Logik

Ralf Schindler

geTEXt von Martina Pfeifer

14. Juni 2011

Dieses Skript basiert auf Vorlesungen, die ich im WiSe 99-00 (Einf. i. d. theoretische Informatik), WiSe 01-02 (Logik 1), SoSe 02 (Grundbegriffe der Logik), SoSe 02 (Logik 2), WiSe 02-03 (Einf. i. d. theoretische Informatik), SoSe 03 (Grundbegriffe der Logik) an der Universität Wien und im WiSe 05-06 (Einf. i. d. math. Logik und theoretische Informatik) und WiSe 08-09 (Berechenbarkeitstheorie) an der WWU Münster gehalten habe. Dabei habe ich vor allem die beiden folgenden sehr schönen Textbücher verarbeitet:

Herbert B. Enderton, *A mathematical introduction to logic*, San Diego, 1972 + 2001.

Michael Sipser, *Introduction to the theory of computation*, Boston, 1997.

Ralf Schindler

Inhaltsverzeichnis

Kapitel 0

Worum geht es in der Logik?

Betrachten Sie den folgenden Satz, nennen wir ihn S:

Dieser Satz ist nicht wahr.

Der Satz S stellt eine Behauptung auf. Ist S wahr oder falsch? Nun, wenn S wahr ist, dann ist S offensichtlich falsch, da S ja sagt, dass S *nicht* wahr ist; und wenn S falsch ist, dann ist S wahr, da S ja sagt, dass S *nicht wahr* ist. Damit ist dann wohl S weder wahr noch falsch, also vielleicht einfach unsinnig ... Aber ein unsinniger Satz ist ja wohl doch immerhin *nicht wahr* und damit stimmt dann doch, was S sagt, und S ist am Ende doch wahr? Ihre Gedanken fangen an, sich in einem Kreis zu bewegen. Vielleicht ist der Satz S *so* unsinnig, dass er eben wirklich ganz und gar sinnlos ist, so wie wohl die Begriffe "Hump" und "Dump"[1]. Aber ganz so einfach ist es nicht. Sie haben ja eben eine Weile lang durchaus logisch über den Satz S nachgedacht. Also scheint nichts zu passen: S ist weder wahr, noch falsch, noch unsinnig, noch ganz und gar sinnlos — also insbesondere ist S nicht wahr! Daher ...

Sie geben auf. Der Satz S ist eine verfeinerte Variante der "Lügner–Paradoxie", die in der Bibel zwar besprochen, aber nicht gelöst wurde[2]. Hier ist also ein Satz, S, der in geringfügigen Varianten schon seit mehr als 2000 Jahren durchdiskutiert wird; aber: Eine "Lösung der Lügner–Paradoxie" ist nicht in Aussicht und wird auch in diesem Skript nicht präsentiert werden. Während Sie über S nachgedacht haben, haben Sie jedenfalls *logisch* nachgedacht: In Ihren Gedanken hat sich eins aus dem anderen zwangsweise

[1] Siehe http://www.funfocus.net/bilder/cartoons/deix5.htm

[2] Titus, 1, 12 – 13: "Einer ihrer eigenen Propheten hat gesagt: 'Kreter sind von jeher verlogen, wilde Tiere, faule Bäuche'. Dies Zeugnis ist wahr".

ergeben. Die Logik geht diesem Zwang nach. Sie fragt: “Was bedeutet es, dass etwas *logisch* aus etwas anderem *folgt*?”

Sie haben nun zwei Möglichkeiten:

(1) Die Beschäftigung mit S hat Ihnen gereicht, Sie wollen Ihre Zeit sinnvoller verbringen und nichts weiter über Logik wissen.

(2) Wenn man Ihnen schon keine befriedigende Auskunft hinsichtlich des Satzes S geben kann, dann wollen Sie wenigstens einen Einblick bekommen, was die Logik in den letzten 2000 Jahren Positives erreicht hat (und insbesondere, was die mathematische Logik in den letzten 100 Jahren geleistet hat!). Im letzteren Falle sollten Sie dranbleiben.[3]

Der bedeutendste Logiker des 20. Jahrhunderts heißt Kurt Gödel (*1906, †1978). Er wurde in Brünn geboren und kam dann nach Wien. Er bewies den so genannten Vollständigkeitssatz in seiner Dissertation und den sogenannten Unvollständigkeitssatz in seiner Habilitation. Diese Resultate haben die Logik revolutioniert. Er beschäftigte sich erfolgreich mit dem 1. Hilbertschen Problem. Es hat aber nichts genützt, er bekam keine feste Stelle in Wien. Er emigrierte 1938 in die USA. Er fuhr zunächst mit dem Zug nach Wladiwostok, dann von dort mit dem Schiff nach San Francisco und von dort weiter nach Princeton, NJ, wo er den Rest seines Lebens als Kollege von Albert Einstein (*1897, †1955) am ‘Institute for Advanced Studies’ wirkte. In Princeton bewies Kurt Gödel, dass Einsteins Feldgleichungen eine Lösung besitzen, die Zeitreisen in die Vergangenheit möglich machen.

Wir wollen in dieser Vorlesung den Gödelschen Vollständigkeitssatz beweisen. Man kann leicht missverstehen, was dieser Satz sagt. Man kann es aber schön an einem Beispiel illustrieren.

Eine (additive) *Gruppe* ist ein Objekt der Gestalt

$$(G; 0, +),$$

wobei G eine nichtleere Menge, $0 \in G$ das neutrale Element und $+$ eine zweistellige Verknüpfung ist (die Addition von Elementen aus G), und wobei $(G; 0, +)$ die Gruppenaxiome erfüllt. Gruppentheoretiker möchten herausfinden, welche Aussagen (in der Sprache der Gruppentheorie) in allen Gruppen gelten. Z.B. ist das Zentrum einer beliebigen Gruppe immer eine Untergruppe dieser Gruppe (und diese Aussage lässt sich in der Sprache der

[3] Ach ja, es gibt eine dritte Möglichkeit: Sie wollen zwar eigentlich nichts weiter über Logik wissen, benötigen aber einen Schein.

Gruppentheorie formulieren). Wie zeigt man aber, dass eine solche Aussage in allen Gruppen gilt?

Nun, auf diese Frage gibt es spätestens seit EUKLID (ca. *325, †265 v.u.Z.) nur eine mögliche Antwort: Man *beweist* die fragliche Aussage aus den Gruppenaxiomen. Was aber ist ein Beweis? Wir haben oben davon gesprochen, dass sich (beim Nachdenken über den Satz S) in Ihren Gedanken eins aus dem anderen zwangsweise ergeben hat; Sie haben logische Folgerungen vollzogen. In der Logik (als Teil der Mathematik) wird nun zunächst dieser Folgerungsbegriff (d.h. der Begriff des Beweisens) präzisiert. Es wird sodann nicht schwer sein zu sehen, dass alles, was aus den Gruppenaxiomen beweisbar ist, auch in allen Gruppen gelten muss. Aber gilt auch die Umkehrung? D.h., *wenn eine Aussage in allen Gruppen gilt, haben wir dann die Methoden zur Hand, diese Aussage aus den Gruppenaxiomen streng zu beweisen?*

Der Gödelsche Vollständigkeitssatz beantwortet diese Frage positiv (und das nicht nur für die Gruppentheorie). Ich habe oben gesagt: Man kann leicht missverstehen, was der Vollständigkeitssatz sagt. Eigentlich sollte man sagen: Es liegt nicht unmittelbar auf der Hand, dass er überhaupt etwas sagt. Man muss die Fragestellung wirklich erfassen um zu sehen, welch tiefes Resultat er ist. Wir wollen uns dieser Fragestellung langsam (wenn auch zugegebenermaßen abstrakt!) annähern.

Wir werden im Zuge des Beweises des Gödelschen Unvollständigkeitssatzes ein Resultat kennen lernen, mit dessen Hilfe wir Nichtstandard–Modelle der Zahlentheorie konstruieren werden. Was eine Gruppe ist, das wird von den Gruppenaxiomen ausgedrückt. Kann es eine (natürliche) Menge von Axiomen geben, die uns erklärt, was die natürlichen Zahlen sind? Manche von Ihnen kennen vielleicht die Axiome der PEANO–Arithmetik. Die Menge der natürlichen Zahlen ist ein Modell dieses Axiomensystems, so wie jede Gruppe ein "Modell" der Gruppenaxiome ist. Es gibt viele Gruppen, aber es gibt nur eine Menge der natürlichen Zahlen. Wir werden sehen, dass die Peano–Arithmetik viele (zueinander nicht isomorphe) Modelle besitzt. Das mag auf den ersten Blick etwas paradox erscheinen, die natürlichen Zahlen sind doch etwas so "Konkretes", dass es eigentlich möglich sein müsste, sie vollständig zu beschreiben. Nun ja. Der Unterschied zur "Lügner–Paradoxie" ist der, dass hier alles "Paradoxe" verschwindet, sobald man die Sache verstanden hat.

Apropos: Sei Franz K. ein Kreter. Angenommen Franz K. sagt:

"Jeder Aussagesatz, den ein Kreter jemals sagt, ist nicht wahr".

Diese Äußerung kann nicht wahr sein, da Franz K. selbst ein Kreter ist. Also muss sie falsch sein; d.h. Franz K. sagt in diesem Moment die Unwahrheit und es gibt Äußerungen von Kretern, die wahr sind. Dies allerdings ist konsistent! Die "Lügner–Paradoxie" der Bibel ist also auch keine Paradoxie!

Bleibt der oben diskutierte Satz S als Problem. Er liefert immerhin die Idee zum Beweis des Gödelschen *Un*vollständigkeitssatzes. Gödel hat es geschafft, in der Sprache der Zahlentheorie einen Satz zu formulieren, der sagt: "Dieser Satz ist in der Zahlentheorie nicht beweisbar". Er kann nicht beweisbar sein, wenn die Zahlentheorie konsistent ist. Also ist er wahr. Es gibt also wahre nicht beweisbare Sätze in der Zahlentheorie.

Entsprechendes gilt für die meisten mathematischen Theorien, sogar für die Mengenlehre, die die stärksten Theorien der Mathematik liefert: Für jede ihrer Theorien gibt es wahre, jedoch nicht beweisbare Sätze.

Ein Verwandter des Gödelschen Unvollständigkeitssatzes ist der Unentscheidbarkeitssatz von Alonzo Church (*1903, †1995). Er besagt, dass es kein Entscheidungsverfahren gibt, mit dessen Hilfe wir errechnen können, ob eine vorgelegte Aussage der Zahlentheorie (oder der Mengenlehre) in der Zahlentheorie (bzw. einer Theorie der Mengenlehre) beweisbar ist.

Die mathematische Forschung sähe anders aus, wäre der Churchsche Satz falsch! Er besagt, dass es prinzipiell keinen Computer geben kann, der uns Mathematikern die Arbeit abnimmt.

Bevor Konrad Zuse (*1910, †1995) den ersten programmierbaren Rechner der Welt gebaut hatte, wurden die Möglichkeiten und Grenzen der Berechenbarkeit systematisch untersucht. Das mathematische Modell eines Computers geht auf Alan Turing (*1912, †1954) zurück, der im zweiten Weltkrieg an der Entschlüsselung der Enigma beteiligt war. 1952 hat ihn die rückständige Nachkriegszeit wegen Homosexualität ins Gefängnis gebracht und später in den Selbstmord getrieben.

Neben der Betrachtung der Gödelschen Sätze werden wir in dieser Vorlesung die Grundlagen der Theorie der Berechenbarkeit kennen lernen. Dabei werden wir auch sehen, dass prinzipiell (durch Berechnung) lösbare Probleme nicht unbedingt auch praktisch lösbar sind, wenn nämlich etwa die Rechenzeit zu groß ist. Dies führt uns beispielsweise zur Frage, ob $P = NP$. Wir werden diese Frage formulieren, aber nicht beantworten. Falls Sie eine Antwort finden, dann sind Sie um 1 Mio. $ reicher[4]. Dies ist eine letzte Möglichkeit, inwiefern sich ein Besuch dieser Vorlesung lohnen könnte.

[4]Siehe http://www.claymath.org/millenium/P_vs_NP/

Kapitel 1

Aussagenlogik

Die ganze Logik ist in vier Teile geteilt: Beweistheorie, Rekursionstheorie (Theorie der Berechenbarkeit), Modelltheorie und die Mengenlehre. Die Theoretische Informatik ist nah an der Rekursionstheorie angesiedelt.

Die Begriffe des Beweisens und Rechnens sind grundlegend in der Mathematik. In der Logik werden sie systematisch untersucht. Beweise sind Beweise auf der Grundlage von Theorien. Theorien besitzen Modelle. Wir betrachten hier die grundlegenden Zusammenhänge zwischen Beweisen, Berechnungen und Modellen.

Die einfachsten Beweise sind Beweise in der Aussagenlogik. Beispiel:

$$\frac{\text{Die Werse ist ein Berg oder ein Fluss.} \quad \text{Die Werse ist kein Berg.}}{\text{Die Werse ist ein Fluss.}}$$

Mit A_0 = "Die Werse ist ein Berg" und A_1 = "Die Werse ist ein Fluss" sieht dieser "Beweis" (dieser logische Schluss) so aus:

$$\frac{\begin{array}{l} A_0 \text{ oder } A_1 \\ \text{nicht } A_0 \end{array}}{A_1}$$

Die logischen *Junktoren* sind Zeichen für: *nicht, und, oder, wenn ... , dann ... , genau dann, wenn.*

"$\neg$" steht für "nicht",
"$\wedge$" steht für "und",
"$\vee$" steht für "oder",

"$\rightarrow$" steht für "wenn ... , dann ... ",
"$\leftrightarrow$" steht für "genau dann, wenn".

Unser logischer Schluss sieht dann so aus:

$$\begin{array}{l} A_0 \vee A_1 \\ \neg A_0 \\ \hline A_1 \end{array}$$

Dieser Schluss ist logisch, da es auf die Bedeutung der darin vorkommenden Aussagenvariablen nicht ankommt.

Die *Symbole* der Aussagenlogik sind die folgenden:

Klammern: (und)
Junktoren: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
Aussagenvariablen: $A_0, A_1, A_2 \ldots$

Ein *Ausdruck* ist eine endliche Folge von Symbolen. Z.B. ist $(\wedge A_3 \leftrightarrow)$ ein Ausdruck. Nicht alle Ausdrücke sind "Formeln", d.h. haben Bedeutung.

Welche Ausdrücke sind Formeln? Wir wollen:

(a) Jede Aussagenvariable ist eine Formel.

(b) Wenn φ und ψ Formeln sind, dann sind auch $\neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \rightarrow \psi)$ und $(\varphi \leftrightarrow \psi)$ Formeln.

(c) Kein Ausdruck ist eine Formel, der es nicht auf Grund von (a) oder (b) sein muss.

Wie lässt sich dies mathematisch präziser fassen? Eine *Formel* der Aussagenlogik ist ein Ausdruck, der in jeder Menge M von Ausdrücken enthalten ist, so dass

(a)' jede Aussagenvariable in M enthalten ist, und

(b)' wenn φ und ψ in M enthalten sind, dann auch $\neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \rightarrow \psi)$ und $(\varphi \leftrightarrow \psi)$.

Wenn wir (nur für diesen Zweck!) eine Menge M von Ausdrücken "gut" nennen genau dann, wenn M (a)' und (b)' erfüllt, dann gilt also: Ein Ausdruck ist eine Formel genau dann, wenn er im Durchschnitt aller "guten" Mengen von Ausdrücken liegt.

Die Aussagenvariablen heißen auch *atomare Formeln*, die übrigen Formeln *zusammengesetzte Formeln*. Eine zusammengesetzte Formel ist entweder Negation (d.h. von der Gestalt $\neg\varphi$), oder Konjunktion (von der Gestalt $(\varphi \wedge \psi)$), oder Disjunktion (von der Gestalt $(\varphi \vee \psi)$), oder Konditional (von der Gestalt $(\varphi \to \psi)$) oder Bikonditional (von der Gestalt $(\varphi \leftrightarrow \psi)$).

Die Definition des Formelbegriffs ist Beispiel für eine *rekursive Definition*. Es gilt das *Induktionsprinzip* für Formeln: Sei E eine beliebige Eigenschaft. Angenommen, E gilt für alle atomaren Formeln. Sei weiterhin Folgendes angenommen: wenn E auf die Ausdrücke φ und ψ zutrifft, dann gilt E auch für $\neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi)$ und $(\varphi \leftrightarrow \psi)$. Dann gilt E für alle Formeln.

Hier ist ein Beispiel. Wir zeigen mit Hilfe des Induktionsprinzips, dass jede Formel die gleiche Anzahl von linken und rechten Klammern hat. Diese Aussage gilt nämlich offensichtlich für alle atomaren Formeln, und sie vererbt sich von φ und ψ weiter auf $\neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi)$ und $(\varphi \leftrightarrow \psi)$. Also gilt die Aussage für alle Formeln.

Warum gilt das Induktionsprinzip? Sei M die Menge aller Ausdrücke, auf die E zutrifft. Dann gilt für M nach Voraussetzung (a)' und (b)'. Also ist (nach Definition dessen, was es heißt, eine Formel zu sein) die Menge aller Formeln eine Teilmenge von M; d.h., auf jede Formel trifft E zu!

Rekursive Definitionen sind in der Mathematik sehr häufig. Für sie alle gibt es ein entsprechendes Induktionsprinzip. Das Induktionsprinzip für $\mathbb{N}$ ist ein weiteres Beispiel. Wir werden im Folgenden viele Beispiele zur Rekursion und Induktion sehen.

Wir wollen nun definieren, was es heißt, dass eine Formel logisch aus einer anderen Formel folgt. Hierzu definieren wir zunächst den Begriff der Belegung; eine Belegung β ordnet jeder Formel φ einen "Wahrheitswert" $\beta(\varphi) \in \{0,1\}$ zu. Dabei lesen wir $\beta(\varphi) = 0$ auch als "φ ist falsch" und $\beta(\varphi) = 1$ als "φ ist wahr".

Sei F_0 die Menge aller atomaren Formeln (d.h. $F_0 = \{A_0, A_1, A_2, \dots\}$), und sei $F \supset F_0$ die Menge aller Formeln. Sei $\overline{\beta} : F_0 \to \{0,1\}$ eine beliebige Funktion, die allen atomaren Formeln "Wahrheitswerte" zuordnet. Wir definieren dann die *zu $\overline{\beta}$ gehörige Belegung* $\beta : F \to \{0,1\}$ rekursiv wie folgt:

(1) $\beta(\varphi) = \overline{\beta}(\varphi)$ für alle $\varphi \in F_0$

und für alle $\varphi, \psi \in F$:

(2) $\beta(\neg\varphi) = 1 - \beta(\varphi)$,

(3) $\beta((\varphi \wedge \psi)) = \beta(\varphi) \cdot \beta(\psi) = \min\{\beta(\varphi), \beta(\psi)\}$

(4) $\beta((\varphi \vee \psi)) = \max\{\beta(\varphi), \beta(\psi)\}$

(5) $\beta((\varphi \to \psi)) = \max\{1 - \beta(\varphi), \beta(\psi)\}$

(6) $\beta((\varphi \leftrightarrow \psi)) = \beta((\varphi \to \psi)) \cdot \beta((\psi \to \varphi))$

Es gilt also Folgendes: $\neg\varphi$ ist wahr gdw.[1] φ falsch ist; $(\varphi \wedge \psi)$ ist wahr gdw. φ und ψ beide wahr sind; $(\varphi \vee \psi)$ ist wahr gdw. φ oder ψ wahr ist (im nicht ausschließenden Sinne); $(\varphi \to \psi)$ ist wahr gdw. $\neg\varphi$ oder ψ wahr ist; $(\varphi \leftrightarrow \psi)$ ist wahr gdw. φ und ψ dieselben Wahrheitswerte besitzen.

Zu jedem $\overline{\beta} : F_0 \to \{0, 1\}$ ist dadurch eindeutig eine zugehörige Belegung $\beta : F \to \{0, 1\}$ definiert.

Wir nennen $\beta(\varphi)$ auch den *zu $\overline{\beta}$ gehörigen Wahrheitswert von φ*. Für eine gegebene Formel errechnet sich der Wahrheitswert am leichtesten mit Hilfe einer "Wahrheitstafel". Sei etwa die Formel $(A_0 \to (\neg A_1 \to A_0))$ gegeben. Sei $\overline{\beta}(A_0) = 0$, $\overline{\beta}(A_1) = 1$. Dann ergibt sich für den zugehörigen Wahrheitswert $\beta((A_0 \to (\neg A_1 \to A_0)))$:

A_0	A_1	$(A_0$	$\to$	$(\neg$	A_1	$\to$	$A_0))$
0	1		1	0		1	

D.h. $\beta((A_0 \to (\neg A_1 \to A_0))) = 1$. Offensichtlich hängt der Wahrheitwert $\beta(\varphi)$ einer Formel φ nur von den (endlich vielen) Werten $\overline{\beta}(A_n)$ ab, für die die atomare Formel A_n in φ vorkommt. In unserem Falle errechnen sich die zu verschiedenen $\overline{\beta}$ gehörigen Wahrheitswerte von $(A_0 \to (\neg A_1 \to A_0))$ wie folgt:

A_0	A_1	$(A_0$	$\to$	$(\neg$	A_1	$\to$	$A_0))$
0	0		1	1		0	
0	1		1	0		1	
1	0		1	1		1	
1	1		1	0		1	

Sei $\overline{\beta} : F_0 \to \{0, 1\}$. Wir sagen, dass $\overline{\beta}$ die Formel φ *erfüllt* gdw. $\beta(\varphi) = 1$, wobei β die zu $\overline{\beta}$ gehörige Belegung ist. Sei Σ eine Menge von Formeln. (D.h. $\Sigma \subset F$.) Wir sagen, dass $\overline{\beta}$ die Formelmenge Σ *erfüllt* gdw. $\beta(\varphi) = 1$ für alle $\varphi \in \Sigma$, wobei β die zu $\overline{\beta}$ gehörige Belegung ist.

Definition 1.1 *Sei $\Sigma \cup \{\varphi\}$ eine Menge von Formeln.* Σ impliziert tautologisch *φ, in Zeichen $\Sigma \models \varphi$, gdw. für alle $\overline{\beta} : F_0 \to \{0, 1\}$ Folgendes gilt: wenn $\overline{\beta}$ Σ erfüllt, dann erfüllt $\overline{\beta}$ auch φ. Anstelle von $\emptyset \models \varphi$ schreiben wir auch $\models \varphi$; in diesem Falle nennen wir φ eine* Tautologie.

[1] "gdw." steht für "genau dann wenn"

Die oben betrachtete Formel $(A_0 \to (\neg A_1 \to A_0))$ ist also eine Tautologie. Hier sind einige Beispiele für $\Sigma \models \varphi$:

$$\begin{aligned}
&\{\neg A_1\} \models A_1 \to A_0, \\
&\{A_3 \to A_5, A_5 \to A_3\} \models A_3 \leftrightarrow A_5, \\
&\{\neg A_0 \vee A_1\} \models A_0 \to A_1.
\end{aligned}$$

Die Menge Σ in der obigen Definition muss übrigens nicht endlich sein. Wir schreiben auch $\psi \models \varphi$ anstelle von $\{\psi\} \models \varphi$. ψ und φ heißen *tautologisch äquivalent* gdw. $\psi \models \varphi$ und $\varphi \models \psi$ gelten.

Sei $J \subset \{\neg, \wedge, \vee, \to, \leftrightarrow\}$ eine Menge von Junktoren. J heißt *vollständig* gdw. es zu jeder Formel φ eine tautologisch äquivalente Formel ψ gibt, in der nur Junktoren aus J vorkommen. Z.B. ist $\{\neg\}$ nicht vollständig. Es gilt aber:

Satz 1.2 *Die folgenden Mengen J von Junktoren sind vollständig.*

(1) $J = \{\neg, \wedge, \vee\}$,

(2) $J = \{\neg, \wedge\}$,

(3) $J = \{\neg, \vee\}$,

(4) $J = \{\neg, \to\}$.

Beweis von (1): Wir konstruieren rekursiv eine Funktion $\Phi : F \to F$, die jeder Formel φ eine tautologisch äquivalente Formel $\Phi(\varphi)$ zuordnet, in der höchstens die Junktoren $\neg, \wedge, \vee$ vorkommen.

Wir setzen $\Phi(\varphi) = \varphi$ für jedes atomare φ. Seien $\Phi(\varphi)$ und $\Phi(\varphi')$ bereits definiert. Dann setzen wir

$$\begin{aligned}
&\Phi(\neg\varphi) = \neg\Phi(\varphi), \\
&\Phi((\varphi \wedge \varphi')) = (\Phi(\varphi) \wedge \Phi(\varphi')), \\
&\Phi((\varphi \vee \varphi')) = (\Phi(\varphi) \vee \Phi(\varphi')), \\
&\Phi((\varphi \to \varphi')) = \neg\Phi(\varphi) \vee \Phi(\varphi'), \\
&\Phi((\varphi \leftrightarrow \varphi')) = \Phi((\varphi \to \varphi')) \wedge \Phi((\varphi' \to \varphi)).
\end{aligned}$$

Damit ist $\Phi : F \to F$ (durch "Rekursion längs der Formelkomplexität") wohldefiniert.

Man überlegt sich leicht induktiv, dass φ und $\Phi(\varphi)$ immer tautologisch äquivalent sind. Für atomares φ ist das trivial. Sei nun etwa φ ein Konditional, etwa φ gleich $(\psi \to \psi')$. Dann sind nach Induktionsvoraussetzung ψ

und $\Phi(\psi)$ sowie ψ' und $\Phi(\psi')$ jeweils tautologisch äquivalent. Damit sind aber auch $\neg\psi$ und $\neg\Phi(\psi)$ sowie schließlich $(\neg\psi \vee \psi')$ und

$$(\neg\Phi(\psi) \vee \Phi(\varphi') = \Phi((\psi \rightarrow \psi')))$$

tautologisch äquivalent. Es sind aber $(\psi \rightarrow \psi')$ (d.h. φ) und $(\neg\psi \vee \psi')$ tautologisch äquivalent. □

Im Beweis dieses Satzes sahen wir ein Beispiel für eine Definition durch "Rekursion längs der Formelkomplexität" und ein Beispiel für den Beweis einer Aussage durch "Induktion nach der Formelkomplexität".

Wir beweisen nun den Kompaktheitssatz der Aussagenlogik. Sei Σ eine Menge von Formeln. Σ heißt *erfüllbar* gdw. es ein $\overline{\beta} : F_0 \rightarrow \{0,1\}$ gibt, so dass $\overline{\beta}$ jedes φ aus Σ erfüllt. Σ heißt *endlich* erfüllbar gdw. jede endliche Teilmenge $\overline{\Sigma}$ von Σ erfüllbar ist. Offensichtlich ist jedes erfüllbare Σ auch endlich erfüllbar.

Satz 1.3 Kompaktheitssatz. *Sei Σ eine Menge von Formeln. Wenn Σ endlich erfüllbar ist, dann ist Σ auch erfüllbar.*

Beweis: Sei $(\varphi_n : n \in \mathbb{N})$ eine Aufzählung *aller* Formeln. Eine solche Aufzählung erhält man z.B., indem man im m^{ten} Schritt alle Formeln der Länge $\leq m$ aufzählt, in denen höchstens die Aussagenvariablen $A_0, \ldots, A_{m-1}$ vorkommen.

Sei nun Σ endlich erfüllbar. Wir konstruieren nun rekursiv eine Folge $(\Sigma_n : n \in \mathbb{N})$ von Formelmengen Σ_n wie folgt. Setze $\Sigma_0 = \Sigma$. Sei nun Σ_n konstruiert. Setze dann $\Sigma_{n+1} = \Sigma_n \cup \{\varphi_n\}$, falls $\Sigma_n \cup \{\varphi_n\}$ endlich erfüllbar ist; ansonsten setze $\Sigma_{n+1} = \Sigma_n \cup \{\neg\varphi_n\}$. Schließlich sei Σ_∞ die Vereinigung aller Σ_n. Wir zeigen zunächst durch Induktion, dass alle Σ_n endlich erfüllbar sind. Dies gilt nach Annahme für $n = 0$. Sei nun Σ_n endlich erfüllbar. Falls $\Sigma_n \cup \{\varphi_n\}$ endlich erfüllbar ist, dann ist der Induktionsschritt trivial. Sei also o.B.d.A. $\Sigma_n \cup \{\varphi_n\}$ nicht endlich erfüllbar und $\Sigma_{n+1} = \Sigma_n \cup \{\neg\varphi_n\}$. Sei $\overline{\Sigma} \subset \Sigma_n \cup \{\neg\varphi_n\}$ endlich. Sei $\overline{\Sigma}' \subset \Sigma_n \cup \{\varphi_n\}$ endlich und nicht erfüllbar.

Nach Induktionsvoraussetzung existiert ein $\overline{\beta} : F_0 \rightarrow \{0,1\}$, das $(\overline{\Sigma} \cup \overline{\Sigma}')\backslash\{\varphi_n, \neg\varphi_n\}$ erfüllt. Sei β die zu $\overline{\beta}$ gehörige Belegung. Da Σ_n endlich erfüllbar und $\overline{\Sigma}'$ nicht erfüllbar ist, muss φ_n in $\overline{\Sigma}'$ enthalten sein und $\beta(\varphi_n) = 0$. Dann gilt aber $\beta(\neg\varphi_n) = 1$ und $\overline{\beta}$ erfüllt $(\overline{\Sigma} \cup \overline{\Sigma}' \cup \{\neg\varphi_n\})\backslash\{\varphi_n\}$, also auch $\overline{\Sigma}$.

Damit ist nun sofort auch Σ_∞ endlich erfüllbar. Nach Konstruktion haben wir, dass für jede Formel φ entweder φ oder $\neg\varphi$ in Σ_∞ liegt.

Wir definieren nun ein $\overline{\beta} : F_0 \to \{0,1\}$ wie folgt. Wir setzen $\overline{\beta}(A_n) = 1$ gdw. A_n in Σ_∞ enthalten ist.

