kapitel 3

Rekursionstheorie

11 Registermaschinen

Wir fixieren eine L–elementiges Alphabet $\mathcal{A} = \{a_1, \ldots, a_L\}$. Mit $\mathcal{A}^*$ bezeichnen wir die Menge der *Wörter*, die sich aus den Buchstaben von $\mathcal{A}$ bilden lassen.

Eine *Registermaschine* über $\mathcal{A}$ mit Registern $\mathcal{R}_0, \ldots, \mathcal{R}_{R-1}$ ist eine Folge

$$\mathcal{M} = (b_0, \ldots, b_N)$$

von *Befehlen*. Es gibt drei Sorten von Befehlen:

Stopbefehl	:	0	Wir nehmen an, daß $b_N = 0$
Schreibbefehl	:	(r, l)	$(r < R,\ l \leq L)$
Verzweigung	:	$(r, c_0, \ldots, c_L)$	$(r < R,\ c_i \leq N)$

Eine *Konfiguration* ist ein $R+1$–Tupel $\mathcal{K} = (c, R_0, \ldots, R_{R-1})$ mit $c \leq N$ und $R_i \in \mathcal{A}^*$.

Die *Anfangskonfiguration* beim Input $w_1, \ldots, w_n$ ist $(0, \emptyset, w_1, \ldots, w_n, \emptyset, \ldots)$.

Eine *Stopkonfiguration* ist eine Konfiguration $(c, \ldots)$ mit $b_c = 0$).

Die *Nachfolgekonfiguration* $\mathcal{M}(\mathcal{K})$ ist wie folgt definiert: Sei

$$\mathcal{K} = (c, R_0, \ldots, R_{R-1})$$

und $b = b_c$ der aktuelle Befehl.

1.Fall	$b = 0$	Dann ist $\mathcal{M}(\mathcal{K}) = \mathcal{K}$.
2.Fall	(r, l)	Dann ist $\mathcal{M}(\mathcal{K}) = (c+1, R_0, \ldots, \overline{R}_r, \ldots, R_{R-1})$, wobei $\overline{R}_r = \begin{cases} R_r a_l & (l \geq 1) \\ R_r \dot{-} 1 & (l = 0) \end{cases}$

3.Fall	$b = (r, c_0, \ldots, c_L)$	Falls $R_r \neq \emptyset$, sei a_i der letzte Buchstabe von R_r. Dann ist $\mathcal{M}(\mathcal{K}) = (\bar{c}, R_0, \ldots, R_{R-1})$, wobei $\bar{c} = \begin{cases} c_0 & \text{falls } R_r = \emptyset \\ c_i & \text{sonst} \end{cases}$

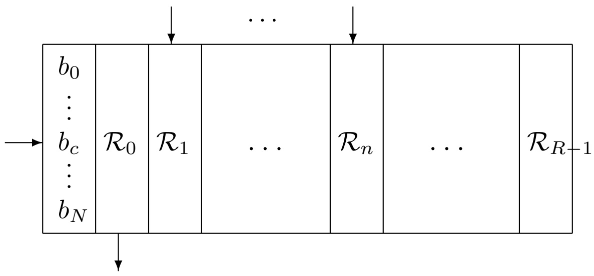
Dabei entsteht $w \dot{-} 1$ aus w durch Streichen des letzten Buchstabens.

$\mathcal{M}$ berechnet auf folgende Weise eine partielle Funktion

$$F^n_{\mathcal{M}} : \underbrace{\mathcal{A}^* \times \ldots \mathcal{A}^*}_{n} \to \mathcal{A}^*.$$

Seien $w_1, \ldots, w_n$ der Input und $\mathcal{K}_0$ die Anfangskonfiguration. Wenn für alle s $\mathcal{M}^s(\mathcal{K}_0)$ kein Stopkonfiguration ist, dann ist $F^n_{\mathcal{M}}(w_1, \ldots, w_n)$ undefiniert. Wenn $\mathcal{M}^s(\mathcal{K}_0) = (c, R_0, \ldots)$ eine Stopkonfiguration ist, setzen wir $F^n_{\mathcal{M}}(w_1, \ldots, w_n) = R_0$.

Die Funktion $F^n_{\mathcal{M}}$ heißt *maschinenberechenbar*.



Im Alphabet $\mathcal{A} = \{ \mid \} = \{a_1\}$ stellen wir jede natürliche Zahl m durch m Striche $|^m$ dar. $\mathcal{M}$ berechnet so eine partielle Funktion

$$F^n_{\mathcal{M}} : \mathbb{N}^n \to \mathbb{N}.$$

Wir geben eine äquivalente Beschreibung dieser Funktionen:

Definition *Eine Funktion $f : \mathbb{N}^n \to \mathbb{N}$, $(n \geq 0)$ heißt rekursiv, wenn sie sich aus den Grundfunktionen*

R0	$\mathrm{S}(x)$	$=$	$x + 1$	
	$\mathrm{I}^n_i(x_1, \ldots, x_n)$	$=$	x_i	$(1 \leq i \leq n)$
	C^0_0	$=$	0	*nullstellig*

durch Anwenden der Regeln

R1 *Sind die g_i und h rekursiv, dann auch*

$$f(x_1,\ldots,x_n) = h(g_1(x_1,\ldots,x_n),\ldots,g_k(x_1,\ldots,x_n))$$

(Einsetzung)

R2 *Sind g und h rekursiv, dann auch*

$$f(x_1,\ldots,x_n,y),$$

wobei

$$f(x_1,\ldots,x_n,0) = g(x_1,\ldots,x_n)$$

und

$$f(x_1,\ldots,x_n,y+1) = h(x_1,\ldots,x_n,y,f(x_1\ldots,x_n,y))$$

(primitive Rekursion)

R3 *g sei rekursiv und es gelte $\forall x_1,\ldots,x_n \exists y\ g(x_1,\ldots,x_n,y) = 0$. Dann ist auch*

$$f(x_1,\ldots,x_n) = \mu y\ (g(x_1,\ldots,x_n,y) = 0)$$

rekursiv, wobei

$$\mu y\ A(y) = \textit{das kleinste } y \textit{ mit } A(y).$$

(μ–Rekursion)

ergibt.

Anmerkungen:

Verwendet man nur **R0**, **R1** und **R2**, heißt f *primitiv rekursiv.*
Die konstante Funktionen

$$\mathrm{C}^n_m(x_1,\ldots,x_n) = m$$

sind zum Beispiel primitiv rekursiv: Es ist $\mathrm{C}^0_{m+1} = \mathrm{S}(\mathrm{C}^0_m)$. C^n_m entsteht aus C^0_m durch "Einsetzen"von $k = 0$–vielen n–stelligen Funktionen

Man kann rekursive Funktionen beliebig ineinander einsetzen. Zum Beispiel ist

$$f(x_1,x_2,x_3) = h(x_1,g(x_2,x_2))$$

rekursiv, wenn g und h rekursiv sind.

Satz 11.1 *Die rekursiven Funktionen stimmen mit den maschinenberechenbaren Funktionen überein.*

In diesem Paragraphen beweisen wir eine Richtung: Die rekursiven Funktionen sind berechenbar. Wir beschreiben Maschinen in naheliegender Weise durch

Flußdiagramme. Unser Alphabet ist $\mathcal{A} = \{ | \}$. I und J seien Registerinhalte (also R–Tupel $(R_0, \ldots, R_{R-1})$). Wir schreiben

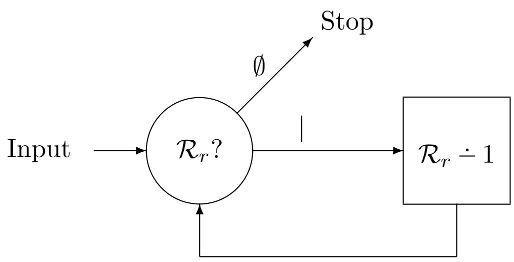
$$I \xrightarrow[\mathcal{M}]{} J,$$

wenn für ein s $\mathcal{M}^s((0, I))$ eine Stopkonfiguration (c, J) ist.

Die Löschmaschine $\mathcal{L}^r$

$$(R_0, \ldots, R_r, \ldots, R_{R-1}) \xrightarrow[\mathcal{L}^r]{} (R_0, \ldots, \emptyset, \ldots, R_{R-1})$$

löscht das r–te Register. Das Flußdiagramm von $\mathcal{L}^r$ ist



Formal:

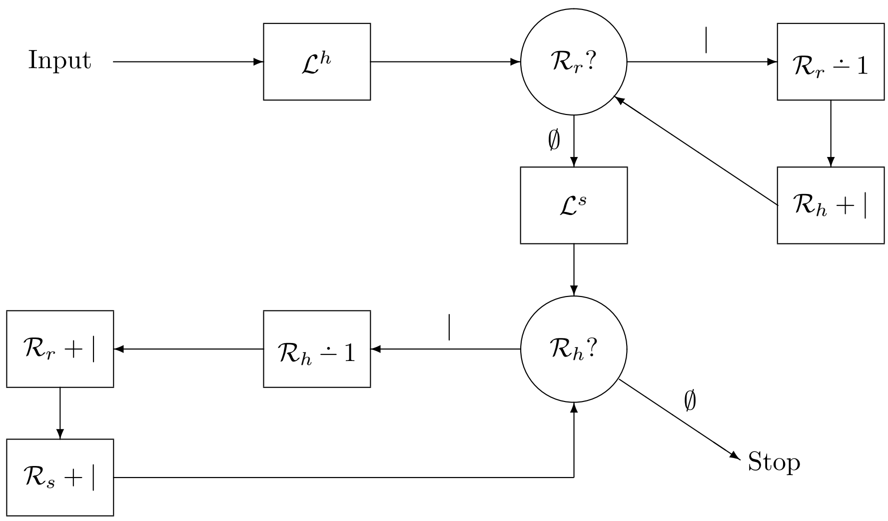
$$\mathcal{L}^r = \big((r, 3, 1), (r, 0), (0, 0, 0), 0\big)$$

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

$$(R_0, \ldots, R_r, \ldots, R_s, \ldots, R_h, \ldots) \xrightarrow[\mathcal{K}_h^{r,s}]{} (R_0, \ldots, R_r, \ldots, R_r, \ldots, *, \ldots)$$

kopiert $\mathcal{R}_r$ auf $\mathcal{R}_s$ mit Hilfsregister $\mathcal{R}_h$, $(h \notin \{r, s\})$

Flußdiagramm:



Formal:

$$\mathcal{K}_h^{r,s} = \big((h,3,1),(h,0),(0,0,0),(r,7,4),(r,0),(h,1),(0,3,3),(s,10,8),(s,0),\\ (0,7,7),(h,15,11),(h,0),(r,1),(s,1),(0,10,10),0\big)$$

Für das Hintereinanderausführen der Maschinen $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$ verwenden wir die Notation

$$\mathcal{M}_1\mathcal{M}_2\mathcal{M}_3.$$

Zum Beispiel kopiert die Maschine

$$\mathcal{K}_h^{r_1,\ldots,r_n;s_1,\ldots,s_n} = \mathcal{K}_h^{r_1,s_1} \ldots \mathcal{K}_h^{r_n,s_n}$$

die Register $\mathcal{R}_{r_1},\ldots,\mathcal{R}_{r_n}$ nach $\mathcal{R}_{s_1},\ldots,\mathcal{R}_{s_n}$. Wenn $\mathcal{M}$ eine n–stellige Funktion mit R–Registern berechnet, bezeichnen wir mit $\mathcal{M}^*$ die Maschine

$$\mathcal{M}^* = \mathcal{L}^0\mathcal{L}^{n+1}\ldots\mathcal{L}^{R-1}\mathcal{M}.$$

Zuerst zeigen wir, daß die Grundfunktionen **R0** maschinenberechenbar sind:

S	wird berechnet von	$\mathcal{K}_2^{1,0}(\mathcal{R}_0 + \vert)$
I_i^n	wird berechnet von	$\mathcal{K}_{n+1}^{i,0}$
C_0^0	wird berechnet von	”Stop”

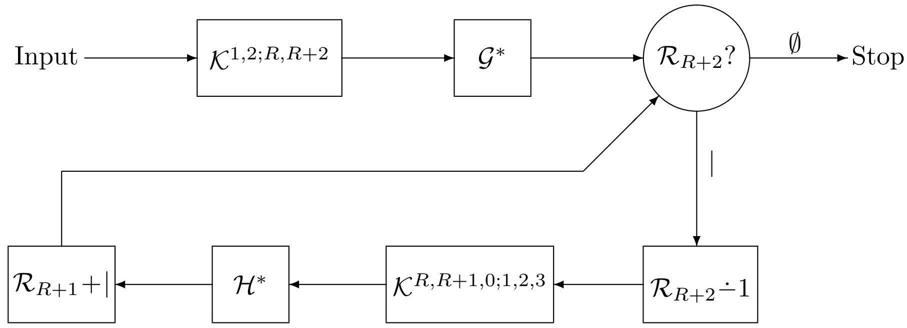
Die maschinenberechenbare Funktionen sind abgeschlossen unter der Regel **R1**:

Wenn zum Beispiel $h(y_1,y_2)$ von $\mathcal{H}$ und die Funktionen $f_1(x)$ und $f_2(x)$ von $\mathcal{F}_1$ und $\mathcal{F}_2$ mit R Registern berechnet werden, wird $f(x) = h(f_1(x), f_2(x))$ berechnet von der Hintereinanderausführung der folgenden Maschinen. (Wir verwenden das Hilfsregister $\mathcal{R}_{R+2}$.)

