Wolfgang Rautenberg

Berlin

Einführung in die Mathematische Logik

Ein Lehrbuch

Zweite verbesserte und erweiterte Auflage

Satz und Layout: Der Autor
Fassung vom 27. Februar 2002

Vorwort

zur 2. Auflage

Nach der freundlichen Aufnahme der ersten Auflage wurde das Gesamtkonzept nicht verändert, der Text aber in allen Details gründlich überarbeitet. Wesentlich verändert und erweitert wurde Kapitel **7** über den zweiten Gödelschen Unvollständigkeitssatz und sein Umfeld. Der Beweis der Ableitungsbedingungen ist jetzt vollständig unabhängig von anderer Literatur. Auch das den ersten Unvollständigkeitssatz enthaltende Kapitel **6** wurde erweitert und neu organisiert.

Das Buch wendet sich an Studenten und Dozenten der Mathematik oder Informatik, und wegen der ausführlich diskutierten Gödelschen Unvollständigkeitssätze, die ja von hohem erkenntnistheoretischem Interesse sind, auch an Fachstudenten der Philosophischen Logik. Es enthält über den Stoff einer einsemestrigen Einführung in die Mathematische Logik hinaus auch das Basismaterial für eine Vorlesung *Logik für Informatiker* unter Einschluß der Grundlagen der Logik-Programmierung, in Kapitel **5** das Material für eine die Logik fortsetzende Vorlesung *Modelltheorie* und in Kapitel **6** für eine Vorlesung *Rekursionstheorie* mit Anwendungen auf Entscheidungsprobleme. Für eine gekürzte Einführungsvorlesung, z.B. kombiniert mit einer Einführung in die Mengenlehre, empfiehlt sich für den logischen Teil der Stoff der ersten drei, insgesamt rund 100 Seiten umfassenden Kapitel, die auch eine Diskussion des mengentheoretischen Axiomensystems ZFC einschließen. In Kapitel **3** wird nicht nur der Gödelsche Vollständigkeitssatz für Sprachen der ersten Stufe bewiesen, sondern auch der Birkhoffsche Vollständigkeitssatz. Die letzten Abschnitte diese Kapitels befassen sich vornehmlich mit Anwendungen der Vollständigkeit und haben teilweise beschreibenden Charakter, mit Ausblicken auf weitere Themen.

Das Buch kann ganz unabhängig von Vorlesungen aber auch zum Selbststudium genutzt werden. Nicht zuletzt deshalb wurden Stichwort- und Symbolverzeichnis recht ausführlich verfaßt und vor Beginn des Haupttextes ein Abschnitt *Notationen* eingefügt. Für den Großteil der Übungen gibt es Lösungshinweise in einem gesonderten Abschnitt am Ende des Buches. Außer einer hinreichenden Schulung im logischen Schließen sind spezielle Vorkenntnisse nicht erforderlich; lediglich für Teile von Kapitel **5** wären algebraische Grundkenntnisse nützlich, und für den allerletzten Abschnitt in Kapitel **7** gewisse Kenntnisse über Modelle der Mengenlehre.

Die Anforderungen an den Leser steigen allmählich ab Kapitel **4**. Diese meistert man am sichersten durch ein selbstständiges Lösen der Übungen, möglichst ohne die Lösungshinweise dabei zu Rate zu ziehen. Stil und Darstellung sind in den ersten drei Kapiteln breit genug gehalten, so daß auch der Student noch vor dem Einstieg in eine Spezialdisziplin den Stoff mühelos bewältigen kann.

Zwar verdichtet sich die Darstellung ab Kapitel **4**, jedoch nicht auf Kosten sprachlicher Präzision. Klarheit und angemessener Umgang mit Notationen bleiben oberstes Gebot. Der weniger erfahrene Leser wird allerdings nicht darauf verzichten können Bleistift und Papier parat zu haben um gewisse Dinge nachzurechnen.

Eine Besonderheit dieser Darstellung ist die eingehende Behandlung der Gödelschen Unvollständigkeitssätze. Diese beruhen auf der Repräsentierbarkeit rekursiver Prädikate in formalisierten Theorien, die in ihrer Urform den Hauptteil der Gödelschen Arbeit [Go2] ausmacht. Dieser Linie folgend gewinnt wir in Kapitel **6** den ersten Unvollständigkeitssatz, die Unentscheidbarkeit des Tautologieproblems der Logik nach Church und die Resultate über Nichtdefinierbarkeit des Wahrheitsbegriffs von Tarski in einem Zuge. Das letzte Kapitel ist ausschließlich dem zweiten Unvollständigkeitssatz und seinem Umfeld gewidmet. Von besonderem Interesse ist dabei, daß fragliche Behauptungen über selbstbezügliche Aussagen aufgrund der Solovayschen und weiterführender Vollständigkeitssätze algorithmisch entscheidbar sind. In den Abschnitten **7.3** bis **7.6** werden erstmals Ergebnisse in einem Lehrbuch systematisch behandelt, die über den zweiten Unvollständigkeitssatz hinausreichen.

Die Klassifikation definierender Formeln für arithmetische Prädikate wird recht frühzeitig, schon bei der Repräsentation rekursiver Prädikate in **6.3** eingeführt. Denn sie trägt in besonderem Maße dazu bei, den engen Zusammenhang zwischen Logik und Rekursionstheorie sichtbar zu machen, wie ihn die arithmetische Hierarchie in **6.7** oder Satz 6.4.5 zu Tage fördern. Weitere Unentscheidbarkeitsresultate über formalisierte Theorien werden in den Abschnitten **6.5** und **6.6** behandelt, einschließlich einer Skizze über die Lösung des 10. Hilbertschen Problems.

In Kapitel **4** werden berechenbare Funktionen in natürlicher Weise durch PROLOG-Programme präzisiert. Dies ist für Studierende der Informatik interessant, heißt dies doch einerseits, PROLOG ist eine universelle Programmiersprache, in der prinzipiell alle Algorithmen beschrieben werden können; andererseits werden durch den Nachweis der Unentscheidbarkeit des Existenzproblems erfolgreicher Resolutionen in **4.4** die prinzipiellen Schwierigkeiten erklärt, die mit der Problemlösung durch Anfragen an Logik-Programme zusammenhängen. Kapitel **4** muß in einer Vorlesung Logik für Informatiker mit Abschnitt **6.1** über Grundbegriffe der traditionellen Rekursionstheorie natürlich in Zusammenhang gebracht werden.

Kapitel **5** behandelt die Grundlagen der erst um 1950 entstandenen und inzwischen weit gefächerten Modelltheorie. Hier werden in der mathematischen Logik entwickelte Techniken mit Konstruktionstechniken anderer Gebiete zum gegenseitigen Nutzen miteinander verbunden. Durch den Einsatz weitreichender Methoden gelingt es, klassische Resultate wie die Eliminierbarkeit der Quantoren in der Theorie des reellen und der des komplexen Zahlenkörpers recht schnell zu gewinnen.

Trotz seiner Themenvielfalt umfaßt dieses Buch bei weitem nicht alles was die Mathematische Logik vorzuweisen hat. Lehrbücher mit enzyklopädischem Anspruch lassen sich heute selbst für deren Teilgebiete nicht mehr verfassen. Bei der Stoffauswahl können bestenfalls Akzente gesetzt werden. Das bezieht sich vor allem auf die über elementare Dinge hinausführenden Kapitel **4**, **5**, **6** und **7**. Die Auswahl orientiert sich durchweg an Grundergebnissen der Mathematischen Logik, die mit hoher Wahrscheinlichkeit von bleibendem Bestand sind.

Wo immer dies gelang, wurden in der Literatur vorliegende Beweise vereinfacht. Philosophische und grundlagentheoretische Probleme der Mathematik ebenso wie rein beweistheoretische Aspekte werden nicht systematisch behandelt, aber diesbezügliche Fragen werden an geeigneten Stellen im Text angeschnitten, vor allem im Zusammenhang mit den Gödelschen Sätzen.

Bemerkungen im Kleindruck enthalten in der Regel weiterführende Informationen oder verweisen auf das Literaturverzeichnis, das angesichts der Literaturfülle nur eine Auswahl repräsentieren kann. Zitiert wird im Text einem maximal 4-buchstabigen Kürzel um den Textumfang in Grenzen zu halten.

Die sieben Kapitel des Buches sind in Abschnitte gegliedert. Eine Referenz wie z.B. **4.5** bedeutet Kapitel **4**, Abschnitt **5** und Satz 4.5 meint den Satz Nr. 5 im 4. Abschnitt eines gegebenen Kapitels. Bei Rückbezug auf diesen Satz in einem anderen Kapitel wird die Kapitelnummer hinzugefügt wie z.B. in Satz 6.4.5.

Was die Rechtschreibung angeht, so wurden sinnvolle Reformvorschläge wie die Liberalisierung der Komma-Regeln freudig aufgegriffen, nicht allerdings gewisse Worttrennungen und den Buchstaben ß betreffende Vorschriften, weil diese den Text nicht unerheblich verlängern. Damit hätte der Zeilen- und Seitenumbruch insgesamt neu organisiert werden müssen (ein professioneller Gebrauch von LaTeX bedeutet für textintegrierte Formeln immer auch eine Nachbearbeitung des ursprünglichen Zeilenumbruchs). Es gibt in diesem Buche keine Formeltrennungen im fließenden Text. Dies kommt nicht nur dem Schriftbild zugute sondern dient vor allem einem unbehinderten Informationsfluß.

Für hilfreiche Kritik danke ich zahlreichen Kollegen und Studenten; die Namensliste ist zu lang, um sie hier anzugeben. Besonderer Dank gilt L.D. Beklemishev, sowie dem durch einen tragischen Unfall zu früh aus dem Leben geschiedenen jungen Mathematiker und Informatiker Ullrich Fuchs, der mich sowohl bei der technischen Organisation als auch bei inhaltlichen Fragen wesentlich unterstützt hat. Dem Vieweg-Verlag bin ich für die gute Zusammenarbeit verbunden.

Berlin, im Februar 2002,

Wolfgang Rautenberg

Inhaltsverzeichnis

Notationen

In der mathematischen Logik herrscht die allen mathematischen Disziplinen gemeinsame vorwiegend mengentheoretisch geprägte Umgangssprache vor, deren Gebrauch aber nur wenig mehr voraussetzt als die Kenntnis der unten kurz resümierten mengentheoretischen Terminologie. Diese Umgangssprache heißt in der Logik oft die *Metasprache*, um sie von formalisierten Sprachen zu unterscheiden, die in diesem Zusammenhang als *Objektsprachen* bezeichnet werden und zu den Objekten der logischen Analyse gehören. Mit deren Hilfe werden z.B. Verfahrensweisen des logischen Schließens in der Gestalt von sogenannten *Logik-Kalkülen* formalisiert.

Fast alle verwendeten Notationen sind Standard. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ bezeichnen die Mengen der natürlichen Zahlen einschließlich 0, der ganzen, rationalen bzw. der reellen Zahlen. n, m, i, j, k bezeichnen immer natürliche Zahlen, solange nichts anderes gesagt wird. Daher werden Zusätze wie $n \in \mathbb{N}$ in der Regel unterlassen.

$M \cup N$, $M \cap N$ und $M \setminus N$ bezeichnen wie üblich *Vereinigung*, *Durchschnitt*, bzw. *Differenz* der Mengen M, N, und $\subseteq$ die *Inklusion*. $M \subset N$ steht für $M \subseteq N$ und $M \neq N$, wird aber nur benutzt, wenn der Umstand $M \neq N$ besonders betont werden soll. Ist M in einer Betrachtung fest und $N \subseteq M$, darf $M \setminus N$ auch mit $\setminus N$ (oder $\neg N$) bezeichnet werden. $\emptyset$ bezeichnet die *leere Menge*, $\mathfrak{P}M$ die *Potenzmenge* von M, die Menge aller ihrer Teilmengen. Will man hervorheben, dass die Elemente einer Menge F selbst wieder Mengen sind, heißt F auch eine *Mengenfamilie* oder ein *Mengensystem*. $\bigcup F$ bezeichnet die Vereinigung einer Mengenfamilie F, d.h. die Menge der Elemente, die in wenigstens einem $M \in F$ liegen, und $\bigcap F$ für $F \neq \emptyset$ den Durchschnitt von F, d.h. die Menge der zu allen $M \in F$ gehörenden Elemente. Ist $F = \{M_i \mid i \in I\}$, bezeichnet man $\bigcup F$ und $\bigcap F$ meist mit $\bigcup_{i \in I} M_i$ bzw. $\bigcap_{i \in I} M_i$.

Das *Kreuzprodukt* $M \times N$ ist die Menge aller geordneten Paare (a, b) mit $a \in M$ und $b \in N$. Eine *Relation* zwischen M und N ist eine Teilmenge von $M \times N$. Ist $f \subseteq M \times N$ und gibt es zu jedem $a \in M$ genau ein $b \in N$ mit $(a, b) \in f$, heißt f eine *Funktion* oder *Abbildung* von M nach N. Das durch a eindeutig bestimmte Element b mit $(a, b) \in f$ wird je nach Zusammenhang mit $f(a)$ oder fa oder auch a^f bezeichnet. Man nennt b den *Wert von f bei a* sowie $\mathit{ran}\, f = \{fx \mid x \in M\}$ das *Bild* von f, während $\mathit{dom}\, f = M$ der *Definitionsbereich* von f heißt[1)]. Falls lediglich $\mathit{dom}\, f \subseteq M$, heißt f eine *partielle Funktion* von M nach N. Sind $\mathit{dom}\, f = M$ und $N \supseteq \mathit{ran}\, f$ vorgegeben, spricht man oft kurz von der Funktion $f\colon M \to N$ (lies 'f M nach N'), und falls $f(x) = t(x)$ für einen Term t und alle $x \in M$, auch von $f\colon x \mapsto t(x)$.

[1)]Die Abkürzungen *dom* und *ran* kommen aus dem Englischen (von *domain* und *range*).

Die Funktion $f\colon M \to N$ heißt *injektiv*, wenn $fx = fy \;\Rightarrow\; x = y$, für alle $x, y \in M$. Für $M \subseteq N$ ist die *identische Abbildung* $id_M\colon x \mapsto x$ Beispiel einer Injektion. $f\colon M \to N$ heißt *surjektiv*, wenn $ran\, f$ ganz N ausfüllt, und *bijektiv*, wenn f injektiv und surjektiv ist. Sind f, g Abbildungen mit $ran\, g \subseteq dom\, f$, heißt die Funktion $h\colon x \mapsto f(g(x))$ auch deren *Produkt*, $h = f \circ g$. Man sieht leicht, dass $f\colon M \to N$ genau dann bijektiv ist, wenn es ein $g\colon N \to M$ gibt mit $g \circ f = id_M$ und $f \circ g = id_N$. Bei der Schreibweise x^f für fx ist es übrigens bequemer, $f \circ g$ so zu erklären, daß erst f, dann g ausgeführt wird.

Seien I, M beliebige Mengen, wobei I, ziemlich willkürlich, die *Indexmenge* genannt werde. M^I bezeichne die Menge aller $f\colon I \to M$. Oft wird eine Funktion $f \in M^I$ mit $i \mapsto a_i$ durch $(a_i)_{i \in I}$ bezeichnet und heißt, je nach dem Zusammenhang, eine (indizierte) *Familie*, ein *I-Tupel* oder eine *Folge*. Diese heißt *endlich* oder *unendlich*, je nachdem ob I endlich oder unendlich ist. Falls, wie in der Mengenlehre üblich, 0 mit $\emptyset$, und $n > 0$ mit $\{0, 1, \dots, n{-}1\}$ identifiziert wird, lässt M^n sich verstehen als die Menge der Folgen oder n-Tupel $(a_i)_{i<n}$ aus Elementen von M *der Länge n*. Einziges Element von M^0 $(= M^{\emptyset})$ ist die leere Folge $\emptyset$ und diese hat die Länge 0. Gleichwertige Schreibweise für $(a_i)_{i<n}$ bzw. $(a_i)_{i \leqslant n}$ sind $(a_0, \dots, a_{n-1})$ und $(a_0, \dots, a_n)$.