Sei $\beta : F \to \{0,1\}$ die zu $\overline{\beta}$ gehörige Belegung. Wir zeigen jetzt induktiv, dass $\beta(\varphi) = 1$ gdw. φ in Σ_∞ enthalten ist. Dies gilt zunächst für atomare Formeln φ. Sei die Aussage nun für φ gezeigt. Wir zeigen dann, dass sie auch für $\neg\varphi$ gilt. Es gilt aber $\beta(\neg\varphi) = 1$ gdw. $\beta(\varphi) = 0$ gdw. φ nicht in Σ_∞ enthalten ist gdw. $\neg\varphi$ in Σ_∞ enthalten ist. Sei die Aussage für φ und ψ gezeigt. Sie gilt dann auch für $(\varphi \wedge \psi) : \beta((\varphi \wedge \psi)) = 1$ gdw. $\beta(\varphi) = 1 = \beta(\psi)$ gdw. φ und ψ beide in Σ_∞ sind gdw. $(\varphi \wedge \psi)$ in Σ_∞ ist. Letztere Äquivalenz ergibt sich leicht aus der endlichen Erfüllbarkeit von Σ_∞. Ähnlich argumentiert man für die übrigen zusammengesetzten Formeln. $\square$

Aus Satz 1.3 ergibt sich unmittelbar:

Korollar 1.4 *Sei $\Sigma \cup \{\varphi\}$ eine Menge von Formeln. Wenn $\Sigma \models \varphi$, dann gibt es ein endliches $\overline{\Sigma} \subset \Sigma$ mit $\overline{\Sigma} \models \varphi$.*

Diese Aussage ist sogar äquivalent zu 1.3.

Eine Formel ist in *konjunktiver Normalform*, falls sie die Gestalt

$$(\varphi_{0,0} \vee \cdots \vee \varphi_{0,i_0}) \wedge \cdots \wedge (\varphi_{k-1,0} \vee \cdots \vee \varphi_{k-1,i_{k-1}})$$

besitzt, wobei jedes $\varphi_{l,m}$ entweder Aussagenvariable oder Negation einer Aussagenvariablen ist. Analog ist eine Formel in *disjunktiver Normalform*, falls sie die Gestalt

$$(\varphi_{0,0} \wedge \cdots \wedge \varphi_{0,i_0}) \vee \cdots \vee (\varphi_{k-1,0} \wedge \cdots \wedge \varphi_{k-1,i_{k-1}})$$

besitzt, wobei jedes $\varphi_{l,m}$ entweder Aussagenvariable oder Negation einer Aussagenvariablen ist. Man zeigt leicht, dass es zu jeder aussagenlogischen Formel φ aussagenlogische Formeln ψ und ψ' gibt, so dass sowohl φ und ψ als auch φ und ψ' tautologisch äquivalent sind und ψ ist in konjunktiver Normalform und ψ' ist in disjunktiver Normalform.

Kapitel 2

Logik erster Stufe

Nicht alle logischen Schlüsse sind aussagenlogische Schlüsse. Betrachten wir das Beispiel des SOKRATES–Schülers ARISTOTELES:

$$\begin{array}{l} \text{Alle Flüsse fließen ins Meer.} \\ \text{Die Aa ist ein Fluss .} \\ \hline \text{Die Aa fließt ins Meer.} \end{array}$$

In der Logik erster Stufe lässt sich dieser Schluss nachvollziehen. Analog zu den aussagenlogischen Tautologien wird es "logische Wahrheiten" geben, d.h. (logisch) gültige Formeln (der Logik erster Stufe). Die Menge der gültigen Formeln ist zwar rekursiv aufzählbar, aber nicht entscheidbar. Dies wird sich aus den Gödelschen Sätzen ergeben.

Die Logik erster Stufe ist die Logik, die wir in der Mathematik benutzen. Allerdings ist es nicht ganz richtig, von der Logik erster Stufe im Singular zu sprechen, da wir mit verschiedenen Mengen von Prädikatsymbolen, Konstanten und Funktoren arbeiten können.

Seien I, K, J (womöglich leere, womöglich unendlich große) paarweise disjunkte Indexmengen, und sei $n : I \cup J \to \mathbb{N}$; wir schreiben n_i für $n(i)$, wobei $i \in I \cup J$. Die zu I, K, J, n gehörige Sprache der Logik erster Stufe besitzt die folgenden *Symbole*:

Klammern: (und)
Junktoren: $\neg$ und $\to$
Allquantor: $\forall$
Variablen: $v_0, v_1, v_2, \ldots$
Gleichheitszeichen: $=$
Prädikatsymbole: für jedes $i \in I$ ein n_i–stelliges Prädikatsymbol P_i

Konstanten: für jedes $k \in K$ eine Konstante c_k
Funktoren: für jedes $j \in J$ einen n_j–stelligen Funktor f_j.

Ein Beispiel für eine solche Sprache ist die Sprache der Gruppentheorie: diese enthält einen zweistelligen Funktor für die Addition (bzw. Multiplikation) und eine Konstante für das neutrale Element. Die Sprache der Körpertheorie enthält zwei zweistellige Funktoren für die Addition und die Multiplikation und zwei Konstanten für die 0 und die 1. Die Sprache der *elementaren Zahlentheorie* enthält ein zweistelliges Prädikatsymbol $<$, eine Konstante 0 für die Null, einen einstelligen Funktor S für die Nachfolgeroperation $n \mapsto n+1$ und drei zweistellige Funktoren $+, \cdot, E$ für die Addition, die Multiplikation und die Exponentiation.[1] Die Sprache der Mengenlehre schließlich hat lediglich das zweistellige Prädikatsymbol $\in$.

Sei $\mathcal{L}$ eine Sprache der Logik erster Stufe. Ein $\mathcal{L}$*–Ausdruck* ist eine endliche Folge von Symbolen von $\mathcal{L}$. Wir wollen nun die Begriffe "$\mathcal{L}$–Term" und "$\mathcal{L}$–Formel" definieren. Dies geschieht wieder rekursiv. Sei $\mathcal{L}$ durch I, K, J, n gegeben.

Ein $\mathcal{L}$*–Term* ist ein $\mathcal{L}$–Ausdruck, der in jeder Menge M von $\mathcal{L}$–Ausdrücken liegt mit:

(a) jede Konstante und jede Variable liegt in M, und

(b) für $j \in J$ und $\tau_0, \dots \tau_{n_j-1} \in M$ ist auch $f_j\tau_0 \dots \tau_{n_j-1} \in M$.

Beispielsweise sind die folgenden Ausdrücke Terme der elementaren Zahlentheorie:

$$+S0v_3,\ SSS0,\ \cdot SS0SSS0.$$

Wir werden natürlich $S(0) + v_3$ (oder besser $1 + v_3$) für $+S0v_3$ schreiben, usw.

Eine *atomare* $\mathcal{L}$*–Formel* ist jeder Ausdruck der Form $P\tau_0 \dots \tau_{n-1}$, wobei P ein n–stelliges Prädikatsymbol ist und $\tau_0, \dots, \tau_{n-1}$ $\mathcal{L}$–Terme sind, oder ein Ausdruck der Form $\tau_0 = \tau_1$, wobei τ_0, τ_1 $\mathcal{L}$–Terme sind.

Schließlich ist eine $\mathcal{L}$*–Formel* ein Ausdruck, der in jeder Menge M von Ausdrücken liegt mit:

(1) jede atomare $\mathcal{L}$–Formel ist in M,

(2) wenn φ und ψ in M sind, dann auch $\neg\varphi$ und $(\varphi \to \psi)$,

(3) wenn φ in M ist und $n \in \mathbb{N}$, dann ist auch $\forall v_n \varphi$ in M.

[1] Diese Sprache werden wir später mit $\mathcal{L}_A$ bezeichnen.

Beispiele für Formeln der Sprache der Mengenlehre sind etwa $\in v_3 v_0$ oder $\forall v_3 \in v_3 v_0$. Wir werden natürlich $v_3 \in v_0$ anstelle von $\in v_3 v_0$ und entsprechend $\forall v_3\ v_3 \in v_0$ anstelle von $\forall v_3 \in v_3 v_0$ schreiben. $v_3 \in v_0$ ist eine atomare Formel der Sprache der Mengenlehre.

Wir vereinbaren einige Schreibkonventionen, um Formeln besser lesen zu können. So schreiben wir:

$$
\begin{array}{lll}
(\varphi \vee \psi) & \text{für} & (\neg\varphi \to \psi), \\
(\varphi \wedge \psi) & \text{für} & \neg(\varphi \to \neg\psi), \\
(\varphi \leftrightarrow \psi) & \text{für} & ((\varphi \to \psi) \wedge (\psi \to \varphi)), \\
\exists v_n \varphi & \text{für} & \neg\forall v_n \neg\varphi, \\
\tau = \tau' & \text{für} & = \tau\tau', \text{ und} \\
\tau \neq \tau' & \text{für} & \neg\tau = \tau',
\end{array}
$$

wobei φ, ψ Formeln und τ, τ' Terme sind. Diese abkürzenden Schreibweisen sind sinnvoll: für die ersten drei Zeilen überlegt man sich leicht, dass, wären φ und ψ aussagenlogische Formeln, die jeweiligen Formeln (also $(\varphi \vee \psi)$ und $(\neg\varphi \to \psi)$, usw.) tautologisch äquivalent wären.

Mit diesen Konventionen ist nun also auch $\forall v_0 \exists v_1\ v_0 \in v_1$ eine Formel der Sprache der Mengenlehre, bei der es sich in nicht abgekürzter Schreibweise um die Formel

$$\forall v_0 \neg\forall v_1 \neg \in v_0 v_1$$

handelt. Als weitere Schreibkonvention lassen wir von nun an die äußeren Klammern weg, schreiben also z.B. $\varphi \to \psi$ anstelle von $(\varphi \to \psi)$.

Wir wollen nun wieder definieren, wann eine Formelmenge Σ eine Formel φ impliziert. Wieder arbeiten wir mit Belegungen, diesmal aber von Variablen mit Elementen eines Modells; dies entspricht der Einsetzung solcher Elemente für freie Variablen in Formeln.

Wir fixieren nun I, K, J, n, wodurch eine Sprache $\mathcal{L}$ gegeben ist. Anstelle von $\mathcal{L}$–Termen und (atomaren) $\mathcal{L}$–Formeln sprechen wir nun auch einfach von Termen und Formeln.

Wir definieren zunächst den Begriff der "freien Variablen".

Sei $n \in \mathbb{N}$. Wir definieren "v_n kommt frei in der Formel φ vor". Wenn φ atomar ist, dann kommt v_n frei in φ vor gdw. v_n überhaupt in φ vorkommt. v_n kommt frei in $\neg\varphi$ vor gdw. v_n frei in φ vorkommt. v_n kommt frei in $\varphi \to \psi$ vor gdw. v_n frei in φ oder frei in ψ vorkommt. Schließlich kommt v_n frei in $\forall v_m \varphi$ vor gdw. $m \neq n$ und v_n frei in φ vorkommt.

Ein $\mathcal{L}$*–Satz* ist eine $\mathcal{L}$*–Formel*, in der keine freien Variablen vorkommen.

Beispielsweise ist $\forall v_1 \neg v_1 \in v_0$ eine Formel der Sprache der Mengenlehre (aber kein Satz) und $\exists v_0 \forall v_1 \neg v_1 \in v_0$ ein Satz der Sprache der Mengenlehre.

Wir wollen jetzt den Sätzen der Sprache $\mathcal{L}$ Bedeutung verleihen. Oft hat eine Sprache einen "intendierten Objektbereich" im Auge. Mit der Sprache der elementaren Zahlentheorie wollen wir über die Struktur der natürlichen Zahlen sprechen, mit der Sprache der Mengenlehre über die Struktur des Universums aller Mengen.

Ebenso oft gibt es aber auch keinen intendierten Objektbereich: die Sprache der Gruppentheorie hat nicht eine feste Gruppe im Auge, sondern "beliebige Gruppen".

Allgemein bekommen Sätze Bedeutung, indem wir ein Modell von $\mathcal{L}$ betrachten. Ein *Modell von* $\mathcal{L}$ ist eine Struktur der Form

$$\mathcal{M} = (M; (R_i : i \in I), (a_k : k \in K), (F_j : j \in J)),$$

wobei M eine nichtleere Menge ist (das *Universum*, oder die *Trägermenge* von $\mathcal{M}$), jedes R_i eine n_i–stellige Relation auf M ist (d.h. $R_i \subset M^{n_i}$), jedes a_k ein Element von M ist und jedes F_j eine n_j–stellige Funktion auf M ist (d.h. $F_j : M^{n_j} \to M$).

Ein solches Modell interpretiert $\mathcal{L}$ in offensichtlicher Weise: das Prädikatsymbol P_i wird durch die Relation R_i interpretiert (in Zeichen: $P_i^{\mathcal{M}} = R_i$), die Konstante c_k wird durch a_k interpretiert (in Zeichen: $c_k^{\mathcal{M}} = a_k$), und der Funktor f_j wird durch die Funktion F_j interpretiert (in Zeichen: $f_j^{\mathcal{M}} = F_j$).

Wir wollen nun sagen, was es heißt, dass ein gegebener Satz im Modell $\mathcal{M}$ gilt. Hierzu gehen wir einen kleinen (aber sehr effektiven) Umweg und definieren allgemeiner, was es heißt, dass eine gegebene Formel unter einer gegebenen Belegung in $\mathcal{M}$ gilt.

Eine $\mathcal{M}$*–Belegung* ist eine Funktion $\overline{\beta} : \{v_0, v_1, \dots\} \to M$, die allen Variablen Elemente der Trägermenge von $\mathcal{M}$ zuordnet. Durch eine $\mathcal{M}$–Belegung ist eine Interpretation beliebiger Terme gegeben. Eine solche durch $\overline{\beta}$ induzierte *Terminterpretation* ist eine Funktion $\beta : T \to M$ (wobei T die Menge aller Terme ist), für die gilt:

(1) $\beta(v_n) = \overline{\beta}(v_n)$ für $n \in \mathbb{N}$,

(2) $\beta(c_k) = a_k$ für $k \in K$, und

(3) $\beta(f_j \tau_0 \dots \tau_{n_j-1}) = F_j(\beta(\tau_0), \dots, \beta(\tau_{n_j-1}))$ für $j \in J$ und Terme $\tau_0, \dots, \tau_{n_j-1}$.

Wir definieren nun "φ gilt in $\mathcal{M}$ unter der Belegung $\overline{\beta}$". Hierzu ist die folgende Schreibweise hilfreich.

Sei $n \in \mathbb{N}$, und sei $a \in M$. Dann bezeichnet $\overline{\beta}(v_n|a)$ diejenige Belegung, die mit $\overline{\beta}$ überall übereinstimmt, außer an der Stelle v_n, wo der Wert a angenommen wird, d.h.

$$\overline{\beta}(v_n|a)(v_m) = \begin{cases} \overline{\beta}(v_m), \text{ falls } m \neq n \\ a \qquad\;\;, \text{ falls } m = n. \end{cases}$$

Wir schreiben "φ gilt in $\mathcal{M}$ unter der Belegung $\overline{\beta}$" oder "$\mathcal{M}$ ist Modell von φ unter $\overline{\beta}$" als

$$\mathcal{M} \models \varphi[\overline{\beta}]$$

und definieren diese Relation wie folgt. Hierbei sei β die durch $\overline{\beta}$ induzierte Terminterpretation. Die folgende Definition ist rekursiv "nach der Formelkomplexität" und simultan für alle Belegungen.

(1) $\mathcal{M} \models \tau_0 = \tau_1[\overline{\beta}]$ gdw. $\beta(\tau_0) = \beta(\tau_1)$ für Terme τ_0, τ_1

(2) $\mathcal{M} \models P_i\tau_0 \ldots \tau_{n_j-1}[\overline{\beta}]$ gdw. $(\beta(\tau_0), \ldots, \beta(\tau_{n_j-1})) \in R_i$

(3) $\mathcal{M} \models \neg\varphi[\overline{\beta}]$ gdw. $\mathcal{M} \models \varphi[\overline{\beta}]$ nicht gilt

(4) $\mathcal{M} \models \varphi \rightarrow \psi[\overline{\beta}]$ gdw. $\mathcal{M} \models \varphi[\overline{\beta}]$ nicht gilt oder $\mathcal{M} \models \psi[\overline{\beta}]$ gilt

(5) $\mathcal{M} \models \forall v_n \varphi[\overline{\beta}]$ gdw. für alle $a \in M$, $\mathcal{M} \models \varphi[\overline{\beta}(v_n|a)]$.

Betrachten wir den Satz $\forall v_0\ v_0 = v_0$. Es gilt $\mathcal{M} \models \forall v_0\ v_0 = v_0[\overline{\beta}]$ gdw. für alle $a \in M$, $\mathcal{M} \models v_0 = v_0[\overline{\beta}(v_0|a)]$ gdw. für alle $a \in M$, $\beta(v_0) = \beta(v_0)$ (d.h. $\overline{\beta}(v_0) = \overline{\beta}(v_0)$). $\forall v_0\ v_0 = v_0$ gilt also in jedem Modell unter jeder Belegung.

Definition 2.1 *Sei $\Sigma \cup \{\varphi\}$ eine Menge von Formeln. Wir sagen, dass Σ (logisch) φ impliziert, in Zeichen: $\Sigma \models \varphi$ gdw. für jedes Modell $\mathcal{M}$ und für jede Belegung $\overline{\beta}$ gilt: wenn $\mathcal{M} \models \psi[\overline{\beta}]$ für alle $\psi \in \Sigma$, dann auch $\mathcal{M} \models \varphi[\overline{\beta}]$. Anstelle von $\emptyset \models \varphi$ schreiben wir auch $\models \varphi$ und sagen in diesem Falle, dass φ (logisch) gültig ist.*

Für jede Menge Σ von Formeln schreiben wir $\mathcal{M} \models \Sigma[\overline{\beta}]$ anstelle von: für alle $\varphi \in \Sigma$, $\mathcal{M} \models \varphi[\overline{\beta}]$. Es gilt also $\Sigma \models \varphi$ gdw. für jedes Modell $\mathcal{M}$ und für jede Belegung $\overline{\beta}$ gilt: wenn $\mathcal{M} \models \Sigma[\overline{\beta}]$, dann $\mathcal{M} \models \varphi[\overline{\beta}]$.

Der oben betrachtete Satz $\forall v_0\ v_0 = v_0$ ist also gültig. Dasselbe gilt übrigens auch für $\exists v_0\ v_0 = v_0$, das abkürzend die Formel $\neg\forall v_0\ \neg v_0 = v_0$ darstellt. Dies ist leicht nachzurechnen. Hingegen ist $\exists v_0 \exists v_1\ v_0 \neq v_1$ nicht gültig, aber es gilt z.B.

$$\{\exists v_0 \exists v_1 \exists v_2 (v_0 \neq v_1 \wedge v_1 \neq v_2 \wedge v_0 \neq v_2)\} \models \exists v_0 \exists v_1 v_0 \neq v_1.$$

Wir schreiben $\varphi \models \psi$ anstelle von $\{\varphi\} \models \psi$. φ und ψ heißen *(logisch) äquivalent* gdw. $\varphi \models \psi$ und $\psi \models \varphi$ gelten.

Satz 2.2 *Sei φ eine $\mathcal{L}$–Formel, und sei $\mathcal{M}$ ein Modell von $\mathcal{L}$. Seien $\overline{\beta}_0$ und $\overline{\beta}_1$ $\mathcal{M}$–Belegungen, so dass $\overline{\beta}_0(v_n) = \overline{\beta}_1(v_n)$ für alle v_n, die frei in φ vorkommen. Dann gilt*

$$\mathcal{M} \models \varphi[\overline{\beta}_0] \text{ gdw. } \mathcal{M} \models \varphi[\overline{\beta}_1].$$

Beweis: Wir zeigen diesen Satz durch Induktion "nach der Formelkomplexität". Die Aussage gilt zunächst für atomares φ, da dann v_n frei in φ vorkommt gdw. v_n überhaupt in φ vorkommt. Sodann ergibt sich aus der Tatsache, dass die Aussage für ψ_0 und ψ_1 gilt, sofort, dass die Aussage auch für φ gleich $\neg\psi_0$ und für φ gleich $\psi_0 \to \psi_1$ gilt.

Sei nun φ gleich $\forall v_m \psi$. v_n kommt frei in φ vor gdw. $n \neq m$ und v_n frei in ψ vorkommt. Für ein beliebiges a gilt also

$$\overline{\beta}_0(v_m|a)(v_n) = \overline{\beta}_1(v_m|a)(v_n)$$

für alle v_n, die frei in ψ vorkommen.

Damit gilt aber mit Hilfe der Induktionsvoraussetzung: $\mathcal{M} \models \varphi[\overline{\beta}_0]$ gdw. für alle $a \in M$, $\mathcal{M} \models \psi[\overline{\beta}_0(v_m|a)]$ gdw. für alle $a \in M$, $\mathcal{M} \models \psi[\overline{\beta}_1(v_m|a)]$ gdw. $\mathcal{M} \models \varphi[\overline{\beta}_1]$. □

Korollar 2.3 *Sei φ ein $\mathcal{L}$–Satz, und sei $\mathcal{M}$ ein Modell von $\mathcal{L}$. Seien $\overline{\beta}_0$ und $\overline{\beta}_1$ beliebige $\mathcal{M}$-Belegungen. Dann gilt*

$$\mathcal{M} \models \varphi[\overline{\beta}_0] \text{ gdw. } \mathcal{M} \models \varphi[\overline{\beta}_1].$$

Für Sätze φ schreiben wir im Folgenden $\mathcal{M} \models \varphi$ anstelle von $\mathcal{M} \models \varphi[\overline{\beta}]$ und sagen, dass φ *in $\mathcal{M}$ gilt* (oder, dass $\mathcal{M}$ *Modell von* φ ist).

Eine $\mathcal{L}$–Forml φ heißt *erfüllbar* gdw. $\neg\varphi$ nicht logisch gültig ist, d.h. wenn es ein Modell $\mathcal{M}$ und eine $\mathcal{M}$–Belegung $\overline{\beta}$ gibt, so dass $\mathcal{M} \models \varphi[\overline{\beta}]$. Die Erfüllbarkeit aussagenlogischer Formeln ist — wie wir gesehen haben — Turing–entscheidbar. Wir werden später sehen, dass hingegen die Erfüllbarkeit von $\mathcal{L}$–Formeln *nicht* Turing–entscheidbar ist (dies ist der Satz von Church, aus dem wir dann auch den ersten Gödelschen Unvollständigkeitssatz ableiten werden).

Der Gödelsche Vollständigkeitssatz auf der anderen Seite sagt, dass die Menge der logisch gültigen $\mathcal{L}$–Formeln Turing–erkennbar ist.

Sei $\mathcal{M}$ ein Modell von $\mathcal{L}$. Sei φ eine Formel, in der genau die Variablen $v_{i_0}, \dots, v_{i_{n-1}}$ frei vorkommen. Sei $a_{i_0}, \dots, a_{i_{n-1}} \in M$, der Trägermenge von $\mathcal{M}$. Wir schreiben dann kurz

$$\mathcal{M} \models \varphi(a_{i_0}, \dots, a_{i_{n-1}})$$

anstelle von: $\mathcal{M} \models \varphi[\overline{\beta}]$, wobei $\overline{\beta}(v_{i_j}) = a_{i_j}$ für alle $j < n$.

Eine n–stellige Relation $R \subset M^n$ heißt *über* $\mathcal{M}$ *definierbar* gdw. es eine Formel φ gibt, in der genau die Variablen $v_0, \dots, v_{n-1}$ frei vorkommen, so dass für alle $a_0, \dots, a_{n-1} \in M$:

$$(a_0, \dots, a_{n-1}) \in R \text{ gdw. } \mathcal{M} \models \varphi(a_0, \dots, a_{n-1}).$$

Für $\mathcal{M} = (M; (R_i : i \in I), (c_k : k \in K), (F_j : j \in J))$ sind trivialerweise alle Relationen R_i über $\mathcal{M}$ definierbar; es gibt aber im Allgemeinen noch weitere definierbare Relationen.

Betrachten wir die Struktur

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

wobei $<$ die Kleiner–Relation, 0 die Null, S die Nachfolgeroperation $n \mapsto n + 1$, $+$ die Addition, $\cdot$ die Multiplikation und E die Exponentiation ist. Offenbar ist $\mathcal{N}$ ein Modell der Sprache der elementaren Zahlentheorie[2] (das “Standardmodell”; wir werden sehen, dass es noch weitere Modelle gibt). Es ist nicht wirklich nötig, $<$ zu $\mathcal{N}$ hinzuzunehmen: die Relation $<$ ist über dem Modell

$$(\mathbb{N}; 0, +)$$

mit Hilfe der Formel $\exists v_2(v_2 \neq 0 \wedge v_0 + v_2 = v_1)$ definierbar:

$$n < m \text{ gdw. } (\mathbb{N}; 0, +) \models \exists v_2(v_2 \neq 0 \wedge n + v_2 = m).$$

Wir werden später sehen, dass die Exponentiation über

$$(\mathbb{N}; <, 0, S, +, \cdot)$$

definierbar ist, d.h. dass es eine Formel φ gibt, so dass

$$n^m = q \text{ gdw. } (\mathbb{N}; <, 0, S, +, \cdot) \models \varphi(n, m, q).$$

[2]Damit bezeichnet $<$ sowohl das Symbol für die Kleiner–Relation als auch die Relation selbst, usw.

Dies wird einige Arbeit erfordern.

Auf der anderen Seite ist z.B. die Addition nicht über

$$(\mathbb{N}; \cdot)$$

und die Multiplikation nicht über

$$(\mathbb{N}; <, 0, S, +)$$

definierbar. Ersteres lässt sich folgendermaßen zeigen.

Seien $\mathcal{M}$ und $\mathcal{P}$ zwei Modelle von $\mathcal{L}$ mit Trägermenge M bzw. P. Eine Abbildung $\pi\colon M \to P$ heißt ein *Homomorphismus von* $\mathcal{M}$ *nach* $\mathcal{P}$ gdw.

(1) $(a_0, ..., a_{n-1}) \in P^{\mathcal{M}}$ gdw. $(\pi(a_0), ..., \pi(a_{n-1})) \in P^{\mathcal{P}}$,

(2) $\pi(f^{\mathcal{M}}(a_0, ..., a_{n-1})) = f^{\mathcal{P}}(\pi(a_0), ..., \pi(a_{n-1}))$, und

(3) $\pi(c^{\mathcal{M}}) = c^{\mathcal{P}}$

für alle Prädikatsymbole P, alle Funktoren f, alle a_0, ..., $a_{n-1} \in M$ und für alle Konstanten c ist (hierbei ist n, abhängig von P bzw. f, jeweils die Stelligkeit von P bzw. f). Eine Abbildung $\pi\colon M \to P$ heißt ein *Isomorphismus von* $\mathcal{M}$ *nach* $\mathcal{P}$ gdw. π ein bijektiver Homomorphismus von $\mathcal{M}$ nach $\mathcal{P}$ ist. Die folgende Aussage ist leicht zu zeigen.

Satz 2.4 *Sei $\pi\colon M \to P$ ein Homomorphismus von $\mathcal{M}$ nach $\mathcal{P}$. Sei $\bar{\beta}$ eine M-Belegung, und sei β die durch $\bar{\beta}$ induzierte Terminterpretation. Sei die P-Belegung $\bar{\beta}'$ definiert durch $\bar{\beta}'(v_i) = \pi(\bar{\beta}(v_i))$ für $i \in \mathbb{N}$, und sei β' die durch $\bar{\beta}'$ induzierte Terminterpretation. Dann haben wir:*

(a) Für alle Terme τ ist $\pi(\beta(\tau)) = \beta'(\tau)$.

(b) Wenn π ein Isomorphismus von $\mathcal{M}$ nach $\mathcal{P}$ ist, dann gilt für alle Formeln φ, dass $\mathcal{M} \models \phi[\bar{\beta}]$ gdw. $\mathcal{P} \models \phi[\bar{\beta}']$.

Die Äquivalenz in (b) bedeutet, dass

$$\mathcal{M} \models \phi(a_{i_0}, ..., a_{i_{n-1}}) \text{ gdw. } \mathcal{P} \models \phi(\pi(a_{i_0}), ..., \pi(a_{i_{n-1}})),$$

wenn in der Formel φ die Variablen $v_{i_0}, ..., v_{i_{n-1}}$ frei vorkommen und $\bar{\beta}(v_{i_0}) = a_{i_0}$, ..., $\bar{\beta}(v_{i_{n-1}}) = a_{i_{n-1}}$.

Angenommen nun, die Addition wäre über der Struktur $(\mathbb{N}; \cdot)$ definierbar. Dann hätten wir für jeden Isomorphismus[3] $\pi\colon \mathbb{N} \to \mathbb{N}$ von $(\mathbb{N}; \cdot)$ nach $(\mathbb{N}; \cdot)$,

[3] d.h. Automorphismus

dass $\pi(n+m) = \pi(n) + \pi(m)$ für alle n, $m \in \mathbb{N}$. Ein Isomorphismus π ist aber wie folgt gegeben. Sei $p_0 = 2$, $p_1 = 3$, ... die natürliche Aufzählung aller Primzahlen. Setze $\pi(0) = 0$, $\pi(1) = 1$, $\pi(2) = 3$, $\pi(3) = 2$ und $\pi(p_i) = p_i$ für alle $i \geq 2$. Für natürliche Zahlen $n \geq 2$ mit Primfaktorzerlegung

$$n = \prod p_{i_0}^{k_0} \cdot \cdots \cdot p_{i_{m-1}}^{k_{m-1}}$$

ist

$$\pi(n) = \prod \pi(p_{i_0})^{k_0} \cdot \cdots \cdot \pi(p_{i_{m-1}})^{k_{m-1}}.$$

Es gilt aber dann $\pi(1+1) = \pi(2) = 3 \neq 2 = 1+1 = \pi(1) + \pi(1)$.

