Mathematische Logik

Skript zur
im Sommersemester 2007
in Wien gehaltenen
vierstündigen Vorlesung

Heike Mildenberger

Inhaltsverzeichnis

KAPITEL 1

Kurzeinführung

Literaturempfehlungen: Die folgenden Bücher stehen immer in unserer Bücherei und können nicht ausgeliehen werden. Sie sind eingeladen, Lesebesuche abzustatten.
Herbert Enderton. *A Mathematical Introduction to Logic.* Accademic Press, 3 edition, 2001.[**2**]
W. Thomas, H.-D. Ebbinghaus, J. Flum. *Einführung in die Mathematische Logik.* Hochschultaschenbuch, 4 edition, 1996. [**1**]
Daniel Lascar, René Cori. *Logique mathématique. Cours et exercices*, volume I and II. Masson, 1993.[**5**]
Daniel Lascar, René Cori.[**6**] *Mathematical Logic. A course with exercises*, volume I and II. Oxford University Press, 2000. (Dies ist die Übersetzung des vorigen Werkes ins Englische)

Wir beginnen auf der spielerischen Seite der Kunst mit einem Gedicht von Hans Magnus Enzensberger:

Hommage à Gödel

Münchhausens Theorem, Pferd, Sumpf und Schopf,
ist bezaubernd, aber vergiß nicht:
Münchhausen war ein Lügner.

Gödels Theorem wirkt auf den ersten Blick
etwas unscheinbar, doch bedenk:
Gödel hat Recht.

„In jedem genügend reichhaltigen System,
lassen sich Sätze formulieren,
die innerhalb des Systems
weder beweisbar noch widerlegbar sind,
es sei denn, das System
wäre selber inkonsistent."

Du kannst deine eigene Sprache
in deiner eigenen Sprache beschreiben:
aber nicht ganz.
Du kannst dein eigenes Gehirn
mit deinem eigenen Gehirn erforschen,

aber nicht ganz.
Usw.

Um sich zu rechtfertigen
muß jedes denkbare System
sich transzendieren,
d.h. zerstören.

„Genügend reichhaltig" oder nicht:
Widerspruchsfreiheit
ist eine Mangelerscheinung
oder ein Widerspruch.

(Gewißheit = Inkonsistenz.)

Jeder denkbare Reiter,
also auch Münchhausen,
also auch du bist ein Subsystem
eines genügend reichhaltigen Sumpfes.

Und ein Subsystem dieses Subsystems
ist der eigene Schopf, dieses Hebezeug,
für Reformisten und Lügner.

In jedem genügend reichhaltigen System,
also auch in diesen Sumpf hier
lassen sich Sätze formulieren
die innerhalb des Systems
weder beweis- noch widerlegbar sind.

Diese Sätze nimm in die Hand
und zieh.

1. Kurt Gödel

1906 in Brünn geboren
ab 1924 Studium an der Universität Wien
1930 Promotion: Vollständigkeitssatz
1931 Habilitation: Unvollständigkeitssatz
1937 Mengenlehre: das Universum der konstruktiblen Mengen, die relative Konsistenz des Auswahlaxioms und der Kontinuumshypothese
1940 Flucht nach Princeton
1978 in Princeton gestorben

Gödel war der „Vater der modernen Logik"

Drei philosophische Fragen stehen am Anfang. Gödel beantwortete diese mit mathematischen Methoden und gründete damit ein Gebiet, das eher zur Mathematik gehört als zur Philosophie: die mathematische Logik.

1. Was ist eine logische Implikation?

2. Hat jedes mathematische Problem eine definitive Antwort?
3. Ist die Mathematik widerspruchsfrei?

In unserer eine Sitzung dauernden Kurzeinführung umreißen wir jetzt sehr kursorisch und auch nicht mit mathematischer Strenge die Antworten. Die Gödelsche Arbeit von 1937 kann in dieser Vorlesung nicht behandelt werden. Sie wird am Wiener Kurt Gödel Research Center for Mathematical Logic üblicherweise in der Axiomatischen Mengenlehre oder in der Vorlesung Mathematische Logik II vorgestellt.

2. Die Aussagenlogik

Die Formeln der Aussagenlogik werden aufgebaut aus:

Symbolen für Aussagen: $A, B, C \dots$ oder $A_0, A_1, \dots$

Junktoren: $\wedge$ und, $\vee$ oder, $\sim$ nicht.

Alle Satzsymbole sind Aussagen. Sind φ und ψ Aussagen, so auch $\sim \varphi$ und $\varphi \wedge \psi$ und $\varphi \vee \psi$.

Äquivalent formuliert: Die Menge der aussagenlogischen Formeln über der Menge $\mathcal{S}$ der Satzvariablen ist der Abschluss von $\mathcal{S}$ unter $\wedge$, $\vee$ und $\sim$.

Einige Beispiele von Formeln:

$A \wedge \sim A$,

$A \vee \sim A$.

$(A \vee B) \wedge (A \vee \sim B) \wedge (\sim A \vee B) \wedge (\sim A \vee \sim B)$

Definition 1.1. *φ ist eine Tautologie, gwd φ immer wahr ist, das heißt, daß für alle Wahrheitsbelegungen $v \colon S \to \{w, f\}$, $\bar{v}(\varphi) = w$.*

3. Die Prädikatenlogik oder die Logik erster Stufe

Andere Namen: first-order logic, die Sprache der ersten Stufe....

Wir beginnen mit zwei Beispielen:

(i) Der Satz von Lagrange: Jede natürliche Zahl ist die Summe vierer Quadratzahlen.

Für jedes n gibt es a, b, c, d, so daß $n = a^2 + b^2 + c^2 + d^2$.

In Symbolen: $\forall n \exists a, b, c, d(n = a^2 + b^2 + c^2 + d^2)$.

Wir verwendeten hier also Quantoren:

für jedes n: $\forall n$

es gibt a: $\exists a$

In der Logik der ersten Stufe gibt es diese beiden Quantoren.

(ii) Unendlich viele Primzahlen

Zu jeder natürlichen Zahl gibt es eine grössere Primzahl.-

$\forall n \exists p(n < p \wedge p$ ist prim$)$

$\forall n \exists p(p > n \wedge \forall q, r < p(p \neq r \cdot q))$

In der Sprache erster Stufe gibt es

Variablen, zum Beispiel n, a, b, c, d

Quantoren: für alle $\forall$, es gibt $\exists$
Junktoren: und $\wedge$, oder $\vee$, nicht $\sim$, wenn, dann $\rightarrow$
Konstantensymbole, zum Beispiel 1,2
Funktionssymbole, zum Beispiel $+$, $\cdot$, Exponentiation
Prädikatssymbole, zum Beispiel $=$, $<$.

(Man schränkt die letzteren drei Mengen nicht ein, sie können bei Bedarf auch unendlich sein. Auch die Menge der Variablen kann sehr groß sein. Dagegen haben wir die Quantoren und auch die Junktoren schon ziemlich vollständig benannt.)

Wir betrachten nun {Tautologien der Prädikatenslogik}. Ist die Menge entscheidbar?

Gödelscher Vollständigkeitssatz: Die Menge der Tautologien der Prädikatenlogik ist effektiv aufzählbar.

Gödelscher Unvollständigkeitssatz: Die Menge der Tautologien der Prädikatenlogik ist nicht entscheidbar.

4. Die Grundlagen der Mathematik

Das Hilbertsche Programm (1900):

(1) Übersetze die Mathematik in ein logischen System von Axiomen und Schlußregeln.

(2) Zeige, daß dieses System konsistent und vollständig ist: Für jedes ψ ist entweder ψ oder $\sim\psi$ beweisbar.

(1) Diese Aufgabe kann ausgeführt werden: Das System ZFC (Zermelo Fraenkel mit Auswahlaxiom) für die Mengenlehre dient als axiomatische Grundlage. Es wird in der Sprache der ersten Stufe formuliert. Die Schlußregeln sind die „klassischen”, die wir in etwa drei Wochen kennenlernen werden, und die Sie eh schon in Ihrem mathematischen Schließen täglich verwenden.

Die Sprache der ersten Stufe für die Mengenlehre hat
Symbole: x, y, z für Mengen (beliebig viele Symbole)
ein Prädikat: $\in$
Typische Axiome:
Es gibt eine Menge x ohne Elemente

Für jede Menge x gibt eine Menge y deren Elemente genau die Teilmenge von x sind, die Potenzmenge von x, $P(x)$.

Gödel bewies: (2) des Hilbertschen Programms ist prinzipiell nicht durchführbar.

Ein minimales Kodierungsystem, nach Raffael Robinson auch „das System Q” genannt, gestattet die Kodierung aller Beweise (in jeder effektiven Sprache). Die endliche Liste der Sätze zur Beschreibung eines solchen Kodierungssystems wird zum Beispiel im Teiluniversum der endlichen Mengen erfüllt. ZFC enthält solch ein Kodierungssystem für $\mathscr{L}(\in)$. Das System A_E der Zahlentheorie, das wir später angeben werden, umfasst das System Q.

Gödelscher Vollständigkeitssatz: Sei $\mathcal{S}$ ein aufzählbares logisches System. Dann ist die Menge der aus $\mathcal{S}$ beweisbaren Sätze effektiv aufzählbar.

Gödelsche verallgemeinerte Unentscheidbarkeit: Sei $\mathcal{S}$ ein konsistentes logisches System, das ein minimales Kodierungssystem enthält. Dann ist die Menge der aus $\mathcal{S}$ beweisbaren Sätze nicht entscheidbar.

Überraschende Schlußfolgerung:

Gödelsche Unvollständigkeit: Sei $\mathcal{S}$ ein konsistentes logisches System, das ein minimales Kodierungssystem enthält. Dann ist die Menge der aus $\mathcal{S}$ beweisbaren Sätze unvollständig.

Beweis der Unvollständigkeit aus der verallgemeinerten Unentscheidbarkeit: Annahme: $\mathcal{S}$ enthalte ein minimales Kodierungssystem und sei konsistent und vollständig und effektiv aufzählbar. Dann ist $\{\mathcal{S}$-beweisbare Sätze$\}$ effektiv aufzählbar und $\{\mathcal{S}$-widerlegbare Sätze$\}$ effektiv aufzählbar. Und jedes φ ist entweder beweisbar oder widerlegbar. Es folgt, daß $\{\mathcal{S}$-beweisbare Sätze$\}$ entscheidbar ist. Dies widerspricht der verallgemeinerten Gödelschen Unvollständigkeit.

KAPITEL 2

Die Aussagenlogik

Wir beginnen jetzt die formale Entwicklung der Aussagenlogik (propositional logic). Die Symbole dieser Logik sind wie folgt:

Klammern: (und)

Junktoren: $\sim$ (nicht), $\wedge$ (und), $\vee$ oder, $\rightarrow$ (wenn ... dann), $\leftrightarrow$ (genau dann, wenn).

Satzsymbole: A_0, A_1,...

Ein Ausdruck ist eine endliche Folge von Symbolen. Zum Beispiel ist $\rightarrow ((A_4$ ein Ausdruck. Aber nur gewisse Ausdrücke haben eine Bedeutung, und diese werden Formel genannt. Wir definieren die Menge der Formeln wie folgt:

Definition 2.1. *(a) Jedes Satzsymbol ist eine Formel.*

(b) Wenn α und β Formeln sind, dann sind auch $(\sim \alpha)$ und $(\alpha \wedge \beta)$ und $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ und $(\alpha \leftrightarrow \beta)$ Formeln.

(c) Kein Ausdruck ist dann eine Formel, wenn er es nicht aufgrund von (a) oder (b) sein muß.

Eine andere Art, (c) auszudrücken, ist zu sagen, daß die Menge der Formeln dadurch erzeugt wird, daß die „Menge der Satzsymbole unter den Junktoren abgeschlossen wird". Da der (im Sinne von $\subseteq$) kleinste Abschluß genommen wird, gibt es ein *Induktionsprinzip* für Formeln:

Es besagt folgendes: Wenn eine Eigenschaft für die Satzsymbole wahr ist und bei Anwendung der Junktoren erhalten bleibt, so ist sie für jede Formel wahr. Zum Beispiel:

Lemma 2.2. *Jede Formel hat gleich viele Linksklammern wie Rechtsklammern.*

Beweis: Die Behauptung ist wahr für Satzsymbole, da diese keine Klammern enthalten. Wenn α und β Formeln mit der behaupteten Eigenschaft sind, dann haben auch $(\sim \alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ und $(\alpha \leftrightarrow \beta)$ die behauptetete Eigenschaft. Wegen des Induktionsprinzips hat jede Formel die gewünschte Eigenschaft. $\square$

0.1. Wahrheitsbelegungen. Wir möchten nun definieren, was es bedeutet, daß eine Formel aus anderen Formeln logisch folgt. Es bedeuten W wahr und F falsch. Sie werden die Wahrheitswerte genannt.

DEFINITION 2.3. *Eine* Wahrheitsbelegung v *für eine Menge* $\mathcal{S}$ *von Satzsymbolen ist eine Funktion*

$$v\colon \mathcal{S} \to \{W, F\}.$$

Sei $\bar{\mathcal{S}}$ die Menge der Formeln, die unter Verwendung von Satzsymbolen aus $\mathcal{S}$ entstehen, d.h. Formeln, die entstehen, wenn $\mathcal{S}$ unter den fünf Junktoren abgeschlossen wird.

DEFINITION 2.4. *Nun definieren wir eine Erweiterung* $\bar{v}$ *von* v *auf* $\bar{\mathcal{S}}$ *wie folgt:*

(1) $\bar{v}(A) = v(A)$ *für* $A \in \mathcal{S}$,

(2) $\bar{v}(\sim \alpha) = W$ *gdw* $\bar{v}(\alpha) = F$,

(3) $\bar{v}(\alpha \wedge \beta) = W$ *gdw* $\bar{v}(\alpha) = W$ *und* $\bar{v}(\beta) = W$,

(4) $\bar{v}(\alpha \vee \beta) = W$ *gdw* $\bar{v}(\alpha) = W$ *oder* $\bar{v}(\beta) = W$,

(5) $\bar{v}(\alpha \to \beta) = W$ *gdw* $\bar{v}(\alpha) = F$ *oder* $\bar{v}(\beta) = W$,

(6) $\bar{v}(\alpha \leftrightarrow \beta) = W$ *gdw* ($\bar{v}(\alpha) = W$ *gdw* $\bar{v}(\beta) = W$, *(hierbei binden "oder" und "und" stärker als "gdw", oder man setzt in den Punkten (3), (4), (5) auch Klammern).*

(Konvention: $\wedge$ *und* $\vee$ *binden stärker als* $\leftrightarrow$*.)*

Nach dem Induktionsprinzip ist somit $\bar{v}$ auf ganz $\mathcal{S}$ wohldefiniert.

Zum Beispiel betrachten wir folgende Formel α:

$$((A_2 \to (A_1 \to A_6)) \leftrightarrow ((A_2 \wedge A_1) \to A_6))$$

mit der Wahrheitsbelegung v für A_1, A_2, A_6: $v(A_1) = W$, $v(A_2) = W$, $v(A_6) = F$. Wir rechnen $\bar{v}(A_1 \to A_6) = F$, $\bar{v}(A_1 \wedge A_2) = W$, $\bar{v}(((A_2 \to A_1) \to A_6)) = F$, und wir erhalten schließlich $\bar{v}(\alpha) = W$.

Wir sagen, daß eine Wahrheitsbelegung v eine Formel φ genau dann erfüllt, wenn $\bar{v}(\varphi) = W$ ist. Dazu muß natürlich der Definitionsbereich von v jedes Satzsymbol in φ enthalten. Nun betrachten wir sowohl eine Formelmenge Σ (ihre Elemente sind die Hypothesen) als auch eine weitere Formel τ (die die Schlußfolgerung sein soll).

DEFINITION 2.5. *(1)* Σ *impliziert tautologisch* τ, *in Zeichen* $\Sigma \models \tau$, *gdw folgendes der Fall ist: Für jede Wahrheitsbelegung* v *aller Symbole, die in* Σ *oder in* τ *auftreten, gilt: Wenn* $\bar{v}$ *jedes Element von* Σ *erfüllt, dann erfüllt* $\bar{v}$ *auch* τ.

(2) *Falls* Σ *die leere Menge ist, dann bedeutet das, daß jede Wahrheitsbelegung der Satzsymbole in* τ τ *erfüllt. In diesen Falle sagen wir, daß* τ *eine (aussagenlogische) Tautologie ist und schreiben* $\models \tau$.

(3) *Wenn* Σ *nur ein Element enthält, dann schreiben wir* $\sigma \models \tau$ *statt* $\{\sigma\} \models \tau$.

(4) *Wenn sowohl $\sigma \models \tau$ als auch $\tau \models \sigma$, dann sagen wir, daß σ und τ tautologisch äquivalent sind.*

Einschub: Sie wundern sich vielleicht über die Vagheit der Festlegung, welche Junktoren zum Aufbau der aussagenlogischen Formeln zulässig sind. Die folgenden Übungsaufgaben zeigen, daß es Spielraum gibt:

DEFINITION 2.6. *Eine Junktorenmenge $\mathcal{J}$ heißt vollständig, gdw es zu jeder aussagenlogischen Formel σ eine tautologisch äquivalente aussagenlogische Formel τ gibt, die nur Junktoren aus $\mathcal{J}$ enthält.*

Ü1. Für den Junktor | („Scheffer stroke", „weder noch") gilt: $\bar{\nu}((\varphi|\psi)) = W$ gdw $\bar{\nu}(\varphi) = F$ und $\bar{\nu}(\psi) = F$ für alle Erweiterungen $\bar{\nu}$ von Wahrheitsbelegungen ν. Zeigen Sie, daß $\{|\}$ eine vollständige Junktorenmenge ist.

Ü2. Zeigen Sie, daß $\{\sim, \rightarrow\}$ eine vollständige Junktorenmenge ist. Analoges gilt für $\vee$ anstelle von $\rightarrow$ und für $\wedge$ anstelle von $\rightarrow$. Wie ist die Lage für $\leftrightarrow$ anstelle von $\rightarrow$?

Ü3.* Für den Junktor + („entweder oder") gilt: $\bar{\nu}((\varphi + \psi)) = W$ gdw $\bar{\nu}(\varphi) = W$ oder $\bar{\nu}(\psi) = W$, aber nicht beide wahr, für alle Erweiterungen $\bar{\nu}$ von Wahrheitsbelegungen ν. Zeigen Sie, daß $\{\wedge, \leftrightarrow, +\}$ eine vollständige Junktorenmenge ist und — ist der *-Teil der Aufgabe — daß jedoch keine ihrer echten Teilmengen vollständig ist.

Eine wichtige Tatsache ist der Kompaktheitssatz der Aussagenlogik.

DEFINITION 2.7. *Eine Menge Σ von Formeln ist erfüllbar gdw es eine Wahrheitsbelegung gibt, die jedes Element von Σ erfüllt.*

SATZ 2.8. *Kompaktheitssatz. Sei Σ eine unendliche Menge von Formeln, so daß jede endliche Teilmenge von Σ erfüllbar ist. Dann ist auch Σ erfüllbar.*

KOROLLAR 2.9. *Wenn $\Sigma \models \tau$, dann gibt es ein endliches $\Sigma_0 \subseteq \Sigma$, so daß $\Sigma_0 \models \tau$.*

Beweis: Nennen wir Σ endlich erfüllbar gdw jede endliche Teilmenge von Σ erfüllbar ist. Unter Verwendung dieser Definition können wir den Kompaktheitssatz wie folgt formulieren: Wenn Σ endlich erfüllbar ist, dann ist Σ erfüllbar. Der Beweis besteht aus zwei Teilen. Im ersten Teil erweitern wir unsere gegebene endlich erfülbare Menge Σ zu einer maximalen Menge Δ dieser Art. Im zweiten Schritt verwenden wir Δ, um eine Wahrheitsbelegung zu wählen, die Σ erfüllt.

Eine Menge heißt abzählbar, gdw wenn sie endlich ist oder mit den natürlichen Zahlen indiziert aufgelistet werden kann: x_0, x_1, $x_2 \ldots$ Nun ist die Menge der Symbole der Aussagenlogik anzählbar. Es folgt, daß auch die Menge aller endlichen Folgen über $\{A_0, A_1, \ldots\} \cup \{(,), \wedge, \vee, \sim, \rightarrow, \leftrightarrow\}$ abzählbar ist. Da die

Menge der Formeln eine Teilmenge ist, ist auch die Menge der Formeln abzählbar. Deshalb können wir eine Liste $\alpha_0, \alpha_1, \ldots$ der Menge der Formeln wählen, die mit den natürlichen Zahlen indiziert ist.

Wir definieren nun $\Delta_0 = \Sigma$. Für jede natürliche Zahl n definieren wir nun $\Delta_{n+1} = \Delta_n \cup \{\alpha_{n+1}\}$, wenn dies endlich erfüllbar ist, sonst definieren wir $\Delta_{n+1} = \Delta_n \cup \{\sim \alpha_{n+1}\}$. Sei Δ die Vereinigung der Δ_n.

Wir beweisen nun durch Induktion über n: Jedes Δ_n ist endlich erfüllbar. Die Induktionsaussage gilt für $n = 0$, weil Σ nach Voraussetzung des Satzes endlich erfüllbar ist. Wie nehmen nun an, daß Δ_n endlich erfüllbar sei, und zeigen, daß dann auch Δ_{n+1} endlich erfüllbar ist. Wir müssen zeigen, daß $\Delta_n \cup \{\alpha_{n+1}\}$ oder $\Delta_n \cup \{\sim \alpha_{n+1}\}$ endlich erfüllbar ist. Wenn dies nicht der Fall ist, können wir endliche Teilmengen Σ_0 und Σ_1 von Δ_n wählen, so daß beide, $\Sigma_0 \cup \{\alpha_{n+1}\}$ und $\Sigma_1 \cup \{\sim \alpha_{n+1}\}$, nicht erfüllbar sind. Dann ist aber $\Sigma_0 \cup \Sigma_1 \subseteq \Delta_n$ endlich und nicht erfüllbar, weil jede Wahrheitsbelegung entweder α_{n+1} oder $(\sim \alpha_{n+1})$ erfüllen muß. Das steht im Widerspruch zu unserer Induktionsannahme.

Dann ist auch Δ, die aufsteigende Vereinigung der Δ_n, endlich erfüllbar. Und Δ ist maximal im folgenden Sinn: Für jede Formel α ist $\alpha \in \Delta$ oder $\sim \alpha \in \Delta$.

Nun definieren wie eine Wahrheitsbelegung v wie folgt: Für jedes Satzsymbol A setzen wir $v(A) = W$ gdw $A \in \Delta$.

Behauptung: Für jede Formel φ gilt: $\bar{v}(\varphi) = W$ gdw $\varphi \in \Delta$.

Wir beweisen die Behauptung durch Induktion über den Aufbau von φ. Wenn φ ein Satzsymbol ist, dann gilt die Behauptung aufgrund der Definition von v und von $\bar{v}$. Nun sei $\varphi = \sim \psi$ und die Behauptung gelte für ψ. Dann ist $\bar{v}(\varphi) = W$ gdw $\bar{v}(\psi) = F$ gdw $\psi \notin \Delta$ wegen der Induktionsannahme. $\psi \notin \Delta$ impliziert aber nun $\sim \psi = \varphi \in \Delta$, da Δ ja maximal ist. Umgekehrt gilt auch, wenn $\varphi \in \Delta$ dann $\psi \notin \Delta$, da Δ ja endlich erfüllbar ist. Dehalb haben wir $\bar{v}(\varphi) = W$ gdw $\varphi \in \Delta$, wie gewünscht. Die anderen Fälle, in denen φ von der Form $(\psi \wedge \chi)$, $(\psi \vee \chi)$, $(\psi \rightarrow \chi)$, $(\psi \leftrightarrow \chi)$ ist, sind ähnlich. Wenn Sie die Aufgabe Ü2 über die Junktoren gemacht haben, können Sie sich auf $\vee$ oder $\wedge$ oder $\rightarrow$ alleine beschränken (nicht jedoch auf $\leftrightarrow$, wie Ü3 zeigt).

Nun haben wir, daß v eine Wahrheitsbelegung ist, die jede Formel von Δ erfüllt und daher erst recht jede Formel von $\Sigma \subseteq \Delta$ erfüllt. Also ist Σ wie gewünscht erfüllbar. $\square$

Beweis des Korollars aus dem Kompaktheitssatz: Wenn es keine endliche Teilmenge Σ_0 von Σ gibt, die φ impliziert, dann ist $\Sigma \cup \{\sim \varphi\}$ endlich erfüllbar, und daher nach dem Kompakheitssatz erfüllbar.

Aus zeitlichen Gründen lagern wir etwas Technik in die Übungen aus.

Definition 2.10. *Eine Menge X heißt* abzählbar *gdw es eine surjektive Funktion $f \colon \mathbb{N} \rightarrow X$ gibt.*

DEFINITION 2.11. *Eine Menge X heißt* abzählbar' *gdw es eine injektive Funktion $f\colon X \to \mathbb{N}$ gibt.*

Ü4 Zeigen Sie, daß abzählbar und abzählbar' äquivalent sind.

Ü5. Zeigen Sie, daß $\bigcup_{n\in\mathbb{N}} \mathbb{N}^n$ abzählbar ist.

Ü6. Nun eine anspruchvollere Aufgabe mit etwas Mengenlehre: Zeigen Sie, daß die Anzahl der logisch nicht äquivalenten Vervollständigungen einer konsistenten Menge aussagenlogischer Formeln entweder endlich oder abzählbar oder 2^ω (dies ist die Mächtigkeit des Kontinuums) ist.

Hinweis: Für analytische Mengen $A \subseteq 2^\omega$ gilt: Wenn A überabzählbar ist, dann ist $|A| = 2^\omega$. Beweise dieser wichtigen Tatsache findet man in Jech [**3**] oder Lévy [**4**].

Nun muß noch gezeigt werden, daß die Menge der logisch nicht äquivalenten Vervollständigungen einer konsistenten Theorie analytisch ist. Sie ist sogar G_δ.

SATZ 2.12. *Die Menge der aussagenlogischen Tautologien ist entscheidbar.*

Beweis: Für eine gegebene Formel gibt es einen Algorithmus oder eine effektive Prozedur, die in endlicher Zeit entscheidet, ob φ eine Tautologie ist oder nicht. Wir erstellen eine Liste aller Möglichkeiten, den in φ auftretenden Satzsymbolen Wahrheitswerte zuzuordnen. Für jede dieser Möglichkeiten v berechnen wir den sich ergebenden Wahrheitwert von φ, $\bar{v}(\varphi)$. Wenn dieser Wahrheitswert für alle v W ist, dann ist φ eine Tautologie, sonst nicht. $\square$

KAPITEL 3

Die Logik der ersten Stufe

Wie betrachten jetzt eine Logik, die viel reicher als die Aussagenlogik ist, nämlich die Logik der ersten Stufe. Insbesondere kann diese Logik Ideen ausdrücken, die in verschiedenen mathematischen Theorien vorkommen. Zuerst führen wie eine Beschreibung der Symbole einer Sprache erster Stufe ein:

Logische Symbole

0. Klammern (und),
1. Junktoren $\to$ und $\sim$,
2. Variablen $v_0, v_1, \ldots$
3. Gleichheitszeichen $=$,
4. Quantor $\forall$.

Zur Menge τ der nichtlogischen Symbole gehören (je nach Auswahl)

1. Prädikatssymbole: Für jede natürliche Zahl $n > 0$ eine möglicherweise leere, möglicherweise unendliche Menge n-stelliger Prädikatssymbole,
2. Konstantensymbole: Eine möglicherweise leere, möglicherweise unendliche Menge von Symbolen,
3. Funktionssymbole: Für jede natürliche Zahl $n > 0$ eine möglicherweise leere Menge n-stelliger Funktionssymbole.

τ wird Symbolmenge, Sprache, similarity type, signature, Signatur genannt. Es ist auch $\tau = \emptyset$ gestattet. τ und $\mathscr{L}(\tau)$ (s.u.) werden Sprache genannt.

Bemerkung: Das Gleichheitszeichen ist ein zweistelliges Prädikatssymbol, es wir jedoch im Gegensatz zu den anderen zweistelligen Prädikatssymbolen als logisches Symbol betrachtet.

Andernfalls sagt man explizit, daß man mit einer Sprache ohne Gleichheit arbeitet (non-equational language).

Beachten Sie, daß es tatsächlich viele verschiedene Sprachen der ersten Stufe gibt, die von der Wahl der Prädikats-, Konstanten- und Funktionssymbole abhängen. Zwei Beispiele sind:

In der *Sprache der Mengenlehre* gibt neben dem Gleichheitszeichen nur ein zweistelliges Prädikatssymbol: $\in$. Es gibt keine Prädikatssymbole anderer Stelligkeit und keine Konstantensymbole und keine Funktionssymbole.

In der Sprache der elementaren Zahlentheorie gibt es genau ein zweistelliges Prädikatssymbol $<$, ein Konstantensymbol 0, ein einstelliges Funktionssymbol

S (für die Nachfolgerfunktion) und drei zweistellige Funktionssymbole $+$, $\cdot$, E, die die Addition, die Multiplikation und die Exponentiation darstellen. Die Exponentiation gehört manchmal nicht dazu.

Terme und Formeln. Wie bisher ist ein Ausdruck eine endliche Folge von Symbolen. Nur bestimmte Ausdrücke haben eine Bedeutung, und diese heißen Formeln. Zunächst legen wir fest, was Terme sind.

DEFINITION 3.1. *Terme*

1. *Jedes Konstantensymbol und jede Variable ist ein Term.*
2. *Wenn f ein n-stelliges Funktionssymbol ist und $t_1, \ldots, t_n$ Terme sind, dann ist auch $ft_1 \ldots t_n$ ein Term. (Beachten Sie, daß wir keine Klammern und keine Kommata schreiben. Wenn Sie dies auf $+$, $\cdot$ und E anwenden, erhalten Sie die sogenannte polnische Notation. Eine Zeitlang wurde die umgekehrte polnische Notation $t_1 \ldots t_n f$ auf Hewlett-Packard-Taschenrechnern benutzt.)*

Natürlich liegt uns hier ein weiteres Beispiel einer induktiven Definition vor: Ein Ausdruck ist demnach ein Term genau dann, wenn er es aufgrund der Regeln 1 und 2 sein muß. Wir sagen, daß die Menge der Terme durch Abschluß der Menge der Konstantensymbole und der Variablen unter den Funktionssymbolen erzeugt wird. Wenn es keine Funktionssymbole in der Sprache gibt, dann sind die Konstantensymbole und die Variablen die einzigen Terne und eine Definition durch Induktion ist nicht notwendig. Einige Beispiele für Terme in der Sprache der elementaren Zahlentheorie:
$+v_2Sv_1$,
$SSS0$
$+Ev_1SSEv_300$.

Als nächstes kommen wir nun zu der einfachsten Art von Formeln, den sogenannten atomaren Formeln.

DEFINITION 3.2. *Atomare Formeln sind Ausdrücke der Form $Pt_1 \ldots t_n$ mit einem n-stelligen Prädikatssymbol P oder dem Gleichheitssymbol $=$ (dann ist $n = 2$) und Termen $t_1, \ldots, t_n$.*

Dieser Begriff wird also explizit definiert und nicht durch Induktion. Die atomaren Formel sind die Bausteine, aus denen kompliziertere Formeln aufgebaut werden. Die Rolle der atomaren Formeln ist also analog zur Rolle der Satzvariablen in der Aussagenlogik. Wenn die Symbolmenge groß ist, kann schon die Menge der atomaren Formel überabzählbar sein.

DEFINITION 3.3. *Formel.*

1. *Jede atomare Formel ist eine Formel.*
2. *Wenn φ eine Formel ist, dann ich auch $(\sim \varphi)$ eine Formel.*
3. *Wenn φ und ψ Formeln ist, dann ist auch $(\varphi \to \psi)$ eine Formel*

4. *Wenn ψ eine Formel ist und v eine Variable ist, dann ich auch $(\forall v\psi)$ eine Formel.*

Wir sagen, daß die Menge der Formeln dadurch erzeugt wird, daß die Menge der atomaren Formeln unter den Junktoren und den Quantoren abgeschlossen wird.