Für $k \leqslant n$ heißt $(a_0, \dots, a_k)$ ein *Anfang* von $(a_i)_{i \leqslant n}$. Ein Anfang ist stets nichtleer. Ist $k < n$, spricht man von einem *echten* Anfang. Häufig betrachten wir auch Folgen der Gestalt $(a_1, \dots, a_n)$, im Text durchweg mit $\vec{a}$ bezeichnet. Hier ist für $n = 0$ die leere Folge gemeint, so wie $\{a_1, \dots, a_n\}$ dann stets die leere Menge bedeutet.

Das Aneinanderfügen endlicher Folgen heißt auch deren *Verkettung*. Die leere Folge spielt die Rolle des neutralen Elements dieser Operation. Ist A ein *Alphabet*, d.h. sind die Elemente von A *Symbole* oder werden sie als solche bezeichnet, wird $(a_1, \dots, a_n)$ meistens in der Weise $a_1 \cdots a_n$ geschrieben und heißt ein *Wort* oder eine *Zeichenfolge* über A. Die leere Folge wird dann konsequenterweise das *leere Wort* genannt. Ein Anfang einer Zeichenfolge ξ heißt auch ein *Anfangswort* von ξ.

Teilmengen $P, Q, R, \ldots \subseteq M^n$ heißen *n-stellige Prädikate* oder *Relationen* von M, $n \geqslant 1$. Einstellige Prädikate werden mit den entsprechenden Teilmengen von M identifiziert, z.B. das Primzahlprädikat mit der Menge aller Primzahlen. Statt $\vec{a} \in P$ schreiben wir $P\vec{a}$, statt $\vec{a} \notin P$ auch $\neg P\vec{a}$. Falls $P \subseteq M^2$ und P ein Symbol ist wie z.B. $\lhd, <, \leqslant, \in$, wird aPb statt Pab geschrieben, also $a \lhd b$ statt $\lhd\, ab$ usw. In Worten formulierte Prädikate werden oft durch '. . .' vom umgebenden Text abgehoben, etwa wenn vom syntaktischen Prädikat 'Die Variable x kommt in der Formel α vor' die Rede ist. Für $P \subseteq M^n$ heiße die durch

$$\chi_P \vec{a} = \begin{cases} 1 & \text{falls } P\vec{a}, \\ 0 & \text{falls } \neg P\vec{a} \end{cases}$$

definierte n-stellige Funktion χ_P die *charakteristische Funktion* von P. Dabei ist unerheblich, ob man die Werte $0, 1$ als Wahrheitswerte oder als natürliche Zahlen versteht wie dies in Kaptitel **6** geschieht, oder ob $0, 1$ in der Definition gar vertauscht werden. Wichtig ist nur, dass P durch χ_P eindeutig bestimmt ist.

Jedes $f\colon M^n \to M$ heißt eine n-stellige *Operation von M*. Meistens schreiben wir $f\vec{a}$ für $f(a_1, \ldots, a_n)$. Eine 0-stellige Operation von M hat wegen $A^0 = \{\emptyset\}$ mengentheoretisch die Gestalt $\{(\emptyset, c)\}$ mit $c \in M$, wird kurz mit c bezeichnet und heißt eine *Konstante*. Jede n-stellige Operation von f von M wird durch

$$\mathit{graph}\, f := \{(a_1, \ldots, a_{n+1}) \in M^{n+1} \mid f(a_1, \ldots, a_n) = a_{n+1}\}$$

eindeutig beschrieben. Es handelt sich hier um eine $(n+1)$-stellige Relation, welche der *Graph von f* genannt wird. f und $\mathit{graph}\, f$ sind dasselbe, wenn – wie dies gelegentlich geschieht – M^{n+1} mit $M^n \times M$ identifiziert wird. Für die von uns verfolgten Zwecke ist es jedoch vorteilhafter, zwischen f und $\mathit{graph}\, f$ zu unterscheiden.

Am häufigsten werden 2-stellige Operationen angetroffen. Bei diesen wird das entsprechende Operationssymbol in der Regel zwischen die Argumente gesetzt. Eine derartige, hier mit $\circ$ bezeichnete Operation $\circ : M^2 \to M$ heißt

kommutativ	wenn $a \circ b = b \circ a$ für alle $a, b \in M$,
assoziativ	wenn $a \circ (b \circ c) = (a \circ b) \circ c$ für alle $a, b, c \in M$,
idempotent	wenn $a \circ a = a$ für alle $a \in M$,
invertierbar	wenn zu allen $a, b \in M$ Elemente $x, y \in M$ existieren mit $x \circ a = b$ und $a \circ y = b$.

Man beachte, Invertierbarkeit umfaßt genau besehen zwei voneinander unabhängige Forderungen, die sogenannte *Linksinvertierbarkeit* und die *Rechtsinvertierbarkeit*

Als Verallgemeinerung von $M_1 \times M_2$ lässt sich das *direkte Produkt* $N = \prod_{i \in I} M_i$ einer Mengenfamilie $(M_i)_{i \in I}$ verstehen. Jedes $a \in N$ ist eine auf I erklärte Funktion $a = (a_i)_{i \in I}$ mit $a_i \in M_i$ (eine *Auswahlfunktion*). Die Abbildung $a \mapsto a_i$ von N nach M_i heißt *die i-te Projektion*. Das Element a_i heißt auch die *i-te Komponente* von a. Falls $M_i = M$ für alle $i \in I$, ist $\prod_{i \in I} M_i$ mit M^I identisch. Dies gilt auch für $I = \emptyset$, weil dann $\prod_{i \in I} M_i = \{\emptyset\} = M^I$.

Bezeichnen A, B metasprachliche Ausdrücke, stehen $A \Leftrightarrow B$, $A \Rightarrow B$, $A \,\&\, B$ und $A \vee B$ für *A genau dann wenn B*, *wenn A so B*, *A und B* bzw. *A oder B*. Dabei sollen die Symbole $\Rightarrow$, $\Leftrightarrow, \ldots$ stärker trennen als sprachliche Bindungspartikel. Deshalb darf in einem Textteil wie z.B.

$$T \vDash \alpha \;\Leftrightarrow\; \alpha \in T, \text{ für alle } \alpha \in \mathcal{L}^0 \quad \text{(Seite 64)}$$

das Komma nicht fehlen, weil '$\alpha \in T$ für alle $\alpha \in \mathcal{L}^0$' fälschlicherweise gelesen werden könnte als 'T ist inkonsistent'.

Sind s, t Terme mit Werten in einer geordneten Menge, sei $s > t$ grundsätzlich nur eine andere Schreibweise für $t < s$. Dieselbe Bemerkung bezieht sich auch auf andere unsymmetrische Relationssymbole wie $\leqslant$, $\subseteq$, $\subset$ usw. Terme sind grob gesagt Zeichenfolgen, die aus Variablen und Operationssymbolen zusammengebaut sind. Wie dies im einzelnen geschieht, wird in **2.2** ausführlich dargelegt.

$s := t$ bedeutet, dass s durch den Term t definiert wird, oder wenn s eine Variable ist, auch die Zuweisung des Wertes von t zu s.

In der mathematischen Umgangssprache werden Formeln oft direkt in den Text integriert und man bedient sich dabei auch gewisser verkürzender Schreibweisen. So wie man z.B. '$a < b$ und $b < c$' häufig zu $a < b < c$, oder '$a < b$ und $b \in M$' zu $a < b \in M$ verkürzt, darf $X \vdash \alpha \equiv \beta$ für '$X \vdash \alpha$ und $\alpha \equiv \beta$' geschrieben werden ('aus der Formelmenge X ist die Formel α beweisbar und α ist äquivalent zu β'). Dies ist erlaubt, solange das Symbol $\equiv$ nicht zur formalen Sprache gehört, aus der die Formeln α, β stammen. $\equiv$ wird von uns nur metasprachlich verwendet.

In einem Lehrbuch wie diesem kommt man nicht umhin, das in der Metasprache verwendete Gleichheitszeichen $=$ deutlich zu unterscheiden von einem in einer formalen Sprache vorkommenden Gleichheitszeichen. Das geschieht im Buchtext durchweg durch Fettdruck des Gleichheitszeichens in der formalen Sprache. Ist dies z.B. die Sprache der Arithmetik, wird

$$(x+y)^2 \boldsymbol{=} x^2 + 2xy + y^2 \text{ anstelle von } (x+y)^2 = x^2 + 2xy + y^2$$

geschrieben um die Wertverlaufsgleichheit der Terme links und rechts vom Gleichheitszeichen zu kennzeichnen. Hingegen soll $s = t$ ausnahmslos bedeuten, daß die beiden Terme s, t syntaktisch übereinstimmen, Buchstabe für Buchstabe.

Kapitel 6

Unvollständigkeit und Unentscheidbarkeit

Die fundamentalen Resultate von Gödel über Unvollständigkeit genügend reichhaltiger formaler Systeme sowie von Tarski über Nichtdefinierbarkeit des Wahrheitsbegriffs und von Church über die Unentscheidbarkeit der Logik und andere Unentscheidbarkeitsresultate beruhen sämtlich auf gewissen Diagonalargumenten. Eine bekannte Popularisierung des 1. Gödelschen Unvollständigkeitssatzes ist diese:

Man betrachte eine formalisierte axiomatische Theorie T, die im Rahmen der T zugrundeliegenden Sprache $\mathcal{L}$ über deren Syntax und das Beweisen aus den Axiomen von T zu reden imstande ist. Dies ist häufig auch dann möglich, wenn in T offiziell von anderen Dingen die Rede ist (etwa von Zahlen oder Mengen), nämlich vermittels einer internen Kodierung der Syntax von $\mathcal{L}$, siehe **6.2**. Dann gehört zu $\mathcal{L}$ – was für einen formalen Begriff von Beweisbarkeit im einzelnen zu begründen ist – auch die Aussage γ: „Ich bin in T unbeweisbar“, wobei sich das *Ich* genau auf die Aussage γ selbst bezieht. Nehmen wir weiter an, T soll einen gewissen Gegenstandsbereich $\mathcal{A}$ korrekt und möglichst vollständig beschreiben, und alle Aussagen von T haben in $\mathcal{A}$ einen adäquaten Sinn. *Dann ist γ in $\mathcal{A}$ wahr, in T aber unbeweisbar.*

In der Tat, wäre γ beweisbar, so wäre γ wie jede in T beweisbare Aussage auch wahr in $\mathcal{A}$ und damit aber unbeweisbar, weil γ genau dies behauptet. Die Annahme führt zum Widerspruch. Also ist γ in T tatsächlich unbeweisbar und damit zugleich wahr in $\mathcal{A}$, weil die Behauptung von γ ja zutrifft. Das Ziel, die in $\mathcal{A}$ gültigen Sätze durch T vollständig zu erfassen, ist also nicht erreicht.

Das ist natürlich nur eine grob vereinfachte Beschreibung des 1. Unvollständigkeitssatzes, der über Gegenstandsbereiche gar nicht redet, sondern ein *beweistheoretischer* Satz ist, dessen Beweis im Rahmen der finiten Metamathematik Hilberts ausführbar ist, was grob gesagt dasselbe bedeutet wie die Ausführbarkeit des Beweises in

PA. Dies war ein entscheidender Punkt für eine begründete Kritik am *Hilbertschen Programm*, das auf eine durchgehend finite Formulierung der Metamathematik zur Rechtfertigung infinitistischer Methoden abzielte, siehe hierzu [HB].

Paradigma eines Gegenstandsbereichs im anfänglich erwähnten Sinne ist aus verschiedenen Gründen die Struktur $\mathcal{N} = (\mathbb{N}, 0, \mathtt{S}, +, \cdot)$. Der 1. Unvollständigkeitssatz besagt, daß eine vollständige axiomatische Charakterisierung von $\mathcal{N}$ unmöglich ist. Das ist eine Erkenntnis mit weitreichenden Konsequenzen. Insbesondere erweist sich die Peano-Arithmetik PA als unvollständig. Diese Theorie steht im Mittelpunkt von Kapitel **7**. Sie ist deshalb besonders wichtig, weil in ihr nebst der klassischen Zahlentheorie und weiten Teilen der diskreten Mathematik ziemlich genau diejenigen Hilfsmittel der mathematischen Grundlagenforschung formulierbar und beweisbar sind, die nach allgemeiner Ansicht jeder Kritik standhalten, sieht man von gewissen Einwänden gegen den uneingeschränkten Gebrauch 2-wertiger Logik ab.

Für wesentliche Schritte im Gödelschen Beweis benötigt man nur bescheidene Voraussetzungen über T, nämlich die ziffernweise Repräsentierbarkeit der relevanten syntaktischen Prädikate und Funktionen in T im Sinne von **6.3**. Es war eine der entscheidenden Entdeckungen Gödels, daß alle zur Konstruktion von γ erforderlichen Prädikate primitiv-rekursiv sind [1)] und *alle* derartigen Prädikate und Funktionen unter ziemlich allgemeinen Voraussetzungen in T repräsentierbar sind.

Wie von Tarski und Mostowski bemerkt, funktioniert dies bereits in gewissen endlich axiomatisierbaren, hochgradig unvollständigen Theorien T. Die in **6.4** ausführlich bewiesene Repräsentierbarkeit aller rekursiven Funktionen ergibt – wieder durch ein Diagonalargument – leicht die rekursive Unentscheidbarkeit von T und sämtlicher Teiltheorien, insbesondere der Theorie $\mathit{Taut}_{\mathcal{L}}$ aller tautologischen Aussagen von $\mathcal{L}$, sowie aller konsistenten Erweiterungstheorien von T. Daher lassen sich der erste Unvollständigkeitssatz und die Resultate von Church und Tarski einheitlich gewinnen, und zwar im wesentlichen durch das Fixpunktlemma in **6.5**.

In **6.1** wird die Theorie der rekursiven und primitiv-rekursiven Funktionen im erforderlichen Maße entwickelt. **6.2** behandelt die Gödelisierung der Syntax und des Beweisens. **6.3** und **6.4** befassen sich mit der Repräsentierbarkeit rekursiver Funktionen. In **6.5** werden alle oben erwähnten Resultate bewiesen, während der tieferliegende zweite Unvollständigkeitssatz in Kapitel **7** behandelt wird. **6.6** befaßt sich mit der Übertragbarkeit von Entscheidbarkeit und Unentscheidbarkeit durch Interpretation, und **6.7** mit der arithmetischen Hierarchie der 1. Stufe, die den engen Zusammenhang zwischen Logik und Rekursionstheorie plastisch verdeutlicht.

[1)] Alle diese Prädikate sind bereits elementar im Sinne der Rekursionstheorie, siehe etwa [Mo]. Doch erfordert dieser Nachweis mehr Aufwand. Die elementaren sind grob gesagt die nicht zu schnell wachsenden primitiv rekursiven Funktionen. Die Exponentialfunktion $(m, n) \mapsto m^n$ ist noch elementar, nicht aber die auf Seite 186 definierte Hyper-Exponentialfunktion.