Wir wollen zeigen, dass die Exponentiation mit Hilfe der Addition und Multiplikation definierbar ist. Wir benutzen hierzu die folgenden beiden einfachen zahlentheoretischen Aussagen, die wir der Vollständigkeit halber ebenfalls beweisen.

Lemma 2.5 (Chinesischer Restsatz) *Sei $m \in \mathbb{N}$, seien $d_0, \ldots, d_m \in \mathbb{N}$ relativ prim, und seinen $a_0, \ldots, a_m \in \mathbb{N}$ so, dass $a_i < d_i$ für $i \leq m$. Dann existiert ein c, so dass*

$$c \equiv a_i \bmod(d_i)$$

für alle $i \leq m$.

Beweis. Wir definieren

$$\Phi\colon \{0, \ldots (d_0 \cdot \cdots \cdot d_m) - 1\} \to \{0, \ldots, d_0 - 1\} \times \cdots \times \{0, \ldots, d_m - 1\}$$

durch $\Phi(c) = (a_0, \ldots, a_m)$, wobei $a_i \equiv c \bmod(d_i)$ für alle $i \leq m$ ist. Die Funktion Φ ist dann injektiv. Ist nämlich $\Phi(c) = \Phi(c')$, dann wird die Differenz $c - c'$ von allen d_i geteilt; da die d_i paarweise relativ prim sind, teilt also $d_0 \cdot \cdots \cdot d_m$ die Differenz $c - c'$. Es folgt dann $c - c' = 0$, also $c = c'$.

Damit ist Φ auch surjektiv, und es gibt ein c wie gewünscht.

Lemma 2.6 *Die $k+1$ zahlen $1 + i \cdot k!$, $1 \leq i \leq k+1$ sind paarweise relativ prim.*

Beweis. Angenommen, die Primzahl p teilt sowohl $1 + i \cdot k!$ als auch $1 + j \cdot k!$, wobei $1 \leq i \leq j \leq k+1$. Dann teilt p also $(j-i) \cdot k!$. Da p die Zahl $k!$ nicht teilen kann, muss also p die Zahl $j - i$ teilen, was wegen $0 \leq j - i \leq k$ nur funktioniert, wenn $j - i = 0$, d.h. $i = j$.

Es gilt $n^0 = 1$ und $n^{m+1} = n^m \cdot n$, so dass n^m das letzte Glied einer Folge $(e_0, e_1, \ldots, e_m)$ der Länge $m+1$ ist mit $e_0 = 1$ und $e_{k+1} = e_k \cdot n$ für alle k

mit $0 < k < m$. Um jedoch über Folgen zu reden, brauchen wir scheinbar die Exponentiation!

Wir lösen dieses Dilemma wie folgt:

Lemma 2.7 *Über* $(\mathbb{N}; <, +, \cdot, 0, 1)$ *ist eine Funktion* $\delta\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *mit folgender Eigenschaft definierbar. Für alle* m, $a_0, \cdots, a_m$ *existiert ein* s, *so dass* $\delta(s, i) = a_i$ *für alle* $i \leq m$.

Korollar 2.8 (K. Gödel) *Die Exponentiation ist über* $(\mathbb{N}; <, +, \cdot, 0, 1)$ *definierbar.*

Beweis des Korollars aus Lemma 2.7: Wir definieren eine Funktion $e\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ über $(\mathbb{N}; <, +, \cdot, 0, 1)$ wie folgt. Sei $e(n, m)$ das kleinste s, so dass $\delta(s, 0) = 1$ und für alle $i < m$: $\delta(s, i+1) = \delta(s, i) \cdot n$. Dann gilt $n^m = \delta(e(n, m), m)$ für alle n, m, und die Exponentiation ist in der Tat über $(\mathbb{N}; <, +, \cdot, 0, 1)$ definierbar.

Wir bereiten nun den Beweis von Lemma 2.7 vor. Wir wollen zunächst $\mathbb{N} \times \mathbb{N}$ aufzählen, indem wir (n, m) vor (n', m') aufzählen gdw. $n+m < n'+m'$ oder $n+m = n'+m'$ und $n < n'$. Es gibt $n+1$ (geordnete) Paare natürlicher Zahlen, deren Summe gleich n ist, nämlich $(0, n)$, $(1, n-1)$, $\cdots$, $(n, 0)$. Also gibt es $\sum_{i=0}^{n-1} i + 1 = \frac{n \cdot (n+1)}{2}$ (geordnete) Paare natürlicher Zahlen, deren Summe kleiner als n ist. Wir schreiben

$$E(n, m) = \frac{(n+m)(n+m+1)}{2} + n.$$

Dann ist E^{-1} Aufzählung von $\mathbb{N} \times \mathbb{N}$ im Sinne der obigen Aufzählungsordnung. Wir können die beiden Komponenten des Paares (n, m) anhand von $E(n, m)$ wie folgt ablesen:

$$L(k) = \text{ dasjenige } n\text{, so dass } k = E(n, m) \text{ für ein } m.$$

$$R(k) = \text{ dasjenige } m\text{, so dass } k = E(n, m) \text{ für ein } n.$$

Die Funktionen E, L und R sind also über $(\mathbb{N}; <, +, \cdot, 0, 1)$ definierbar.

Die Gödelsche β–Funktion $\beta\colon \mathbb{N}^3 \to \mathbb{N}$ ist wie folgt über $(\mathbb{N}; <, +, \cdot, 0, 1)$ definiert:

$$\beta(l, r, i) = \text{ der Rest von } l \text{ bei Division durch } r \cdot (i+1) + 1,$$

d.h.

$$\beta(l, r, i) = \text{ dasjenige } L < r \cdot (i+1) + 1\text{, so dass } L \equiv l \bmod (r \cdot (i+1) + 1$$

$=$ dasjenige $L < r\cdot(i{+}1){+}1$, so dass ein q mit $l = (r\cdot(i{+}1){+}1)\cdot q{+}L$ existiert .

Wir schreiben nun

$$\delta(s, i) = \beta(L(s), R(s), i).$$

Offensichtlich ist dann δ über $(\mathbb{N}; <, +, \cdot, 0, 1)$ definierbar. Mit Hilfe des Chinesischen Restsatzes 2.5 und Lemma 2.6 zeigen wir schliesslich, dass δ der Aussage von Lemma 2.7 genügt.

Seien $m, a_0, \ldots, a_m$ gegeben, und sei k das Maximum von $m, a_0, \ldots, a_m$. Die Zahlen $1 + (i + 1) \cdot k!$, $0 \leq i \leq k$, sind dann nach Lemma 2.6 paarweise relativ prim, so dass nach dem Chinesischen Restsatz 2.5 ein c mit

$$c \equiv a_i \bmod(1 + (i + 1) \cdot k!)$$

für alle $i \leq m$ existiert. Dies bedeutet, dass $a_i = \beta(c, k!, i)$ für alle $i \leq m$. Wenn wir also $s = E(c, k!)$ setzen, dann gilt

$$\delta(s, i) = \beta(L(s), R(s), i) = \beta(c, k!, i) = a_i$$

für alle $i \leq m$ und Lemma 2.7 ist bewiesen.

Kapitel 3

Was ist ein Beweis?

Mathematiker beweisen Sätze. Was aber ist ein Beweis? Seit Euklid gibt es darauf im Wesentlichen *eine* Antwort: ein Beweis ist die logische Ableitung einer Aussage aus einer Menge von vorausgesetzten Aussagen, den "Axiomen". Dies wollen wir nun präzisieren. Wir werden sehen, dass Turing–Maschinen Beweise führen können.

Logische Ableitungen werden mit Hilfe von logischen Regeln vollzogen. Es stellt sich heraus, dass die einzige derartige Regel, die wir wirklich benötigen, der *modus ponens* ist. Der modus ponens ist ein logischer Schluss der folgenden Form:

$$\begin{array}{l} \varphi \to \psi \\ \varphi \\ \hline \psi \end{array}$$

Dieser Schluss ist korrekt in dem Sinne, dass für beliebige Modelle $\mathcal{M}$ und $\mathcal{M}$–Belegungen $\overline{\beta}$ gilt: aus $\mathcal{M} \models \varphi \to \psi[\overline{\beta}]$ und $\mathcal{M} \models \varphi[\overline{\beta}]$ folgt $\mathcal{M} \models \psi[\overline{\beta}]$.

Zusätzlich zu den Axiomen einer bestimmten Theorie benötigen wir immer auch "logische Axiome". Beispielsweise ist die Aussage $\forall v_0\ v_0 = v_0$ ein logisches Axiom: wir wollen sie nicht im Rahmen der Gruppentheorie (oder einer anderen Theorie) jedes Mal eigens fordern wollen.

Bis auf Weiteres fixieren wir eine Sprache $\mathcal{L}$ der Logik erster Stufe. Wir wollen definieren, was es heißt, dass eine $\mathcal{L}$–Formel φ aus einer Menge Γ von $\mathcal{L}$–Formeln beweisbar ist.

Wir definieren zunächst (unabhängig von Γ!) eine feste Menge Λ, die Menge der logischen Axiome.

Eine Formel ψ heißt *Verallgemeinerung* von φ gdw. ψ von der Gestalt

$$\forall v_{i_0} \dots \forall v_{i_{n-1}} \varphi$$

ist. (Dabei erlauben wir $n = 0$; φ ist auch Verallgemeinerung von sich selbst.) Eine $\mathcal{L}$–Formel φ ist ein *logisches Axiom* gdw. φ Verallgemeinerung einer Formel ist, die zu einer der folgenden Klassen gehört:

(1) Tautologien,

(2) Ersetzungsaxiome: $\forall v_i \varphi \to \varphi^{v_i}_{\tau}$, falls τ für v_i in φ einsetzbar ist,

(3) $\forall v_i (\varphi \to \psi) \to (\forall v_i \varphi \to \forall v_i \psi)$,

(4) $\varphi \to \forall v_i \varphi$, falls v_i in φ nicht frei vorkommt,

(5) $v_i = v_i$, und

(6) $v_i = v_j \to (\varphi \to \varphi')$, wobei φ atomar ist und φ' aus φ dadurch entsteht, dass an null oder mehr Stellen v_i durch v_j ersetzt wird.

Wir werden nun diese Klassen erklären. Wir werden sodann sehen, dass jedes logische Axiom logisch gültig ist. (1) Eine Formel φ ist eine *Tautologie* der Logik erster Stufe gdw. es möglich ist, φ auf folgende Art und Weise zu generieren. Es existiert eine aussagenlogische Tautologie ψ, in der als Junktoren lediglich $\neg$ und $\to$ vorkommen und es gibt ein Verfahren der Ersetzung von Aussagenvariablen durch Formeln der Logik erster Stufe, wobei gleiche Aussagenvariablen immer durch gleiche derartige Formeln ersetzt werden, so dass aus ψ die Formel φ hervorgeht.

Beispielsweise ist $A_0 \to (\neg A_1 \to A_0)$ eine aussagenlogische Tautologie. Angenommen, $\mathcal{L}$ enthält das einstellige Prädikatssymbol P. Dann ist

$$\forall v_2 P v_2 \to (\neg P v_0 \to \forall v_2 P v_2)$$

eine Tautologie der Logik erster Stufe. Damit ist übrigens auch

$$\forall v_0 (\forall v_2 P v_2 \to (\neg P v_0 \to \forall v_2 P v_2))$$

ein logisches Axiom. (2) Wir denfinieren zunächst $\varphi^{v_i}_{\tau}$; dies ist das Resultat der Ersetzung von v_i durch τ an allen Stellen, an denen v_i frei vorkommt. Sei φ eine Formel und τ ein Term. Für atomares φ ist $\varphi^{v_i}_{\tau}$ das Resultat der Ersetzung aller Vorkommnisse von v_i in φ durch τ. Sodann gelte[1]

$$(\neg\varphi)^{v_i}_{\tau} \equiv \neg\varphi^{v_i}_{\tau},\ (\varphi \to \psi)^{v_i}_{\tau} \equiv \varphi^{v_i}_{\tau} \to \psi^{v_i}_{\tau}$$

[1] Wir benutzen $\equiv$ zur Mitteilung der Gleichheit zweier Ausdrücke.

und

$$(\forall v_j \varphi)^{v_i}_\tau \equiv \begin{cases} \forall v_j \varphi^{v_i}_\tau, \text{ falls } j \neq i \\ \forall v_j \varphi, \text{ falls } j = i \end{cases}$$

Ist $\forall v_i \varphi \to \varphi^{v_i}_\tau$ immer ein vernünftiges Axiom? Betrachten wir $i = 0$ und $\varphi \equiv \exists v_1\ v_1 \neq v_0$. (D.h. $\varphi \equiv \neg\forall v_1 \neg\neg v_1 = v_0$!) Dann wird aus $\forall v_i \varphi \to \varphi^{v_i}_\tau$ die Formel

$$\forall v_0 \exists v_1\ v_1 \neq v_0 \to \exists v_1\ v_1 \neq v_1,$$

die nicht logisch gültig ist: dies sieht man schnell, indem man ein Modell $\mathcal{M}$ betrachtet, dessen Trägermenge M mindestens zwei Elemente enthält.

Wir lösen dieses Problem, indem wir dieses Axiom nur verlangen, falls τ für v_i in φ eingesetzt werden kann. Wir definieren diese Phrase wie folgt: Für atomares φ kann jedes τ für jedes v_i in φ eingesetzt werden. τ kann für v_i in $\neg\varphi$ eingesetzt werden gdw. τ für v_i in φ eingesetzt werden kann. τ kann für v_i in $\varphi \to \psi$ eingesetzt werden gdw. τ für v_i sowohl in φ als auch in ψ eingesetzt werden kann. τ kann für v_i in $\forall v_j \varphi$ eingesetzt werden gdw. v_i in $\forall v_j \varphi$ nicht frei vorkommt oder v_j in τ nicht vorkommt und τ für v_i in φ eingesetzt werden kann.

Damit kann beispielsweise v_1 für v_0 in $\exists v_1\ v_1 \neq v_0$ nicht eingesetzt werden.

Die Klassen (3), (4), (5) und (6) bedürfen keiner weiteren Erklärung.

Definition 3.1 *Sei* $\Gamma \cup \{\varphi\}$ *eine Menge von Formeln. Ein* Beweis von φ aus Γ *ist eine (endliche!) Folge* $(\varphi_0, \varphi_1, \ldots, \varphi_{N-1})$ *von Formeln, so dass Folgendes gilt:*

(a) $\varphi_{N-1} \equiv \varphi$,

(b) für jedes $i < N$ *ist* $\varphi_i \in \Gamma \cup \Lambda$ *oder es existieren* $j, k < i$*, so dass* φ_i *mit Hilfe des modus ponens aus* φ_j *und* φ_k *hervorgeht, d.h.* $\varphi_j \equiv \varphi_k \to \varphi_i$.

Die Formel φ ist *aus* Γ *beweisbar*, in Zeichen $\Gamma \vdash \varphi$, gdw. es einen Beweis von φ aus Γ gibt. Anstelle von $\emptyset \vdash \varphi$ schreiben wir auch $\vdash \varphi$.

Ein einfaches Beispiel für einen Beweis ist das folgende. Die Sprache $\mathcal{L}$ enthalte die einstelligen Prädikate M und S, sowie die Konstante s. Dann gilt

$$\{\forall v_0(Mv_0 \to Sv_0), Ms\} \vdash Ss.$$

Es ist nämlich $\forall v_0(Mv_0 \to Sv_0) \to (Ms \to Ss)$ ein logisches Axiom; mit Hilfe von $\forall v_0(Mv_0 \to Sv_0)$ ergibt sich daraus durch Anwendung des modus ponens $Ms \to Ss$; unter Verwendung von Ms liefert dann eine weitere Anwendung des modus ponens Ss.

Wir wollen nun den folgenden Korrektheitssatz zeigen: Sei φ aus Γ beweisbar, und sei $\mathcal{M} \models \Gamma[\overline{\beta}]$; dann gilt auch $\mathcal{M} \models \varphi[\overline{\beta}]$.

Wir beschäftigen uns zunächst mit den logischen Axiomen. Die meisten Umstände bereitet die Klasse (2). Für Terme ρ, τ ist $\rho^{v_i}_{\tau}$ das Resultat der Ersetzung aller Vorkommnisse von v_i in ρ durch τ.

Lemma 3.2 *Sei $\mathcal{M}$ ein Modell, und sei $\overline{\beta}$ eine $\mathcal{M}$–Belegung. Seien τ, ρ Terme. Sei β die durch $\overline{\beta}$ induzierte Terminterpretation, und sei $\widetilde{\beta}$ die durch $\overline{\beta}(v_i|\beta(\tau))$ induzierte Terminterpretation. Dann gilt*

$$\beta(\rho^{v_i}_{\tau}) = \widetilde{\beta}(\rho).$$

Beweis durch Induktion nach der "Komplexität" von ρ: Wenn ρ eine Konstante oder eine Variable v_j mit $j \neq i$ ist, dann ist $\rho^{v_i}_{\tau} \equiv \rho$ und $\widetilde{\beta}(\rho) = \beta(\rho)$. Wenn $\rho \equiv v_i$, dann ist $\rho^{v_i}_{\tau} \equiv \tau$, also $\widetilde{\beta}(\rho) = \widetilde{\beta}(v_i) = \beta(\tau) = \beta(\rho^{v_i}_{\tau})$.

Sei schließlich $\rho \equiv f\rho_0 \dots \rho_{n-1}$ für einen n–stelligen Funktor f. Dann gilt

$$\begin{aligned}
&\widetilde{\beta}(\rho) = \widetilde{\beta}(f\rho_0 \dots \rho_{n-1}) = \\
&f^{\mathcal{M}}(\widetilde{\beta}(\rho_0), \dots, \widetilde{\beta}(\rho_{n-1})) = \\
&f^{\mathcal{M}}(\beta((\rho_0)^{v_i}_{\tau}, \dots, \beta(\rho_{n-1})^{v_i}_{\tau})) \text{ nach Induktionsvoraussetzung, } = \\
&\beta(f(\rho_0)^{v_i}_{\tau} \dots (\rho_{n-1})^{v_i}_{\tau}) = \\
&\beta((f\rho_0 \dots \rho_{n-1})^{v_i}_{\tau}) = \beta(\rho^{v_i}_{\tau}).
\end{aligned}$$

□

Lemma 3.3 *Sei $\mathcal{M}$ ein Modell, und sei $\overline{\beta}$ eine $\mathcal{M}$–Belegung. Sei φ eine Formel und τ ein Term, der für v_i in φ eingesetzt werden kann. Sei β die durch $\overline{\beta}$ induzierte Terminterpretation. Dann gilt*

$$\mathcal{M} \models \varphi^{v_i}_{\tau}[\overline{\beta}] \textit{ gdw. } \mathcal{M} \models \varphi[\overline{\beta}(v_i|\beta(\tau))].$$

Beweis durch Induktion nach der "Komplexität" von φ: Sei zunächst φ atomar, etwa $\varphi \equiv P\rho$, wobei P einstelliges Prädikatssymbol und ρ ein Term ist (alle übrigen Fälle sind analog). Dann gilt $\mathcal{M} \models \varphi^{v_i}_{\tau}[\overline{\beta}]$ gdw. $\mathcal{M} \models P\rho^{v_i}_{\tau}[\overline{\beta}]$ gdw. $\beta(\rho^{v_i}_{\tau}) \in P^{\mathcal{M}}$ gdw. $\widetilde{\beta}(\rho) \in P^{\mathcal{M}}$, nach obigem Lemma, wobei $\widetilde{\beta}$ die durch $\overline{\beta}(v_i|\beta(\tau))$ induzierte Terminterpretation ist, gdw. $\mathcal{M} \models P\rho[\overline{\beta}(v_i|\beta(\tau))]$ gdw. $\mathcal{M} \models \varphi[\overline{\beta}(v_i|\beta(\tau))]$. Für $\varphi \equiv \neg\psi$ oder $\varphi \equiv \psi \to \psi'$ ergibt sich die Aussage leicht aus der Induktionsvoraussetzung.

Sei nun $\varphi \equiv \forall v_j \psi$. Falls v_i nicht frei in φ vorkommt, dann stimmen $\overline{\beta}$ und $\overline{\beta}(v_i|\beta(\tau))$ auf den freien Variablen von φ überein und es gilt $\varphi^{v_i}_\tau \equiv \varphi$, so dass die Aussage sehr einfach folgt.

Angenommen nun, v_i kommt frei in φ vor. τ kann für v_i in φ eingesetzt werden, so dass also jetzt v_j in τ nicht vorkommt und τ für v_i in ψ eingesetzt werden kann. Es gilt somit $\mathcal{M} \models \varphi^{v_i}_\tau[\overline{\beta}]$ gdw. $\mathcal{M} \models \forall v_j \psi^{v_i}_\tau[\overline{\beta}]$ gdw. für alle $a \in M$, $\mathcal{M} \models \psi^{v_i}_\tau[\overline{\beta}(v_j|a)]$ gdw. für alle $a \in M$, $\mathcal{M} \models \psi[\overline{\beta}(v_j|a)(v_i|\beta(\tau))]$ wegen Induktionsvoraussetzung, gdw. $\mathcal{M} \models \forall v_j \psi[\overline{\beta}(v_i|\beta(\tau))]$ gdw. $\mathcal{M} \models \varphi[\overline{\beta}(v_i|\beta(\tau))]$. □

Satz 3.4 (Gültigkeitssatz). *Jedes $\varphi \in \Lambda$, d.h. jedes logische Axiom, ist logisch gültig.*

Beweis: Es ist leicht zu sehen, dass mit φ auch jede Verallgemeinerung von φ logisch gültig ist. Es genügt daher zu zeigen, dass jedes Axiom aus einer der Klassen (1) bis (6) logisch gültig ist.

Sei φ zunächst eine Tautologie. Dann existiert eine aussagenlogische Tautologie ψ, in der lediglich die Junktoren $\neg$ und $\to$ vorkommen, und ein Ersetzungsverfahren $A_0 \mapsto \varphi_0$, $A_1 \mapsto \varphi_1, \dots$, das φ produziert. Sei $\mathcal{M}$ ein Modell und $\overline{\beta}$ eine $\mathcal{M}$–Belegung. Wir definieren ein $\overline{\alpha} : \{A_0, A_1, \dots\} \to \{0, 1\}$ durch $\overline{\alpha}(A_n) = 1$ gdw. $\mathcal{M} \models \varphi_n[\overline{\beta}]$. Wenn α die zu $\overline{\alpha}$ gehörige Belegung (im Sinne der Aussagenlogik) ist, dann gilt $\alpha(\psi) = 1$, da ψ Tautologie ist. Daraus folgt aber offensichtlich $\mathcal{M} \models \varphi[\overline{\beta}]$. Da $\mathcal{M}$ und $\overline{\beta}$ beliebig waren, ist φ logisch gültig.

Sei nun eines der Ersetzungsaxiome gegeben. Sei $\mathcal{M}$ ein Modell und $\overline{\beta}$ eine $\mathcal{M}$–Belegung. Sei $\mathcal{M} \models \forall v_i \varphi[\overline{\beta}]$, und sei τ für v_i in φ einsetzbar. Dann gilt, wenn β die durch $\overline{\beta}$ induzierte Terminterpretation ist, $\mathcal{M} \models \varphi[\overline{\beta}(v_i|\beta(\tau))]$, also auch $\mathcal{M} \models \varphi^{v_i}_\tau[\overline{\beta}]$ nach Lemma 3.3. Dies zeigt $\mathcal{M} \models \forall v_i \varphi \to \varphi^{v_i}_\tau[\overline{\beta}]$, falls τ für v_i in φ einsetzbar ist.

Wir zeigen jetzt $\mathcal{M} \models \forall v_i(\varphi \to \psi) \to (\forall v_i \varphi \to \forall v_i \psi)[\overline{\beta}]$ für alle $\mathcal{M}$ und alle $\mathcal{M}$–Belegungen $\overline{\beta}$. Es genügt zu zeigen, dass aus $\mathcal{M} \models \forall v_i(\varphi \to \psi)[\overline{\beta}]$ und $\mathcal{M} \models \forall v_i \varphi[\overline{\beta}]$ folgt, dass $\mathcal{M} \models \forall v_i \psi[\overline{\beta}]$. Sei aber $a \in M$ beliebig. Dann liefert $\mathcal{M} \models \forall v_i \varphi[\overline{\beta}]$, dass $\mathcal{M} \models \varphi[\overline{\beta}(v_i|a)]$, und $\mathcal{M} \models \varphi \to \psi[\overline{\beta}(v_i|a)]$. Damit gilt dann auch $\mathcal{M} \models \psi[\overline{\beta}(v_i|a)]$.

Die logische Gültigkeit von Formeln aus der Klasse (4) ist einfach zu sehen: Wegen Satz 2.2 gilt, wenn v_i in φ nicht frei vorkommt, für ein beliebiges Modell $\mathcal{M}$, für eine beliebige M–Belegung $\overline{\beta}$ und für ein beliebiges $a \in M$, $\mathcal{M} \models \varphi[\overline{\beta}]$ gdw. $\mathcal{M} \models \varphi[\overline{\beta}(v_i|a)]$. Also gilt dann auch $\mathcal{M} \models \varphi[\overline{\beta}]$ gdw. $\mathcal{M} \models \forall v_i \varphi[\overline{\beta}]$

Die logische Gültigkeit von Formeln aus der Klasse (5) ist trivial.

Sei nun ein Axiom aus Klasse (6) gegeben, d.h. etwa $v_i = v_j \to (\varphi \to \varphi')$, wobei φ atomar ist und φ' aus φ hervorgeht, indem an null oder mehr Stellen v_i durch v_j ersetzt wird. Sei etwa φ von der Gestalt $P\tau_0 \dots \tau_{n-1}$, wobei P n–stellig ist. Es genügt zu zeigen, dass aus $\mathcal{M} \models v_i = v_j[\overline{\beta}]$ und $\mathcal{M} \models \varphi[\overline{\beta}]$ folgt, dass $\mathcal{M} \models \varphi'[\overline{\beta}]$. Sei also β die durch $\overline{\beta}$ induzierte Terminterpretation, und sei φ' gleich $P\tau'_0 \dots \tau'_{n-1}$ (so dass τ'_i aus τ_i hervorgeht, indem an null oder mehr Stellen v_i durch v_j ersetzt wird). Dann gilt offenbar $\mathcal{M} \models \varphi[\overline{\beta}]$ gdw. $(\beta(\tau_0), \dots, \beta(\tau_{n-1})) \in P^{\mathcal{M}}$ gdw. $(\beta(\tau'_0), \dots, \beta(\tau'_{n-1})) \in P^{\mathcal{M}}$ gdw. $\mathcal{M} \models \varphi'[\overline{\beta}]$. □

Wir zeigen nun, dass aus $\Gamma \vdash \varphi$ folgt, dass $\Gamma \models \varphi$. Der Gödelsche Vollständigkeitssatz wird sagen, dass sogar die Umkehrung gilt.

Satz 3.5 (Korrektheitssatz). *Sei $\Gamma \cup \{\varphi\}$ eine Menge von Formeln. Wenn $\Gamma \vdash \varphi$, dann gilt auch $\Gamma \models \varphi$.*

Beweis: Sei $\Gamma \vdash \varphi$ vorausgesetzt. Sei $(\varphi_0, \varphi_1, \dots, \varphi_{N-1})$ ein Beweis von φ aus Γ. Es ist leicht zu sehen, dass dann auch für jedes $n \leq N (\varphi_0, \dots, \varphi_{n-1})$ ein Beweis von φ aus Γ ist.

Sei $\mathcal{M}$ ein Modell, und sei $\overline{\beta}$ eine $\mathcal{M}$–Belegung. Wir müssen zeigen, dass aus $\mathcal{M} \models \Gamma[\overline{\beta}]$ folgt, dass $\mathcal{M} \models \varphi[\overline{\beta}]$. Wir zeigen durch Induktion nach $n \leq N$, dass $\mathcal{M} \models \varphi_{n-1}[\overline{\beta}]$.

Sei also $n > 0$ und gelte $\mathcal{M} \models \Gamma[\overline{\beta}]$, sowie $\mathcal{M} \models \varphi_i[\overline{\beta}]$ für alle $i < n-1$. Falls dann $\varphi_{n-1} \in \Gamma \cup \Lambda$, haben wir $\mathcal{M} \models \varphi_{n-1}[\overline{\beta}]$ (für $\varphi_{n-1} \in \Lambda$ benutzt dies den Gültigkeitssatz).

Andernfalls existieren $j, k < n-1$ mit $\varphi_j \equiv \varphi_k \to \varphi_{n-1}$. Dann folgt aber aus $\mathcal{M} \models \varphi_k \to \varphi_{n-1}[\overline{\beta}]$ und $\mathcal{M} \models \varphi_k[\overline{\beta}]$ sofort $\mathcal{M} \models \varphi_{n-1}[\overline{\beta}]$. □

Eine Menge Γ von Formeln heißt *(syntaktisch) konsistent* gdw. es keine Formel φ gibt, so dass Γ sowohl φ als auch $\neg\varphi$ beweist. Γ heißt *erfüllbar* (oder *semantisch konsistent*) gdw. ein Modell $\mathcal{M}$ und eine $\mathcal{M}$–Belegung $\overline{\beta}$ mit $\mathcal{M} \models \Gamma[\overline{\beta}]$ existieren. Der Korrektheitssatz besitzt folgendes

Korollar 3.6 *Sei Γ eine Menge von Formeln. Wenn Γ erfüllbar ist, dann ist Γ konsistent.*

Während, wie wir sehen werden, $\{\varphi : \emptyset \vdash \varphi\}$ nicht entscheidbar ist, gilt folgender

Satz 3.7 *Sei die Sprache $\mathcal{L}$ gegeben durch I, J, K, wobei $I \cup J \cup K$ höchstens abzählbar ist. Sei Γ eine rekursiv aufzählbare Menge von $\mathcal{L}$-Formeln. Dann ist auch $\{\varphi : \Gamma \vdash \varphi\}$ rekursiv aufzählbar.*

Beweis: Zunächst ist $\{\varphi : \varphi \text{ ist ein logisches Axiom}\}$ entscheidbar. Jedes logische Axiom ist nämlich Verallgemeinerung eines Axioms aus einer der Klassen (1) bis (6). Dass die Menge der Tautologien aus (1) entscheidbar ist, kann mit den Methoden des 2. Kapitels gezeigt werden. Dass die Mengen von Axiomen, die zu den Klassen (2) bis (6) gehören, entscheidbar ist, zeigt man mit ähnlichen Mitteln.