$K^{1,R}$	(rettet x auf $\mathcal{R}_R$)
$\mathcal{F}_1\mathcal{K}^{0,R+1}$	(berechnet $f_1(x)$ und speichert den Wert in $\mathcal{R}_{R+1}$.)
$\mathcal{K}^{R,1}\mathcal{F}_2^*\mathcal{K}^{0,2}$	(berechnet $f_2(x)$ und speichert den Wert in $\mathcal{R}_2$.)
$\mathcal{K}^{R+1,1}\mathcal{H}^*$	(berechnet $h(f(x), f_2(x))$.

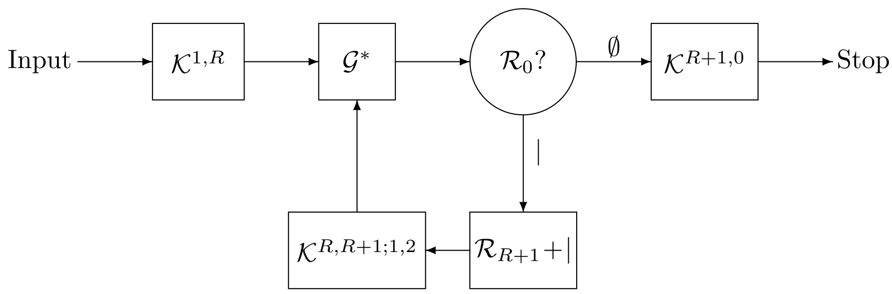
Die maschinenberechenbare Funktionen sind abgeschlossen unter der Regel **R2**:

Wir zeigen das für den Fall $n = 1$. $g(x)$ werde von $\mathcal{G}$ und $h(x, y, z)$ werde von $\mathcal{H}$ mit R Registern berechnet. Dann wird f berechnet von folgendem Flußdiagramm: (Hilfsregister $\mathcal{R}_{R+3}$)



Die maschinenberechenbare Funktionen sind abgeschlossen unter der Regel **R3**:

Wir zeigen das für den Fall $n = 1$. Nehmen wir an, daß $g(x, y)$ von $\mathcal{G}$ mit R Registern berechnet wird. Dann wird $f(x)$ berechnet von der Maschine mit dem folgendem Flußdiagramm: (Hilfsregister $\mathcal{R}_{R+2}$)



12 Primitiv rekursive Funktionen und Gödelisierung

Lemma 12.1 *Die Funktionen*

$$x + y, \quad x \cdot y, \quad x^y, \quad x!, \quad x \dot{-} y$$

sind primitiv rekursiv.

Dabei ist

$$x \dot{-} y = \begin{cases} x - y & \text{wenn } y \leq x \\ 0 & \text{sonst} \end{cases}$$

Beweis:

$x + y$ läßt sich, wie die anderen Funktionen, leicht durch primitive Rekursion definieren:

$$x + 0 = x, \quad x + (y + 1) = S(x + y).$$

Ein Problem stellt vielleicht $x \dot{-} y$ dar. Zuerst definieren wir $y \dot{-} 1$ durch $0 \dot{-} 1 = 0$ und $(y + 1) \dot{-} 1 = y$. Und dann $x \dot{-} 0 = x$ und $x \dot{-} (y + 1) = (x \dot{-} y) \dot{-} 1$. □

Definition *Eine Relation (oder* Prädikat*) R heißt (primitiv) rekursiv, wenn die charakteristische Funktion*

$$\mathrm{K}_R(x_1, \ldots, x_n) = \begin{cases} 0 & \textit{wenn } R(x_1, \ldots, x_n) \\ 1 & \textit{sonst} \end{cases}$$

(primitiv) rekursiv ist.

Zum Beispiel ist die Relation $x \doteq 0$ primitiv rekursiv, weil $\mathrm{K}_{\doteq 0}(0) = 0$ und $\mathrm{K}(x + 1) = 1$. $x < y$ ist primitiv rekursiv, weil $\mathrm{K}_<(x, y) = \mathrm{K}_{\doteq 0}((x + 1 \dot{-} y))$.

Lemma 12.2 *Wenn P und Q (primitiv) rekursive Prädikate sind, dann auch $P \wedge Q$, $P \vee Q$, $\neg P$ und $P(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n))$ für alle (primitiv) rekursiven $f_1, \ldots, f_k$.*

Beweis:

Es ist

$$\begin{aligned} \mathrm{K}_{P \vee Q} &= \mathrm{K}_P \cdot \mathrm{K}_Q \\ \mathrm{K}_{\neg P} &= 1 \dot{-} \mathrm{K}_P \\ P \wedge Q &\Leftrightarrow \neg(\neg P \vee \neg Q). \end{aligned}$$

Wenn man die f_i in die charakteristische Funktion von P einsetzt, erhält man die charakteristische Funktion von $P(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n))$. □

Lemma 12.3 *Wenn $P_0 \ldots, P_{n-1}$ (primitiv) rekursive Prädikate und $f_0, \ldots, f_n$ (primitiv) rekursive Funktionen sind, so ist auch*

$$f(\overline{x}) = \begin{cases} f_0(\overline{x}) & \textit{falls} \quad P_0(\overline{x}) \\ f_1(\overline{x}) & \textit{falls} \quad \neg P_0(\overline{x}) \wedge P_1(\overline{x}) \\ \vdots & \\ f_n(\overline{x}) & \textit{falls} \quad \neg P_0(\overline{x}) \wedge \ldots \wedge \neg P_{n-1}(\overline{x}) \end{cases}$$

(primitiv) rekursiv.

Beweis:

Die Prädikate $Q_0 = P_0$, $Q_1 = \neg P_0 \wedge P_1, \ldots,$ $Q_n = \neg P_0 \wedge \ldots \wedge \neg P_{n-1}$ sind (primitiv) rekursiv, also auch

$$f(\overline{x}) = \sum_{i=0}^{n} (1 \dot{-} \mathrm{K}_{Q_i}(\overline{x})) f_i(\overline{x}).$$

□

Lemma 12.4 *Sei P (primitiv) rekursiv. Dann sind auch die Relationen*

$$\begin{aligned} R(\overline{x}, z) \quad &\Leftrightarrow \quad \forall y < z \; P(\overline{x}, y) \\ S(\overline{x}, z) \quad &\Leftrightarrow \quad \exists y < z \; P(\overline{x}, y) \end{aligned}$$

(primitiv) rekursiv.

Beweis:

Man definiert R durch primitive Rekursion:

$$\begin{aligned} R(\overline{x}, 0) \quad &\Leftrightarrow \quad \text{wahr} \\ R(\overline{x}, z+1) \quad &\Leftrightarrow \quad R(\overline{x}, z) \wedge P(\overline{x}, z) \end{aligned}$$

Schließlich ist $S(\overline{x}, z) \Leftrightarrow \neg \forall y < z \neg P(\overline{x}, y)$ □

Lemma 12.5 *$R(\overline{x}, y)$ sei eine primitiv rekursive Relation und $b(\overline{x})$ eine primitiv rekursive Funktion. Wenn*

$$\forall \overline{x} \, \exists y \leq b(\overline{x}) \; R(\overline{x}, y),$$

ist

$$f(\overline{x}) = \mu y \, R(\overline{x}, y)$$

primitiv rekursiv.

Beweis:

Die Funktion $h(\overline{x}, y) = \mu z \, (R(\overline{x}, z) \vee z = y)$ ist primitiv rekursiv, weil $h(\overline{x}, 0) = 0$ und

$$h(\overline{x}, y+1) = \begin{cases} h(\overline{x}, y) & \text{falls } R(\overline{x}, h(\overline{x}, y)) \\ y+1 & \text{sonst.} \end{cases}$$

Es ist $f(\overline{x}) = h(\overline{x}, b(\overline{x}))$. □

Beispiele

$x|y$ (x *teilt* y) ist primitiv rekursiv (12.4).

x *ist Primzahl* ist primitiv rekursiv (12.4).

$\mathrm{p}(x) = (n+1)$*–te Primzahl* ist primitiv rekursiv wegen 12.5, weil sich μy in

$$\mathrm{p}(x+1) = \mu y\ (y \text{ prim } \wedge y > \mathrm{p}(x))$$

durch $\mathrm{p}(x)! + 1$ beschränken läßt.

Wir schreiben p_n für $\mathrm{p}(n)$.

Lemma 12.6 *Durch*

$$\langle x_0, \ldots, x_{n-1} \rangle \ = \ \mathrm{p}_0^{x_0} \ldots \mathrm{p}_{n-2}^{x_{n-2}} \mathrm{p}_{n-1}^{x_{n-1}+1} - 1$$

ist eine Bijektion

$$\langle \quad \rangle : \mathbb{N}^* \to \mathbb{N}$$

definiert. Es gilt

a) Die zweistellige Funktion Komponentenfunktion $(x)_i$*, definiert durch*

$$\big(\langle x_0, \ldots, x_{n-1} \rangle\big)_i = \begin{cases} x_i & (i < n) \\ 0 & \textit{sonst} \end{cases}$$

ist primitiv rekursiv.

b) Die Längenfunktion $\lg(x)$*, definiert durch*

$$\lg\big(\langle x_0, \ldots, x_{n-1} \rangle\big) = n$$

ist primitiv rekursiv.

c) Für alle n *ist* $\langle \quad \rangle : \mathbb{N}^n \to \mathbb{N}$ *primitiv rekursiv.*

d) Für alle x *ist* $\lg(x) \leq x$*. Wenn* $x > 0$*, ist* $(x)_i < x$*.*

Wir nennen $\langle x_0, \ldots, x_{n-1} \rangle$ die *Gödelnummer* der Folge $(x_0, \ldots, x_{n-1})$.

Beweis:

c) Folgt aus 12.1.

d) Klar

b) Es ist

$$\lg(x) = \mu y\ \forall z \leq x\big(y \leq z \to \ \mathrm{p}(y) \nmid (x+1)\big).$$

y kann durch x beschränkt werden. Wende jetzt 12.4 und 12.5 an.

a) Es ist

$$(x)_i = \begin{cases} \mu y \;\; \mathrm{p}(i)^{y+1} \not| \, (x+1) & (i < \lg(x) - 1) \\ \mu y \;\; \mathrm{p}(i)^{y+2} \not| \, (x+1) & (i = \lg(x) - 1) \\ 0 & (i \geq \lg(x) - 1) \end{cases}$$

y ist durch $x \dot{-} 1$ beschränkt.

□

Wenn es uns nur auf Rekursivität ankommt, sind nur die beiden Eigenschaften a) und b) von Bedeutung. Sei $\beta : \mathbb{N} \to \mathbb{N}$ eine rekursive Bijektion[1]. Dann definiert

$$< x_0, \dots, x_{n-1} >^{\beta} = \beta \langle x_0, \dots, x_{n-1} \rangle$$

eine Gödelnumerierung mit rekursiver Komponentenfunktion und rekursiver Längenfunktion. Es gilt aber auch die Umkehrung:

Bemerkung *Sei* $[\;] : \mathbb{N}^* \to \mathbb{N}$ *eine Gödelnumerierung mit rekursiver Komponentenfunktion* $[x]_i$ *und rekursiver Längenfunktion* $\mathrm{Lg}(x)$*. Dann gibt es eine rekursive Bijektion* $\beta : \mathbb{N} \to \mathbb{N}$ *mit* $[\;] = \langle\;\rangle^{\beta}$*.*

Beweis:

Man definiert β durch

$$\beta(s) = \mu t \, \big(\mathrm{Lg}(t) = \lg(s) \land \forall i < \lg(s) \; [t]_i = (s)_i\big).$$

□

Gödelisierung von Registermaschinen

Wir ordnen allen Befehlen, Maschinen, Wörtern und Konfigurationen eine Zahl, ihre *Gödelnummer* zu:

Objekt	Gödelnummer
Stopbefehl $b = 0$	$\ulcorner 0 \urcorner \; = \; 0$
Schreibbefehl $b = (r, l)$	$\ulcorner b \urcorner \; = \; \langle r, l \rangle$
Verzweigung $b = (r, c_0, \dots, c_L)$	$\ulcorner b \urcorner \; = \; \langle r, c_0, \dots, c_L \rangle$
Maschine $\mathcal{M} = (b_0, \dots, b_N)$	$\ulcorner \mathcal{M} \urcorner \; = \; \langle \ulcorner b_0 \urcorner, \dots, \ulcorner b_N \urcorner \rangle$
Wort $w = (a_{i_1}, \dots, a_{i_n})$	$\ulcorner w \urcorner \; = \; \langle i_1, \dots, i_n \rangle$
Konfiguration $\mathcal{K} = (c, R_0, \dots, R_{R-1})$	$\ulcorner \mathcal{K} \urcorner \; = \; \langle c, \ulcorner R_0 \urcorner, \dots, \ulcorner R_{R-1} \urcorner \rangle$

Lemma 12.7 *Es gibt eine primitiv rekursive Funktion* $\mathrm{N}(x, y)$*, sodaß für alle Maschinen* $\mathcal{M}$ *und passende Konfigurationen* $\mathcal{K}$

$$\mathrm{N}(\ulcorner \mathcal{M} \urcorner, \ulcorner \mathcal{K} \urcorner) = \ulcorner \mathcal{M}(\mathcal{K}) \urcorner.$$

[1] Die Umkehrung $\mu y \, \beta(y) = x$ einer rekursiven Bijektion ist wieder rekursiv