6.1 Rekursive und primitiv-rekursive Funktionen

Im folgenden bezeichnen nebst $i, \dots, n$ auch $a, \dots, e$ durchweg natürliche Zahlen. Die Menge aller n-stelligen Funktionen mit Argumenten und Werten aus $\mathbb{N}$ werde mit $\mathbf{F}_n$ bezeichnet. $\mathbf{F}_0$ besteht aus allen Konstanten. Sind $h \in \mathbf{F}_m$ und $g_1, \dots, g_m \in \mathbf{F}_n$, so heiße $f : \vec{a} \mapsto h(g_1\vec{a}, \dots, g_m\vec{a})$ die durch *Komposition* aus h und den g_i entstehende Funktion, Schreibweise: $f = h[g_1, \dots, g_m]$. Die Stellenzahl von f ist n. Analog sei $P[g_1, \dots, g_m]$ für $P \subseteq \mathbb{N}^m$ das n-stellige Prädikat $\{\vec{a} \in \mathbb{N}^n \mid P(g_1\vec{a}, \dots, g_m\vec{a})\}$.

$f \in \mathbf{F}_n$ ist im intuitiven Sinne berechenbar, wenn es einen Algorithmus gibt, der zu jedem $\vec{a} \in \mathbb{N}^n$ den Wert $f\vec{a}$ in endlich vielen Schritten zu berechnen gestattet. Einfache Beispiele sind Summe und Produkt. Es gibt überabzählbar viele einstellige Funktionen über $\mathbb{N}$; davon können wegen der Endlichkeit einer jeden Berechnungsvorschrift nur abzählbar viele berechenbar sein. Folglich gibt es nicht berechenbare Funktionen. Dieser Existenzbeweis erinnert an denjenigen transzendenter reeller Zahlen, wie ihn die Abzählbarkeit aller algebraischen Zahlen liefert. Konkrete Beispiele anzugeben ist in dem einen wie dem anderen Falle weniger einfach.

Die im intuitiven Sinne berechenbaren Funktionen haben ganz offensichtlich die Eigenschaften

Oc : Mit $h \in \mathbf{F}_m$ und $g_1, \dots, g_m \in \mathbf{F}_n$ ist auch $f = h[g_1, \dots, g_m]$ berechenbar.

Op : Sind $g \in \mathbf{F}_n$ und $h \in \mathbf{F}_{n+2}$ berechenbar, so auch $f \in \mathbf{F}_{n+1}$, bestimmt durch

$$f(\vec{a}, 0) = g\vec{a} \quad \text{und} \quad f(\vec{a}, \mathtt{S}b) = h(\vec{a}, b, f(\vec{a}, b)).$$

f heißt die *aus g, h durch primitive Rekursion entstehende* Funktion und werde auch als $f = \boldsymbol{Op}(g, h)$ notiert.

Oμ : Ist $g \in \mathbf{F}_{n+1}$ und gilt $\forall\vec{a}\,\exists b\, g(\vec{a}, b) = 0$, so ist mit g auch f berechenbar, wobei $f\vec{a} = \mu b[g(\vec{a}, b) = 0]$ (das kleinste b mit $g(\vec{a}, b) = 0$), die *μ-Operation.*

Wir betrachten nun ***Oc***, ***Op*** und ***Oμ*** als Erzeugungsoperationen zur Gewinnung neuer Funktionen und beginnen mit der folgenden auf S. Kleene zurückgehenden

Definition. Die Menge der p.r. (*primitiv-rekursiven*) Funktionen bestehe aus allen Funktionen über $\mathbb{N}$, die sich mittels ***Oc*** und ***Op*** erzeugen lassen aus folgenden

Anfangsfunktionen: die Konstante 0, die Nachfolgerfunktion $\mathtt{S}$ und die Projektionsfunktionen $\mathrm{I}^n_\nu : \vec{a} \mapsto a_\nu$ $(1 \leqslant \nu \leqslant n,\ n = 1, 2, \dots)$.

Mit dem zusätzlichen Erzeugungsschema ***Oμ*** erhält man die Menge aller *rekursiven* oder *μ-rekursiven* Funktionen. $P \subseteq \mathbb{N}^n$ heißt p.r. bzw. *rekursiv* (oder *entscheibar*), wenn die charakteristische Funktion χ_P p.r. bzw. rekursiv ist.

Bemerkung 1. Nach dem Dedekindschen Rekursionssatz (siehe z.B. [Ra2]) wird durch ***Op*** genau eine Funktion $f \in \mathbf{F}_{n+1}$ definiert. Man beachte, für $n = 0$ reduzieren sich diese Gleichungen auf $f0 = c$ und $fSb = h(b, fb)$, mit $c \in \mathbf{F}_0$ und $h \in \mathbf{F}_2$. Läßt man in $\boldsymbol{O\mu}$ die Bedingung $\forall\vec{a}\,\exists b\, g(\vec{a}, b) = 0$ weg, sagt man gelegentlich auch, f sei an allen Stellen $\vec{a}$ mit $\neg\exists b\, g(\vec{a}, b) = 0$ nicht definiert. Man gelangt so zu den sogenannten partiell-rekursiven Funktionen, die wir aber nicht benötigen werden.

Die folgenden Beispiele verdeutlichen, daß sich mittels der I^n_ν die normierten Stellenzahlvorschriften in ***Oc*** und ***Op*** weitgehend liberalisieren lassen. Eine normgerechte Niederschrift wird hierbei zunächst noch in Klammern hinzugesetzt.

Beispiele. Sei $\mathtt{S}^0 = \mathrm{I}^1_1$ und $\mathtt{S}^{k+1} = \mathtt{S}[\mathtt{S}^k]$, so daß offenbar $\mathtt{S}^k\colon a \mapsto a + k$. Diese einstelligen Funktionen sind nach ***Oc*** alle p.r. Die n-stelligen *konstanten Funktionen* $\mathrm{K}^n_c\colon \vec{a} \mapsto c$ erweisen sich wie folgt als primitiv rekursiv: $\mathrm{K}^0_0 = 0$, $\mathrm{K}^0_c = \mathtt{S}^c[0]$, sowie $\mathrm{K}^1_c 0 = c$ $(= \mathrm{K}^0_c)$ und $\mathrm{K}^1_c\mathtt{S}b = c$ $(= \mathrm{I}^2_2(b, \mathrm{K}^1_c b)\,)$. Für $n > 1$ hat man $\mathrm{K}^n_c = \mathrm{K}^1_c[\mathrm{I}^n_1]$. Also sind sämtliche konstanten Funktionen p.r. Ferner bestimmen

$$a + 0 = a \ \big(= \mathrm{I}^1_1(a)\big), \quad a + \mathtt{S}b = \mathtt{S}(a + b)\ \big(= \mathtt{S}\mathrm{I}^3_3(a, b, a + b)\big)$$

die Addition als p.r. Funktion. Durch $a \cdot 0 = 0$ $(= \mathrm{K}^1_0 a)$ sowie $a \cdot \mathtt{S}b = a \cdot b + a$ $(= \mathrm{I}^3_3(a, b, a \cdot b) + \mathrm{I}^3_1(a, b, a \cdot b)\,)$ gewinnt man $\cdot$ als p.r. Funktion und völlig analog auch $(a, b) \mapsto a^b$. Ferner ist die Vorgängerfunktion $\mathtt{R}$ p.r. Denn

$$\mathtt{R}0 = 0 \quad ; \quad \mathtt{R}(\mathtt{S}b) = b\ \big(= \mathrm{I}^2_1(b, \mathtt{R}b)\big).$$

Die „gestutzte Subtraktion“ $\dot{-}$, definiert durch $a \dot{-} b = a - b$ für $a \geqslant b$ und $a \dot{-} b = 0$ sonst, ist p.r. Denn $a \dot{-} 0 = a$ und $a \dot{-} \mathtt{S}b = \mathtt{R}(a \dot{-} b)$ $\big(= \mathtt{R}\mathrm{I}^3_3(a, b, a \dot{-} b)\big)$. Damit ist die absolute Differenz p.r. Denn $|a - b| = (a \dot{-} b) + (b \dot{-} a)$.

Man sieht leicht, daß mit jeder Funktion f auch jede Funktion p.r. bzw. rekursiv ist, die aus f durch Vertauschung, Gleichsetzung oder Hinzufügen von fiktiven Argumenten hervorgeht. Sei z.B. $f \in \mathbf{F}_2$. Für $g = f[\mathrm{I}^2_2, \mathrm{I}^2_1]$ ist dann $g(a, b) = f(b, a)$. Für $h = f[\mathrm{I}^1_1, \mathrm{I}^1_1]$ ist $ha = f(a, a)$, und für $f' = f[\mathrm{I}^3_1, \mathrm{I}^3_2]$ ist $f'(a, b, c) = f(a, b)$.

Ab jetzt sind wir großzügiger bei den Niederschriften der Anwendungen von ***Oc*** und ***Op***. Mit $f \in \mathbf{F}_{n+1}$ ist auch $(\vec{a}, b) \mapsto \prod_{k<b} f(\vec{a}, k)$ p.r., definiert durch

$$\textstyle\prod_{k<0} f(\vec{a}, k) = 1 \quad ; \quad \prod_{k<\mathtt{S}b} f(\vec{a}, k) = (\prod_{k<b} f(\vec{a}, k)) \cdot f(\vec{a}, b).$$

Analoges gilt für $(\vec{a}, b) \mapsto \sum_{k<b} f(\vec{a}, k)$, mit der Startbedingung $\sum_{k<0} f(\vec{a}, k) = 0$.

Durch $\delta 0 = 1$ und $\delta\mathtt{S}n = 0$ wird die *δ-Funktion* definiert, die charakteristische Funktion der Einermenge $\{0\}$. Damit erkennt man z.B. die Identitätsrelation leicht als p.r. Offenbar ist $\chi_=(a, b) = \delta|a - b|$. Das wiederum impliziert, daß jede endliche Teilmenge $E = \{a_1, \ldots, a_n\}$ von $\mathbb{N}$ p.r. ist. Denn

$$\chi_E(a) \ = \ \chi_=(a, a_1) + \ldots + \chi_=(a, a_n).$$

$\neq$ ist p.r. weil $\chi_{\neq}(a,b) = \sigma|a{-}b|$ mit der *Signumfunktion* σ, definiert durch $\sigma 0 = 0$, $\sigma \mathsf{S} n = 1$. Das ergibt auch die Abgeschlossenheit der p.r. bzw. der rekursiven Funktionen gegenüber *Definition durch* p.r. (bzw. *rekursive) Fallunterscheidung*: Mit P, g, h ist auch f p.r. (bzw. rekursiv), definiert durch $f\vec{a} = g\vec{a} \cdot \chi_P \vec{a} + h\vec{a} \cdot \delta(\chi_P \vec{a})$. Diese Gleichung läßt sich auch schreiben in der Weise

$$f\vec{a} = \begin{cases} g\vec{a}, & \text{falls } P\vec{a}, \\ h\vec{a}, & \text{falls } \neg P\vec{a}. \end{cases}$$

Auch weitere Standardfunktionen sind p.r., darunter $n \mapsto n!$ und die *Primzahlaufzählung* $n \mapsto p_n$ (mit $p_0 = 2,\ p_1 = 3, \dots$). Gleiches gilt für Prädikate wie $\mathsf{|}$ (teilt), prim (Primzahl sein), usw. Siehe hierzu (B) und (C) unten sowie die Übungen. Wir vermerken, mit f ist auch *graph* f p.r. weil $\chi_{\mathit{graph}\,f}(\vec{a}, b)$ mit $\chi_{=}(f\vec{a}, b)$ offenbar übereinstimmt. Die Umkehrung hiervon gilt i.a. nicht, siehe hierzu Übung 1.

Von grundlegender Bedeutung, speziell für die Gewinnung von Unentscheidbarkeitsresultaten, ist die Hypothese, daß die rekursiven Funktionen alle irgendwie berechenbaren Funktionen über $\mathbb{N}$ bereits ausschöpfen, die sogenannte *Churchsche These*. Der Definition rekursiver Funktionen ist dies kaum anzusehen, aber alle auf unterschiedliche Weise definierten Berechenbarkeitskonzepte erweisen sich als äquivalent und stützen damit die These. Für einige dieser oft langwierigen Beweise sei auf [Ob] verwiesen. Ein solches Konzept ist z.B. die Berechenbarkeit mittels einer *Turing-Maschine*, eines besonders einfachen Modells von strikt mechanischer Informationsverarbeitung. Gödels Resultate sind von Churchs These unabhängig. Sie haben eher umgekehrt die Entwicklung der Rekursionstheorie beeinflußt und beschleunigt.

Es folgt eine Zusammenstellung leicht beweisbarer Grundfakten über primitiv und allgemein rekursive Prädikate („allgemein“ akzentuiert hier nur den Unterschied zu „primitiv“). Weitere Einsichten, vor allem über die Gestalt definierender Formeln werden sich ab **6.3** ergeben. P, Q, R bezeichnen jetzt ausschließlich Prädikate über $\mathbb{N}$. Um die formale Niederschrift von metasprachlich formulierten Eigenschaften solcher Prädikate zu erleichtern, benutzen wir als weitere metasprachliche Abkürzungen die Präfixe $(\exists k{<}a)$, $(\exists k{\leqslant}a)$, $(\forall k{<}a)$ und $(\forall k{\leqslant}a)$, deren Sinn sich von selbst erklärt.

(A) Die Menge der p.r. bzw. rekursiven Prädikate ist abgeschlossen gegenüber Komplementbildung, Vereinigung und Durchschnitt von Prädikaten derselben Stellenzahl und gegenüber Einsetzung p.r. bzw. rekursiver Funktionen sowie gegenüber Gleichsetzung, Vertauschung und Hinzufügung von fiktiven Argumenten.

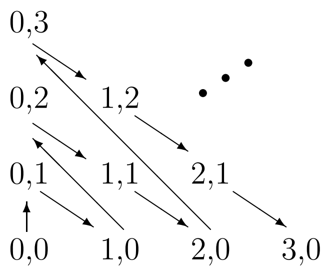
Das ergibt sich wie folgt: Für $P \subseteq \mathbb{N}^n$ ist $\delta[\chi_P]$ gerade die charakteristische Funktion von $\neg P = \mathbb{N}^n \setminus P$; ferner ist $\chi_{P \cap Q} = \chi_P \cdot \chi_Q$ und $\chi_{P \cup Q} = \mathrm{sg}[\chi_P + \chi_Q]$ sowie $\chi_{P[g_1,\dots,g_m]} = \chi_P[g_1, \dots, g_m]$. Die übrigen Abgeschlossenheitseigenschaften ergeben sich einfach aus entsprechenden Eigenschaften der charakteristischen Funktionen.

(B) Seien $P, Q, \ldots \subseteq \mathbb{N}^{n+1}$. Ist $Q(\vec{a}, b) \Leftrightarrow (\forall k{<}b)P(\vec{a}, k)$, $R(\vec{a}, b) \Leftrightarrow (\exists k{<}b)P(\vec{a}, k)$, $Q'(\vec{a}, b) \Leftrightarrow (\forall k{\leqslant}b)P(\vec{a}, k)$ und $R'(\vec{a}, b) \Leftrightarrow (\exists k{\leqslant}b)P(\vec{a}, k)$ sagt man, Q, R, Q', R' entstünden aus P durch *beschränkte Quantifizierung*. Mit P sind alle diese Prädikate p.r. So ist $\chi_Q(\vec{a}, b) = \prod_{k<b} \chi_P(\vec{a}, k)$ und $\chi_R(\vec{a}, b) = \mathrm{sg}(\sum_{k<b} \chi_P(\vec{a}, k))$. Die Beweise dieser Gleichungen sind so einfach, daß wir sie ganz übergehen können. Kurzum, die Menge der p.r. bzw. der rekursiven Prädikate ist abgeschlossen gegenüber beschränkter Quantifizierung. Weil z.B. $a \,|\, b \Leftrightarrow (\exists k{\leqslant}b)[a \cdot k = b]$, erweist sich das Prädikat $|$ als p.r. Auch prim ist wegen $\mathsf{prim}\, p \Leftrightarrow p \neq 0, 1 \;\&\; (\forall k < p)[k \,|\, p \Rightarrow k = 1]$ p.r. Man beachte, $a \,|\, p \Rightarrow a = 1$ ist gleichwertig zu $a \nmid p \vee a = 1$ und als Vereinigung p.r. Prädikate wieder p.r.