Sei nun Γ rekursiv aufzählbar. Sei $\top_\Gamma$ eine Turing–Maschine, die dies bezeugt (d.h. $\top_\Gamma(\psi) \downarrow +$ gdw. $\psi \in \Gamma$). Wir bauen nun eine Turing–Maschine $\top$, die Folgendes leistet.

Es werde φ eingegeben. Hinter φ schreibt $\top$ in der n^{ten} Runde jeweils voneinander abgetrennt durch ein Trennungszeichen, etwa #, alle Ausdrücke der Sprache $\mathcal{L}$ der Länge $\leq n$ nebeneinander auf das Rechenband.[2] Diejenigen von ihnen werden markiert, die entweder ein logisches Axiom sind, oder die von $\top_\Gamma$ in $\leq n$ Rechenschritten als Element von Γ erkannt werden. Sodann schreibt $\top$ (immer noch in der n^{ten} Runde) hinter die entstandene Liste wieder jeweils abgetrennt voneinander alle Beweise

$$(\varphi_0, \varphi_1, \dots, \varphi_{N-1})$$

mit $N \leq n$, wobei aber jedes φ_i entweder *eines der nun markierten* Axiome aus $\Lambda \cup \Gamma$ ist oder durch modus ponens aus früheren φ_j und φ_k hervorgeht. Falls dabei φ als eine Formel φ_{N-1} in einem solchen Beweis gesichtet wird, akzeptiert $\top$ die Eingabe φ. Andernfalls begibt sich $\top$ in die $(n+1)^{\text{te}}$ Runde.

Offensichtlich folgt aus $\top(\varphi) \downarrow +$, dass $\Gamma \vdash \varphi$. Wenn aber Γ die Formel φ beweist, dann existiert ein $n \in \mathbb{N}$, so dass $(\varphi_0, \varphi_1, \dots, \varphi_{N-1})$ ein Beweis von φ aus Γ ist, für den gilt: $N \leq n$, jedes $\varphi_i \in \Lambda \cup \Gamma$ hat Länge $\leq n$, und für $\varphi_i \in \Gamma$ erkennt $\top_\Gamma$ in $\leq n$ Rechenschritten, dass φ_i in Γ ist; also gilt dann auch $\top(\varphi) \downarrow +$. $\square$

[2] Wir fassen dabei, analog zur Verfahrensweise hinsichtlich der Aussagenvariablen im 2. Kapitel, die Variable v_n etwa als eine Folge von $n+1$ Symbolen $*$ auf.

Kapitel 4

Der Gödelsche Vollständigkeitssatz

Wir beweisen zunächst einige Lemmata zur Beweisbarkeit.

Die Formeln $\varphi_0, \ldots, \varphi_{n-1}$ *implizieren tautologisch* die Formel ψ gdw. die Formel

$$\varphi_0 \to (\varphi_1 \to (\ldots(\varphi_{n-1} \to \psi)\ldots))$$

eine Tautologie ist (vgl. Definition 1.1).

Lemma 4.1 (Tautologische Implikation) *Wenn die Formelmenge Γ die Formeln $\varphi_0, \ldots, \varphi_{n-1}$ beweist und wenn $\varphi_0, \ldots, \varphi_{n-1}$ tautologisch ψ implizieren, dann beweist Γ die Formel ψ.*

Beweis: $\varphi_0 \to (\varphi_1 \to (\ldots(\varphi_{n-1} \to \psi)\ldots))$ ist Tautologie, also aus Γ beweisbar. Da $\varphi_0, \ldots, \varphi_{n-1}$ aus Γ beweisbar sind, liefert eine n–fache Anwendung des modus ponens, dass auch ψ beweisbar ist. $\square$

Lemma 4.2 (Deduktion) *Wenn die Formelmenge $\Gamma \cup \{\varphi\}$ die Formel ψ beweist, dann beweist Γ die Formel $\varphi \to \psi$.*

Beweis: Sei $(\varphi_0, \ldots, \varphi_{N-1})$ ein Beweis von ψ aus $\Gamma \cup \{\varphi\}$. Wir zeigen durch Induktion nach $i < N$, dass $\Gamma \vdash \varphi \to \varphi_i$.

1. Fall: $\varphi_i \equiv \varphi$. Dann ist $\varphi \to \varphi_i$ Tautologie und wird von Γ bewiesen.

2. Fall: $\varphi_i \in \Gamma \cup \Lambda$. Da φ_i tautologisch $\varphi \to \varphi_i$ impliziert, folgt mit dem Lemma zur tautologischen Implikation aus $\Gamma \vdash \varphi_i$, dass $\Gamma \vdash \varphi \to \varphi_i$.

3. Fall: φ_i geht durch modus ponens aus φ_j, φ_k hervor, d.h. $\varphi_k \equiv \varphi_j \to \varphi_i$, wobei $j, k < i$. Nach Induktionsannahme sind $\varphi \to \varphi_j$ und $\varphi \to \varphi_k$ (d.h. $\varphi \to (\varphi_j \to \varphi_i)$) aus Γ beweisbar. Da $\varphi \to \varphi_j$, $\varphi \to (\varphi_j \to \varphi_i)$ tautologisch $\varphi \to \varphi_i$ implizieren, folgt mit dem Lemma zur tautologischen Implikation aus $\Gamma \vdash \varphi \to \varphi_j$ und $\Gamma \vdash \varphi \to (\varphi_j \to \varphi_i)$, dass $\Gamma \vdash \varphi \to \varphi_i$. □

Eine Formelmenge Γ heißt *inkonsistent* gdw. Γ nicht konsistent ist.

Lemma 4.3 (Widerspruchsbeweis) *Sei die Formelmenge $\Gamma \cup \{\varphi\}$ inkonsistent. Dann gilt $\Gamma \vdash \neg\varphi$.*

Beweis: Sei ψ so, dass $\Gamma \cup \{\varphi\} \vdash \psi$ und $\Gamma \cup \{\varphi\} \vdash \neg\psi$. Nach obigem Lemma zur Deduktion gilt dann $\Gamma \vdash \varphi \to \psi$ und auch $\Gamma \vdash \varphi \to \neg\psi$. Da aber $\varphi \to \psi$, $\varphi \to \neg\psi$ tautologisch $\neg\varphi$ implizieren, gilt dann auch $\Gamma \vdash \neg\varphi$ nach dem Lemma zur tautologischen Implikation. □

Lemma 4.4 (Verallgemeinerung 1) *Sei Γ eine Formelmenge, und sei $i \in \mathbb{N}$ so, dass v_i in keiner Formel aus Γ frei vorkommt. Sei φ eine Formel mit $\Gamma \vdash \varphi$. Dann gilt auch $\Gamma \vdash \forall v_i \varphi$.*

Beweis: Sei $(\varphi_0, \ldots, \varphi_{N-1})$ ein Beweis von φ aus Γ. Wir zeigen durch Induktion nach $j < N$, dass $\Gamma \vdash \forall v_i \varphi_j$.

1. Fall: $\varphi_j \in \Lambda$. Dann ist auch $\forall v_i \varphi_j \in \Lambda$, mithin $\Gamma \vdash \forall v_i \varphi_j$.

2. Fall: $\varphi_j \in \Gamma$. Da v_i nicht frei in φ_j vorkommt, ist $\varphi_j \to \forall v_i \varphi_j$ ein logisches Axiom der Klasse (4). Aus $\Gamma \vdash \varphi_j$ und $\Gamma \vdash \varphi_j \to \forall v_i \varphi_j$ ergibt sich dann $\Gamma \vdash \forall v_i \varphi_j$.

3. Fall: Es existieren $k, l < j$ mit $\varphi_l \equiv \varphi_k \to \varphi_j$. Nach Induktionsvoraussetzung gilt sowohl $\Gamma \vdash \forall v_i \varphi_k$ als auch $\Gamma \vdash \forall v_i \varphi_l$ (d.h. $\forall v_i (\varphi_k \to \varphi_j)$). Nun ist aber $\forall v_i (\varphi_k \to \varphi_j) \to (\forall v_i \varphi_k \to \forall v_i \varphi_j)$ ein logisches Axiom der Klasse (3). Damit ergibt sich nun leicht, dass $\Gamma \vdash \forall v_i \varphi_j$. □

Wir benötigen die folgenden Tatsachen zur Ersetzbarkeit. Hierbei ist φ eine Formel, τ ist ein Term, c ist eine Konstante, und $i, j, k \in \mathbb{N}$.

(a) v_i kann für v_i in φ eingesetzt werden.

(b) Wenn keine in φ vorkommende Variable in τ vorkommt, dann kann τ für v_i in φ eingesetzt werden.

(c) Wenn v_j nicht in φ vorkommt, dann kann v_i für v_j in $\varphi^{v_i}_{v_j}$ eingesetzt werden und es gilt $(\varphi^{v_i}_{v_j})^{v_j}_{v_i} \equiv \varphi$.

(d) Wenn $i \neq k$ und wenn τ für v_i in φ eingesetzt werden kann, dann kann τ für v_i in $\varphi^{v_i}_{v_k}$ eingesetzt werden.

(e) Wenn τ für v_i in φ eingesetzt werden kann und wenn v_j nicht in φ vorkommt, dann kann der Term $\tau^c_{v_j}$ für v_i in $\varphi^c_{v_j}$ eingesetzt werden. ($\tau^c_{v_j}$ bzw. $\varphi^c_{v_j}$ entsteht aus τ bzw. φ, indem überall c durch v_j ersetzt wird.)

Die folgenden beiden Lemmata lassen sich ähnlich zeigen wie obiges 1. Lemma zur Verallgemeinerung.

Lemma 4.5 (Verallgemeinerung 2) *Sei $\Gamma \cup \{\varphi\}$ eine Formelmenge, und sei c eine Konstante, die in keiner der Formeln aus Γ vorkommt. Sei $\Gamma \vdash \varphi$. Dann existiert ein $i \in \mathbb{N}$, so dass v_i nicht in φ vorkommt, $\Gamma \vdash \varphi^c_{v_i}$ und $\Gamma \vdash \forall v_i \varphi^c_{v_i}$, und es gibt Beweise sowohl von $\varphi^c_{v_i}$ als auch von $\forall v_i \varphi^c_{v_i}$ aus Γ, so dass c in keiner Formel dieser Beweise vorkommt.*

Lemma 4.6 (Verallgemeinerung 3) *Sei $\Gamma \cup \{\varphi\}$ eine Formelmenge, sei $i \in N$, und sei c eine Konstante, die in keiner Formel aus $\Gamma \cup \{\varphi\}$ vorkommt. Dann folgt aus $\Gamma \vdash \varphi^{v_i}_c$, dass $\Gamma \vdash \forall v_i \varphi$.*

Wir benötigen schließlich die folgenden weiteren Tatsachen, die leicht einzusehen sind.

Variablen–Umbenennung: Sei φ ein Formel, sei τ ein Term, und sei $i \in \mathbb{N}$. Dann existiert eine Formel φ', so dass τ für v_i in φ' eingesetzt werden kann, und es gilt sowohl $\vdash \varphi \to \varphi'$ als auch $\vdash \varphi' \to \varphi$. (Man erhält φ' durch Umbenennung der gebundenen, d.h. nicht freien Variablen.)

Tatsachen zur Gleichheit:

(a) $\vdash \forall v_i\, v_i = v_i$

(b) $\vdash \forall v_i \forall v_j (v_i = v_j \to v_j = v_i)$

(c) $\vdash \forall v_i \forall v_j \forall v_k (v_i = v_j \to (v_j = v_k \to v_i = v_k))$.
$(v_i = v_j \to (v_i = v_k \to v_j = v_k)$ ist ein logisches Axiom der Klasse (6). $(v_i = v_j \to (v_i = v_k \to v_j = v_k)) \to (v_i = v_j \to (v_j = v_k \to v_i = v_k))$ ist ein logisches Axiom der Klasse (1). Dies liefert (c), mit Hilfe des modus ponens. Insbesondere ist aber auch $v_i = v_j \to (v_i = v_i \to v_j =$

v_i) logisches Axiom der Klasse (6). Da $v_i = v_i$ logisches Axiom der Klasse (5) ist und $v_i = v_i,\ v_i = v_j \to (v_i = v_i \to v_j = v_i)$ tautologisch $v_i = v_j \to v_j = v_i$ implizieren, sieht man dann (b).)

(d) Sei P ein n–stelliges Prädikatsymbol. Dann gilt

$$\vdash \forall v_{i_0} \forall v_{i'_0} \dots \forall v_{i_{n-1}} \forall v_{i'_{n-1}} (v_{i_0} = v_{i'_0} \to$$
$$(\dots (v_{i_{n-1}} = v_{i'_{n-1}} \to (P v_{i_0} \dots v_{i_{n-1}} \to P v_{i'_0} \dots v_{i'_{n-1}})) \dots)).$$

(e) Sei f ein n–stelliger Funktor. Dann gilt

$$\vdash \forall v_{i_0} \forall v_{i'_0} \dots \forall v_{i_{n-1}} \forall v_{i'_{n-1}} (v_{i_0} = v_{i'_0} \to$$
$$(\dots (v_{i_{n-1}} = v_{i'_{n-1}} \to f v_{i_0} \dots v_{i_{n-1}} = f v_{i'_0} \dots v_{i'_{n-1}}) \dots)).$$

Wir beweisen nun den GÖDELschen Vollständigkeitssatz. Dieser lautet wie folgt.

Satz 4.7 (Gödelscher Vollständigkeitssatz)

(*) Sei $\Gamma \cup \{\varphi\}$ ein Menge von Formeln. Wenn Γ (logisch) φ impliziert, dann ist φ aus Γ beweisbar. D.h. wenn $\Gamma \models \varphi$, dann gilt auch $\Gamma \vdash \varphi$.

(**) Jede (syntaktisch) konsistente Formelmenge ist erfüllbar (d.h. semantisch konsistent).

Zusammen mit dem Korrektheitssatz besagt dies also, dass $\Gamma \models \varphi$ gdw. $\Gamma \vdash \varphi$. Der Gödelsche Vollständigkeitssatz teilt mit, dass die Beweismethoden, die wir vorgestellt haben, vollständig sind.

Beweis des Vollständigkeitssatzes: Wir zeigen zunächst, dass (*) aus (**) folgt. Angenommen, $\Gamma \models \varphi$. Dann kann mit Hilfe von (**) $\Gamma \cup \{\neg\varphi\}$ nicht konsistent sein, da sonst $\Gamma \cup \{\neg\varphi\}$ erfüllbar wäre im Widerspruch zu $\Gamma \models \varphi$. Aus der Inkonsistenz von $\Gamma \cup \{\neg\varphi\}$ ergibt sich aber $\Gamma \vdash \neg\neg\varphi$ mit dem obigen Lemma zum Widerspruchsbeweis. Da aber $\neg\neg\varphi$ tautologisch φ impliziert, gilt dann auch $\Gamma \vdash \varphi$ wie gewünscht.

Es bleibt also, (*) zu beweisen. Sei Γ eine konsistente Menge von Formeln, wobei nun daran erinnert sei, dass diese Formeln $\mathcal{L}$–Formeln sind für eine Sprache $\mathcal{L}$ der Logik 1. Stufe. Der Beweis von (*) hat Ähnlichkeiten mit dem Beweis des Kompaktheitssatzes der Aussagenlogik. Wir werden Γ zu einer Menge Δ von Formeln einer reicheren Sprache $\mathcal{L}^*$ vergrößern, so dass Folgendes gilt:

(a) $\Gamma \subset \Delta$,

(b) Δ ist *maximal–konsistent*, d.h. Δ ist konsistent und für jede $\mathcal{L}^*$–Formel φ gilt $\varphi \in \Delta$ oder $\neg\varphi \in \Delta$, und

(c) Δ ist eine *Henkin–Menge*, d.h. für jede $\mathcal{L}^*$–Formel φ und für jedes $i \in \mathbb{N}$ existiert eine Konstante $c = c(\varphi, i)$, so dass $\neg\forall v_i\varphi \to \neg\varphi^{v_i}_c$ Element von Δ ist.[1]

Sodann verwenden wir Δ, um ein Modell $\mathfrak{M}$ und eine M–Belegung $\overline{\beta}$ mit $\mathfrak{M} \models \Delta[\overline{\beta}]$ zu konstruieren. Dies liefert dann auch ein Modell $\overline{\mathfrak{M}}$ (mit gleicher Trägermenge wie $\mathfrak{M}$), so dass $\overline{\mathfrak{M}} \models \Gamma[\overline{\beta}]$. $\overline{\mathfrak{M}}$ und $\overline{\beta}$ bezeugen also, dass Γ erfüllbar ist.

Für die Konstruktion von Δ benötigen wir die folgende Aussage.

Satz 4.8 (Hausdorffsches Maximalitätsprinzip) *Sei F eine beliebige Menge, und sei $\mathcal{F}$ eine Menge von Teilmengen F. Angenommen, es gilt Folgendes: für alle $\overline{\mathcal{F}} \subset \mathcal{F}$, so dass $X \subset Y$ oder $Y \subset X$ für beliebige $X, Y \in \overline{\mathcal{F}}$, ist auch $\bigcup \overline{\mathcal{F}} = \{a \in F : a \in X \text{ für ein } X \in \overline{\mathcal{F}}\}$ Element von $\mathcal{F}$. Dann existiert ein $X_{\max} \in \mathcal{F}$, so dass keine echte Obermenge von $X_{\max}$ ebenfalls ein Element von $\mathcal{F}$ ist.*

Das Hausdorffsche Maximalitätsprinzip ist äquivalent sowohl zum Zornschen Lemma als auch zum Auswahlaxiom.

Wir beginnen damit, $\mathcal{L}^*$ zu definieren. Wir setzen $\mathcal{L}_0 = \mathcal{L}$. Sei $\mathcal{L}_n, n \in \mathbb{N}$, gegeben. Für jedes Paar (i, φ), wobei $i \in \mathbb{N}$ und φ eine $\mathcal{L}_n$–Formel ist, wählen wir eine eigene neue Konstante $c = c(i, \varphi)$, die wir zur Sprache $\mathcal{L}_n$ hinzufügen; $\mathcal{L}_{n+1}$ ist die Sprache $\mathcal{L}_n$, erweitert genau um all diese Konstanten $c(i, \varphi)$. Schließlich sei $\mathcal{L}^*$ die "Vereinigung" aller Sprachen $\mathcal{L}_n, n \in \mathbb{N}$. Offensichtlich gilt für $\mathcal{L}^*$ Folgendes: für jedes Paar (i, φ), wobei $n \in \mathbb{N}$ und φ eine $\mathcal{L}^*$–Formel ist, existiert eine eigene Konstante $c(i, \varphi)$ der Sprache $\mathcal{L}^*$.

Wir fassen jetzt Γ als Menge von Formeln der erweiterten Sprache $\mathcal{L}^*$ auf. Als Menge von $\mathcal{L}$–Formeln war Γ als (syntaktisch) konsistent vorausgesetzt. Auch wenn es eine Subtilität darstellt, wir müssen uns nun überzeugen, dass Γ als Menge von $\mathcal{L}^*$–Formeln weiterhin (syntaktisch) konsistent ist.

Angenommen, es gibt eine $\mathcal{L}^*$–Formel φ, so dass sowohl $\Gamma \vdash \varphi$ als auch $\Gamma \vdash \neg\varphi$ gilt. In den in den Beweisen von φ und $\neg\varphi$ auftauchenden Formeln kommen nur endlich viele der neuen Konstanten der Form $c(i, \overline{\varphi})$ vor. Seien dies etwa k viele, $c_0, \ldots, c_{k-1}$. Auf Grund von k–facher

[1] Für $\varphi \equiv \neg\psi$ ist $\neg\forall v_i\varphi \to \neg\varphi^{v_i}_c$ im Wesentlichen die Formel $\exists v_i\psi \to \psi^{v_i}_c$.

Anwendung des 2. Lemmas zur Verallgemeinerung existieren dann Variablen $v_{i_0}, \ldots, v_{i_{k-1}}$, so dass Γ auch die Formeln $\varphi' \equiv (\ldots(\varphi^{c_0}_{v_{i_0}})\ldots)^{c_{k-1}}_{v_{i_{k-1}}}$ und $\neg\varphi' \equiv (\ldots(\neg\varphi^{c_0}_{v_{i_0}})\ldots)^{c_{k-1}}_{v_{i_{k-1}}}$ beweist. (Die Konstanten $c_0, \ldots, c_{k-1}$ kommen ja in den Formeln von Γ nicht vor.) Darüber hinaus gibt es Beweise dieser beiden Formeln, so dass $c_0, \ldots, c_{k-1}$ nicht mehr in den Formeln dieser Beweise vorkommen. Wir sehen, dass es Beweise dieser beiden Formeln φ' und $\neg\varphi'$ gibt, die nur aus $\mathcal{L}$–Formeln bestehen. Dies widerspricht der (syntaktischen) Konsistenz von Γ (als Menge von $\mathcal{L}$–Formeln).

Wir erweitern nun die Formelmenge Γ. Wir setzen $\Gamma_H = \Gamma \cup H$, wobei H alle Formeln der Gestalt $\neg\forall v_i\varphi \to \neg\varphi^{v_i}_{c(i,\varphi)}$ enthält, wobei $i \in \mathbb{N}$ und φ eine $\mathcal{L}^*$–Formel ist. Wir behaupten, dass Γ_H ebenfalls (syntaktisch) konsistent ist.

Wenn Γ_H nicht konsistent ist, dann existiert offensichtlich eine endliche Teilmenge $\overline{H}$ von H, so dass $\Gamma \cup \overline{H}$ inkonsistent ist. Sei $m_0 \in \mathbb{N}$ das kleinste m, so dass ein m–elementiges $\overline{H} \subset H$ existiert, so dass $\Gamma \cup \overline{H}$ inkonsistent ist. Da Γ konsistent ist, ist $m_0 > 0$. Sei $\neg\forall v_i\varphi \to \neg\varphi^{v_i}_{c(i,\varphi)}$ in $\overline{H}$, und sei $\overline{H}_0 = \overline{H} \setminus \{\neg\forall v_i\varphi \to \neg\varphi^{v_i}_{c(i,\varphi)}\}$. $\Gamma \cup \overline{H}_0$ ist also konsistent.

Schreibe $c = c(i,\varphi)$. Da $\Gamma \cup \overline{H} = \Gamma \cup \overline{H}_0 \cup \{\neg\forall v_i\varphi \to \neg\varphi^{v_i}_c\}$ inkonsistent ist, beweist nach dem Lemma zum Widerspruchsbeweis $\Gamma \cup \overline{H}_0$ die Formel $\neg(\neg\forall v_i\varphi \to \neg\varphi^{v_i}_c)$, d.h. die Formel $\neg\forall v_i\varphi \wedge \varphi^{v_i}_c$. Da diese Formel $\varphi^{v_i}_c$ tautologisch impliziert, beweist $\Gamma \cup \overline{H}_0$ also auch $\varphi^{v_i}_c$. Die Konstante c kommt aber in keiner Formel aus $\Gamma \cup \overline{H}_0$ vor, so dass nach dem 3. Lemma zur Verallgemeinerung $\Gamma \cup \overline{H}_0$ die Formel $\forall v_i\varphi$ beweist. Andererseits impliziert $\neg\forall v_i\varphi \wedge \varphi^{v_i}_c$ tautologisch $\neg\forall v_i\varphi$, so dass aus $\Gamma \cup \overline{H}_0 \vdash \neg\forall v_i\varphi \wedge \varphi^{v_i}_c$ auch $\Gamma \cup \overline{H}_0 \vdash \neg\forall v_i\varphi$ folgt. $\Gamma \cup \overline{H}_0$ beweist also sowohl $\neg\forall v_i\varphi$ als auch $\forall v_i\varphi$, ist also inkonsistent.

Dieser Widerspruch zeigt, dass Γ_H konsistent ist.

Wir wollen nun Γ_H zu einer maximal–konsistenten Menge Δ von $\mathcal{L}^*$–Formeln erweitern. Hierzu benutzen wir einfach das Hausdorffsche Maximalitätsprinzip. Sei $\mathcal{F}$ die Gesamtheit aller konsistenten Mengen X von $\mathcal{L}^*$–Formeln mit $X \supset \Gamma_H$. Da Beweise endlich sind, überzeugt man sich sehr leicht, dass $\mathcal{F}$ die Voraussetzung des Hausdorffschen Maximalitätsprinzips erfüllt.

Sei $X_{\max} \in \mathcal{F}$, so dass keine echte Obermenge von $X_{\max}$ auch in $\mathcal{F}$ ist. Schreibe $\Delta = X_{\max}$. Sei φ eine beliebige $\mathcal{L}^*$–Formel. Entweder $\Delta \cup \{\varphi\}$ oder $\Delta \cup \{\neg\varphi\}$ ist konsistent, da ansonsten Δ sowohl φ als auch $\neg\varphi$ bewiese, also inkonsistent wäre. Δ ist als Element von $\mathcal{F}$ aber konsistent. Da Δ keine konsistente echte Obermenge besitzt, ist also $\Delta \cup \{\varphi\} = \Delta$ (d.h. $\varphi \in \Delta$) oder $\Delta \cup \{\neg\varphi\} = \Delta$ (d.h. $\neg\varphi \in \Delta$). Δ ist also maximal–konsistent. Außerdem ist

$\Gamma \subset \Delta$, und Δ ist eine Henkin–Menge.

Wir konstruieren nun ein Modell von Δ.

Aufgrund der Maximalität von Δ sind für eine beliebige $\mathcal{L}^*$–Formel φ die folgenden Aussagen äquivalent: $\Delta \cup \{\varphi\}$ ist konsistent; $\varphi \in \Delta$; $\Delta \vdash \varphi$; $\Delta \cup \{\neg\varphi\}$ ist inkonsistent; $\neg\varphi \notin \Delta$; es gilt nicht $\Delta \vdash \neg\varphi$. Entsprechend sind für beliebige $\mathcal{L}^*$–Formeln die folgenden Aussagen äquivalent: wenn $\psi \in \Delta$, dann $\psi' \in \Delta$; $\psi \to \psi' \in \Delta$. Da Δ darüber hinaus eine Henkin–Menge ist, gilt für $i \in \mathbb{N}$ und eine beliebige $\mathcal{L}^*$-Formel: wenn $\neg\forall v_i \varphi \in \Delta$, dann existiert eine Konstante c (nämlich $c(i,\varphi)$), so dass $\neg\varphi^{v_i}_c \in \Delta$.

Wir konstruieren $\mathfrak{M}$ als "Termmodell".

Da Δ eine Henkin–Menge ist, haben wir genug Terme zur Verfügung. Da Δ maximal ist, ist die Theorie von $\mathfrak{M}$ vollständig festgelegt.

Die Trägermenge von $\mathfrak{M}$ besteht aus Äquivalenzklassen von Termen. Für $\mathcal{L}^*$–Terme τ und σ schreiben wir $\tau{\sim}\sigma$ (τ und σ sind *äquivalent*) gdw. die Formel $\tau = \sigma$ zu Δ gehört.

Wir behaupten, dass $\sim$ eine Äquivalenzrelation auf der Menge aller $\mathcal{L}^*$–Terme ist. Hierzu ist für beliebige $\mathcal{L}^*$–Terme τ, σ, ρ Folgendes zu zeigen:

(a) $\tau = \tau \in \Delta$.

(b) $\tau = \sigma \in \Delta \Rightarrow \sigma = \tau \in \Delta$

(c) $\tau = \sigma \in \Delta$ und $\sigma = \rho \in \Delta \Rightarrow \tau = \rho \in \Delta$

Betrachten wir etwa (b). Sei $\tau = \sigma \in \Delta$, d.h. $\Delta \vdash \tau = \sigma$. Die obige Tatsache (b) zur Gleichheit sagt, dass $\Delta \vdash \forall v_i \forall v_j (v_i = v_j \to v_j = v_i)$. Mit Hilfe der logischen Axiomenklasse (2) und zweifacher Anwendung des modus ponens sieht man dann

$$\Delta \vdash \tau = \sigma \to \sigma = \tau;$$

nochmalige Anwendung des modus ponens gibt schließlich $\Delta \vdash \sigma = \tau$, also

$$\sigma = \tau \in \Delta.$$

Analog beweist man (a) bzw. (c) mit Hilfe der Tatsachen (a) bzw. (c) zur Gleichheit.

Für einen $\mathcal{L}^*$–Term τ schreiben wir nun $[\tau]$ für $\{\sigma : \sigma{\sim}\tau\}$, d.h. für die zu τ gehörige Äquivalenzklasse von Termen. Es gilt $\sigma{\sim}\tau$ gdw. $[\sigma] = [\tau]$.

Es sei dann M die Menge aller Äquivalenzklassen $[\tau]$ für $\mathcal{L}^*$–Terme τ. M ist die Trägermenge unseres Modells $\mathfrak{M}$. Wir können nun $\mathfrak{M}$ definieren; hierzu müssen wir für jedes Prädikatsymbol P die Interpretation $P^{\mathfrak{M}}$, für jeden

Funktor f die Interpretation $f^{\mathfrak{M}}$ und für jede Konstante c die Interpretation $c^{\mathfrak{M}}$ angeben.