Beweis:
Wir überlegen zuerst, daß die folgenden Funktionen primitiv rekursiv sind:[2]

$$\begin{array}{lcl} \mathrm{Ers}(\langle x_0,\ldots,x_i,\ldots,x_{n-1}\rangle,i,y) & = & \langle x_0,\ldots,y,\ldots,x_{n-1}\rangle \\ \mathrm{Anh}(\langle x_0,\ldots,x_{n-1}\rangle,y) & = & \langle x_0,\ldots,x_{n-1},y\rangle \\ \mathrm{Str}(\langle x_0,\ldots,x_{n-1}\rangle) & = & \langle x_0,\ldots,x_{n-2}\rangle \end{array}$$

Um $\mathrm{N}(m,k)$ zu definieren, verwenden wir die Abkürzungen $c=(k)_0$, $b=(m)_c$, $r=(b)_0$, $w=(k)_{r+1}$, $l=\lg(w)\dot{-}1$ und $a=(w)_l$. Dann ist

$$\mathrm{N}(m,k)=\begin{cases} k & (\lg(b)<2) \\ \mathrm{Ers}\big(\mathrm{Ers}(k,0,c+1),r+1,\mathrm{Str}(w)\big) & (\lg(b)=2\wedge(b)_1=0) \\ \mathrm{Ers}\big(\mathrm{Ers}(k,0,c+1),r+1,\mathrm{Anh}(w,(b)_1)\big) & (\lg(b)=2\wedge(b)_1>0) \\ \mathrm{Ers}(k,0,(b)_{a+1}) & (\lg(b)>2). \end{cases}$$

□

<u>Beweis von 11.1</u>

Wir zeigen, daß jede maschinenberechenbare Funktion $f(x_1,\ldots,x_n)$ rekursiv ist. Wir machen Gebrauch von den folgenden Funktionen und Relationen, die man leicht als primitiv rekursiv erkennt:

$$\mathrm{Input}(R,x_1,\ldots,x_n)=\ulcorner\big(0,\emptyset,\underbrace{|^{x_1},\ldots,|^{x_n}}_{n},\underbrace{\emptyset,\ldots,\emptyset}_{R-n-1}\big)\urcorner$$

ist die Anfangskonfiguration einer R–Registermaschine mit Input $x_1,\ldots,x_n$.

$$\mathrm{Stop}(m,k)\iff m_{(k)_0}=0$$

trifft auf eine Maschine $m=\ulcorner\mathcal{M}\urcorner$ und eine Konfiguration $k=\ulcorner\mathcal{K}\urcorner$ zu, wenn $\mathcal{K}$ eine Stopkonfiguration von $\mathcal{M}$ ist.

$$\mathrm{Output}(k)=\lg((k)_1)$$

ist der Inhalt von Register $\mathcal{R}_0$, als Zahl interpretiert.

$$\mathrm{N}^s(m,k)$$

ist die s–fach iterierte Nachfolgerfunktion, definiert durch $\mathrm{N}^0(m,k)=k$ und

[2] In der Tat ist

$$\mathrm{Ers}(x,i,y)=\mu z\ \Big(\lg(z)=\lg(x)\wedge\forall j<\lg(x)(j\neq i\rightarrow(z)_j=(x)_j)\wedge(z)_i=y\Big).$$

Weil $\mathrm{Ers}(x,i,y)<(x+1)\mathrm{p}(i)^{y+2}$ läßt sich 12.5 anwenden. Weiterhin ist

$$\mathrm{Anh}(x,y)=\mu z\ \Big(\lg(z)=\lg(x)+1\wedge\forall j<\lg(x)((z)_j=(x)_j)\wedge(z)_{\lg(x)}=y\Big).$$

Wieder hat man eine primitiv rekursive Schranke:

$$\mathrm{Anh}(x,y)<(x+1)\mathrm{p}(\lg(x))^{y+2}$$

Schließlich ist

$$\mathrm{Str}(x)=\mu z\ \Big(\lg(z)=\lg(x)\dot{-}1\wedge\forall j<\lg(z)((z)_j=(x)_j)\Big)$$

und $\mathrm{Str}(x)<(x+1)\mathrm{p}(\lg(x)\dot{-}1)$.

$N^{s+1}(m,k) = N(m, N^s(m,k))$.

Wir definieren das primitiv rekursive *Kleene–Prädikat*

$$\begin{aligned} T_n(m, x_1, \dots, x_n, g) \iff\ & N^{(g)_1}\big(m, \mathrm{Input}(m, x_1, \dots, x_n)\big) = (g)_2 \\ & \wedge \mathrm{Stop}\big(m, (g)_2\big) \wedge \mathrm{Output}\big((g)_2\big) = (g)_0, \end{aligned}$$

das besagt, daß die Maschine m mit dem Input[3] $x_1, \dots, x_n$ nach $(g)_1$ Schritten mit dem Output $(g)_0$ stoppt[4].

Wenn f von $\mathcal{M}$ berechnet wird, ist

$$f(x_1 \dots, x_n) = \big(\mu g\ T_n(\ulcorner\mathcal{M}\urcorner, x_1, \dots, x_n, g)\big)_0. \tag{1}$$

f ist also rekursiv. Man nennt (1) die *Kleene–Normalform* von f.

Unser Beweis der Umkehrung von 11.1 macht keinen Gebrauch von den Details der Definition der Arbeitsweise von Registermaschinen. Er zeigt, daß *alle* irgendwie systematisch arbeitenden Rechenmaschinen nur rekursive Relationen berechnen können. Man nennt diese Erfahrungstatsache die

Churchsche These:

Alle irgendwie berechenbaren Funktionen sind rekursiv.

[3] dem wir sicherheitshalber m Register gegeben haben.
[4] Außerdem ist $(g)_2$ die Stopkonfiguration.

13 Rekursiv aufzählbare Mengen

Definition *Eine Relation R heißt rekursiv aufzählbar (r.a.), wenn für eine rekursive Relation $\overline{R}$*

$$R(x_1, \ldots, x_n) \iff \exists y\, \overline{R}(x_1, \ldots, x_n, y).$$

Insbesondere sind rekursive Relationen rekursiv aufzählbar.

Lemma 13.1 *Wenn P und R rekursiv aufzählbar sind, dann sind auch*

1. $P \vee R$
2. $P \wedge R$
3. $\exists z R(x_1, \ldots, x_n, z)$
4. $T(x_1, \ldots, x_n, w) \iff \forall z < w R(x_1, \ldots, x_n, z)$
5. $R(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n))$

rekursiv aufzählbar.

Beweis:

1. $P(\overline{x}) \vee R(\overline{x}) \iff \exists y \left(\overline{P}(\overline{x}, y) \vee \overline{R}(\overline{x}, y)\right)$
2. $P(\overline{x}) \wedge R(\overline{x}) \iff \exists s \left(\overline{P}(\overline{x}, (s)_0) \wedge \overline{R}(\overline{x}, (s)_1)\right)$
3. $\exists z R(\overline{x}, z) \iff \exists s\, \overline{R}(\overline{x}, (s)_0, (s)_1)$
4. $T(\overline{x}, w) \iff \exists s \forall z < w\, \overline{R}(\overline{x}, z, (s)_z)$
5. $R(f_1(\overline{x}), \ldots, f_k(\overline{x})) \iff \exists y\, \overline{R}(f_1(\overline{x}), \ldots, f_k(\overline{x}), y)$

□

Lemma 13.2 *Eine Menge von natürlichen Zahlen ist genau dann rekursiv aufzählbar, wenn sie leer ist oder das Bild einer rekursiven Funktion.*

Beweis:

Das Bild R der rekursiven Funktion f ist rekursiv aufzählbar, weil $R(x) \iff \exists z\, f(z) = x$.

Wenn umgekehrt $R(x) \iff \exists y\, \overline{R}(x, y)$ und $r \in R$, ist R Bild der rekursiven Funktion

$$f(z) = \begin{cases} (x)_0 & \text{wenn } \overline{R}((x)_0, (x)_1) \\ r & \text{sonst} \end{cases}$$

□

Satz 13.3 *Es gibt eine universelle rekursiv aufzählbare Relation $U \subset \mathbb{N}^2$. Das heißt*

a) U ist rekursiv aufzählbar.

b) Für jede rekursiv aufzählbare Menge R gibt es ein e, sodaß

$$R = \mathrm{W}_e = \{x \mid U(e,x)\}.$$

Beweis:
Sei $S(x,y)$ rekursiv und $\mathcal{M}$ eine Maschine, die versucht $\mu y \ \mathrm{K}_S(x,y) = 0$ zu berechnen. M stoppt genau dann beim Input x, wenn $\exists y \ S(x,y)$. Wir haben also $\exists y \ S(x,y) \iff \exists g \ \mathrm{T}_1(\ulcorner \mathcal{M} \urcorner, x, g)$. Die rekursiv aufzählbare Relation

$$U(e,x) \iff \exists g \ \mathrm{T}_1(e,x,g)$$

ist also universell. □

Folgerung 13.4 *Es gibt eine Menge, die rekursiv aufzählbar aber nicht rekursiv ist.*

Beweis:
$\neg\, U(x,x)$ kann nicht die Form W_e haben, weil $\neg\, U(e,e) \iff e \notin \mathrm{W}_e$. Also ist $\neg\, U(x,x)$ nicht rekursiv aufzählbar. $U(x,x)$ ist daher nicht rekursiv, aber rekursiv aufzählbar. □

Lemma 13.5 *R ist genau dann rekursiv, wenn R und $\neg\, R$ rekursiv aufzählbar sind.*

Beweis:
Sei $R(\overline{x}) \iff \exists y \ \overline{V}(\overline{x},y)$ und $\neg\, R(\overline{x}) \iff \exists y \ \overline{W}(\overline{x},y)$ für rekursive $\overline{V}$ und $\overline{W}$. Dann ist

$$g(x) = \mu y \ \big(\overline{V}(\overline{x},y) \vee \overline{W}(\overline{x},y)\big)$$

für alle x definiert und rekursiv. Und wir haben

$$R(\overline{x}) \iff \overline{V}(\overline{x}, g(\overline{x})).$$

□

14 Gödelnummern von Formeln

Sei $L = \{\lambda_1, \ldots, \lambda_l\}$ eine endliche Sprache[5]. Wir ordnen den Zeichen ζ

$$\begin{array}{cccccc} \dot{=} & \wedge & \neg & (&) & \exists \\ \lambda_1 & \ldots & \lambda_l & v_0 & v_1 & \ldots \end{array}$$

die folgenden Gödelnummern $\ulcorner\zeta\urcorner$ zu:

$$\begin{array}{cccccc} \langle 0,0\rangle & \langle 0,1\rangle & \langle 0,2\rangle & \langle 0,3\rangle & \langle 0,4\rangle & \langle 0,5\rangle \\ \langle 0,6\rangle & \ldots & \langle 0,l+5\rangle & \langle 1,0\rangle & \langle 1,1\rangle & \ldots \end{array}$$

Eine Zeichenreihe $\phi = \zeta_1\zeta_2\ldots\zeta_n$ hat die Gödelnummer[6]

$$\ulcorner\phi\urcorner = \langle\ulcorner\zeta_1\urcorner, \ulcorner\zeta_2\urcorner, \ldots, \ulcorner\zeta_n\urcorner\rangle.$$

Lemma 14.1 *Die folgenden Mengen sind rekursiv (sogar primitiv rekursiv).*

1. $\left\{\ulcorner t\urcorner \;\middle|\; t\ L\text{–}\mathit{Term}\right\}$
2. $\left\{\ulcorner\phi\urcorner \;\middle|\; \phi\ L\text{–}\mathit{Formel}\right\}$
3. $\left\{\ulcorner\phi\urcorner \;\middle|\; \phi\ L\text{–}\mathit{Aussage}\right\}$

Beweis:

Nach Churchs These sind die Mengen rekursiv. Eine genauere Überlegung zeigt die primitive Rekursivität. □

Definition *Eine Theorie T heißt*

1. *axiomatisierbar, wenn* $\left\{\ulcorner\phi\urcorner \;\middle|\; \phi \in T\right\}$ *rekursiv aufzählbar ist.*
2. *entscheidbar, wenn* $\left\{\ulcorner\phi\urcorner \;\middle|\; T \vdash \phi\right\}$ *rekursiv ist.*

Ein Beweis von ϕ ist eine Folge $\phi_0, \ldots, \phi_n = \phi$ von Formeln, die logische Axiome sind (siehe Seite 16) oder aus jeweils früheren Formeln mit Modus Ponens oder $\exists$–Einführung folgen. Die Gödelnummer eines solchen Beweises ist $\langle\ulcorner\phi_0\urcorner, \ldots, \ulcorner\phi_n\urcorner\rangle$.

Lemma 14.2 $\left\{(x, \ulcorner\phi\urcorner) \;\middle|\; x \text{ ist Gödelnummer eines Beweises von } \phi\right\}$ *ist primitiv rekursiv.*

Beweis:

Churchs These zeigt die Rekursivität. □

[5]Die Ergebnisse dieses Abschnitts verallgemeinern sich leicht auf *rekursive* Sprachen. Das sind Sprachen mit ausgezeichneten Aufzählungen (c_i), (f_i), (R_i) der Konstanten, Funktionszeichen und Relationszeichen, mit rekursiv von i abhängenden Stelligkeiten.

[6]Im Abschnitt 10 bezeichnete $\ulcorner\psi\urcorner$ einen Mengenterm.