(C) $P \subseteq \mathbb{N}^{n+1}$ erfülle $\forall \vec{a}\, \exists m\, P(\vec{a}, m)$. Ist $f(\vec{a}) = \mu k[P(\vec{a}, k)]$ das kleinste k mit $P(\vec{a}, k)$, so ist nach $\boldsymbol{O\mu}$ mit P auch f rekursiv, denn $f\vec{a} = \mu k[\delta\chi_P(\vec{a}, k) = 0]$; doch ist f in der Regel nicht mehr p.r. Das gilt aber noch für die *beschränkte μ-Operation*: Mit $P \subseteq \mathbb{N}^{n+1}$ ist auch $f\colon (\vec{a}, m) \mapsto \mu k{\leqslant}m[P(\vec{a}, k)]$ p.r. Dabei sei

$$\mu k{\leqslant}m[P(\vec{a}, k)] = \begin{cases} \text{kleinstes } k \leqslant m \text{ mit } P(\vec{a}, k), \text{ falls ein solches } k \text{ existiert,} \\ m \quad \text{sonst.} \end{cases}$$

Offenbar ist $f(\vec{a}, 0) = 0$, sowie $f(\vec{a}, \mathtt{S}m) = f(\vec{a}, m)$ falls $(\exists k{\leqslant}m)P(\vec{a}, k)$, und sonst ist $f(\vec{a}, \mathtt{S}m) = \mathtt{S}m$, was eine p.r. Fallunterscheidung darstellt. Also ist f p.r.



Durch Einsetzung einer p.r. Funktion h für m erkennt man leicht auch $\vec{a} \mapsto \mu k{\leqslant}h\vec{a}[P(\vec{a}, k)]$ als p.r. Eine nützliche Anwendung ist die *Paarkodierung* $\wp$, die $\mathbb{N}^2$ bijektiv auf $\mathbb{N}$ abbildet (Übung 3), und zwar gemäß der in der Figur gezeigten Abzählung der Zahlenpaare a, b. Es ist $\wp(a, b) = a + \frac{1}{2}(a + b)(a + b + 1)$. Eine Darstellung mit Hilfe der beschränkten μ-Operation erhalten wir in $\wp(a, b) = \mu k{\leqslant}(a + b + 1)^2\, [2k = 2a + (a + b)(a + b + 1)]$. Man erkennt aber auch auf andere Weise, daß $\wp$ p.r. ist. Denn nach einer bekannten Summationsformel ist $\wp(a, b) = a + \sum_{i \leqslant a+b} i$. Eine weitere Anwendung ist diese: Sei $\mathrm{kgV}\{a_\nu | \nu{\leqslant}n\}$ das kleinste gemeinsame Vielfache von $a_0, \ldots, a_n$. Dann ist mit f auch $n \mapsto \mathrm{kgV}\{f\nu | \nu{\leqslant}n\}$ p.r. Denn $\mathrm{kgV}\{f\nu | \nu{\leqslant}n\} = \mu k{\leqslant} \prod_{\nu \leqslant n} f\nu[(\forall \nu{\leqslant}n) f\nu \,|\, k]$.

Noch eine weitere Anwendung. Ist p Primzahl, so ist $p! + 1$ gewiß durch keine Primzahl $q \leqslant p$ teilbar; denn $q \,|\, p!{+}1$ und $q \,|\, p!$ liefern den Widerspruch $q \,|\, 1$. Ein Primteiler von $p! + 1$ ist mithin eine neue Primzahl und die kleinste auf p folgende Primzahl ist $\leqslant p! + 1$. Also ist die Funktion $n \mapsto p_n$ wohldefiniert und charakterisiert durch

$$(\star) \qquad p_0 = 2 \quad ; \quad p_{n+1} = \mu q \leqslant p_n! + 1[q\, \mathsf{prim} \;\&\; q > p_n].$$

Auch $(\star)$ ist eine Anwendung von $\boldsymbol{Op}$. Denn mit $f\colon (a, b) \mapsto \mu q \leqslant b[q\, \mathsf{prim} \;\&\; q > a]$

ist auch $g\colon (a,b) \mapsto f(a, b!+1)$ p.r. und die zweite Gleichung in $(\star)$ läßt sich einfach schreiben als $p_{n+1} = g(n, p_n)$. Folglich ist die Primzahlaufzählung $n \mapsto p_n$ p.r.

(C) macht den Unterschied zwischen p.r. und rekursiven Funktionen etwas deutlicher. Erstere lassen sich mit einem im Prinzip abschätzbaren Aufwand berechnen, während die Existenzbedingung $\forall\vec{a}\,\exists m\, P(\vec{a}, m)$ in (C) nichtkonstruktiv sein kann, so daß selbst grobe Abschätzungen über den Berechnungsaufwand unmöglich sind.

Bemerkung 2. Anders als alle p.r. Funktionen lassen sich die μ-rekursiven Funktionen nicht mehr effektiv aufzählen, auch nicht alle einstelligen. Denn wäre $(f_n)_{n\in\mathbb{N}}$ eine solche Aufzählung, so wäre $f\colon n \mapsto f_n(n)+1$ sicher berechenbar und nach der Churchschen These rekursiv. Also $f = f_m$ für ein m, was den Widerspruch $f_m(m) = f(m) = f_m(m)+1$ ergibt. Das spricht anscheinend gegen die These, die sich mit etwas Rekursionstheorie aus dem Argument aber eliminieren läßt. Wiederholt man die Argumentation mit einer Aufzählung aller p.r. einstelligen Funktionen, haben wir einen wenn auch nichtkonstruktiven Existenzbeweis für eine einstellige berechenbare aber nicht p.r. Funktion vor uns.

Die nachfolgenden Ausführungen dieses Abschnitts benötigen wir in **6.2**. Es geht um die Kodierung endlicher Zahlenfolgen durch natürliche Zahlen. Dafür gibt es grundsätzlich mehrere Möglichkeiten. Eine davon ist, mit Hilfe der Paarkodierung $\wp$ (oder einer ähnlichen Funktion, siehe z.B. [Shoe]) den 1-Tupeln (a) die Zahlen $\wp(a,0)$, den Paaren (a,b) die Zahlen $\wp(\wp(a,b),1)$ zuzuordnen, usw. Das ergibt eine Bijektion zwischen $\bigcup_{k>0}\mathbb{N}^k$ und $\mathbb{N}$. Wir wählen indes die besonders anschauliche, auf der eindeutigen Primfaktorzerlegung beruhende Kodierung nach [Go2].

Definition. Die natürliche Zahl $\langle a_0,\dots,a_n\rangle := p_0^{a_0+1}\cdot\ldots\cdot p_n^{a_n+1}$ heiße die *Gödelzahl* der Zahlenfolge $(a_0,\dots,a_n)$. Dabei sei $k \mapsto p_k$ die Primzahlaufzählung. Die leere Folge habe die Gödelzahl $\langle\rangle := 1$. Es bezeichne Gz die Menge aller Gödelzahlen.

$\langle a_0,\dots,a_n\rangle = \langle b_0,\dots,b_m\rangle$ impliziert offenbar $m = n$ & $a_i = b_i$ für alle $i \leqslant n$. Diese unabdingbare Eindeutigkeits-Eigenschaft ist der Grund, warum in obiger Definition die Exponenten „um 1 erhöht“ wurden. Auch ist $\vec{a} \mapsto \langle a_1,\dots,a_n\rangle$ sicher p.r. Und nach (A), (B) oben auch Gz. Denn

$$a \in Gz \;\Leftrightarrow\; a \neq 0 \;\&\; (\forall p{\leqslant}q)(\forall q{\leqslant}a)[\mathsf{prim}\,p,q \;\&\; q\,|\,a \;\Rightarrow\; p\,|\,a].$$

Wir verschaffen uns einen kleinen Vorrat p.r. Funktionen, die u.a. in **6.2** wichtig sind. Nach (C) wird wie folgt eine p.r. Funktion $a \mapsto \ell a$ definiert:

$$\ell a = \mu k{\leqslant}a[p_k \nmid a].$$

ℓa gibt für Gödelzahlen a gerade die „Länge“ von a an. Denn offenbar ist $\ell 1 = 0$, und für $a = \langle a_0,\dots,a_n\rangle = \prod_{i\leqslant n} p_i^{a_i+1}$ ist $\ell a = n+1$, weil $k = n+1$ der kleinste Index ist mit $p_k \nmid a$, der wegen $n+1 < p_n \leqslant a$ zugleich auch die Bedingung $k \leqslant a$

erfüllt. Was ℓa für Zahlen a bewirkt, die keine Gödelzahlen sind, müssen wir nicht wissen. Man könnte auch einfach $\ell a = 0$ setzen für alle $a \notin Gz$.

Auch die wie folgt definierte 2-stellige Operation $(a,i) \mapsto (a)_i$ ist primitiv rekursiv:

$$(a)_i = \mu k \leqslant a[p_i^{k+2} \nmid a].$$

Dies ist die „Komponenten-Erkennungsfunktion". Denn für $p_i^{k+1} | a$ und $p_i^{k+2} \nmid a$ gilt gewiß $k = (a)_i$. Daher $(\langle a_0, \dots, a_n \rangle)_i = a_i$ für alle $i \leqslant n$. Diese durch leichten Fettdruck auffallende Funktion beginnt die Komponentenzählung stets mit $i = 0$, so daß $(a)_{last} := (a)_{\ell a \dot{-} 1}$ die letzte Komponente einer Gödelzahl $a \neq 1$ ist.

Aus diesen Definitionen folgt $a = \prod_{i<\ell a} p_i^{(a)_i+1}$ für Gödelzahlen a, inklusive $a = 1$. Sei die *arithmetische Verkettung* $*$ erklärt durch

$$a * b = a \cdot \prod_{i<\ell b} p_{\ell a+i}^{(b)_i+1} \text{ für } a, b \in Gz, \text{ sowie } a * b = 0 \text{ sonst.}$$

Offenbar gilt $\langle a_1, \dots, a_n \rangle * \langle b_1, \dots, b_m \rangle = \langle a_1, \dots, a_n, b_1, \dots, b_m \rangle$, so daß Gz unter $*$ abgeschlossen ist. Ferner ist $a, b \leqslant a * b$ und $a, b \in Gz$ wenn immer $a * b \in Gz$.

Die Definition der Operation $*$ läßt klar erkennen, daß sie p.r. ist. Diese ist u.a. nützlich für folgende Verallgemeinerung von ***Op***, die *Wertverlaufsrekursion.* Jedem $f \in \mathbf{F}_{n+1}$ entspricht eine Funktion $\bar{f} \in \mathbf{F}_{n+1}$, die definiert sei durch

$$\bar{f}(\vec{a}, 0) = \langle\rangle \ \big(= 1\big) \quad ; \quad \bar{f}(\vec{a}, b) = \langle f(\vec{a}, 0), \dots, f(\vec{a}, b-1) \rangle \text{ für } b > 0.$$

$\bar{f}$ kodiert den Wertverlauf von f. Sei nun F eine gegebene Funktion aus $\mathbf{F}_{n+2}$. Dann gibt es ganz ähnlich wie bei ***Op*** genau ein $f \in \mathbf{F}_{n+1}$, das der Funktionalgleichung

$$\boldsymbol{Oq} \quad f(\vec{a}, b) = F(\vec{a}, b, \bar{f}(\vec{a}, b))$$

genügt. Es gilt nämlich $f(\vec{a}, 0) = F(\vec{a}, 0, \langle\rangle) = F(\vec{a}, 0, 1),\ f(\vec{a}, 1) = F(\vec{a}, 1, \langle f(\vec{a}, 0) \rangle)$, $f(\vec{a}, 2) = F(\vec{a}, 2, \langle f(\vec{a}, 0), f(\vec{a}, 1) \rangle)$ usw. $f(\vec{a}, b)$ hängt für $b > 0$ i.a. von allen Werten $f(\vec{a}, 0), \dots, f(\vec{a}, b-1)$ ab, nicht nur von $f(\vec{a}, b-1)$ wie bei ***Op***. Daher heißt ***Oq*** das Schema der *Wertverlaufsrekursion.* Ein einfaches Beispiel ist die Folge $(fn)_{n \in \mathbb{N}}$ von Fibonacci, definiert durch $f0 = 0,\ f1 = 1$ und $fn = f(n-1) + f(n-2)$ für $n \geqslant 2$. In der „Normalform" ***Oq*** ist hier F $(\in \mathbf{F}_2)$ gegeben durch $F(b, c) = b$ für $b \leqslant 1$ und $F(b, c) = (c)_{b-1} + (c)_{b-2}$ sonst. Mit diesem F gilt nämlich $fn = F(n, \bar{f}n)$ für alle n.

Op ist ein Sonderfall von ***Oq***. Ist $f = \boldsymbol{Op}(g, h)$ und wird die Funktion F durch $F(\vec{a}, 0, c) = g(\vec{a})$ und $F(\vec{a}, \mathtt{S}b, c) = h(\vec{a}, b, (c)_b)$ erklärt, so erfüllt f mit diesem F auch ***Oq***, wie man unter Beachtung von $f(\vec{a}, b) = (\bar{f}(\vec{a}, \mathtt{S}b))_b$ leicht nachrechnet.

Satz 1.1. *Sei f durch F mittels* ***Oq*** *definiert. Dann ist mit F auch f p.r.*

Beweis. Weil allgemein $\langle c_0, \dots, c_b \rangle * \langle c_{b+1} \rangle = \langle c_0, \dots, c_{b+1} \rangle$, genügt $\bar{f}$ dem Schema

$$(\star) \qquad \bar{f}(\vec{a}, 0) = 1 \quad ; \quad \bar{f}(\vec{a}, \mathtt{S}b) = \bar{f}(\vec{a}, b) * \langle F(\vec{a}, b, \bar{f}(\vec{a}, b)) \rangle.$$

Die zweite Gleichung läßt sich offenbar schreiben als $\bar{f}(\vec{a}, \mathtt{S}b) = h(\vec{a}, b, \bar{f}(\vec{a}, b))$, mit $h(\vec{a}, b, c) = c * \langle F(\vec{a}, b, c)\rangle$, also ist h p.r. Nach ($\star$) ist dann aber $\bar{f}$ p.r. Somit aber auch f, denn f ist nach ***Oq*** eine simple Komposition p.r. Funktionen. ❏

Neben der Wertverlaufsrekursion gibt es noch andere Rekursionsvorschriften, die zwar berechenbare, aber nicht mehr p.r. Funktionen definieren. Berühmtes Beispiel ist die rekursive aber nicht mehr p.r. *Ackermann-Funktion* $\circ \in \mathbf{F}_2$, definiert durch

$$0 \circ b = \mathtt{S}b \quad ; \quad \mathtt{S}a \circ 0 = a \circ 1 \quad ; \quad \mathtt{S}a \circ \mathtt{S}b = a \circ (\mathtt{S}a \circ b)$$

Wir präzisieren noch den fundamentalen und recht anschaulichen Begriff rekursiv (oder effektiv) aufzählbar. Eine Menge $M \subseteq \mathbb{N}$ heißt r.a. (= *rekursiv aufzählbar*), wenn $M = \{b \in \mathbb{N} \mid (\exists a{\in}\mathbb{N})Rab\}$ für eine rekursive Relation $R \subseteq \mathbb{N}^2$. Kurzum, M ist der *Nachbereich* von R. In jedem Falle ist M dann zugleich auch der *Vorbereich* einer rekursiven Relation, denn $a \in M \Leftrightarrow (\exists b{\in}\mathbb{N})R'ab$ mit $R'ab \Leftrightarrow Rba$.