Sei zunächst c eine Konstante von $\mathcal{L}^*$. Wir setzen dann $c^{\mathfrak{M}} = [c]$. Sei f ein n–stelliger Funktor von $\mathcal{L}^*$ (d.h. von $\mathcal{L}$). Wir setzen dann $f^{\mathfrak{M}}([\tau_0], \dots, [\tau_{n-1}]) = [\sigma]$ gdw. die Formel $f\tau_0 \dots \tau_{n-1} = \sigma$ in Δ ist. Um zu zeigen, dass $f^{\mathfrak{M}}$ wohldefiniert ist, müssen wir zwei Dinge einsehen: $f^{\mathfrak{M}}$ ist "total", d.h. für beliebige Terme $\tau_0 \dots \tau_{n-1}$ existiert ein Term σ, so dass $f\tau_0 \dots \tau_{n-1} = \sigma$ in Δ ist; und: $f^{\mathfrak{M}}$ ist "funktional", d.h. für beliebige Terme $\tau_0 \dots \tau_{n-1}, \sigma, \tau_0', \dots, \tau_{n-1}', \sigma'$ folgt aus $\tau_0 \sim \tau_0', \dots, \tau_{n-1} \sim \tau_{n-1}'$, $f\tau_0 \dots \tau_{n-1} \sim \sigma$ und $f\tau_0' \dots \tau_{n-1}' \sim \sigma'$ so dass $\sigma \sim \sigma'$.

Die Totalität von $f^{\mathfrak{M}}$ ist trivial: man wähle einfach für σ den Term $f\tau_0 \dots \tau_{n-1}$. Die Funktionalität von $f^{\mathfrak{M}}$ ergibt sich wie folgt: die Annahme liefert mit Hilfe der Tatsache (e) zur Gleichheit, dass $\Delta \vdash f\tau_0 \dots \tau_{n-1} = f\tau_0' \dots \tau_{n-1}'$, d.h. $f\tau_0 \dots \tau_{n-1} \sim f\tau_0' \dots \tau_{n-1}'$; da $\sim$ Äquivalenzrelation ist, ergibt die Annahme dann sofort $\sigma \sim \sigma'$.

Sei dann R ein n–stelliges Prädikatsymbol. Wir setzen dann $([\tau_0], \dots, [\tau_{n-1}]) \in R^{\mathfrak{M}}$ gdw. die Formel $R\tau_0 \dots \tau_{n-1}$ in Δ ist.

Mit Hilfe der Tatsache (d) zur Gleichheit sieht man dann wie im Falle eines Funktors, dass $R^{\mathfrak{M}}$ wohldefiniert ist. Wir haben damit $\mathfrak{M}$ definiert. Eine natürliche M–Belegung $\overline{\beta}$ ergibt sich wie folgt: $\overline{\beta}(v_i) = [v_i]$.

Wir wollen schließlich zeigen, dass für eine beliebige $\mathcal{L}^*$–Formel Folgendes gilt: $\mathfrak{M} \models \varphi[\overline{\beta}]$ gdw. $\varphi \in \Delta$. Damit gilt insbesondere $\mathfrak{M} \models \varphi[\overline{\beta}]$ für alle φ aus Γ. $\mathfrak{M}$ ist ein Modell von $\mathcal{L}^*$; wir erhalten daraus ein Modell $\overline{\mathfrak{M}}$ von $\mathcal{L}$, indem wir dasjenige "Redukt" von $\mathfrak{M}$ betrachten, das aus $\mathfrak{M}$ hervorgeht, indem man von den Interpretationen der neu hinzugefügten Konstanten $c(i, \overline{\varphi})$ absieht. Dann gilt auch $\overline{\mathfrak{M}} \models \varphi[\overline{\beta}]$ für alle $\varphi \in \Gamma$, und (**) ist bewiesen.

Sei β die durch $\overline{\beta}$ induzierte Terminterpretation. Man sieht leicht, dass $\beta(\tau) = [\tau]$ für alle Terme τ: für Variablen und Konstanten τ ergibt sich dies unmittelbar aus den Definitionen, und für ein τ von der Gestalt $f\tau_0 \dots \tau_{n-1}$ ergibt sich dies induktiv, da dann

$$\begin{aligned}&\beta(f\tau_0 \dots \tau_{n-1}) = f^{\mathfrak{M}}(\beta(\tau_0), \dots, \beta(\tau_{n-1})) = \\ &f^{\mathfrak{M}}([\tau_0], \dots, [\tau_{n-1}]) = [f\tau_0 \dots \tau_{n-1}].\end{aligned}$$

Wir beweisen jetzt die Aussage, dass $\mathfrak{M} \models \varphi[\overline{\beta}]$ gdw. $\varphi \in \Delta$ für alle $\mathcal{L}^*$–Formeln φ gilt, durch Induktion nach der Komplexität von φ.

Sei zuerst φ atomar. Sei etwa $\varphi \equiv \tau = \sigma$. Dann gilt $\mathfrak{M} \models \tau = \sigma[\overline{\beta}]$ gdw. $\beta(\tau) = \beta(\sigma)$ gdw. $[\tau] = [\sigma]$ gdw. $\tau \sim \sigma$ gdw. $\tau = \sigma \in \Delta$. Völlig analog argumentiert man, falls φ von der Gestalt $P\tau_0 \dots \tau_{n-1}$ für ein Prädikatsymbol P und Terme $\tau_0 \dots \tau_{n-1}$ ist.

Sei sodann $\varphi \equiv \neg\psi$. Dann gilt $\mathfrak{M} \models \neg\psi[\overline{\beta}]$ gdw. es nicht der Fall ist, dass $\mathfrak{M} \models \psi[\overline{\beta}]$ gdw. (nach Induktionsvoraussetzung) $\psi \notin \Delta$ gdw. $\neg\psi \in \Delta$.

Für $\psi \equiv \psi \to \psi'$ kann ähnlich argumentiert werden: $\mathfrak{M} \models \psi \to \psi'[\overline{\beta}]$ gdw. aus $\mathfrak{M} \models \psi[\overline{\beta}]$ folgt, dass $\mathfrak{M} \models \psi'[\overline{\beta}]$ gdw. (nach Induktionsvoraussetzung) aus $\psi \in \Delta$ folgt, dass $\psi' \in \Delta$ gdw. $\psi \to \psi' \in \Delta$.

Sei schließlich $\psi \equiv \forall v_i\psi$. Sei zuerst $\forall v_i\psi \in \Delta$ vorausgesetzt. Wir wollen sehen, dass $\mathfrak{M} \models \forall v_i\psi[\overline{\beta}]$, d.h. dass für alle $a \in M$, $\mathfrak{M} \models \psi[\overline{\beta}](v_i|a)]$. Sei $a \in M$ beliebig, $a = [\tau]$ für einen Term τ. Auf Grund der Möglichkeit der Variablen–Umbenennung existiert eine Formel ψ', so dass τ für v_i in ψ' eingesetzt werden kann und es gilt sowohl $\vdash \psi \to \psi'$ als auch $\vdash \psi' \to \psi$, auf Grund des Korrektheitssatzes also $\mathfrak{M} \models \psi[\overline{\beta}(v_i|a)]$ gdw. $\mathfrak{M} \models \psi'[\overline{\beta}(v_i|a)]$. Angenommen, $\mathfrak{M} \models \psi[\overline{\beta}(v_i|a)]$ gilt nicht; dann haben wir $\mathfrak{M} \models \neg\psi'[\overline{\beta}(v_i|[\tau])]$. Da $[\tau] = \beta(\tau)$, und da τ für v_i in ψ' eingesetzt werden kann, gilt dann wegen Lemma 3.3 $\mathfrak{M} \models \neg{\psi'}^{v_i}_{\tau}$. Nach Induktionsvoraussetzung ist dann $\neg{\psi'}^{v_i}_{\tau} \in \Delta$. Aus $\vdash \psi \to \psi'$ ergibt sich $\vdash \forall v_i(\psi \to \psi')$, und daraus mit Hilfe der logischen Axiome aus Klasse (3) $\forall v_i\psi \in \Delta$, und nach zweifacher Anwendung des modus ponens $\Delta \vdash \forall v_i\psi'$. Auf Grund eines Ersetzungsaxioms und einer weiteren Anwendung des modus ponens haben wir dann aber $\Delta \vdash \forall v_i\psi'$, also ${\psi'}^{v_i}_{\tau} \in \Delta$. Es ist also ${\psi'}^{v_i}_{\tau} \in \Delta$ und $\neg{\psi'}^{v_i}_{\tau} \in \Delta$ im Widerspruch zur Konsistenz von Δ.

Sei dann $\mathfrak{M} \models \forall v_i\psi[\overline{\beta}]$ vorausgesetzt. Wir müssen sehen, dass $\forall v_i\psi \in \Delta$. Hierfür benutzen wir, dass Δ eine Henkin–Menge ist. Angenommen, $\forall v_i\psi \notin \Delta$, also $\neg\forall v_i\psi \in \Delta$. Da für $c = c(i, \psi)$ gilt, dass $\neg\forall v_i\psi \to \neg\psi^{v_i}_c \in \Delta$, liefert der modus ponens $\Delta \vdash \neg\psi^{v_i}_c$, d.h. $\neg\psi^{v_i}_c \in \Delta$. Nach Induktionsvoraussetzung ist dann aber $\mathfrak{M} \models \neg\psi^{v_i}_c[\overline{\beta}]$, und eine Anwendung von Lemma 3.3 liefert $\mathfrak{M} \models \neg\psi[\overline{\beta}(v_i|\beta(c))]$. Dies widerspricht aber $\mathfrak{M} \models \forall v_i\psi[\overline{\beta}]$.

Damit ist der Vollständigkeitssatz bewiesen. □

Der Beweis des Vollständigkeitssatzes benutzt das Hausdorffsche Maximalitätsprinzip. Falls $\mathcal{L}$ höchstens abzählbar ist, wird das Maximalitätsprinzip nicht benötigt. $\mathcal{L}$ heißt *höchstens abzählbar* gdw. $I \cup J \cup K$ höchstens abzählbar ist, d.h. gdw. es höchstens abzählbar viele Prädikatsymbole, Funktoren und Konstanten gibt. $\mathcal{L}^*$ entsteht dann aus $\mathcal{L}$ durch Hinzufügung abzählbar vieler Konstanten. Wir können uns dann (ähnlich wie im Beweis des Kompaktheitssatzes der Aussagenlogik) eine maximal–konsistente Menge $\Delta \supset \Gamma_H$ wie folgt konstruieren. Sei $(\varphi_n : n \in \mathbb{N})$ eine Aufzählung aller $\mathcal{L}^*$–Formeln. Sei $\Gamma_0 = \Gamma_H$. Sei $\Gamma_{n+1} = \Gamma_n \cup \{\varphi_n\}$, falls $\Gamma_n \cup \{\varphi_n\}$ konsistent ist; andernfalls sei $\Gamma_{n+1} = \Gamma_n \cup \{\neg\varphi_1\}$. Schließlich sei $\Delta = \bigcup_{n\in\mathbb{N}} \Gamma_n$.

Mit Hilfe von Satz 3.7 hat der Vollständigkeitssatz trivialerweise die allerdings erstaunliche Konsequenz, dass für eine rekursiv aufzählbare Formelmenge Γ auch $\{\varphi : \Gamma \models \varphi\}$ rekursiv aufzählbar ist.

Kapitel 5

Kompaktheit, Löwenheim–Skolem und Ultraprodukte

Satz 5.1 *Sei* Γ *eine Menge von Formeln. Wenn jede endliche Teilmenge von* Γ *erfüllbar ist, dann ist auch* Γ *erfüllbar.*

Beweis: Der Kompaktheitssatz ist eine unmittelbare Konsequenz aus dem Vollständigkeitssatz. Angenommen, Γ ist nicht erfüllbar. Dann ist Γ inkonsistent, d.h. es existiert ein φ mit $\Gamma \vdash \varphi$ und $\Gamma \vdash \neg\varphi$. Dann gibt es natürlich eine endliche Teilmenge $\overline{\Gamma}$ von Γ mit $\overline{\Gamma} \vdash \varphi$ und $\overline{\Gamma} \vdash \neg\varphi$. $\overline{\Gamma}$ ist dann aber sicherlich nicht erfüllbar. $\square$

Der Kompaktheitssatz hat erstaunliche Auswirkungen. Sei beispielsweise Γ eine Menge von Sätzen, so dass Γ beliebig große endliche Modelle besitzt, d.h. für jedes $n \in \mathbb{N}$ existiert ein $m \in \mathbb{N}, m \geq n$, und ein Modell $\mathfrak{M}$, dessen Trägermenge m Elemente besitzt, so dass $\mathfrak{M} \models \Gamma$. Dann besitzt Γ ein unendlich großes Modell $\mathfrak{M}$, d.h. es existiert ein $\mathfrak{M}$, dessen Trägermenge unendlich groß ist, so dass $\mathfrak{M} \models \Gamma$. Sei nämlich für $n \in \mathbb{N}$ φ_n der Satz

$$\begin{aligned}\exists v_0 \ldots \exists v_{n-1}(&v_0 \neq v_1 \wedge v_0 \neq v_2 \wedge \ldots \wedge v_0 \neq v_{n-1} \wedge \\ &v_1 \neq v_2 \wedge \ldots \wedge v_1 \neq v_{n-1} \wedge \ldots \wedge v_{n-2} \neq v_{n-1}),\end{aligned}$$

der besagt, dass es mindestens n Dinge gibt. Nach Annahme ist jede endliche Teilmenge von $\Gamma \cup \{\varphi_n : n \in \mathbb{N}\}$ konsistent, so dass auch $\Gamma \cup \{\varphi_n : n \in \mathbb{N}\}$ konsistent ist.

Eine durch I, J, K, n gegebene Sprache der Logik 1. Stufe heißt höchstens abzählbar gdw. $I \cup J \cup K$ höchstens abzählbar ist.

Satz 5.2 (Löwenheim–Skolem) *Sei $\mathcal{L}$ eine höchstens abzählbare Sprache der Logik 1. Stufe. Sei Γ eine konsistente (erfüllbare) Menge von $\mathcal{L}$–Formeln. Dann besitzt Γ ein höchstens abzählbares Modelle, d.h. es existiert ein Modell $\mathfrak{M}$, dessen Trägermenge M höchstens abzählbar ist, und es existiert eine M–Belegung $\overline{\beta}$ mit $\mathfrak{M} \models \Gamma[\overline{\beta}]$.*

Beweis: Dies ergibt sich aus dem Beweis des Vollständigkeitssatzes. Mit $\mathcal{L}$ ist auch das dort definierte $\mathcal{L}^*$ höchstens abzählbar, so dass $\mathcal{L}^*$ abzählbar viele Terme enthält. Damit ist das dort konstruierte $M = \{[\tau] : \tau \text{ ist } \mathcal{L}^*\text{–Term}\}$ auch höchstens abzählbar. □

Wir werden weiter unten eine allgemeinere Version des Satzes von Löwenheim–Skolem formulieren.

Betrachten wir etwa das Modell

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

das wir bereits kurz in Kapitel 3 erwähnt haben. Zur Erinnerung: Dieses Modell besitzt das Universum $\mathbb{N}$ (= die Menge der natürlichen Zahlen = $\{0, 1, 2, \dots\}$). 0 ist die Null. S ist die Nachfolgeroperation, die definiert ist durch $S(n) = n + 1$ für $n \in \mathbb{N}$. $<$ ist die übliche strikte Ordnung auf $\mathbb{N}$. $+, \cdot$ und E bezeichnen die Addition, die Multiplikation und die Exponentiation.

Die zum Modell $\mathcal{N}$ gehörige Sprache der elementaren Zahlentheorie, die wir nun $\mathcal{L}_A$ nennen, enthält die Symbole 0 als Konstante, S als 1–stelligen Funktor, $<$ als 2–stelliges Relationssymbol, sowie $+, \cdot$ und E als 2–stellige Funktoren. Wir beabsichtigen natürlich $0^{\mathcal{N}} = 0, S^{\mathcal{N}} = S, <^{\mathcal{N}} = <, +^{\mathcal{N}} = +, \cdot^{\mathcal{N}} = \cdot$ und $E^{\mathcal{N}} = E$.

Hier ist eine Liste einiger Sätze φ der Sprache $\mathcal{L}_A$ mit $\mathcal{N} \models \varphi$:

(1) $\forall v_1 S(v_1) \neq 0$

(2) $\forall v_1 \forall v_2 (S(v_1) = S(v_2) \rightarrow v_1 = v_2)$

(3) $\forall v_1 \forall v_2 (v_1 < S(v_2) \leftrightarrow (v_1 < v_2 \vee v_1 = v_2))$

(4) $\forall v_1 \neg v_1 < 0$

(5) $\forall v_1 \forall v_2 (v_1 < v_2 \vee v_1 = v_2 \vee v_2 < v_1)$

(6) $\forall v_1 v_1 + 0 = v_1$

(7) $\forall v_1 \forall v_2 v_1 + S(v_2) = S(v_1 + v_2)$

(8) $\forall v_1 v_1 \cdot 0 = 0$

(9) $\forall v_1 \forall v_2 v_1 \cdot S(v_2) = v_1 \cdot v_2 + v_1$

(10) $\forall v_1 v_1 E 0 = S(0)$

(11) $\forall v_1 \forall v_2 v_1 E S(v_2) = (v_1 E v_2) \cdot v_1$

Wir wollen nun zeigen, dass $\mathcal{N}$ nicht das einzige Modell dieser Sätze ist. Genauer: Wir wollen zeigen, dass es Modelle dieser Sätze gibt, die *nicht isomorph* zu $\mathcal{N}$ sind.

Wir wollen nun zunächst zeigen, dass Modelle der obigen Sätze (1) bis (3) und (6) bis (11) eine "isomorphe Kopie" von $\mathcal{N}$ enthalten.

Sei

$$\mathcal{M} = (M; 0^{\mathcal{M}}, S^{\mathcal{M}}, <^{\mathcal{M}}, +^{\mathcal{M}}, \cdot^{\mathcal{M}}, E^{\mathcal{M}})$$

ein Modell der Sätze (1) bis (3) und (6) bis (11). Betrachten wir die Funktion $\pi_{\mathcal{M}} = \pi : \mathbb{N} \to M$, die wie folgt definiert ist:

$$\pi(n) = \underbrace{S^{\mathcal{M}}(S^{\mathcal{M}}(\ldots S^{\mathcal{M}}}_{n\text{–viele } S^{\mathcal{M}}}(0^{\mathcal{M}})\ldots)),$$

d.h., $\pi(0) = 0^{\mathcal{M}}$ und $\pi(n+1) = S^{\mathcal{M}}(\pi(n))$ für $n \in \mathbb{N}$.

Sei $\pi(m) = \pi(n)$ für $m \leq n \in \mathbb{N}$. Auf Grund von (2) ist dann $\pi(n-m) = 0^{\mathcal{M}}$, auf Grund von (1) also $n - m = 0$, d.h. $m = n$. Es ist also π injektiv. Wir werden später sehen, dass f nicht surjektiv sein muss.

Sei $m \in \mathbb{N}$. Mit Hilfe von (3) zeigt man dann leicht induktiv, dass $f(m) <^{\mathcal{M}} f(n)$ für alle $n > m$ gilt.

Ebenso leicht zeigt man mit Hilfe von (6) bis (11), dass für alle $m, n \in \mathbb{N}$ gilt: $\pi(m+n) = \pi(m) +^{\mathcal{M}} \pi(n), \pi(m \cdot n) = \pi(m) \cdot^{\mathcal{M}} \pi(n)$ und $\pi(m^n) = \pi(m) E^{\mathcal{M}} \pi(n)$.

Wir haben damit gesehen, dass π ein Monomorphismus, d.h. ein injektiver Homomorphismus, ist.

Nehmen wir nun zusätzlich an, dass $\mathcal{N}$ und $\mathcal{M}$ isomorph sind. Sei $\pi' : \mathbb{N} \to M$ ein Isomorphismus. Es ist leicht induktiv zu zeigen, dass dann $\pi'(n) = \pi_{\mathcal{M}}(n)$ für alle $n \in \mathbb{N}$ gelten muss. Es gilt also

Satz 5.3 *Wenn $\mathcal{M}$ ein Modell der Sätze (1) bis (3) und (6) bis (11) ist, dann ist $\mathcal{M}$ isomorph zu $\mathcal{N}$, gdw. $\pi_{\mathcal{M}}$ surjektiv ist.*

Sei nun $\mathcal{M}$ ein Modell der Sätze (1) bis (11). Mit Hilfe von (3) bis (5) ist leicht zu sehen, dass für alle $n \in \mathbb{N}$ und für alle x außerhalb des Wertebereichs von $\pi_{\mathcal{M}}$ gelten muss: $\pi_{\mathcal{M}}(n) <^{\mathcal{M}} x$. Ein solches x ist also "unendlich groß". Wir bezeichnen mit $\mathrm{Th}(\mathcal{N})$ die Menge aller Sätze φ der Sprache $\mathcal{L}_A$ mit $\mathcal{N} \models \varphi$. (Th steht für "Theorie".) Selbstverständlich gilt

$$\mathcal{N} \models \mathrm{Th}(\mathcal{N}),$$

d.h. $\mathcal{N} \models \varphi$ für alle $\varphi \in \mathrm{Th}(\mathcal{N})$. Wir wollen weitere Modelle $\mathcal{M}$ mit

$$\mathcal{M} \models \mathrm{Th}(\mathcal{N})$$

kennen lernen.

Satz 5.4 *Es existiert ein $\mathcal{M}$ mit abzählbarer Trägermenge und $\mathcal{M} \models \mathrm{Th}(\mathcal{N})$, so dass $\mathcal{M}$ und $\mathcal{N}$ nicht isomorph sind.*

Auf Grund dieses Satzes wird $\mathcal{N}$ als das *Nichtstandardmodell* von $\mathrm{Th}(\mathcal{N})$ bezeichnet. Jedes Modell von $\mathrm{Th}(\mathcal{N})$, das nicht zum Standardmodell isomorph ist, heißt ein *Nonstandardmodell*. Der Satz sagt also, dass es Nonstandardmodelle von $\mathrm{Th}(\mathcal{N})$ gibt.

Beweis: Der Beweis ist eine Anwendung des Kompaktheitssatzes. Wir erweitern die Sprache $\mathcal{L}_A$ durch Hinzunahme einer neuen Konstanten, c. Nennen wir die so erweiterte Sprache $\mathcal{L}_c$.

Sei $n \in \mathbb{N}$. Dann ist

$$\neg \underbrace{S(S(S \dots (S}_{n \text{ viele } S}(0)) = c$$

ein Satz der Sprache $\mathcal{L}_c$. (Dieser Satz sagt, dass das durch c bezeichnete Objekt verschieden von n ist.) Nennen wir diesen Satz φ_n.

Wir betrachten nun die Menge

$$T = \mathrm{Th}(\mathcal{N}) \cup \{\varphi_n | n \in \mathbb{N}\}$$

von Sätzen der Sprache $\mathcal{L}_c$. T ist erfüllbar. Sei nämlich $\overline{T} \subset T$ endlich. Aufgrund des Kompaktheitssatzes genügt es zu zeigen, dass $\overline{T}$ erfüllbar ist.

Es existiert ein $n_0 \in \mathbb{N}$, so dass

$$\overline{T} \subset \mathrm{Th}(\mathcal{N}) \cup \{\varphi_n | n < n_0\}.$$

Es ist dann einfach zu sehen, dass

$$\mathcal{N}' = (\mathbb{N}; 0, S, <, +, \cdot, E, n_0) \models \overline{T}.$$

Hierbei beabsichtigen wir $0^{\mathcal{N}'} = 0, S^{\mathcal{N}'} = S, <^{\mathcal{N}'}=<, +^{\mathcal{N}'} = +, \cdot^{\mathcal{N}'} = \cdot, E^{\mathcal{N}'} = E$ und $c^{\mathcal{N}'} = n_0$.

Sei nun

$$\widetilde{\mathcal{M}} = (\widetilde{M}; 0^{\widetilde{\mathcal{M}}}, S^{\widetilde{\mathcal{M}}}, <^{\widetilde{\mathcal{M}}}, +^{\widetilde{\mathcal{M}}}, \cdot^{\widetilde{\mathcal{M}}}, E^{\widetilde{\mathcal{M}}}, c^{\widetilde{\mathcal{M}}}) \models T,$$

wobei $\widetilde{M}$ abzählbar ist. Ein solches $\widetilde{\mathcal{M}}$ existiert jetzt auf Grund des Satzes von Löwenheim–Skolem. Setze

$$\widetilde{\mathcal{M}} = (\widetilde{M}; 0^{\widetilde{\mathcal{M}}}, S^{\widetilde{\mathcal{M}}}, <^{\widetilde{\mathcal{M}}}, +^{\widetilde{\mathcal{M}}}, \cdot^{\widetilde{\mathcal{M}}}, E^{\widetilde{\mathcal{M}}}).$$

Selbstverständlich gilt

$$\widetilde{\mathcal{M}} \models \mathrm{Th}(\mathcal{N}).$$

Angenommen, $\pi = \pi_{\mathcal{M}}$ wäre surjektiv. Dann existiert ein $n \in \mathbb{N}$ mit $\pi(n) = c^{\widetilde{\mathcal{M}}}$. Es gilt $\widetilde{\mathcal{M}} \models \varphi_n$, d.h.

$$\widetilde{\mathcal{M}} \models \neg \underbrace{S(S(S \ldots (S}_{n \text{ viele } S}(0)) \ldots)) = c.$$

Dies besagt, dass

$$\pi(n) = \underbrace{S^{\mathcal{M}}(S^{\mathcal{M}}(\ldots S^{\mathcal{M}}}_{n \text{ viele } S^{\mathcal{M}}}(0^{\mathcal{M}}) \ldots)) \neq c^{\widetilde{\mathcal{M}}} = \pi(n).$$

Dies ist ein Widerspruch!

Der Monomorphismus $\pi_{\mathcal{M}}$ ist also nicht surjektiv, womit auf Grund von Satz 5.2 $\mathcal{M}$ nicht isomorph zu $\mathcal{N}$ ist. □

Sei M mit Trägermenge M ein Nonstandardmodell von $\mathrm{Th}(\mathcal{N})$. Jedes $x \in M$, das außerhalb des Wertebereichs von $\pi_{\mathcal{N}}$ liegt, heißt eine Nonstandardzahl. Ein $x \in M$ ist Nonstandardzahl gdw. $\pi_{\mathcal{M}}(n) <^{\mathcal{M}} x$ für alle $n \in \mathbb{N}$, d.h. gdw. x "unendlich groß" ist.

Wir wollen nun zeigen, dass es "sehr viele" paarweise nicht isomorphe abzählbare Modelle von $\mathrm{Th}(\mathcal{N})$ gibt. Um genau formulieren zu können, war "sehr viele" hier bedeutet, benötigen wir einen Begriff.

Sei M eine Menge. Wir sagen, dass M reellviele Elemente besitzt, falls eine Bijektion $f : M \to \mathcal{P}(\mathbb{N})$ existiert. Hierbei ist $\mathcal{P}(\mathbb{N})$ die Menge aller Teilmengen von $\mathbb{N}$. Insbesondere hat $\mathcal{P}(\mathbb{N})$ selbst reellviele Elemente. Wir sagen, dass die Menge M weniger als reellviele Elemente besitzt, falls keine

Surjektion $f : M \to \mathcal{P}(\mathbb{N})$ existiert. Beispielsweise besitzt $\mathbb{N}$ weniger als reellviele Elemente: wenn $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$, dann ist

$$\{n \in \mathbb{N} | n \notin f(n)\} \in \mathcal{P}(\mathbb{N})$$

nicht im Wertebereich von f.

Die Aussage, dass jede überabzählbare Teilmenge von $\mathbb{R}$ reellviele Elemente besitzt, heißt *Kontinuumshypothese*. Diese Aussage wird in der Mengenlehre studiert.

Für den Beweis des folgenden Satzes benötigen wir eine Tatsache, die wir hier nicht zeigen können.

Tatsache: Sei $\mathcal{Z}$ eine Menge. Angenommen, $\mathcal{Z}$ besitzt weniger als reellviele Elemente und jedes $\mathcal{X} \in \mathcal{Z}$ ist eine abzählbare Menge. Dann ist auch

$$\bigcup \mathcal{Z} = \{X | \exists \mathcal{X} \in \mathcal{Z} X \in \mathcal{X}\}$$

eine Menge, die weniger als reellviele Elemente besitzt.

Es ist nicht schwierig zu zeigen, dass es höchstens reellviele nicht–isomorphe abzählbare Modelle von $\mathcal{L}_A$ geben kann. Der nachfolgende Satz sagt, dass es sogar mindestens so viele Modelle von $\mathrm{Th}(\mathcal{N})$ gibt.

Satz 5.5 *Es existieren reellviele paarweise nicht–isomorphe abzählbare Modelle $\mathcal{M}$ mit $\mathcal{M} \models \mathrm{Th}(\mathcal{N})$.*

Beweis: Wir erweitern wieder die Sprache $\mathcal{L}_A$ durch Hinzunahme einer neuen Konstanten c und nennen die so erweiterte Sprache $\mathcal{L}_c$.

Sei $p_0, p_1, p_2, \ldots$ die strikt monotone Aufzählung aller Primzahlen. D.h., $p_0 = 2, p_1 = 3, p_2 = 5$, etc.

Sei $n \in \mathbb{N}$. Dann bezeichnen wir mit φ_n den Satz

$$\exists v_1 \underbrace{S(S(S \ldots (S}_{p_n \text{ viele } S}(0)) \ldots)) \cdot v_1 = c$$

der Sprache $\mathcal{L}_c$. Dieser Satz sagt, dass p_n (die Interpretation von) c teilt. Mit $\overline{\varphi}_n$ bezeichnen die Negation von φ_n, d.h. den Satz

$$\neg\exists v_1 \underbrace{S(S(S \ldots (S}_{p_n \text{ viele } S}(0)) \ldots)) \cdot v_1 = c.$$

Sei nun $X \subset \mathbb{N}$. Wir bezeichnen dann mit T_X die Menge

$$\mathrm{Th}(\mathcal{N}) \cup \{\varphi_n | n \in X\} \cup \{\overline{\varphi}_n | n \notin X\}$$

von Sätzen der Sprache $\mathcal{L}_c$. Für jedes $X \subset \mathbb{N}$ ist T_X ist erfüllbar. Sei nämlich $\overline{T} \subset T_X$ endlich. Auf Grund des Kompaktheitssatzes genügt es zu zeigen, dass $\overline{T}$ erfüllbar ist.