Wir geben als Beispiele zwei Formeln der Mengenlehre:

$$\forall v_2 \in v_2 v_1$$

$$(\sim \forall v_1(\sim \forall v_2 \in v_2 v_1))$$

Diese erste Formel sagt: „Jede Menge ist ein Element von v_1", und die zweite drückt aus: „es gibt eine Menge, die jede Menge als Element enthält." Es gibt einen wichtigen Unterschied zwischen diesen beiden Beipielen: Im zweiten Beispiel haben wir einen vollständigen Satz, im ersten Beispiel hingegen haben wir eine Formel, deren Bedeutung von der Interpretation der Variablen abhängt. v_1 wird eine freie Variable der ersten Formel genannt. Wir geben jetzt eine genaue Definition dieses Begriffs:

Definition 3.4. *Die Eigenschaft „v tritt frei in der Formel φ auf" wird induktiv über den Aufbau von φ definiert.*

0. *Wenn φ atomar ist, dann tritt v frei in φ auf gdw v eine Variable in φ ist.*
1. *v tritt frei in $(\sim \varphi)$ auf gdw v frei in φ auftritt.*
2. *v tritt frei in $(\varphi \to \psi)$ auf gdw v in φ oder in ψ frei auftritt.*
3. *v tritt frei in $(\forall v_i \varphi)$ auf gdw v frei in φ auftritt und ungleich v_i ist.*

Wir schreiben $\mathrm{fr}(\varphi)$ *für die Menge aller Variablen, die frei in φ auftreten,*

Wenn keine Variable frei in der Formel φ auftritt, dann sagen wir, daß φ ein Satz ist. Dies sind die Formeln mit einer vollständigen Bedeutung. Sie ist unabhängig von der Interpretion der Variaben. Die Variablen, die nicht frei in der Formel φ auftreten, heißen die gebundenen Variablen von φ. Wir werden das präziser diskutieren, wenn wir die Semantik der Logik der ersten Stufe vorstellen.

Abkürzungen und Klammern. Um unsere Fomeln einfacher lesen zu können, erlauben wir uns, Ausdrücke zu schreiben, die streng genommen keine Formeln sind, aber einfach in Formeln übertragen werden können:

Abkürzungen.

$(\alpha \vee \beta)$ für $((\sim \alpha) \to \beta)$
$(\alpha \wedge \beta)$ für $(\sim (\alpha \to (\sim \beta)))$
$(\alpha \leftrightarrow \beta)$ für $((\alpha \to \beta) \wedge (\beta \to \alpha))$
$(\exists v \alpha)$ für $(\sim \forall v(\sim \alpha))$
$t_1 = t_2$ für $= t_1 t_2$

$t_1 \neq t_2$ für $(\sim= t_1 t_2)$

Klammern
0. Wir lassen die äußersten Klammern weg.
1. $\exists v$ und $\forall v$ beziehen sich auf sowenig wie möglich.
2. $\alpha \to \beta \to \gamma$ steht für $\alpha \to (\beta \to \gamma)$.

Wahrheit und Modelle. In der Aussagenlogik dienen Wahrheitsbelegungen, um den Satzsymbolen und dann auch beliebigen Formeln Wahrheitswerte zuzuweisen. In der Logik der ersten Stufe wird die Rolle der Wahrheitbelegung durch die Strukturen übernommen. Strukturen liefern eine Bedeutung für die nichtlogischen Symbole der jeweiligen Sprache ersten Stufe.

Definition 3.5. *Eine Struktur $\mathfrak{A}$ für eine gegebene Sprache erster Stufe ist eine Funktion, die als Definitionsbereich $\{\forall\} \cup \tau$ hat und für die folgendes gilt:*

0. *$\mathfrak{A}$ weist dem Quantor $\forall$ eine nicht leere Menge $|\mathfrak{A}|$ zu, die das Universum von $\mathfrak{A}$ oder der Träger von $\mathfrak{A}$ (domain, universe, support) genannt wird.*

1. *$\mathfrak{A}$ weist jedem n-stelligen Prädikatssymbol ein n-stelliges Prädikat $P \subseteq |\mathfrak{A}|^n$ zu, d.h. $P^{\mathfrak{A}}$ ist eine Menge von n-Tupeln von Elementen des Universums $|\mathfrak{A}|$.*

2. *$\mathfrak{A}$ weist jedem Konstantensymbol c ein Element $c^{\mathfrak{A}} \in |\mathfrak{A}|$ zu.*

3. *$\mathfrak{A}$ weist jedem n-stelligen Funktionssymbol eine n-stellige Funktion $f^{\mathfrak{A}}\colon |\mathfrak{A}|^n \to |\mathfrak{A}|$ zu.*

Die Idee ist: $\mathfrak{A}$ gibt dem Quantor $\forall$ die Bedeutung für jedes Element von $|\mathfrak{A}|$. Außerdem weist $\mathfrak{A}$ den Prädikats-, Funktions- und Konstantensymbolen der Sprache Bedeutungen zu. Wir verlangen, daß die n-stelligen Funktionssymbole so interpretiert werden wie totale Funktionen auf dem Definitionsbereich $|\mathfrak{A}|^n$.

Nun möchten wir eine Bedeutung für den Satz „die Formel φ ist wahr in der Struktur $\mathfrak{A}$" angeben. Hierfür müssen wir zuerst eine Bedeutung für die Vabiablen unserer Logik definieren. Eine Belegung in $\mathfrak{A}$ oder eine $\mathfrak{A}$-Belegung ist eine Funktion s von der Menge der Variablen in $|\mathfrak{A}|$. Wir wollen

„$\mathfrak{A}$ mit der Belegung s erfüllt φ",

kurz $\mathfrak{A} \models \varphi[s]$ für beliebige $\mathfrak{A}$-Belegungen per Induktion über φ definieren.

Zuerst erhalten alle Terme Bedeutungen, indem wir s zu einer Funktion $\bar{s}$ auf der Menge der Terme erweitern:

Definition 3.6. *1.* $\bar{s}(v) = s(v)$
2. $\bar{s}(c) = c^{\mathfrak{A}}$
3. Wenn $t_1, \ldots, t_n$ Terme sind und f eine n-stelliges Funktionssymbol ist, dann ist $\bar{s}(ft_1 \ldots t_n) = f^{\mathfrak{A}}(\bar{s}(t_1), \ldots, \bar{s}(t_n))$.

Um die Quantorenschritte in der Definition von '$\mathfrak{A}$ mit der Belegung s erfüllt φ" richtig zu behandeln, definieren wir zunächst eine Art, Belegungen s in einem ihrer Argumente eventuell zu ändern:

DEFINITION 3.7. *Wenn s eine $\mathfrak{A}$-Belegung ist und x eine Variable ist und a ein Element von $|\mathfrak{A}|$ ist, dann ist $s(x|a)$ (sprich „s, x ersetzt durch a") die folgende $\mathfrak{A}$-Belegung:*

$$s(x|a)(y) = \begin{cases} s(y), & \text{falls } y \neq x \\ a, & \text{falls } y = x. \end{cases}$$

DEFINITION 3.8. *„$\mathfrak{A}$ mit der Belegung s erfüllt φ" wird induktiv über den Aufbau von φ gleichzeitig für alle s definiert:*

Wenn φ atomar ist, dann

1. $\mathfrak{A} \models = t_1 t_2[s]$ *gdw* $\bar{s}(t_1) = \bar{s}(t_2)$.
2. *Für jedes n-stellige Prädikatssymbol P,* $\mathfrak{A} \models P t_1 \dots t_n[s]$ *gdw* $\langle \bar{s}(t_1), \dots, \bar{s}(t_n) \rangle \in P^{\mathfrak{A}}$.
3. $\mathfrak{A} \models (\sim \varphi)[s]$ *gdw nicht* $\mathfrak{A} \models \varphi[s]$.
4. $\mathfrak{A} \models (\varphi \to \psi)[s]$ *gdw* $\mathfrak{A} \not\models \varphi[s]$ *oder* $\mathfrak{A} \models \psi[s]$.
5. $\mathfrak{A} \models \forall x \varphi[s]$ *gdw für jedes* $a \in |A|$, $\mathfrak{A} \models \varphi[s(x|a)]$.

Aus der „Erfüllt-Relation" $\models$ wird nun, analog wie in der Aussagenlogik, die logische Implikation für die Logik der ersten Stufe definiert:

DEFINITION 3.9. *Sei Γ eine Formelmenge und sei φ eine Formel. Γ impliziert φ , (oder aus Γ folgt φ oder φ folgt aus Γ oder, in Zeichen, $\Gamma \models \varphi$) gdw für jede Struktur $\mathfrak{A}$ der Sprache von $\Gamma \cup \{\varphi\}$ und für jede $\mathfrak{A}$-Belegung s gilt: Wenn $\mathfrak{A}$ jedes Element von Γ erfüllt, dann erfüllt $\mathfrak{A}$ auch φ.*

Wenn Γ nur ein Element Γ hat, dann schreiben wir $\gamma \models \varphi$ statt $\{\gamma\} \models \varphi$. Wenn Γ leer ist, dann schreiben wir $\models \varphi$ statt $\emptyset \models \varphi$, und sagen daß φ allgemeingültig (valid, gültig) ist. Die gültigen Formeln der Logik der ersten Stufe entsprechen den Tautologien der Aussagenlogik. φ ist gültig gdw wenn jede Struktur $\mathfrak{A}$ und jede $\mathfrak{A}$ Belegung zusammen φ erfüllen.

Vorsicht: Die logische Implikation $\models$ heißt auf deutsch die Folge-Relation oder auch die Folgerungsrelation. Letzters ist leicht zweideutig, wie Sie in den nächsten Vorlesungen sehen werden (es kann auch die Relation $\vdash$ unter „Folgerung"verstanden werden).

Der folgende Satz beschreibt die Rolle der freien Variablen.

SATZ 3.10. *Koinzidenzsatz. Seien s_1 und s_2 $\mathfrak{A}$-Belegungen, die auf den Variablen, die frei in φ auftreten, übereinstimmen. Dann gilt*

$$\mathfrak{A} \models \varphi[s_1] \text{ gdw } \mathfrak{A} \models \varphi[s_2].$$

Beweis durch Induktion über den Aufbau von φ.

Fall 1: φ ist atomar. $\varphi = Pt_1 \dots t_n$ (P kann auch das Gleichheitszeichen sein). In diesem Fall tritt jede Variable in φ frei auf. Deshalb stimmen s_1 und s_2 auf allen Variablen in t_i für jedes i überein, und $\bar{s_1}(t_i) = \bar{s_2}(t_i)$ für jedes i. Daher ist $\mathfrak{A} \models \varphi[s_1]$ gdw $(\bar{s_1}(t_1), \dots, \bar{s_1}(t_n)) \in P^{\mathfrak{A}}$ gdw $(\bar{s_2}(t_1), \dots, \bar{s_2}(t_n)) \in P^{\mathfrak{A}}$ gdw $\mathfrak{A} \models \varphi[s_2]$. wie gewünscht.

Fall 2 und Fall 3: φ ist von der Form $(\sim \alpha)$ oder $(\alpha \to \beta)$. Diese Fälle folgen direkt aus den Induktionsannahmen.

Fall 4 (der interessante Fall): $\varphi = \forall x \psi$. Dann ist jede Variable frei in φ gdw sie frei in ψ und nicht gleich x ist. Somit stimmen $s_1(x|a)$ und $s_2(x|a)$ für jedes Element a von $|\mathfrak{A}|$ auf den freien Variablen von ψ überein. Nach der Induktionannahmen ist $\mathfrak{A} \models \psi[s(x|a)]$ gdw $\mathfrak{A} \models \psi[s(x|a)]$. Da dies für beliebiges a gilt, folgt, daß $\mathfrak{A} \models \forall y \psi[s_1]$ gdw $\mathfrak{A} \models \forall x \psi[s_2]$. □

Korollar 3.11. *Wenn σ ein Satz ist, dann gilt $\mathfrak{A} \models \sigma[s]$ für keine Belegung oder aber für alle Belegungen.*

Wir sagen, daß der Satz σ wahr in $\mathfrak{A}$ ist gdw wenn $\mathfrak{A}$ mit mit jeder $\mathfrak{A}$-Belegung erfüllt, geschrieben $\mathfrak{A} \models \sigma$. Sonst ist σ falsch in $\mathfrak{A}$. Wenn σ wahr in $\mathfrak{A}$ ist, dann ist $\mathfrak{A}$ ein Modell von σ. Wenn Σ eine Menge von Sätzen ist, dann ist $\mathfrak{A}$ ein Modell von Σ gdw $\mathfrak{A}$ ein Modell von jedem Satz Σ ist.

Korollar 3.12. *Seien Σ eine Menge von Sätzen und sei τ ein Satz. Dann gilt $\Sigma \models \tau$ gdw jedes Modell von Σ auch ein Modell von τ ist.*

Beachten Sie, daß die Definition der logischen Implikation für die Logik der ersten Stufe viel komplizierter als für die Aussagenlogik ist. Um zu entscheiden, ob eine Formel gültig ist oder nicht, müssen wir jede Struktur der Sprache und jede Belegung beachten und dann prüfen, ob $(\mathfrak{A}, s)$ φ erfüllt oder nicht. Deshalb ist es nicht klar, ob die Menge der gültigen Formeln der Logik der ersten Stufe entscheidbar ist. Tatsächlich werden wir zeigen, daß die Gültigkeit nicht entscheidbar ist. Überraschenderweise impliziert der Gödelsche Vollständigkeitssatz, daß die Menge der gültigen Formeln der Logik der ersten Stufe effektiv aufzählbar ist. Wir werden diese Aufzählbarkeit und die Unentscheidbarkeit später zeigen.

In einer vielleicht etwas willkürlichen, jedoch allgemein akzeptierten Aufteilung gehört $\models$ zu den semantischen Begriffen, die sich unmittelbar mit den Strukturen beschäftigen. Wir werden nun noch zwei weitere semantische Begriffe definieren, bevor wir uns dann auf die sogenannte synaktische Seite begeben.

Definition 3.13. *Sei $\mathfrak{A}$ eine Struktur und sei $\mathrm{fr}(\varphi) \subseteq \{v_0, \dots, v_{n-1}\}$ und seien $a_0, \dots, a_{n-1}$ Elemente aus $|\mathfrak{A}|$. Dann schreiben wir*

$$\mathfrak{A} \models \varphi[a_0, \dots, a_{n-1}]$$

gdw $(\mathfrak{A}, s) \models \varphi$ für $s(v_i) = a_i$, $i = 0, \dots, n-1$.

DEFINITION 3.14. *$P \subseteq |\mathfrak{A}|^n$ ist definierbar in $\mathfrak{A}$ gdw es eine Formel φ mit den freien Variablen aus $\{v_0, \ldots, v_{n-1}\}$ gibt, so daß $P = \{(a_0, \ldots, a_{n-1}) \mid \mathfrak{A} \models \varphi[a_0, \ldots, a_{n-1}])\}$. Wir sagen hierzu φ definiert P in $\mathfrak{A}$.*

Ein Beispiel für die Struktur $\mathfrak{N} = (\mathbb{N}, 0, 1, +, \cdot)$: Einige Relationen sind in $\mathfrak{N}$ definierbar, andere nicht. Da es nur abzählbar viele Formeln gibt, sind nur abzählbar viele Relationen definierbar. Es gibt jedoch überabzählbar viele Relationen auf $\mathbb{N}$. Zum Beispiel ist die Ordungsrelation $\{(n, m) \mid n < m\}$ definierbar und die Menge der Primzahlen und die Exponentiationsrelation $\{(n, m, s) \mid s = n^m\}$. Die erstgenannte wird durch die Formel $\exists v_3 v_1 + S v_3 = v_2$ definiert, die zweite durch die Formel $1 < v_1 \wedge \forall v_2 \forall v_3 (v_1 = v_2 \cdot v_3 \rightarrow v_2 = 1 \vee v_3 = 1)$ und die dritte durch eine kompliziertere Formel, die später vielleicht skizziert wird. Wir werden später auch zeigen, daß jede entscheidbare Relation und jede effektiv aufzählbare Relation und viele weitere Relationen auf $\mathbb{N}$ in $\mathfrak{N}$ definierbar sind.

Es ist oft viel schwieriger zu zeigen, daß eine gegebene Relation in einer gegebenen Struktur nicht definierbar ist. Ein hinreichendes Kriterium für Nicht-Definierbarkeit ist zum Beispiel die Existenz eines Isomorphismus, der P bewegt. (Isomorphismen erhalten alle in definierbaren Relationen, dies zeigt man induktiv über den Aufbau der definierenden Formel. Übung!)

Beweistheorie. Der Begriff der Gültigkeit ist in der Logik der ersten Stufe ziemlich kompliziert. Gibt es eine einfachere Definition? Können wir zum Beispiel für eine Sprache mit nur endlich vielen nichtlogischen Symbolen die Menge der gültigen Formeln effektiv aufzählen? Gödel gab eine positive Antwort. Dieses Ergebnis wird der Gödelsche Vollständigkeitssatz genannt.

Fie Idee ist einfach. Wir geben eine enscheidbare Menge Λ von gültigen logischen Axiomen an. Dann nennen wir eine endliche Folge von Formeln einen formalen Beweis, wenn jede dieser Formeln ein logisches Axiom ist oder unter Verwendung der Schlußregel Modus Ponens aus früheren Formeln folgt. Die Modus Ponens Regel (MP) lautet:

$$\text{Aus } \varphi \text{ und } (\varphi \rightarrow \psi) \text{ folgt } \psi.$$

Die Menge der Beweise ist entscheidbar. Nun ist eine Formel ein formaler Satz gdw sie die letzte Formel eines Beweises ist. Da die Menge der Beweise entscheidbar ist, folgt, daß die Menge der formalen Sätze effektiv aufzählbar ist.

Formale Beweise

Sei eine Sprache τ der ersten Stufe gegeben. Wir werden eine besondere Menge von Formeln Λ definieren, die Menge der logischen Axiome. Diese wird in unseren formalen Beweisen benutzt.

DEFINITION 3.15. *Die Menge Λ der logischen Axiome besteht aus sechs Teilmengen. φ heißt eine Verallgemeinerung von ψ gdw für ein $n \geq 0$ und*

Variablen $x_1 \ldots, x_n$ gilt

$$\varphi = \forall x_1 \ldots \forall x_n \psi.$$

Wir gestatten auch $n = 0$. Die logischen Axiome sind Verallgemeinerungen von Formeln aus den Gruppen 1 bis 6. Seien x, y Variablen und α, β Formeln. Wir beschreiben nun die Gruppen 1 bis 6:

1. *Tautologien der Aussagenlogik.*
2. *Ersetzungsaxiome: $\forall x \alpha \to \alpha_t^x$, wenn t für x in α eingesetzt werden kann. Die Formel α_t^x wird in Definition 3.16 definiert. Wann t überhaupt für x eingesetzt werden kann, wird in Definition 3.17 beschrieben.*
3. $\forall x(\alpha \to \beta) \to (\forall x \alpha \to \forall x \beta)$.
4. $\alpha \to \forall x \alpha$, *wenn x nicht frei in α auftritt.*
5. $x = x$.
6. $x = y \to (\alpha \to \alpha')$, *wenn α atomar ist und α' aus α dadurch entsteht, daß x durch y an einigen Stellen ersetzt wird.*

Sei nun Γ eine Menge von Formeln und sei φ eine Formel. Ein Beweis von φ aus Γ ist eine Folge $\langle \alpha_0, \ldots, \alpha_n \rangle$ von Formeln, so daß $\alpha_n = \varphi$ und für jedes $i \leq n$ gilt:

1. $\alpha_i \in \Gamma \cup \Lambda$ *oder*
2. *es gibt $j, k < i$ so daß $\alpha_k = (\alpha_j \to \alpha_i)$ ist. In diesem Falle ergibt sich α_i aus vorangehenden α_j und α_k aus dem modus ponens.*

Wenn es einen Beweis von φ aus Γ gibt, dann sagen wir, daß φ aus Γ beweisbar ist, und schreiben $\Gamma \vdash \varphi$.

Gruppe 1: Tautologien.

Die Tautologien der Logik der ersten Stufe ergeben sich aus den Tautologien der Aussagenlogik, die nur $\sim$ und $\to$ (nicht aber $\wedge$, $\vee$, $\leftrightarrow$ enthalten), indem wir jedes Satzsymbol durch eine Formel der Logik der ersten Stufe ersetzen. In Gruppen 1 erlauben wir alle Verallgemeinerungen solcher Formeln. Zum Beispiel gehört die Formel $\forall x[(\forall y \sim Py \to\sim Px) \to (Px \to\sim \forall y \sim Py)]$ zu Gruppe 1, weil sie eine Verallgemeinerung der Formel in eckigen Klammern ist und sich die Formel in eckigen Klammern aus der folgenden Tautologie der Aussagenlogik ergibt:

$$(A \to\sim B) \to (B \to\sim A).$$

Eine andere Art, die Menge der Tautologien der ersten Stufe zu erklären, ist folgende: Nennen wir eine Formel prim gdw sie entweder atomar ist oder von der Form $\forall x \alpha$ ist. Jede Formel der Logik der ersten Stufe wird aus Primformeln mithilfe der Junktoren $\sim$ und $\to$ aufgebaut. Nun definieren wir die Tautologien der Aussagenlogik um, indem wir die Primformeln wie Satzsymbole behandeln und nur die Junktoren $\sim$ und $\rightarrow$ verwenden. Dann darf „außen" noch verallgemeinert werden. Das Ergebnis ist die Menge der Tautologien der Logik der ersten Stufe.

Gruppe 2: Ersetzung.

DEFINITION 3.16. *Zuerst definieren wir für Formeln α, Variablen x und Terme t die Formel α_t^x. Dies ist die Ersetzung von x durch t in α. Dies wird indukiv über den Aufbau von α definiert, und — Vorsicht — ist nicht immer definiert.*

1. *Für atomares α ergibt sich α_t^x, indem wir in α alle x durch t ersetzen.*
2. $(\sim \alpha)_t^x = (\sim \alpha_t^x)$.
3. $(\alpha \rightarrow \beta)_t^x = (\alpha_t^x \rightarrow \beta_t^x)$.
4. $(\forall y \alpha)_t^x$ *ist* $\forall y \alpha$ *wenn* $x = y$, *und* $\forall y(\alpha_t^x)$ *sonst.*

Hier wird es interessant. Es scheint, daß $(\forall x \alpha \rightarrow \alpha_t^x)$ ein vernünftiges (d.h. korrektes, s.u.) Axiom ist. Dieses Axiom kann aber falsch sein, wenn nämlich z für ein freies y eingesetzt wird. Zum Beispiel schauen wir die Formel $\alpha = \exists y(y \neq x)$ und $t = y$ an. Dann wird $\forall x \alpha \rightarrow \alpha_t^x$ zu

$$\forall x \exists y(x \neq y) \rightarrow \exists y(y \neq y),$$

was offensichtlich für jede Struktur falsch ist, deren Universum mehr als ein Element hat. Wir lösen dieses Problem, indem wir α, x und t einschränken.

DEFINITION 3.17. *Wir definieren induktiv über den Aufbau von α, wann t für x in α eingesetzt werden kann.*

1. *t kann in atomaren α immer für x eingesetzt werden.*
2. *t kann in $\sim \alpha$ für x eingesetzt werden gdw dies für α möglich ist. t kann in $(\alpha \rightarrow \beta)$ für x eingesetzt werden, gdw dies für α und für β der Fall ist.*
3. *t kann in $\forall y \alpha$ für x eingesetzt werden gdw*
   (a) *x in $\forall y \alpha$ nicht frei auftritt, oder*
   (b) *$x \neq y$ und y in t nicht auftritt und t in α für x eingesetzt werden kann.*

Erhalten wir nun tatsächlich eine gültige Formel $\forall x \alpha \rightarrow \alpha_t^x$, wenn t für x in α eingesetzt werden kann?

LEMMA 3.18. *Ersetzungslemma. Wenn der Term t in der Formel α für die Variable x eingesetzt werden kann, dann*

$$\mathfrak{A} \models \alpha_t^x[s] \text{ gdw } \mathfrak{A} \models \alpha[s(x|\bar{s}(t))].$$

Beweis: Wir führen den interessantesten Schritt vor: Sei $\varphi = \forall y\alpha$, und sei $x \neq y$ und trete y nicht in t auf und möge t für x in α eingesetzt werden können.
Dann $\mathfrak{A} \models \varphi^x_t[s]$
gdw $\mathfrak{A} \models \forall y\alpha^x_t[s]$
gdw f.a. $a \in A$, $\mathfrak{A} \models \alpha^x_t[s(y|a)]$
gdw (IV) f.a. $a \in A$, $\mathfrak{A} \models \alpha[s(y|a)(x|\bar{s}(t))]$
gdw (da $x \neq y$ und da y in t nicht auftritt) f.a. $a \in A$, $\mathfrak{A} \models \alpha[s(x|\bar{s}(t))(y|a)]$
gdw $\mathfrak{A} \models \forall y\alpha[s(x|\bar{s}(t))]$
gdw $\mathfrak{A} \models \varphi[s(x|\bar{s}(t))]$. □

Korollar 3.19. *Unter Verwendung dieses Lemmas können wird jetzt zeigen, daß die Ersetzungsaxiome gültig sind.*

Beweis: Nehmen wir an, daß t in α für x eingesetzt werden kann und $(\mathfrak{A}, s)$ die Formel $\forall x\alpha$ erfüllt . Wir müssen zeigen, daß $(\mathfrak{A}, s)$ auch α^x_t erfüllt. Wir wissen, daß $\mathfrak{A} \models \alpha[s(x|a)]$ für jedes $a \in |\mathfrak{A}|$. Dann gilt dies insbesondere für $a = \bar{s}(t)$. Damit ist die Formel $(\forall x\alpha \to \alpha^x_t)$ gültig, wie gewünscht. □

Satz 3.20. *Gültigkeitssatz. Jedes Axiom ist gültig, d.h., wenn φ ein logisches Axiom ist und $\mathfrak{A}$ eine Struktur ist und s eine $\mathfrak{A}$-Belegung ist, dann gilt $(\mathfrak{A}, s) \models \varphi$.*

Beweis: Beachten wir zuerst, daß jede Verallgemeinerung einer gültigen Formel auch gültig ist. Wenn zum Beispiel φ die Formel $\forall x\psi$ mit einem gültigen ψ ist, dann haben wir $\mathfrak{A} \models \psi[s]$ für alle $\mathfrak{A}$, s, gdw $\mathfrak{A} \models \psi[s(x|a)]$ für alle $\mathfrak{A}$, s, a, gdw $\mathfrak{A} \models \varphi[s]$.

Derselbe Beweis funktioniert, wenn φ von der Form $\forall x_1 \dots \forall x_n\psi$ ist.

Somit ist zu zeigen, daß alle Formeln in allen sechs Axiomengruppen gültig sind. Das ist klar für die Tautologien, da sie sich aus Tautologien der Aussagenlogik ergeben. Wir haben für die 2. Gruppe schon gezeigt, daß die Ersetzungsaxiome gültig sind.

Nun kommen wir zur Gruppe 3:

Betrachten wir das Axiom

$$\forall x(\alpha \to \beta) \to (\forall x\alpha \to \forall x\beta)$$

Um die Gültigkeit dieses Axioms zu sehen, genügt es zu zeigen, daß $\mathfrak{A} \models \forall x\beta[s]$, wenn $\mathfrak{A} \models \forall x(\alpha \to \beta)[s]$ und $\mathfrak{A} \models \forall x\alpha[s]$. Die beiden Voraussetzungen implizieren $\mathfrak{A} \models (\alpha \to \beta)[s(x|a)]$ für alle $a \in |\mathfrak{A}|$ und $\mathfrak{A} \models \alpha[s(x|a)]$ für alle $a \in |\mathfrak{A}|$. Zusammen ergibt dies und $\mathfrak{A} \models \beta[s(x|a)]$ für alle $a \in |\mathfrak{A}|$, also $\mathfrak{A} \models \forall x\beta[s]$.

Gruppe 4. Betrachten wir das Axiom

$$\alpha \to \forall x\alpha,$$

für α, in dem x nicht frei auftritt. Für die Korrektheit haben wir zu zeigen: Für alle $(\mathfrak{A}, s)$: Wenn $(\mathfrak{A}, s) \models \alpha$, dann auch $(\mathfrak{A}, s) \models \forall x\alpha$. Letzteres heißt, daß für jedes $a \in A$, $\mathfrak{A} \models \alpha[s(x|a)]$. Nun stimmen aber s und $s(x|a)$ für alle $a \in |\mathfrak{A}|$ auf den freien Variablen von α überein, da x nicht frei in α auftritt. Nach dem Koinzidenzlemma für Belegungen gilt, daß $\mathfrak{A} \models \alpha[s(x|a)]$ für jedes $a \in \mathfrak{A}$. Deshalb ist $\mathfrak{A} \models \forall x\alpha[s]$.

Gruppe 5: Klar.

Gruppe 6: Wir nehmen ein atomares α und betrachten das Axiom. $x = y \rightarrow (\alpha \rightarrow \alpha')$. Hierbei sei α' wie α, in dem x an manchen Stellen durch y ersetzt wurde. Wir haben für alle $(\mathfrak{A}, s)$ zu zeigen: Wenn $\mathfrak{A} \models \alpha[s]$ und $s(x) = s(y)$, dann $\mathfrak{A} \models \alpha'[s]$. Nehmen wir an, daß $\alpha = Pt_1 \dots t_n$ und $\alpha' = Pt'_1 \dots t'_n$ und daß t'_i aus t_i durch Ersetzung einiger x durch y entsteht. Da $s(x) = s(y)$ ist, ist auch $\bar{s}(t_i) = \bar{s}(t'_i)$, wie man induktiv über den Aufbau der Terme zeigt. Daher ist $(\bar{s}(t_1), \dots, \bar{s}(t_n)) \in P^{\mathfrak{A}}$ gdw $(\bar{s}(t'_1), \dots, \bar{s}(t'_n)) \in P^{\mathfrak{A}}$ und daher $\mathfrak{A} \models Pt_1 \dots t_n[s]$ gdw $\mathfrak{A} \models Pt'_1 \dots t'_n[s]$. Es folgt, daß $\mathfrak{A} \models \alpha'[s]$. $\square$

So, nun haben wir also zwei Begriffe logischer Implikation: $\Gamma \vdash \varphi$ bedeutet, daß es einen Beweis von φ aus Γ (und den logischen Axiomen Λ) gibt. Und $\Gamma \models \varphi$ (Γ impliziert φ logisch) bedeutet: Für jede Struktur $\mathfrak{A}$ und jede Belegung s gilt: Wenn $(\mathfrak{A}, s)$ alle γ aus Γ erfüllt, dann erfüllt $(\mathfrak{A}, s)$ auch φ. Der Gültigkeitssatz oder Korrektheitssatz stellt eine Verbindung zwischen den beiden Begriffen her:

SATZ 3.21. *Korrektheitssatz. Wenn $\Gamma \vdash \varphi$, dann $\Gamma \models \varphi$.*

Beweis: Per Induktion über die kürzeste Länge eines Beweises von φ aus Γ. Sei $\varphi_1 \dots \varphi_n = \varphi$ ein Beweis von φ aus Γ minimaler Länge.

Fall 1: φ ist ein logisches Axiom. Dann folgt aus dem Gültigkeitssatz, daß $\emptyset$ die Formel φ logisch impliziert. Daher impliziert Γ die Formel φ logisch.

Fall 2: $\varphi \in \Gamma$. Dann impliziert Γ φ.