Man beweist unschwer $M \neq \emptyset$ ist r.a. genau dann, wenn $M = \mathit{ran}\, f$ für eine rekursive Funktion $f \in \mathbf{F}_1$, Übung 4. Diese Kennzeichnung entspricht der Intuition in vollkommener Weise: Die schrittweise Berechnung von $f0, f1, \ldots$ liefert eine effektive Aufzählung von M im anschaulichen Sinne. Die leere Menge ist trivial r.a. Denn sie ist der Vorbereich der sogar p.r. leeren 2-stelligen Relation. Deren charakteristische Funktion ist nämlich gerade die eingangs vorgestellte Funktion K_0^2.

Allgemein heiße $P \subseteq \mathbb{N}^n$ r.a., falls $P\vec{a} \Leftrightarrow (\exists x{\in}\mathbb{N})Q(x, \vec{a})$ für ein $(n+1)$-stelliges rekursives Prädikat Q. Jedes rekursive Prädikat P ist auch r.a. Und zwar deshalb weil $P\vec{a} \Leftrightarrow (\exists b \in \mathbb{N})P'(b, \vec{a})$, mit $P'(b, \vec{a}) \Leftrightarrow P\vec{a}$ (Hinzufügen einer fiktiven Variablen). Man hätte natürlich nichtleere r.a. Mengen gleich als Bildmengen einstelliger rekursiver Funktionen erklären können. Aber die anfängliche Definition hat, wie man sieht, den Vorteil der natürlichen Ansdehnbarkeit auf den n-stelligen Fall.

Übungen

1. Sei $f \in \mathbf{F}_n$. Man zeige, f ist rekursiv genau dann, wenn $\mathit{graph}\, f$ dies ist [2)].

2. Sei $a \leqslant fa$ für alle a. Man zeige, mit f ist auch $\mathit{ran}\, f$ p.r. bzw. rekursiv. Damit ist $\mathit{ran}\, f$ für jede echt monoton wachsende rekursive Funktion $f \in \mathbf{F}_1$ wieder rekursiv. Das gilt übrigens auch dann noch wenn f nur monoton ist, also $a < b \Rightarrow fa \leqslant fb$. Obige Behauptung gilt auch für mehrstellige Funktionen $f \in \mathbf{F}_n$, falls $a_1, \ldots, a_n \leqslant f\vec{a}$ für alle $\vec{a} \in \mathbb{N}^n$ angenommen wird.

3. Man beweise, die Paarkodierung $\wp\colon \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ ist bijektiv.

4. Sei M eine nichtleere Teilmenge natürlicher Zahlen. Man zeige, M ist genau dann r.a. wenn $M = \mathit{ran}\, f$ für ein rekursives $f \in \mathbf{F}_1$.

[2)] Es gibt rekursive Funktionen f, deren Graph p.r. ist, nicht aber f, [Fe1, Seite 83]

6.2 Gödelisierung

Gödelisierung oder Arithmetisierung ist etwas grob formuliert die Beschreibung der Syntax einer formalen Sprache $\mathcal{L}$ und des Beweisen durch arithmetische Operationen mit natürlichen Zahlen. Sie setzt die Kodierung von Zeichenfolgen über dem Alphabet von $\mathcal{L}$ durch natürliche Zahlen voraus. Wortfunktionen und Wortprädikate entsprechen auf diese Weise wohlbestimmten Funktionen und Prädikaten über $\mathbb{N}$. Dadurch lassen sich gleich mehrere Ziele erreichen. Erstens läßt sich die intuitive Vorstellung von einer berechenbaren Wortfunktion durch den Begriff der rekursiven Funktion präzisieren. Zweitens kann man syntaktische Prädikate wie z.B. '$x \in \mathit{var}\,\alpha$' durch entsprechende arithmetische Prädikate ersetzen. Drittens lassen sich in formalen Theorien $T \subseteq \mathcal{L}$ vermittels der Kodierung auch Aussagen über Wortfunktionen, oder allgemeiner, über syntaktische Prädikate formulieren, die das Beweisen in T mit vorgegebenen Mitteln betreffen.

Wir behandeln die Gödelisierung der Syntax exemplarisch am Beispiel der formalen Sprache $\mathcal{L} = \mathcal{L}_{ar}$ in den nichtlogischen Symbolen $0, \mathtt{S}, +, \cdot$, die z.B. der Peanoarithmetik PA zugrundliegt. Entsprechendes läßt sich für andere formale Sprachen völlig analog durchführen, wie im Verlaufe der Betrachtungen leicht einzusehen ist.

Der erste Schritt ist, jedem Grundzeichen ζ von $\mathcal{L}$ umkehrbar eindeutig eine Zahl $\sharp\zeta$, seine *Nummer* zuzuordnen. Für $\mathcal{L} = \mathcal{L}_{ar}$ z.B. durch folgende Tabelle:

ζ	$=$	$\neg$	$\wedge$	$\forall$	(	)	0	$\mathtt{S}$	$+$	$\cdot$	$\boldsymbol{v}_0$	$\boldsymbol{v}_1$	...
$\sharp\zeta$	1	3	5	7	9	11	13	15	17	19	21	23	

Danach kodieren wir das Wort $\xi = \zeta_0 \cdots \zeta_n$ durch seine *Gödelzahl*

$$\langle \sharp\zeta_0, \ldots, \sharp\zeta_n \rangle = p_0^{1+\sharp\zeta_0} \cdot \ldots \cdot p_n^{1+\sharp\zeta_n}.$$

Beispiel. Der Term 0 und die Primformel $0 = 0$ haben die noch recht kleinen Gödelzahlen $2^{1+\sharp 0} = 2^{14}$ und $2^{14} \cdot 3^2 \cdot 5^{14}$. Diese Kodierung nicht gerade ökonomisch. Aber darauf kommt es hier nicht an. Es stört nicht, daß die Nummer von $=$ zugleich Gödelzahl des leeren Wortes ist. Denn $=$ als *Wort* hat die Gödelzahl $2^2 = 4$.

Weil die Symbolnummern ungerade sind, kommt 2 immer in gerader Potenz in der Primzerlegung der Gödelzahl eines nichtleeren Wortes vor. Das hat die angenehme Folge, daß sich die Gödelzahlen von Formeln und Termen von den unten definierten Gödelzahlen endlicher Formelfolgen bequem unterscheiden lassen. ξ, η, ϑ bezeichnen im folgenden Worte (oder Zeichenfolgen) aus den Grundzeichen von $\mathcal{L}$, deren Gesamtheit mit $\mathcal{S}_{\mathcal{L}}$ bezeichnet sei. $\dot{\xi}$ sei die Gödelzahl des Wortes ξ und $\dot{\alpha}$ daher die der Formel α. Schreibt man $\xi\eta$ für die Verkettung von $\xi, \eta \in \mathcal{S}_{\mathcal{L}}$, gilt offenbar $(\xi\eta)^{\cdot} = \dot{\xi} * \dot{\eta}$, mit der arithmetischen Verkettungsoperation $*$ aus **6.1**. $\dot{\mathcal{S}}_{\mathcal{L}} = \{\dot{\xi} \mid \xi \in \mathcal{S}_{\mathcal{L}}\}$ ist eine primitiv rekursive Teilmenge der Menge aller Gödelzahlen, denn

$$n \in \dot{\mathcal{S}}_{\mathcal{L}} \;\Leftrightarrow\; n \in Gz \;\&\; (\forall k{<}\ell n)\, 2 \nmid (n)_k.$$

Man muß wenigstens vorübergehend zwischen dem *Symbol* ζ und dem *Wort* ζ unterscheiden, welches eigentlich die Einerfolge (ζ) ist. $\dot{\zeta} = 2^{1+\sharp\zeta}$ ist die Gödelzahl des *Wortes* ζ. So hat der Primterm 0 die Gödelzahl $\dot{0} = 2^{1+\sharp 0}$ (Terme sind stets Worte). Ebenso muß zwischen dem Symbol $\boldsymbol{v}_0$ und dem Term $\boldsymbol{v}_0$ begrifflich unterschieden werden. Der Term $\boldsymbol{v}_0$ hat eine Gödelzahl, das Symbol $\boldsymbol{v}_0$ nur eine Nummer.

Bemerkung 1. Man könnte von Anfang Formeln auch mit ihren Gödelzahlen identifizieren, so daß syntaktische Prädikate von vornherein arithmetische sind und zwischen $\dot{\varphi}$ und φ nicht unterschieden wird. Das sollte aber erst geschehen, wenn die arithmetische Formulierbarkeit der Syntax restlos klar ist. Ferner ließe sich das Alphabet von $\mathcal{L}_{ar}$ leicht durch ein endliches ersetzen, z.B. bestehend aus $\boldsymbol{=}, \neg, \dots, \boldsymbol{\cdot}, \boldsymbol{v}$, indem man $\boldsymbol{v}_0$ durch $\boldsymbol{v}0$, $\boldsymbol{v}_1$ durch $\boldsymbol{v}\mathtt{S}0$ usw. ersetzt. Andere oft anzutreffende Kodierungen entstehen durch Identifikation der Buchstaben solcher Alphabete mit den Ziffern passender p-adischer Systeme.

Im folgenden sei stets $\dot{W} = \{\dot{\xi} \mid \xi \in W\}$ für eine Menge $W \subseteq \mathcal{S}_{\mathcal{L}}$. Eine entsprechende Notation sei auch für mehrstellige Wortprädikate P verwendet. P heiße p.r. bzw. *rekursiv*, falls $\dot{P}$ p.r. bzw. rekursiv ist. Wenn also z.B. von einem rekursiven Axiomensystem $X \subseteq \mathcal{L}$ die Rede ist, meint man stets, $\dot{X}$ sei rekursiv. Auch andere Redeweisen wie rekursiv aufzählbar oder repräsentierbar seien mittels obiger oder einer ähnlichen Gödelisierung auf Wortprädikate übertragen.

Alle diese Bemerkungen beziehen sich nicht nur auf $\mathcal{L} = \mathcal{L}_{ar}$, sondern auf eine beliebige *gödelisierbare* (oder *arithmetisierbare*) Sprache $\mathcal{L}$, womit nur gemeint ist, daß $\mathcal{L}$ endlich oder abzählbar viele genau spezifizierte Grundsymbole besitzt, damit den Zeichenfolgen Zahlenkodes in berechenbarer Weise zugeordnet werden können. Damit erhalten auch die in **3.3** schon benutzten Begriffe einer axiomatisierbaren oder entscheidbaren Theorie einen restlos klaren Sinn. Man muß natürlich zwischen den Axiomen und den Sätzen einer axiomatischen Theorie deutlich unterscheiden. Denn die Axiomensysteme der wichtigsten Theorien wie etwa PA und ZFC erweisen sich als p.r. Doch sind diese Theorien als Satzmengen nach **6.5** unentscheidbar.

Das Hauptziel des Unternehmens ist die Arithmetisierung des formalen Beweisens. Deshalb bezeichne $\vdash$ der Eindeutigkeit halber den Hilbertkalkül aus **3.6**, bestehend aus dem Axiomensystem Λ mit den dort genannten Axiomenschemata $\Lambda 1$ - $\Lambda 10$ und MP als Schlußregel, jeweils bezogen auf eine fest gewählte gödelisierbare Sprache $\mathcal{L}$.

Analog wie bei Zeichenfolgen heiße für eine Formelfolge $\Phi = (\varphi_0, \dots, \varphi_n)$ von $\mathcal{L}$-Formeln $\dot{\Phi} := \langle \dot{\varphi}_0, \dots, \dot{\varphi}_n \rangle$ deren *Gödelzahl*. Das betrifft speziell den Fall, daß Φ ein Beweis aus X ($\subseteq \mathcal{L}$) im Sinne von **3.6** ist, der i.a. auch Formeln aus Λ enthält. Stets ist $\dot{\Phi} \neq \dot{\xi}$ für alle $\xi \in \mathcal{S}_{\mathcal{L}}$. Denn $(\dot{\Phi})_0 = \dot{\varphi}_0$ ist gerade, also $2 \mid (\dot{\Phi})_0$, während immer

$2 \nmid (\dot{\xi})_0$, weil die Symbolnummern ungerade sind. Dies setzen wir wie im Beispiel $\mathcal{L} = \mathcal{L}_{ar}$ stets voraus, um eben in dieser Weise schließen zu können.

Sei nun T ($\subseteq \mathcal{L}^0$) eine durch ein Axiomensystem $X \subseteq T$ axiomatisierte Theorie, etwa PA oder auch die Theorie ZFC, deren Sprache einfacher ist als $\mathcal{L}_{ar}$, was natürlich auch die Kodierung vereinfacht. Ein Beweis $\Phi = (\varphi_0, \ldots, \varphi_n)$ aus X heiße auch *ein Beweis in* T – man faßt X hierbei stillschweigend als wesentlichen Bestandteil von T auf. Dem syntaktischen Prädikat 'Φ ist ein Beweis in T' möge das einstellige arithmetische Prädikat $beweis_T$ entsprechen, und den Prädikaten 'Φ ist ein Beweis für α' (dem letztem Glied von Φ) und 'es gibt einen Beweis für α in T' die arithmetischen Prädikate bew_T bzw. bwb_T. Ihre präzisen Definitionen lauten:

$$(1) \quad beweis_T(b) \ \Leftrightarrow\ b \in Gz \ \ \& \ \ b \neq 1 \\ \& \ \ (\forall k{<}\ell b)[(b)_k \in \dot{X} \cup \dot{\Lambda} \vee (\exists\, i,j < k)(b)_i = (b)_j \mathbin{\tilde{\to}} (b)_k],$$

$$(2) \quad bew_T(b,a) \Leftrightarrow beweis_T(b)\ \&\ a = (b)_{last}, \qquad (3) \quad bwb_T(a) \Leftrightarrow \exists b\ bew_T(b,a).$$

Dabei definiert man die p.r. Funktionen $\tilde{\neg}$, $\tilde{\wedge}$, $\tilde{\to}$ durch $\tilde{\neg} a = \dot{\neg} {*} a$, $a \mathbin{\tilde{\wedge}} b = \dot{(} {*} a {*} \dot{\wedge} {*} b {*} \dot{)}$ und $a \mathbin{\tilde{\to}} b = \tilde{\neg}(a \mathbin{\tilde{\wedge}} \tilde{\neg} b)$. Den Definitionen (1), (2), (3) entnimmt man leicht

(4) $\vdash_T \alpha \ \Leftrightarrow\ $ es gibt ein n mit $bew_T(n, \dot{\alpha}) \ \Leftrightarrow\ bwb_T(\dot{\alpha})$,

(5) $bew_T(c,a)\ \&\ bew_T(d, a \mathbin{\tilde{\to}} b) \Rightarrow bew_T(c * d * \langle b \rangle, b)$, für alle a,b,c,d,

(6) $bwb_T(a)\ \&\ bwb_T(a \mathbin{\tilde{\to}} b) \Rightarrow bwb_T(b)$, für alle a,b,

(7) $bwb_T(\dot{\alpha})\ \&\ bwb_T((\alpha \to \beta)^{\boldsymbol{\cdot}}) \Rightarrow bwb_T(\dot{\beta})$, für alle Formeln α, β.

(4) ist klar, denn ist $\vdash_T \alpha \ \Leftrightarrow\ $ es gibt einen Beweis Φ für $\alpha \ \Leftrightarrow\ \exists n\, bew_T(n, \dot{\alpha})$ (man wähle $n = \dot{\Phi}$). (5) erzählt uns in arithmetischer Sprache die bekannte Geschichte, daß Verketten von Beweisen für $\alpha, \alpha \to \beta$ und Anhängen von β einen Beweis für β ergibt. Partikularisierung liefert sofort (6). Hieraus ergibt sich (7) mit $a = \dot{\alpha},\ b = \dot{\beta}$.