Es existiert ein $n_0 \in \mathbb{N}$, so dass

$$\overline{T} \subset \mathrm{Th}(\mathcal{N}) \cup \{\varphi_n | n < n_0 \wedge n \in X\} \cup \{\overline{\varphi}_n | n < n_0 \wedge n \notin X\}.$$

Setze

$$q = \prod_{n<n_0, n\in X} p_n.$$

Es ist dann einfach zu sehen, dass

$$\mathcal{N}' = (\mathbb{N}; 0, S, <, +, \cdot, E, q) \models \overline{T}.$$

Hierbei beabsichtigen wir $0^{\mathcal{N}'} = 0, S^{\mathcal{N}'} = S, <^{\mathcal{N}'} = <, +^{\mathcal{N}'} = +, \cdot^{\mathcal{N}'} = \cdot, E^{\mathcal{N}'} = E$ und $c^{\mathcal{N}'} = q$. Für $X \subset \mathbb{N}$ sei nun

$$\widetilde{\mathcal{M}} = (M_X; 0^{\widetilde{\mathcal{M}}_X}, S^{\widetilde{\mathcal{M}}_X}, <^{\widetilde{\mathcal{M}}_X}, +^{\widetilde{\mathcal{M}}_X}, \cdot^{\widetilde{\mathcal{M}}_X}, E^{\widetilde{\mathcal{M}}_X}, c^{\widetilde{\mathcal{M}}_X}) \models T_{\mathcal{X}},$$

wobei M_X abzählbar ist. Ein solches $\widetilde{\mathcal{M}}_X$ existiert auf Grund der Behauptung 1 und des Satzes von Löwenheim–Skolem. Setze

$$\mathcal{M}_X = (M_X; 0^{\widetilde{\mathcal{M}}_X}, S^{\widetilde{\mathcal{M}}_X}, <^{\widetilde{\mathcal{M}}_X}, +^{\widetilde{\mathcal{M}}_X}, \cdot^{\widetilde{\mathcal{M}}_X}, E^{\widetilde{\mathcal{M}}_X}).$$

Selbstverständlich gilt

$$\mathcal{M}_X \models \mathrm{Th}(\mathcal{N}).$$

Für $X, Y \subset \mathbb{N}$ ist es möglich, dass $\mathcal{M}_X$ und $\mathcal{M}_Y$ isomorph sind. Wir wollen jedoch zeigen, dass eine Teilmenge von $\{\mathcal{M}_X | X \subset \mathbb{N}\}$ mit reellvielen Elementen existiert, die aus paarweise nicht–isomorphen Modellen besteht. Sei

$$\mathcal{M} = (M; 0^{\mathcal{M}}, S^{\mathcal{M}}, <^{\mathcal{M}}, +^{\mathcal{M}}, \cdot^{\mathcal{M}}, E^{\mathcal{M}}) \models \mathrm{Th}(\mathcal{N}).$$

Für jedes $x \in M$ sei

$$X_x^{\mathcal{M}} = \{n \in \mathbb{N} : \mathcal{M} \models \exists v_1 \underbrace{S(S(S \ldots (S}_{p_n \text{ viele } S}(0)) \ldots)) \cdot v_1 = v_2[\bar{\beta}] \text{ mit } \bar{\beta}(v_2) = x\}.$$

Jedes solche $X_x^{\mathcal{M}}$ ist eine Menge natürlicher Zahlen, die durch das Modell $\mathcal{M}$ und $x \in M$ "kodiert" wird. Sei

$$\mathcal{X}^{\mathcal{M}} = \{X_x^{\mathcal{M}} : x \in M\}$$

die Menge aller Teilmengen von $\mathbb{N}$, die durch $\mathcal{M}$ und seine Elemente in diesem Sinne "kodiert" werden. Offensichtlich ist $\mathcal{X}^{\mathcal{M}}$ eine abzählbare Menge von Teilmengen von $\mathbb{N}$, wenn M abzählbar ist. Für jedes $X \subset \mathbb{N}$ gilt offensichtlich

$$X = X^{\mathcal{M}_X}_{c^{\mathcal{M}_X}} \in \mathcal{X}^{\mathcal{M}_X}.$$

Wir zeigen nun: Seien $\mathcal{M}$ und $\mathcal{P}$ isomorphe Modelle von $\mathrm{Th}(\mathcal{N})$. Dann gilt $\mathcal{X}^{\mathcal{M}} = \mathcal{X}^{\mathcal{P}}$. Sei nämlich $\pi : M \to P$ ein Isomorphismus. Sei $X \in \mathcal{X}^{\mathcal{M}}$. Sei $x \in M$ so, dass $X = X^{\mathcal{M}}_x$. Sei $\bar\beta : \{v_1, v_2, \dots\} \to M$, und sei $\bar\beta' : \{v_1, v_2, \dots\} \to P$ definiert durch $\bar\beta'(v_k) = \pi(\bar\beta(v_k))$. Für jedes $n \in \mathbb{N}$ gilt dann auf Grund von Satz 5.1

$$\mathcal{M} \models \exists v_1 \underbrace{S(S(S \dots (S}_{p_n \text{ viele } S}(0)) \dots)) \cdot v_1 = v_2[\bar\beta] \Leftrightarrow$$

$$\mathcal{P} \models \exists v_1 \underbrace{S(S(S \dots (S}_{p_n \text{ viele } S}(0)) \dots)) \cdot v_1 = v_2[\bar\beta].$$

Damit haben wir $X = X^{\mathcal{P}}_{\pi(x)}$, also $X \in \mathcal{X}^{\mathcal{P}}$.

Wir haben gezeigt, dass $\mathcal{X}^{\mathcal{M}} \subset \mathcal{X}^{\mathcal{P}}$. Aus Symmetriegründen gilt ebenso $\mathcal{X}^{\mathcal{P}} \subset \mathcal{X}^{\mathcal{M}}$. Damit ist $\mathcal{X}^{\mathcal{M}} = \mathcal{X}^{\mathcal{P}}$.

Kehren wir nun zu den Modellen $\mathcal{M}_X$ für $X \subset \mathbb{N}$ zurück. Für $X \subset \mathbb{N}$ sei

$$[\mathcal{M}_X] = \{\mathcal{M}_Y | Y \subset \mathbb{N} \text{ und } \mathcal{M}_Y \text{ ist isomorph mit } \mathcal{M}_X\}$$

die Äquivalenzklasse aller zu $\mathcal{M}_X$ isomorphen Modelle $\mathcal{M}_Y$. Wir definieren

$$\mathcal{X}^{[\mathcal{M}_X]} = \mathcal{X}^{\mathcal{M}_X}.$$

Auf Grund der Behauptung 2 folgt aus $[\mathcal{M}_X] = [\mathcal{M}_Y]$, dass $\mathcal{X}^{\mathcal{M}_X} = \mathcal{X}^{\mathcal{M}_Y}$. Auf Grund dieser Unabhängigkeit von der Wahl des Repräsentanten ist $\mathcal{X}^{[\mathcal{M}_X]}$ wohldefiniert. Jedes $\mathcal{X}^{[\mathcal{M}_X]}$ abzählbar.

Nehmen wir nun an, es gäbe weniger als reellviele Äquivalenzklassen $[\mathcal{M}_X]$. Dann wäre auf Grund der oben unbewiesen mitgeteilten Tatsache

$$\mathcal{Z} = \bigcup \{\mathcal{X}^{[\mathcal{M}_X]} | X \subset \mathbb{N}\}$$

eine Menge, die weniger als reellviele Elemente besitzt.

Auf der anderen Seite gilt für ein beliebiges $X \subset \mathbb{N}$, dass $X \in \mathcal{X}^{\mathcal{M}_X} = \mathcal{X}^{[\mathcal{M}_X]} \subset \mathcal{Z}$. Also enthält $\mathcal{Z}$ *alle* Teilmengen von $\mathbb{N}$, besteht also aus reellvielen Elementen. Widerspruch! $\square$

Wir formulieren nun eine allgemeinere Version des Satzes von Löwenheim–Skolem.

Definition 5.6 *Sei $\mathcal{L}$ eine Sprache der Logik 1. Stufe, und seien $\mathcal{M}$ und $\mathcal{N}$ Modelle von $\mathcal{L}$. Dann heißt $\mathcal{M}$* elementar äquivalentes Submodell *von $\mathcal{N}$, geschrieben $\mathcal{M} \prec \mathcal{N}$ gdw. für alle $\mathcal{L}$–Formeln φ und für alle M–Belegungen $\bar{\beta}$ (wobei M die Trägermenge von $\mathcal{M}$ ist) gilt:*

$$\mathcal{M} \models \varphi[\bar{\beta}] \text{ gdw. } \mathcal{N} \models \varphi[\bar{\beta}].$$

Satz 5.7 (Allgemeiner Löwenheim–Skolem) *Sei $\mathcal{L}$ eine Sprache der Logik 1. Stufe, die durch I, J, K, n gegeben ist. Sei Γ eine Menge von Formeln, so dass $\mathcal{M}$ und $\overline{\beta}$ existieren, wobei $\mathcal{M} \models \Gamma[\overline{\beta}]$ und die Trägermenge von $\mathcal{M}$ unendlich groß ist. Sei X eine beliebige unendliche Menge, wobei eine Injektion $f : I \cup J \cup K \to X$ existiert. Dann existieren $\mathcal{N}$ und $\overline{\beta}'$, wobei $\mathcal{M} \models \Gamma[\overline{\beta}']$ und X die Trägermenge von $\mathcal{M}$ ist. Ebenfalls existiert ein $\mathcal{N}$, so dass $\mathcal{N} \prec \mathcal{M}$ oder $\mathcal{M} \prec \mathcal{N}$ und so dass es eine Bijektion von X mit der Trägermenge von $\mathcal{N}$ gibt.*

Insbesondere besitzen konsistente Formelmengen beliebig große Modelle.

Beweis: Der Allgemeine Löwenheim–Skolem–Satz ergibt sich schnell aus dem Beweis des Vollständigkeitssatzes. Wir erweitern zunächst $\mathcal{L}$ zu $\mathcal{L}'$ durch Hinzufügung einer eigenen Konstante c_x für jedes $x \in X$. Sodann erweitern wir Γ zu Γ' durch Hinzufügung genau aller $\mathcal{L}'$–Sätze $c_x \neq c_y$ für $x \neq y, x, y \in X$. Γ' ist dann konsistent. Wir produzieren nun wie im Beweis des Vollständigkeitssatzes $\mathcal{M}$ und $\overline{\beta}$ (ausgehend von $\mathcal{L}'$ und Γ' an Stelle von $\mathcal{L}$ und Γ). Es lässt sich zeigen, dass eine Bijektion zwischen X und der Trägermenge M von $\mathcal{M}$ existiert. Wir können dann die Elemente von M durch X ersetzen und erhalten $\mathcal{M}, \overline{\beta}$ wie gewünscht. Der Rest ist einfach.$\square$

Insbesondere existiert z.B. ein Modell von $\mathrm{Th}(\mathcal{N})$, dessen Trägermenge die Menge $\mathbb{R}$ aller reellen Zahlen ist!

Wir wollen nun einen alternativen Beweis des Kompaktheitssatzes kennen lernen. Dieser Beweis verwendet die Methode der Konstruktion neuer Modelle durch Ultraprodukte.

Definition 5.8 *Sei $I \neq \emptyset$ eine beliebige Menge. Eine Menge F von Teilmengen von I heißt ein* Filter auf I *gdw.*

(a) wenn $X \in F$ und $Y \in F$, dann ist auch $X \cap Y \in F$,

(b) wenn $X \in F$ und $Y \supset X$, wobei $Y \subset I$, dann ist auch $Y \in F$,

(c) $I \in F$*, und*

(d) $\emptyset \notin F$.

Sei etwa u eine nichtleere Teilmenge von I. Dann ist

$$\{X \subset I : u \subset X\}$$

ein Filter auf I. Dieser heißt der *von u erzeugte prinzipale Filter*. Sei I unendlich. Dann ist

$$\{X \subset I : I \backslash X \text{ ist endlich}\}$$

ein Filter auf I, der aus allen *koendlichen* Teilmengen von I besteht. Dieser heißt der Frechét–Filter auf I.

Definition 5.9 *Sei $I \neq \emptyset$, und sei F ein Filter auf I. Dann heißt F* Ultrafilter *auf I gdw für jedes $X \in I$ gilt: $X \in F$ oder $I \backslash X \in F$. wenn F Ultrafilter auf I ist, dann gilt für jedes $X \subset I$ genau eine der beiden Aussagen $X \in F, I \backslash X \in F$. Mit Hilfe des Hausdorffschen Maximalitätsprinzip (siehe Satz 5.8) zeigt man den folgenden*

Satz 5.10 (Tarski) *Sei $I \neq \emptyset$, und sei F ein Filter auf I. Dann existiert ein Ultrafilter U auf I, der F fortsetzt, d.h. so dass $U \supset F$.*

Sei nun $\mathcal{L}$ eine Sprache der Logik erster Stufe. Sei $I \neq \emptyset$, und sei für jedes $i \in I$ ein $\mathcal{L}$–Modell $\mathfrak{M}_i$ gegeben. Sei weiterhin U ein Ultrafilter auf I. Wir wollen dann das Ultraprodukt der Modelle $\mathfrak{M}_i$ mittels U, in Zeichen

$$\prod_{i \in I} \mathfrak{M}_i / U,$$

definieren. Für diesen Zweck wollen wir voraussetzen, dass $\mathcal{L}$ weder Konstanten noch Funktoren und ein einziges Relationssymbol, nämlich das zweistellige Relationssymbol R, besitzt.[1] Alles, was im Folgenden entwickelt wird, lässt sich aber in offensichtlicher Weise für beliebige Sprachen verallgemeinern.

Wir definieren zunächst die Trägermenge des Ultraproduktes. Mit $|\mathfrak{M}_i|$ bezeichnen wir die Trägermenge des Modells $\mathfrak{M}_i$. Es sei F^* die Menge aller Funktionen f mit Definitionsbereich I, so dass $f(i) \in |\mathfrak{M}_i|$ für alle $i \in I$. Für $f, g \in F^*$ schreiben wir $f \sim g$ gdw. $\{i \in I : f(i) = g(i)\} \in U$.

[1]Die Sprache $\mathcal{L}_\in$ der Mengenlehre besitzt beispielsweise diese Gestalt.

Lemma 5.11 $\sim$ *ist eine Äquivalenzrelation.*

Beweis: Lediglich die Transitivität von $\sim$ ist nicht trivial. Aus $f \sim g$ und $g \sim h$, d.h. $\{i \in I : f(i) = g(i)\} \in U$ und $\{i \in I : g(i) = h(i)\} \in U$ folgt aber wegen $\{i \in I : f(i) = h(i)\} \supset \{i \in I : f(i) = g(i)\} \cap \{i \in I : g(i) = h(i)\}$, dass $\{i \in I : f(i) = h(i)\} \in U$, also $f \sim h$. □

Wir schreiben $[f]$ für die Äquivalenzklasse von $f \in F^*$, d.h. $[f] = \{g \in F^* : g \sim f\}$. Wir schreiben auch $\mathfrak{F}$ für die Menge aller $[f]$ mit $f \in F^*$. $\mathfrak{F}$ wird die Trägermenge des Ultraproduktes sein.

Jedes der Modelle $\mathfrak{M}_i$ interpretiert R, d.h. $R^{\mathfrak{M}_i} \subset |\mathfrak{M}_i| \times |\mathfrak{M}_i|$. Wir wollen nun ein $\tilde{R} \subset \mathfrak{F} \times \mathfrak{F}$ definieren. Wir setzen $([f],[g]) \in \tilde{R}$ gdw. $\{i \in I : (f(i), g(i)) \in R^{|\mathfrak{M}_i|}\} \in U$. Man sieht leicht, d.h. für $f \sim f'$ und $g \sim g'$ gilt $\{i \in I : (f(i), g(i)) \in R^{|\mathfrak{M}_i|}\} \in U$ gdw. $\{i \in I : (f'(i), g'(i)) \in R^{|\mathfrak{M}_i|}\} \in U$. Wir haben damit ein $\mathcal{L}$–Modell konstruiert, nämlich $(\mathfrak{F}; \tilde{R})$. Dieses Modell besitzt die Trägermenge $\mathfrak{F}$ und interpretiert F durch $\tilde{R}$. Dieses so konstruierte Modell bezeichnen wir als das *Ultraprodukt der Modelle $\mathfrak{M}_i$ mittels U.*

Die folgende Aussage ist von zentraler Bedeutung.

Satz 5.12 (Łoś) *Seien für $i \in I \beta_i$ eine $\mathfrak{M}_i$–Belegung, und sei die $\prod_{i \in I} \mathfrak{M}_i/u$–Belegung β wie folgt definiert: $\beta(v_k) = [f]$, wobei $f(i) = \beta_i(v_k)$ für alle $i \in I$. Dann gilt für alle Formeln φ*

$$\prod_{i \in I} \mathfrak{M}_i/u \models \varphi[\beta] \textit{ gdw. } \{i \in I : \mathfrak{M}_i \models \varphi[\beta]\} \in U.$$

Beweis durch Induktion nach der Komplexität von φ. Wir schreiben $\tilde{\mathfrak{M}}$ für $\prod_{i \in I} \mathfrak{M}/U$.

Sei zunächst φ atomar. Sei etwa $\varphi \equiv v_k = v_l$. Dann gilt $\tilde{\mathfrak{M}} \models v_k = v_l[\beta]$ gdw. $\beta(v_k) = \beta(v_l)$ gdw. $[f] = [g]$, wobei $f(i) = \beta_i(v_k)$ und $g(i) = \beta_i(v_l)$ für alle $i \in I$, gdw. $\{i \in I : \beta_i(v_k) = \beta_i(v_l)\} \in U$ gdw. $\{i \in I : \mathfrak{M}_i \models v_k = v_l[\beta_i]\} \in U$. Für $\varphi \equiv R v_k v_l$ ist das Argument völlig analog.

Sei nun $\varphi \equiv \neg\psi$. Hier benutzt der Induktionsschritt die Tatsache, dass U ein Ultrafilter (und nicht etwa nur ein Filter) auf I ist. Es gilt $\mathfrak{M} \models \neg\psi[\beta]$ gdw. $\mathfrak{M} \not\models \psi[\beta]$ gdw. $\{i \in I : \mathfrak{M}_i \models \psi[\beta_i]\} \notin U$ nach Induktionsvoraussetzung, gdw. $\{i \in I : \mathfrak{M}_i \not\models \psi[\beta_i]\} \in U$, da U ein Ultrafilter ist, gdw. $\{i \in I : \mathfrak{M}_i \models \neg\psi[\beta_i]\} \in U$.

Der Induktionsschritt für $\varphi \equiv \psi \rightarrow \psi'$ ist sehr einfach.

Wir betrachten schließlich den Fall, dass $\varphi \equiv \forall v_k \psi$.

Setzen wir zunächst voraus, dass $\{i \in I : \mathfrak{M}_i \models \forall v_k \psi[\beta_i]\} \in U$. Sei $[f] \in |\tilde{\mathfrak{M}}| = \mathfrak{F}$ beliebig. Dann gilt $\{i \in I : \mathfrak{M}_i \models \psi[\beta_i(v_k|f(i))]\} \supset \{i \in I : \mathfrak{M}_i \models \forall v_k \psi[\beta_i]\}$, also $\{i \in I : \mathfrak{M}_i \models \psi[\beta_i(v_k|f(i))]\} \in U$. Die Induktionsvoraussetzung liefert dann $\tilde{\mathfrak{M}} \models \psi[\beta(v_k|[f])]$. Da $[f]$ beliebig war, haben wir also $\mathfrak{M} \models \forall v_k \psi[\beta]$ gezeigt.

Setzen wir nun voraus, dass $\{i \in I : \mathfrak{M}_i \models \forall v_k \psi[\beta_i]\} \notin U$, d.h. $\{i \in I : \mathfrak{M}_i \models \exists v_k \neg\psi[\beta_i]\} \in U$. Wir wollen zeigen, dass $\tilde{\mathfrak{M}} \not\models \forall v_k \psi[\beta]$, d.h. $\tilde{\mathfrak{M}} \models \exists v_k \neg\psi[\beta]$. Mit Hilfe des Auswahlaxioms finden wir ein $f \in F^*$, so dass $\mathfrak{M}_i \models \neg\psi[\beta_i(v_k|f(i))]$ für alle $i \in I$, für die ein $a \in |\mathfrak{M}_i|$ mit $\mathfrak{M}_i \models \neg\psi[\beta_i(v_k|a)]$ existiert. Dann gilt offensichtlich

$$\{i \in I : \mathfrak{M}_i \models \neg\psi[\beta_i(v_k|f(i))]\} = \{i \in I : \mathfrak{M}_i \models \exists v_k \psi[\beta_i]\} \subset U,$$

und damit mit Hilfe der Induktionsvoraussetzung $\mathfrak{M} \models \neg\psi[\beta(v_k|[f])]$, wie gewünscht. □

Mit Hilfe dieser Methode zeigt sich nun der Kompaktheitssatz sehr leicht wie folgt. Sei Σ eine endlich erfüllbare Menge von $\mathcal{L}$–Formeln, d.h. für jedes endliche $\sigma \subset \Sigma$ existiert ein $\mathcal{L}$–Modell $\mathfrak{M}_\sigma$ und eine $\mathfrak{M}_\sigma$–Belegung β_σ mit

$$\mathfrak{M}_\sigma \models \sigma[\beta_\sigma].$$

Gesucht ist ein $\mathcal{L}$–Modell $\tilde{\mathfrak{M}}$ und eine $\tilde{\mathfrak{M}}$–Belegung β mit $\tilde{\mathfrak{M}} \models \Sigma[\beta]$. Sei I die Menge aller endlichen Teilmengen von Σ. Für $\sigma \in I$ sei

$$X_\sigma = \{\tau \in I : \tau \supset \sigma\}.$$

Die Menge X_σ genieren einen Filter F auf I wie folgt: Wir setzen

$$X \in F \text{ gdw. } \exists \sigma \in I X \supset X_\sigma.$$

Lemma 5.13 *F ist ein Filter auf I.*

Beweis: (a): Seien $X, Y \in F$. Seien $\sigma, \tau \in I$ so, dass $X \supset X_\sigma$ und $Y \supset X_\tau$. Dann gilt $X \cap Y \supset X_\sigma \cap X_\tau = X_{\sigma\cup\tau}$, also auch $X \cap Y \in F$. (b) ist trivial. (c): Da $\emptyset \in I$, gilt $I \in F$. (d): Da $\sigma \in X_\sigma$ für alle $\sigma \in I$, gilt $\emptyset \notin F$. □

Sei nun (mit Hilfe des Satzes von Tarski) U ein Ultrafilter auf I, der F fortsetzt. Wir setzen dann $\tilde{\mathfrak{M}} = \prod_{\sigma\in I} \mathfrak{M}_\sigma / U$. Wir definieren eine $\tilde{\mathfrak{M}}$–Belegung β durch: $\beta(v_k) = [f]$, wobei $f(\sigma) = \beta_\sigma(v_k)$ für alle $\sigma \in I$. Es genügt nun zu zeigen, dass $\mathfrak{M} \models \Sigma[\beta]$. Sei also $\varphi \in \Sigma$. Dann folgt aus $\varphi \in \sigma$ (d.h.

$\{\varphi\} \subset \sigma\}$, dass $\mathfrak{M}_\sigma \models \varphi[\beta_\sigma]$, also $\{\sigma : \mathfrak{M}_\sigma \varphi[\beta_\sigma]\} \supset X_{\{\varphi\}} \in UK$, und damit auch $\{\sigma : \mathfrak{M}_\sigma \models \varphi[\beta_\sigma]\} \in U$. Auf Grund des Satzes von Łoś gilt dann $\tilde{\mathfrak{M}} \models \varphi[\beta]$ wie gewünscht.

Ein Spezialfall von Ultraprodukten ist die Ultrapotenz. Sei $I \neq \emptyset$, und sei U ein Ultrafilter auf I. Sei $\mathfrak{M}$ ein $\mathcal{L}$–Modell, und sei $\mathfrak{M}_i = \mathfrak{M}$ für alle $i \in I$. Dann schreiben wir:

$$Ult(\mathfrak{M}; U)$$

für $\prod_{i \in I} \mathfrak{M}_i / U$ und nennen dies die *Ultrapotenz von* $\mathfrak{M}$ *mittels* U.

Der Satz von Łoś ergibt sofort das folgende

Korollar 5.14 *Sei $\bar{\beta}$ eine $\mathfrak{M}$–Belegung, und sei die $Ult(\mathfrak{M}; U)$–Belegung β definiert durch $\beta(v_k) = [c_{\bar{\beta}(v_k)}]$, wobei $c_{\bar{\beta}(v_k)}$ die konstante Funktion mit Wert $\bar{\beta}(v_k)$ (und Definitionsbereich I) ist. Dann gilt*

$$Ult(\mathfrak{M}; U) \models \varphi[\beta] \text{ gdw. } \mathfrak{M} \models \varphi[\bar{\beta}]$$

für alle Formeln φ.

Es existiert auch eine natürliche "Einbettung" e von $\mathfrak{M}$ nach $Ult(\mathfrak{M}; U)$. Für $a \in |\mathfrak{M}|$ setzen wir $e(a) = [c_a]$, wobei c_a die konstante Funktion mit Wert a (und Definitionsbereich I) ist. Es gilt dann (unter Verwendung der Schreibweise aus Kapitel 3):

Korollar 5.15 *Es gilt*

$$Ult(\mathfrak{M}; U) \models \varphi(e(a_0), \dots, e(a_{j-1})) \text{ gdw. } \mathfrak{M} \models \varphi(a_0, \dots, a_{j-1})$$

für alle Formeln φ und $a_0, \dots, a_{j-1} \in |\mathfrak{M}|$.

Auf diese Art und Weise lassen sich sehr leicht "Nichtstandardmodelle" konstruieren. Sei etwa

$$\mathfrak{N} = (\mathbb{N}; 0, S, <, +, \cdots, E),$$

und sei U ein Ultrafilter auf $\mathbb{N}$, der den Frechét–Filter auf $\mathbb{N}$ fortsetzt. Dann ist $Ult(\mathfrak{N}; U)$ nicht isomorph zu $\mathfrak{N}$ (d.h. die Einbettung e ist nicht surjektiv). Sei

$$\mathcal{R} = (\mathbb{R}; 0, 1, <, +, \cdot, E),$$

und sei wieder U ein Ultrafilter auf $\mathbb{N}$, der den Frechét–Filter auf $\mathbb{N}$ fortsetzt. Dann enthält $Ult(\mathcal{R}; U)$ "infinitesimale" Zahlen als auch "unendlich große" Zahlen.

Kapitel 6

Peano–Arithmetik und der 2. Gödelsche Unvollständigkeitssatz

Die Sprache der PEANO–Arithmetik ist $\mathcal{L}_A$[1], d.h., die Sprache der elementaren Zahlentheorie. Diese Sprache besitzt die Konstante 0, die Funktoren $S, +, \cdot$ und E, sowie das Relationssymbol $<$. Das Standardmodell von $\mathcal{L}_A$ ist $\mathcal{N} = (\mathbb{N}; 0, <, S, +, \cdot, E)$.[2]

Die *Peano–Arithmetik*, kurz PA, besitzt die folgenden Axiome. Zunächst sind alle Axiome von A_E aus Kapitel 6 Axiome von PA, d.h.

(1) $\forall v_1 S(v_1) \neq 0$

(2) $\forall v_1 \forall v_2 (S(v_1) = S(v_2) \to v_1 = v_2)$

(3) $\forall v_1 \forall v_2 (v_1 < S(v_2) \leftrightarrow (v_1 < v_2 \vee v_1 = v_2))$

(4) $\forall v_1 \neg v_1 < 0$

(5) $\forall v_1 \forall v_2 (v_1 < v_2 \vee v_1 = v_2 \vee v_2 < v_1)$

(6) $\forall v_1 v_1 + 0 = v_1$

(7) $\forall v_1 \forall v_2 v_1 + S(v_2) = S(v_1 + v_2)$

(8) $\forall v_1 v_1 \cdot 0 = 0$

(9) $\forall v_1 \forall v_2 v_1 \cdot S(v_2) = v_1 \cdot v_2 + v_1$

[1] Das A steht für “Arithmetik”.

[2] Das Symbol 0 steht also für die Null, d.h. für 0, etc. Zur Differenzierung hätten wir vielleicht $\dot{0}$ für das Symbol und 0 für das Objekt Null schreiben sollen.

(10) $\forall v_1 v_1 E 0 = S(0)$

(11) $\forall v_1 \forall v_2 v_2 E S(v_2) = (v_1 E v_2) \cdot v_1$

Sodann enthält PA unendlich viele weitere Axiome. Sei φ eine $\mathcal{L}_A$–Formel, in der die Variablen $v_{i_0}, v_{i_1}, \ldots, v_{i_n}$ frei vorkommen. Dann ist das zu φ gehörige *Induktionsaxiom*

$$(12)_\varphi \ \ \forall v_{i_1} \ldots \forall v_{i_n} (\varphi_0^{v_{i_0}} \wedge \forall v_{i_0} (\varphi \rightarrow \varphi_{S v_{i_0}}^{v_{i_0}}) \rightarrow \forall v_{i_0} \varphi)$$

ebenfalls zu PA. Die Axiome von PA sind die $\mathcal{L}_A$–Sätze, die in der Menge

$$A_E \cup \{(12)_\varphi : \varphi \text{ ist } \mathcal{L}_A\text{–Formel}\}$$

liegen. Satz 7.4 besagt, dass A_E alle wahren Σ_1–Sätze von $\mathcal{L}_A$ beweist. Wir hatten diese Aussage benutzt, um den 1. Gödelschen Unvollständigkeitssatz zu zeigen. Die Induktionsaxiome können benutzt werden, um wahre Π_1–Sätze von $\mathcal{L}_A$ zu beweisen. Insbesondere werden wir sehen, dass PA den Satz

“alle wahren Σ_1–Sätze von $\mathcal{L}_A$ sind in A_E beweisbar”,

bzw. die Übersetzung dieses Satzes in die Sprache $\mathcal{L}_A$ beweist. Dies wird sodann benutzt, um den 2. Gödelschen Unvollständigkeitssatz zu zeigen. Dieser besagt Folgendes: wenn $\top$ eine (u.U. triviale) rekursiv aufzählbare konsistente Erweiterung von PA ist, dann beweist $\top$ nicht die Konsistenz von $\top$. Da PA offensichtlich rekursiv aufzählbar ist und da (wie wir annehmen dürfen) PA konsistent ist, beweist also insbesondere PA nicht die Konsistenz von PA. Nach den Gödelschen Unvollständigkeitssätzen gibt es also ein (Nichtstandard–) Modell von PA $\cup$\{PA ist inkonsistent\}.