Fall 3: Es gibt $i, j < n$, so daß $\varphi_i = (\varphi_j \rightarrow \varphi)$. Nach der Induktionsannahme impliziert Γ die beiden Formeln φ_i und φ_j logisch, weil es kürzerere Beweise aus Γ für φ_i und für φ_j gibt. Es folgt, daß $\Gamma\varphi$ logisch impliziert. $\square$

Der Korrektheitssatz hat Folgen für die Begriffe Konsistenz und Erfüllbarkeit.

DEFINITION 3.22. *1. Eine Formelmenge Γ ist widerspruchsfrei oder konsistent (consistent) gdw es keine Formel φ gibt, so daß Γ sowohl φ als auch $\sim \varphi$ beweist.*

2. Γ ist erfüllbar (satisfiable) gdw es eine Struktur $\mathfrak{A}$ und eine Belegung s gibt, so daß $(\mathfrak{A}, s) \models \varphi$ für jedes $\varphi \in \Gamma$.

Die Konsistenz wird als syntaktischer Begriff aufgefasst, da sie sich mit dem Konzept „Beweis” befasst, die Erfüllbarkeit hingegen wird als semantischer Begriff aufgefasst. Da sie sich mit dem Konzept „Struktur” befasst. Der Korrektheitsatz liefert uns nun folgendes

KOROLLAR 3.23. *Wenn* Γ *erfüllbar ist, dann ist* Γ *auch konsistent.*

Beweis: Wenn Γ nicht konsistent wäre, dann würde Γ sowohl φ als auch $\sim \varphi$ für ein φ beweisen. Wegen des Korrektheitssatzes bedeutet dies, daß Γ die Formel φ und $\sim \varphi$ logisch impliziert. Da $\varphi \wedge \sim \varphi$ in jeder Struktur $\mathfrak{A}$ mit jeder $\mathfrak{A}$-Belegung s falsch ist, kann Γ nicht erfüllbar sein. □

Der Vollständigkeitssatz liefert Umkehrungen zum Korrektheitssatz und zu dessen Korollar.

SATZ. **Vollständigkeitssatz.**

(a) *Jede konsistente Formelmenge ist erfüllbar.*

(b) *Wenn* $\Gamma \models \varphi$, *dann* $\Gamma \vdash \varphi$.

KAPITEL 4

Der Beweis des Vollständigkeitssatzes

1. Metasätze

Dem Beweis des Vollständigkeitssatzes müssen wir zunächst einige Sätze über formale Beweise voranstellen. Diese werden Metasätze genannt, da sie Sätze über das Konzept von Sätzen sind. Diese Ergebnisse erklären auch unsere Wahl der logischen Axiome.

Wir sagen, daß $\{\alpha_1, \ldots, \alpha_n\}$ die Formel β tautologisch impliziert gdw die Formel $\alpha_1 \to \alpha_2 \to \cdots \to \alpha_n \to \beta$ eine Tautologie ist. Erinnern Sie sich daran, daß $\alpha_1 \to \alpha_2 \to \cdots \to \alpha_n \to \beta$ nach unseren Klammerunterdrückungsregeln für $(\bigwedge_{1 \leq i \leq n} \alpha_i) \to \beta$ steht.

Lemma 4.1. *(Metasatz über die Tautologische Implikation) Wenn* Γ *die Formeln* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *beweist, und* $\{\alpha_1, \ldots, \alpha_n\}$ *die Formel* β *tautologisch impliziert, dann beweist* Γ *auch* β.

Beweis: Da die Formel $\alpha_1 \to \alpha_2 \to \cdots \to \alpha_n \to \beta$ eine Tautologie ist, ist sie ein logisches Axiom und somit aus Γ beweisbar. Wir können nun den modus ponens n Mal anwenden, um zu zeigen, daß Γ die Formel β beweist. □

Lemma 4.2. *(Deduktionsmetasatz) Wenn* $\Gamma \cup \{\gamma\}$ *die Formel* φ *beweist, dann beweist* Γ *auch die Formel* $(\gamma \to \varphi)$.

Beweis: Wir zeigen durch Induktion über die kürzeste Länge eines Beweises von φ aus $\Gamma \cup \{\gamma\}$, daß $(\gamma \to \varphi)$ aus Γ beweisbar ist.

Fall 1: $\varphi = \gamma$. Dann beweist Γ offensichtlich $(\gamma \to \varphi)$, da $\gamma \to \gamma$ eine Tautologie ist.

Fall 2: φ ist ein logisches Axiom oder ein Element von Γ. Dann beweist schon Γ alleine die Formel φ. Und $\{\varphi\}$ impliziert tautologisch $(\gamma \to \varphi)$. Es folgt aus der tautologischen Implikation, daß Γ die Formel $(\gamma \to \varphi)$ beweist.

Fall 3: φ entsteht durch modus ponens aus ψ und $\psi \to \varphi$. Nach Induktionsannahme beweist Γ dann die Formeln $(\gamma \to \psi)$ und $(\gamma \to (\psi \to \varphi))$. Aus dem Lemma über die tautologischen Implikation folgt nun, daß Γ die Formel $(\gamma \to \varphi)$ beweist. □

Lemma 4.3. *Reductio ad absurdum, Widerspruchsbeweis, RAA. Wenn* $\Gamma \cup \{\varphi\}$ *nicht konsistent ist, dann beweist* Γ *die Formel* $\sim \varphi$.

Beweis: Nach Annahme gibt es eine Formel β, so daß $\Gamma \cup \{\varphi\}$ sowohl β als auch $(\sim \beta)$ beweist. Mit dem Deduktionsmetasatz erhalten wir, daß Γ sowohl $(\varphi \to \beta)$ als auch $(\varphi \to \sim \beta)$ beweist. Es folgt aus der tautologischen Implikation, daß Γ die Formel $(\sim \varphi)$ beweist.

Viele einzelne Beweisschritte verstecken sich hinter dem vorigen deutschen Satz: Aus $(\varphi \to \beta)$ beweist man mit einer Tautologie und MP $(\sim \beta \to \sim \varphi)$. Aus $(\varphi \to \sim \beta)$ beweist man mit einer Tautologie und MP $(\sim\sim \beta \to \sim \varphi)$. Hieraus erhält man mit MP $(\sim \beta \to \sim \varphi) \wedge (\sim\sim \beta \to \sim \varphi)$. Außerdem ist $(\sim \beta \vee \sim\sim \beta)$ eine Tautologie. MP gibt nun $(\sim \varphi)$. □

LEMMA 4.4. *(Erste Regel über die Verallgemeinerung). Wenn Γ die Formel φ beweist, und x in keiner Formel von Γ frei auftritt, dann beweist Γ die Formel $\forall x \varphi$.*

Beweis. Wir zeigen durch Induktion über die kürzeste Länge eines Beweises von φ aus Γ, daß Γ die Formel $\forall x \varphi$ beweist.

Fall 1: φ ist ein logisches Axiom. Dann ist $\forall x \varphi$ auch ein logisches Axiom und somit beweist Γ die Formel $\forall x \varphi$. Wir haben aber vereinbart, daß alle Verallgemeinerungen logischer Axiome wieder logische Axiome sind.

Fall 2: $\varphi \in \Gamma$. Dann tritt x nicht frei in φ auf. Deshalb ist $(\varphi \to \forall x \varphi)$ ein Axiom der Gruppe 3. Somit beweist Γ sowohl φ als auch $(\varphi \to \forall x \varphi)$. Also beweist Γ auch $\forall x \varphi$.

Fall 3: φ entsteht via modus ponens aus ψ und $\psi \to \varphi$. Jedoch gehört folgende Formel zu Axiomengruppe 3:

$$\forall x(\psi \to \varphi) \to (\forall x \psi \to \forall x \varphi).$$

Aus der Induktionsvoraussetzung erhalten wir $\Gamma \vdash \forall x \psi$ und $\Gamma \vdash \forall x(\psi \to \varphi)$. Aus der doppelten Anwendung des modus ponens erhalten wir einen Beweis von $\forall x \varphi$ aus Γ. □

LEMMA 4.5. *Fakten über die Ersetzung.*

(a) *x kann in jeder Formel für sich selbst eingesetzt werden.*

(b) *t kann in φ für x eingesetzt werden, wenn keine Variable von φ in t auftritt.*

(c) *Wenn x, y Variablen sind und y nicht in φ auftritt, dann kann x in φ^x_y für y eingesetzt werden, und es gilt $(\varphi^x_y)^y_x = \varphi$ (x wird zu y und dann wieder zu x).*

(d) *Wenn x, y, z Variablen sind und $x \neq z$ ist und t für x in φ eingesetzt werden kann, dann kann t für x in φ^y_z eingesetzt werden.*

(e) *Wir nehmen an, daß t für x in φ eingesetzt werden könne, y ein Variable sei, die nicht in φ auftrete, und c ein Konstantensymbol sei. Der Term*

t^c_y und die Formel φ^c_y entstehen dadurch, daß wir in t und φ c durch y ersetzen. Dann kann in φ^c_y t^c_y für x eingesetzt werden.

Beweis: **Übung**

LEMMA 4.6. *Zweite Regel über die Verallgemeinerung. Wenn Γ die Formel φ beweist und c ein Konstantensymbol ist, das nicht in Γ auftritt, dann gibt es eine Variable y, die in φ nicht auftritt, so daß Γ die Formel $\forall y \varphi^c_y$ beweist.*

Beweis: Induktiv über den Aufbau eines Beweises von φ aus Γ. Beim Induktionsschritt: modus ponens.

LEMMA 4.7. *Dritte Regel über die Verallgemeinerung. Wenn Γ die Formel φ^x_c beweist und c ein Konstantensymbol ist, das weder in Γ noch in φ auftritt, dann beweist Γ die Formel $\forall x \varphi$, und es gibt eine Ableitung hierfür, in der c nicht auftritt.*

Beweis: Vom vorigen Lemma haben wir eine Ableitung von $\forall y((\varphi^x_c)^c_y)$ aus Γ, in der c nicht auftritt, wenn y neu ist. Aber da c nicht in φ auftritt, haben wir auch

$$((\varphi^x_c)^c_y) = \varphi^x_y.$$

Es bleibt zu zeigen, daß $\forall y \varphi^x_y \vdash \forall x \varphi$. Dies folgt, wenn man weiß, daß $\forall y \varphi^x_y \to \varphi$ ein Axiom ist. Dies folgt aus $(\varphi^x_y)^y_x = \varphi$ und den Ersetzungsaxiomen in Gruppe 2. □

LEMMA 4.8. *Metasatz über die Umbenennung von Variablen. Wenn φ eine Formel, t ein Term und x eine Variable ist, dann gibt es eine Formel φ' so daß*

(a) *t für x in φ' eingesetzt werden kann, und*

(b) *$\varphi \to \varphi'$ und $\varphi' \to \varphi$ beweisbar sind.*

Beweis: **Übung**

Als allerletzte Vorbereitung brauchen wir

LEMMA 4.9. *Fakten über die Gleichheit.*

(a) *Die Formel $\forall x(x = x)$ ist beweisbar.*

(b) *Die Formel $\forall x \forall y(x = y \to y = x)$ ist beweisbar.*

(c) *Die Formel $\forall x \forall y \forall z(x = y \to y = z \to x = z)$ ist beweisbar.*

(d) *Für jedes zweistellige Relationssymbol P ist die Formel $\forall x_1 \forall x_2 \forall y_1 \forall y_2(x_1 = x_2 \to y_1 = y_2 \to P x_1 x_2 \to P y_1 y_2)$ beweisbar. Analoges gilt für n-stellige Prädikatssymbole.*

(e) *Für jedes zweistellige Funktionssymbol f ist die Formel $\forall x_1 \forall x_2 \forall y_1 \forall y_2(x_1 = x_2 \to y_1 = y_2 \to f x_1 x_2 = f y_1 y_2)$ beweisbar. Analoges gilt für n-stellige Funktionssymbole.*

Beweis: **Übung**

2. Der eigentliche Beweis

Satz 4.10. **Der Gödelsche Vollständigkeitssatz**

(a) *Jede konsistente Formelmenge ist erfüllbar.*

(b) *Wenn* $\Gamma \models \varphi$, *dann* $\Gamma \vdash \varphi$

Beweis: Es genügt, (a) zu beweisen, denn aus (a) erhält man (b) wie folgt: Impliziere Γ die Formel φ logisch. Wir möchten zeigen, daß Γ φ auch beweist. Wenn $\Gamma \cup \{\sim \varphi\}$ inkonsistent ist, dann beweist Γ die Formel $\sim\sim \varphi$ durch reductio ad absurdum, und deshalb beweist Γ φ durch tautologische Implikation, wie gewünscht. Daher können wir annehmen, daß $\Gamma \cup \{\sim \varphi\}$ konsistent ist. Dann ist nach (a) dieses auch erfüllbar. Dies widerspricht unserer Annahme, daß Γ die Formel φ logisch impliziert.

Nun beweisen wir (a). Sei Γ konsistent. Dann definieren wir eine neue Formelmenge Δ in einer um die Konstantensymbole $c_0, c_1 \dots$ erweiterten Sprache, so daß folgendes gilt:

(i) $\Gamma \subseteq \Delta$,

(ii) Δ ist in der erweiterten Sprache maximalkonsistent, d.h. für alle $\varphi \in \mathscr{L}(\tau \cup \{c_i \mid i \in \mathbb{N}\})$ ist $\varphi \in \Delta$ oder ist $\sim \varphi \in \Delta$.

(iii) Δ ist eine Henkin-Menge, d.h. für jede Formel φ und jede Variable x gibt es eine Konstante c, so daß die Formel $(\sim \forall x\varphi \rightarrow\sim \varphi^x_c)$ ein Element von Δ ist.

Danach konstruieren wir aus Δ eine Struktur $\mathfrak{A}$ und eine Belegung s, so daß $(\mathfrak{A}, s)$ φ erfüllt.

Wir beschreiben nun die Definition von Δ, die sich in abzählbar viele Erweiterungen der ersten Art und eine Erweiterung der zweiten Art zergliedert. Für jede Formel der Sprache $\mathscr{L} = \mathscr{L}_0$ und jede Variable x wählen wir ein neues Konstantensymbol c^x_φ, das wir zu $\mathscr{L}$ hinzufügen, und erhalten so die Sprache $\mathscr{L}_1$. Dann erweitern wir Γ für alle $\varphi \in \mathscr{L}$ und alle Variablen x um die Formel $(\sim \forall x\varphi \rightarrow\sim \varphi^x_{c^x_\varphi})$ und erhalten so Γ_1.

Behauptung 4.11. Γ_1 *ist konsistent.*

Beweis: Annahme: Γ_1 wäre widerspruchsvoll. Wir denken uns Γ_1 schrittweise aus Γ aufgebaut, und nehmen die minimale Schrittzahl, so daß $\Gamma \cup \{\psi_0, \dots, \psi_n, \psi_{n+1}\}$ widerspruchsvoll ist. Dann folgt nach RAA: $\Gamma \cup \{\psi_0, \dots, \psi_n\} \vdash\sim \psi_{n+1}$. ψ_{n+1} ist von der Form $(\sim \forall x\varphi \rightarrow\sim \varphi^x_{c^x_\varphi})$. Also ist $\sim \psi_{n+1} =\sim \forall x\varphi \wedge \varphi^x_{c^x_\varphi}$. Wir haben daher $\Gamma \cup \{\psi_0, \dots, \psi_n\} \vdash\sim \forall x\varphi$ und $\Gamma \cup \{\psi_0, \dots, \psi_n\} \vdash \varphi^x_{c^x_\varphi}$.

Aus letzterem erhalten wir mit dem Lemma 4.7 (der dritten Regel über die Verallgemeinerung) $\Gamma \cup \{\psi_0, \dots, \psi_n\} \vdash \forall x\varphi$. Nun ist also schon $\Gamma \cup \{\psi_0, \dots, \psi_n\}$ widerspruchsvoll, im Widerspruch zur Minimalität. □

Jetzt wiederholen wir diese Konstruktion, und erhalten aus der Sprache $\mathscr{L}_1$ die Sprache $\mathscr{L}_2$ und die Formelmenge Γ_2, so daß Γ_2 alle Formeln der Form $(\sim$

$\forall\varphi \to\sim \varphi^x_{c^x_\varphi}$) enthält, für jede Formel φ, die in $\mathscr{L}_1$, aber nicht in $\mathscr{L}_0$ ausgedrückt werden kann. Dann folgt wieder aus der Behauptung 4.11, daß die Konsistenz von Γ_1 jene von Γ_2 impliziert. Durch wiederholte Erweiterungen dieser Art erhalten wir eine Kette $\Gamma \subseteq \Gamma_1 \subseteq \Gamma_2 \ldots$ in den Spachen $\mathscr{L} \subseteq \mathscr{L}_1 \subseteq \mathscr{L}_2 \ldots$. Schließlich definieren wir $\Gamma^* = \bigcup\{\Gamma_n \mid n \in \mathbb{N}\}$ und $\mathscr{L}^* = \bigcup\{\mathscr{L}_n \mid n \in \mathbb{N}\}$. Eine aufsteigende Vereinigung von widerspruchsfreien Mengen ist widerspruchsfrei, da man für einen Widerspruch nur endlich viel Elemente braucht.

Behauptung 4.12. Γ^* *ist Teilmenge einer maximalkonsistenten Formelmenge* Δ *in der Sprache* $\mathscr{L}^*$. Δ *ist ebenfalls eine Henkin-Menge, da Erweiterungen von Henkin-Mengen in derselben Sprache Henkin-Mengen bleiben.*

Wir beweisen die Behauptung hier nur für den Fall eine abzählbaren Formelmenge Γ. Die Behauptung für überabzählbare Γ ist auch richtig, doch hierzu braucht man überabzählbar lange Auflistungen, und das heißt überabzählbare Ordinalzahlen.

Behauptung 4.13. *Jede konsistente Formelmenge* Γ *in einer abzählbaren Sprache* $\mathscr{L}$ *kann zu einer maximalkonsistenten Formelmenge* Δ *erweitert werden.*

Beweis Sei $\varphi_0, \varphi_1 \ldots$ eine Liste der Formeln der Sprache $\mathscr{L}$. Wir definieren ψ_n per Induktion über n. Wenn $\Gamma \cup \{\psi_0, \ldots, \psi_{n-1}\} \cup \{\varphi_n\}$ konsistent ist, dann setzen wir $\psi_n = \varphi_n$. Sonst beweist $\Gamma \cup \{\psi_0, \ldots, \psi_{n-1}\}$ die Formel $\sim \varphi_n$ und wir definieren $\psi_n =\sim \varphi_n$. Induktiv über n zeigt man nun, daß $\Gamma \cup \{\psi_0, \ldots, \psi_n\}$ konsistent ist. Daher ist $\Gamma \cup \{\psi_i \mid i < \omega\}$ konsistent. Da für jede Formel φ oder $\sim \varphi$ zu Δ gehört, ist Δ maximalkonsistent, wie gewünscht. □

Somit sind nun (i), (ii) und (iii) unseres Beweisplanes erreicht. Wir definieren nun die Struktur $\mathfrak{A}$ wie folgt: Sei $\mathcal{T}$ die Menge der $\mathscr{L}^*$-Terme. Wir schreiben $t \approx t_2$ und sagen, daß t_1 und t_2 äquivalent sind, wenn die Formel $t_1 = t_2$ in Δ ist.

Behauptung 4.14. $\approx$ *ist eine Äquivalenzrelation.*

Beweis: Dies folgt aus den Fakten über die Gleichheit (a), (b), (c) und Einsetzen der Terme für x, y, z. Falls dies verboten sein sollte, nimmt man zuerst andere Variablennamen anstelle von x, y, z, die nicht in den fraglichen Termen vorkommen. □

Nun schreiben wir $[t]$ für die Äquivalenzklasse von t. Das Universum von $\mathfrak{A}$ ist die Menge $\mathcal{T}/\approx$ all dieser Äquivalenzklassen. Nun sei

(a) Für jedes n-stelliges Prädikatssymbol P

$$P^{\mathfrak{A}} = \{\langle [t_1], \ldots, [t_n]\rangle \mid Pt_1 \ldots t_n \in \Delta\}.$$

(b) Für jedes n-stelliges Funktionssymbol f

$$f^{\mathfrak{A}}([t_1], \ldots, [t_n]) = [ft_1 \ldots t_n].$$

(c) Für jedes Konstantensymbol c ist $c^{\mathfrak{A}} = [c]$.

Behauptung 4.15. *$P^{\mathfrak{A}}$ und $f^{\mathfrak{A}}$ sind wohldefiniert. Wenn für $i < n$, $[t_i] = [t'_i]$, dann gehört $Pt_0 \ldots t_{n-1}$ zu Δ gdw $Pt'_0 \ldots t'_{n-1}$ zu Δ gehört. $[ft_0 \ldots t_{n-1}] = [ft'_0 \ldots t'_{n-1}] \in \Delta$.*

Beweis: Die Wohldefiniertheit folgt aus den Teilen (d) und (e) des Lemmas über die Fakten über die Gleichheit. Wenn $[t_i] = [t'_i]$, dann ist $t_i = t'_i \in \Delta$. Daher ist wieder nach den Fakten über die Gleichheit und der Abgeschlossenheit von Δ unter $\vdash$ (Δ ist ja maximal widerspruchsfrei) auch $(Pt_0 \ldots t_{n-1} \leftrightarrow Pt'_0 \ldots t'_{n-1})$ in Δ gehört. Hieraus folgt dann, daß $Pt_0 \ldots t_{n-1}$ zu Δ gehört gdw $Pt'_0 \ldots t'_{n-1}$ zu Δ gehört. Wenn für alle i $t_i = t'_i \in \Delta$, dann ist nach selben Argumenten auch $ft_0 \ldots t_{n-1} = ft'_0 \ldots t'_{n-1} \in \Delta$. $\square$

Die $\mathfrak{A}$-Belegung s ist definiert durch $s(x) = [x]$ für jede Variable x.

Behauptung 4.16. *$(\mathfrak{A}, s) \models \varphi$ gdw $\varphi \in \Delta$.*

Beweis: Wir verwenden die erste Regel über die Verallgemeinerung, den Metasatz über die tautologische Implikation, das Ersetzungslemma, die Eigenschaften einer maximalkonsistenten Henkin-Menge und den Metasatz über die Umbenennung von Variablen.

Zuerst beachten wir, daß für jedes Term t die Gleichheit $\bar{s}(t) = [t]$ gilt. Dies beweisen wir durch Induktion über den Aufbau von t: Wenn t eine Variable oder ein Konstantensymbol ist, dann folgt dies aus der Definition von s. Wenn t von der Form $ft_1, \ldots t_n$ ist dann haben wir $\bar{s}(t) = f^{\mathfrak{A}}(\bar{s}(t_1), \ldots, \bar{s}(t_n))$, das nach Induktionsannahme gleich $f^{\mathfrak{A}}([t_1], \ldots [t_n])$ ist. Letzteres ist nach Definition von $f^{\mathfrak{A}}$ gleich $[t]$.

Wir beweisen nun die zentrale Behauptung der Induktion über den Aufbau von φ. φ sei atomar. Wenn φ die Formel $t_1 = t_2$ ist, dann haben wir $\mathfrak{A} \models \varphi[s]$ gdw $\bar{s}(t_1) = \bar{s}(t_2)$ gdw $[t_1] = [t_2]$ gdw $t_1 = t_2 \in \Delta$. Wenn φ die Formel $Pt_1 \ldots t_n$ ist, dann $\mathfrak{A} \models \varphi[s]$ gdw $\langle \bar{s}(t_1), \ldots, \bar{s}(t_n) \rangle) \in P^{\mathfrak{A}}$ gdw $\langle [t_1], \ldots, [t_n] \rangle \in P^{\mathfrak{A}}$ gdw $Pt_1 \ldots t_n \in \Delta$. Der letzte Schritt verwendete die Definition von $P^{\mathfrak{A}}$.

$\varphi = \sim \psi$. Wir haben $(\mathfrak{A}, s) \models \varphi$ gdw $(\mathfrak{A}, s) \not\models \psi$ gdw $\psi \notin \Delta$ gdw $\varphi \in \Delta$. Der letzte Schritt verwendete die Maximalkonsistenz von Δ.

$\varphi = (\psi \to \gamma)$. Wir haben $\mathfrak{A} \models (\psi \to \gamma)[s]$ gdw ($\mathfrak{A} \not\models \psi[s]$ oder $\mathfrak{A} \models \gamma[s]$) gdw ($\psi \notin \Delta$ oder $\gamma \in \Delta$) gdw ($\sim \psi \in \Delta$ oder $\gamma \in \Delta$). Letzteres impliziert wegen der Maximalität von Δ, daß $(\psi \to \gamma) \in \Delta$. Sei umgekehrt $(\psi \to \gamma) \in \Delta$. Dann können wegen der Konsistenz von Δ nicht sowohl ψ als auch $\sim \gamma$ zu Δ gehören. Wegen der Maximalkonsistenz von Δ erhalten wie daher $\sim \psi \in \Delta$ oder $\gamma \in \Delta$.

$\varphi = \forall x\psi$. Zu zeigen ist $\mathfrak{A} \models \forall x\psi([s])$ gdw $\forall x\psi \in \Delta$. Erfülle $\mathfrak{A}$ die Formel $\forall x\psi$ mit s. Wir wählen ein Konstantensymbol c, so daß das Axiom $(\sim \forall x\psi \rightarrow \sim \psi^x_c)$ zu Δ gehört. Dies ist möglich, da Δ eine Henkin-Menge ist. Nach Annahme gilt $\mathfrak{A} \models \psi[s(x|[c])]$ und $[c] = \bar{s}(c)$. Nach Ersetzungslemma ist $\mathfrak{A} \models \psi^x_c[s]$. Nach Induktionsannahme ist $\psi^x_c \in \Delta$ und deshalb $\sim \forall x\psi \notin \Delta$ wegen des obigen Henkinaxioms. Weil Δ maximal konsistent ist, ist daher $\forall x\psi \in \Delta$.

Nun nehmen wir an, daß $\mathfrak{A} \not\models \forall x\psi[s]$. Dann gibt es einen Term t, so daß $\mathfrak{A} \not\models \psi[s(x|[t])]$ und $[t] = \bar{s}(t)$. Wir möchten nun mithilfe des Ersetzungslemmas folgern, daß $\mathfrak{A} \not\models \psi^x_t[s]$. Das Problem ist aber, daß wir nicht wissen, ob das Ersetzungslemma anwendbar ist, da nicht klar ist, ob t für x in ψ eingesetzt werden kann. Mit dem Metasatz zu Umbenennung von Variablen können wir eine Formel ψ' wählen, so daß $\psi \vdash \psi' \vdash \psi$ und so daß in ψ' t für x eingesetzt werden kann. Nach der ersten Verallgemeinerungsregel haben wir $\forall x\psi \vdash \forall x\psi'$, da $\forall x\psi$ die Formel ψ und ψ die Formel ψ' beweist. Wir haben:

$\mathfrak{A} \not\models \psi[s(x|[t])]$ nach Voraussetzung. Da ψ und ψ' logisch äquivalent sind, ist $\mathfrak{A} \not\models \psi'[s(x|[t])]$. Nach dem Ersetzungslemma folgt hieraus $\mathfrak{A} \not\models (\psi')^x_t[s]$. Dann ist nach Induktionsannahme $(\psi')^x_t \notin \Delta$. Da $\forall x\psi' \rightarrow (\psi')^x_t$ ein logisches Axiom und Δ abgeschlossen unter beweisbarer Implikation ist, haben wir daher $\forall x\psi' \notin \Delta$. Da $\forall x\psi \vdash \forall x\psi'$, ist $\forall x\psi \notin \Delta$. $\square$

KAPITEL 5

Korollare zum Vollständigkeitssatz

Der Vollständigkeitssatz hat wichtige Folgen für die Relation $\models$ der logischen Implikation und für die Größe von Modellen von Theorien in der Sprache erster Stufe.

SATZ 5.1. *Der Kompaktheitssatz.*

(a) *Wenn jede endliche Teilmenge von Γ erfüllbar ist, dann ist auch Γ erfüllbar.*

(b) *Wenn Γ die Formel φ logisch impliziert, dann gibt es ein endliches $\Gamma_0 \subseteq \Gamma$, so daß Γ_0 die Formel φ impliziert.*

Beweis. (a) Wegen des Vollständigkeitssatzes sind Erfüllbarkeit und Konsistenz gleichwertig. Deshalb genügt es, (a) für „konsistent" statt „erfüllbar" zu beweisen. Wenn jede endliche Teilmenge von Γ konsistent ist, dann ist auch Γ konsistent, da ein Widerspruchsbeweis aus Γ nur eine endliche Teilmenge von Γ verwenden würde.

(b) Der Vollständigkeitssatz impliziert, daß die Relationen $\vdash$ (beweist) und $\models$ (impliziert logisch) gleichwertig sind. Deshalb genügt es, (b) für die Relation $\vdash$ zu beweisen. Wenn Γ die Formel φ beweist, dann gibt ein einen endlichen Beweis von φ aus Γ. Sei Γ_0 die endliche Menge von Formeln aus Γ, die im Beweis verwendet werden. Dann beweist Γ_0 φ. □

Ein Beispiel für eine Anwendung des Kompaktheitssatzes: Ein Modell einer Satzmenge Γ ist eine Struktur $\mathfrak{A}$, in der jeder Satz aus Γ wahr ist. Da Γ nur Sätze enthält, brauchen wir keine Belegung. Der Kompaktheitssatz impliziert, daß es keine Satzmenge gibt, deren Modelle genau die Strukturen mit endlichen Universum sind: Wenn Γ eine solche Satzmenge wäre und für n der Satz φ_n sagt, daß es mindestens n Elemente im Universum gibt, dann wäre die Menge $\Gamma^* = \Gamma \cup \{\varphi_n \mid n < \omega\}$ endlich erfüllbar. („Γ ist endlich erfüllbar" ist ein Jargon-Ausdruck, und heißt korrekt: „jede endliche Teilmenge von Γ ist erfüllbar".) Nach dem Kompaktheitssatz hat Γ^* ein Modell. Diese ist auch ein Modell von Γ und hat natürlich ein unendliches Universum.

Unsere nächste Anwendung des Vollständigkeitssatzes verwendet die informalen Begriffe „Entscheidbarkeit" und „effektive Aufzählbarkeit". Eine Sprache erster Stufe heißt „effektiv" gdw wenn die Menge ihrer nichtlogischen Symbole abzählbar ist und darüber hinaus die drei Relationen

$$\{(P,n) \mid P \text{ ist ein } n\text{-stelliges Prädikatssymbol}\}$$

$$\{(f,n) \mid f \text{ ist ein } n\text{-stelliges Funktionssymbol}\}$$

$$\{c \mid c \text{ ist ein Konstantensymbol}\}.$$

„entscheidbar" sind. Zum Beispiel ist jede Sprache mit nur endlich vielen nichtlogischen Symbolen effektiv. Das Teilgebiet er mathematischen Logik, das Rekursiontheorie oder auch Berechenbarkeitstheorie genannt wird, gibt eine exakte Definition der Begriffe „Entscheidbarkeit" und „effektive Aufzählbarkeit" und erforscht diese und weitere Begriffe über Algorithmen.

Satz 5.2. *Aufzählbarkeitssatz. Sei* Γ *eine entscheidbare Formelmenge in einer effektiven Sprache. Dann ist die Menge der logischen Implikationen aus* Γ $\{\varphi \mid \Gamma \models \varphi\}$ *effektiv aufzählbar.*

Beweis. Weil die Sprache effektiv ist, sind die Menge der Formel die Menge A der logischen Axiome und die Menge der endlichen Beweise aus Γ entscheidbar. Somit können wir eine effektive Liste der logischen Implikationen aus Γ herstellen, indem wir die Menge der Beweise aus Γ aufzählen und die letzte Formel jedes Beweises in unsere effektive Aufzählung aufnehmen. $\square$

Eine Theorie ist eine Satzmenge Γ. Genauer: Eine τ-Theorie oder auch $\mathscr{L}(\tau)$-Theorie ist eine Satzmenge in $\mathscr{L}(\tau)$. Dies könnte man natürlich auch für andere Logiken als die Logik $\mathscr{L}$ erster Stufe betrachten, und dieses Spezialgebiet heißt allgemeine Modelltheorie (abstract model theory).