Folgerung 14.3 $\left\{\ulcorner\phi\urcorner \mid \vdash \phi\right\}$ *ist rekursiv aufzählbar.*

Beweis:

$$\vdash \phi \Longleftrightarrow \exists x \;\; (x \text{ ist Gödelnummer eines Beweises von } \phi)$$

$\square$

Satz 14.4 *Wenn T axiomatisierbar ist, ist $\left\{\ulcorner\phi\urcorner \mid T \vdash \phi\right\}$ rekursiv aufzählbar.*

Beweis:
Die Funktion f, die der Gödelnummer einer Folge von Formeln $\phi_0, \ldots, \phi_n$ die Gödelnummer der Implikation $(\phi_1 \wedge \ldots, \phi_n) \to \phi_0$ zuordnet, ist rekursiv. Sei $T^* = \left\{\ulcorner\phi\urcorner \mid \phi \in T\right\}$ und $A = \left\{\ulcorner\phi\urcorner \mid \vdash \phi\right\}$. Weil T^* und A rekursiv aufzählbar sind, ist auch

$$\left\{\ulcorner\phi\urcorner \mid T \vdash \phi\right\} = \left\{(x)_0 \mid f(x) \in A \wedge \forall\, i < \lg(x)\; (0 < i \to (x)_i \in T^*)\right\}$$

rekursiv aufzählbar. $\square$

Definition *Eine widerspruchsfreie L–Theorie T heißt vollständig, wenn*

$$T \vdash \phi \quad \textit{oder} \quad T \vdash \neg\,\phi$$

für jede L–Aussage ϕ.

Folgerung 14.5 *Wenn T axiomatisierbar und vollständig ist, ist T entscheidbar.*

Beweis:
Sei A die Menge der Gödelnummern aller L–Aussagen, und B die Menge der Gödelnummern der T beweisbaren L–Aussagen. f sei eine rekursive Funktion mit $f(\ulcorner\phi\urcorner) = \ulcorner\neg\,\phi\urcorner$. Aus der Vollständigkeit von T folgt dann

$$x \notin B \;\Leftrightarrow\; x \notin A \vee f(x) \in B.$$

Mit 13.5 folgt die Behauptung. $\square$

15 Ein anderer Aufbau der rekursiven Funktionen

Satz 15.1 *Alle rekursiven Funktionen lassen sich aus den Grundfunktionen*

$$\mathrm{S}(x),\ \mathrm{I}_i^n,\ \mathrm{C}_0^0,\ +,\ \cdot,\ \mathrm{K}_<$$

durch Anwenden der Regeln **R1** *(Einsetzung) und* **R3** *(μ–Rekursion) gewinnen.*

Wir werden den Satz im Rest dieses Abschnitts beweisen. Wir nennen die Funktionen, die sich so aufbauen wie im Satz angegeben, *$*$–rekursiv* . Wenn wir zeigen können, daß die Klasse der $*$–rekursiven Funktionen abgeschlossen ist unter **R2** (primitive Rekursion), sind wir fertig.

Lemma 15.2

1. *$x \dot{-} y$ ist $*$–rekursiv.*
2. *Die Klasse der $*$–rekursiven Relationen ist abgeschlossen unter Booleschen Kombinationen und beschränkter Quantifizierung. (Siehe 12.2 und 12.4.)*
3. *$x \doteq y$ ist $*$–rekursiv.*
4. *$x \equiv y \pmod z$ ist $*$–rekursiv.*
5. *Die Klasse der $*$–rekursiven Funktionen ist abgeschlossen unter Definition durch Fallunterscheidung. (Siehe 12.3.)*

Beweis:

1. $x \dot{-} y \quad = \quad \mu z\ \ x < (y + z) + 1$
2. Die Abgeschlossenheit unter booleschen Kombinationen sieht man wie in 12.2.
   Wenn $P(x, y)$ $*$–rekursiv ist, definieren wir
   $$g(x, z) = \mu y\ \big(P(x, y) \vee y \doteq z\big).$$
   Dann ist
   $$\exists y < z\ P(x, y) \Leftrightarrow g(x, z) < z$$
   $*$–rekursiv.
3. $x \doteq y \Leftrightarrow (\neg\, x < y \wedge \neg\, y < x)$
4. $x \equiv y \pmod z \Leftrightarrow \exists w < (x + y + 1)\big(x \doteq y + wz \vee y \doteq x + wz\big)$
5. Wie 12.3.

$\square$

Lemma 15.3 (Gödels β–Funktion) *Es gibt eine $*$–rekursive Funktion $\beta(a,b,i)$ mit folgender Eigenschaft. Für jede endliche Folge $c_0, c_1, \ldots, c_{n-1}$ gibt es a und b, sodaß*

$$\beta(a,b,i) = c_i$$

für $i = 0, \ldots, n-1$.

Beweis:

$$\beta(a,b,i) = \mu z\; z \equiv a \pmod{b(i+1)+1}$$

ist $*$–rekursiv. Seien $c_0, c_1, \ldots, c_{n-1}$ 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. Dann sind die $b \cdot 1 + 1, b \cdot 2 + 1, \ldots, b \cdot n + 1$ 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 $b(j-i)$ und daher auch von von $j - i$. $j - i$ könnte kein Teiler von b sein, ein Widerspruch.

a sei eine gemeinsame Lösung der Kongruenzen

$$\begin{array}{lcll} a & \equiv & c_0 & \pmod{b \cdot 1 + 1} \\ a & \equiv & c_1 & \pmod{b \cdot 2 + 1} \\ \vdots & & \vdots & \\ a & \equiv & c_{n-1} & \pmod{b \cdot n + 1} \end{array}$$

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. □

Beweis (von 15.1):

Wir müssen zeigen, daß die $*$–rekursiven Funktionen unter primitiver Rekursion abgeschlossen sind. Nehmen wir also an, daß g und h $*$–rekursiv sind und daß f definiert ist durch

$$\begin{array}{rcl} f(x,0) & = & g(x) \\ f(x,y+1) & = & h(x,y,f(x,y)). \end{array}$$

Die Relation

$$R(x,y,a,b) \Leftrightarrow \big(\beta(a,b,0) = g(x) \;\wedge\; \forall i < y\; \beta(a,b,i+1) = h(x,i,\beta(a,b,i))\big)$$

ist $*$–rekursiv. Offenbar gilt $\forall x, y\; \exists a, b\; R(x,y,a,b)$. Also ist

$$S(x,y) = \mu s\; \exists a, b \leq s\; R(x,y,a,b)$$

$*$–rekursiv. Dann ist

$$f(x,y) = \mu z\; \exists a, b \leq S(x,y)\; \big(R(x,y,a,b) \wedge z = \beta(a,b,y)\big)$$

und f ist $*$–rekursiv. □

Kapitel 4

Arithmetik

16 Definierbare Relationen

Definition *Eine Relation $R \subset \mathbb{N}^n$ heißt arithmetisch, wenn sie in der Struktur*

$$\mathfrak{N} = (\mathbb{N}, 0, \mathrm{S}, +, \cdot, <)$$

definierbar ist.

Das bedeutet, daß für eine L_N–Formel ϕ

$$R(a_1, \ldots, a_n) \Longleftrightarrow \mathfrak{N} \models \phi[a_1, \ldots, a_n].$$

Eine Funktion heißt f arithmetisch, wenn ihr Graph arithmetisch ist:

$$f(a_1, \ldots, a_n) = a_0 \Longleftrightarrow \mathfrak{N} \models \phi_f[a_0, \ldots, a_n].$$

Lemma 16.1 *Rekursive Funktionen sind arithmetisch.*

Beweis:

Wir verwenden 15.1: Die Grundfunktionen $\mathrm{S}(x)$, I_i^n, C_0^0, $+$, $\cdot$, $\mathrm{K}_<$ sind klarerweise arithmetisch. Zum Beispiel ist

$$\mathrm{K}_<(a_1, a_2) = a_0 \Longleftrightarrow \mathfrak{N} \models (a_0 \doteq \underline{0} \wedge a_1 < a_2) \vee (a_0 \doteq \mathrm{S}(\underline{0}) \wedge \neg\, a_1 < a_2).$$

Es bleibt zu zeigen, daß das System aller arithmetischen Funktionen unter den Regeln **R1** und **R3** abgeschlossen ist. Um die Notation zu vereinfachen, nehmen wir an, daß $n = 2$.

R1: Sei h durch ϕ_h und die g_i durch ϕ_i definiert. Dann wird $h(g_1(x_1), g_2(x_1)) = x_0$ durch $\exists y_1, y_2 \left(\phi_1(y_1, x_1) \wedge \phi(y_2, x_2) \wedge \phi_h(x_0, y_1, y_2)\right)$ definiert.

R3 : Sei $g(x_1, x_2) = x_0$ definiert durch $\phi(x_0, x_1, x_2)$. Dann wird $\mu x_2\ (g(x_1, x_2) \doteq 0) = x_0$ definiert durch

$$\phi(\underline{0}, x_1, x_0) \wedge \forall x_2 < x_0\, \neg\, \phi(\underline{0}, x_1, x_2).$$

$\square$

Folgerung 16.2 *Alle rekursiv aufzählbaren Relationen sind arithmetisch.*

Beweis:
Sei $R(x_1, \dots, x_n) \Leftrightarrow \exists y\ \overline{R}(x_1, \dots, x_n, y)$ für eine rekursiv Relation $\overline{R}$. Wenn $\phi(x_0, \dots, x_n, y)$ die charakteristische Funktion von $\overline{R}$ definiert, wird R definiert von $\exists y\ \phi(\underline{0}, x_1, \dots, x_n, y)$. $\square$

Folgerung 16.3 *Die Theorie*

$$\mathrm{Th}(\mathfrak{N}) = \{\phi \mid \phi\ L_N\text{–}Aussage,\ \mathfrak{N} \models \phi\}$$

der natürlichen Zahlen ist unentscheidbar.

Beweis:
Sei

$$\Delta_a = \mathrm{S}^a(\underline{0})$$

der kanonische L_N–Term, der in $\mathfrak{N}$ die Zahl a darstellt[1]. Wenn $\mathrm{Th}(\mathfrak{N})$ entscheidbar wäre, wären alle arithmetischen Mengen

$$\{a \mid \phi(\Delta_a) \in \mathrm{Th}(\mathfrak{N})\}$$

rekursiv. Es gibt aber rekursiv aufzählbare Mengen, die nicht rekursiv sind (13.4). $\square$
Es gilt sogar:

Satz 16.4 $\mathrm{Th}(\mathfrak{N})$ *ist nicht arithmetisch.*

Beweis:
Betrachte die Relation $U(e, a)$, die genau dann gilt, wenn e die Gödelnummer einer Formel $\phi = \phi(v_0)$ ist, für die $\mathfrak{N} \models \phi(\Delta_a)$. Weil jede arithmetische Relation die Form

$$\{a \mid U(e, a)\}$$

für geeignetes e hat, kann die Relation $\neg\, U(x, x)$ nicht arithmetisch sein. Daraus folgt, daß auch $\mathrm{Th}(\mathfrak{N})$ nicht arithmetisch ist. $\square$

Folgerung 16.5 (Erster Gödelscher Unvollständigkeitssatz) *Jede arithmetische Teiltheorie von* $\mathrm{Th}(\mathfrak{N})$ *ist unvollständig.*

Beweis:
Wenn T arithmetisch ist, ist auch $T^* = \{\phi \mid T \vdash \phi\}$ arithmetisch. Wäre T vollständig, wäre aber $T^* = \mathrm{Th}(\mathfrak{N})$ und $\mathrm{Th}(\mathfrak{N})$ arithmetisch. $\square$

[1] Rekursive Definition: $\Delta_0 = \underline{0}$, $\Delta_{a+1} = \mathrm{S}(\Delta_a)$

17 Das System Q

Die Axiome des Systems Q sind

Q1 $\forall x \;\; x + \underline{0} \doteq x$

Q2 $\forall x, y \;\; x + \mathrm{S}(y) \doteq \mathrm{S}(x + y)$

Q3 $\forall x \;\; x \cdot \underline{0} \doteq \underline{0}$

Q4 $\forall x, y \;\; x \cdot \mathrm{S}(y) \doteq x \cdot y + x$

Q5 $\forall x \;\; \neg\, x < \underline{0}$

Q6 $\forall x, y \;\; x < \mathrm{S}(y) \longleftrightarrow (x \doteq y \lor x < y)$

Q ist offenbar eine *wahre* L_N–Theorie (damit meinen wir, daß die Axiome von Q in $\mathfrak{N}$ gelten.) Die ersten zwei Axiome kann man auffassen als eine rekursive Definition der Addition, die nächsten beiden als eine rekursive Definition der Multiplikation und die letzten beiden als eine rekursive Definition der Kleiner–Relation. Man erhält zum Beispiel sofort:

Lemma 17.1 *In* Q *sind für alle a und b ableitbar:*

Q*1 $\Delta_a + \Delta_b \doteq \Delta_{a+b}$

Q*2 $\Delta_a \cdot \Delta_b \doteq \Delta_{ab}$

Q*3 $\forall x \;\; x < \Delta_a \longleftrightarrow \big(x \doteq \Delta_0 \lor x \doteq \Delta_1 \lor \cdots \lor x \doteq \Delta_{a-1}\big)$ □

Man nennt die Theorie, die aus den drei Axiomenschemata **Q*1**, **Q*2**, **Q*3** besteht, Q* .[2] Wir fassen Q* als Teiltheorie von Q auf.