Der Beweis des 2. Gödelschen Unvollständigkeitssatzes erfordert einige Vorbereitung. Insbesondere muss z.B. geklärt werden, wie “$\top$ ist konsistent” in der Sprache $\mathcal{L}_A$ ausdrückbar ist. Die Formalisierung des Satzes “$\top$ ist konsistent” wird ein Π_1–Satz sein, so dass für $\top \supset$ PA aus dem 2. Gödelschen Unvollständigkeitssatz der 1. Unvollständigkeitssatz folgt.

Zuerst müssen wir $\mathcal{L}_A$ “gödelisieren”. Derartiges wurde bereits in Kapitel 7 getan. Wir wollen diesen Vorgang hier wiederholen und gründlicher darstellen.

$\mathcal{L}_A$ besitzt die folgenden Symbole: $0, <, S, +, \cdot, E,$ sowie $(,), \neg, \rightarrow, \forall, =$ und $v_0, v_1, v_2, \ldots$ $\mathcal{L}_A$–Ausdrücke sind endliche Folgen derartiger Symbole. Seien γ_0, γ_1, ..., γ_{n-1} Symbole. Wir wollen dem Ausdruck

$$a \equiv \gamma_0 \gamma_1 \ldots \gamma_{n-1}$$

eine “Gödelnummer” $\ulcorner a \urcorner$ zuordnen. Hierzu nehmen wir zunächst die folgenden Identifizierungen vor:

0	0
$<$	1
S	2
$+$	3
$\cdot$	4
E	5
$($	6
$)$	7
$\neg$	8
$\rightarrow$	9
$\forall$	10
$=$	11
v_0	12
v_1	13
v_2	14
$\vdots$	$\vdots$

Die Folge

$$a \equiv \gamma_0 \gamma_1 \ldots \gamma_{n-1}$$

wird damit zu einer Folge natürlicher Zahlen. Die “Gödelnummer” $\ulcorner a \urcorner$ von a sei dann die Zahl

$$\ulcorner a \urcorner = p_0^{\gamma_0+1} \cdot p_1^{\gamma_1+1} \cdot \ldots \cdot p_{n-1}^{\gamma_{n-1}+1}.$$

Hierbei sei $p_0, p_1, \ldots$ die natürliche Aufzählung aller Primzahlen. Offensichtlich können wir aus der Gödelnummer $\ulcorner a \urcorner$ die Folge (d.h. den Ausdruck) a “ablesen”.

Bevor wir nun sagen können, was zu tun ist, um den 2. Unvollständigkeitssatz zu beweisen, wollen wir einige Konventionen vereinbaren.

Sei $n \in \mathbb{N}$. Wir wollen dann in Zukunft

$$\underbrace{SS \ldots S}_{n\text{–viele}} 0$$

als den Standardnamen von n bezeichnen; wir schreiben auch $\check{n}$ für diesen Standardnamen. Sei φ eine Formel, in der genau die Variablen $v_{i_0}, \ldots, v_{i_{k-1}}$ mit $i_0 < \ldots < i_{k-1}$ frei vorkommen. Seien $m_0, \ldots, m_{k-1} \in \mathbb{N}$. Wir schreiben dann

$$\varphi(m_0, \ldots, m_{k-1})$$

für die Formel

$$\left(\dots\left(\varphi^{v_{i_0}}_{\check{m}_0}\right)\dots\right)^{v_{i_{k-1}}}_{\check{m}_{k-1}},$$

die aus φ hervorgeht, indem die Variable v_i (an ihren freien Vorkommnissen) durch den Standardnamen $\check{m}_i$ ersetzt wird, für $i = i_0, \dots, i_{k-1}$.[3] Sei nun $\top \supset$ PA eine rekursiv aufzählbare Menge von Axiomen (d.h. von $\mathcal{L}_A$–Formeln). Der technische Teil des Beweises des 2. Unvollständigkeitssatzes besteht in der Produktion einer Σ_1–Formel, für die wir $Bew_\top$ schreiben. $Bew_\top$ besitzt v_0 als einzige freie Variable, und es gelten die folgenden Aussagen.

Satz 6.1 (Fixpunktsatz) *Es gibt einen $\mathcal{L}_A$–Satz γ mit*

$$\top \vdash \gamma \leftrightarrow \neg Bew_\top(\ulcorner\gamma\urcorner).$$

In der Tat gibt es für jede $\mathcal{L}_A$–Formel ψ mit freier Variable v_i einen $\mathcal{L}_A$–Satz γ_ψ mit

$$\top \vdash \gamma_\psi \leftrightarrow \psi(\ulcorner\gamma_\psi\urcorner).$$

Satz 6.2 *Seien φ, ψ beliebige $\mathcal{L}_A$–Formeln. Dann gilt:*

(a) Wenn $\top \vdash \varphi$, dann $\top \vdash Bew_\top(\ulcorner\varphi\urcorner)$.

(b) $\top \vdash Bew_\top(\ulcorner\varphi \to \psi\urcorner) \to (Bew_\top(\ulcorner\varphi\urcorner) \to Bew_\top(\ulcorner\psi\urcorner))$.

(c) $\top \vdash Bew_\top(\ulcorner\varphi\urcorner) \to Bew_\top(\ulcorner Bew_\top(\ulcorner\varphi\urcorner)\urcorner)$.

Die Teilaussage (a) von Satz 6.2 wird sich daraus ergeben, dass für alle $\mathcal{L}_A$–Formeln φ gelten wird:

(*) $\top \vdash \varphi$ gdw. $\mathfrak{N} \models Bew_\top(\ulcorner\varphi\urcorner)$.

(Da $Bew_\top$ eine Σ_1–Formel ist, folgt dann aus $\top \vdash \varphi$ sogar $A_E \vdash Bew_\top(\ulcorner\varphi\urcorner)$.) Insbesondere können wir sagen, dass $Bew_\top$ das "Beweisbarkeitsprädikat" formalisiert. Darüber hinaus folgt aus (*):

(**) $\top$ ist inkonsistent gdw. $\mathfrak{N} \vdash Bew_\top(\ulcorner 0 \neq 0\urcorner)$.

$Bew_\top(\ulcorner 0 \neq 0\urcorner)$ ist also eine faire Formalisierung der Tatsache, dass $\top$ inkonsistent ist.

Die Teilaussage (c) von Satz 6.2 ist eine formale Variante der Teilaussage (a).

Aus den beiden obigen Sätzen ergibt sich nun der

[3] Eine frühere Konvention erklärte, was wir z.B. unter $\mathfrak{N} \models \varphi(m_0, \dots, m_{k-1})$ verstehen. Die beiden Konventionen stehen offenbar nicht in Konflikt miteinander.

Satz 6.3 (Zweiter Gödelscher Unvollständigkeitssatz) *Sei* $\top \supset \mathrm{PA}$ *rekursiv aufzählbar und konsistent. Dann gilt*

$$\top \nvdash \neg Bew_\top(\ulcorner 0 \neq 0 \urcorner).$$

Falls $\top$ inkonsistent ist, dann beweist $\top$ natürlich auch $\neg Bew_\top(\ulcorner 0 \neq 0 \urcorner)$, so dass $\top$ seine eigene Konsistenz genau dann beweist, wenn $\top$ inkonsistent ist.

Beweis des 2. Unvollständigkeitssatzes: Sei zunächst γ wie in Satz 6.1, d.h.

$$\top \vdash \gamma \leftrightarrow \neg Bew_\top(\ulcorner \gamma \urcorner).$$

Angenommen, $\top \vdash \gamma$. Dann gilt $\top \vdash Bew_\top(\ulcorner \gamma \urcorner)$ nach Satz 6.2 (a) und damit $\top \vdash \neg\gamma$ wegen der Eigenschaft von γ. Also beweist $\top$ sowohl γ als auch $\neg\gamma$, so dass $\top$ inkonsistent ist.

Dies zeigt: aus der Konsistenz von $\top$ (die wir voraussetzen) folgt $\top \nvdash \gamma$.

Wir betrachten nun den Satz $\gamma \to (\neg\gamma \to 0 \neq 0)$. Da dieser eine Tautologie ist, haben wir $\top \vdash \gamma \to (\neg\gamma \to 0 \neq 0)$. Wegen $\top \vdash \neg\gamma \leftrightarrow Bew_\top(\ulcorner \gamma \urcorner)$ folgt aber dann $\top \vdash \gamma \to (Bew_\top(\ulcorner \gamma \urcorner) \to 0 \neq 0)$. Satz 6.2 (a) liefert daraus $\top \vdash Bew_\top(\ulcorner \gamma \to (Bew_\top(\ulcorner \gamma \urcorner) \to 0 \neq 0) \urcorner)$. Zweimalige Anwendung von Satz 6.2 (b) ergibt dann

$$\top \vdash Bew_\top(\ulcorner \gamma \urcorner) \to (Bew_\top(\ulcorner Bew_\top(\ulcorner \gamma \urcorner) \urcorner) \to Bew_\top(\ulcorner 0 \neq 0 \urcorner)).$$

Satz 6.2 (c) besagt aber, dass

$$\top \vdash Bew_\top(\ulcorner \gamma \urcorner) \to Bew_\top(\ulcorner Bew_\top(\ulcorner \gamma \urcorner) \urcorner),$$

so dass also

$$\top \vdash Bew_\top(\ulcorner \gamma \urcorner) \to Bew_\top(\ulcorner 0 \neq 0 \urcorner),$$

und damit

$$\top \vdash \neg Bew_\top(\ulcorner 0 \neq 0 \urcorner) \to \neg Bew_\top(\ulcorner \gamma \urcorner).$$

Mit Hilfe der Eigenschaft von γ ergibt sich dann

$$\top \vdash \neg Bew_\top(\ulcorner 0 \neq 0 \urcorner) \to \gamma.$$

Hätten wir jetzt $\top \vdash \neg Bew_\top(\ulcorner 0 \neq 0 \urcorner)$, dann folgte $\top \vdash \gamma$, was nicht der Fall ist.

Wir haben also gezeigt, dass $\top \nvdash \neg Bew_\top(\ulcorner 0 \neq 0 \urcorner)$. $\square$

Leider ergeben sich oft die Dinge, die zu Gödels Zeiten in der Logik bewiesen wurden, durch ein derartiges Herumschieben von Symbolen.

Übrigens ergibt sich aus Satz 6.1 ein weiteres schönes Resultat, nämlich Tarskis Satz zur Undefinierbarkeit der Wahrheit:

Satz 6.4 (Tarski). *Es gibt keine $\mathcal{L}_A$–Formel φ mit freier Variable v_0, so dass*

$$\mathfrak{N} \models \varphi(\ulcorner\psi\urcorner) \text{ gdw. } \mathfrak{N} \models \psi$$

für alle $\mathcal{L}_A$–Sätze ψ.

Beweis: Andernfalls betrachte γ mit PA $\vdash \gamma \leftrightarrow \neg\varphi(\ulcorner\gamma\urcorner)$. Dann folgt aus $\mathfrak{N} \models \gamma$, dass $\mathfrak{N} \models \neg\varphi(\ulcorner\gamma\urcorner)$, also $\mathfrak{N} \models \neg\gamma$. Widerspruch! □

Mit Hilfe des Beweises des Fixpunktsatzes ergibt sich weiterhin auch, dass $\top \vdash Bew_\top(\ulcorner\varphi\urcorner) \to \varphi$ nicht für alle Σ_1–Sätze φ gelten kann, da γ mit $\top \vdash \gamma \leftrightarrow \neg Bew_\top(\ulcorner\gamma\urcorner)$ ein Σ_1–Satz sein wird und $\top \vdash \gamma \to Bew_\top(\ulcorner\gamma\urcorner)$.

Wie wird der obige Fixpunktsatz gezeigt? Hierzu benötigen wir eine $\mathcal{L}_A$–Formel, Sub, in der genau die Variablen v_0, v_1, v_2, v_3 frei vorkommen und die ausdrückt, dass "v_0 aus v_1 hervorgeht, indem jedes freie Vorkommnis der v_2–ten Variable durch den Standardnamen von v_3 ersetzt wird". Um dies genauer zu formulieren, vereinbaren wir eine Verallgemeinerung der oben getroffenen Konvention.

Sei φ eine Formel, in der genau die Variablen $v_{i_0}, \ldots, v_{i_{k-1}}$ mit $i_0 < \ldots < i_{k-1}$ frei vorkommen. Seien $m_0, \ldots, m_{k-1} \in \mathbb{N}$. Wir schreiben dann z.B.

$$\varphi(v_{i_0}, \ldots, v_{i_{l-1}}, m_l, v_{i_{l+1}}, \ldots, v_{i_{k-1}})$$

für die Formel

$$\varphi^{v_{i_l}}_{\check{m}_l}.$$

Analog dürfte klar sein, was wir mit

$$\varphi(v_{i_0}, \ldots, v_{i_{l-1}}, m_l, v_{i_{l+1}}, \ldots, v_{i_{j-1}}, m_j, v_{i_{j+1}}, \ldots, v_{i_{k-1}})$$

meinen, usw.

Wir wollen nun Folgendes.

Lemma 6.5 *Für alle $\mathcal{L}_A$–Formeln φ und für alle $i, n \in \mathbb{N}$ gilt*

$$\top \vdash \forall v_0(\mathrm{Sub}(v_0, \ulcorner\varphi\urcorner, i, n) \leftrightarrow v_0 = \ulcorner\varphi^{v_i}_{\check{n}}\urcorner).$$

Mit Hilfe dieses Lemmas zeigt sich der Fixpunktsatz wie folgt. Sei ψ eine $\mathcal{L}_A$–Formel mit freier Variable v_i. Sei o.B.d.A. $i = 0$. Wir definieren φ mit freier Variable v_3 durch

$$\varphi \equiv \exists v_0 \exists v_1 (\mathrm{Sub}(v_0, v_1, 3, v_3) \wedge v_1 = v_3 \wedge \psi).$$

Sei dann

$$\gamma \equiv \gamma_\psi \equiv \varphi^{v_3}_{\ulcorner \varphi \urcorner \, \mathrm{v}} \equiv \varphi(\ulcorner \varphi \urcorner).$$

Es gilt dann auf Grund des obigen Lemmas

$$\top \vdash \forall v_0 (\mathrm{Sub}(v_0, \ulcorner \varphi \urcorner, 3, \ulcorner \varphi \urcorner) \leftrightarrow v_0 = \ulcorner \gamma \urcorner).$$

Nun haben wir also

$$\top \vdash \psi(\ulcorner \gamma \urcorner) \leftrightarrow \exists v_0 (v_0 = \ulcorner \gamma \urcorner \wedge \psi),$$

und damit

$$\top \vdash \psi(\ulcorner \gamma \urcorner) \leftrightarrow \exists v_0 (\mathrm{Sub}(v_0, \ulcorner \varphi \urcorner, 3, \ulcorner \varphi \urcorner) \wedge \psi),$$

also auch

$$\top \vdash \psi(\ulcorner \gamma \urcorner) \leftrightarrow \exists v_0 \exists v_1 (\mathrm{Sub}(v_0, v_1, 3, \ulcorner \varphi \urcorner) \wedge v_1 = \ulcorner \varphi \urcorner \wedge \psi),$$

d.h.

$$\top \vdash \psi(\ulcorner \gamma \urcorner) \leftrightarrow \varphi(\ulcorner \varphi \urcorner),$$

und damit

$$\top \vdash \psi(\ulcorner \gamma \urcorner) \leftrightarrow \gamma.$$

Es bleibt uns also, die $\mathcal{L}_A$–Formeln Sub und $Bew_\top$ so zu konstruieren, dass Lemma 6.5 und Satz 6.2 für sie gelten.

Wir wollen jetzt die Formeln Sub und $Bew_\top$ produzieren.

Eine Relation $R \subset \mathbb{N}^k$ ist (*über* $\mathfrak{N}$) *durch eine* Σ_0– bzw. Σ_1– bzw. Π_1–*Formel definierbar* gdw. es eine Σ_0– bzw. Σ_1– bzw. Π_1–Formel φ mit freien Variablen $v_0, \ldots, v_{k-1}$ gibt, so dass für alle $n_0, \ldots, n_{k-1} \in \mathbb{N} : (n_0, \ldots, n_{k-1}) \in R$ gdw. $\mathfrak{N} \models \varphi(n_0, \ldots, n_{k-1})$.

Analog ist eine Funktion $f : \mathbb{N}^k \to \mathbb{N}$ *(über* $\mathfrak{N}$*) durch eine* Σ_0– bzw. Σ_1– bzw. Π_1–*Formel definierbar* gdw. die Relation $R \subset \mathbb{N}^{k+1}$ mit $(n_0, \ldots, n_{k-1}, n_k) \in R$ gdw. $f((n_0, \ldots, n_{k-1}) = n_k$ für alle $n_0, \ldots, n_k \in \mathbb{N}$ (über $\mathfrak{N}$) durch eine Σ_0– bzw. Σ_1– bzw. Π_1–Formel definierbar ist.

Zur besseren Lesbarkeit verwenden wir im Folgenden neben $v_0, v_1, \ldots$ auch $v, w, \ldots, n, m, \ldots, a, b, \ldots$ als formalsprachliche Variablen.

Lemma 6.6 *Die folgenden Relationen sind durch Σ_0–Formeln über $\mathfrak{N}$ zu definieren.*

(a) $n|m$ (d.h. n teilt m),

(b) p ist prim.

Beweis: (a) $\exists v n \cdot v = m$.
(b) $p > 1 \wedge \neg \exists v < p(v > 1 \wedge v|p)$. □

Lemma 6.7 *Die folgende Relation ist sowohl durch eine Σ_1– als auch durch eine Π_1–Formel definierbar:*

$$p \text{ ist die } n\text{–te Primzahl.}$$

Beweis:

$$\begin{aligned}
&\exists x(p^{n+1}|x \wedge \neg p^{n+2}|x \wedge 2|x \wedge \neg 4|x \wedge \forall q < x \forall r < x \\
&(q, r \text{ beide prim } \wedge q < r \wedge \forall s < r(s > q \to s \text{ nicht prim}) \wedge \\
&r|x \to \forall m < x(q^m|x \leftrightarrow r^{m+1}|x)).
\end{aligned}$$

Dies zeigt die Σ_1–Definierbarkeit. Die Π_1–Definierbarkeit ist ebenso einfach. □

Lemma 6.8 *Die folgenden Relationen sind durch Σ_1–Formeln definierbar:*

(a) n ist Gödelnummer.

(b) n ist die Gödelnummer eines Ausdrucks der Länge k.

Beweis: Gödelnummern sind natürliche Zahlen der Form $p_0^{m_0} \cdot \ldots \cdot p_{k-1}^{m_{k-1}}$, wobei $m_0, \ldots, m_{k-1} > 0$. Es genügt offensichtlich, (b) zu zeigen.

$$\forall p < n + 1(p \text{ ist prim } \to (p|n \leftrightarrow \exists l < k \; p \text{ ist die } l\text{–te Primzahl}).$$

Mit Hilfe des Beweises des vorigen Lemmas lässt sich dies leicht als Σ_1–Formel schreiben. □

Wir wollen nun sehen, dass “n ist die Gödelnummer einer Formel” durch eine Σ_1–Formel definierbar ist.

Ein Term entsteht durch wiederholte Verknüpfung aus “atomaren Termen”, d.h. Variablen und der Konstante 0. Ein Term ist also letztes Glied einer Folge

$$\tau_0, \tau_1, \ldots, \tau_{N-1},$$

wobei jedes Folgenglied entweder ein "atomarer Term" ist oder sich durch "Verknüpfung" aus früheren Termen ergibt, z.B. $\tau_i \equiv \tau_j + \tau_k$ für $j, k < i$.

Eine Formel entsteht durch wiederholte Verknüpfung aus atomaren Formeln. Eine Formel ist also letztes Glied einer Folge

$$\varphi_0, \varphi_1, \dots, \varphi_{N-1},$$

wobei jedes Folgenglied φ_i entweder atomare Formel ist oder sich durch "Verknüpfung" aus früheren Formeln ergibt, z.B. $\varphi_i \equiv (\varphi_j \to \varphi_k)$ für $j, k < i$ oder $\varphi_i \equiv \forall v_l \varphi_j$ für $j < i$ und ein beliebiges $l \in \mathbb{N}$.

Seien a, b Ausdrücke, d.h. etwa

$$a \equiv \gamma_0 \dots \gamma_{n-1}$$

und

$$b \equiv \gamma'_0 \dots \gamma'_{m-1}.$$

Die *Konkatenation von* a *und* b, in Zeichen $a^\frown b$ ist dann definiert als der Ausdruck

$$a^\frown b \equiv \gamma_0 \dots \gamma_{n-1} \gamma'_0 \dots \gamma'_{m-1}.$$

Analog sind Konkatenationen mehrerer (aber endlich vieler) Ausdrücke wie z.B. $a^\frown b^\frown c$ etc. definiert.

Lemma 6.9 *Die folgenden Relationen sind durch Σ_1–Formeln definiert:*

(a) Es gibt Ausdrücke a und b, so dass $n = \ulcorner a \urcorner, m = \ulcorner b \urcorner$ und $q = \ulcorner a^\frown b \urcorner$.

(b) Es gibt Ausdrücke a, b, c, so dass $n = \ulcorner a \urcorner, m = \ulcorner b \urcorner, q = \ulcorner c \urcorner$ und $r = \ulcorner a^\frown b^\frown c \urcorner$.

Analoges gilt für beliebig lange endliche Folgen $a, b, c, \dots$ von Ausdrücken.

Beweis von (a): $\exists k \exists l$ (n ist die Gödelnummer eines Ausdrucks der Länge $k \wedge m$ ist die Gödelnummer eines Ausdrucks der Länge $l \wedge q$ ist die Gödelnummer eines Ausdrucks der Länge $k + l \wedge \forall i < k \forall p < n(p$ ist die i–te Primzahl $\to \forall s < n(p^s | n \leftrightarrow p^s | q)) \wedge \forall i < l \forall p < m \forall p' < q(p$ ist die i–te Primzahl $\wedge p'$ ist die $k + i$–te Primzahl $\to \forall s < m(p^s | m \leftrightarrow p'^s | q)))$. $\square$

In unserer (halbumgangssprachlichen) Metasprache identifizieren wir Symbole von $\mathcal{L}_A$ mit Folgen der Länge 1, die nur aus diesem einen Symbol bestehen. Dann ist z.B. die Konkatenation

$$(^\frown \varphi^\frown \to^\frown \psi^\frown)$$

nichts anderes als die Formel $(\varphi \to \psi)$. Das vorige Lemma liefert dann sehr einfach:

Lemma 6.10 *Die folgenden Relationen sind durch Σ_0– (im Falle (a)) bzw. Σ_1–Formeln (in den Fällen (b) – (e)) definierbar.*

(a) n ist die Gödelnummer von 0 (genauer, eine Folge der Länge 1, die nur aus der Konstanten 0 besteht) bzw. von v_i.

(b) Es gibt einen Ausdruck a, so dass $n = \ulcorner a \urcorner$ und $m = \ulcorner S^\frown a \urcorner$.

(c) Es gibt Ausdrücke a, b, so dass $n = \ulcorner a \urcorner, m = \ulcorner b \urcorner$ und $q = \ulcorner +^\frown a^\frown b \urcorner$[4]

(d) Es gibt Ausdrücke a, b, so dass $n = \ulcorner a \urcorner, m = \ulcorner b \urcorner$ und $q = \ulcorner \cdot^\frown a^\frown b \urcorner$.

(e) Es gibt Ausdrücke a, b, so dass $n = \ulcorner a \urcorner, m = \ulcorner b \urcorner$ und $q = \ulcorner E^\frown a^\frown b \urcorner$.

Lemma 6.11 *Die folgende Relation ist durch eine Σ_1–Formel definierbar. n ist die Gödelnummer eines Terms.*

Beweis. Wir drücken aus, dass es ein x gibt, welches von der Gestalt

$$p_0^{n_0} \cdot p_1^{n_1} \cdot \ldots \cdot p_{s-1}^{n_{s-1}}$$

ist, so dass für jedes $j < s$ gilt: n_j ist Gödelnummer von 0 bzw. von v_i (für ein $i \in \mathbb{N}$), oder es gibt ein $k < j$, so dass $n_j = \ulcorner S^\frown a \urcorner$ und $n_k = \ulcorner a \urcorner$ für ein a ist, oder es gibt $k, l < j$, so dass $n_j = \ulcorner +^\frown a^\frown b \urcorner$ oder $n_j = \ulcorner \cdot^\frown a^\frown b \urcorner$ oder $n_j = \ulcorner E^\frown a^\frown b \urcorner$, $n_k = \ulcorner a \urcorner$ und $n_l \ulcorner b \urcorner$ für irgendwelche a, b ist, und schließlich ist $n = n_{s-1}$. □

Wir bekommen hiermit sehr einfach:

Lemma 6.12 *Die folgenden Relationen sind durch Σ_1–Formeln definierbar.*

(a) n ist die Gödelnummer einer atomaren Formel.

(b) Es gibt einen Ausdruck a, so dass $n = \ulcorner a \urcorner$ und $m = \ulcorner \neg^\frown a \urcorner$.

(c) Es gibt Ausdrücke a und b, so dass $n = \ulcorner a \urcorner, m = \ulcorner b \urcorner$ und $q = \ulcorner (^\frown a^\frown \to^\frown b^\frown) \urcorner$.

(d) Es gibt einen Ausdruck a, so dass $n = \ulcorner a \urcorner$ und $m = \ulcorner \forall^\frown v_i^\frown a \urcorner$.

[4] Wir verwenden hier wieder die polnische Notation.

Lemma 6.13 *Die folgende Relation ist durch eine Σ_1–Formel definierbar. n ist die Gödelnummer einer Formel.*

Beweis: Wir drücken aus, dass es ein x gibt, welches von der Gestalt

$$p_0^{n_0} \cdot p_1^{n_1} \cdot \ldots \cdot p_{s-1}^{n_{s-1}}$$

ist, so dass für jedes $j < s$ gilt: n_j ist Gödelnummer einer atomaren Formel, oder es gibt ein $k < j$, so dass $n_j = \ulcorner \neg a \urcorner$ und $n_k = \ulcorner a \urcorner$ für ein a ist, oder es gibt $k, l < j$, so dass $n_j = \ulcorner (^\frown a^\frown \rightarrow^\frown b^\frown) \urcorner$, $n_k = \ulcorner a \urcorner$ und $n_l = \ulcorner b \urcorner$ für irgendwelche a, b ist, oder es gibt $k < j$ und ein i, so dass $n_j = \ulcorner \forall^\frown v_i^\frown a \urcorner$ und $n_k = \ulcorner a \urcorner$ für ein a ist, und schließlich ist $n = n_{s-1}$. □

Wir haben somit zwei Beispiele für *rekursive Definitionen* gesehen. Sei $A \subset \mathbb{N}$ die kleinste Menge mit $B \subset \mathbb{N}$, die abgeschlossen unter Funktionen $F_0, \ldots, F_{l-1}$ ist. Dann ist $n \in A$ gdw. es eine Folge $(n_0, \ldots, n_{k-1})$ gibt mit $n_{k-1} = n$ und jedes Folgenglied gehört entweder zu B oder ergibt sich durch Anwendung einer der Funktionen $F_0, \ldots, F_{l-1}$ aus früheren Folgengliedern.

Wenn dann $B, F_0, \ldots, F_{l-1}$ durch Σ_1–Formeln definierbar sind, dann ist auch A durch eine Σ_1–Formel definierbar. Beispiele sind $A =$ die Menge aller $\mathcal{L}_A$–Terme oder $A =$ die Menge aller $\mathcal{L}_A$–Formeln. Wir werden nun weitere Beispiele sehen.

Lemma 6.14 *Die folgenden Relationen sind durch Σ_1–Formeln definierbar.*

(a) Es gibt eine Formel φ, so dass $n = \ulcorner \varphi \urcorner$ und die Variable v_i kommt an der k–ten Stelle der Formel φ frei vor.

(b) n ist die Gödelnummer eines Satzes.

Beweis von (a): Wir drücken aus, dass es x und y mit folgenden Eigenschaften gibt. x ist von der Gestalt

$$p_0^{n_0} \cdot p_1^{n_1} \cdot \ldots \cdot p_{s-1}^{n_{s-1}},$$

y ist von der Gestalt

$$p_0^{m_0} \cdot p_1^{m_1} \cdot \ldots \cdot p_{s-1}^{m_{s-1}},$$

und x bezeugt, dass n die Gödelnummer einer Formel ist. Darüber hinaus sei für $j < s$ die Zahl m_j Gödelnummer einer Folge, die alle Paare (k', i') auflistet, so dass gilt: wenn $n_j = \ulcorner \psi \urcorner$, dann kommt die Variable v_i, frei an der k'–ten Stelle der Formel ψ vor. Wir kennen mittlerweile die Methoden, mit deren Hilfe dies zu bewerkstelligen ist. Schließlich sei das Paar (k, i) in der Liste, die durch m_{s-1} kodiert wird. $\Box$

Wir bekommen nun recht einfach das

Lemma 6.15 *Die folgende Relation ist durch eine Σ_1–Formal definierbar. Es gibt Formeln ψ und φ mit $m = \ulcorner\psi\urcorner, n = \ulcorner\varphi\urcorner$, und ψ geht aus φ hervor, indem an jeder Stelle, an der v_i frei in φ vorkommt, der Term $\check{n}$ eingesetzt wird, d.h. $m = \ulcorner\psi^{v_i}_{\check{n}}\urcorner$.*

Wir haben somit Sub gewonnen. Mit Hilfe von Sub können wir nun die Menge der logischen Axiome der Klasse (2) (und auch die Menge der logischen Axiome der Klasse (6)) durch eine Σ_1–Formel definieren. Dies liefert schließlich:

Lemma 6.16 *Die Menge der logischen Axiome ist durch eine Σ_1–Formel definierbar.*

Da wir voraussetzen, dass $\top \supset \mathrm{PA}$ rekursiv aufzählbar ist, ist $\{\ulcorner\varphi\urcorner : \varphi \in \top\}$ durch eine Σ_1–Formel definierbar. Wir könnten diese Σ_1–Definierbarkeit auch zur Voraussetzung machen. Man überzeugt sich leicht, dass $\{\ulcorner\varphi\urcorner : \varphi \in \mathrm{PA}\}$ durch eine Σ_1–Formel definierbar ist.