Definition 5.3. Γ *heißt vollständig in* $\mathscr{L}(\tau)$ *gdw für jeden Satz* $\varphi \in \mathscr{L}(\tau)$ *gilt:* $\Gamma \models \varphi$ *oder* $\Gamma \models \sim \varphi$.

Die meisten konsistenten Theorien sind nicht vollständig! Ohne Beweis geben wir hier Beispiele für vollständige Theorien:

1. In the Sprache $\mathscr{L}(\emptyset)$: die Theorie der unendlichen Mengen.

2. In der Sprache $\mathscr{L}(<)$: die Theorie der dichten offenen linearen Ordnungen.

3. In der Sprache $\mathscr{L}(+,\cdot)$: die Theorie der algebraisch abgeschlossenen Körper einer festen Charakteristik.

Definition 5.4. *Sei* $\mathfrak{M}$ *eine* τ*-Struktur.* $Th(\mathfrak{M}) = \{\varphi \in \mathscr{L}(\tau) \mid \varphi$ *Satz und* $\mathfrak{M} \models \varphi\}$ *heißt die Theorie von* $\mathfrak{M}$ *(in der Sprache erster Stufe).*

4. Die Theorie jeder τ-Struktur $\mathfrak{M}$ ist vollständig. (Genau dann, wenn $\mathfrak{M}$ endlich ist, beschreibt die Theorie von $\mathfrak{M}$ bis auf Isomorphie eindeutig, d.h., alle Elemente von $\mathrm{Mod}(Th(\mathfrak{M})) = \{\mathfrak{N} \mid \mathfrak{N} \models Th(\mathfrak{M})\}$ sind zu $\mathfrak{M}$ isomorph. Falls zusätzlich τ endlich ist, ist diese Theorie sogar endlich axiomatisierbar.)

Korollar 5.5. *Sei* Γ *eine entscheidbare Satzmenge einer effektiven Sprache. Sei* Γ *vollständig. Dann ist die Menge der Folgerungen aus* Γ *entscheidbar.*

Beweis: Nach dem Aufzählbarkeitssatz sind sowohl diese Menge als auch ihr Komplement (die Menge der Formeln φ, daß Γ die Formel $\sim \varphi$ beweist) effektiv aufzählbar. Jede effektiv aufzählbare Menge, die ein effektiv auszählbares Komplement hat, ist aber entscheidbar mit folgendem Verfahren: Wir können schrittweise abwechselnd die Menge und auch ihr Komplement aufzählen und darauf warten, daß ein gegebener Satz in einer der zwei Aufzählungen auftritt. □

Unsere dritte Anwendung des Vollständigkeitssatzes betrifft die Größe (Mächtigkeit) von Modellen. Eine Struktur heißt abzählbar gdw ihr Universum abzählbar ist.

Satz 5.6. *Satz von Löwenheim und Skolem, Spezialfall für abzählbare Sprachen. Sei Γ eine konsistente Menge von Sätzen in einer abzählbaren Sprache. Dann hat Γ ein abzählbares Modell. Wenn Γ ein unendliches Modell hat, dann hat Γ auch ein überabzählbares Modell.*

Beweis. Des Beweis des Vollständigkeitssatzes zeigt, daß jede konsistente Satzmenge in einer abzählbaren Sprache ein abzählbares Modell hat.

Nun nehmen wir an, daß $\mathfrak{A}$ ein unendliches Modell von Γ ist. Wir nehmen eine überabzählbare Menge neuer Konstantensymbole $\{c_i \mid i < \aleph_1\}$ und erweitern Γ, indem wir für je zwei neue ungleiche Konstantensymbole c_i und c_j den Satz $c_i \neq c_j$ zu Γ hinzufügen.

Wir nennen diese erweiterte Satzmenge Γ^*. Jede endliche Teilmenge Γ_0^* von Γ^* ist erfüllbar, denn wir können in $\mathfrak{A}$ die endlich vielen in Γ_0^* vorkommenden c_i durch endlich viele verschiedene Punkte interpretieren und so ein Modell für Γ_0^* erhalten. Nach der Version des Vollständigkeitssatzes für überabzählbare Formelmengen (– wenn Sie mißtrauisch sind, da in der Vorlesung nur die abzählbare Version bewiesen wurde, machen Sie die Aufgaben auf Blatt 7 –) hat Γ^* ein Modell $\mathfrak{B}^* = (\mathfrak{B}, (c_i^{\mathfrak{B}^*})_{i<\aleph_1})$. Wenn wir die nun $\mathfrak{B}^*$ auf die Sprache τ beschränken, dann haben wir ein überabzählbares Modell $\mathfrak{B}$ von Γ. □

Der Satz von Löwenheim und Skolem hat überrraschende Konsequenzen. Zum Beispiel haben die natürlichen Axiome für die Struktur $\mathfrak{N} = (\mathbb{N}, 0, 1, +, \cdot)$ der Arithmetik auch ein überabzählbares Modell. Wenn wir hingegen in einer abzählbaren Sprache Axiome für eine große Struktur wie das Mengenuniversum hinschreiben, dann haben unsere Axiome, wenn sie konsistent sind, notwendig ein abzählbares Modell (dieser Sachverhalt heißt das Skolemsche Paradoxon).

Diese Sachverhalte zeigen eine Schwäche der Sprache der ersten Stufe: Keine Axiomenmenge (auch nicht in einer überabzählbaren Symbolmenge) kann eine gegebene unendliche Struktur bis auf Isomorphie eindeutig charakterisieren.

KAPITEL 6

Der erste Unvollständigkeitssatz

Sei Γ eine entscheidbare Satzmenge in einer effektiven Sprache der ersten Stufe. Wir haben gesehen, daß die Menge der Sätze, die aus Γ logisch folgen, effektiv aufzählbar ist. Muß sie entscheidbar sein? In diesem Teil der Vorlesung beschreiben wir eine einfache, endliche Menge A_E von Sätzen in der Sprache der Arithmetik, und zeigen, daß die Menge der logischen Folgerungen aus jeder konsistenten Satzmenge, die A_E enthält, unentscheidbar ist. Als Korollar erhalten wir, daß keine entscheidbare konsistente Satzmenge, die A_E enthält, vollständig ist. Denn wir haben bewiesen (Satz von Janiczak), daß eine entscheidbare, vollständige Satzmenge eine entscheidbare Menge logischer Folgerungen hat. Das Korollar ist sehr wichtig und wird *Gödelscher Unvollständigkeitssatz* genannt.

Bei unseren Entscheidbarkeitsresultaten gaben wir uns mit einem intuitiven Begriff von Entscheidbarkeit zufrieden. Da wir aber nun Sätze über die Unentscheidbarkeit beweisen wollen, werden wir zuerst einen exakten, mathematischen Begriff von Entscheidbarkeit einführen. Dieser Begriff heißt „Rekursivität” und wird als nächstes definiert. Warnung: Es gibt etwa 10 Hauptarten von äquivalenten Definitionen für „Rekursivität”. Unsere Definition ist nicht gerade die gängigste.

Eine *Theorie* ist eine Menge von Sätzen in einer Sprache erster Stufe.

Definition 6.1. *Sei T eine Theorie in einer Sprache, die die Symbole* 0 *und S (für Null und die Nachfolgerfunktion $n \mapsto n+1$) enthält. Wir verwenden den Term S^n0 für die natürliche Zahl n und schreiben einfach n.*

(1) *Eine Formel φ* stellt *eine k-stellige Relation $R \subseteq \mathbb{N}^k$* in T dar *gdw für alle $n_1, ..., n_k \in \mathbb{N}$ folgendes gilt:*

$$(n_1, ..., n_k) \in R \quad \textit{gdw} \quad T \vdash \varphi(n_1, ..., n_k), \ \textit{und}$$
$$(n_1, ..., n_k) \notin R \quad \textit{gdw} \quad T \vdash \sim \varphi(n_1, ..., n_k).$$

(2) *R ist* darstellbar in T *gdw es eine Formel φ gibt, die R in T darstellt.*

Wir geben nun eine mathematische Definition für den Begriff der Entscheidbarkeit (=Rekursivität).

Definition 6.2. *Eine k-stellige Relation $R \subseteq N^k$ heißt* rekursiv*gdw R in einer endlichen Theorie darstellbar ist.*

Wir beachten, daß jede rekursive Relation entscheidbar ist, weil die Menge der logischen Folgerungen einer endlichen Theorie effektiv aufzählbar ist und deshalb sowohl R als auch $\sim R$ effektiv aufzählbar sind. Der Umkehrschluß, daß jede entscheidbare Relation auch rekursiv ist, wird *die Churchsche These* genannt und wird von den meisten Mathematikern gewöhnlich angenommen.

Das zentrale Hilfsmittel zum Beweis des Unvollständigkeitssatzes ist folgendes: Wir definieren eine endliche Theorie A_E, die einige der Eigenschaften des Standardmodells $\mathfrak{N} = (\mathbb{N}, 0, S, <, +, \cdot, E)$ der Arithmetik beschreibt. Wir zeigen, daß jede rekursive Relation tatsächlich in A_E darstellbar ist. Aus dieser Tatsache und einigen Lemmata erhalten wir recht einfach die gewünschte Ergebnisse über Unentscheidbarkeit und Unvollständigkeit.

DEFINITION 6.3. *Die Axiome von* A_E

S1. $\forall x(Sx \neq 0)$.
S2. $\forall x \forall y(Sx = Sy \rightarrow x = y)$.
L1. $\forall x \forall y(x < Sy \leftrightarrow x \leq y)$.
L2. $\forall x(x \not< 0)$.
L3. $\forall x \forall y(x < y \vee x = y \vee y < x)$.
A1. $\forall x(x + 0 = x)$.
A2. $\forall x \forall y(x + Sy = S(x + y))$.
M1. $\forall x(x \cdot 0 = 0)$.
M2. $\forall x \forall y(x \cdot Sy = x \cdot y + x)$.
E1. $\forall x(xE0 = S0)$.
E2. $\forall x \forall y(xESy = xEy \cdot x)$.

Jedes Axiom und somit jede Folgerung aus A_E ist im Standardmodell $\mathfrak{N}$ wahr. Jedoch ist nicht jeder Satz, der in $\mathfrak{N}$ wahr ist, eine Folgerung aus A_E. Für quantorenfreie Sätze gilt aber, daß sie in $\mathfrak{N}$ wahr sind gdw sie aus A_E bewiesen können.

1. Vollständig bestimmte Formeln

Der folgende Begriff ist oft nützlich, um zu zeigen, daß eine Relation R darstellbar in A_E ist:

DEFINITION 6.4. *Eine Formel φ mit freien Variablen aus $v_1, ..., v_k$ ist* (durch A_E) vollständig bestimmt *gdw für alle $n_1, ..., n_k \in \mathbb{N}$ entweder $\varphi(n_1, ..., n_k)$ oder $\sim \varphi(n_1, ..., n_k)$ beweisbar aus A_E ist.*

Es folgt, daß die durch φ definierte Relation $R = \{\langle n_1, ..., n_k\rangle \mid \mathfrak{N} \models \varphi(n_1, ..., n_k)\}$ darstellbar in A_E ist. Wir haben:

LEMMA 6.5. *(Das Bestimmbarkeitslemma).*

(a) *Jede atomare Formel ist vollständig bestimmt.*

(b) *Wenn φ und ψ vollständig bestimmt sind, dann sind auch $\sim \varphi$ und $\varphi \to \psi$ vollständig bestimmt.*

(c) *Wenn φ vollständig bestimmt ist, dann sind auch $\forall x(x < y \to \varphi)$ und $\exists x(x < y \wedge \varphi)$vollständig bestimmt.*

Beweis. (a) Wir beachten zuerst, daß $x \nless 0$ und $x < k+1 \leftrightarrow (x = 0 \vee x = 1 \vee \cdots \vee x = k)$ (für jedes k) beweisbar aus A_E sind. Ersteres gilt nach Axiom L2. Letzteres wird per Induktion über k bewiesen: Wenn $k = 0$, haben wir $x < 1 \leftrightarrow x \leq 0$ nach Axiom L1 und dann erhalten wir $x \leq 0 \leftrightarrow x = 0$ nach Axiom L2. Für den Induktionsschritt haben wir $x < k+1 \leftrightarrow x < k \vee x = k$ nach L1, und nach Induktionsannahme kann $x < k$ durch $x = 0 \vee \cdots \vee x = k-1$ ersetzt werden. Daraus folgt $x < k+1 \leftrightarrow (x = 0 \vee \cdots \vee x = k)$, wie gewünscht.

Als nächstes beachten wir, daß es für jeden Term t ohne Variable eine eindeutig bestimmte natürliche Zahl n gibt, so daß $A_E \vdash t = n$. Die Eindeutigkeit ist klar, da A_E nur wahre Sätzen beweisen kann. Nun zeigen wir per Induktion über t, daß es ein solches n gibt: Wenn t gleich 0 ist, dann ist das Ergebnis offensichtlich. Wenn t von der Form Su ist, dann erhalten wir nach Induktionsannahme n, so daß $A_E \vdash u = n$ und deshalb $A_E \vdash t = n+1$. Wenn t von der Form $u_1 + u_2$ ist, dann gibt es nach Induktionsannahme n_1 und n_2, so daß $A_E \vdash u_1 = n_1$ und $A_E \vdash u_2 = n_2$; durch eine n_2-malige Anwendung von Axiom A2 und Anwendung von Axiom A1 erhalten wir $A_E \vdash t = n_1 + n_2$. Ein ähnliches Argument gilt für Exponentiation und Multiplikation unter Verwendung von Axiomen M1, M2, E1 und E2.

Nun beweisen wir (a). Sei φ atomar von der Form $u_1 = u_2$. Sei $t_1 = t_2$ der Satz, der dadurch entsteht, daß wir die Variablen von φ durch Zahlen ersetzen. Wie wir oben gesehen haben, gibt es dann n_1 und n_2, so daß $A_E \vdash t_1 = n_1$ und $A_E \vdash t_2 = n_2$. Wenn $n_1 = n_2$, dann gilt offensichtlich $A_E \vdash t_1 = t_2$. Sonst müssen wir nur noch zeigen, daß $A_E \vdash n_1 \neq n_2$; wenn $n_1 < n_2$, folgt dies, indem wir Axiom S2 n_1 mal und Axiom S1 einmal anwenden. Daher ist φ vollständig bestimmt. Ein ähnliches Argument gilt, wenn φ von der Form $u_1 < u_2$ ist.

(b) Es ist klar, daß $\sim \varphi$ ist vollständig bestimmt gdw φ vollständig bestimmt ist. Und wenn φ und ψ vollständig bestimmt sind, dann beweist A_E den Satz $\sim (\varphi \to \psi)(n_1, ..., n_k)$ gdw A_E sowohl $\varphi(n_1, ..., n_k)$ als auch $\sim \psi(n_1, ..., n_k)$ beweist, anderenfalls beweist A_E den Satz $(\varphi \to \psi)(n_1, ..., n_k)$.

(c) Es genügt, den Fall $\exists x(x < y \wedge \varphi)$ zu betrachten, da $\forall x(x < y \to \varphi)$ äquivalent zu $\sim \exists x(x < y \wedge \sim \varphi)$ ist. Nehmen wir an, daß φ nur die freien Variablen x, y und z hat. Seien a und b natürliche Zahlen; wir müssen zeigen, daß A_E entweder $\exists x(x < a \wedge \varphi(x, a, b))$ oder $\sim \exists x(x < a \wedge \varphi(x, a, b))$ beweist. Wenn es ein $c < a$ gibt, so daß A_E $\varphi(c, a, b)$ beweist, dann beweist A_E auch den Satz $\exists x(x < a \wedge \varphi(x, a, b))$, da $A_E \vdash c < a$. Sonst beweist A_E den Satz $\sim \varphi(c, a, b)$ für jedes $c < a$ und somit den Satz $\forall x(x < a \to \sim \varphi(x, a, b))$ (nach dem ersten Teil des Beweises von (a)). Daher beweist A_E den Satz $\sim \exists x(x < a \wedge \varphi(x, a, b))$, wie gewünscht. □

2. Darstellbare Funktionen

Definition 6.6. *Eine Funktion* $f : \mathbb{N}^k \to \mathbb{N}$ *ist* (in A_E) durch φ darstellbar *gdw für alle* $n_1, ..., n_k$ *aus* $\mathbb{N}$*:*

$$A_E \vdash \forall x(\varphi(n_1, ..., n_k, x) \leftrightarrow x = f(n_1, ..., n_k)).$$

Dies ist der Form nach stärker als die Eigenschaft, daß der Graph von f als eine $k+1$-stellige Relation in A_E durch φ darstellbar ist. Doch wir sehen, daß beide Definitionen äquivalent sind:

Lemma 6.7. *Wenn der Graph von* f *in* A_E *darstellbar ist, dann ist* f *auch als Funktion in* A_E *darstellbar.*

Beweis. Wir nehmen an, daß f eine 1-stellige Funktion ist. Sei $\theta(x, y)$ eine Formel, die den Graphen von f darstellt. Deshalb haben wir für jedes n:

$$\begin{aligned} A_E &\vdash \theta(n, f(n)) \text{ und} \\ A_E &\vdash \sim\theta(n, m) \text{ für jedes } m \neq f(n). \end{aligned}$$

Nun definieren $\varphi(x, y)$ als

$$\theta(x, y) \wedge \forall z(z < y \to \sim\theta(x, z)).$$

Natürlich beweist A_E den Satz $\varphi(n, f(n))$ für jedes n, weil $\sim\theta(n, 0), \ldots, \sim\theta(n, f(n)-1)$ und $\theta(n, f(n))$ Folgerungen aus A_E sind. Nach Beweis des Bestimmbarkeitslemmas ist $\forall z(z < f(n) \leftrightarrow z = 0 \vee z = 1 \vee \cdots z = f(n) - 1)$ beweisbar aus A_E.

$$A_E \vdash \forall v_2(\varphi(n, v_2) \to v_2 = f(n)) \tag{1}$$

heißt nun also

$$A_E \vdash \forall v_2(\theta(n, v_2) \wedge \forall z(z < v_2 \to \sim\theta(n, z)) \to v_2 = f(n)) \tag{2}$$

Es genügt

$$A_E \cup \{\theta(n, v_2), \forall z(z < v_2 \to \sim\theta(n, z))\} \vdash v_2 = f(n) \tag{3}$$

zu zeigen. Nach Axiom L3 haben wir $A_E \vdash \forall z(z = 0 \vee \cdots \vee z = f(n) - 1 \vee z = f(n) \vee f(n) < z)$.

Wir nennen die Hypothesen zu Gleichung (3) Γ. Es genügt,

$$\Gamma \vdash v_2 \not< f(n) \tag{4}$$

und

$$\Gamma \vdash f(n) \not< v_2 \tag{5}$$

zu zeigen.

Das letztere folgt aus den beiden letzten Voraussetzungen in Γ, die nach Einsetzen von $f(n)$ für z sagen: $f(n) < v_2 \rightarrow \sim \theta(n, f(n))$. Dann bildet man die Kontraposition des letzteren.

Um die vorletzte Implikation (4) zu beweisen nehmen wir das Bestimmbarkeitslemma $v_2 < f(n) \leftrightarrow (v_2 = 0 \vee \cdots \vee v_2 = f(n) - 1)$, und

$$A_E \vdash \sim \theta(n, m) \text{ für } m = 0, \ldots, f(n) - 1. \tag{6}$$

Die Formeln geben

$$A_E \vdash v_2 < f(n) \rightarrow \sim \theta(n, v_2) \tag{7}$$

und daher impliziert $\theta(n, v_2)$ die Formel (4).

□

Definition 6.8. *Für jede Relation $R \subseteq \mathbb{N}^k$ definieren wir $\chi_R : \mathbb{N}^k \rightarrow \mathbb{N}$ wie folgt: $\chi_R(n_1, ..., n_k) = 1$ gdw $\langle n_1, ..., n_k \rangle \in R$, $\chi_R(n_1, ..., n_k) = 0$ gdw $\langle n_1, ..., n_k \rangle \notin R$. Die Funktion χ_R wird die* charakteristische Funktion von R *genannt.*

Eine nützliche Tatsache ist folgendes

Lemma 6.9. *R ist in A_E darstellbar gdw χ_R es ist.*

Beweis. Stelle $\varphi(x_1, ..., x_k, y)$ die Funktion χ_R in A_E dar. Dann stellt $\psi = \varphi(x_1, ..., x_k, 1)$ die Relation R dar, weil ψ vollständig bestimmt ist und R definiert.

Wenn umgekehrt $\varphi(x_1, ..., x_k)$ die Relation R darstellt, dann stellt die folgende Formel χ_R dar:

$$(\varphi(x_1, ..., x_k) \wedge y = 1) \vee (\sim \varphi(x_1, ..., x_k) \wedge y = 0).$$

Dies gilt, weil letzteres χ_R definiert und vollständig bestimmt ist. □

Manchmal werden die rekursiven Funktionen durch ein Aufbau-Schema definiert.

Definition 6.10. *Die Menge der* S-rekursiven *(Schema-rekursiven) Funktionen wird wie folgt definiert.*

1. *Die Nachfolgerfunktion $S(n) = n + 1$ ist S-rekursiv.*
2. *Die konstanten Funktionen $f(n_1, ..., n_k) = c$, $c \in \mathbb{N}$, sind S-rekursiv.*
3. *Die Projektionen $I_i^k(n_1, ..., n_k) = n_i$ sind S-rekursiv.*
4. *Addition, Multiplikation und Exponentiation sind S-rekursiv.*

5. *(Komposition) Wenn g eine n-stellige, S-rekursive Funktion und $h_1, \ldots, h_n$ k-stellige, S-rekursive Funktionen sind, dann ist die wie folgt definierte Funktion f S-rekursiv:*

$$f(n_1, ..., n_k) = g(h_1(n_1, ..., n_k), ..., h_n(n_1, ..., n_k)).$$

6. *(μ-Operator) Wenn g eine $k+1$-stellige, S-rekursive Funktion ist und für alle $n_1, \ldots, n_k$ es ein m gibt, so daß $g(n_1, ..., n_k, m) = 0$, dann ist die wie folgt definierte Funktion f S-rekursiv:*

$$f(n_1, ..., n_k) = \text{ das kleinste } m, \text{ so daß } g(n_1, ..., n_k, m) = 0.$$

Lemma 6.11. *S-Rekursionslemma. Jede S-rekursive Funktion ist in A_E darstellbar.*

Beweis. Für die Funktionen in 1.-4. können wir die folgenden Formeln verwenden:

1. $v_2 = Sv_1$.
2. $v_{k+1} = c$.
3. $v_{k+1} = v_i$.
4. $v_3 = v_1 + v_2$, $v_3 = v_1 \cdot v_2$, $v_3 = v_1 E v_2$.

Für die Komposition betrachten wir den Spezialfall $f(n) = g(h_1(n), h_2(n))$ und zeigen, daß f darstellbar in A_E ist, wenn g, h_1 und h_2 dies sind. Seien ψ, θ_1 und θ_2 Formeln, die g, h_1 und h_2 darstellen. Wir definieren:

$$\varphi(v_1, v_2) \leftrightarrow \exists y_1 \exists y_2 (\theta_1(v_1, y_1) \wedge \theta_2(v_1, y_2) \wedge \psi(y_1, y_2, v_2)).$$

Wir müssen zeigen: Für jedes n beweist A_E den Satz $\varphi(n, f(n))$, und für jedes $m \neq f(n)$ beweist A_E den Satz $\sim \varphi(n, m)$. Ersteres ist klar, da $A_E \vdash \theta_1(n, h_1(n)) \wedge \theta_2(n, h_2(n)) \wedge \psi(h_1(n), h_2(n), f(n))$, und daher können wir y_1 und y_2 als $h_1(n)$ und $h_2(n)$ nehmen. Für letzteres wissen wir, daß A_E den Satz $\sim \psi(h_1(n), h_2(n), m)$ beweist, wenn $m \neq f(n)$, und A_E den Satz $\forall y_i(\theta_i(n, y_i) \rightarrow y_i = h_i(n))$, $i = 1, 2$, beweist. Es folgt, daß $A_E \vdash \sim \varphi(n, m)$.

Für den μ-Operator zeigen wir: Wenn g darstellbar in A_E ist und f wie in 6. aus g definiert wird, dann ist auch f darstellbar in A_E. Sei g durch $\psi(v_1, ..., v_{k+2})$ in A_E dargestellt; wir definieren:

$$\varphi(v_1, ..., v_{k+1}) \leftrightarrow \psi(v_1, ..., v_k, v_{k+1}, 0) \wedge \forall y(y < v_{k+1} \rightarrow \sim \psi(v_1, ..., v_k, y, 0)).$$

φ ist dann vollständig bestimmt und definiert f als eine Relation im Standardmodell $\mathfrak{N}$. □

Schreibweisen: Für $f(n_1, ..., n_k)$ schreiben wir oft $f(\vec{n})$. Die durch 6. definierte Funktion f wird oft $f(\vec{n}) = \mu m(g(\vec{n}, m) = 0)$ geschrieben.

3. Eine Liste darstellbarer Funktionen und Relationen

Um den Beweis, daß jede rekursive Relation darstellbar in A_E ist, vorzubereiten, erstellen wir nun eine Liste nützlicher Funktionen und Relationen, deren Darstellbarkeit unter Verwendung des Bestimmbarkeitslemmas und des S-Rekursionslemmas gezeigt werden kann. In dieser Liste schreiben wir „darstellbar" für „darstellbar in A_E".

Lemma 6.12. *Die Relation* $\{\langle a,b\rangle \mid a$ *teilt* b *in* $N\}$ *ist darstellbar.*

a teilt b gdw es ein $c \leq b$ gibt, so daß $a \cdot c = b$. Die rechte Seite dieser Äquivalenz ist eine darstellbare Eigenschaft von a und b, denn sie verwendet nur eine quantorenfreie Relation und beschränkte Quantoren. □

Lemma 6.13. *Die Menge der Primzahlen ist darstellbar.*

p ist prim gdw $p > 1$ und für jedes $a < p$: (a teilt p) $\to a = 1$. □

Lemma 6.14. *Die Menge* $\{\langle p,q\rangle \mid p < q$ *sind aufeinanderfolgende Primzahlen*$\}$ *ist darstellbar. Hier sind* $p < q$ aufeinanderfolgende Primzahlen *gdw* p *und* q *prim sind und es keine Primzahl* r *gibt, so daß* $p < r < q$.

Beweis: $p < q$ sind aufeinanderfolgende Primzahlen gdw $p < q$ prim sind und für jede Primzahl $r < q$, $r \leq p$ ist. □

Lemma 6.15. *Sei* p_a *die* $a+1$*-ste Primzahl, d.h.* $p_0 = 2$, $p_1 = 3$, *usw. Dann ist die Funktion* $a \mapsto p_a$ *darstellbar.*

Beweis: Wir zeigen, daß $p_a = b$ gdw b prim ist und es ein $c \leq b^{a^2}$ gibt, so daß gilt:

(a) 2 teilt c nicht.
(b) Für alle aufeinanderfolgenden Primzahlen $q < r$ mit $q < b$ und $r \leq b$ und jedes $j < c$ teilt q^j c gdw r^{j+1} c teilt.
(c) b^a teilt c, und b^{a+1} teilt c nicht.

Wenn die obige Äquivalenz gilt, dann ist $a \mapsto p_a$ darstellbar, da alle Quantoren beschränkt sind. Nehmen wir an, daß $b = p_a$ ist und wähle c als $2^0 \cdot 3^1 \cdot 5^2 \cdots p_a^a$. Dann ist $c \leq p_a^{a^2} = b^{a^2}$, und c erfüllt die Bedingungen (a), (b) und (c). Umgekehrt nehmen wir an, daß c die Bedingungen (a), (b) und (c) erfüllt; dann muß c von der Form $2^0 \cdot 3^1 \cdots b^a \cdot$ Potenzen größerer Primzahlen sein. Dies impliziert, daß b gleich p_a ist, weil b^a c teilt und b^{a+1} c nicht teilt. □

Definition 6.16. *Für alle* $a_0, \ldots, a_k$ *sei*

$$\ll a_0, ..., a_k \gg := p_0^{a_0+1} \cdot p_1^{a_1+1} \cdots p_k^{a_k+1} = \prod_{i \leq k} p_i^{a_i+1}.$$

Wir setzen $\ll\gg = 1$.

LEMMA 6.17. *Für jedes* k *ist die Funktion*

$$(a_0, \ldots, a_k) \mapsto \ll a_0, ..., a_k \gg$$

darstellbar.

Beweis: Dies ist klar, da $\ll a_0, ..., a_k \gg$ aus einem Term definert wird. $\square$

DEFINITION 6.18. *(a) Wir definieren die einstellige Funktion* Länge *mit Funktionszeichen* Lg, *so daß für alle*

$$\mathrm{Lg}(a) = \min\{b \mid p_b \not| a \wedge (\forall x \leq a)(x > b \rightarrow p_x \not| a)\}.$$

(b) Wir definieren die Dekodierungsfunktion $\langle a, b\rangle \mapsto (a)_b$, *so daß für jedes* $b \leq k$ *gilt:*

$$(a)_b = \begin{cases} a_b, & \text{falls } b < \mathrm{Lg}(a) \wedge a \text{ ist Sequenzenkode } \wedge p_b^{a_b+1} | \, a \wedge p_b^{a_b+2} \not| a, \\ p_{\mathrm{Lg}(a)}, & \text{sonst.} \end{cases}$$

Man überlegt sich leicht, daß in unserer wichtigsten Anwendung, $a_0, \ldots, a_{k-1}$, $\mathrm{Lg}(\ll a_0, ..., a_{k-1} \gg) = k$ und $\mathrm{Lg}(\ll\gg) = 0$.

LEMMA 6.19. *Die Funktion* Länge *ist darstellbar.*

Beweis: $\mathrm{Lg}(a)$ ist das kleinste n, so daß p_n, p_{n+1}, $\ldots$, p_a die Zahl a nicht teilt. $\square$

LEMMA 6.20. *Wir sagen, daß* b *ein* Sequenzencode *ist gdw es* k *und* $a_0, \ldots, a_{k-1}$ *gibt, so daß* $b = \ll a_0, ..., a_{k-1} \gg$. *Dann ist die Menge der Sequenzencodes darstellbar.*

Beweis: b ist ein Sequenzcode gdw $b \neq 0$ und mit jeder Primzahl $p \leq b$, die b teilt, auch jede kleinere Primzahl b teilt. $\square$

LEMMA 6.21. *Die Dekodierungsfunktion ist darstellbar.*

Beweis: $(a)_b = p_{\mathrm{Lg}(a)}$, falls $b \geq \mathrm{Lg}(a)$. Für $b < \mathrm{Lg}(a)$ und, falls a Sequenzencode ist, ist $(a)_b$ das kleinste n, so daß p_b^{n+2} die Zahl a nicht teilt. Dann ist, für jedes $a \neq 0$ die Zahl $(a)_b + 1$ der Exponent von p_b in der Primfaktorzerlegung von a (wenn p_b die Zahl a teilt). Deshalb ist $(\ll a_0, ..., a_{k-1} \gg)_b = (p_0^{a_0+1} \cdot p_1^{a_1+1} \cdots p_{k-1}^{a_{k-1}+1})_b = a_b$ für alle $b < k$. Unter Verwendung des μ-Operators zeigt dies, daß $(a)_b$ darstellbar ist. $\square$

LEMMA 6.22. *Es gibt eine darstellbare Funktion* $\langle a, b\rangle \mapsto a \restriction b$ *(die Einschränkungsfunktion), so daß*

$$\ll a_0, ..., a_k \gg \restriction b = \ll a_0, ..., a_{b-1} \gg$$

für jedes $b \leq k+1$. (Wenn $b = 0$ ist, erhalten wir $\ll\gg = 1$.)