Bemerkung 2. Wir benötigen (5),(6),(7) erst in **7.1**, aber es ist für die spätere Beweisübertragung nach PA lehrreich, (5) zuerst naiv zu verifizieren. Dies ist einfach, wenn man folgende Fakten benutzt: Für alle $a, b \in Gz$ ist $\ell(a * b) = \ell a + \ell b$, $(a * b)_i = (a)_i$ für $i < \ell a$, $(a * b)_{\ell a + i} = (b)_i$ für $i{<}\ell b$, und $\ell\langle c \rangle = 1$, $(\langle c \rangle)_0 = c$ für alle c. Wir weisen darauf hin, daß $(\forall k{<}b)(b)_k \in \dot{\mathcal{L}}$ rechts in (1) nicht erscheint. Dies ist auch nicht nötig, denn induktiv über die Beweislänge folgt gemäß Übung 2 leicht $beweis_T(b) \Rightarrow (\forall k{<}\ell b)(b)_k \in \dot{\mathcal{L}}$.

Nun machen wir uns an die eigentliche Arbeit und zeigen, daß die syntaktischen Grundbegriffe bis hin zum Prädikat bew_T alle primitiv rekursiv sind. In **6.5** spielt im Grunde nur ihre Rekursivität eine Rolle; erst in Kapitel **7** wird wesentlich von ihrem primitiv rekursiven Charakter Gebrauch gemacht. Wir kehren dabei zu unserer Beispielsprache $\mathcal{L} = \mathcal{L}_{ar}$ zurück, weil die Beweise der folgenden Lemmata von der Syntax der Sprache und der gewählten Kodierung nicht ganz unabhängig sind.

Wir erklären nun auch $n \tilde{\boldsymbol{=}} m := n * \dot{\boldsymbol{=}} * m$ $(= n * 2^2 * m)$ und $\tilde{\forall}(i, n) := \dot{\forall} * i * n$. Auch $\tilde{\exists}$ sei entsprechend erklärt. Für $\mathtt{S}, +, \boldsymbol{\cdot}$ sei schließlich $\tilde{\mathtt{S}}n = \dot{\mathtt{S}} * n$, $n \tilde{+} m = \dot{(} * n * \dot{+} * m * \dot{)}$ und analog für $\boldsymbol{\cdot}$. Dann gelten z.B. $(s \boldsymbol{=} t)^{\boldsymbol{\cdot}} = \dot{s} \tilde{\boldsymbol{=}} \dot{t}$, $(\mathtt{S}t)^{\boldsymbol{\cdot}} = \tilde{\mathtt{S}}\dot{t}$, sowie $(\forall x \alpha)^{\boldsymbol{\cdot}} = \tilde{\forall} \dot{x} \dot{\alpha}$ $(= \tilde{\forall}(\dot{x}, \dot{\alpha}))$. Alle diese Funktionen sind offensichtlich primitiv rekursiv.

Die Menge $\mathcal{V}$ der Variablenterme ist p.r. Denn $n \in \dot{\mathcal{V}} \Leftrightarrow (\exists k \leqslant n)\, n = 2^{22+2k}$. Damit ist auch $\mathcal{T}_{prim} := \mathcal{V} \cup \{0\}$, die Menge aller Primterme von $\mathcal{L}$, p.r. Für beliebige Worte ξ, η bedeute $\xi \leqslant \eta$ überall, daß $\dot{\xi} \leqslant \dot{\eta}$. Zum Beispiel ist $\xi \leqslant \eta$, falls ξ ein Teilwort von η ist, d.h. $\eta = \vartheta_1 \xi \vartheta_2$ für gewisse ϑ_1, ϑ_2. Das folgt unmittelbar aus der leicht verifizierbaren Eigenschaft $a, b \leqslant a * b$ für Gödelzahlen a, b.

Lemma 2.1. *Die Menge $\mathcal{T}$ aller Terme ist primitiv rekursiv.*

Beweis. Entsprechend der rekursiven Definition von $\mathcal{T}$ ist $t \in \mathcal{T}$ genau dann, wenn

$$t \in \mathcal{T}_{prim} \vee (\exists\, t_1, t_2 \leqslant t)[t_1, t_2 \in \mathcal{T} \;\&\; (t = \mathtt{S}t_1 \vee t = (t_1 + t_2) \vee t = (t_1 \boldsymbol{\cdot} t_2))].$$

Daher gilt auch die entsprechende arithmetische Äquivalenz, nämlich

$$(\star) \qquad n \in \dot{\mathcal{T}} \;\Leftrightarrow n \in \dot{\mathcal{T}}_{prim} \vee (\exists\, i, k < n)[i, k \in \dot{\mathcal{T}} \;\&\; Q(n, i, k)]$$

mit $Q(n, i, k) \Leftrightarrow (n = \tilde{\mathtt{S}}i \vee n = i \tilde{+} k \vee n = i \tilde{\boldsymbol{\cdot}} k)$. Wir zeigen nun, wie man diese „informelle Definition“ von $\dot{\mathcal{T}}$, die auf der rechten Seite aber nur Bezug nimmt auf kleinere Elemente von $\dot{\mathcal{T}}$, in eine Wertverlaufsrekursion von $\chi_{\dot{\mathcal{T}}}$ verwandelt, womit $\chi_{\dot{\mathcal{T}}}$ (also $\dot{\mathcal{T}}$) als p.r. nachgewiesen wäre. Wir betrachten zu diesem Zwecke das sicher p.r. 2-stellige arithmetische Prädikat P, definiert durch

$$P(a, n) \;\Leftrightarrow\; n \in \dot{\mathcal{T}}_{prim} \vee (\exists\, i, k < n)[(a)_i = (a)_k = 1 \;\&\; Q(n, i, k)].$$

Für den Zweck des Beweises werde die charakteristische Funktion $\chi_{\dot{\mathcal{T}}}$ mit f bezeichnet. Wir behaupten, f erfüllt die Rekursionsgleichung

$$\boldsymbol{Oq}: \qquad fn = \chi_P(\bar{f}n, n) \qquad \big(\bar{f}n = \langle f(0), \ldots, f(n-1) \rangle\big)$$

und ist nach Satz 1.1 damit p.r. $\boldsymbol{Oq}$ gilt, weil $fi = fk = 1 \Leftrightarrow i, k \in \dot{\mathcal{T}}$ und

$$\begin{aligned} n \in \dot{\mathcal{T}} \quad &\Leftrightarrow \quad n \in \dot{\mathcal{T}}_{prim} \vee (\exists\, i, k < n)[fi = fk = 1 \;\&\; Q(n, i, k)] \quad \text{(nach } (\star) \text{)} \\ &\Leftrightarrow \quad P(\bar{f}n, n) \qquad \text{(weil } (\bar{f}n)_i = fi \text{ und } (\bar{f}n)_k = fk). \end{aligned}$$

Hieraus folgt aber sofort $fn = 1 \Leftrightarrow \chi_P(\bar{f}n, n) = 1$ und damit offenbar auch $\boldsymbol{Oq}$. ❏

Lemma 2.2. *Die Menge $\mathcal{L}$ $(= \mathcal{L}_{ar})$ aller Formeln ist primitiv rekursiv.*

Beweis. $\mathcal{L}_{prim}$ ist p.r. Denn $n \in \dot{\mathcal{L}}_{prim} \;\Leftrightarrow\; (\exists\, i, k < n)[i, k \in \dot{\mathcal{T}} \;\&\; n = i \tilde{\boldsymbol{=}} k]$. Beachtet man $\dot{\boldsymbol{v}}_0 < \dot{\varphi}$ für jedes $\varphi \in \mathcal{L}$, so ist das Prädikat '$\varphi \in \mathcal{L}$' für ein beliebiges Wort φ aus $\mathbb{S}_{\mathcal{L}}$ offenbar gekennzeichnet durch

$\varphi \in \mathcal{L}_{prim} \vee (\exists\, \alpha, \beta, x < \varphi)[\alpha, \beta \in \mathcal{L} \;\&\; x \in \mathcal{V} \;\&\; (\varphi = \neg\alpha \vee \varphi = (\alpha \wedge \beta) \vee \varphi = \forall x\alpha)]$.

Diese informelle Definition verwandelt man nun ganz analog wie in Lemma 2.1 in eine Wertverlaufsrekursion der charakteristischen Funktion von $\dot{\mathcal{L}}$ mittels der charakteristischen Funktion des gewiß p.r. Prädikats P, das definiert sei durch

$$P(a, n) \;\Leftrightarrow\; n \in \dot{\mathcal{L}}_{prim} \vee (\exists\, i, k, j < n)[(a)_i = (a)_k = 1 \;\&\; j \in \dot{\mathcal{V}} \\ \& \; (n = \tilde{\neg} i \vee n = i \;\tilde{\wedge}\; k \vee n = \tilde{\forall} jk)]. \quad \square$$

Ausgehend von der Substitution $\xi \mapsto \xi\,\frac{t}{x}$, die nicht für alle Zeichenfolgen ξ, sondern nur für Formeln und Terme von Interesse ist, läßt sich nun unschwer eine p.r. Funktion $(m, i, k) \mapsto [m]_i^k$ definieren mit

$$(\star) \qquad [\dot{\xi}]_{\dot{x}}^{\dot{t}} = (\xi\,\tfrac{t}{x})^{\cdot} \text{ für alle } \xi \in \mathcal{L} \cup \mathcal{T}.$$

Man übersetzt dazu die Rekursionsgleichungen für $\xi\,\frac{t}{x}$ zunächst einmal in entsprechende Forderungen an $[m]_i^k$. Für alle $m \in \dot{\mathcal{L}} \cup \dot{\mathcal{T}}$, $i \in \dot{\mathcal{V}}$ und $k \in \mathbb{N}$ sei

$$[m]_i^k = k \text{ falls } i = m \in \dot{\mathcal{T}}_{prim}, \;\; [m]_i^k = m \text{ falls } i \neq m \in \dot{\mathcal{T}}_{prim}, \;\; [\tilde{\neg} m]_i^k = \tilde{\neg}[m]_i^k,$$
$$[\tilde{\mathsf{S}} m]_i^k = \tilde{\mathsf{S}}[m]_i^k, \;\; [m \tilde{+} n]_i^k = [m]_i^k \tilde{+} [n]_i^k \text{ und analog für } \cdot, \wedge \text{ und } =,$$
$$[\tilde{\forall} jm]_i^k = \tilde{\forall}(j, m) \text{ für } j = i, \;\; [\tilde{\forall} jm]_i^k = \tilde{\forall}(j, [m]_i^k) \text{ für } j \neq i.$$

Für alle übrigen Tripel m, i, k sei $[m]_i^k = 0$. Wir überlassen es dem Leser, hieraus eine Wertverlaufsrekursion zur Bestimmung von $[m]_i^k$ durch p.r. Fallunterscheidung so zu basteln, daß die angegebenen Bedingungen und damit $(\star)$ erfüllt sind.

Man sieht leicht, daß das Prädikat 'x kommt in ξ vor', kurz '$x \in var\,\xi$' p.r. ist. Denn $x \in var\,\xi \;\Leftrightarrow\; x \in \mathcal{V} \;\&\; (\exists\, \eta, \vartheta \leqslant \xi)(\xi = \eta x \vartheta)$. Ersetzt man rechts x durch $\forall x$, ergibt sich '$x \in gbd\,\alpha$' als p.r. zu erkennen. Auch das zweistellige Prädikat '$x \in frei\,\alpha$' ist p.r. Denn $x \in frei\,\alpha \;\Leftrightarrow\; x \in \mathcal{V} \;\&\; \alpha\,\frac{0}{x} \neq \alpha$ ($\Leftrightarrow\; x \in \mathcal{V} \;\&\; [\dot{\alpha}]_{\dot{x}}^{\dot{0}} \neq \dot{\alpha}$). Folglich ist auch $\mathcal{L}^0$ p.r. Nach diesen Vorbereitungen beweisen wir

Lemma 2.3. *Die Menge Λ der logischen Axiome ist primitiv rekursiv.*

Beweis. $\Lambda 1$ ist p.r. weil $\varphi \in \Lambda 1$ genau dann, wenn

$$(\exists\, \alpha, \beta, \gamma < \varphi)[\alpha, \beta, \gamma \in \mathcal{L} \;\&\; \varphi = (\alpha \to \beta \to \gamma) \to (\alpha \to \beta) \to (\alpha \to \gamma)].$$

Die Kennzeichnung des entsprechenden arithmetischen Prädikats verwendet die p.r. Funktion $\tilde{\to}$. Ähnlich argumentiert man für $\Lambda 2$ - $\Lambda 4$. Für eine p.r. Kennzeichnung von $\Lambda 5$ benutzt man, daß '$\alpha, \frac{t}{x}$ kollisionsfrei' p.r. ist, denn dies trifft zu genau dann, wenn $(\forall y {<} \alpha)(y \in gbd\,\alpha \;\&\; y \in var\,t \Rightarrow y = x)$. Ferner ist das von φ, α, x, t abhängige Prädikat '$\varphi = \forall x\alpha \to \alpha\,\frac{t}{x}$' p.r. wie man unter Verwendung von $(m, i, k) \mapsto [m]_i^k$ leicht sieht. Mithin ist auch $\Lambda 5$ p.r. Denn φ gehört zu $\Lambda 5$ genau dann, wenn

$$(\exists\, \alpha, x, t < \varphi)(\alpha \in \mathcal{L} \;\&\; x \in \mathcal{V} \;\&\; t \in \mathcal{T} \;\&\; \varphi = \forall x\alpha \to \alpha\,\tfrac{t}{x} \;\;\&\;\; \alpha, \tfrac{t}{x} \text{ kollisionsfrei}).$$

Analog sieht man, daß auch $\Lambda 6$ - $\Lambda 10$ p.r. sind, also ist jedes der Schemata Λi p.r. und somit auch $\Lambda_0 := \Lambda 1 \cup \cdots \cup \Lambda 10$. Dann gilt dasselbe aber für Λ. Denn weil $k \mapsto \sharp \boldsymbol{v}_k$ sicher p.r. ist, und weil jedes $\alpha \in \Lambda$ eine Darstellung $\alpha = \forall \vec{x} \alpha_0$ mit einem (eventuell leeren) Präfix $\forall \vec{x}$ und einem $\alpha_0 \in \Lambda_0$ hat, gilt offenbar

$$n \in \dot{\Lambda} \;\Leftrightarrow\; n \in \dot{\mathcal{L}} \;\&\; (\exists\, m, k < n)[n = m * k \;\&\; 2 \,|\, \ell m \;\&\; k \in \dot{\Lambda}_0$$
$$\&\;\; (\forall i{<}\ell m)(2 \,|\, i \;\&\; (m)_i = \sharp\forall \;\;\vee\;\; 2 \nmid i \;\&\; (\exists k{\leqslant}n)(m)_i = \sharp \boldsymbol{v}_k)].$$

Die zweite Zeile dieser Formel erzählt uns, daß m die Gödelzahl eines Präfixes der Gestalt $\forall x_1 \cdots \forall x_l$ mit $2l = \ell m$ ist. ❑

Diese Lemmata gelten völlig analog für jede gödelisierbare Sprache. Damit ist für jedes p.r. bzw. rekursive Axiomensystem X auch $X \cup \Lambda$ p.r. bzw. rekursiv. Das betrifft insbesondere die Axiomensysteme von PA und ZFC. Diese sind wie fast alle gebräuchlichen Axiomensysteme trotz ihrer unterschiedlichen Stärke p.r., was man ähnlich beweist wie für Λ. Sie sind aus rekursionstheoretischer Perspektive also ziemlich banal. Das folgende Hauptergebnis des Abschnitts ist aber ganz unabhängig von der Stärke von T. Diese spielt erst eine Rolle, wenn man über bew_T und bwb_T *im Rahmen von* T etwas beweisen will, wie dies in **7.1** geschieht.