Nun ist φ aus $\top$ beweisbar gdw. es eine Folge

$$(\varphi_0, \dots, \varphi_{N-1})$$

gibt, so dass jedes φ_i entweder zu $\top \cup \Lambda$ gehört oder durch modus ponens aus φ_k, φ_j für $k, j < i$ hervorgeht, d.h. etwa $\varphi_j \equiv \varphi_k \rightarrow \varphi_i$, und so dass $\varphi_{N-1} \equiv \varphi$. Unsere Methoden liefern sodann das

Lemma 6.17 *Die folgende Relation ist durch eine Σ_1–Formel definierbar. Es gibt eine Formel φ, die aus $\top$ beweisbar ist, so dass $n = \ulcorner\varphi\urcorner$.*

Wir haben damit $Bew_\top$ hergestellt.

Wir betrachten nun Satz 6.2 und Lemma 6.5.

Der Beweis von Lemma 6.5 verläuft wie folgt. Zu zeigen ist

(1) $\top \vdash (\mathrm{Sub}(\ulcorner\varphi^{v_i}_{\check{n}}\urcorner, \ulcorner\varphi\urcorner, i, n),$

was einfach ist, und

(2) $\top \vdash \forall v_0 \forall v_0' (\mathrm{Sub}(v_0, \ulcorner\varphi\urcorner, i, n) \wedge \mathrm{Sub}(v_0', \ulcorner\varphi\urcorner, i, n) \rightarrow v_0 = v_0').$

Zu Letzterem zeigt man induktiv in $\top$, dass Sub in der nullten Komponente funktional ist. Wir übergehen die Details.

Wir müssen uns damit Satz 6.2 zuwenden.

Wir beginnen mit Satz 6.2 (a). Sei zunächst $\top \vdash \varphi$ für eine $\mathcal{L}_A$–Formel φ vorausgesetzt. Dann gilt auch $\mathfrak{N} \models Bew_\top(\ulcorner\varphi\urcorner)$ auf Grund der Wahl von $Bew_\top$. Da aber $Bew_\top$ Σ_1 ist, folgt damit aus Satz 7.4, dass $A_E \vdash Bew_\top(\ulcorner\varphi\urcorner)$, also erst recht $\top \vdash Bew_\top(\ulcorner\varphi\urcorner)$. Dies zeigt Satz 6.2 (a).

Die Aussage von Satz 6.2 (b) ist die formale Variante der Tatsache, dass aus $\top \vdash \varphi \to \psi$ und $\top \vdash \varphi$ auch $\top \vdash \psi$ folgt (welches sich wiederum daraus ergibt, dass man die Beweise von $\varphi \to \psi$ und φ aus $\top$ neben–/untereinander schreibt und sodann einmal den modus ponens anwendet). Satz 6.2 (b) ergibt sich somit leicht aus der Konstruktion von $Bew_\top$.

Anstelle von Satz 6.2 (c) zeigen wir die folgende allgemeine Aussage:

Lemma 6.18 *Sei ψ ein Σ_1–Satz von $\mathcal{L}_A$. Dann gilt*

$$\top \vdash \psi \to Bew_\top(\ulcorner\psi\urcorner).$$

Die Aussage dieses Lemmas kann als formalisierte Variante von Satz 7.4 angesehen werden.

Wir zeigen Lemma 6.18 zunächst für Σ_0–Sätze ψ. Nun gilt sicherlich $\mathfrak{N} \models \psi \to Bew_\top(\ulcorner\psi\urcorner)$ auf Grund von Satz 7.4, also $\mathfrak{N} \models \neg\psi$ oder $\mathfrak{N} \models Bew_\top(\ulcorner\psi\urcorner)$. Falls $\mathfrak{N} \models \neg\psi$, dann ist, da $\neg\psi$ Σ_0 ist, $\neg\psi$ in A_E beweisbar, d.h. $A_E \vdash \neg\psi$. Falls $\mathfrak{N} \models Bew_\top(\ulcorner\psi\urcorner)$, dann ist $Bew_\top(\ulcorner\psi\urcorner)$. In jedem Falle ergibt sich also $A_E \vdash \neg\psi \vee Bew_\top(\ulcorner\psi\urcorner)$, also auch $\top \vdash \psi \to Bew_\top(\ulcorner\psi\urcorner)$.

Dieses Argument funktioniert nicht mehr, falls ψ ein Σ_1–Satz ist, da dann $\neg\psi$ Π_1 ist. Der Beweis von Lemma 6.18 benutzt in der Tat $\top \supset$ PA.

Eine unmittelbare Konsequenz aus dem Zweiten Gödelschen Unvollständigkeitssatz ist das folgende

Korollar 6.19 *Sei $\Gamma \supset PA$ eine rekursiv aufzählbare konsistente Menge von $\mathcal{L}_A$–Formeln. Dann gilt es reellviele konsistente Mengen $\widetilde{\Gamma} \supset \Gamma$ von $\mathcal{L}_A$–Formeln, die sich paarweise widersprechen, d.h. für zwei verschiedene derartige Mengen $\widetilde{\Gamma}$ und $\widetilde{\Gamma}'$ gibt es eine $\mathcal{L}_A$–Formel φ mit $\varphi \in \widetilde{\Gamma}$ und $\neg\varphi \in \widetilde{\Gamma}'$.*

Beweis: Wir definieren zunächst rekursiv nach der Länge von s für jede endliche 0-1–Folge $s \in \{0,1\}^*$ eine Menge $\Gamma_s \supset \Gamma$. Sei $(\varphi_n : n \in \mathbb{N})$ eine Aufzählung aller $\mathcal{L}_A$–Formeln. Wir definieren jedes Γ_s so, dass Γ_s aus Γ

durch Hinzunahme endlich vieler Formeln entsteht; insbesondere ist jedes Γ_s immer noch rekursiv aufzählbar.

Wir setzen $\Gamma_\emptyset = \Gamma$. Sei nun Γ_s definiert. Auf Grund des ersten Gödelschen Unvollständigkeitssates gibt es ein kleinstes $k = k(s)$, so dass Γ_s weder φ_k noch $\neg\varphi_k$ beweist. Wir setzen sodann $\Gamma_{s0} = \Gamma_s \cup \{\varphi_k\}$ und $\Gamma_{s1} = \Gamma_s \cup \{\neg\varphi_k\}$.[5]

Für jede unendliche 0-1–Folge f definieren wir $\Gamma_f = \bigcup\{\Gamma_s : s \subset f\}$ und $\widetilde{\Gamma}_f = \{\varphi : \Gamma_f \vdash \varphi\}$. Offenbar ist jedes Γ_f konsistent und die Familie aller $\widetilde{\Gamma}_f$ ist wie gewünscht. □

Wir wollen nun eine alternativen Beweis einer Variante des 1. Gödelschen Unvollständigkeitssatzes kennen lernen. Dieser Beweis wurde von S. Kripke gefunden. Er ist weniger indirekt als der oben angegebene Beweis: wir sehen tatsächlich eine Aussage, die weder beweisbar noch widerlegbar ist!

Im Folgenden sei $\mathcal{N}$ wieder das Modell $(\mathbb{N}; 0, 1, <, +, \cdot, E)$ und $\mathcal{L}_A$ sei die zugehörige Sprache der elementaren Zahlentheorie Stufe.

Sei s eine endliche oder unendliche (echt) aufsteigende Folge natürlicher Zahlen. Wir bezeichnen mit $(s)_k$ das k^{te} Element von s (falls $k < lh(s) =$ Länge von s; sonst ist $(s)_k$ nicht definiert). D.h. $s = (s)_0, (s)_1, \ldots, (s)_{lh(s)-1}$ mit $(s)_0 < (s)_1 < \ldots < (s)_{lh(s)-1}$ falls $lh(s) < \infty$ und $s = (s)_0, (s)_1, \ldots$ mit $(s)_0 < (s)_1 < \ldots$ falls $lh(s) = \infty$.

Sei ein solches s mit $lh(s) \geq 2$ gegeben. Sei $\varphi(v, w)$ eine Formel der Sprache $\mathcal{L}_A$. Wir betrachten das folgende Spiel $\mathcal{G}(s, \varphi)$ zwischen den Spielern I und II. I spielt zunächst ein $k < lh(s) - 1$ und eine natürliche Zahl $m_0 < (s)_k$. II spielt daraufhin eine natürliche Zahl $m_1 < (s)_{k+1}$:

$$\begin{array}{c|ccc} I & k & m_0 & \\ \hline II & & & m_1 \end{array}$$

II gewinnt $\mathcal{G}(s, \varphi)$ gdw. $\mathcal{N} \models \varphi(m_0, m_1)$. Wir sagen, dass II eine Gewinnstrategie für $\mathcal{G}(s, \varphi)$ besitzt, oder auch: dass s φ erfüllt, gdw.

$$\forall k < lh(s) - 1 \forall m_0 < (s)_k \exists m_1 < (s)_{k+1} \varphi(m_0, m_1).$$

Sei nun s gegeben mit $lh(s) \geq 2n (n > 0)$. Sei $\varphi(v_0, \ldots, v_{2n-1})$ eine Formel der Sprache $\mathcal{L}_A$. Dann bezeichnet $\mathcal{G}(s, \varphi)$ das folgende Spiel zwischen den Spielern I und II.

$$\begin{array}{c|ccccccccccc} I & k_0 & m_0 & & k_2 & m_2 & & \ldots & & k_{2n-2} & m_{2n-2} & \\ \hline II & & & m_1 & & & m_3 & & \ldots & & & m_{2n-1} \end{array}$$

[5] Hierbei ist sh, für $h = 0, 1$, das Resultat des Anfügens des neuen Folgengliedes h an die Folge s.

Regeln: $k_0 < lh(s)-1, m_0 < (s)_{k_0}, m_1 < (s)_{k_0+1}$, und $k_{2i} < k_{2i+2} < lh(s)-1$, $m_{2i+2} < (s)_{k_{2i+3}}, m_{2i+3} < (s)_{k_{2i+3}}$ für $i < n-1$. II gewinnt $\mathcal{G}(s,\varphi)$ gdw. $\mathcal{N} \models \varphi(m_0, \dots, m_{2n-1})$. Man definiert "$II$ hat eine Gewinnstrategie für $\mathcal{G}(s,\varphi)$" (= "s erfüllt φ") völlig analog zum obigen Spezialfall.

Wenn s *un*endlich und $\varphi(v_0, \dots, v_{2n-1})$ beliebig ist, dann gilt: Wenn s die Formel $\varphi(v_0, \dots, v_{2n-1})$ erfüllt, dann gilt

$$\mathcal{N} \models \forall m_0 \exists m_1 \dots \forall m_{2n-2} \exists m_{2n-1} \varphi(m_0, \dots, m_{2n-1}),$$

Da $\lim_{k\to\infty}(s)_k = \infty$.

Eine endliche Folge s heißt gut, gdw. $(s)_0 > lh(s)$ und für $0 < i < lh(s)$ ist $(s)_i > ((s)_{i-1})^{(s)_{i-1}}$. Eine Formel $\varphi(v_0, \dots, v_{2n-1})$ heißt m–erfüllbar (für $m \geq 2n$) gdw. es eine gute Folge s der Länge m gibt, so dass s φ erfüllt.

Wenn

$$\mathcal{N} \models \forall m_0 \exists m_1 \dots \forall m_{2n-2} \exists m_{2n-1} \varphi(m_0, \dots, m_{2n-1}),$$

dann ist φ m–erfüllbar für alle $m \geq 2n$.

Die Axiome der Peano–Arithmetik (kurz: PA) sind im Kapitel 13 aufgelistet; PA entsteht aus A_E (siehe Kapitel 6) durch Hinzunahme der Induktionsaxiome.

Im Folgenden sei $(\varphi_m | m \in \mathbb{N})$ eine beliebige feste rekursive Aufzählung der Axiome von PA. Für $m \in \mathbb{N}$ bezeichnen wir mit Φ_m die Formel $\varphi_0 \wedge \dots \wedge \varphi_m$. Wir setzen im Folgenden voraus, dass $(\varphi_m | m \in \mathbb{N})$ so gewählt wurde, dass Φ_m logisch äquivalent zu einer Formel der folgenden Gestalt ist:

$$\forall v_0 \exists v_1 \dots \forall v_{2m-1} \Psi(v_0, v_1, \dots, v_{2m-2}, v_{2m-1}).$$

wobei Ψ keine Quantoren enthält.

Sei $m \in \mathbb{N}$. Es gibt dann eine unendliche (echt aufsteigende) Folge s, die Ψ_m erfüllt. Es gilt auch: Ψ_m ist $2m$–erfüllbar.

Wir bezeichnen mit σ den Satz: für alle m ist Ψ_m $2m$–erfüllbar. σ ist von der Gestalt $\forall v_0 \dots \forall v_k \exists v_{k+1} \dots \exists v_l \psi(v_0, \dots, v_l)$, wobei $\psi(v_0, \dots, v_m)$ keine *unbeschränkten* Quantoren besitzt. (D.h. σ ist Π_2.) Es gilt $\mathcal{N} \models \sigma$.

Wir wollen nun ein Modell von PA konstruieren, in dem σ falsch ist.

Sei Φ ein Satz der Gestalt

$$\forall v_0 \exists v_1 \dots \forall v_{2m-1} \Psi(v_0, v_1, \dots, v_{2m-2}, v_{2m-1}),$$

wobei Ψ keine Quantoren enthält. Dann gilt

$$\text{PA} \vdash \Phi \to \Psi \text{ ist } 2m\text{–erfüllbar}.$$

Es gilt also in PA auch, dass Ψ_m $2m$–erfüllbar ist. Die Aussage

$$\exists m \Psi_m \text{ ist nicht } 2m\text{–erfüllbar}$$

(d.h. $\neg\sigma$!) ist *nicht* in PA beweisbar (falls alle in PA beweisbaren Sätze wahr sind). Wir wollen zeigen, dass σ nicht beweisbar ist.

Sei $\mathfrak{M}$ ein Nichtstandardmodell von PA. Da für fede Standard–Zahl $n \in |\mathfrak{M}|$ gilt, dass $\mathfrak{M} \models \Psi_n$ ist $2n$–erfüllbar, gibt es eine Nichtstandard–Zahl $N \in |\mathfrak{M}|$ mit

$$\mathfrak{M} \models \Psi_N \text{ ist } 2N\text{–erfüllbar.}$$

Es gibt also ein $S \in |\mathfrak{M}|$, so dass $\mathfrak{M} \models S$ erfüllt Ψ_N. Seien o.B.d.A. $0, 1, 2 \ldots \in |\mathfrak{M}|$ die Standard–Zahlen in $\mathfrak{M}$. Bezeichne $\vec{S}$ die unendliche Folge $(S)_0, (S)_1, \ldots$ Jedes echte Anfangsstück dieser Folge existiert in $\mathfrak{M}$, aber $\vec{S}$ existiert nicht in $\mathfrak{M}$ (da die Menge der Standard–Zahlen nicht über $\mathfrak{M}$ definierbar ist).

Sei $n \in |\mathfrak{M}|$ eine Standard–Zahl. Dann gilt

$$(\mathfrak{M}, \vec{S}) \text{ erfüllt } \Psi_n.$$

Sei nun H dasjenige Submodell von $\mathfrak{M}$, das genau alle Zahlen aus $|\mathfrak{M}|$ enthält, die (in $\mathfrak{M}$) kleiner als ein Element der Folge $\vec{S}$ sind. Da $\vec{S}$ gut ist, ist H abgeschlossen unter $+$, $\cdot$ und E.

Es gilt $H \models$ PA. [Sei $n \in |\mathfrak{M}|$ eine Standard–Zahl. $(\mathfrak{M}, \vec{S}) \models \vec{S}$ erfüllt Ψ_n. $\vec{S}$ ist "kofinal in" H. Damit gilt dann Ψ_n in H.]

Wir nehmen nun o.B.d.A. an, dass S (in $\mathfrak{M}$) minimal gewählt war, so dass S die Länge $2N$ hat und $\mathfrak{M} \models S$ erfüllt Ψ_N gilt. Dann gilt $S \notin H$, und $H \models P_N$ ist nicht $2N$–erfüllbar. [Angenommen, $H \models \overline{S}$ erfüllt P_N. Dann gilt $\mathfrak{M} \models \overline{S}$ erfüllt P_N. Aber $\overline{S}$ ist kleiner als S in $\mathfrak{M}$.]

Damit gilt $\neg\sigma$ in H!

Wir haben damit die folgende Variante des Ersten Gödelschen Unvollständigkeitssatzes gezeigt:

Satz 6.20 *Der oben angegebene Π_2–Satz σ der Sprache der Zahlentheorie, ist in* PA *weder beweisbar noch widerlegbar.*

Kapitel 7

Arithmetik und Mengenlehre

Wir wollen nun die natürlichen Zahlen benutzen, um ein Modell der Mengenlehre zu konstruieren. In der Mengenlehre kann mit weniger Kodierungsaufwand über mehr Dinge gesprochen werden.

Wir fassen natürliche Zahlen wie folgt als "Mengen" auf. Sei $n \in \mathbb{N}$. Schreibe n in Dualdarstellung, d.h. $n = \Sigma m_j \cdot 2^i$, wobei $m_i \in \{0, 1\}$ für alle i. Wir fassen dann n als die Menge aller i auf, so dass $m_i = 1$. Anders gesagt: wir definieren eine zweistellige Relation $E \subset \mathbb{N} \times \mathbb{N}$ auf $\mathbb{N}$ wie folgt. Seien $k, n \in \mathbb{N}$. Dann gelte kEn gdw. $m_k = 1$, wobei $n = \Sigma m_i \cdot 2^i$ die Dualdarstellung von n ist.

Die Sprache $\mathcal{L}_\in$ der Mengenlehre besitzt weder Konstanten noch Funktoren und als einziges Relationssymbol das zweistellige $\in$ für "ist Element von". Wenn $M \neq \emptyset$ und $R \subset M \times M$, so ist $(M; R)$ Modell von $\mathcal{L}_\in$. Insbesondere is $(\mathbb{N}; E)$ Modell von $\mathcal{L}_\in$. Wir wollen nun untersuchen, ob $(\mathbb{N}; E)$ ein "sinnvolles" Modell von $\mathcal{L}_\in$ ist, d.h. ob $(\mathbb{N}; E)$ Modell eines hinreichend großen Fragments der Standardaxiomatisierung der Mengenlehre ist. Hierzu müssen wir letztere kennen lernen.

Das erste Axiom, das *Extensionalitätsaxiom*, besagt, dass zwei Mengen gleich sind gdw. sie dieselben Elemente besitzen.

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

Offensichtlich gilt $(\mathbb{N}; E) \models (Ext)$.

Das nächste Axiom, das *Fundierungsaxiom*, besagt, dass jede nichtleere Menge ein $\in$–minimales Element besitzt.

$$(Fund)\ \forall x (\exists y\, y \in x \rightarrow \exists y (y \in x \wedge \neg \exists z (z \in y \wedge z \in x))).$$

Mit Hilfe von Abkürzungen schreibt sich dies besser. Wir schreiben $x = \emptyset$ für $\neg\exists y\ y \in x, x \neq \emptyset$ für $\neg x = \emptyset, x \cap y = \emptyset$ für $\neg\exists z(z \in x \wedge z \in y)$. Dann liest sich $(Fund)$ wie folgt:

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

Seien $k, n \in \mathbb{N}$. Dann folgt aus $(\mathbb{N}; E) \models k \in n$, dass $k < n$: dies folgt einfach daraus, dass $2^k > k$ für alle $k \in \mathbb{N}$. Sei also $n \in \mathbb{N}$ so, dass $(\mathbb{N}; E) \models n \neq \emptyset$ d.h. $n \neq 0$!). Sei $k < n$ das kleinste k' mit $(\mathbb{N}; E) \models k \in n$. Dann gilt $(\mathbb{N}; E) \models k \cap n = \emptyset$. Wir haben $(\mathbb{N}; E) \models Fund$ gezeigt.

Wir schreiben $x = \{y, z\}$ für

$$y \in x \wedge z \in x \wedge \forall u \in x(u = y \vee u = z).$$

Das *Paarmengenaxiom* lautet

$(Paar)$ $\forall x \forall y \exists z\ z = \{x, y\}$.

$(\mathbb{N}; E) \models Paar$ zeigt sich wie folgt.

Seien $n, m \in \mathbb{N}$. Sei

$$q = \begin{cases} 2^n + 2^m, & \text{falls } n \neq m \\ 2^n & \text{, falls } n = m. \end{cases}$$

Dann gilt offensichtlich $(\mathbb{N}; E) \models q = \{n, m\}$.

Wir schreiben $x = \bigcup y$ für

$$\forall z(z \in x \leftrightarrow \exists u \in y\ z \in u).$$

Das *Vereinigungsaxiom* lautet

(Ver) $\forall x \exists y\ y = \bigcup x$.

Wir zeigen $(\mathbb{N}; E) \models Ver$ folgendermaßen. Sei $n \in \mathbb{N}$. Sei $n = \Sigma m_i \cdot 2^i$ die Dualdarstellung von n, und sei für $m_i = 1$ $i = \Sigma m_k^i \cdot 2^k$ die Dualdarstellung von i. Wir setzen dann

$$m = \sum_{\substack{m_k^i = i \\ \text{für ein } i \\ \text{mit } m_i = 1}} 2^k.$$

Offensichtlich gilt $(\mathbb{N}; E) \models m = \bigcup n$.

Wir schreiben $x \subset y$ für $\forall z \in x\ z \in y$ und $x = \mathcal{P}(y)$ für $\forall z(z \in x \leftrightarrow z \subset y)$. Das *Potenzmengenaxiom* besagt

(Pot) $\forall x \exists y\ y = \mathcal{P}(x)$.

$(\mathbb{N}; E) \models Pot$ zeigt man mit Hilfe derselben Methode, die auch $(\mathbb{N}; E) \models Ver$ zeigte. Sei $n \in \mathbb{N}$. Sei $n = \Sigma m_i \cdot 2^i$ die Dualdarstellung von n. Für ein $m \in \mathbb{N}$ mit Dualdarstellung $\Sigma m'_i \cdot 2^i$ gilt offenbar $(\mathbb{N}; E) \models m \subset n$ gdw. für alle $i, m'_i = 1 \Rightarrow m_i = 1$. Sei also I die (endliche!) Menge aller i mit $m_i = 1$ und sei P die Menge aller Teilmengen von I. Für $I^* \in P$ sei

$$n_{I^*} = \Sigma_{i \in I^*} 2^i.$$

(Offensichtlich ist $I^* \mapsto n_{I^*}$ injektiv.) Schließlich sei

$$m = \sum_{I^* \subset I} 2^{n_{I^*}}.$$

Es ist leicht zu sehen, dass $(\mathbb{N}; E) \models m = \mathcal{P}(n)S$.

Die Aussonderungsaxiome werden benötigt, um die Existenz definierbarer Teilmengen von einer gegebenen Menge zu zeigen.

Sei φ eine $\mathcal{L}_\in$–Formel, in der (o.B.d.A.) die Variablen $x, v_1, \ldots, v_p$ frei vorkommen. Das zu φ gehörige *Aussonderungsaxiom* lautet:

(Aus_φ) $\forall v_1 \ldots v_p \forall a \exists b \forall x (x \in b \leftrightarrow x \in a \wedge \varphi)$.

Die (unendliche!) Menge aller Aussonderungsaxiome wird auch als *Aussonderungsschema* bezeichnet. Man beweist leicht, dass $(\mathbb{N}; E)$ Modell des Aussonderungsschemas ist. Wir gehen einen Umweg.

Sei φ eine $\mathcal{L}_\in$–Formel, in der (o.B.d.A.) die Variablen $x, y, v_1, \ldots, v_p$ frei vorkommen. Das zu φ gehörige *Ersetzungsaxiom* lautet[1]

(Ers_φ) $\forall v_1 \ldots \forall v_p (\forall x \in a \forall y \forall y' (\varphi \wedge \varphi^y_{y'} \rightarrow y = y') \rightarrow \exists b \forall y (y \in b \leftrightarrow \exists x \in a \varphi))$.

Die (wiederum unendliche!) Menge aller Ersetzungsaxiome wird auch als *Ersetzungsschema* bezeichnet. Aus dem Ersetzungsschema zeigt sich das Aussonderungsschema sehr leicht wie folgt. Sei φ wie im zu φ gehörigen Aussonderungsaxiom gegeben. Setze $\psi \equiv \varphi \wedge x = y$. Dann gilt $Ers_\psi \vdash Aus_\varphi$.

Wir zeigen $(\mathbb{N}; E) \models Ers_\varphi$ für ein beliebiges φ wie folgt. Sei φ wie im zu φ gehörigen Ersetzungsaxiom gegeben. Seien $n_1, \ldots, n_p \in \mathbb{N}$ und sei $a \in \mathbb{N}$. Wir setzen voraus, dass

$$(\mathbb{N}; E) \models \forall x \in a \forall y \forall y' (\varphi(x, y, n_1, \ldots, n_p) \wedge \varphi(x, y', n_1, \ldots, n_p) \rightarrow y = y').$$

[1] o.B.d.A. komme y' in φ gar nicht vor.

Sei $(\mathbb{N}; E) \models k \in a$, d.h. für die Dualdarstellung $a = \Sigma m_i \cdot 2^i$ von a gilt $m_k = 1$. Falls ein l mit

$$(\mathbb{N}; E) \models \varphi(k, l, n_1, \ldots, n_p)$$

existiert, so sei $l(k)$ das eindeutige derartige l. Andernfalls sei $l(k)$ nicht definiert.

Setze dann

$$b = \sum_{\substack{(\mathbb{N}; E) \models k \in a \\ \text{und } l(k) \text{ ist} \\ \text{definiert.}}} 2^{l(k)}.$$

Es ist leicht zu sehen, dass

$$(\mathbb{N}; E) \models \forall y (y \in b \leftrightarrow \exists x \in a \varphi).$$

Aus dem Aussonderungsschema folgt die Existenz der leeren Menge, indem $\varphi \equiv x \neq x$ gewählt wird. Mit Hilfe des Paarmengen– und des Vereinigungsmengenaxioms zeigt sich dann leicht die Existenz der Mengen

$$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},$$

usw. Das *Auswahlaxiom* lautet

(AC) $\forall x (x \neq \emptyset \wedge \forall y \in x \forall y' \in x (y \cap y' \neq \emptyset \leftrightarrow y = y') \rightarrow (\exists z \forall y \in x \exists u z \cap y = \{u\})$.

AC besagt also, dass jede nichtleere Menge, die aus paarweise disjunkten Mengen besteht, eine “Auswahlmenge” besitzt. Wir zeigen $(\mathbb{N}; E) \models AC$ wie folgt.

Sei $n \in \mathbb{N}$. Sei $(\mathbb{N}; E) \models n \neq \emptyset$, d.h. für die Dualdarstellung $n = \Sigma m_i \cdot 2^i$ von n gilt, dass ein i mit $m_i = 1$ existiert. Für jedes i mit $m_i = 1$ sei $i = \Sigma m_k^i \cdot 2^k$ die Dualdarstellung von i. Unter der Voraussetzung

$$(\mathbb{N}; E) \models \forall y \in n \forall y' \in n (y \cap y' \neq \emptyset \leftrightarrow y = y')$$

gilt dann, dass aus $i \neq j$ mit $m_i = 1 = m_j$ folgt: $m_k^i \neq m_k^j$ für alle k. Außerdem ist für alle i mit $m_i = 1$ eines der m_k^i gleich 1. Sei für $m_i = 1$ $k(i)$ das kleinste k mit $m_k^i = 1$. Es ist dann leicht zu sehen, dass

$$\sum_{m_i = 1} 2^{k(i)}$$

bezeugt, dass im Sinne von $(\mathbb{N}; E)$ n das Auswahlaxiom erfüllt.

Wir bezeichnen die Menge der Aussagen Ext, $Fund$, $Paar$, Ver, Pot, Ers_φ (für beliebige φ) und AC als $ZFC^{-\infty}$. Hierbei steht ZFC für Zermelo-Fraenkel, C für "choice" (Auswahl) und "$-\infty$" für die Abwesenheit des Unendlichkeitsaxioms. Letzterem wollen wir uns nun zuwenden.

Wir schreiben $x = y \cup z$ für $x = \bigcup\{y, z\}$. Wir schreiben $y = x + 1$ für $y = x \cup \{x\}$.

Eine Menge x heißt *induktiv* gdw. $\emptyset \in x \wedge \forall y \in x \; y + 1 \in x$. Das *Unendlichkeitsaxiom* besagt:

(∞) $\exists x$ (x ist induktiv).

Das System ZFC (Zermelo–Fraenkel, mit Auswahlaxiom) entsteht aus $ZFC^{-\infty}$ durch Hinzunahme des Unendlichkeitsaxioms.

Sei $(\mathbb{N}; E) \models m = n + 1$, d.h. $(\mathbb{N}; E) \models m = n \cup \{n\}$. Dann gilt insbesondere $(\mathbb{N}; E) \models n \in m$, also ist $n < 2^n \leq m$. Damit kann $(\mathbb{N}; E)$ *nicht* das Unendlichkeitsaxiom erfüllen.