Beweis: Sei $a \restriction b$ das kleinste c, so daß ($b = 0$ und $c = 1$) oder $b > 0 \wedge \forall j < b \forall m < a\ (p_j^m | a \rightarrow p_j^m | c)$. $\square$

Lemma 6.23. *(Primitive Rekursion) Wenn f eine $k+1$-stellige Funktion ist, dann wird die $k+1$-stellige Funktion $\bar{f}$ wie folgt definiert:*

$$\bar{f}(a, \vec{b}) = \ll f(0, \vec{b}), ..., f(a-1, \vec{b}) \gg .$$

(z.B. $\bar{f}(0, \vec{b}) = \ll\gg = 1$ und $\bar{f}(1, \vec{b}) = \ll f(0, \vec{b}) \gg$.) Sei g eine darstellbare, $k+2$-stellige Funktion; definiere die $k+1$-stellige Funktion f wie folgt:

$$f(a, \vec{b}) = g(\bar{f}(a, \vec{b}), a, \vec{b}).$$

Dann ist f darstellbar.

Beweis: Wir beachten zuerst, daß $\bar{f}$ darstellbar ist: $\bar{f}(a, \vec{b})$ = das kleinste s, so daß s ein Sequenzcode der Länge a ist und $(s)_i = g(s \restriction i, i, \vec{b})$ für jedes $i < a$. Es folgt, daß f darstellbar ist, weil $f(a, \vec{b}) = g(\bar{f}(a, \vec{b}), a, \vec{b})$. $\square$

Lemma 6.24. *Wenn F darstellbar ist, dann auch G, wobei $G(a, \vec{b}) = \prod_{i<a} F(i, \vec{b})$. Dasselbe gilt, wenn $\prod$ durch $\sum$ ersetzt wird.*

Beweis: Dies folgt aus der primitiven Rekursion, denn $G(a, \vec{b}) = (\bar{G}(a, \vec{b}))_{a-1} \cdot F(a-1, \vec{b})$. $\square$

Lemma 6.25. *Es gibt eine darstellbare* Verkettungsfunktion *(auch Konkatenation genannt) $\langle a, b \rangle \mapsto a * b$, so daß $\ll a_1, ..., a_k \gg * \ll b_1, ..., b_l \gg = \ll a_1, ..., a_k, b_1, ..., b_l \gg$.*

Beweis: Wir definieren: $a * b = a \cdot \prod_{i<\mathrm{Lg}(b)} p_{i+\mathrm{Lg}(a)}^{(b)_i+1}$. $\square$

Lemma 6.26. *Für eine darstellbare Funktion F sei $\bigstar_{i<a} F(i, \vec{b}) = F(0, \vec{b}) * F(1, \vec{b}) * \cdots * F(a-1, \vec{b})$, der Wertverlauf von $F(\cdot, \vec{b})$ unterhalb a. Dann ist die Funktion $\langle a, \vec{b} \rangle \mapsto \bigstar_{i<a} F(i, \vec{b})$ darstellbar.*

Beweis: Ähnlich wie im vorvorigen Lemma: $\bigstar_{i<a} F(i, \vec{b}) = \bigstar_{i<a-1} F(i, \vec{b}) * F(a-1, \vec{b})$. $\square$

4. Gödelnummern

Wir möchten zeigen, daß jede rekursive Relation in A_E darstellbar ist. Wir haben „Rekursivität" definiert, indem wir den Begriff „Beweisbarkeit" aus der Logik verwendet haben; wie können wir zeigen, daß eine Relation auf den natürlichen Zahlen, die unter Verwendung der Logik definiert wird, in einer Theorie der Arithmetik wie A_E dargestellt werden kann?

Die Lösung dieses Problems wird durch die Verwendung von *Gödelnummern* geliefert. Diese sind Codenummern in $\mathbb{N}$ für die zentralen syntaktischen Objekte der Logik: Symbole, Terme, Formeln und Beweise. Wir werden zeigen, daß die Menge der natürlichen Zahlen, die Beweise der Logik der ersten Stufe kodieren, in A_E darstellbar ist. Aus diesem Resultat folgt die Darstellbarkeit beliebiger rekursiver Relationen in A_E.

Zuerst beschreiben wir eine Funktion h, die jedem Symbol einer gegebenen Sprache der ersten Stufe eine Codenummer zuweist. Für die logischen Symbole wird h wie folgt definiert: Die Zahlen $1, 3, 5, 7, 9$ sind die Werte von h für die Symbole $(,), \sim, \rightarrow, =$. Und die Zahlen $11 + 2n$ sind die Werte von h für die Variablen v_n, $n \geq 1$. Wir definieren $h(\forall)$ gleich 0 und verwenden die geraden, von Null verschiedenen Zahlen, um die anderen nichtlogischen Symbole zu kodieren. Obwohl unser Interesse hauptsächlich den Sprachen mit endlich vielen nichtlogischen Symbolen gilt, nehmen wir lediglich an, daß unsere Sprache *rekursiv* ist. Dies bedeutet, daß die folgenden Mengen in A_E darstellbar sind: (Beachten Sie, daß wir hier eine engere Definition von Rekursivität nehmen als die vom Kapitelanfang!)

$\{k \mid k$ ist der Wert von h für ein Konstantensymbol$\}$
$\{\langle k, m\rangle \mid k$ ist der Wert von h für ein m-stelliges Prädikatssymbol$\}$
$\{\langle k, m\rangle \mid k$ ist der Wert von h für ein m-stelliges Funktionssymbol$\}$

Dies gilt offensichtlich, wenn diese Menge endlich sind.

Definition 6.27. *(1) Für eine endliche Folge $s_0, \ldots, s_n$ von Symbolen unserer Sprache definieren wir die* Gödelnummer $\#(s_0, \ldots, s_n)$ *wie folgt:*

$$\#(s_0, ..., s_n) = \ll h(s_0), ..., h(s_n) \gg .$$

(2) Wenn Φ eine Menge endlicher Folgen von Symbolen ist, schreiben wir $\#\Phi$ für die Menge $\{\#(\varepsilon) \mid \varepsilon \in \Phi\}$.

(3) Wir führen Codenummern für Beweise ein: Wenn $\langle \alpha_0, \ldots, \alpha_n\rangle$ eine endliche Folge von Formeln ist, dann setzen wir $\mathcal{G}(\langle \alpha_0, \ldots, \alpha_n\rangle) = \ll \#\alpha_0, \ldots, \#\alpha_n \gg$.

Nun muß man zeigen, daß jeder syntaktische Begriff unserer Sprache der ersten Stufe in A_E darstellbar ist, nachdem er in Gödelnummern übersetzt wurde. Im Folgenden verwenden wir das Wort „darstellbar” für „darstellbar in A_E”.

Lemma 6.28. *Die Menge der Gödelnummern von Variablen ist darstellbar.*

Dies ist die Menge $\{a \mid (\exists b < a)\ a = \ll 11 + 2b \gg\}$. Aus früherem folgt, daß diese Menge darstellbar ist. $\square$

Lemma 6.29. *Die Menge der Gödelnummern von Termen ist darstellbar.*

Sei f die charakteristische Funktion der Menge der Gödelnummern von Termen. Also ist $f(a) = 1$ gdw es einen Term t gibt, so daß $a = \#t$; sonst ist $f(a) = 0$. Unter Verwendung der induktiven Definition von Termen folgt:

$f(a) = 1$, wenn a die Gödelnummer einer Variablen oder eines Konstantensymbols ist, und
$f(a) = 1$, wenn $(\exists i, k < a^{a \cdot \text{Länge } a})$ $[i$ Sequenzcode $\wedge$
$(\forall j < \ \text{Lg}(i)) f((i)_j) = 1 \wedge$
k der Wert von h auf einem $(\text{Lg}(i))$-stelligen Funktionssymbol $\wedge$
$a = \ll k \gg * \bigstar_{j < \ \text{Lg}(i)} (i)_j]$,
sonst $f(a) = 0$.

Nun wenden wir primitive Rekursion an, um die Darstellbarkeit von f zu zeigen. Wir haben, daß $f(a) = g(\bar{f}(a), a)$ mit folgender Funktion g:
$g(s, a) = 1$, wenn a die Gödelnummer einer Variablen oder eines Konstantensymbols ist
$g(s, a) = 1$, wenn $(\exists i, k < a^{a \cdot \text{Lg}(a)})$ $[i$ Sequenzcode $\wedge$
$(\forall j < \ \text{Lg}(i)) (s)_{(i)_j} = 1 \wedge$
k der Wert von h auf einem $(\text{Lg}(i))$-stelligen Funktionssymbol $\wedge$
$a = \ll k \gg * \bigstar_{j < \ \text{Lg}(i)} (i)_j]$
sonst $g(s, a) = 0$.

Aus früherem folgt, daß mit g auch f darstellbar ist. $\square$

Lemma 6.30. *Die Menge der Gödelnummern atomarer Formeln ist darstellbar.*

Beweis: a ist die Gödelnummer einer atomaren Formel gdw $(\exists i, k < a^{a \cdot \text{Länge } a})[i$ Sequenzcode $\wedge (\forall j < \text{Lg}(i))(i)_j$ die Gödelnummer eines Terms $\wedge$ (k ist der Wert von h auf einem $(\text{Lg}(i))$-stelligen Prädikatssymbol oder $k = h(=)$) $\wedge$
$a = \ll k \gg * \bigstar_{j < \text{Lg}(i)} (i)_j]$. $\square$

Lemma 6.31. *Die Menge der Gödelnummern von Formeln ist darstellbar.*

Beweis: Sei f die charakteristische Funktion der Menge der Gödelnummern von Formeln. Nach der induktiven Definition der Formeln:

$f(a) = 1$, wenn a die Gödelnummer einer atomaren Formel ist
$f(a) = 1$, wenn $(\exists i < a)[a = \ll h((), h(\sim) \gg * i * \ll h()) \gg \wedge f(i) = 1]$
$f(a) = 1$, wenn $(\exists i, j < a)[a = \ll h(() \gg * i * \ll h(\rightarrow) \gg * j * \ll h()) \gg \wedge f(i) =$

$f(j) = 1]$
$f(a) = 1$, wenn $(\exists i, j < a)[a = \ll h(\forall) \gg *i*j \wedge i$ Gödelnummer einer Variablen $\wedge\ f(j) = 1]$
sonst $f(a) = 0$

Wie im Termfall ist f darstellbar. □

Lemma 6.32. *Es gibt eine darstellbare Funktion* Ers*, so daß* $\mathrm{Ers}(\#\alpha, \#x, \#t) = \#\alpha^x_t$ *für Terme oder Formeln* α*, Variablen* x *und Terme* t *gilt.*

Wir definieren Ers durch $\mathrm{Ers}(a, b, c) = d$ gdw eine der folgenden Bedingungen gilt:

(a) a ist die Gödelnummer einer Variablen, $a = b$ und $d = c$.

(b) $(\exists i, k < a^{a \cdot \mathrm{Lg}(a)})[i$ Sequenzcode $\wedge$ $(\forall j < \mathrm{Lg}(i))(i)_j$ Gödelnummer eines Terms $\wedge$ k der Wert von h auf einem $(\mathrm{Lg}(i))$-stelligen Funktions- oder Prädikatssymbol $\wedge$ $a = \ll k \gg * \bigstar_{j<\mathrm{Lg}(i)}(i)_j$ $\wedge$ $d = \ll k \gg * \bigstar_{j<\mathrm{Lg}(i)}\mathrm{Ers}((i)_j, b, c)]$.

(c) $(\exists i < a)[i$ Gödelnummer einer Formel $\wedge$ $a = \ll h((), h(\sim) \gg *i* \ll h()) \gg \wedge\ d = \ll h((), h(\sim) \gg * \mathrm{Ers}(i, b, c) * \ll h()) \gg]$.

(d) $(\exists i, j < a)[i$ und j Gödelnummern von Formeln $\wedge$ $a = \ll h(() \gg *i* \ll h(\to) \gg *j* \ll h()) \gg \wedge\ d = \ll h(() \gg * \mathrm{Ers}(i, b, c) * \ll h(\to) \gg * \mathrm{Ers}(j, b, c) * \ll h()) \gg]$.

(e) $(\exists i, j < a)[i$ Gödelnummer einer Variablen $\wedge$ $i \neq b$ $\wedge$ j Gödelnummer einer Formel $\wedge$ $a = \ll h(\forall) \gg *i*j \wedge d = \ll h(\forall) \gg *i* \mathrm{Ers}(j, b, c)]$.

(f) Keine der obigen Bedingungen gilt für a und b, und $d = a$.

Man rechnet nach, daß hierdurch eindeutig eine Funktion definiert wird. □

Lemma 6.33. *Die Funktion* $n \mapsto \#(S^n 0)$ *ist darstellbar.*

Wir nennen diese Funktion f. Dann haben wir $f(0) = \ll h(0) \gg$ und $f(n+1) = \ll h(S) \gg *f(n)$. Deshalb ist f nach primitiver Rekursion darstellbar. □

Lemma 6.34. *Es gibt eine darstellbare Relation* Frei*, so daß für Terme oder Formeln* α *und Variablen* x *gilt:* $\langle \#\alpha, \#x \rangle \in \mathrm{Frei}$ *gdw* x *frei in* α *auftritt.*

$\langle a, b \rangle \in \mathrm{Frei}$ gdw $\mathrm{Ers}(a, b, \#0) \neq a$.

Nun geben wir einen anderen Beweis, der nicht auf Ers zurückgreift. $\langle \#\alpha, \#x \rangle \in$ Frei gdw
($a = \#\alpha$ Gödelnummer einer atomaren Formel und $(\exists i < \mathrm{Lg}(a)((a)_i = x))$
oder (α ist eine Formel $\sim \beta$ und x ist frei in β)

oder (α ist eine Formel $\beta \to \gamma$ und (x ist frei in β oder x ist frei in γ))
oder ($\alpha = \forall y \beta$ und $x \neq y$ und x ist frei in β).

Aus dem Lemma über primitive Rekursion folgt, daß Frei ein in A_E darstellbares Prädikat ist. $\square$

LEMMA 6.35. *Die Menge der Gödelnummern von Sätzen ist darstellbar.*

Beweis: a ist die Gödelnummer eines Satzes gdw a die Gödelnummer einer Formel ist und für jedes $b < a$ gilt: b Gödelnummer einer Variablen $\to \langle a, b\rangle \notin$ Frei. $\square$

LEMMA 6.36. *Es gibt eine darstellbare Relation* Ein*, so daß für Formeln α, Variablen x und Terme t gilt: $\langle \#\alpha, \#x, \#t\rangle \in \mathrm{Ein}$ gdw t für x in α eingesetzt werden kann.*

Wir definieren: $\langle a, b, c\rangle \in \mathrm{Ein}$ gdw a die Gödelnummer einer Formel, b die Gödelnummer einer Variablen und c die Gödelnummer eines Terms ist und (a) oder (b) oder (c) oder (d) gilt:

(a) a ist die Gödelnummer einer atomaren Formel.

(b) $(\exists d < a)[a = \ll h((), h(\sim) \gg *d* \ll h()) \gg \wedge \langle d, b, c\rangle \in \mathrm{Ein}$.

(c) $(\exists d, e < a)[a = \ll h(() \gg *d* \ll h(\to) \gg *e* \ll h()) \gg \wedge \langle d, b, c\rangle \in \mathrm{Ein} \wedge \langle e, b, c\rangle \in \mathrm{Ein}$.

(d) $(\exists d, e < a)[a = \ll h(\forall) \gg *d*e \wedge \langle a, b\rangle \notin \mathrm{Frei}$ oder $(\langle c, d\rangle \notin \mathrm{Frei} \wedge \langle e, b, c\rangle \in \mathrm{Ein})]$.

$\square$

LEMMA 6.37. *Die Relation* All*, die durch ($\langle a, b\rangle \in \mathrm{All}$ gdw a die Gödelnummer einer Formel ist und b die Gödelnummer einer Verallgemeinerung dieser Formel ist) definiert wird, ist darstellbar.*

Beweis: $\langle a, b\rangle \in \mathrm{All}$ gdw $a = b$ oder $(\exists i, j < b)[i$ die Gödelnummer einer Variablen, $\langle a, j\rangle \in \mathrm{All}$ und $b = \ll h(\forall) \gg *i*j]$. Deshalb ist All darstellbar nach primitiver Rekursion. $\square$

LEMMA 6.38. *Die Menge der Gödelnummern der Formeln von der Form $\forall x \varphi \to \varphi^x_t$, im Falle, daß t für x in φ eingesetzt werden kann, ist darstellbar.*

Beweis: a gehört zu dieser Menge gdw $(\exists f < a)(\exists x < a)(\exists t < a)[f$ die Gödelnummer einer Formel, x die Gödelnummer einer Variablen und t die Gödelnummer eines Terms $\wedge \langle f, x, t\rangle \in \mathrm{Ein} \wedge a = \ll h((), h(\forall) \gg *x*f* \ll h(\to) \gg * \mathrm{Ers}(f, x, t)* \ll h()) \gg]$. $\square$

Lemma 6.39. *Die Menge der Gödelnummern der Formeln von der Form* $\forall x(\alpha \to \beta) \to \forall x\ \alpha \to \forall x\beta$ *ist darstellbar.*

Beweis: c gehört zu dieser Menge gdw $(\exists x < c)(\exists a, b < c)[x$ die Gödelnummer einer Variablen und a und b Gödelnummern für Formeln $\wedge\ c = \ll h((), h(\forall) \gg *x*$
$\ll h(() \gg *a* \ll h(\to) \gg *b* \ll h()), h(\to), h((), h(\forall) \gg *x*a*$
$\ll h(\to), h(\forall) \gg *x*b* \ll h()), h()) \gg]$. □

Lemma 6.40. *Die Menge der Gödelnummern der Formeln von der Form* $\alpha \to \forall x\alpha$*, im Falle, daß* x *nicht frei in* α *auftritt, ist darstellbar.*

Beweis: b gehört zu dieser Menge gdw $(\exists x, a < b)[a$ die Gödelnummer einer Formel und x die Gödelnummer einer Variablen, $\langle a, x\rangle \notin \text{Frei} \wedge b = \ll h(() \gg *a*$
$\ll h(\to), h(\forall) \gg *x*a* \ll h()) \gg]$. □

Lemma 6.41. *Die Menge der Gödelnummern der Formeln von der Form* $x = x$*,* x *eine Variable, ist darstellbar.*

Beweis: a gehört zu dieser Menge gdw $(\exists x < a)[x$ die Gödelnummer einer Variablen $\wedge\ a = x* \ll h(=) \gg *x]$. □

Lemma 6.42. *Die Menge der Gödelnummern der Formeln von der Form* $x = y \to \alpha \to \alpha'$*, wobei* α *atomar ist und* α' *aus* α *dadurch entsteht, daß wir* x *durch* y *an einigen Stellen ersetzen, ist darstellbar.*

Wir definieren eine „partielle Ersetzung" pErs wie folgt: $\langle a, b, x, y\rangle \in \text{pErs}$ gdw x und y Gödelnummern von Variablen, a die Gödelnummer einer atomaren Formel und b ein Sequenzcode der Länge Länge $a \wedge$ für jedes $j < \text{Lg}(a)$ $(a)_j = (b)_j$ oder $((a)_j = x \wedge (b)_j = y)$. Unter Verwendung dieser darstellbaren Relation haben wir: c gehört zur gewünschten Menge gdw

$$(\exists a, b, x, y < c)[\langle a, b, x, y\rangle \in \text{pErs} \wedge c = \ll h(() \gg *x* \ll h(=) \gg *y* \\ \ll h(\to) \gg * \ll h(() \gg *a* \ll h(\to) \gg *b* \ll h()), h()) \gg].$$

□

Lemma 6.43. *Die Menge der Gödelnummern der Tautologien ist darstellbar.*

Beweis: Wir definieren ad hoc den Begriff der Primformel, der die syntaktische Struktur einer Tautologie der Sprache der ersten Stufe genauer beschreibt:

Eine *Primformel* ist eine Formel, die entweder atomar oder von der Form $\forall x\alpha$ ist. Wir lassen hier die äußersten Klammern um die $\forall$-Formeln hier weg und tun dies aber nicht bei booleschen Formel-Aufbau-Schritten. Jede Formel kann aus Primformeln unter Verwendung der Junktoren $\sim$ und $\to$ aufgebaut werden. Genauer gesagt, definieren wir die *Primbestandteile* von φ per Induktion über den Formelaufbau wie folgt:

Wenn φ prim ist, dann ist φ der einzige Primbestandteil von sich selbst.
Wenn $\varphi = (\sim \psi)$, dann sind die Primbestandteile von φ diejenigen von ψ.
Wenn $\varphi = (\psi \to \gamma)$, dann sind die Primbestandteile von φ diejenigen von ψ und γ.

Deshalb ist eine Tautologie eine Formel, die wahr ist, egal welche Wahrheitswerte ihren Primbestandteilen zugewiesen werden. Wir müssen dies nun als eine darstellbare Eigenschaft von Gödelnummern ausdrücken.

Die folgende 4 Lemmata sind Unterlemmata:

LEMMA 6.44. *Wir definieren:* $\langle a, b\rangle \in \mathrm{PBT}$ *gdw* a *die Gödelnummer einer Formel* α *und* b *die Gödelnummer eines Primbestandteils von* α *ist. Dann ist* PBT *darstellbar.*

Beweis:

$$\begin{aligned}&\langle a,b\rangle \in \mathrm{PBT}\ \text{ gdw } (a \text{ die Gödelnummer einer Formel ist und}\\ &((a)_0 \neq h(() \wedge a = b \vee\\ &(\exists i < a)[a = \ll h((), h(\sim) \gg *i* \ll h()) \gg \wedge \langle i, b\rangle \in \mathrm{PBT}] \vee\\ &(\exists i, j < a)[a = \ll h(() \gg *i* \ll h(\to) \gg *j* \ll h()) \gg\\ &\wedge (\langle i, b\rangle \in \mathrm{PBT}\ \vee \langle j, b\rangle \in \mathrm{PBT})]))\end{aligned}$$

Deshalb ist PBT nach primitiver Rekursion darstellbar. □

LEMMA 6.45. *Es gibt eine darstellbare Funktion* Prim*, so daß* $\mathrm{Prim}(\#\alpha) = \ll \#\beta_1, \ldots, \#\beta_n \gg$ *für jede Formel* α*, wobei* $\#\beta_1, \ldots, \#\beta_n$ *die Gödelnummern der Primbestandteile von* α *in aufsteigender Reihenfolge sind.*

Beweis: $\mathrm{Prim}(a) = s$ gdw a Gödelnummer einer Formel
$\wedge$ s Sequenzcode
$\wedge[(s)_0 = \mu n(\langle a, n\rangle \in \mathrm{PBT})$
$\wedge(\forall i < \mathrm{Lg}(s))[(i+1 < \mathrm{Lg}(s) \wedge (s)_{i+1} = \mu n((s)_i < n \wedge \langle a, n\rangle \in \mathrm{PBT}))$
$\vee(i+1 = \mathrm{Lg}(s) \wedge \sim\ \exists n < a\ ((s)_i < n \wedge \langle a, n\rangle \in \mathrm{PBT}))]$. □

LEMMA 6.46. *Die natürliche Zahl* v kodiert eine Wahrheitsbelegung für α *gdw* v *ein Sequenzcode der Länge* $\mathrm{Lg}(\mathrm{Prim}(\#\alpha))$ *ist und entweder* $(v)_i = \ll (\mathrm{Prim}(\#\alpha))_i, 0 \gg$ *oder* $(v)_i = \ll (\mathrm{Prim}(\#\alpha))_i, 1 \gg$ *für jedes* $i < \mathrm{Lg}(v)$*. Es gibt eine darstellbare Relation* Beleg*, so daß* $\langle a, v\rangle \in$ Beleg *gdw* a *die Gödelnummer einer Formel* α *ist und* v *eine Wahrheitsbelegung für* α *kodiert. Und wenn*

$\langle a, v\rangle \in \text{Beleg}$, *dann:*

$$v \leq \bigstar_{i<\text{Lg}(\text{Prim}(\#\alpha))} \ll\ll \#\alpha, 1 \gg\gg .$$

Beweis: Die Definition von „v kodiert eine Wahrheitsbelegung für α" war in Form einer darstellbaren Eigenschaft für $v, \#\alpha$. Der größtmögliche Wert von v ist $\ll\ll \#\alpha, 1 \gg, ..., \ll \#\alpha, 1 \gg\gg$, wobei diese Folge dieselbe Länge wie $\text{Prim}(\#\alpha)$ hat. Daher ist die gegebene obere Schranke richtig. $\square$

LEMMA 6.47. *Es gibt eine darstellbare Relation* Wahr*, so daß für jede Formel α und jedes v, das eine Wahrheitsbelegung s für α kodiert, gilt:* $\langle \#\alpha, v\rangle \in$ Wahr *gdw α wahr unter s ist.*

Beweis: $\langle a, v\rangle \in \text{Wahr}$ gdw a Gödelnummer einer Formel
$\wedge\ \langle a, v\rangle \in \text{Beleg} \wedge$
$[((a)_0 \neq h(() \wedge ((v)_0)_1 = 1)$
$\vee(\exists b < a(a = \ll h((), h(\sim) \gg *b* \ll h()) \gg \wedge\langle b, v \upharpoonright \text{Lg}(\text{Prim}(b))\rangle \notin \text{Wahr}))$
$\vee(\exists b, c < a(a = \ll h(() \gg *b* \ll h(\to) \gg *c* \ll h()) \gg \wedge(\langle b, v \upharpoonright \text{Prim}(b)\rangle \notin$ $\text{Wahr} \vee\langle c, v \upharpoonright \text{Prim}(c)\rangle \in \text{Wahr})))]$.

Nun beenden wir den Beweis des Lemmas 6.43. Nun haben wir: a ist die Gödelnummer einer Tautologie gdw a die Gödelnummer einer Formel ist und für jedes v, wenn $\langle a, v\rangle \in \text{Beleg}$, $\langle a, v\rangle \in \text{Wahr}$. Der Quantor auf v kann wie im vorigen Lemma beschränkt werden. $\square_{6.43}$

LEMMA 6.48. *Die Menge der Gödelnummern der logischen Axiome ist darstellbar.*

Beweis: a ist die Gödelnummer eines logischen Axioms gdw es ein $b < a$ gibt, so daß $\langle b, a\rangle \in \text{All}$ und b zu den Axiomen oder den Tautologien gehört. $\square$

LEMMA 6.49. *Sei A eine Menge von Formeln, so daß $\#A = \{\#\varphi \,|\, \varphi \in A\}$ darstellbar ist (z.B. wenn A endlich ist). Dann ist $\{\mathcal{G}(D) \,|\, D$ ist ein Beweis aus $A\}$ darstellbar.*

Beweis: d gehört zu dieser Menge gdw d ein Sequenzcode positiver Länge ist und für jedes $i < \text{Lg}(d)$ eine der folgenden Bestimmungen gilt:
$(d)_i \in \#A$
$(d)_i$ ist die Gödelnummer eines logischen Axioms
$(\exists j, k < i)[(d)_j = \ll h(() \gg *(d)_k* \ll h(\to) \gg *(d)_i* \ll h()) \gg]$
Dies ist darstellbar, weil A es ist. $\square$

LEMMA 6.50. *Jede rekursive Relation ist darstellbar in A_E.*

Beweis: Sei R eine einstellige, rekursive Relation. Dann ist R in einer endlichen Theorie A durch eine Formel φ darstellbar. Wir definieren: $f(n) =$ das kleinste d, so daß $d = \mathcal{G}(D)$, wobei D ein Beweis aus A ist, dessen letzte Komponente entweder $\varphi(S^n 0)$ oder $\sim \varphi(S^n 0)$ ist. Diese Funktion f ist darstellbar in A_E. Da $n \in R$ gdw die letzte Komponente von $f(n)$ die Zahl $\#\varphi(S^n 0)$ ist, ist auch R darstellbar in A_E. Dasselbe Argument gilt für n-stellige Relationen. $\square$

Wir sind jetzt bereit, den Gödelschen Unvollständigkeitssatz zu beweisen.

Satz 6.51. **Starker Unentscheidbarkeitssatz.** *Sei $T \subseteq \mathscr{L}(\tau)$ eine Theorie, so daß $T \cup A_E$ konsistent ist. Sei $\tau_{ar} = \{+, \cdot, E, S, 0, 1, <\}$ die Symbolmenge der Arithmetik. Dann ist die Menge*

$$\{\#\psi \mid \psi \textit{ ist ein } \mathscr{L}(\tau \cup \tau_{ar})\textit{-Satz und } T \vdash \psi\}$$

nicht rekursiv.

Beweis. Für jedes n definieren wir die Formel φ_n wie folgt: Wenn n die Gödelnummer einer Formel φ ist, wobei φ nur die eine freie Variable v_1 hat, dann setzen wir $\varphi_n = \varphi$. Sonst ist φ_n die Formel $v_1 = v_1$. Wir definieren: $R_n = \{k \mid T \cup A_E \vdash \varphi_n(S^k 0)\}$. Jetzt ist noch nicht klar, ob R_n rekursiv ist.

Sei R eine rekursive Teilmenge von $\mathbb{N}$. Dann gibt es eine Formel $\varphi(v_1)$, so daß:

$$\begin{aligned} k \in R \quad &\text{gdw} \quad A_E \vdash \varphi(S^k 0), \text{ und} \\ k \notin R \quad &\text{gdw} \quad A_E \vdash \sim \varphi(S^k 0). \end{aligned}$$

Weil $T \cup A_E$ konsistent ist, erhalten wir:

$$\begin{aligned} k \in R \quad &\text{gdw} \quad T \cup A_E \vdash \varphi(S^k 0), \text{ und} \\ k \notin R \quad &\text{gdw} \quad T \cup A_E \vdash \sim \varphi(S^k 0). \end{aligned}$$

Es folgt, daß $R = R_n$ für $n = \#\varphi(v_1)$.

Nun geht der Beweis indirekt: Annahme: Sei nun $\{\#\psi \mid \psi$ ist ein Satz und $T \vdash \psi\}$ rekursiv. Dann ist $\{\#\psi \mid \psi$ ist ein Satz und $T \cup A_E \vdash \psi\}$ auch rekursiv. Dies gilt, weil $T \cup A_E \vdash \psi$ gdw $T \vdash \wedge A_E \to \psi$, wobei $\wedge A_E$ die Konjunktion der Axiome von A_E ist. Daher ist jedes R_n eine rekursive Menge, und somit ist die Zusammenfassung der R_n genau die Zusammenfassung der rekursiven Mengen.

Wenn wir jedoch die folgende Menge R definieren:

$$n \in R \text{ gdw } n \notin R_n.$$

so ist diese rekursiv, da $n \in R$ gdw $T \cup A_E \nvdash \varphi_n(S^n 0)$. Wiederum folgt aus unserer Annahme, daß R rekursiv ist.

Dies führt aber zu einem Widerspruch, weil für jedes n die Mengen R und R_n auf n nicht übereinstimmen und daher für jedes n die Mengen R und R_n ungleich sind. $\square$

Das folgende Korollar ist eine starke Version des Gödelschen Unvollständigkeitssatzes.