Aus **Q*3** folgt sofort (durch Induktion über b)

Folgerung *Für alle natürlichen Zahlen a und b*

$$\begin{array}{rcl} a \neq b & \Longrightarrow & \mathrm{Q}^* \vdash \neg\, \Delta_a \doteq \Delta_b \\ a < b & \Longrightarrow & \mathrm{Q}^* \vdash \Delta_a < \Delta_b \\ a \not< b & \Longrightarrow & \mathrm{Q}^* \vdash \neg\, \Delta_a < \Delta_b \end{array}$$

Man schließt leicht daraus (vgl. den Beweis von 17.2):

Folgerung *Alle wahren quantorenfreien L_N–Aussagen sind in* Q* *beweisbar.*

Das läßt sich auch so ausdrücken: Sei $\mathfrak{M}$ ein Modell von Q* und $\mathfrak{U}$ die Unterstruktur mit Universum $\{\Delta_a^{\mathfrak{M}} \mid a \in \mathbb{N}\}$. Dann ist $\mathfrak{U} \cong \mathfrak{N}$.

[2] Oder auch *Cobhams Theorie.*

Definition *Eine Σ_1–Formel entsteht aus quantorenfreien Formeln durch Anwenden von $\wedge$, $\vee$, $\exists x$ und beschränkten Allquantoren*

$$\forall x < t.$$

Dabei ist t ein Term und $\forall x < t\ \phi$ bedeutet $\forall x\ (x < t \to \phi)$.

Eine Σ_1–Formel im engeren Sinn entsteht aus Formeln der Form $\underline{0} \doteq x$, $\mathrm{S}(x) \doteq y$, $x + y \doteq z$, $x \cdot y \doteq z$, $x \doteq y$, $\neg x \doteq y$, $x < y$, $\neg x < y$ durch Anwenden von $\wedge$, $\vee$, $\exists x$, $\forall x < y$.

Bemerkung *Jede Σ_1–Formel ist zu einer Σ_1–Formel im engeren Sinn äquivalent.*

Beweis: Man eliminiert kompliziertere Terme mit Hilfe von Existenzquantoren. Zum Beispiel ist $\mathrm{S}(x) + y \doteq \mathrm{S}(z)$ äquivalent zu

$$\exists\, x_1, z_1\ (\mathrm{S}(x) \doteq x_1 \wedge \mathrm{S}(z) \doteq z_1 \wedge x_1 + y \doteq z_1).$$

Satz 17.2 *Alle wahren Σ_1–Aussagen sind in Q^* beweisbar.*

Beweis:

Wir zeigen für alle Σ_1–Formeln $\phi(x_1, \ldots, x_n)$ im engeren Sinn und alle natürlichen Zahlen $a_1, \ldots, a_n$, daß

$$\mathfrak{N} \models \phi[a_1, \ldots, a_n] \Longrightarrow \mathrm{Q}^* \vdash \phi(\Delta_{a_1}, \ldots, \Delta_{a_n})$$

durch Induktion über den Aufbau von ϕ. Wenn ϕ eine Primformel ist, folgt die Behauptung aus Lemma 17.1. Der Induktionsschritt ist einfach, wenn ϕ eine Konjunktion oder eine Disjunktion ist.

Wenn $\mathfrak{N} \models \exists x_0 \psi[a_1, \ldots, a_n]$, ist $\mathfrak{N} \models \psi[a_0, a_1, \ldots, a_n]$ für ein $a_0 \in \mathbb{N}$. Nach Induktionsvoraussetzung $\mathrm{Q}^* \vdash \psi(\Delta_{a_0}, \Delta_{a_1}, \ldots, \Delta_{a_n})$ und daher

$$\mathrm{Q}^* \vdash \exists x_0 \psi(x_0, \Delta_{a_1}, \ldots, \Delta_{a_n}).$$

Wenn $\mathfrak{N} \models \forall x_0 < x_1 \psi[a_1, \ldots, a_n]$, ist $\mathfrak{N} \models \phi[a_0, a_1, \ldots, a_n]$ und daher nach Induktionsvoraussetzung $\mathrm{Q}^* \vdash \phi[\Delta_{a_0}, \Delta_{a_1}, \ldots, \Delta_{a_n}]$ für alle $a_0 < a_1$. Wegen $\mathbf{Q^*3}$ folgt daraus

$$\mathrm{Q}^* \vdash \forall x_0 < x_1 \psi[a_1, \ldots, a_n].$$

□

Lemma 17.3 *Alle rekursiven Funktionen und alle rekursiv aufzählbaren Relationen sind mit Σ_1–Formeln definierbar.*

Beweis:

Der Beweis von Lemma 16.1 muß nur an einer Stelle abgeändert werden. Wenn man zeigen will, daß die Σ_1–definierbaren Funktionen unter **R3** abgeschlossen sind, verwendet man statt $\neg\, \phi(\underline{0}, x_1, x_2)$ die Formel $\exists y (\neg\, \underline{0} \doteq y \wedge \phi(y, x_1, x_2))$.
□

Übung *Σ_1–definierbare Relationen sind rekursiv aufzählbar, Σ_1–definierbare Funktionen rekursiv.*

Folgerung 17.4 Q *ist unentscheidbar. Es ist sogar jede wahre Erweiterung von* Q^* *unentscheidbar.*[3]

Beweis:

Sei $R(x)$ rekursiv aufzählbar und definiert durch die Σ_1–Formel ϕ. T sei eine wahre Erweiterung von Q^*. Dann ist für alle a

$$\begin{array}{rcccccc} R(a) & \to & \mathfrak{N} \models \phi(\Delta_a) & \to & Q^* \vdash \phi(\Delta_a) & \to & T \vdash \phi(\Delta_a) \\ \neg\, R(a) & \to & \mathfrak{N} \not\models \phi(\Delta_a) & \to & & & T \not\vdash \phi(\Delta_a) \end{array}$$

Wenn T entscheidbar wäre, wären also alle rekursiv aufzählbare Relationen rekursiv. □

Satz 17.5 *Der Prädikatenkalkül ist unentscheidbar: Es gibt eine endliche Sprache L, für die*

$$\{\phi \mid \phi \text{ allgemeingültige } L\text{–Formel}\}$$

nicht rekursiv ist.

Beweis:

Man überlegt sich leicht:

Übung *Wenn man eine entscheidbare Theorie um endlich viele Axiome erweitert, erhält man wieder eine entscheidbare Theorie.*

Q ist endliche unentscheidbare Erweiterung der leeren L_N–Theorie. Also ist die leere L_N–Theorie unentscheidbar und $L = L_N$ beweist den Satz. □

Definition *Sei T eine L_N–Theorie und $f : \mathbb{N}^n \to \mathbb{N}$ eine Funktion. Die Formel $\phi(x_0, \ldots, x_n)$ repräsentiert f in T, wenn für alle $a_0 = f(a_1, \ldots, a_n)$*

$$T \vdash \forall x(x_0 \doteq \Delta_{a_0} \longleftrightarrow \phi(x_0, \Delta_{a_1}, \ldots, \Delta_{a_n})$$

Wenn T eine wahre Theorie ist und ϕ die Funktion f repräsentiert, wird f auch von ϕ definiert. Wenn ϕ eine Σ_1–Formel ist, und T wahre Σ_1–Formeln beweist, repräsentiert eine Σ_1–Formel ϕ die Funktion f genau dann, wenn ϕ f definiert und für alle $a_1, \ldots, a_n$

$$T \vdash \forall x_0, x_0' \left(\phi(x_0, \Delta_{a_1}, \ldots, \Delta_{a_n}) \wedge \phi(x_0', \Delta_{a_1}, \ldots, \Delta_{a_n})\right) \to x_0 \doteq x_0'.$$

Wenn die wahre Theorie T axiomatisierbar ist, und f in T von ϕ repräsentierbar wird, ist f rekursiv, weil dann die Relation

$$a_0 = f(a_1, \ldots, a_n) \Longleftrightarrow T \vdash \phi(\Delta_{a_0}, \Delta_{a_1}, \ldots, \Delta_{a_n})$$

rekursiv aufzählbar ist.

[3] …und damit auch Q^*.

Lemma 17.6 *Jede rekursive Funktion läßt sich in* Q^* *durch eine* Σ_1*–Formel repräsentieren.*

Beweis:
Die Konstruktion im Beweis von 16.1 (und 17.3) funktioniert auch hier, bis auf den Fall **R3**. Sei also $g(x_1, x_2) = x_0$ in Q^* repräsentiert durch $\phi(x_0, x_1, x_2)$. Dann wird $f(x_1) = \mu x_2\ (g(x_1, x_2) = 0)$ definiert durch

$$\psi(x_0, x_1) = \big(\alpha(x_0, x_1) \wedge \beta(x_0, x_1) \wedge \gamma(x_0)\big),$$

wobei

$$\begin{aligned} \alpha(x_0, x_1) &= \phi(\underline{0}, x_1, x_0) \\ \beta(x_0, x_1) &= \forall x_2 < x_0\, \exists y\, \big(\neg\, \underline{0} \doteq y\ \wedge\ \phi(y, x_1, x_2)\big) \\ \gamma(x_0) &= \big(\underline{0} \leq x_0\ \wedge\ \forall z < x_0\ \mathrm{S}(z) \leq x_0\big)^4. \end{aligned}$$

$(\alpha \wedge \beta)$ ist die schon im Beweis von 17.3 benutzte Formel; $\gamma(x_0)$ trifft in $\mathfrak{N}$ auf alle Zahlen zu. Also wird f von ψ definiert. Sei nun $a_0 = f(a_1)$. Wir müssen zeigen, daß

$$\mathrm{Q}^* \vdash \forall x_0\ \big(\psi(x_0, \Delta_{a_1}) \rightarrow x_0 \doteq \Delta_{a_0}\big)$$

Wir argumentieren in Q^*: Zunächst ist klar, daß, für alle $a_2 \in \mathbb{N}$, $\exists y\, \big(\neg\, \underline{0} \doteq y\ \wedge\ \phi(y, a_1, a_2)\big)$ gleichbedeutend ist mit $\neg\, \phi(\underline{0}, a_1, a_2)$. Nehmen wir an, daß $\psi(x_0, a_1)$. Aus $\gamma(x_0)$ folgt induktiv, daß x_0 entweder größer ist als alle $0, \ldots, a_0$, oder gleich einer dieser Zahlen ist. Im ersten Fall würde aus $a_0 < x_0$ folgen, daß sich $\alpha(a_0, a_1)$ und $\beta(x_0, a_1)$ widersprechen. Wenn x_0 gleich einer der Zahlen $0, \ldots, a_0 - 1$ ist, folgt $x_0 < a_0$, und $\alpha(x_0, a_1)$ liegt im Widerspruch mit $\beta(a_0, a_1)$. Also ist $x = a_0$. □

Folgerung 17.7 *Jeder rekursive Relation* R *wird in* Q^* *von einer* Σ_1*–Formel* ϕ *repräsentiert:*

$$\begin{aligned} R(a_1, \ldots, a_n) &\ \Rightarrow\ \mathrm{Q}^* \vdash \phi(\Delta_{a_1}, \ldots, \Delta_{a_n}) \\ \neg\, R(a_1, \ldots, a_n) &\ \Rightarrow\ \mathrm{Q}^* \vdash \neg\, \phi(\Delta_{a_1}, \ldots, \Delta_{a_n}) \end{aligned}$$

Beweis:
Sei K_R repräsentiert von ρ. Setze $\phi(x_1, \ldots, x_n) = \rho(\underline{0}, x_1, \ldots, x_n)$. □

Satz 17.8 (Fixpunktsatz) *Zu jeder* L_N*–Formel* $\psi(v_0)$ *gibt es eine* L_N*–Aussage* ϕ *mit*

$$\mathrm{Q}^* \vdash \phi \longleftrightarrow \psi\big(\Delta_{\ulcorner \phi \urcorner}\big).$$

Wenn $\psi(v_0)$ *eine* Σ_1*–Formel ist, findet man auch* ϕ *als* Σ_1*–Formel.*

Beweis:

[4] $s \leq t$ steht für $(s < t \vee s \doteq t)$.