Satz 2.4. *Sei X ein p.r. Axiomensystem für eine Theorie T einer gödelisierbaren Sprache. Dann ist das Prädikat bew_T p.r. Hingegen sind bwb_T und T selbst i.a. nur rekursiv aufzählbar. Dasselbe gilt, wenn hier überall rekursiv statt p.r. gesagt wird.*

Beweis. (1) und (2) Seite 178 zeigen, daß bew_T p.r. ist. Damit ist bwb_T r.a. gemäß Definition dieses Begriffs, und zwar auch dann, wenn X und damit bew_T nur rekursiv statt p.r. sind. Dasselbe gilt für T; denn $a \in \dot{T} \Leftrightarrow \exists b(bew_T(b, a))$ & $a \in \dot{\mathcal{L}}^0)$ und $\mathcal{L}^0$ ist rekursiv (sogar p.r.) wie vor Lemma 2.3 festgestellt wurde. ❑

Dieses Ergebnis kann nur unter besonderen Umständen verbessert werden. bwb_T ist z.B. für $T = \mathsf{Q}$ zwar r.a., nicht aber rekursiv wie in **6.5** nachgewiesen wird.

Übungen

1. Man beweise: hat eine Theorie T ein rekursiv aufzählbares Axiomensystem, so besitzt T auch ein rekursives Axiomensystem (W. Craig).

2. Man zeige (für $\mathcal{L} = \mathcal{L}_{ar}$): $a, a \tilde{\to} b \in \dot{\mathcal{L}} \Rightarrow b \in \dot{\mathcal{L}}$, für alle $a, b \in \mathbb{N}$ (die arithmetische Version von $\alpha, \alpha \to \xi \in \mathcal{L} \Rightarrow \xi \in \mathcal{L}$, vergleiche Übung 2 in **2.2**).

3. Es sei T ($\subseteq \mathcal{L}^0_{ar}$) axiomatisierbar und $\alpha \in \mathcal{L}^0_{ar}$. Man definiere ein p.r. $f \in \mathbf{F}_2$ mit $bew_{T+\alpha}(\dot{\Phi}, \dot{\varphi}) \Rightarrow bew_T(f(\dot{\Phi}, \dot{\alpha}), (\alpha \to \varphi)^{\boldsymbol{\cdot}})$ für alle φ (Arithmetisierung des Deduktionstheorems). Daraus schließe man $bwb_{T+\alpha}\dot{\varphi} \;\Leftrightarrow\; bwb_T(\alpha \to \varphi)^{\boldsymbol{\cdot}}$.

4. Man zeige, die Menge aller quantorenfreien $\alpha \in \mathcal{L}^0_{ar}$ mit $\mathcal{N} \vDash \alpha$ ist p.r.

6.3 Repräsentierbarkeit arithmetischer Prädikate

Wir betrachten zuerst die endlich axiomatisierte Theorie Q mit den Axiomen

Q1: $\forall x\, \mathtt{S}x \neq 0$ Q2: $\forall x \forall y(\mathtt{S}x = \mathtt{S}y \to x = y)$ Q3: $(\forall x \neq 0)\exists y\, x = \mathtt{S}y$

Q4: $\forall x\, x + 0 = x$ Q5: $\forall x \forall y\, x + \mathtt{S}y = \mathtt{S}(x + y)$

Q6: $\forall x\, x \cdot 0 = 0$ Q7: $\forall x \forall y\, x \cdot \mathtt{S}y = x \cdot y + x$

Diese Axiome kennzeichnen Q als bescheidene Subtheorie der Peano-Arithmetik PA. Beide Theorien sind formuliert in $\mathcal{L}_{ar}$, der Sprache 1. Stufe in $0, \mathtt{S}, +, \cdot$.

In Q, PA und allen weiteren Theorien in $\mathcal{L}_{ar}$ seien $\leqslant$ und $<$ explizit definiert durch $x \leqslant y \leftrightarrow \exists z\, z + x = y$ und $x < y \leftrightarrow x \leqslant y \wedge x \neq y$. Wie bisher sei $\underline{n}$ der Term $\mathtt{S}^n 0$.

Aus den Resultaten dieses und des nächsten Abschnitts wird sich nicht nur die rekursive Unentscheidbarkeit von Q ergeben, sondern auch die jeder Subtheorie und jeder konsistenten Erweiterung von Q, siehe **6.5**. Wären wir nur auf Unentscheidbarkeitsresultate aus, ließe sich der Beweis des Repräsentationssatzes 4.2 durch Vermehrung der Anfangsfunktionen und Elimination des Schemas der primitiven Rekursion etwas vereinfachen, doch verwischt ein solches Vorgehen den für einige Details in Kapitel **7** wichtigen Unterschied zwischen primitiv rekursiven und μ-rekursiven Funktionen.

Wir zeigen induktiv $\vdash_{\mathsf{Q}} \underline{n} \neq \mathtt{S}\underline{n}$ für alle n. Denn $\vdash_{\mathsf{Q}} 0 \neq \mathtt{S}0$ ist klar nach Q1 und der Induktionsschritt folgt aus $\underline{n} \neq \mathtt{S}\underline{n} \vdash_{\mathsf{Q}} \mathtt{S}\underline{n} \neq \mathtt{SS}\underline{n}$, weil $\mathtt{S}\underline{n} = \mathtt{SS}\underline{n} \vdash_{\mathsf{Q}} \underline{n} = \mathtt{S}\underline{n}$ nach Q2. Hier handelt es sich um eine *Metainduktion* (Induktion in der Metatheorie, zu der die natürlichen Zahlen stets gehören). In PA ist z.B. $\forall x\, x \neq \mathtt{S}x$ leicht durch *Induktion in der Theorie* beweisbar. Q aber ist so schwach, daß $\forall x\, x \neq \mathtt{S}x$ dort unbeweisbar ist. Dies ergibt sich daraus, daß $(\mathbb{N} \cup \{\infty\}, 0, \mathtt{S}, +, \cdot)$ alle Axiome von Q erfüllt, nicht aber α. Dabei sei ∞ ein neues Objekt und die Operationen $\mathtt{S}, +, \cdot$ von $\mathbb{N}$ wie folgt auf $\mathbb{N} \cup \{\infty\}$ erweitert: $\mathtt{S}\infty = \infty$, $\infty \cdot 0 = 0$, $\infty \cdot n = n$ für alle $n > 0$, sowie

$$\infty + n = n + \infty = \infty + \infty = n \cdot \infty = \infty \text{ für alle } n.$$

Dieses Modell zeigt, daß viele bekannte Rechengesetze in Q unbeweisbar sind, die uns sagen, daß $\mathcal{N}$ mit obiger Definition von $\leqslant$ ein geordneter kommutativer Halbring mit kleinstem Element 0 und Einselement 1 ($:= \mathtt{S}0$) ist, in dem $\mathtt{S}x$ ($:= x + 1$) unmittelbarer Nachfolger von x ist. Die dies leistenden Rechengesetze denken wir uns in folgendem Axiomensystem N zusammengefaßt.

N0: $x + 0 = x$ N1: $x + y = y + x$ N2: $(x + y) + z = x + (y + z)$

N3: $x \cdot 1 = x$ N4: $x \cdot y = y \cdot x$ N5: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

N6: $x + z = y + z \to x = y$ N7: $x \leqslant y \vee y \leqslant x$ N8: $x \cdot (y + z) = x \cdot y + x \cdot z$

N9: $x < y \leftrightarrow x + 1 \leqslant y$ N10: $x \leqslant 0 \to x = 0$

$\forall$-Quantoren in den Axiomen wurden unterdrückt. N ist wie Q eine Subtheorie von PA (siehe Übung 2 in **3.3**) und wird in der Literatur auch mit PA^- bezeichnet.

In diesem Abschnitt schreiben wir einfach nur $\vdash \alpha$ für $\vdash_{\mathsf{Q}} \alpha$ und $\alpha \vdash \beta$ für $\alpha \vdash_{\mathsf{Q}} \beta$ usw. Auch schreiben wir gelegentlich $\alpha \vdash \beta \vdash \gamma$ für $\alpha \vdash \beta$ und $\beta \vdash \gamma$. Die Benutzung des Symbols $\vdash$ in folgenden Ableitungen erleichtert die Übersicht und macht die dabei verwendete Metainduktion etwas plastischer. Einige der Beweise kann man als „Verlegungen von Induktionen in PA in die Metatheorie" ansehen. So entspricht dem induktiven (genauer, metainduktiven) Beweis von C0 in Q dem induktiven Beweis von $\mathtt{S}x + y = x + \mathtt{S}y$ in PA. Wir zeigen für alle n, m

$$
\begin{array}{llll}
\text{C0:} & \vdash \mathtt{S}x + \underline{n} = x + \mathtt{S}\underline{n}, & & \\
\text{C1:} & \vdash \underline{m} + \underline{n} = \underline{m+n},\ \underline{m} \cdot \underline{n} = \underline{m \cdot n}, & \text{C2:} & \vdash \underline{m} \neq \underline{n} \quad \text{falls } m \neq n, \\
\text{C3:} & \vdash \underline{m} \leqslant \underline{n} \quad \text{falls } m \leqslant n, & \text{C4:} & \vdash \underline{m} \nleqslant \underline{n} \quad \text{falls } m \nleqslant n, \\
\text{C5:} & x \leqslant \underline{n} \vdash x = \underline{0} \vee \ldots \vee x = \underline{n}, & \text{C6:} & \vdash x \leqslant \underline{n} \ \vee\ \underline{n} \leqslant x.
\end{array}
$$

C5 ergibt offenbar $x < \underline{n} \vdash x = \underline{0} \vee \ldots \vee x = \underline{n-1}$. Kurz, $x < \underline{n} \vdash \bigvee_{i<n} x = \underline{i}$. Dies ist die leere Disjunktion für $n = 0$, also $\bot$. Die nachfolgenden Beweise erfolgen induktiv über n. Man beachte dabei stets $0 = \underline{0}$ und $\mathtt{S}\underline{n} = \underline{\mathtt{S}n} = \underline{n+1}$.

C0: Klar für $n = 0$, weil $\vdash \mathtt{S}x + 0 = \mathtt{S}x = \mathtt{S}(x + 0) = x + \mathtt{S}0$ nach Q4,Q5. Annahme: $\mathtt{S}x + \underline{n} = x + \mathtt{S}\underline{n}$. Dann folgt $\mathtt{S}x + \mathtt{S}\underline{n} = \mathtt{S}(\mathtt{S}x + \underline{n}) = \mathtt{S}(x + \mathtt{S}\underline{n}) = x + \mathtt{SS}\underline{n}$. Das beweist $\mathtt{S}x + \underline{n} = x + \mathtt{S}\underline{n} \vdash x + \mathtt{S}\underline{n} = x + \mathtt{SS}\underline{n}$ und damit den Induktionsschritt.

C1: Nach Q4 ist $\vdash \underline{m} + 0 = \underline{m}$, und weil $\underline{m} = \underline{m+0}$, ist $\vdash \underline{m} + \underline{0} = \underline{m+0}$. Aus $\vdash \underline{m} + \underline{n} = \underline{m+n}$ (Induktionsannahme) folgt mit Q5 $\vdash \underline{m} + \mathtt{S}\underline{n} = \mathtt{S}(\underline{m} + \underline{n}) = \mathtt{S}\,\underline{m+n}$ und der letzte Term ist derselbe wie $\underline{m + \mathtt{S}n}$. Das beweist den Induktionsschritt. Analog zeigt man $\vdash \underline{m} \cdot \underline{n} = \underline{m \cdot n}$ mit Q6, Q7 und dem schon Bewiesenen.

C2: $m \neq 0$ impliziert $m = \mathtt{S}k$ für ein k. Damit $\vdash \underline{m} \neq 0$ nach Q1. Sei $m \neq \mathtt{S}n$. Dann ist sicher $\vdash m \neq \mathtt{S}n$ falls $m = 0$ oder $m = n$ (wegen $\vdash \underline{n} \neq \mathtt{S}\underline{n}$, siehe Vorseite). Andernfalls ist $m = Sk$ für ein k mit $k \neq n$ – sonst wäre $m = \mathtt{S}n$. Weil $\vdash \underline{k} \neq \underline{n}$ nach Induktionsannahme, ergibt sich $\vdash \underline{m} \neq \underline{\mathtt{S}}n$ nach Q2.

C3: $m \leqslant n$ impliziert $k+m = n$ für ein k, also $\underline{k+m} = \underline{n}$. Das ergibt $\vdash \underline{k} + \underline{m} = \underline{n}$ nach C1, und folglich $\vdash \underline{m} \leqslant \underline{n}$. Der Beweis von C4 sei dem Leser als Übung überlassen.

C5: Klar für $n = 0$, weil $x \leqslant 0, x \neq 0 \vdash \exists z \mathtt{S}z = 0 \vdash \bot$ nach Q3, Q5, Q1. Gleichwertig mit der Induktionsbehauptung ist $x \leqslant \underline{\mathtt{S}n}, x \neq 0 \vdash \bigvee_{i=1}^{n+1} x = \underline{i}$. Dies folgt aus

$$
\begin{array}{rll}
x \leqslant \underline{\mathtt{S}n}, x \neq 0 & \vdash \exists y \exists z (x = \mathtt{S}y \wedge z + \mathtt{S}y = \mathtt{S}\underline{n}) & \text{(Q3)} \\
& \vdash \exists y (x = \mathtt{S}y \wedge y \leqslant \underline{n}) & \text{(Q5, Q2)} \\
& \vdash \exists y (x = \mathtt{S}y \wedge \bigvee_{i \leqslant n} y = \underline{i}) & \text{(Induktionsannahme)} \\
& \vdash \exists y (x = \mathtt{S}y \wedge \bigvee_{i=1}^{n+1} \mathtt{S}y = \underline{i}) \quad \equiv & \bigvee_{i=1}^{n+1} x = \underline{i}.
\end{array}
$$

C6: Klar für $n = 0$, weil bereits $\vdash 0 \leqslant x$ nach Q4. Sonst ist $\underline{n} < x \vdash \exists y \mathtt{S}y + \underline{n} = x$. Das aber ergibt $\underline{n} < x \vdash \mathtt{S}\underline{n} \leqslant x$ nach C0. Ferner ergibt C5 leicht $x \leqslant \underline{n} \vdash x \leqslant \mathtt{S}\underline{n}$. Damit folgt der Induktionsschritt: $x \leqslant \underline{n} \vee \underline{n} \leqslant x \ \vdash \ x \leqslant \underline{n} \vee \underline{n} < x \ \vdash \ x \leqslant \mathtt{S}\underline{n} \vee \mathtt{S}\underline{n} \leqslant x$.

Nach diesen Vorbereitungen nun die folgende entscheidende

Definition. $P \subseteq \mathbb{N}^n$ heiße *ziffernweise repräsentierbar* oder kurz *repräsentierbar* in $T \supseteq \mathsf{Q}$ [3], falls es ein $\alpha = \alpha(\vec{x})$ gibt (eine *repräsentierende Formel*) mit

$$\mathrm{R}^+: \quad P\vec{a} \Rightarrow \vdash_T \alpha(\underline{\vec{a}}) \qquad ; \qquad \mathrm{R}^-: \quad \neg P\vec{a} \Rightarrow \vdash_T \neg\alpha(\underline{\vec{a}}).$$

Beispiele. Die Identitätsrelation $\{(a, a) \mid a \in \mathbb{N}\}$ wird repräsentiert durch die Formel $x = y$. Denn $\vdash \underline{a} = \underline{b}$ für $a = b$ ist trivial, und $\vdash \underline{a} \neq \underline{b}$ für $a \neq b$ gilt nach C2. Die Formel $x \leqslant y$ repräsentiert gemäß C3, C4 das $\leqslant$-Prädikat. Dieses wird auch durch die zu $x \leqslant y$ in Q nicht äquivalente Formel $\forall z\, x \neq z + \mathtt{S}y$ repräsentiert. Die leere Menge wird durch $x \neq x$ repräsentiert, aber auch durch jede *Aussage* α mit $\neg\alpha \in \mathsf{Q}$.