SATZ 6.52. **Starker Unvollständigkeitssatz.** *Sei T eine rekursive Theorie und $T \cup A_E$ konsistent. Dann ist T unvollständig: Es gibt einen Satz ψ, so daß $T \nvdash \psi$ und $T \nvdash \sim \psi$.*

Beweis. Nach dem Satz über starke Unentscheidbarkeit ist die Menge $X = \{\#\psi \mid \psi \text{ ist ein Satz und } T \vdash \psi\}$ nicht rekursiv. Wenn T vollständig wäre, könnten wir eine totale Funktion f wie folgt definieren: $f(n) =$ das kleinste d, so daß entweder n keine Gödelnummer eines Satzes ist oder d von der Form $\mathcal{G}(D)$ ist für eine Deduktion D aus T, so daß die letzte Komponente von d entweder n oder $\ll h((), h(\sim) \gg * n * \ll h()) \gg$ ist. Die Funktion f ist rekursiv, da T eine rekursive Axiomenmenge ist. Es folgt aber, daß $n \in X$ gdw n die Gödelnummer eines Satzes und die letzte Komponente von $f(n)$ gleich n ist. Dies widerspricht der Nicht-Rekursivität von X. $\square$

Es gibt zwei wichtige Korollare:

KOROLLAR 6.53. *Sei* Theorie$(\mathfrak{N}) = \{\psi \mid \psi$ *ist ein Satz und* $\mathfrak{N} \vDash \psi\}$. *Dann ist* $\#$ Theorie$(\mathfrak{N})$ *nicht rekursiv.*

Beweis. Sei $T =$ Theorie$(\mathfrak{N})$. $T \cup A_E$ ist konsistent, da T A_E als eine Teiltheorie enthält. Und die Menge $\{\psi \mid \psi \text{ ist ein Satz und } T \vdash \psi\}$ ist gleich T. Deshalb folgt das Ergebnis aus dem starken Unentscheidbarkeitssatz. $\square$

KOROLLAR 6.54. *Sei S die Menge der (allgemein)gültigen Sätze in der Sprache der Arithmetik. Dann ist $\#S$ nicht rekursiv.*

Beweis. Dies folgt aus dem starken Unentscheidbarkeitssatz, weil $S \cup A_E$ offensichtlich konsistent ist. $\square$

Wir können das erste Korollar verstärken. Erinnern wir uns daran, daß $A \subseteq N$ *definierbar in* $\mathfrak{N}$ ist gdw es eine Formel φ gibt, so daß $k \in A$ gdw $\mathfrak{N} \vDash \varphi(k)$. Ein rekursives A ist definierbar in $\mathfrak{N}$, da jede Formel φ, die A in A_E darstellt, A in $\mathfrak{N}$ auch definiert. Die Umkehrung ist falsch; als Beispiel ist die Menge $\#\{\psi \mid \psi \text{ ist ein Satz und } A_E \vdash \psi\}$ nicht rekursiv aber definierbar in $\mathfrak{N}$. Wir haben gesehen, daß $\#$ Theorie$(\mathfrak{N})$ nicht rekursiv ist; tatsächlich haben wir den

Satz 6.55. *Undefinierbarkeitssatz.* $\#\,\mathrm{Theorie}(\mathfrak{N})$ *ist nicht definierbar in* $\mathfrak{N}$.

Beweis. Dieser ist ähnlich wie der Beweis des starken Unentscheidbarkeitssatzes. Für jedes n sei φ_n die Formel mit der Gödelnummer n, wenn eine solche existiert und nur die eine freie Variable v_1 hat; sonst sei φ_n die Formel $v_1 = v_1$. Sei $A_n = \{k \mid \mathfrak{N} \models \varphi_n(k)\}$. Dann sind die A_n die in $\mathfrak{N}$ definierbaren Mengen. Nehmen wir nun an, daß $\#\,\mathrm{Theorie}(\mathfrak{N})$ in $\mathfrak{N}$ definierbar war. Dann wäre die Menge

$$A = \{n \mid n \notin A_n\}$$

auch definierbar in $\mathfrak{N}$, da $n \in A$ gdw $\#\varphi_n(n) \notin \#\,\mathrm{Theorie}(\mathfrak{N})$. Aber natürlich ist A ungleich jedem A_n, und dies liefert einen Widerspruch. □

Die vorstehenden Ergebnisse wurden in der Sprache der Arithmetik mit Exponentiation ausgedrückt. Sie gelten aber auch für Arithmetik ohne Exponentiation. Bevor wir dies beweisen, machen wir einige Bemerkungen über die Entscheidbarkeit einiger ähnlichen Strukturen.

Eine Struktur $\mathfrak{A}$ ist *entscheidbar* gdw $\#\,\mathrm{Theorie}(\mathfrak{A})$ rekursiv ist. Also haben wir gezeigt, daß $\mathfrak{N}$ eine unentscheidbare Struktur ist. Der Unentscheidbarkeitssatz ist nicht auf die Struktur $\mathfrak{N}_A = \langle \mathbb{N}, 0, S, <, + \rangle$ anwendbar, in der die Multiplikation aus $\mathfrak{N}_M$ entfernt wurde. Tatsächlich ist diese Struktur entscheidbar. Weil 0 und S definierbar in $\langle \mathbb{N}, +, \cdot \rangle$ sind, ist $\langle \mathbb{N}, +, \cdot \rangle$ wie $\mathfrak{N}_M$ unentscheidbar.

Wir können auch die verwandten Strukturen $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ und $\langle \mathbb{C}, +, \cdot \rangle$ betrachten. Hier bezeichnen wie üblich $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ die natürlichen, die rationalen, die reellen bzw. die komplexen Zahlen. Wir haben:

Satz 6.56. $\langle \mathbb{Z}, +, \cdot \rangle$ *ist unentscheidbar.*

Beweis. Wir wenden noch einen Satz aus der Zahlentheorie (ohne Beweis) an:

Satz 6.57. *Satz von Lagrange. Für jede natürliche Zahl* n *gibt es natürliche Zahlen* a, b, c *und* d *mit* $a^2 + b^2 + c^2 + d^2 = n$.

Aus dem Satz von Lagrange erhalten wir: Eine ganze Zahl n ist eine natürliche Zahl gdw es ganze Zahlen a, b, c und d gibt, so daß $n = a^2 + b^2 + c^2 + d^2$. Deshalb ist die Menge der natürlichen Zahlen in der Struktur $\langle Z, +, \cdot \rangle$ definierbar. Es folgt, daß wir jeden Satz φ über natürliche Zahlen in einen Satz φ^* über ganze Zahlen effektiv übersetzen können, so daß $\langle \mathbb{N}, +, \cdot \rangle \models \varphi$ gdw $\langle \mathbb{Z}, +, \cdot \rangle \models \varphi^*$. Da $\langle \mathbb{N}, +, \cdot \rangle$ unentscheidbar ist, gilt dies auch für $\langle \mathbb{Z}, +, \cdot \rangle$. □

Satz 6.58. $\langle \mathbb{Q}, +, \cdot \rangle$ *ist unentscheidbar.*

Dieser Beweis ist schwieriger. Man kann wiederum zeigen, daß die Menge der natürlichen Zahlen in der gegebenen Struktur definierbar ist. Dies zitiert Zahlentheorie von Hasse und war Julia Robinson's Doktorarbeit [**7**].

Die Struktur $\langle \mathbb{Q}, + \rangle$ ohne Multiplikation hingegen ist entscheidbar.

SATZ 6.59. *$\langle \mathbb{R}, +, \cdot \rangle$ und $\langle \mathbb{C}, +, \cdot \rangle$ sind entscheidbar.*

Der Beweis dieses Satzes benötigt Ergebnisse aus der Körpertheorie und würde im Rahmen dieser Vorlesung sprengen.

Wir zeigen nun, daß Exponentiation für unsere Resultate über Unentscheidbarkeit, Unvollständigkeit und Undefinierbarkeit nicht notwendig ist. Die Hauptarbeit besteht darin, den folgenden Satz zu zeigen.

SATZ 6.60. *E ist in $\mathfrak{N}_M = \langle \mathbb{N}, 0, S, <, +, \cdot \rangle$ definierbar.*

Beweis. Wir zeigen zuerst, daß die Kodierung von endlichen Folgen natürlicher Zahlen mit natürlichen Zahlen ohne Exponentiation durchgeführt werden kann. Das zentrale Lemma ist folgendes:

LEMMA 6.61. *Es gibt eine $\mathfrak{N}_M$-definierbare Funktion δ, so daß es für alle $n, a_0, ..., a_n$ in $\mathbb{N}$ ein s gibt mit $\delta(s, i) = a_i$ für $i \leq n$.*

Beweis des Lemmas. Wir zeigen zuerst, daß es eine $\mathfrak{N}_M$-definierbare Bijektion J von $\mathbb{N} \times \mathbb{N}$ auf $\mathbb{N}$ gibt. Wir ordnen Paare natürlicher Zahlen wie folgt: $\langle m_0, m_1 \rangle \leq \langle n_0, n_1 \rangle$ gdw $m_0 + m_1 < n_0 + n_1$ oder $(m_0 + m_1 = n_0 + n_1$ und $m_0 < n_0)$. (D.h. wir vergleichen die Summen $m_0 + m_1, n_0 + n_1$ und verwenden dann die lexikographische Ordnung.) Sei $J(a, b)$ die Anzahl der Paare natürlicher Zahlen, die kleiner als $\langle a, b \rangle$ in dieser Ordnung sind. Dann ist J eine Bijektion zwischen $\mathbb{N} \times \mathbb{N}$ und $\mathbb{N}$. Da $J(a, b) = (1 + 2 + 3 + \cdots (a + b)) + a = (a+b)(a+b+1)/2 + a =$ (das kleinste c, so daß $2c = (a+b)(a+b+1)) + 2a$, ist J in $\mathfrak{N}_M$ definierbar. Seien K und L eindeutig definiert durch $K(J(a, b)) = a$ und $L(J(a, b)) = b$. Dann sind K und L auch in $\mathfrak{N}_M$ definierbar.

Nun definiere $\delta(s, i) = \beta(K(s), L(s), i)$, wobei:

$$\beta(c, d, i) = \text{ der Rest, wenn } c \text{ durch } 1 + (i + 1) \cdot d \text{ geteilt wird.}$$

Wir müssen zeigen:

$(*)$ Für alle $n, a_0, ...a_n$ gibt es c und d, so daß $\beta(c, d, i) = a_i$ für jedes $i \leq n$.

Diese Tatsache aus der Zahlentheorie kann wie folgt bewiesen werden: Die natürlichen Zahlen $d_0, ..., d_n$ sind *paarweise relativ prim* gdw für alle $i < j \leq n$ keine Primzahl sowohl d_i als auch d_j teilt. Wir benutzen den

SATZ 6.62. *Chinesischen Restsatz. Seien $d_0, ..., d_n$ paarweise relativ prim und $a_i < d_i$ für alle $i \leq n$. Dann gibt es ein c, so daß für alle $i \leq n$ a_i der Rest der Division von c durch d_i ist.*

Beweis. Sei $p = \prod_{i \leq n} d_i$. Für jedes c sei $F(c)$ das $(n+1)$-Tupel der Reste der Divisionen von c durch die d_i. F ist injektiv auf die Menge der Zahlen kleiner p: Wenn $F(c_1) = F(c_2)$, $c_1 \leq c_2 < p$, dann teilt jedes d_i die Differenz $c_2 - c_1$, und auch p muss diese Differenz teilen, da die d_i paarweise relativ prim sind. Weil c_1 und c_2 kleiner p sind, folgt $c_1 = c_2$.

Wir sehen nun aber, daß F eingeschränkt auf die Menge der Zahlen kleiner p eine injektive Funktion von einer Menge mit p Elementen in eine Menge mit p Elementen ist. Es folgt, daß F surjektiv ist. Daher können wir $c < p$ wählen, so daß $F(c) = \langle a_0, ..., a_n \rangle$, wie gewünscht. $\square_{\text{Fixpunktsatz}}$

Wir beachten nun, daß für jedes s die $s+1$ Zahlen $1 + 1 \cdot s!$, $1 + 2 \cdot s! \ldots 1 + (s+1) \cdot s!$ paarweise relativ prim sind: Wenn eine Primzahl p sowohl $1 + j \cdot s!$ als auch $1 + k \cdot s!$, $j \leq k$, teilt, dann teilt sie die Differenz $(k - j) \cdot s!$. p kann aber $s!$ nicht teilen, und daher ist $p > s$ und teilt $k - j$. Da $k - j \leq s$, folgt $k = j$.

Wir beweisen jetzt $(*)$. Seien $n, a_0, ..., a_n$ wie in der Annahme von $(*)$ und s das Maximum von $n, a_0, ..., a_n$. Wenn $d = s!$, dann sind die Zahlen $1 + (i+1) \cdot d$, $i \leq n$ paarweise relativ prim. Nach dem Chinesischen Restsatz gibt es ein c, so daß für jedes $i \leq n$ der Rest der Division von c durch $1 + (i+1) \cdot d$ wie gewünscht a_i ist.

Damit ist das Lemma bewiesen. $\square$

Um schließlich den Satz zu beweisen, verwenden wir die Funktion δ, um zu zeigen, daß die Exponentiation definierbar in $\mathfrak{N}_M$ ist. Wir definieren die Funktion E^* wie folgt: $E^*(a, b) =$ das kleinste s, so daß $\delta(s, 0) = 1$ und für jedes $i < b$ $\delta(s, i+1) = \delta(s, i) \cdot a$. Somit ist $E^*(a, b)$ die Zahl, die mittels der Funktion δ die Folge $a^0, a^1, ..., a^b$ kodiert. Also haben wir $a^b = \delta(E^*(a, b), b)$, und daher ist die Exponentiation in $\mathfrak{N}_M$ definierbar. $\square$

Die Theorie A_M ergibt sich, indem wir die Axiome von A_E bezüglich der Exponentiation streichen. Unsere früheren Ergebnisse über Darstellbarkeit in A_E gelten auch für A_M: Die in A_M darstellbaren Relationen enthalten alle Relationen, die in $\mathcal{N}_M$ ohne Quantoren definierbar sind, und sind unter Junktoren, beschränkten Quantoren und dem μ-Operator abgeschlossen. Die in A_M darstellbaren Funktionen sind auch unter Komposition abgeschlossen. Es folgt, daß die obigen Funktionen δ und E^* in A_M darstellbar sind und somit auch die Exponentiation. Deshalb ist es möglich, unsere früheren Betrachtungen in A_E genauso in A_M zu wiederholen. Also haben wir: Jede rekursive Relation ist in A_M darstellbar; wenn $T \cup A_M$ konsistent ist, dann ist $\#\{\psi \mid \psi$ ist ein Satz, $T \vdash \psi\}$ nicht rekursiv; und wenn $T \cup A_M$ konsistent und $\#T$ rekursiv ist, dann ist T unvollständig. Zusätzlich ist $\#$ Theorie $\mathfrak{N}_M$ in $\mathfrak{N}_M$ nicht definierbar, und die Menge der Gödelnummern der gültigen Sätze der Sprache von $\mathfrak{N}_M$ ist nicht rekursiv.

5. Effektive Aufzählbarkeit

Wir sahen, daß $A \subseteq \mathbb{N}^k$ ist *rekursiv* gdw A darstellbar in A_E ist.

Definition 6.63. *A ist* rekursiv aufzählbar (RE) *gdw A* schwach darstellbar in *A_E ist, d.h. wenn es eine Formel φ gibt, so daß:*

$$\langle n_1, \dots, n_k \rangle \in A \textit{ gdw } A_E \vdash \varphi(n_1, \dots, n_k).$$

Die schwache Darstellbarkeit unterscheidet sich von Darstellbarkeit darin, daß wir nicht verlangen, daß A_E den Satz $\sim \varphi(n_1, \dots, n_k)$ für $\langle n_1, \dots, n_k \rangle \notin A$ beweist. Während rekursive Mengen offensichtlich „berechenbar" sind, sind rekursiv aufzählbare Menge also nur „effektiv aufzählbar".

Jede RE Relation ist definierbar im Standardmodell der Arithmetik $\mathfrak{N} = \langle \mathbb{N}, 0, S, <, +, \cdot, E \rangle$ durch eine Formel spezieller Form.

Definition 6.64. *Die Menge der Δ_0* Formeln *(in der Sprache der Arithmetik) ist wie folgt definiert:*
(i) Jede atomare Formel ist Δ_0.
(ii) Wenn φ, ψ Δ_0 sind, dann auch $\sim \varphi$ und $\varphi \wedge \psi$.
(iii) Wenn φ Δ_0 ist, dann auch $\forall x < t\ \varphi$, wobei t ein Term ohne x ist.

Definition 6.65. *Eine Formel ist Σ_1 gdw sie von der Form $\exists x_1 \exists x_2 \cdots \exists x_k\ \psi$ ist, wobei ψ Δ_0 ist. Eine Relation ist Σ_1 gdw sie in $\mathfrak{N}$ durch eine Σ_1 Formel definierbar ist.*

Satz 6.66. *Sei $A \subseteq \mathbb{N}^k$. Folgende Aussagen sind äquivalent:*
(a) A ist RE.
(b) $A = \{(x_1, \dots, x_k) \mid \exists y (x_1, \dots, x_k, y) \in B\}$, für ein rekursives $B \subseteq \mathbb{N}^{k+1}$.
(c) A ist Σ_1.

Beweis. Wir nehmen an, daß $k = 1$ ist. (a) $\to$ (c): Sei $n \in A$ gdw $A_E \vdash \varphi(n)$. Dann haben wir: $n \in A$ gdw $\exists d(d$ ist die Gödelnummer eines Beweises aus A_E von $\varphi(n))$. Nach früherer Arbeit ist $\{(d, n) \mid d$ die Gödelnummer eines Beweises aus A_E von $\varphi(n)\}$ darstellbar in A_E; tatsächlich ist diese Menge in A_E darstellbar durch eine Formel φ mit nur beschränkten Quantoren. Folgt, daß A Σ_1 ist.
(c) $\to$ (b): Klar, da durch Δ_0 Formeln definierbare Relationen sind auch rekursiv.
(b) $\to$ (a): Sei B darstellbar in A_E durch die Formel $\psi(x_1, \dots, x_k, y)$. Sei $\varphi(x_1, \dots, x_k)$ die Formel $\exists y\ \psi(x_1, \dots, x_k, y)$. Dann haben wir:

$$(x_1, \dots, x_k) \in A \text{ gdw } \exists y (A_E \vdash \psi(x_1, \dots, x_k, y)) \text{ gdw } A_E \vdash \exists y\ \psi(x_1, \dots, x_k, y).$$

und deshalb ist A schwach darstellbar in A_E. □

KAPITEL 7

Der zweite Unvollständigkeitssatz

Sei T eine rekursive Axiomenmenge, die A_E enthält. Dann ist die Menge der Gödelnummern der Sätze aus T RE, und deshalb gibt es eine Σ_1-Formel $\mathrm{Bew}_T(x)$, so daß gilt:

$\mathrm{Bew}_T(n)$ ist wahr gdw es einen Satz ψ gibt, so daß $n = \#\psi$ und $T \vdash \psi$.

Wir können die Konsistenz von T durch den Satz $\mathrm{Kon}_T = \sim \mathrm{Bew}_T(\#(0 = 1))$ ausdrücken. Der zweite Gödelsche Unvollständigkeitssatz besagt, daß, wenn die Formel $\mathrm{Bew}_T(x)$ geeignet eingeschränkt wird, T den Satz Kon_T nicht beweist.

DEFINITION 7.1. $\mathrm{Bew}_T(x)$ *ist eine* gute T-Beweisbarkeitsformel *gdw die folgenden Bedingungen erfüllt sind:*

(1) $\mathrm{Bew}_T(x)$ *ist* Σ_1, *und* $\mathrm{Bew}_T(n)$ *ist wahr gdw es einen Satz* ψ *gibt, so daß* $n = \#\psi$ *und* $T \vdash \psi$.

(2) *Für* Σ_1*-Sätze* ψ: $T \vdash (\psi \to \mathrm{Bew}_T(\#\psi))$.

(3) *Für alle Sätze* ψ *und* γ: $T \vdash (\mathrm{Bew}_T(\#\psi) \wedge \mathrm{Bew}_T(\#(\psi \to \gamma))) \to \mathrm{Bew}_T(\#\gamma)$.

SATZ 7.2. *Zweiter Gödelscher Unvollständigkeitssatz. Sei* T *eine konsistente, rekursive Axiomenmenge die* A_E *enthält, und sei* $\mathrm{Bew}_T(x)$ *eine gute* T*-Beweisbarkeitsformel. Dann* $T \nvdash \mathrm{Kon}_T$.

Beweis. Wir verwenden den

SATZ 7.3. *Fixpunktsatz. In der Sprache der Arithmetik gibt es für jede Formel* β *mit nur einer freien Variablen einen Satz* σ, *so daß*

$$A_E \vdash \sigma \leftrightarrow \beta(\#\sigma).$$

Beweis. Sei f die Funktion, die $\#\alpha(n)$ einem Paar $\langle \#\alpha, n\rangle$ zuweist. Sei f darstellbar in A_E durch die Formel $\theta(v_1, v_2, v_3)$. Betrachten wir nun die Formel $\gamma(v_1) = \forall v_3(\theta(v_1, v_1, v_3) \to \beta(v_3))$. (Diese Formel sagt aus, daß β für die Gödelnummer von ψ wahr ist, wenn ψ aus der Formel δ mit Gödelnummer v_1 dadurch entsteht, daß wir ihre freie Variable durch v_1 ersetzen.) Sei q die Gödelnummer von γ. Dann ist der gesuchte Satz

$$\sigma = \gamma(q) = \forall v_3(\theta(q, q, v_3) \to \beta(v_3)).$$

Weil $\theta(v_1, v_2, v_3)$ die obige Funktion f darstellt und $\#\sigma$ der Wert dieser Funktion auf $\langle q, q\rangle$ ist, haben wir, daß $A_E \vdash \forall v_3(\theta(q, q, v_3) \leftrightarrow v_3 = \#\sigma)$. Somit:

$$\begin{aligned} \sigma &= \forall v_3(\theta(q, q, v_3) \to \beta(v_3)), \\ A_E &\vdash \theta(q, q, \#\sigma), \\ A_E \cup \{\sigma\} &\vdash \beta(\#\sigma), \\ A_E &\vdash \sigma \to \beta(\#\sigma). \end{aligned}$$

Für die umgekehrte Richtung haben wir:

$$\begin{aligned} A_E &\vdash \beta(\#\sigma) \to (\forall v_3(\theta(q, q, v_3) \to \beta(v_3))), \\ A_E &\vdash \beta(\#\sigma) \to \sigma. \end{aligned}$$

Somit $A_E \vdash \sigma \leftrightarrow \beta(\#\sigma)$, wie gewünscht. $\square_{\text{Fixpunktsatz}}$

Sei nun σ ein Satz, so daß $A_E \vdash \sigma \leftrightarrow\sim \mathrm{Bew}_T(\#\sigma)$. Zuerst zeigen wir, daß $T \nvdash \sigma$: Sonst ist $\mathrm{Bew}_T(\#\sigma)$ wahr, und deshalb, da A_E alle wahren Σ_1-Sätze beweist, $A_E \vdash \mathrm{Bew}_T(\#\sigma)$. Da $A_E \vdash \sigma \leftrightarrow\sim \mathrm{Bew}_T(\#\sigma)$, erhalten wir $A_E \vdash\sim \sigma$. Somit ist $T \supseteq A_E$ inkonsistent, im Widerspruch zu unserer Hypothese. Daher $T \nvdash \sigma$.

Nun beweisen wir den zweiten Gödelschen Unvollständigkeitssatz. Sei σ wie oben. Zuerst zeigen wir, daß $T \vdash \mathrm{Kon}_T \to \sigma$. Da $T \nvdash \sigma$, folgt, daß $T \nvdash \mathrm{Kon}_T$.

Es genügt zu zeigen, daß $T \vdash\sim \sigma \to\sim \mathrm{Kon}_T$. Wir haben:

$T \vdash \mathrm{Bew}_T(\#\sigma) \to \mathrm{Bew}_T(\#(\mathrm{Bew}_T(\#\sigma)))$ nach Eigenschaft (2) der guten T-Beweisbarkeitsformel $\mathrm{Bew}_T(x)$

$T \vdash \mathrm{Bew}_T(\#\sigma) \to (\sigma \to 0 = 1)$ nach Wahl von σ

$T \vdash \mathrm{Bew}_T(\#(\mathrm{Bew}_T(\#\sigma) \to (\sigma \to 0 = 1)))$, denn $A_E \subseteq T$ beweist alle wahren Σ_1-Sätze

$T \vdash (\mathrm{Bew}_T(\#(\mathrm{Bew}_T(\#\sigma))) \wedge \mathrm{Bew}_T(\#(\mathrm{Bew}_T(\#\sigma) \to (\sigma \to 0 = 1)))) \to \mathrm{Bew}_T(\#(\sigma \to 0 = 1))$ nach Eigenschaft (3) der guten Beweisbarkeitsformel $\mathrm{Bew}_T(x)$.

Wir wissen aber, daß T sowohl die zweite Hypothese der letzten Implikation als auch den Satz $\mathrm{Bew}_T(\#\sigma) \to \mathrm{Bew}_T(\#(\mathrm{Bew}_T(\#\sigma)))$ beweist. Somit haben wir: $T \vdash \mathrm{Bew}_T(\#\sigma) \to \mathrm{Bew}_T(\#(\sigma \to 0 = 1))$.
Nach Eigenschaft (3) der guten T-Beweisbarkeitsformel $\mathrm{Bew}_T(x)$ erhalten wir:

$$T \vdash (\mathrm{Bew}_T(\#\sigma) \wedge \mathrm{Bew}_T(\#(\sigma \to 0 = 1))) \to \mathrm{Bew}_T(\#(0 = 1)).$$

Also $T \vdash \mathrm{Bew}_T(\#\sigma) \to \mathrm{Bew}_T(\#(0 = 1))$. $T \vdash\sim \sigma \to \mathrm{Bew}_T(\#\sigma)$ nach Wahl von σ. Es folgt, daß $T \vdash\sim \sigma \to\sim \mathrm{Kon}_T$, wie gewünscht. $\square$

Ein wichtiges Beispiel einer Theorie T, die A_E enthält, für die es eine gute T-Beweisbarkeitsformel gibt, ist die *Peano-Arithmetik*, kurz PA. Diese ergibt sich, indem wir zu A_E für jede Formel φ, die möglicherweise zusätzlich zu x weitere freie Variablen enthält, das folgende Induktionsaxiom hinzufügen:

$$(\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(Sx))) \rightarrow \forall x \varphi(x),$$

Der zweite Gödelsche Unvollständigkeitssatz kann auch auf beliebige, rekursive, konsistente Theorien, die PA enthalten, angewandt werden.

KAPITEL 8

Vier Teilgebiete der Logik, ein wenig Modelltheorie

Wir haben gesehen, daß die Menge der Sätze, die im Standardmodell $\mathfrak{N}$ der Arithmetik wahr sind, nicht rekursiv ist. Dieses Ergebnis ist nicht auf die Arithmetik beschränkt; z.B. betrachten wir die Sprache der Mengenlehre. Die Arithmetik kann in die Sprache der Mengenlehre übersetzt werden, in dem Sinne, daß es eine rekursive Funktion gibt, die jedem Satz ψ der Arithmetik einen Satz ψ^* der Mengenlehre zuweist, so daß:

$$\begin{gathered}\psi \text{ ist wahr im Standardmodell } \mathfrak{N} \text{ der Arithmetik gdw} \\ \psi^* \text{ wahr im Standardmodell der Mengenlehre ist.}\end{gathered}$$

Nun sei T die Menge der Sätze, die wahr im Standardmodell der Mengenlehre sind. Dann ist ψ im Standardmodell der Arithmetik wahr gdw $\psi^* \in T$, und deshalb ist T nicht rekursiv. Ein ähnliches Argument zeigt: Die Menge aller Sätze einer beliebigen Menge von Axiomen der Mengenlehre, die zusammen mit dem üblichen System ZFC konsistent ist, ist nicht rekursiv. Und keine solche rekursive Axiomenmenge ist vollständig oder kann seine eigene Konsistenz beweisen.

Daher zeigen Gödels Ergebnisse, daß *Nicht-Rekursivität, Unvollständigkeit* und *Unbeweisbarkeit der Konsistenz* nötige Aspekte der Grundlagen der Mathematik sind. Logiker sind diese Probleme auf vier verschiedenen Arten angegangen.

1. Unvollständigkeit. Wir können nur diejenigen Theorien betrachten, die die Arithmetik nicht enthalten und auf die daher der Gödelsche Unvollständigkeitssatz nicht angewandt werden kann. Dies führt uns zur *Modelltheorie*.
2. Nicht-Rekursivität. Wir können *den Grad der Nicht-Rekursivität* von mathematischen Eigenschaften untersuchen. Dies führt uns zur *Rekursionstheorie*.
3. Unbeweisbarkeit der Konsistenz. Wir können versuchen, einen Beweis der Konsistenz der Arithmetik zu finden, der — obwohl kein Beweis aus der Arithmetik — trotzdem „konstruktiv" ist. Dies führt uns zur *Beweistheorie*.
4. Unvollständigkeit, die Zweite. Wir können versuchen, eine sehr starke Theorie zu finden, die vollständig für „natürliche" mathematische Probleme ist. Dies führt uns zur *Mengenlehre*.

Im Rest dieses Kurses betrachten wir ein wenig Modelltheorie.

1. Quantorenelimination

Die stärkste Methode, um die Vollständigkeit einer rekursiven Theorie zu zeigen, ist *Quantorenelimination*. Wir beginnen mit einer allgemeinen Beschreibung dieser Methode und wenden sie dann auf einige Beispiele an.

Definition. Eine Theorie T *erlaubt Quantorenelimination* (T hat *QE*) gdw es für jede Formel φ eine quantorenfreie Formel ψ gibt, so daß $T \vdash \varphi \leftrightarrow \psi$.

Das nächste Lemma gibt eine hinreichende Bedingung dafür, daß eine Theorie QE hat. Eine Formel φ ist *primitiv* gdw sie von der Form

$$\varphi = \exists x(\psi_1 \wedge \cdots \wedge \psi_n)$$

ist, wobei jedes ψ_i entweder atomar oder negiert atomar ist. (ψ ist *negiert atomar* gdw es die Negation einer atomaren Formel ist.)

Lemma 8.1. *Sei T eine Theorie, so daß es für jede primitive Formel φ eine quantorenfreie Formel ψ gibt mit $T \vdash \varphi \leftrightarrow \psi$. Dann hat T QE.*

Beweis. Wir zeigen per Induktion über den Formelaufbau, daß es eine quantorenfreie Formel ψ gibt, so daß $T \vdash \varphi \leftrightarrow \psi$. Dies gilt offensichtlich für atomares φ. Wenn $\varphi = \sim \gamma$ oder $(\gamma \rightarrow \delta)$, dann folgt das Ergebnis leicht aus der Induktionsannahme. Nehmen wir nun an, daß φ von der Form $\forall x \gamma$ ist. Nach Induktionsannahme sei ψ' eine quantorenfreie Formel, so daß $T \vdash \gamma \leftrightarrow \psi'$. Dann gilt $T \vdash \forall x \gamma \leftrightarrow \forall x \psi'$. Nun ist ψ' logisch äquivalent zu einer Konjunktion $\psi'_1 \wedge \cdots \wedge \psi'_n$, in der jedes ψ'_i eine Disjunktion von atomaren und negatomaren Formeln ist. Deshalb beweist T den Satz $\forall x \gamma \leftrightarrow (\forall x \psi'_1 \wedge \forall x \psi'_2 \wedge \cdots \wedge \forall x \psi'_n)$, worin jedes $\forall x \psi'_i$ logisch äquivalent zur Negation einer primitiven Formel ist. Nach Annahme gibt es quantorenfreie Formeln ψ_i, so daß $T \vdash \forall x \psi'_i \leftrightarrow \sim \psi_i$ für jedes i; und daher beweist T die Äquivalenz $\varphi \leftrightarrow (\sim \psi_1 \wedge \cdots \wedge \sim \psi_n)$. $\square$

Unser nächstes Lemma zeigt, wie Quantorenelimination verwendet werden kann, um Vollständigkeit zu beweisen.