(Eine Variante des Beweises von 10.1) Termeinsetzen wird beschrieben durch eine rekursive Funktion

$$\mathrm{Sub}(\ulcorner\chi(v_0)\urcorner, a) = \ulcorner\chi(\Delta_a)\urcorner.$$

Sei Sub in Q^* repräsentiert durch die Σ_1–Formel σ. Dann ist also für alle $\chi(v_0)$ und a

$$\mathrm{Q}^* \vdash \forall x_0 \; \big(x_0 \doteq \Delta_{\ulcorner\chi(\Delta_a)\urcorner} \longleftrightarrow \sigma(x_0, \Delta_{\ulcorner\chi(v_0)\urcorner}, \Delta_a) \big).$$

Wir setzen

$$\rho(v_0) = \exists x_0 \; (\psi(x_0) \wedge \sigma(x_0, v_0, v_0)).$$

Dann ist für alle $\chi(v_0)$

$$\mathrm{Q}^* \vdash \rho\big(\Delta_{\ulcorner\chi(v_0)\urcorner}\big) \longleftrightarrow \psi\big(\Delta_{\ulcorner\chi(\Delta_{\ulcorner\chi(v_0)\urcorner})\urcorner}\big).$$

Für $\chi = \rho$ ergibt sich

$$\mathrm{Q}^* \vdash \rho\big(\Delta_{\ulcorner\rho(v_0)\urcorner}\big) \longleftrightarrow \psi\big(\Delta_{\ulcorner\rho(\Delta_{\ulcorner\rho(v_0)\urcorner})\urcorner}\big).$$

Also leistet $\phi = \rho\big(\Delta_{\ulcorner\rho(v_0)\urcorner}\big)$ das Gewünschte. □

Folgerung 17.9 *Jede konsistente Erweiterung von* Q^* *ist unentscheidbar.*

Beweis:
Sei T eine entscheidbare Erweiterung von Q^*. Die Menge der Gödelnummern aller T beweisbaren Aussagen sei in Q^* durch die Formel τ repräsentiert. Das heißt, daß $\mathrm{Q}^* \vdash \tau(\Delta_{\ulcorner\phi\urcorner})$ für in T beweisbare und $\mathrm{Q}^* \vdash \neg\,\tau\big(\Delta_{\ulcorner\phi\urcorner}\big)$ für in T unbeweisbare ϕ. Mit dem Fixpunktsatz verschaffen wir uns eine Aussage δ mit

$$\mathrm{Q}^* \vdash \delta \longleftrightarrow \neg\,\tau\big(\Delta_{\ulcorner\delta\urcorner}\big).$$

Die beiden Implikationsketten

$$T \not\vdash \delta \;\Rightarrow\; \mathrm{Q}^* \vdash \neg\,\tau\big(\Delta_{\ulcorner\delta\urcorner}\big) \;\Rightarrow\; \mathrm{Q}^* \vdash \delta \;\Rightarrow\; T \vdash \delta,$$

und

$$T \vdash \delta \;\Rightarrow\; \mathrm{Q}^* \vdash \tau\big(\Delta_{\ulcorner\delta\urcorner}\big) \;\Rightarrow\; \mathrm{Q}^* \vdash \neg\,\delta \;\Rightarrow\; T \vdash \neg\,\delta,$$

zeigen, daß T inkonsistent ist. □

Folgerung 17.10 *Jede mit* Q *konsistente* L_N*–Theorie ist unentscheidbar.*

Beweis:
$T \cup \mathrm{Q}$ ist eine unentscheidbare endliche Erweiterung von T. □

Man kann zeigen, daß sogar jede mit Q^* konsistente L_N–Theorie unentscheidbar ist.

Gödel hat den Ersten Unvollständigkeitssatz (16.5) auf folgende Weise mit dem Fixpunktsatz bewiesen: Sei T eine wahre arithmetischen Theorie. Wir wollen zeigen, daß T unvollständig ist. Die Folgerungen aus T bilden eine arithmetische Menge. Also gibt es ein τ mit

$$\mathfrak{N} \models \tau\bigl(\Delta_{\ulcorner \chi \urcorner}\bigr) \;\Leftrightarrow\; T \vdash \chi$$

für alle χ. Sei ϕ eine Aussage mit

$$\mathrm{Q}^* \vdash \phi \longleftrightarrow \neg\,\tau\bigl(\Delta_{\ulcorner \phi \urcorner}\bigr).$$

Dann ist

$$\mathfrak{N} \models \phi \;\Leftrightarrow\; \mathfrak{N} \models \neg\,\tau\bigl(\Delta_{\ulcorner \phi \urcorner}\bigr) \;\Leftrightarrow\; T \not\vdash \phi.$$

Weil T wahr ist, ist das ist nur möglich, wenn $\mathfrak{N} \models \phi$ und $T \not\vdash \phi$, wenn also ϕ eine wahre, aber unbeweisbare Aussage ist.

Aus 17.9 folgt, daß jede konsistente axiomatisierbare Erweiterung von Q unvollständig ist. Das gilt nicht für arithmetische Erweiterungen:

Bemerkung *Sei L eine endliche (oder rekursive) Sprache. Dann hat jede arithmetische L–Theorie eine arithmetische Vervollständigung.*

18 Peanoarithmetik

Die Axiome der Peanoarithmetik P sind die Axiome von Q und das *Induktionsschema*:

$$\forall x_1, \ldots, x_n \Big[\big(\phi(\bar{x}, \underline{0}) \wedge \forall y(\phi(\bar{x}, y) \to \phi(\bar{x}, \mathrm{S}(y))\big) \to \forall y \phi(\bar{x}, y) \Big]$$

Ein Modell von Q ist genau dann ein Modell von P, wenn jede definierbare Menge von Elementen, die $\underline{0}$ enthält und unter S abgeschlossen ist, alle Elemente enthält.

Lemma 18.1 *In* P *sind ableitbar:*

1. *Die Nachfolgeroperation* S *ist injektiv. Jedes Element außer* $\underline{0}$ *hat einen Vorgänger.*
2. $<$ *ist eine lineare Ordnung.* $\underline{0}$ *ist kleinstes Element;* $\mathrm{S}(x)$ *ist unmittelbarer Nachfolger von* x*.*
3. $+, \cdot$ *definieren einen kommutativen Halbring mit Nullelement* $\underline{0}$ *und Einselement* Δ_1*.*
4. $+$ *und* $\cdot$ *sind monoton. Es ist gilt* $x \leq y \longleftrightarrow \exists z\; x + z \doteq y$*.*

Das ist alles, was man braucht, um elementare Zahlentheorie zu entwickeln. Nach 16.5 ist P zwar unvollständig (siehe auch 19.4), man hat aber erst vor wenigen Jahren „mathematische" Sätze gefunden, die in P nicht beweisbar sind.

Beweis:

Ich zeige nur 2. Der Beweis der anderen Behauptungen ist ebenso leicht.

Beweis von 2: Aus **Q6** folgt, daß die Menge aller x, die größer oder gleich $\underline{0}$ sind, unter S abgeschlossen ist. Mit dem Induktionsaxiom folgt also

$$\underline{0} \leq y. \tag{1}$$

für alle x. Als nächstes zeigen wir, daß für alle x

$$\forall y\; (y < x \to \mathrm{S}(y) \leq x). \tag{2}$$

Die Menge A aller Elemente mit dieser Eigenschaft enthält $\underline{0}$ wegen **Q5**. Nehmen wir an, daß $x \in A$. Um zu zeigen, daß $\mathrm{S}(x) \in A$, betrachten wir ein $y < \mathrm{S}(x)$. Aus **Q6** folgt $y \leq x$. Wenn $y < x$, folgt $\mathrm{S}(y) \leq x$, weil $x \in A$, und daraus $\mathrm{S}(y) < \mathrm{S}(x)$ wegen **Q6**. Aus $y = x$ folgt $\mathrm{S}(y) = \mathrm{S}(x)$.

Jetzt zeigen wir durch Induktion, daß alle x mit allen anderen Elementen vergleichbar sind. Wegen (1) ist Null mit allen Elementen vergleichbar. Nehmen wir an, daß x mit allen Elementen vergleichbar ist. Dann ist auch $\mathrm{S}(x)$ mit jedem y vergleichbar: Wenn $y \leq x$, ist $y < \mathrm{S}(x)$ wegen **Q6**, und wenn $x < y$, ist $\mathrm{S}(x) \leq y$ wegen (2).

Die Transitivität

$$x < y < z \to x < z$$

beweisen wir mit Induktion über z. Für $z = \underline{0}$, ist nichts zu zeigen. Aus $x < y < \mathrm{S}(z)$ folgt $x < y \leq z$ und daraus, nach Induktionsvoraussetzung, $x < z$ und damit $x < \mathrm{S}(z)$.

Auch die Irreflexivität

$$\neg\, x < x$$

beweisen wir durch Induktion: $\neg\, \underline{0} < \underline{0}$ folgt aus **Q5**. Für den Induktionsschritt nehmen wir an, daß $\mathrm{S}(x) < \mathrm{S}(x)$. Daraus folgt $\mathrm{S}(x) \leq x$. Zusammen mit $x < \mathrm{S}(x)$ und der Transitivität ergibt sich $x < x$, was der Induktionsvoraussetzung widerspricht.

Für lineare Ordnungen drückt **Q6** gerade aus, daß $\mathrm{S}(x)$ unmittelbarer Nachfolger von x ist. □

Das nächste Lemma bedeutet, daß alle Modelle von P definierbar–wohlgeordnet sind: Jede nicht–leere definierbare Teilmenge hat ein kleinstes Element.

Lemma 18.2 (Verallgemeinerte Induktion) *In* P *ist beweisbar:*

$$\forall x_1, \ldots, x_n \Big[\big(\forall y (\forall z < y\, \phi(\bar{x}, z) \rightarrow \phi(\bar{x}, y) \big) \rightarrow \forall y \phi(\bar{x}, y) \Big]$$

Beweis:
Wir halten $x_1, \ldots, x_n$ fest und nehmen an, daß $\forall y (\forall z < y\, \phi(\bar{x}, z) \rightarrow \phi(\bar{x}, y)\big)$. Sei A die Menge aller y mit $\forall z < y\, \phi(\bar{x}, z)$. A enthält $\underline{0}$ und, wenn y zu A gehört, folgt $\phi(\bar{x}, y)$ und damit $\mathrm{S}(y) \in A$. Also gehören alle Elemente zu A. □

Sei $\phi(v_0, \ldots, v_n)$ eine Σ_1–Formel, die in P eine Funktion definiert:

$$\mathrm{P} \vdash \forall v_1, \ldots, v_n \exists !\, v_0 \phi(v_0, \ldots, v_n).$$

Wir führen für jedes solche ϕ ein Funktionszeichen F_ϕ ein. L^* sei die so entstandene Erweiterung von L_N und

$$\mathrm{P}^* = \mathrm{P} \cup \big\{ \forall v_1, \ldots, v_n \phi(F_\phi(v_1, \ldots, v_n), v_1, \ldots, v_n) \bigm| \phi \text{ wie oben} \big\}$$

die entsprechende definitorische Erweiterung von P. Wir nennen F_ϕ eine Σ_1^{P}–Funktion .

Im Exkurs über definitorische Erweiterungen haben wir gesehen, daß P^* eine konservative Erweiterung von P ist und daß jede L^*–Formel in P^* zu einer L_N–Formel äquivalent ist (Satz 7.4). Insbesondere gilt in P^* das Induktionsschema für alle L^*–Formeln. Wenn man sich den Beweis von 7.4 vor Augen führt, sieht man, daß jede Σ_1–Formel aus L^* in eine Σ_1–Formel aus L_N übersetzt wird. Daraus folgt, daß P^{**} nichts neues liefert, was wir als $\mathrm{P}^{**} = \mathrm{P}^*$ notieren.

Jedes F_ϕ definiert eine Funktion $\mathbb{N}^n \rightarrow \mathbb{N}$, die in P^* durch die Formel $v_0 \doteq F_\phi(v_1, \ldots, v_n)$ repräsentiert wird, in P aber durch ϕ.

Satz 18.3 *Jede primitiv rekursive Funktion ist durch eine* Σ_1^{P}*–Funktion definierbar.*

Zum Beweis brauchen wir ein Lemma.

Lemma 18.4

i) Die Gödelsche β–Funktion ist durch eine Σ_1^{P}–Funktion, die wir wieder mit β bezeichnen, definierbar.

ii) Für diese Funktion gilt

$$\mathrm{P}^* \vdash \forall a, b, c, i \, \exists \, a', b' \, \big(\forall j < i \; \beta(a,b,j) \doteq \beta(a',b',j) \wedge c \doteq \beta(a',b',i)\big)$$

Beweis:

1. $\beta(a,b,i)$ wird von der Σ_1–Formel

   $$\phi(v_0,v_1,v_2,v_3) = \big(v_0 < v_2(v_3+1)+1 \wedge \exists y \; v_1 \doteq v_0 + y(v_2(v_3+1)+1)\big)$$

   definiert (vgl. Lemma 15.3).

2. Die in P^* zu beweisende Eigenschaft ist wahr. Denn wenn a, b, c, i gegeben sind, wendet man 15.3 auf die Folge

   $$c_0 = \beta(a,b,0), \, \dots, \, c_{i-1} = \beta(a,b,i-1), \, c_i = c$$

   an. Man erhält a', b' mit

   $$c_0 = \beta(a',b',0), \, \dots, \, c_{i-1} = \beta(a',b',i-1), \, c_i = \beta(a',b',i).$$

   Die Behauptung folgt jetzt aus dem Prinzip, daß sich alle einfachen arithmetischen Sachverhalte in P^* beweisen lassen.

$\square$

Beweis (von 18.3):

Die definierenden Formeln für S, I_i^n und C_0^0 definieren offenbar Σ_1^{P}–Funktionen (siehe 16.1). Ebenso wie in 16.1 sieht man, daß man durch Einsetzen von Σ_1^{P}–Funktionen in Σ_1^{P}–Funktionen wieder Σ_1^{P}–Funktionen erhält. Es bleibt zu zeigen, daß die Σ_1^{P}–Funktionen unter primitiver Rekursion (**R2**) abgeschlossen sind. Sei also f gegeben durch

$$f(x,0) = g(x), \quad f(x,y+1) = h(x,y,f(x,y))$$

und g und h definiert durch die Σ_1^{P}–Funktionen G und H. Dann wird f definiert durch die die Σ_1–Formel

$$\phi(v_0,v_1,v_2) = \exists a, b \; \Phi(v_0,v_1,v_2,a,b),$$

wobei

$$\begin{aligned}\Phi(v_0,v_1,v_2,a,b) \quad = \quad & \big(\beta(a,b,0) \doteq G(v_1) \\ & \wedge \forall x < v_2 \; \beta(a,b,x+1) \doteq H(v_1,x,\beta(a,b,x)) \\ & \wedge v_0 \doteq \beta(a,b,v_2)\big).\end{aligned}$$

Die Funktionalität von ϕ beweisen wir in P^* durch Induktion über v_2:

- $v_2 = 0$:
  Es ist klar, daß $\mathrm{P}^* \vdash \exists!\ v_0\phi(v_0, v_1, \underline{0})$: Nach 18.4 gibt es a, b mit $\beta(a, b, 0) = G(v_1)$. Wenn $\phi(v_0, v_1, \underline{0})$, muß v_0 gleich $G(v_1)$ sein.

- $v_2 \to v_2 + 1$:
  Um zu zeigen, daß es ein v_0 mit $\phi(v_0, v_1, v_2+1)$ gibt, wählen wir zunächst mit Hilfe der Induktionsvoraussetzung ein y für das $\phi(y, v_1, v_2)$ und a', b' mit $\Phi(y, v_1, v_2, a', b')$. Lemma 18.4 liefert a, b mit $\forall x \leq v_2\ \beta(a', b', x) = \beta(a, b, x)$ und $\beta(a, b, v_2 + 1) = H(v_1, v_2, y) = v_0$. Dann gilt $\Phi(v_0, v_1, v_2 + 1, a, b)$ und $\phi(v_0, v_1, v_2 + 1)$.

  Sei $\phi(v_0', v_1, v_2+1)$ für ein anderes v_0'. Es gibt dann a, b mit $\Phi(v_0', v_1, v_2 + 1, a, b)$. Sei $y' = \beta(a, b, v_2)$. Dann gilt $\Phi(y', v_1, v_2, a, b)$ und $y' = y$ nach Induktionsvoraussetzung. Es folgt $v_0' = H(v_1, v_2, y') = H(v_1, v_2, y) = v_0$.

□

Zusatz 18.5 *Wenn die Σ_1^{P}–Funktion $F(x, y)$ wie eben durch primitive Rekursion aus H und G definiert wird, ist in P^* beweisbar:*

(3) $$\forall x\ \big(F(x, \underline{0}) \doteq G(x) \wedge \forall y\ F(x, y + 1) \doteq H(x, y, F(x, y))\big).$$

□

Das Teilsystem von P^*, das aus P durch Hinzufügen der Aussagen (3) für alle primitiv rekursiven Funktionen entsteht, nennt man *primitiv rekursive Arithmetik*. Genauer geht man so vor: Für alle Terme G und H (und jede Stelligkeit), fügt man ein neues Funktionszeichen F und das Axiom (3) ein. Dieser Prozeß wird abzählbar oft iteriert.

Übung *Man zeige, daß nicht jede rekursive Funktion durch eine Σ_1^{P}–Funktion definiert werden kann.*

Hinweis: Sei $\phi_0, \phi_1, \ldots$ eine rekursive Aufzählung aller einstelligen Σ_1^{P}–Funktionen $\phi_i(v_0, v_1)$ und $f_1, f_2, \ldots$ die dadurch definierten Funktionen $\mathbb{N} \to \mathbb{N}$. Dann ist $f(x) = f_x(x) + 1$ ein Gegenbeispiel.

Definition *Eine Δ_1^{P}–Formel ϕ ist eine Σ_1–Formel, die in* P *zur Negation einer Σ_1–Formel ψ äquivalent ist:*

$$\mathrm{P} \vdash \phi \longleftrightarrow \psi$$

Folgerung 18.6 *Jede primitiv rekursive Relation ist durch eine Δ_1^{P}–Formel definierbar.*

Beweis:

Quantorenfreie Formeln aus L^* sind in P^* zu Δ_1^{P}–Formeln äquivalent. Sei R primitiv rekursiv. Nach 18.3 wird K_R von einer Σ_1^{P}–Funktion F definiert und R

daher von der quantorenfreien Formel $F(v_1) \doteq \underline{0}$. □
Man kann mit den eben angegebenen Methoden leicht zeigen, daß sich die primitiv rekursive Funktion

$$\beta'(a,i) = \beta((a)_0,(a)_1,i)$$

mit einer Σ_1^{P}–Funktion definieren läßt, sodaß, wie im Lemma 18.4,

Folgerung 18.7

$$\mathrm{P}^* \vdash \forall a,c,i\,\exists a'\,\big(\forall j < i\;\beta'(a,j) \doteq \beta'(a',j) \wedge c \doteq \beta'(a',i)\big)$$

19 Der Zweite Gödelsche Unvollständigkeitssatz

Wir beginnen mit einer allgemeinen Beobachtung. Wir sagen, daß eine Formel $\phi = \phi(\bar{x})$ logisch aus T folgt, wenn $\forall \bar{x}\, \phi$ in allen Modellen von T gilt (vergleiche die Definition auf Seite 22.)

Lemma 19.1 (Deduktionslemma) *Sei T eine L–Theorie. Eine L–Formel ϕ folgt genau dann logisch aus T, wenn ϕ im Hilbertkalkül aus den Axiomen von T herleitbar ist.*

Beweis:

Nehmen wir an, daß $\phi = \phi(\bar{x})$ logisch aus T folgt. Aus 4.5 folgt die Existenz von $\psi_1, \ldots, \psi_n$ aus T, für die $\psi_1 \wedge \cdots \wedge \psi_n \rightarrow \forall \bar{x}\, \phi$ einen Beweis im Hilbertkalkül hat. Es ist nun leicht zu sehen, daß im Hilbertkalkül ϕ aus $\psi_1 \wedge \cdots \wedge \psi_n \rightarrow \forall \bar{x}\, \phi$ und den Axiomen $\psi_1, \ldots, \psi_n$ herleitbar ist.

Die Umkehrung zeigt man durch Induktion über Länge der Herleitung von ϕ. Die Behauptung ist klar, wenn ϕ ein Kalkülaxiom oder ein Axiom von T ist. Schließlich prüft man leicht nach, daß die beiden Schlußregeln *Modus Ponens* und $\exists$–*Einführung* Formeln, die logisch aus T folgen, in Formeln überführen, die ebenfalls logisch aus T folgen. □

Wir wollen das Beweisbarkeitsprädikat für die Peanoarithmetik definieren. Zunächst beschreiben wir die primitiv rekursiven Relationen

- $Aus = \{\ulcorner\phi\urcorner \mid \phi\ L_N\text{–Aussage}\}$
- $Ax = \{\ulcorner\phi\urcorner \mid \phi\ L_N\text{–Formel, Axiom des Hilbertkalküls oder Axiom von P}\}$
- $Reg = \left\{ (\ulcorner\phi\urcorner, \ulcorner\psi\urcorner, \ulcorner\chi\urcorner) \;\middle|\; \begin{array}{l} \phi,\, \psi,\, \chi\ L_N\text{–Formeln, } \phi \text{ folgt aus } \psi \text{ und } \chi \text{ mit} \\ \text{einer der Regeln des Hilbertkalküls} \end{array} \right\}$

durch Σ_1–Formeln. Die Σ_1–Formel

$$B'(s,n) = \forall i < n \big(Ax(\beta'(s,i)) \vee \exists j,k < i\ Reg(\beta'(s,i), \beta'(s,i), \beta'(s,k)) \big),$$

definiert in dann $\mathfrak{N}$ die Menge aller Paare (s,n), für die $\beta'(s,0)$,... $\beta'(s,n-1)$ eine Herleitung aus den Axiomen von P ist (im Sinn der Definition S. 74). Das vorläufige Beweisbarkeitsprädikat wird dann definiert durch

$$\mathrm{Bew}'(f) = Aus(f) \wedge \exists\, n, s\ \big(\beta'(s,n) \doteq f \wedge B'(s, n+1)\big).$$

Aus dem Deduktionlemma 19.1 folgt, daß Bew in $\mathfrak{N}$ die Menge der Gödelnummern der in P beweisbaren Aussagen definiert.

Man kann leicht zeigen (wie im Beweis von Lemma 19.3), daß Bew' die auf Seite 57 eingeführten Loebaxiome **L1** und **L2** erfüllt. Für die Gültigkeit von **L3** müßte man aber die Formeln Ax und Reg sorgfältiger wählen. Es genügt nicht, zu wissen, daß Ax und Reg in $\mathfrak{N}$ die richtigen Relationen definieren. Um **L3** in einfacher Weise zu erfüllen, verwenden wir einen Kunstgriff. Wir fügen zu den Axiomen von P alle wahren Σ_1–Aussagen hinzu. Das ändert nichts an der Theorie, weil nach Satz 17.2 alle wahren Σ_1–Aussagen in P beweisbar sind.

Wir machen Gebrauch von folgendem Lemma, das wir später (S. 94) beweisen.

Lemma 19.2 *Es gibt eine Σ_1–Formel* $\mathrm{W}_1(x)$*, sodaß für alle Σ_1–Aussagen ϕ*

$$\mathrm{P} \;\vdash\; \phi \longleftrightarrow \mathrm{W}_1(\Delta_{\ulcorner\phi\urcorner}).$$

Für die Peanoarithmetik P läßt sich leicht das Analogon von Tarskis Satz 10.3 beweisen. Das Lemma gilt also nicht für beliebige Aussagen.

Weil die Menge der Gödelnummern von Σ_1–Aussagen primitiv rekursiv ist, können wir annehmen, daß

$$\mathrm{P} \vdash \neg\, \mathrm{W}_1(\Delta_n),$$

wenn n nicht die Gödelnummer einer Σ_1–Aussage ist.

Wir setzen jetzt

$$\begin{aligned} B(s,n) \quad = \quad & \forall i < n\big(\mathrm{W}_1(\beta'(s,i)) \vee (Ax(\beta'(s,i)) \vee \\ & \qquad\qquad \vee\, \exists j,k < i\ Reg(\beta'(s,i), \beta'(s,j), \beta'(s,k))\big) \end{aligned}$$

und

$$\mathrm{Bew}(f) = Aus(f) \wedge \exists\, n, s\ \big(\beta'(s,n) \doteq f \wedge B(s, n+1)\big).$$

Es ist klar, daß Bew in $\mathfrak{N}$ die Menge der Gödelnummern der in P beweisbaren Aussagen definiert.

Lemma 19.3 $\mathrm{Bew}(x)$ *erfüllt die Loeb–Axiome:*

L1 $\mathrm{P} \;\vdash\; \phi \implies \mathrm{P} \;\vdash\; \mathrm{Bew}(\Delta_{\ulcorner\phi\urcorner})$

L2 $\mathrm{P} \;\vdash\; \mathrm{Bew}(\Delta_{\ulcorner\phi\urcorner}) \wedge \mathrm{Bew}(\Delta_{\ulcorner\phi\to\psi\urcorner}) \;\to\; \mathrm{Bew}(\Delta_{\ulcorner\psi\urcorner})$

L3 $\mathrm{P} \;\vdash\; \mathrm{Bew}(\Delta_{\ulcorner\phi\urcorner}) \;\to\; \mathrm{Bew}\big(\Delta_{\ulcorner\mathrm{Bew}(\Delta_{\ulcorner\phi\urcorner})\urcorner}\big)$

Beweis:

L1: Wenn $\mathrm{P} \;\vdash\; \phi$, ist $\mathfrak{N} \models \mathrm{Bew}(\Delta_{\ulcorner\phi\urcorner})$. Weil $\mathrm{Bew}(\Delta_{\ulcorner\phi\urcorner})$ eine Σ_1–Formel ist, folgt $\mathrm{P} \;\vdash\; \mathrm{Bew}(\Delta_{\ulcorner\phi\urcorner})$. Die Umkehrung gilt natürlich auch. (17.2).

L2: Es ist klar, daß $\mathrm{P} \;\vdash\; Reg(\Delta_{\ulcorner\psi\urcorner}, \Delta_{\ulcorner\phi\urcorner}, \Delta_{\ulcorner\phi\to\psi\urcorner})$ und $\mathrm{P} \;\vdash\; Aus(\Delta_{\ulcorner\psi\urcorner})$. Jetzt argumentieren wir in P. Angenommen $\mathrm{Bew}(\ulcorner\phi\urcorner)$ und $\mathrm{Bew}(\ulcorner\phi \to \psi\urcorner)$, Dann gibt es s, m und t, n mit $\beta'(s,m) = \ulcorner\phi\urcorner$, $\beta'(t,n) = \ulcorner\phi \to \psi\urcorner$, $B(s, m+1)$ und $B(t, n+1)$. Wegen der Eigenschaften von β' (Folgerung 18.7), gibt es ein u, sodaß für alle $i \leq m+n+2$

$$\beta'(u,i) = \begin{cases} \beta'(s,i) & \text{, wenn} \quad i \leq m \\ \beta'(t, i-m-1) & \text{, wenn} \quad m < i \leq m+n+1 \\ \ulcorner\psi\urcorner & \text{, wenn} \quad i = m+n+2 \end{cases}$$

Es ist klar, daß $B(u, m+n+3)$. Damit ist gezeigt, daß $\mathrm{Bew}(\ulcorner\psi\urcorner)$.

L3: Für alle Σ_1–Aussagen ψ gilt $\mathrm{P} \vdash \psi \to \mathrm{Bew}(\Delta_{\ulcorner\psi\urcorner})$. Beweis: Weil $Aus(f)$ eine Σ_1–Formel ist, ist $Aus(\Delta_{\ulcorner\psi\urcorner})$ in P beweisbar. Wir argumentieren jetzt in P: Aus ψ folgt wegen 19.2, daß $\mathrm{W}_1(\ulcorner\psi\urcorner)$. Wir wählen ein s, sodaß $\beta'(s,0) = \ulcorner\psi\urcorner$. Dann gilt $B(s,1)$. Zusammen mit $Aus(\ulcorner\psi\urcorner)$ folgt $\mathrm{Bew}(\ulcorner\psi\urcorner)$.