Lemma 8.2. *Sei T eine QE Theorie in einer Sprache mit einem Konstantensymbol. Sei T* vollständig für atomare Sätze*, in dem Sinne, daß für jeden atomaren Satz φ entweder φ oder $\sim \varphi$ beweisbar aus T ist. Dann ist T vollständig.*

Beweis. Sei φ ein Satz. Da T QE hat, gibt es eine quantorenfreie Formel ψ, so daß $T \vdash \varphi \leftrightarrow \psi$. Wir können annehmen, daß ψ auch ein Satz ist; sonst ersetzen wir jede freie Variable von ψ durch ein Konstantensymbol. Wir zeigen nun per Induktion über den Aufbau von ψ, daß für jeden quantorenfreien Satz ψ entweder ψ oder $\sim \psi$ beweisbar aus T ist: Wenn ψ atomar ist, folgt dies aus der Hypothese des Lemmas. Wenn $\psi = \sim \psi'$, dann folgt dies aus der Induktionsannahme. Wenn $\psi = (\gamma \rightarrow \delta)$, dann beweist T entweder sowohl γ als auch

$\sim \delta$, in welchem Fall $T \vdash\sim \psi$, oder $\sim \gamma$ oder δ, in welchem Fall $T \vdash \psi$. $\square$

Leider gibt es nur wenige Theorien T mit QE. Manchmal jedoch hat T eine Erweiterung, die T stark ähnelt und QE hat. Diese Idee wird in der nächsten Definition beschrieben.

DEFINITION 8.3. *Seien $T_1 \subseteq T_2$ Theorien der Sprachen $\mathcal{L}_1 \subseteq \mathcal{L}_2$. Dann ist T_2 eine* konservative Erweiterung *von T_1 gdw jeder in T_2 beweisbare Satz φ in der Sprache $\mathcal{L}_1$ auch in T_1 beweisbar ist.*

Folgendes ist klar:

LEMMA 8.4. *Nehmen wir an, daß T eine vollständige, konservative Erweiterung hat. Dann ist T vollständig.*

Eine konservative Erweiterung T^* von T wird oft wie folgt konstruiert: Wir fügen neue nichtlogische Symbole und dann Axiome hinzu, die einige der neuen Symbole durch Formeln der Sprache von T definieren. Jedes Modell von T kann in ein Modell von T^* umgewandelt werden, indem wir die neuen Symbole unter Verwendung ihrer Definitionen in der Sprache von T interpretieren. Es folgt, daß jeder Satz φ der Sprache von T, der wahr in jedem Modell von T^* ist, auch wahr in jedem Modell von T ist. Deshalb ist T^* eine konservative Erweiterung von T.

Die obigen Lemmata führen uns zu einer allgemeinen Quantoreneliminationsmethode:

SATZ 8.5. *QE-Methode. Nehmen wir an, daß T eine konservative Erweiterung T^* hat mit den folgende vier Eigenschaften:*

(1) Die Sprache von T^* enthält ein Konstantensymbol.

(2) T^* ist vollständig für atomare Sätze.

(3) Für jede primitive Formel φ der Sprache von T^* gibt es eine quantorenfreie Formel ψ der Sprache von T^*, so daß $T^* \vdash \varphi \leftrightarrow \psi$.

Dann ist T vollständig.

Als eine Anwendung dieser Methode beweisen wir die Vollständigkeit der Theorie DLO (dichte lineare Ordnung). DLO ist eine endliche Axiomenmenge für die Ordnung der rationalen Zahlen.

DEFINITION 8.6. *Die Axiome von DLO*

1. $(\forall x)(x \leq x)$
2. $(\forall x, y)(x \leq y \wedge y \leq x \rightarrow x = y)$
3. $(\forall x, y, z)(x \leq y \wedge y \leq z \rightarrow x \leq z)$
4. $(\forall x, y)(x \leq y \vee y \leq x)$

Sei $x < y$ gdw $x \leq y \wedge x \neq y$.
5. $(\forall x, y)(x < y \rightarrow \exists z(x < z < y))$
6. $(\forall x)(\exists y, z(y < x < z))$

Diese Axiome sind offensichtlich wahr in der Struktur $\langle \mathbb{Q}, \leq \rangle$. $\mathbb{Q}$ ist wie schon gehabt die Menge der rationalen Zahlen. Wir zeigen mit Hilfe der Quantorenelimination, daß die Axiomenmenge DLO vollständig ist.

Sei DLO* dasselbe System DLO mit einem zusätzlichen Konstantensymbol 0. DLO* ist eine konservative Erweiterung von DLO. Die einzigen atomaren Sätze sind $0 = 0$ und $0 \leq 0$, die beide beweisbar aus DLO* sind. Um zu zeigen, daß DLO vollständig ist, genügt es daher zu zeigen, daß DLO* QE hat.

Sei φ von der Form $\exists x \psi$ mit einer quantorenfreie Formel ψ. Dann beweist DLO*, daß ψ inkonsistent oder äquivalent zu einer Disjunktion von Formeln der Form $u_1 R_1 u_2 \wedge u_2 R_2 u_3 \wedge \cdots \wedge u_{n-1} R_{n-1} u_n$ ist, wobei die u_i die verschiedenen Variablen oder ggf. das Konstantensymbol in ψ und die R_i entweder $=$ oder $<$ sind. Wenn ψ inkonsistent ist, dann ist φ äquivalent zur quantorenfreien Formel $x \neq x$. Wenn ψ konsistent ist,dann ist φ äquivalent zu einer Disjunktion $\varphi_1 \vee \cdots \vee \varphi_m$ von Formeln der Form $\varphi_j = \exists x(u_1 R_1 u_2 \wedge u_2 R_2 u_3 \wedge \cdots \wedge u_{n-1} R_{n-1} u_n)$, wobei $u_1 R_1 u_2 \wedge u_2 R_2 u_3 \wedge \cdots \wedge u_{n-1} R_{n-1} u_n$ wie oben ist. Wenn x gleich u_1 und R_1 gleich $<$ ist, dann ist φ_j nach Axiom 6 von DLO äquivalent zu $u_2 R_2 u_3 \wedge \cdots \wedge u_{n-1} R_{n-1} u_n$. Wir können x ähnlich eliminieren, wenn x gleich u_n und R_{n-1} gleich $<$ ist, oder, wenn x gleich einem u_i, wobei R_{i-1} und R_i gleich $<$ sind. Schließlich, wenn x gleich u_i, wobei R_{i-1} oder R_i gleich $=$ ist, dann kann x mit Hilfe logischer Axiome eliminiert werden. Daher beweist DLO*, daß φ_j äquivalent zur quantorenfreien Formel ist, die dadurch entsteht, indem wir den Quantor $\exists x$ und die Konjunktionen in $u_1 R_1 u_2 \wedge u_2 R_2 u_3 \wedge \cdots \wedge u_{n-1} R_{n-1} u_n$, in denen x auftritt, eliminieren. Somit ist φ zu einer quantorenfreien Formel äquivalent, da es zur Disjunktion der φ_j äquivalent ist. □

Wir haben gezeigt:

SATZ 8.7. *DLO ist vollständig. Für jeden $\{<\}$-Satz gilt: Der Satz ist wahr in der Struktur $\langle \mathbb{Q}, \leq \rangle$ gdw er beweisbar aus DLO ist.*

Es folgt, daß jedes Modell von DLO dieselben Sätze wie $\langle \mathbb{Q}, \leq \rangle$ erfüllt. Zum Beispiel erfüllen $\langle \mathbb{R}, \leq \rangle$ und $\langle \mathbb{Q}, \leq \rangle$ dieselben Sätze. Desweiteren gilt folgendes: Wenn φ eine Formel der Sprache von DLO und s eine $\langle \mathbb{Q}, \leq \rangle$-Belegung ist, dann $\langle \mathbb{Q}, \leq \rangle \models \varphi[s]$ gdw $\langle \mathbb{R}, \leq \rangle \models \varphi[s]$. Dies gilt, weil wir mittels Quantorenelimination annehmen können, daß φ quantorenfrei ist, und deshalb folgt das Ergebnis allein aus der Tatsache, daß $\langle \mathbb{Q}, \leq \rangle$ eine Substruktur von $\langle \mathbb{R}, \leq \rangle$ ist.

Es gibt allerdings auch einen einfacheren Beweis der Vollständigkeit von DLO gibt, der Quantorenelimination nicht verwendet: Man kann zeigen, daß je zwei abzählbare Modelle von DLO isomorph sind (die heißt manchmal „Satz von Cantor über dichte lineare Ordnungen"), und daher dieselben Sätze erfüllen. Also ist jeder Satz φ in allen abzählbaren oder in keinem Modell von DLO wahr. Nach dem Vollständigkeitssatz ist ein Satz beweisbar aus DLO gdw er in jedem abzählbaren Modell von DLO wahr ist. Deshalb beweist DLO entweder φ oder $\sim \varphi$, und somit ist DLO vollständig.

Unsere zweite Anwendung der Quantorenelimination betrifft die diskrete Ordnung der ganzen Zahlen $\langle \mathbb{Z}, \leq \rangle$.

Definition 8.8. *Die Axiome von DsLO (diskrete lineare Ordnung) entstehen aus den folgenden Formeln, indem alle freien Variablen mit Allquantoren abquantifizert werden:*
1. $x \leq x$
2. $x \leq y \wedge y \leq x \rightarrow x = y$
3. $x \leq y \wedge y \leq z \rightarrow x \leq z$
4. $x \leq y \vee y \leq x$

Sei $x < y$ *gdw* $x \leq y \wedge x \neq y$.
5. $\exists y \exists z (y < x < z \wedge \sim \exists w (y < w < x \vee x < w < z))$

Eine konservative Erweiterung DsLO* von DsLO entsteht dadurch, daß wir das Konstantensymbol 0, die zwei einstelligen Funktionssymbole S und P sowie die folgenden Axiome hinzufügen:

6*. $y = Px \leftrightarrow (y < x \wedge \sim \exists z (y < z < x))$
7*. $y = Sx \leftrightarrow (x < y \wedge \sim \exists z (x < z < y))$

Die variablenfreien Terme sind von der Form $F_1 F_2 \cdots F_n 0$, wobei jedes F_i entweder P oder S ist. Wenn t_1 und t_2 variablenfreie Terme sind, dann beweist DsLO* entweder $t_1 = t_2$, $t_1 < t_2$ oder $t_2 < t_1$, und deshalb ist DsLO* vollständig für atomare Sätze. Wir zeigen, daß DsLO* QE hat, und daher vollständig ist.

Wie im letzten Beweis müssen wir den Quantor einer mit DsLO* konsistenten Formel der Form $\exists x (u_1 R_1 u_2 \wedge u_2 R_2 u_3 \wedge \cdots \wedge u_{n-1} R_{n-1} u_n)$ eliminieren, wobei jedes R_i entweder $<$ oder $=$ ist. Wir können annehmen, daß das Funktionssymbol P nicht auftritt, indem wir S oft genug anwenden, um P zu eliminieren. Wir können auch annehmen, daß, wenn x sowohl in u_i als auch u_j, $i < j$, auftritt, weder 0 noch eine Variable ungleich x in u_k auftritt, $i < k < j$; anderenfalls ist unsere Formel zu einer Disjunktion von Formeln ohne x äquivalent. Weiterhin können wir annehmen, daß, wenn x in u_i auftritt, weder R_{i-1} noch R_i gleich $=$ ist; anderenfalls kann x wieder eliminiert werden. Nehmen wir nun an, daß x in u_1 auftritt; dann kann x eliminiert werden, da die Relation $u_i < u_{i+1}$ erfüllbar ist, wobei i minimal ist, so daß x in u_{i+1} nicht auftritt. Ähnlich kann x eliminiert werden, wenn es in u_n auftritt. Nehmen wir nun an, daß x genau in den Termen $u_i, \ldots, u_j$ auftritt, $1 < i \leq j < n$. Schreibe u_i in der Form $S^k x$ und u_j in der Form $S^l x$. Dann können wir x eliminieren, indem wir die Formel

$S^{l-k+1}u_{i-1} < u_{j+1}$ hinzufügen. Somit haben wir die gewünschte Quantorenelimination gezeigt.

Satz 8.9. *DsLO ist vollständig. Jeder Satz ist wahr in $\langle \mathbb{Z}, \leq \rangle$ gdw er beweisbar aus DsLO ist.*

Unsere dritte Anwendung der Quantorenelimination betrifft die Struktur $\mathfrak{N}_A = \langle \mathbb{N}, 0, S, <, + \rangle$ ohne Exponentiation und Multiplikation.

Definition 8.10. *Sei A_A die Theorie, die sich ergibt, indem wir die Axiome bezüglich $\cdot$ und E aus A_E entfernen, und sei Pres (= die Presburger-Arithmetik) die Theorie, die dadurch entsteht, daß wir zu A_A für jede Formel φ mit derfreien Variable x – und möglicherweise weiteren - die folgenden Induktionsaxiome hinzufügen:*

$$[\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(Sx))] \to \forall x \varphi(x).$$

Wir zeigen mittels Quantorenelimination, daß Pres vollständig ist.

Wir definieren Pres*, eine konservative Erweiterung von Pres, wie folgt: Seien $\equiv_n$ neue, binäre Prädikatssymbole für jedes $n \geq 2$. Dann ist Pres* gleich Pres mit den neuen Axiomen (wieder sind alle freien Variablen als mit $\forall$ abquantifiziert zu verstehen):

$$((*)_n) \qquad x \equiv_n y \leftrightarrow \exists z[(x + z = y \vee y + z = x) \wedge \exists w(z = \underbrace{w + w + \cdots + w}_{m}))].$$

Daher ist $x \equiv_n y$ gdw x und y kongruent modulo n sind. Die atomaren Sätze der Sprache von Pres* sind von der Form $t_1 < t_2$, $t_1 \equiv_n t_2$ oder $t_1 = t_2$, wobei t_1 und t_2 Terme aufgebaut aus $S, +$ und 0 sind. Wie im Falle von A_E ist solch ein Satz wahr gdw er beweisbar aus Pres* ist, und daher ist Pres* vollständig für atomare Sätze.

Deshalb folgt die Vollständigkeit von Pres aus der Quantorenelimination für Pres*. Sei $\varphi = \exists y(\beta_1 \wedge \cdots \wedge \beta_n)$ eine primitive Formel der Sprache von Pres*, in der jedes β_i atomar oder negatomar ist. Wir können annehmen, daß jedes β_i atomar ist: $\sim (t_1 = t_2)$, $\sim (t_1 < t_2)$ und $\sim (t_1 \equiv_m t_2)$ können durch $(t_1 < t_2 \vee t_2 < t_1)$, $(t_1 = t_2 \vee t_2 < t_1)$ bzw $(t_1 \equiv_m t_2 + S0 \vee t_1 \equiv_m t_2 + SS0 \vee \cdots \vee t_1 \equiv_m t_2 + S^{m-1}0)$ ersetzt werden; dann ist die gegebene primitive Formel äquivalent zu einer Disjunktion von primitiven Formeln $\exists y(\alpha_1 \wedge \cdots \wedge \alpha_m)$, in der jedes α_i atomar ist. Betrachten wir nun eine Formel letzterer Form. Wir können annehmen, daß y in jedem α_i auftritt und jedes α_i von einer der folgenden Formen ist:

$$\begin{array}{rcl} n_1 y + t & = & u, \\ n_2 y + t & \equiv_m & u, \\ n_3 y + t & < & u, \\ u & < & n_4 y + t, \end{array}$$

in denen y weder in t noch in u auftritt und ny eine Abkürzung für $y + y + \cdots + y$ (n mal) ist. Statt der vorstehenden Formeln schreiben wir:

$$\begin{array}{rcl} n_1 y & = & u - t, \\ n_2 y & \equiv_m & u - t, \\ n_3 y & < & u - t, \\ u - t & < & n_4 y, \end{array}$$

auch wenn $-$ kein Symbol unserer Sprache ist.

Wir multiplizieren jede dieser atomaren Formeln, so daß n_1, n_2, n_3 und n_4 gleich sind. Sei $n_i = n$ für jedes i, ersetzen wir ny durch x und füge die Formel „$x \equiv_n 0$" hinzu. Wenn $x = u - t$ auftritt, dann können wir x eliminieren, indem wir es durch $u - t$ ersetzen. Daher nehmen wir an, daß $x = u - t$ nicht auftritt, und erhalten eine Formel der Form:

$$\exists x[\bigwedge_{j<l} (r_j - s_j < x) \wedge \bigwedge_{i<k} (x < t_i - u_i) \wedge \bigwedge_{h<n} (x \equiv_{m_h} v_h - w_h)].$$

Wenn $n = 0$ ist, dann ist diese Formel äquivalent zu:

$$\begin{array}{rl} \displaystyle\bigwedge_{j<l, i<k} (r_j - s_j) + S0 < (t_i - u_i), & \qquad \text{wenn } l \neq 0, \\ \displaystyle\bigwedge_{i<k} 0 < (t_i - u_i), & \qquad \text{wenn } l = 0. \end{array}$$

Deshalb können wir annehmen, daß n ungleich 0 ist. Sei M die kleinste gemeinsame Vielfache (kgV) der m_h. Wenn $l = 0$ ist, dann besagt unsere Formel, daß es ein x kleiner als all die $(t_i - u_i)$ gibt, das kongruent zu $v_h - w_h$ mod m_h für jedes h ist. Wenn es aber solch ein x gibt, dann gibt es auch eines kleiner M. Es folgt, daß unsere Formel äquivalent zur folgenden Formel ist:

$$\bigvee_{m<M} [\bigwedge_{i<k} (S^m 0 < t_i - u_i) \wedge \bigwedge_{h<n} (S^m 0 \equiv_{m_h} v_h - w_h)].$$

Wenn $l \neq 0$, müssen wir $S^m 0$ durch $(r_j - s_j) + S^{m+1} 0$ ersetzen, da wir in die Intervalle $[(r_j - s_j) + 1, (r_j - s_j) + M]$ schauen müssen. Wir garantieren, daß diese Zahlen nicht negativ sind, indem wir das Paar $(r_l, s_l) = (0, S0)$ hinzufügen. Also erhalten wir die folgende Formel:

$$\begin{array}{l} \displaystyle\bigvee_{j \leq l} \bigvee_{m<M} [\bigwedge_{j' \leq l} (r_{j'} - s_{j'} < (r_j - s_j) + S^{m+1} 0) \\ \quad \displaystyle\wedge \bigwedge_{i<k} (r_j - s_j + S^{m+1} 0 < t_i - u_i) \wedge \bigwedge_{h<n} (r_j - s_j + S^{m+1} 0 \equiv_{m_h} v_h - w_h)]. \end{array}$$

Es kann gezeigt werden, daß die obigen Äquivalenzen nicht nur wahr sondern auch beweisbar aus Pres* sind. (Tatsächlich brauchen wir die Induktionsaxiome von Pres* nur für Formeln ohne Quantoren.) Deshalb hat Pres* QE.

SATZ 8.11. *Pres ist vollständig. Jeder* $\{0, S, <, +\}$*-Satz ist in der Struktur* $\langle \mathbb{N}, 0, S, <, + \rangle$ *wahr gdw er beweisbar aus Pres ist.*

Die Methode der Quantorenelimination kann auch benutzt werden, um vollständige Theorien für die Strukturen $\langle \mathbb{Z}, <, + \rangle$, $\langle \mathbb{Q}, <, + \rangle$, $\langle \mathbb{R}, <, +, \cdot \rangle$ und $\langle \mathbb{C}, +, \cdot \rangle$ zu liefern. Die Methode kann auch angewandt werden, um sowohl die Entscheidbarkeit der Theorien der Abelschen Gruppen, Booleschen Algebren, Äquivalenzrelationen, Wohlordnungen und endlichen Körper zu zeigen als auch eine Klassifikation der vollständigen Erweiterungen dieser Theorien zu geben.

2. Eine semantische Formulierung von Quantorenelimination

DEFINITION 8.12. *. Eine Theorie* T *ist* substrukturvollständig *gdw für alle Modelle* $\mathfrak{B}_0, \mathfrak{B}_1$ *von* T *mit gemeinsamer Substruktur* $\mathfrak{A}$ *gilt: Für alle* $a_1, \ldots, a_n \in |\mathfrak{A}|$*:*

$$((*)) \qquad \mathfrak{B}_0 \vDash \varphi(a_1, \ldots, a_n) \text{ gdw } \mathfrak{B}_1 \vDash \varphi(a_1, \ldots, a_n)$$

SATZ 8.13. *Sei* T *eine Theorie. Folgende Aussagen sind äquivalent:*

(a) T *ist Substrukturvollständig.*

(b) T *erlaubt QE.*

Beweis. (b) $\to$ (a): Die Gleichung $(*)$ gilt für eine quantorenfreie Formel φ, da $\mathfrak{B}_0 \vDash \varphi(a_1, \ldots, a_n)$ gdw $\mathfrak{A} \vDash \varphi(a_1, \ldots, a_n)$ gdw $\mathfrak{B}_1 \vDash \varphi(a_1, \ldots, a_n)$. Wenn T QE gestattet, folgt, daß $(*)$ für auch beliebige Formeln gilt.

(a) $\to$ (b): Sei $\varphi(x_1, \ldots, x_n)$ eine Formel. Seien $c_1, \ldots, c_n$ neue Konstantensymbole. Wir setzen

$$\Gamma(c_1, \ldots, c_n) = \{\psi(c_1, \ldots, c_n) \,|\, \psi \text{ ist quantorenfrei und } T \vdash \varphi \to \psi\}.$$

BEHAUPTUNG 8.14. $T \cup \Gamma(c_1, \ldots, c_n) \vdash \varphi(c_1, \ldots, c_n)$.

Beweis der Behauptung. Wenn nicht, sei $(\mathfrak{B}_0, b_1^0, \ldots, b_n^0)$ ein Modell von $T \cup \Gamma(c_1, \ldots, c_n) \cup \{\sim \varphi(c_1, \ldots, c_n)\}$. Sei $\mathfrak{A}$ die kleinste Substruktur von $\mathfrak{B}_0$, dessen Universum die b_i^0 enthält. Wir definieren die QF-Theorie von $\mathfrak{A}$ als die Theorie $\{\psi(c_1, \ldots, c_n) \,|\, \psi \text{ ist quantorenfrei}, \mathfrak{A} \vDash \psi(b_1^0, \ldots, b_n^0)\}$.

Dann hat $T \cup \{\varphi(c_1, \ldots, c_n)\} \cup$ QF-Theorie $\mathfrak{A}$ kein Modell: Wenn $(\mathfrak{B}_1, b_1^1, \ldots, b_n^1)$ ein solches Modell war, dann, da $(\mathfrak{B}_1, b_1^1, \ldots, b_n^1)$ ein Modell der QF-Theorie $\mathfrak{A}$ ist, können wir annehmen, daß $\mathfrak{A} \subseteq \mathfrak{B}_1$, $b_i^1 = b_i^0$ für jedes i. Nach Substrukturvollständigkeit $\mathfrak{B}_1 \vDash \sim \varphi(b_1^1, \ldots, b_n^1)$, Widerspruch.

Da $T \cup \{\varphi(c_1, \ldots, c_n)\} \cup$ QF-Theorie $\mathfrak{A}$ kein Modell hat, gibt es $\psi_1(c_1, \ldots, c_n)$, $\psi_2(c_1, \ldots, c_n), \ldots, \psi_m(c_1, \ldots c_n) \in$ QF-Theorie $\mathfrak{A}$, so daß $T \cup \{\psi_1(c_1, \ldots c_n), \ldots, \psi_m(c_1, \ldots, c_n)\} \vdash \sim \varphi(c_1, \ldots, c_n)$. Dann ist $\bigvee_{1 \le j \le m} \sim \psi_j(c_1, \ldots, c_n)$ Element von $\Gamma(c_1, \ldots, c_n)$, und daher $(\mathfrak{B}_0, b_1, \ldots, b_n) \vDash \bigvee_{1 \le j \le m} \sim \psi_j(c_1, \ldots, c_n)$; es folgt, daß $(\mathfrak{A}, b_1, \ldots, b_n) \vDash \bigvee_{1 \le j \le m} \sim \psi_j(c_1, \ldots, c_n)$, im Widerspruch zur Annahme, daß für jedes j $\psi_j \in$ QF-Theorie $\mathfrak{A}$.

Es folgt, daß es $\psi_1(c_1, \ldots c_n), \ldots, \psi_m(c_1, \ldots, c_n) \in \Gamma(c_1, \ldots, c_n)$ gibt, so daß $T \cup \{\psi_1(c_1, \ldots c_n), \ldots, \psi_m(c_1, \ldots, c_n)\} \vdash \varphi(c_1, \ldots, c_n)$. Dann $T \vdash \varphi \leftrightarrow \bigwedge_{1 \leq j \leq m} \psi_j$, und die letztere ist eine quantorenfreie Formel. $\square$

Es folgt leicht aus (b) $\rightarrow$ (a) des obigen Satzes, daß die Theorie DsLO keine QE hat.

KAPITEL 9

Anfänge einer Einführung in die Mengenlehre

Das Axiomensystem ZFC. ZFC: Zermelo, Fraenkel, und Choice.

Duden: Axiom: als absolut richtig anerkannter Grundsatz, gültige Wahrheit, die keines Beweises bedarf.

Axiom 0: Es gibt die leere Menge.

$$\exists x \forall y (y \notin x).$$

Axiom 1: Extensionalität (Ext). Mengen, die dieselben Elemente enthalten, sind gleich.

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

Axiom 2: Fundierung (Fund). Die $\in$-Relation ist fundiert, d.h., jede nicht leere Menge hat ein $\in$-minimales Element,

$$\forall x (\exists y \in x \to \exists y \in x (\neg \exists z (z \in y \wedge z \in x)))$$

Axiom 3: Aussonderungsschema (Comprehension) (Aus). Für alle $\varphi \in \mathscr{L}(\in)$ mit $\mathrm{fr}(\varphi) \subseteq \{x, z, w_1, w_2, \dots, w_n\}$ gilt folgendes

$$\forall z \forall w_1 \dots \forall w_n \exists y \forall x (x \in y \leftrightarrow x \in z \wedge \varphi).$$

Axiom 4: Paarmengenaxiom (Pairing) (Paar)

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

Axiom 5: Vereinigungsmengenaxiom (Union) (Verein)

$$\forall F \exists A \forall Y \forall x (x \in Y \wedge Y \in F \to x \in A).$$

Axiom 6: Ersetzungsschema (Replacement) (Ers).

$\exists! x$ heißt „es gibt genau ein x'.

Für alle $\varphi \in \mathscr{L}(\in)$ mit $\mathrm{fr}(\varphi) \subseteq \{x, y, A, w_1, w_2, \dots, w_n\}$ gilt folgendes

$$\forall A \forall w_1 \dots \forall w_n (\forall x \in A \exists! y \varphi \to \exists Y \forall y (\exists x \in A \varphi \leftrightarrow y \in Y)).$$

Axiom 7: Unendlichkeitsaxiom (Infinity) (Inf)

Sei x eine Menge. Nach (Aus) gibt es $\emptyset = \{z \in x \mid z \neq z\}$.

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

Axiom 8: Potenzmengenaxiom (Pot) powerset

Sei $x \subseteq y$ eine Abkürzung für $\forall z \in x (z \in y)$

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

Axiom 9: Auswahlaxiom (Axiom of Choice)

$$\forall \mathcal{F}(\forall Y \in \mathcal{F} Y \neq \emptyset \rightarrow \exists f \colon \mathcal{F} \rightarrow \bigcup \mathcal{F} \forall Y \in \mathcal{F} f(Y) \in Y).$$

Bemerkung: Warum akzeptiert man das Fundierungsaxiom?

Es gibt zwei Gründe: Wir stellen uns vor, daß die Mengen stufenweise aufgebaut werden, daß die Elemente einer Menge Mengen auf niedrigeren Stufen sind. Es ist vernünftig, anzunehmen, daß die Stufen wohlgeordnet sind, d.h., daß jede Menge von Stufen eine kleinste Stufe enthält. Hieraus folgt die Fundierung; da wir für ein gegebenes nicht leeres x ein $y \in x$ wählen können, das in der kleinstmöglichen Stufe auftritt (unter dem Auftreten alle Elemente aus x). Man kann zeigen, daß jedes Modell von ZF ohne Fundierung in ein Modell von ZF überführt werden kann, indem man einfach zur fundierten Unterklasse übergeht (s.u.). Deshalb ist das Hinzufügen des Fundierungsaxioms zu den anderen ZF Axiomen von der Widerspruchsfreiheit her unproblematisch. Die Fundierung impliziert den Satz von von Neumann, der besagt, daß jede Menge Element einer aus der leeren Menge durch Iteration der Potenzmengenoperation entstandenen Menge ist.

0.1. Konsequenzen der Axiome. Wir haben das Ersetzungsschema in einer starken Form formuliert: Wir fordern genau die Bildmenge, nicht eine Obermenge des Bildes. Der Grund ist, daß wir nur mit einem Schema unter den Axiomen, nämlich mit dem Ersetzungsschema, weiter arbeiten möchten.

PROPOSITION 9.1. *Das Aussonderungsprinzip folgt aus den restlichen Axiomen.*

Beweis: Wenn $\varphi(x)$ für kein $x \in a$ gilt, dann folgt das Resultat aus dem Axiom über die leere Menge. Sonst wählen wie $a_0 \in x$ so daß $\varphi(a_0)$ und definieren die Funktion F wie folgt:

$F(x) = x$ wenn $x \in a$ und $\varphi(x)$, sonst $F(x) = a_0$. Wir wenden das Ersetzungsschema auf die Formel, die F definiert, an, um die Bildmenge von F auf a zu erhalten. Die ist genau die gewünsche Menge $\{x \in a \mid \varphi(x)\}$. □

Wir betrachten nun einige Details

DEFINITION 9.2. *Die Menge $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$ heißt das geordnete Paar von x und y.*

Hat das so definierte geordnete Paar die Eigenschaft, die wir von einem geordneten Paar erwarten?

BEHAUPTUNG 9.3.

$$\forall x \forall y \forall x' \forall y' (\langle x, y\rangle = \langle x', y'\rangle \leftrightarrow (x = x' \wedge y = y'))$$

DEFINITION 9.4. *Eine Menge f ist eine Funktion gdw f eine Menge von Paaren ist und folgendes gilt*

$$\forall x \in \mathrm{dom}(f)\exists! y(\langle x, y\rangle \in f).$$

Der Definitionsbereich (domain) von R ist $\mathrm{dom}(R) = \{x \in \bigcup\bigcup R \mid \exists y\langle x, y\rangle \in R\}$. Wir schreiben Bildmengen wie folgt: $f''C = f[C] = \mathrm{rge}(f \restriction C) = \{f(x) \mid x \in C\}$. Falls $\mathrm{dom}(f) \supseteq C \cup \{C\}$, kann $f(C) \neq f''(C)$ sein.

$A \times B = \{\langle x, y\rangle \mid x \in A \wedge y \in B\}$ ist eine Menge aus Aus und Ers und Verein.

DEFINITION 9.5. *Eine lineare (auch: totale) Ordnung ist ein Paar $\langle A, R\rangle$, so daß R die Menge A linear ordnet, d.h., daß R eine Relation ist, die die folgenden Eigenschaften hat*

Transitivität: $\forall x, y, z \in A(xRy \wedge yRz \rightarrow xRz)$

Irreflexivität: *(auch Antisymmetrie)* $\forall x \in A \sim xRx.$

Trichotomie: *(Linearität, Konnexität, Totalität)* $\forall x, y \in A(xRy \vee yRx \vee x = y).$

DEFINITION 9.6. *$\langle A, R\rangle$ heißt Wohlordnung, gdw $\langle A, R\rangle$ eine Ordnung ist, in der jede nicht leere Teilmenge von A ein R-minimales Element hat.* $\forall y((y \subseteq A \wedge \exists x \in y) \rightarrow \exists z \in y(\forall u \in y(\neg uRz)))$

DEFINITION 9.7. *Eine Menge x heißt Ordinalzahl (kurz On) gdw x transitiv ist und $\langle x, \in\rangle$ eine Wohlordnung ist.*

Unser Ziel ist die Klassifikation aller Wohlordnungen bis auf Isomorphie. Man denke daran, daß in der Mathematik Klassifikationsaufgaben im Allgemeinen immense Unterfangen sind. Zum Glück wird dies bei den Wohlordnungen nicht der Fall sein.

Eine Isomorphieklasse ist eine Klasse isomorpher Strukturen. Jede Isomorphieklasse, außer die zur leeren Struktur, ist eine echte Klasse. Da man zwischen isomorphen Strukturen nicht unterscheiden möchte oder kann, tut man so, als ob sie identisch wären, und nennt das dann Arbeiten „bis auf Isomorphie" oder „modulo Isomorphie".