□

Wenn F eine Formel ist, deren Negation allgemeingültig ist, drückt die Aussage

$$\mathrm{CON_P} = \neg\,\mathrm{Bew}(\Delta_{\ulcorner\mathrm{F}\urcorner})$$

die Konsistenz von P aus. Aus 19.3 und dem Fixpunktsatz 17.8 ergibt sich, wie früher

Satz 19.4 (Zweiter Gödelscher Unvollständigkeitssatz für P**)**
$\mathrm{CON_P}$ *ist wahr, aber in* P *unbeweisbar.* □

Statt den Beweis von 10.5 zu wiederholen, zeigen wir eine Verallgemeinerung, den Satz von Loeb.

Satz 19.5 (Satz von Loeb) *Für jede L_N–Aussage ψ ist*

$$\mathrm{P} \vdash \mathrm{Bew}(\Delta_{\ulcorner\mathrm{Bew}(\Delta_{\ulcorner\psi\urcorner})\to\psi\urcorner}) \to \mathrm{Bew}(\Delta_{\ulcorner\psi\urcorner}).$$

Für $\psi = \mathrm{F}$ ergibt sich

$$\mathrm{P} \vdash \mathrm{Bew}(\Delta_{\ulcorner\mathrm{CON_P}\urcorner}) \to \neg\,\mathrm{CON_P}.$$

Also

$$\mathfrak{N} \models \mathrm{Bew}(\Delta_{\ulcorner\mathrm{CON_P}\urcorner}) \Longrightarrow \mathfrak{N} \models \neg\,\mathrm{CON_P}.$$

Das ist der zweite Gödelscher Unvollständigkeitssatz für P. Umgekehrt läßt sich der Satz von Loeb auffassen als der zweite Gödelsche Unvollständigkeitssatz für $\mathrm{P} \cup \{\neg\,\psi\}$.

Beweis:

Der Übersichtlichkeit zuliebe schreiben wir $\Box\,\phi$ für $\mathrm{Bew}(\Delta_{\ulcorner\phi\urcorner})$.[5] Zunächst bemerken wir, daß, wie in 10.4, aus **L1** und **L2** folgt

(1) $\quad \mathrm{P} \vdash \phi \to \psi \implies \mathrm{P} \vdash \Box\,\phi \to \Box\,\psi$

(2) $\quad \mathrm{P} \vdash \Box\,(\phi \wedge \psi) \longleftrightarrow (\Box\,\phi \wedge \Box\,\psi])$

[5] Diese Notation ist dem Artikel [5] entnommen. Solovay betrachtet *modallogische* Formeln $f = f(p_1, \ldots, p_n)$. Das sind Formeln, die sich aus den Aussagenvariablen p_i mit $\neg$, $\wedge$ und $\Box$ aufbauen. Wir schreiben $\vdash f$, wenn $\mathrm{P} \vdash f(\phi_1, \ldots, \phi_n)$ für alle L_N–Aussagen ϕ_i. Das Hauptresultat von [5] besagt, daß $\vdash f$ genau dann, wenn f sich mit den Regeln

- $\vdash f\ , \vdash f \to g \implies \vdash g$
- $\vdash f \implies \vdash \Box\, f$

aus Tautologien und den Axiomen

- $\vdash \Box\, f \wedge \Box\,(f \to g) \to \Box\, g$
- $\vdash \Box\, f \to \Box\,\Box\, f$
- $\vdash \Box\,(\Box\, f \to f) \to \Box\, f$

herleiten läßt. Das letzte Axiomenschema ist der Loebsche Satz.

Aus 17.8 folgt die Existenz eines ϕ mit

(3) $$\mathrm{P} \vdash \phi \longleftrightarrow (\Box\,\phi \to \psi)$$

Daraus folgt mit (1)

(4) $$\mathrm{P} \vdash \Box\,\phi \to \Box\,(\Box\,\phi \to \psi).$$

L3 ist

(5) $$\mathrm{P} \vdash \Box\,\phi \to \Box\,\Box\,\phi.$$

Aus (2) und (1) folgt

(6) $$\mathrm{P} \vdash (\Box\,(\Box\,\phi \to \psi) \wedge \Box\,\Box\,\phi) \to \Box\,\psi$$

Aus (4),(5) und (6) folgt

(7) $$\mathrm{P} \vdash \Box\,\phi \to \Box\,\psi$$

und daraus mit (3)

$$\mathrm{P} \vdash (\Box\,\psi \to \psi) \to \phi.$$

Mit (1) folgt daraus

$$\mathrm{P} \vdash \Box\,(\Box\,\psi \to \psi) \to \Box\,\phi$$

und nochmal mit (7) die Behauptung

$$\mathrm{P} \vdash \Box\,(\Box\,\psi \to \psi) \to \Box\,\psi.$$

□

Beweis von Lemma 19.2:

Es genügt, die Behauptung für Σ_1–Formeln im engeren Sinn zu beweisen[6]. Alle Σ_1–Formeln im Beweis seien Σ_1–Formeln im engeren Sinn. Wir notieren endliche Folgen von Zahlen als $\sigma, \tau, \ldots$ und schreiben in Anlehnung an die Notation von Lemma 12.6 $(\sigma)_i$ für das Element mit Index i.

Eine Σ_1–Formel $\phi(v_0, \ldots, v_{s-1})$ trifft genau dann eine Folge σ der Länge s zu, wenn, wenn es eine Folge $\phi_0, \ldots, \phi_N$ von Σ_1–Formeln gibt und eine Folge $\sigma_0, \ldots, \sigma_N$ von endlichen Folgen, sodaß $\phi_N = \phi$, $\sigma_N = \sigma$ und für alle $n \leq N$

- Wenn s_n die Länge von σ_n ist, kommen höchsten die Variablen $v_0, \ldots, v_{s_n-1}$ frei in ϕ_n vor.
- Wenn $\phi_n = \underline{0} \doteq v_i$, ist $0 = (\sigma_n)_i$.
- Wenn $\phi_n = \mathrm{S}(v_i) \doteq v_j$, ist $(\sigma_n)_i + 1 = (\sigma_n)_j$.
- Wenn $\phi_n = v_i + v_j \doteq v_k$, ist $(\sigma_n)_i + (\sigma_n)_j = (\sigma_n)_k$.
- Wenn $\phi_n = v_i \cdot v_j \doteq v_k$, ist $(\sigma_n)_i \cdot (\sigma_n)_j = (\sigma_n)_k$.
- Wenn $\phi_n = v_i \doteq v_j$, ist $(\sigma_n)_i = (\sigma_n)_j$.

[6] Sei W_1' eine Wahrheitsdefinition für Σ_1–Formeln im engeren Sinn. Die Funktion, die der Gödelnummer einer Σ_1–Formel die Gödelnummer einer beweisbar äquivalenten Σ_1–Formel im engeren Sinn zuordnet, sei durch eine Σ_1^{P}–Funktion ES definiert, (siehe Bemerkung auf S.81.) Dann funktioniert $\mathrm{W}_1(x) = \mathrm{W}_1'(ES(x))$ für alle Σ_1^{P}–Funktionen.

- Wenn $\phi_n = \neg\, v_i \doteq v_j$, ist $(\sigma_n)_i \neq (\sigma_n)_j$.
- Wenn $\phi_n = v_i < v_j$, ist $(\sigma_n)_i < (\sigma_n)_j$.
- Wenn $\phi_n = \neg\, v_i < v_j$, ist $(\sigma_n)_i \not< (\sigma_n)_j$.
- Wenn $\phi_n = \phi' \wedge \phi''$, gibt es $n', n'' < n$, mit $\phi_{n'} = \phi'$, $\phi_{n''} = \phi''$ und $\sigma_{n'} = \sigma_{n''} = \sigma_n$.
- Wenn $\phi_n = \phi' \vee \phi''$, gibt es $n' < n$, mit $\phi_{n'} = \phi'$ und $\sigma_{n'} = \sigma_n$ oder ein $n'' < n$ mit $\phi_{n''} = \phi''$ und $\sigma_{n''} = \sigma_n$.
- Wenn $\phi_n = \exists v_i\, \phi'$, gibt es ein $n' < n$ mit $\phi_{n'} = \phi'$ und $(\sigma_{n'})_k = (\sigma_n)_k$ für alle k mit $k < \min(s_n, s_{n'})$ und $k \neq i$.
- Wenn $\phi_n = \forall v_i < v_j\, \phi'$, gibt es für alle $a < (\sigma_n)_j$ ein $n' < n$ mit $\phi_{n'} = \phi'$ und $(\sigma_{n'})_i = a$ und $(\sigma_{n'})_k = (\sigma_n)_k$ für alle k mit $k < \min(s_n, s_{n'})$ und $k \neq i$.

Man verwendet jetzt, daß die verwendeten syntaktischen Dekonstruktionen primitiv rekursiv sind. Das heißt zum Beispiel, daß die Menge

$$\{\ulcorner \forall v_i < v_j\, \phi' \urcorner \mid i, j \in \mathbb{N},\ \phi'\ \Sigma_1\text{–Formel}\}$$

und die Funktionen

$$\begin{aligned} f(\ulcorner \forall v_i < v_j\, \phi' \urcorner) &= i \\ g(\ulcorner \forall v_i < v_j\, \phi' \urcorner) &= j \\ h(\ulcorner \forall v_i < v_j\, \phi' \urcorner) &= \ulcorner \phi' \urcorner \end{aligned}$$

primitiv rekursiv sind. Wegen Satz 18.3 ist das also alles Σ_1–definierbar. Wenn wir endliche Folgen mit Hilfe der β'–Funktion beschreiben (siehe Folgerung 18.7), erhalten wir eine Σ_1–Formel $\mathrm{W}'_1(f, a)$, sodaß für alle Σ_1–Formeln $\phi = \phi(v_0, \ldots, v_{s-1})$

$$\mathrm{P}^* \vdash \forall a\ \big(\phi(\beta'(a, \Delta_0), \ldots, \beta'(a, \Delta_{s-1})) \longleftrightarrow \mathrm{W}'_1(\Delta_{\ulcorner \phi \urcorner}, a)\big).$$

Man zeigt das durch Induktion über den Aufbau von ϕ.

Schließlich setzen wir $\mathrm{W}_1(x) = \mathrm{W}'_1(x, \underline{0})$. □

Literaturverzeichnis

[1] H.-D.Ebbinghaus, J.Flum, and W.Thomas. *Einführung in die mathematische Logik*. Spektrum Akademischer Verlag, 1996. 4. Auflage.

[2] Bruno Poizat. *Cours de Théorie des Modèles*. Nur Al-Mantiq Wal-Ma'rifah, Villeurbanne, 1985.

[3] Alexander Prestel. *Einführung in die Mathematische Logik und Modelltheorie*. vieweg studium, Aufbaukurs Mathematik. Friedr. Vieweg & Sohn, Braunschweig, Wiesbaden, 1986.

[4] Joseph R. Shoenfield. *Mathematical Logic*. Addison–Wesley Series in Logic. Addison–Wesley Publishing Company, 1973.

[5] Robert M. Solovay. Provability interpretations of modal logic. *Israel J. Math.*, 25:287–304, 1976.

Index

Änderungen

Version 6.6 (12.11.2006)

Druckfehler auf Seite 33.

Version 6.7 (6.12.2006)

Korrektur des Beweises des Hilfssatzes im Beweis von 1.1.

Version 7.0 (14.1.2007)

Kleine Korrekturen. Neues über Gleichheitszeichen: Lemma 4.8, Bemerkung auf Seite 31, Folgerung 6.8.

Version 7.1 (23.1.2007)

Schreibfehler in 6.1. Bemerkung auf Seite 31 korrigiert.

Version 7.2 (31.1.2007)

Besserer Index in Abschnitt 6. Beweis und Beispiel für Satz 6.7 verbessert.

Version 7.3 (25.4.2007)

Erwähnung von *Prädikat* auf S.4. Falsche Indices auf den Seiten 11 und 21.

Version 7.4 (8.5.2007)

Die Definition definitorischer Erweiterungen auf S.44 wurde auf Konstanten ausgedehnt. Danach wird bemerkt, daß konservative und definitorische Erweiterungen das gleiche sind[1]. Folgerung 7.5 wurde entsprechend erweitert. Der Beweis von Lemma 4.2.1 wurde geändert.

Version 7.5 (9.5.2007)

Der Beweis von 4.2.1 wurde noch einmal geändert.

Version 7.6 (4.6.2007)

Atomare Formeln heißen jetzt überall Primformeln. Druckfehler in Formulierung und Beweis von 5.2. Bemerkung nach 6.2. Die Bemerkung auf S.44 wurde korrigiert.

Version 7.7 (4.7.2007)

Kommafehler und Druckfehler. Formulierung von 8.7 präzisiert. Druckfehler im Beweis von 9.5. Verbesserung im Beweis von 9.7. Umformulierungen im Beweis von 10.6. Druckfehler in den Diagrammen von Abschnitt 11. Fehler in der Definition der Kopiermaschine auf Seite 63.

Version 7.8 (10.7.2007)

Fehler im Beweis von 13.1. Umformulierung des Beweises von 14.5. Druckfehler in Abschnitt 9. Offizielle Definition von vollständiger Theorie auf Seite 75.

Version 7.9 (16.4.2008)

Druckfehler im Beweis von 13.5.

Version 17.10 (22.7.2008)

Wahre Theorie definiert in Kapitel 17. Druckfehler im Paragraphen nach 6.6.

[1] in Version 7.6 korrigiert