DEFINITION 9.8. *Sei $\langle A, R\rangle$ ein geordnetes Paar, $x \in A$. Die Vorgängermenge von x in $\langle A, R\rangle$ ist* $\mathrm{pred}(A, x, R) = \{y \in A \mid yRx\}$.

Diese Festsetzung wird besonders für Ordnungen, lineare Ordnungen und Wohlordnungen $\langle A, R\rangle$ gebraucht.

Wir erarbeiten nun ein Repräsentantensystem für die Isomorphieklassen

$$(\langle A, R\rangle / \cong) = \{\langle B, S\rangle \mid \langle A, R\rangle \cong \langle B, S\rangle\}, \langle A, R\rangle \text{ Wohlordnung.}$$

Wir werden sehen, daß es Klassen-viele Isomorphieklassen gibt.

LEMMA 9.9. *Wenn $\langle A, R\rangle$ eine Wohlordnung ist, dann ist für alle $x \in A$*

$$\langle A, R\rangle \not\cong \langle \mathrm{pred}(A, x, R), R\rangle.$$

Beweis: Angenommen, $f\colon A \to \mathrm{pred}(A,x,R)$ wäre ein Isomorphismus. Da $x \in A \setminus \mathrm{pred}(A,x,R)$, ist $f(x) \neq x$. Die Menge $\{y \mid f(y) \neq y\}$ ist also nicht leer und hat ein kleinstes Element z. Dann ist für alle $z' R z$, $f(z') = z'$. Wegen der Injektivität von f ist daher $zRf(z)$. Dann gilt aber wegen der Ordnungstreue auch für alle u mit zRu, daß $f(z)Rf(u)$. Also ist $z \notin \mathrm{rge}(f)$, im Widerspruch zur Surjektivität von f. □

Frage: Wo bricht der Beweis dieses Lemmas z.B. für $\langle \mathbb{Q}, < \rangle$ und $x \in \mathbb{Q}$ zusammen?

Satz 9.10. *(Der Trichotomiesatz für Wohlordnungen). Seien $\langle A,R\rangle$ und $\langle B,S\rangle$ Wohlordnungen. Dann gilt*

(a) $\langle A,R\rangle \cong \langle B,S\rangle$ *oder*

(b) $(\exists x \in A)\langle \mathrm{pred}(A,x,R),R\rangle \cong \langle B,S\rangle$ *oder*

(c) $(\exists y \in B)\langle A,R\rangle \cong \langle \mathrm{pred}(B,y,S),S\rangle$.

Beweis: Wir setzen

$$f = \{\langle u,v\rangle \in A \times B \mid \langle \mathrm{pred}(A,u,R),R\rangle \cong \langle \mathrm{pred}(B,v,S),S\rangle\}.$$

1. Zu jedem $u \in \mathrm{dom}(f)$ gibt es genau ein v mit $\langle u,v\rangle \in f$. Sonst: Sei vSv',

$$\begin{aligned} g\colon \langle \mathrm{pred}(A,u,R),R\rangle &\cong \langle \mathrm{pred}(B,v,S),S\rangle, \\ g'\colon \langle \mathrm{pred}(A,u,R),R\rangle &\cong \langle \mathrm{pred}(B,v',S),S\rangle. \end{aligned}$$

Dann ist $g' \circ g^{-1}\langle \mathrm{pred}(B,v,S),S\rangle \cong \langle \mathrm{pred}(B,v',S),S\rangle$, im Widerspruch zu Lemma 9.9.

2. $\forall u \in \mathrm{dom}(f)\forall u' Ru(u' \in \mathrm{dom}(f))$, da man die Einschränkung des Zeugen $g\colon \langle \mathrm{pred}(A,u,R),R\rangle \cong \langle \mathrm{pred}(B,v,S),S\rangle$ auf $\mathrm{pred}(A,u',R)$ nehmen kann.

3. $\forall v \in \mathrm{rge}(f)\forall v' Sv(v' \in \mathrm{rge}(f))$, da man die Einschränkung des Zeugen $g\colon \langle \mathrm{pred}(A,u,R),R\rangle \cong \langle \mathrm{pred}(B,v,S),S\rangle$ auf $(g^{-1})''\mathrm{pred}(B,v',S)$ nehmen kann.

4. Echte Teilmengen u von Wohlordnungen $\langle C,T\rangle$, die gegenüber Vorgängern abgeschlossen sind, sind von der Form $\mathrm{pred}(C,x,T)$ für $x = \min C \setminus u$, wobei das Minimum bezüglich T gebildet wird.

Nun gibt es also für $\mathrm{dom}(f)$ und für $\mathrm{rge}(f)$ jeweils zwei Möglichkeiten, und wir gelangen zur folgenden Fallunterscheidung:

1. Fall: $\mathrm{dom}(f) = A$, $\mathrm{rge}(f) = B$. Dann rechnet man leicht nach, daß f ein Isomorphismus von $\langle A,R\rangle$ auf $\langle B,S\rangle$ ist. Wir erhalten also Disjunktionsglied (a) des Satzes.

2. Fall: $\mathrm{dom}(f) = \mathrm{pred}(A,x,R)$ für ein $x \in A$, $\mathrm{rge}(f) = B$. Dann rechnet man leicht nach, daß f ein Isomorphismus von $\langle \mathrm{pred}(A,x,R),R\rangle$ auf $\langle B,S\rangle$ ist. Wir erhalten also Disjunktionsglied (b) des Satzes.

3. Fall: $\mathrm{dom}(f) = A$ und $\mathrm{rge}(f) = \mathrm{pred}(B, y, S)$ für ein $y \in B$. Dann rechnet man leicht nach, daß f ein Isomorphismus von $\langle A, R\rangle$ auf $\langle \mathrm{pred}(B, y, S), S\rangle$ ist. Wir erhalten also Disjunktionsglied (c) des Satzes.

4. Fall: $\mathrm{dom}(f) = \mathrm{pred}(A, x, R)$ für ein $x \in A$, $\mathrm{rge}(f) = \mathrm{pred}(B, y, S)$ für ein $y \in B$. Dann ist aber $\langle x, y\rangle \in f$, wie durch $f \cup \{\langle x, y\rangle\}$ bezeugt wird, im Gegensatz zu $x \notin \mathrm{dom}(f) = \mathrm{pred}(A, x, R)$. Widerspruch. □

Definition 9.11. *Eine Menge x heißt transitiv gdw $\forall y \in x(\forall z \in y(z \in x))$.*

Beipiele: $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.
Gegenbeispiele: $\{\{\emptyset\}\}$, $x \neq \emptyset$, dann ist $\{x\}$ nicht transitiv.

Definition 9.12. *Eine Menge x heißt Ordinalzahl (kurz On) gdw x transitiv ist und $\langle x, \in\rangle$ eine Wohlordnung ist.*

Satz 9.13. *Starrheit von transitiven Mengen. Wenn T und U transitive Mengen sind und f ein Isomorphismus von $(T, \in)$ auf $(U, \in)$ ist, dann ist f die Identität.*

Beweis: Wenn nicht, gibt es ein $\in$-minimals a, so daß $f(a) \neq a$. Aufgrund der Minimalität ist $f(b) = b$ für alle $b \in a$. Wir haben $a \subseteq f(a) = \{f(b) \mid b \in^T a\} = \{b \mid b \in a\}$, da T transitiv ist. Da U transitiv ist, ist, $b \in f(a) \to b \in U \cap f(a) \to \exists a' \in ab = f(a') = a'$, also $f(a) \subseteq a$. Wir haben $f(a) = a$, im Widerspruch zur Wahl von a. □

Satz 9.14. *Wenn x und y Ordinalzahlen sind, dann ist $x = y$ oder $x \in y$ oder $y \in x$.*

Beweis: Dies folgt aus dem Trichotomiesatz für die Wohlordnungen und dem Punkt 2. dieses Satzes: Es gilt $\langle x, \in\rangle \cong \langle y, \in\rangle$ oder $(\exists z \in x\ (\langle z, \in\rangle \cong \langle y, \in\rangle))$ oder $(\exists z \in y\ (\langle x, \in\rangle \cong \langle z, \in\rangle))$. Nun ersetzen wir nach dem vorigen Punkt die Isomorphismen, die ja nach obigem Satz Identitäten sind, durch die Gleichheiten und erhalten $x = y$ oder $y = z \in x$ oder $x = z \in y$. □

Konventionen: Wir schreiben kleine griechische Buchstaben für Ordinalzahlen. Wir schreiben α statt $\langle \alpha, \in\rangle$, wenn dies nicht zu Mißverständnissen führt. Außerdem kürzen wir Quantifizierungen über Ordinalzahlen wie folgt ab: $\forall \alpha \varphi(\alpha)$ steht für $\forall x(xOn \to \varphi(x))$. $\exists \alpha \varphi(\alpha)$ steht für $\exists x(xOn \wedge \varphi(x))$. Wir schreiben manchmal $\alpha < \beta$ für $\alpha \in \beta$ und $\alpha \leq \beta$ für $\alpha < \beta \vee \alpha = \beta$. Wir benützen auch die umgekehrten Ordnungssymbole.

Satz 9.15. *1. Wenn x eine Ordinalzahl ist und $y \in x$ ist, dann ist auch y eine Ordinalzahl.*

2. Wenn C eine nicht leere Menge von Ordinalzahlen ist, dann gibt es ein $x \in C$, so daß $\forall y \in x(y \notin C)$.

Definition 9.16. *Zu jeder On* α *definieren wir ihren ordinalen Nachfolger (successor)* $S(\alpha) = \alpha \cup \{\alpha\}$. *Allgemein setzen wir* $S(x) = x \cup \{x\}$.

$S(\alpha)$ ist eine Ordinalzahl.

Definition 9.17. *Dies sind unendlich viele Definitionen!* $0 := \emptyset$, $1 = S(0)$, $2 = S(1)$, *usf.*

Wir haben also $1 = \{0\}$. $2 = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$, $3 = \{0, 1, 2\}$, $4 = \{0, 1, 2, 3\}$, usf. Die sind die sogenannten von Neumannschen natürlichen Zahlen.

Definition 9.18. *1.* α *heißt Nachfolgerordinalzahl gdw* $\exists \beta(\alpha = S(\beta))$.
2. α *heißt Limesordinalzahl gdw* α *keine Nachfolgerordinalzahl und nicht* $\emptyset$ *ist. Wir schreiben* $\lim(\alpha)$ *für „*α *ist eine Limesordinalzahl".*

Definition 9.19. α *ist eine natürliche Zahl gdw* $\forall \beta \leq \alpha(\beta = 0 \vee \beta$ *Nachfolger*$)$.

Nun berufen wir uns auf das Unendlichkeitsaxiom (Inf), das sagt

$$\exists x(0 \in x \wedge \forall y \in x S(y) \in x).$$

Definition 9.20. *Sei* x *wie in (Inf). Dann ist*

$$\omega = \{z \in x \,|\, z \textit{ ist eine natürliche Zahl}\}$$

Satz 9.21. *Zu jeder Wohlordnung* $\langle A, R\rangle$ *gibt es genau eine Ordinalzahl* x, *so daß* $\langle A, R\rangle \cong \langle x, \in\rangle$.

Beweis: Die Eindeutigkeit folgt aus Punkt 2. des Satzes 9.15. Wir bilden die folgende Menge:

$$B = \{a \in A \,|\, \exists x(xOn \wedge \langle \mathrm{pred}(A, a, R), R\rangle \cong \langle x, \in\rangle)\},$$

und bilden eine Funktion $f \colon B \to On$ mit der Definition, daß $f(a)$ das eindeutig bestimmte x ist, so daß $\langle \mathrm{pred}(A, a, R), R\rangle \cong \langle x, \in\rangle$. Nach dem Ersetzungsaxiom ist $\mathrm{rge}(f)$ ein Menge. Man rechnet leicht nach, daß $\forall x \in \mathrm{rge}(f) \, \forall y \in x(y \in \mathrm{rge}(f))$. Nach dem vorigen Lemma ist $\mathrm{rge}(f)$ eine Ordinalzahl. Wir behaupten daß $B = A$. B ist eine Teilmenge von A, die gegen R-Vorgänger abgeschlossen ist. Falls $B \neq A$, dann sei b das R-minimale Element von $A \setminus B$. Dann ist aber f ein Zeuge für einen Isomorphismus $\langle \mathrm{pred}(A, b, R), R\rangle \cong \langle z, \in\rangle$, und somit $b \in B$, Widerspruch. $\square$

Satz 9.22. *Der Satz über die transfinite Induktion, hier in der Formulierung mit einer Klassenvariablen* X.
Sei $X \subseteq On$ *und sei* $0 \in X$ *und sei für alle* $\alpha \in X$ *auch* $S(\alpha) \in X$ *und sei für alle Limesordinalzahlen* $\lambda \subseteq X$ *auch* $\lambda \in X$. *Dann ist* $X = On$.

Beweis: Wir nehmen an, daß es ein $\alpha \in On \setminus X$ gäbe. Dann gibt es ein minimales Element in der Menge $\alpha \cap (On \setminus X)$, sei dieses β. Nach den Voraussetzungen über X ist $\beta \neq 0$. β kann auch kein Nachfolger sein, da X unter Nachfolgerbildung abgeschlossen ist. Und falls schließlich β eine Limesordinalzahl wäre, hätten wir $\beta \subseteq X$ und daher nach Voraussetzung $\beta \in X$. Also ist $X = On$. □

Definitionen über transfinite Induktion heißen transfinite Rekursion und werde nun begründet. Wieder arbeiten wir mit Klassenvariablen, die für Ausdrücke in der Sprache der ersten Stufe stehen, so daß $\forall x \exists! y \varphi$ gilt für geignetes φ, das die Definition der Operation F ist. Ein geeignetes anderes ψ, das im Beweis erst aufgebaut wird, wird die Definition der Operation G sein.

Definition 9.23. *Ein Klasse G von Paaren heißt Operation auf D gdw $\forall x \in D \exists! y(\langle x, y\rangle \in G)$. Wir schreiben $G\colon D \to \mathbf{V}$.*

Satz 9.24. *Der Satz über die transfinite Rekursion. Für $F\colon \mathbf{V} \to \mathbf{V}$ gibt es ein eindeutig bestimmtes $G\colon On \to \mathbf{V}$ so daß*

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

Beweis: Zunächst zeigen wir die Eindeutigkeit von G. Seien G_1, G_2 zwei Klassen, die den Rekursionsbedingungen genügen. Dann gilt $G_1(0) = F(\emptyset) = G_2(0)$, und, wenn $G_1 \restriction \alpha = G_2 \restriction \alpha$, dann ist $G_(\alpha) = F(G_1 \restriction \alpha) = F(G_2 \restriction \alpha) = G_2(\alpha)$. Nach dem Satz über die transfinite Induktion ist daher $G_1 = G_2$.

Nun zur Existenz: $g \in \mathbf{V}$ heißt δ-Approximation gdw $\mathrm{dom}(g) = \delta \in On$ und $\forall \alpha \in \delta (g(\alpha) = F(g \restriction \alpha))$. Für je zwei Approximationen, sagen wir, für eine δ-Approximation g und eine δ'-Approximation g', zeigt man durch Induktion über $\alpha < \delta \cap \delta'$, daß $g \restriction \delta \cap \delta' = g' \restriction \delta \cap \delta'$. Danach zeigt man durch transfinite Induktion, daß $\forall \delta (\exists \delta\text{-Approximation } g)$. Zum Schluß definiert man $G(\alpha) = g(\alpha)$ für eine beliebige δ-Approximation g, so daß $\delta > \alpha$. □

Definition 9.25. *Für jedes α definieren wir induktiv über On:*

$$\begin{aligned} &\alpha + 0 = \alpha, \\ &\alpha + (S(\beta)) = S(\alpha + \beta), \\ &\alpha + \lambda = \sup\{(\alpha + \beta) \mid \beta \in \lambda\}, \ \textit{für } \lim(\lambda). \end{aligned}$$

Definition 9.26. *Für jedes α definieren wir induktiv über On:*

$$\begin{aligned} &\alpha \cdot 0 = 0, \\ &\alpha \cdot (S(\beta)) = \alpha \cdot \beta + \alpha, \\ &\alpha \cdot \lambda = \sup\{(\alpha \cdot \beta) \mid \beta \in \lambda\}, \ \textit{für } \lim(\lambda). \end{aligned}$$

Warnung: Auch $\cdot$ ist nicht kommutativ, und das Distributivgesetz gilt nur von rechts.

$$2 \cdot \omega = \omega \neq \omega \cdot 2 = \omega + \omega,$$
$$(1+1) \cdot \omega = \omega \neq \omega + \omega.$$

Definition 9.27. *ZF*$^-$. *Die von Neumann Hierarchie.*
$V_0 = \emptyset$.
$V_{\alpha+1} = \mathscr{P}(V_\alpha)$.
$V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$ *für* $\lim(\lambda)$.
$\mathbf{WF} = \bigcup\{V_\alpha \,|\, \alpha\ On\}$.

Lemma 9.28. *1. Alle* V_α *sind transitiv und fundiert.*
2. $\alpha < \beta \to V_\alpha \subseteq V_\beta$.

Beweis: 1. Induktiv über α. Für $\alpha = 0$ und für den Limesschritt ist nichts zu zeigen für die Transitivität. Sei $\beta = \alpha + 1$, und sei $x \in \mathscr{P}(V_\alpha)$. Sei $y \in x$. Dann ist $y \in x \subseteq V_\alpha$. Da V_α transitiv ist, ist $y \subseteq V_\alpha$. Also ist $y \in \mathscr{P}(V_\alpha) = V_{\alpha+1}$.

Für die Fundiertheit: Man hat also $\mathrm{th}(V_\alpha) = V_\alpha$, und $\emptyset$ als $\in$-minimales Element.

2. Bei festem α induktiv über β. Der Fall $\beta = \alpha$ und der Fall $\lim(\beta)$ sind klar. Sei $\beta = \gamma + 1$. $V_\alpha \subseteq V_\gamma \in V_\beta$. Da V_β transitiv ist, ist $V_\alpha \subseteq V_\beta$. $\square$

Satz 9.29. *ZF. Prinzip der* $\in$*-Induktion.*

$$(\varphi(\emptyset) \wedge (\forall x((\forall y \in x\varphi(y)) \to \varphi(x)) \to \forall z\varphi(z).$$

Beweis: Sei z ein $\in$-minimales Element von $\{u \,|\, \neg\varphi(u)\}$. Wenn dies eine Klasse sein sollte, dann schneide man erst in eine Menge hinein: Man nehme u_0 so daß $\neg\varphi(u_0)$ und suche mit dem Fundierungsaxiom ein $\in$-Minimum in $\{u \in u_0 \cup \{u_0\} \,|\, \neg\varphi(u)\}$. Dann gilt $\forall y \in x\varphi(y)$. Also gilt $\varphi(z)$. Widerspruch. $\square$

Satz 9.30. *Der Satz von von Neumann. ZF*$^-$. *Fund* $\leftrightarrow \mathbf{V} = \mathbf{WF}$.

Beweis: $\to$: Durch $\in$-Induktion über $x \in \mathbf{V}$. Sei $\forall y \in x \exists \alpha_y y \in V_{\alpha_y}$. Dann ist $\forall y \in xy \in V_{\sup\{\alpha_y \,|\, y \in x\}}$ nach dem Lemma über das Aufsteigen der V_α. Also ist $x \subseteq V_{\sup\{\alpha_y \,|\, y\in x\}}$ und somit $x \in V_{\sup\{\alpha_y \,|\, y\in x\}+1}$.
$\leftarrow$: Lemma 9.28. $\square$

0.2. Kardinalzahlen.

Satz 9.31. *Der Wohlordnungssatz, Zermelo 1904. Auf der Basis von ZF gilt: AC'* $\leftrightarrow \forall A \exists R(\langle A, R\rangle$ *Wohlordnung).*

Beweis. $\leftarrow$. Sei $\bigcup \mathcal{F}$ via R wohlgeordnet. Dann ist $f(Y) = \min_R(Y)$ eine gewünschte Auswahlfunktion.

$\rightarrow$ Sei A gegeben. Sei $h\colon \mathcal{P}(A) \setminus \{0\} \rightarrow A$ eine Auswahlfunktion auf $\mathcal{P}(A)$. Nun definieren wir durch transfinite Rekursion eine Funktion $g\colon (\beta, \in) \rightarrow A$ durch $g(\alpha) = h(A \setminus g''\alpha)$, falls $g''\alpha \neq A$ g ist injektiv, und daher gibt es ein β so daß $g''\beta = A$. Nun setzen wir für $a, b \in A$, $aRb \leftrightarrow g^{-1}(a) \in g^{-1}(b)$. $\square$

Korollar 9.32. *(AC) Für jedes X gibt es eine Ordinalzahl α und eine Bijektion $f\colon X \rightarrow \alpha$.*

Definition 9.33. *Wenn A wohlgeordnet werden kann, dann sei*

$$|A| = \min\{\alpha \mid \alpha \sim A\}$$

die Mächtigkeit oder Kardinalität (size, cardinality) von A.

Konvention: Wir verwenden $|A|$ nur für Mengen A, die wohlgeordnet werden können. Unter AC sind dies alle Mengen.

Definition 9.34. *α ist eine Kardinalzahl gdw $|\alpha| = \alpha$.*

Nach Definition von $|\alpha|$ ist also $\forall \beta < |\alpha| (\beta \not\sim \alpha)$.

Satz 9.35. *(ZF$^-$ – P). Der Satz von Cantor, Schröder, Bernstein , hier mit dem Beweis von Dedekind 1887.*

$$A \preceq B \wedge B \preceq A \rightarrow A \sim B.$$

Beweis: Dies wird mit Spiegeln gezeigt. Seien $f\colon A \rightarrow B$ and $g\colon B \rightarrow A$ beide injektiv.

Wir setzen $C_0 = A \setminus \mathrm{rge}(g)$. $C_{n+1} = g''f''C_n$

Nun definieren wir $h\colon A \rightarrow B$ durch

$$h(x) = \begin{cases} f(x) & x \in \bigcup_{n<\omega} C_n, \\ g^{-1}(x) & x \in A \setminus \bigcup_{n<\omega} C_n. \end{cases}$$

Dies ist wohldefiniert, da $x \in \mathrm{rge}(g)$, wenn $x \notin C_0$.

Nun zeigen wir: h ist injektiv. Beweis: Sei $x \neq x'$ gegeben. Wenn x' und x im selben Ast der Fallunterscheidung liegen, dann ist nichts zu zeigen, da f injektiv ist, und g funktional ist, also g^{-1} immer injektiv ist.

Sei also $x \in C_m$ and $x' \notin \bigcup_{n<\omega} C_n$. Dann ist $f(x) \in f''C_m$. Andererseits ist $h(x') = g^{-1}(x') \notin f''C_m$, denn sonst wäre $x' \in g''f''C_m = C_{m+1}$.

Nun zeigen wir: h ist surjektiv.

Sei $y \in B$. Falls $y \in \bigcup_{n<\omega} f''C_n$. Dann ist $y \in \mathrm{rge}(h)$. Falls $y \notin \bigcup_{n<\omega} f''C_n$. Dann ist $g(y) \notin \bigcup_{n<\omega} C_{n+1}$ und $g(y) \notin C_0$. Dann ist $h(g(y)) = g^{-1}(g(y)) = y$.
$\square$

Geschichte des Cantor-Schröder-Bernstein-Satzes: Vorgeschlagen wurde der Satz von Cantor, doch Cantor verwendete AC zum Beweis. Ernst Schröder kündigte den Satz 1896 an, und veröffentlichte 1898 einen unvollständigen Beweis. 1898 veröffentlichte Felix Bernstein in einem Buch von Borel den ersten vollständigen Beweis ohne Benutzung des Auswahlaxioms.

Später stelle sich heraus, daß der Satz schon 1887 von Richard Dedekind bewiesen worden war.

SATZ 9.36. *ZF^-. Der Satz von Cantor.* $x \prec \mathscr{P}(x)$.

Beweis: Sei $f : x \to \mathscr{P}(x)$. Wir zeigen, daß f nicht surjektiv ist. Dies genügt, denn es ist $x \preceq \mathscr{P}(x)$, und wenn auch $\mathscr{P}(x) \preceq x$ wäre, dann gäbe es nach dem Satz von Cantor Schröder Bernstein 9.35 eine Bijektion, also zumindest eine Surjektion von x auf $\mathscr{P}(x)$. Wir bilden

$$u = \{y \in x \mid y \notin f(y)\} \in \mathscr{P}(x).$$

Dann gibt es kein $y \in x$, so daß $f(y) = u$: Denn wäre $f(y) = u$, dann hätte man $y \in u \leftrightarrow y \notin f(y) = u$.

Wenn man AC hinzunimmt, dann braucht man den Cantor Schröder Bernstein nicht zu zitieren, denn AC liefert dann an jener Stelle die gewünschte Bijektion. □

Es folgt, daß es keine größte Kardinalzahl gibt und daß jede Menge eine eindeutig bestimmte Mächtigkeit hat.

DEFINITION 9.37. *ZF^-. 1. $\alpha^+ = |\alpha|^+$ ist die kleinste Kardinalzahl $> \alpha$.*
2. κ heißt Nachfolgerkardinalzahl gdw $\exists \alpha < \kappa(\kappa = \alpha^+)$.
3. κ heißt Limeskardinalzahl, gdw $\kappa \neq \omega$ und κ keine Nachfolgerkardinalzahl ist.

DEFINITION 9.38. *$\aleph_\alpha = \omega_\alpha$ wird durch transfinite Induktion über α definiert:*
1. $\aleph_0 = \omega_0 = \omega$,
2. $\aleph_{\alpha+1} = \omega_{\alpha+1} = (\aleph_\alpha)^+$,
3. $\aleph_\lambda = \bigcup\{\aleph_\alpha \mid \alpha < \lambda\}$ für $\lim(\lambda)$.

Diese sind alle unendlichen Kardinalzahlen. Für welches α ist $|\mathscr{P}(\omega)| = \aleph_\alpha$?

DEFINITION 9.39. *1. $\kappa \oplus \lambda = |\kappa \times \{0\} \cup \lambda \times \{1\}|$.*
2. $\kappa \otimes \lambda = |\kappa \times \lambda|$.

LEMMA 9.40. *$\forall n, m < \omega$ $n \oplus m = n + m < \omega$, $m \otimes n = m \cdot n < \omega$.*

SATZ 9.41. *(Hessenberg, um 1900) ZF^- – P. Für jede unendliche Kardinalzahl ist $\kappa \otimes \kappa = \kappa$.*

Beweis: Induktiv über κ. Gelte die Behauptung schon für alle unendlichen Kardinalzahlen $\lambda < \kappa$, und sei κ unendlich. Dann ist nach Induktionsvoraussetzung, bzw. für endliche α nach Lemma 9.40, für alle $\alpha < \kappa$,

$$|\alpha \times \alpha| = |\alpha| \otimes |\alpha| < \kappa.$$

Nun definieren wir $\lhd$ auf $\kappa \times \kappa$ durch $\langle \alpha, \beta \rangle \lhd \langle \gamma, \delta \rangle$ gdw

$$\max(\alpha, \beta) < \max(\gamma, \delta) \vee$$
$$(\max(\alpha, \beta) = \max(\gamma, \delta) \wedge (\alpha < \gamma \vee (\alpha = \gamma \wedge \beta < \delta)))$$

Jedes $\langle \alpha, \beta \rangle \in \kappa \times \kappa$ hat nun nach grober Abschätzung (die Identität als Injektion genügt, sie ist nicht ordnungstreu) wenige Vorgänger in der Ordnung $\lhd$: $|\mathrm{pred}(\kappa \times \kappa, \langle \alpha, \beta \rangle, \lhd)| \leq |(\max(\alpha, \beta) + 1) \times (\max(\alpha, \beta) + 1)| = |\max(\alpha, \beta) + 1| \odot |\max(\alpha, \beta) + 1| < \kappa$.

Da $\lhd$ eine Wohlordnung ist, in der alle Vorgängermengen von Mächtigkeit echt kleiner κ sind, ist $\mathrm{type}(\kappa \times \kappa, \lhd) \leq \kappa$. Also ist $|\kappa \times \kappa| \leq \kappa$.

Da aber andereseits natürlich $|\kappa \times \kappa| \geq \kappa$ ist, folgt somit $\kappa \otimes \kappa = \kappa$. $\square$

Definition 9.42. *ZF⁻.* $(A^B =)^B A = \{f \in \mathcal{P}(A \times B) \mid f \colon B \to A\}$. *ist die Menge aller Funktionen von B nach A.*

Definition 9.43. *ZFC⁻.* $\kappa^\lambda = |^\lambda \kappa|$.

Satz 9.44. *Die Menge der reellen Zahlen hat die Kardinalität* $2^{\aleph_0}$.

Definition 9.45. *AC.* $2^\omega = \omega_1$ *ist die Kontinuumshypothese, CH - continuum hypothesis.* $\forall \alpha (2^{\omega_\alpha} = \omega_{\alpha+1})$ *heißt die allgemeine Kontinuumshypothese, GCH – generalized continuum hypothesis.*

Gödel zeigte 1938: Wenn ZF konsistent ist, dann auch ZFC + CH.

Wir werden dieses in dieser Vorlesung beweisen, auch den Teil von ZF auf ZFC.

Cohen zeigte 1963: Wenn ZFC konsistent ist, dann auch ZFC + ¬ CH. Die Kontinuumshypothese is also unabhängig von ZFC. Der Beweis dieses Satzes wird mit Forcing geführt.

Jack Silver veröffentlichte seinen untenstehenden Satz 1974, und dieses ZFC-Ergebnis war ein Durchbruch. Denn in jener Zeit großer Forcing-Euphorie war eher das Gegenteil vermutet worden: daß man im Rahmen des Lemmas von König und der Monotonie die Kardinalzahlexponentiation durch Forcing „frei einrichten" kann. Für 2^κ, κ regulär, zeigt man mit Easton-Forcing, daß jeder Verlauf der Exponentiationsfunktion in diesem Rahmen in einem Modell von ZFC realisiert werden kann.

Satz 9.46. *Silver* [**9**]. *Sei* κ *eine singuläre Kardinalzahl und sei* $\mathrm{cf}(\kappa) > \omega$, *z.B.* $\kappa = \aleph_{\aleph_1}$. *Sei* $E = \{\mu < \kappa \mid 2^\mu = \mu^+\}$ *stationär in* κ. *Dann ist* $2^\kappa = \kappa^+$.

Satz 9.47. *Shelah* [**8**]. *Wenn für jedes n,* $2^{\aleph_n} < \aleph_\omega$ *dann* $2^{\aleph_\omega} < \aleph_{\omega_4}$.

Literaturverzeichnis

[1] Heinz-Dieter Ebbinghaus, Jörg Flum, and Wolfgang Thomas. *Einfï¿½hrung in die Mathematische Logik*. Hochschultaschenbuch, 4 edition, 1996.

[2] Herbert Enderton. *A Mathematical Introduction to Logic*. Academic Press, 3 edition, 2001.

[3] Thomas Jech. *Set Theory*. Addison Wesley, 1978.

[4] Azriel Levy. *Basic Set Theory*. Springer, 1979.

[5] Daniel Lascar René Cori. *Logique mathématique. Cours et exercices*, volume I and II. Masson, 1993.

[6] Daniel Lascar René Cori. *Mathematical Logic. A course with exercises*, volume I and II. Oxford University Press, 2000.

[7] Julia Robinson. Definability problems and decidability in arithmetic. *J. Symbolic Logic*, 14:98–114, 1949.

[8] Saharon Shelah. *Cardinal Arithmetic*, volume 29 of *Oxford Logic Guides*. Oxford University Press, 1994.

[9] Jack Silver. On the singular cardinal problem. In *Proc. Int. Congr. Math. Vancouver*, volume 35, pages 60–64, 1970.

Index