Ein in Q durch α repräsentiertes P ist im anschaulichen Sinne rekursiv: Man braucht ja nur die Aufzählungsmaschine für Q einzuschalten und abzuwarten bis $\alpha(\vec{a})$ oder $\neg\alpha(\vec{a})$ erscheint. Mehr darüber in **6.4**. Für konsistente $T \supseteq \mathsf{Q}$ gelten mit R^+, R^- offenbar auch deren Umkehrungen, also $P\vec{a} \Leftrightarrow \vdash_T \alpha(\underline{\vec{a}})$ und $\neg P\vec{a} \Leftrightarrow \vdash_T \neg\alpha(\underline{\vec{a}})$.

Die Menge der in T repräsentierbaren n-stelligen Prädikate ist abgeschlossen gegenüber Vereinigung, Durchschnitt und Komplementen, sowie gegenüber Vertauschung, Gleichsetzung und Hinzufügen fiktiver Argumente. Werden z.B. P, Q durch $\alpha(\vec{x}), \beta(\vec{x})$ repräsentiert, so $P \cap Q$ offenbar durch $\alpha(\vec{x}) \wedge \beta(\vec{x})$ und $\neg P$ durch $\neg\alpha(\vec{x})$. Ein in Q repräsentiertes Prädikat P ist ferner in jeder Erweiterung von Q mit demselben Formel α repräsentierbar, speziell in $Th\mathcal{N}$, wobei $\mathcal{N}$ stets das Standardmodell $(\mathbb{N}, 0, \mathtt{S}, +, \cdot)$ bezeichnet. Weil $\mathcal{N} \vDash \alpha(\underline{\vec{a}})$ gleichwertig ist mit $\mathcal{N} \vDash \alpha\ [\vec{a}]$, bedeuten Repräsentierbarkeit von P in $Th\mathcal{N}$ und Definierbarkeit von P in $\mathcal{N}$ durch α im Sinne von **2.3** ein und dasselbe.

Man könnte $f \in \mathbf{F}_n$ als repräsentierbar bezeichnen, wenn *graph* f repräsentierbar ist. Dies erweist sich jedoch als äquivalent mit einer schärferen Form der Repräsentierbarkeit von Funktionen, der wir uns später zuwenden werden.

Die in $\mathcal{N}$, d.h. mit $0, \mathtt{S}, +, \cdot$ definierbaren Prädikate und Funktionen heißen nach [Go2] *arithmetisch*. Von jetzt ab habe dieses Wort stets diese Bedeutung. Die arithmetischen Prädikate umfassen die repräsentierbaren. Um mehr über diese Objekte zu erfahren, betrachten wir deren definierende Formeln etwas näher. Primformeln in

3) Das wird der Einfachheit halber angenommen. Der Begriff ist für alle gödelisierbaren Theorien wohldefiniert. In [Go2] heißen repräsentierbare Prädikate *entscheidungsdefinit*, in [HB] *vertretbar*, in [Kl] *numeralwise expressible*, in [TMR] *definable*, in [Hej] *entscheidbar* und in [En] *representable*.

$\mathcal{L}_{ar}$ sind Gleichungen, auch *diophantische Gleichungen* genannt. Ist $\delta(\vec{x},\vec{y})$ eine solche Gleichung mit $P\vec{a} \Leftrightarrow \mathcal{N} \vDash \exists\vec{y}\delta(\underline{\vec{a}},\vec{y})$, so heißt das Prädikat P *diophantisch.* Ein einfaches Beispiel ist $\leqslant$, denn $a \leqslant b \Leftrightarrow \exists y\, y + a = b$ [4)]. So sind alle durch $\exists$-Formeln $\exists\vec{y}\varphi$ in $\mathcal{N}$ definierbaren Prädikate diophantisch. Der Nachweis ist recht einfach: man denke man sich die quantorenfreie Formel φ mittels $\wedge$, $\vee$ aus Literalen aufgebaut und nutze beim induktiven Nachweis über φ die Äquivalenzen

$$\begin{aligned} s \neq t &\equiv_{\mathcal{N}} \exists z(\mathtt{S}z + s = t \vee \mathtt{S}z + t = s), \\ s_1 = t_1 \wedge s_2 = t_2 &\equiv_{\mathcal{N}} s_1^2 + t_1^2 + s_2^2 + t_2^2 = \underline{2}(s_1t_1 + s_2t_2), \\ s_1 = t_1 \vee s_2 = t_2 &\equiv_{\mathcal{N}} s_1s_2 + t_1t_2 = s_1t_2 + s_2t_1. \end{aligned}$$

Eine nicht nur für Fragen der Repräsentierbarkeit nützliche Klassifikation arithmetischer Formeln und Prädikate liefert folgende in **6.7** verallgemeinerte

Definition. Eine Formel heiße Δ_0 oder eine Δ_0-*Formel*, wenn sie aus Primformeln von $\mathcal{L}_{ar}$ durch $\wedge, \neg$ und *beschränkte Quantifizierung* erzeugt wird, d.h. mit α ist auch $(\forall x{\leqslant}t)\alpha$ eine Δ_0-Formel; dabei sei t ein beliebiger Term in $\mathcal{L}_{ar}$ mit $x \notin var\,t$. Ist φ Δ_0, so heißt jede Formel der Gestalt $\exists\vec{x}\varphi$ eine Σ_1-*Formel* und $\forall\vec{x}\varphi$ eine Π_1-*Formel.* Ferner: das Prädikat $P \subseteq \mathbb{N}^n$ heißt Δ_0, Σ_1 bzw. Π_1, wenn P durch eine Δ_0-Formel, eine Σ_1-Formel bzw. eine Π_1-Formel in $\mathcal{N}$ definiert ist. Δ_0, Σ_1 und Π_1 bezeichnen die Mengen der Δ_0-, Σ_1- bzw. Π_1-Prädikate. Es sei $\Delta_1 := \Sigma_1 \cap \Pi_1$.

Man nennt eine Formel schon dann Δ_0, Σ_1 bzw. Π_1, wenn sie zu einer oben genannten nur äquivalent ist. In diesem Sinne sind mit α z.B. auch $(\exists x{\leqslant}t)\,\alpha$ $\big(\equiv \neg(\forall x{\leqslant}t)\neg\alpha\big)$ und $(\forall x{<}t)\alpha$ $\big(\equiv (\forall x{\leqslant}t)(x = t \vee \alpha)\big)$ Δ_0-Formeln. Man beachte, Δ_1 besteht aus den Prädikaten, die sowohl Σ_1- als auch Π_1-definierbar sind; gleichwertig, P und $\neg P$ gehören beide zu Σ_1, denn Π_1 besteht offenbar gerade aus den Komplementen der $P \in \Sigma_1$. Nach Übung 3 in **2.4** sind Σ_1 und Π_1 unter Vereinigung und Durchschnitten von Prädikaten jeweils gleicher Stellenzahl abgeschlossen, und Δ_1 außerdem unter Komplementen. Man beachte, mit $P \in \mathbb{N}^m$ und $g_1, \dots, g_m \in \mathbf{F}_n$ ist auch das Prädikat $Q = P[g_1, \dots, g_m]$ Σ_1; denn $Q\vec{a} \;\Leftrightarrow\; (\exists\vec{b} \in \mathbb{N}^m)[P\vec{b}\ \&\ \bigwedge_{i=1}^m b_i = g_i\vec{a}]$.

Beispiele. Diophantische Gleichungen sind die einfachsten Δ_0-Formeln. Dazu gehören die Formeln $y = t(\vec{x})$ mit $y \notin var\,t$, die die Termfunktionen $\vec{a} \mapsto t^{\mathcal{N}}(\vec{a})$ definieren. Weil $a \mid b \Leftrightarrow (\exists c{\leqslant}b)a \cdot c = b$, sind Teilbarkeit und damit auch das Prädikat prim Δ_0. Dasselbe gilt für die durch $a \perp b \;\Leftrightarrow\; \forall c(c \mid a, b \Rightarrow c = 1)$ definierte Relation $\perp$ der Teilerfremdheit. Weil $\wp(a,b) = c \Leftrightarrow 2c = (a+b)^2 + 3a + b$, ist die Paarkodierung $\wp$ (genauer, $graph\,\wp$) Δ_0. Diophantische Prädikate sind Σ_1. Nach Satz 5.6 gilt bemerkenswerterweise auch die Umkehrung, obwohl man längere Zeit vermutet hatte, daß z.B. die Menge $P_2 = \{a \in \mathbb{N} \mid (\forall p{\leqslant}a)(\mathsf{prim}\,p\ \&\ p \mid a \Rightarrow p = 2)\}$ der Potenzen von 2 nicht diophantisch sei. Diese ist sicher Δ_0.

[4)] eine der schnelleren Lesbarkeit halber benutzte informelle Schreibweise für $\mathcal{N} \vDash \exists y\, y + \underline{a} = \underline{b}$.

Bemerkung 1. Sogar das Prädikat '$a^b = c$' ist Δ_0, aber dieser Nachweis ist aufwendig. Schon der in **6.4** erbrachte Nachweis, daß dieses Prädikat überhaupt arithmetisch ist, kostet Mühe. Frühere Resultate von Bennet, Paris, Pudlak u.a. werden in [BD] wie folgt verallgemeinert: Ist $f \in \mathbf{F}_{n+1}$ (genauer, $graph\, f$) Δ_0, so auch $g\colon (\vec{a}, n) \mapsto \prod_{i \leqslant n} f(\vec{a}, i)$, und die Rekursionsgleichung $g(\vec{x}, \mathsf{S}y) = g(\vec{x}, y) \cdot f(\vec{x}, y)$ ist bereits in $I\Delta_0$ beweisbar, einer wichtigen Abschwächung von PA. Diese Theorie entsteht aus N durch Hinzufügen des auf Δ_0-Formeln beschränkten Induktionsschemas und spielt eine vielseitige Rolle, siehe z.B. [Kra]. Induktiv über die Δ_0-Formeln folgt leicht, daß alle Δ_0-Prädikate p.r. sind. Die Umkehrung gilt nicht. Ein Beispiel ist die sehr schnell wachsende p.r. *Hyperexponentiation* mit $\mathrm{hex}(a, 0) = 1$ und $\mathrm{hex}(a, Sb) = a^{\mathrm{hex}(a,b)}$. Anschaulich formuliert $\mathrm{hex}(a, n) = \underbrace{a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}}_{n}$.

Ein modelltheoretischer Blick auf Q wird uns einen schnellen Beweis von Satz 3.1 ermöglichen. Er sagt, daß schon die relativ schwache Theorie Q Σ_1-*vollständig* ist. Er wird für PA in **7.1** noch wesentlich verschärft. Formuliert als '$\vdash_{\mathsf{Q}} \alpha$ oder $\vdash_{\mathsf{Q}} \neg\alpha$ für Δ_0-Aussagen α', könnte der Satz auch rein beweistheoretisch verifiziert werden. C1 und C2 garantieren, daß $n \mapsto \underline{n}^{\mathcal{A}}$ eine Einbettung von $\mathcal{N}$ in ein beliebiges $\mathcal{A} \vDash \mathsf{Q}$ darstellt. Also ist $\mathcal{N}$ ein Primmodell von Q im Sinne von **5.1**, o.B.d.A. also $\mathcal{N} \subseteq \mathcal{A}$. Nach C5 ist $\mathcal{A}$ sogar *Enderweiterung* von $\mathcal{N}$: alle Elemente aus $A \setminus \mathbb{N}$ befinden sich „am Ende" von A, oder für alle $a \in A$, $b \in \mathbb{N}$ folgt aus $a \leqslant^{\mathcal{A}} b$ auch $a \in \mathbb{N}$.

Satz 3.1 (über die Σ_1-Vollständigkeit der Theorie Q). *Jede in $\mathcal{N}$ wahre Σ_1-Aussage ist in Q und damit in jeder Theorie $T \supseteq \mathsf{Q}$ schon beweisbar.*

Beweis. Es genügt zu zeigen: für beliebiges $\mathcal{A} \vDash \mathsf{Q}$ mit $\mathcal{N} \subseteq \mathcal{A}$ gilt

$$(\star) \quad \mathcal{N} \vDash \alpha \;\Leftrightarrow\; \mathcal{A} \vDash \alpha, \text{ für alle } \Delta_0\text{-Aussagen } \alpha.$$

In der Tat, sei $\mathcal{N} \vDash \exists\vec{x}\varphi(\vec{x})$ mit der Δ_0-Formel $\varphi(\vec{x})$ und $\mathcal{N} \vDash \alpha := \varphi(\underline{\vec{a}})$. Nach $(\star)$ ist $\mathcal{A} \vDash \alpha$ für jedes $\mathcal{A} \vDash \mathsf{Q}$. Daher $\vdash_{\mathsf{Q}} \alpha$ und so $\vdash_{\mathsf{Q}} \exists\vec{x}\varphi(\vec{x})$. Nun zum Beweis von $(\star)$. Dies gilt sicher für alle Primaussagen α. Induktion über $\wedge, \neg$ ist klar. Es verbleibt der Schritt über die beschränkte Quantifizierung. **Annahme**: Sei $\mathcal{N} \vDash (\forall x {\leqslant} t)\beta(x) \in \mathcal{L}^0_{ar}$ wobei $\beta(x)$ Δ_0 ist und $var\, t = \emptyset$ (weil $x \notin var\, t$). Ferner sei $w\colon Var \to A$ und $a := x^w \leqslant^{\mathcal{A}} t^{\mathcal{A}}$. Gewiß ist $t^{\mathcal{A}} = t^{\mathcal{N}} \in \mathbb{N}$, weil $var\, t = \emptyset$. Also $a \in \mathbb{N}$, denn $\mathcal{A}$ ist Enderweiterung von $\mathcal{N}$. Mithin $a \leqslant^{\mathcal{N}} t^{\mathcal{N}}$. Das ergibt $\mathcal{N} \vDash \beta(\underline{a})$ nach der Annahme und so $\mathcal{A} \vDash \beta(\underline{a})$ gemäß Induktionsvoraussetzung. Folglich $\mathcal{A} \vDash (\forall x {\leqslant} t)\beta$, denn w war beliebig. Die Richtung $\Leftarrow$ im Induktionsschritt ist wegen $\mathcal{N} \subseteq \mathcal{A}$ offenkundig. Damit ist dieser ausgeführt und $(\star)$ somit bewiesen. ❏

Ist $\varphi(\vec{x})$ Δ_0, gilt nach diesem Satz mit $\mathcal{N} \vDash \varphi(\underline{\vec{a}})$ auch $\vdash_{\mathsf{Q}} \varphi(\underline{\vec{a}})$ und mit $\mathcal{N} \vDash \neg\varphi(\underline{\vec{a}})$ auch $\vdash_{\mathsf{Q}} \neg\varphi(\underline{\vec{a}})$. Denn $\varphi(\underline{\vec{a}})$ und $\neg\varphi(\underline{\vec{a}})$ sind trivialerweise Σ_1. Wir erhalten so das

Korollar 3.2. *Jede Δ_0-Formel repräsentiert in Q das durch sie in $\mathcal{N}$ definierte Prädikat.*

Lemma 3.3. *Es sei* $P \subseteq \mathbb{N}^{n+1}$ *repräsentiert durch* $\alpha(\vec{x}, y)$*, sowie* $z \notin \mathit{frei}\,\alpha$*. Dann repräsentieren* $(\exists z{<}y)\alpha(\vec{x}, z)$ *und* $(\forall z{<}y)\alpha(\vec{x}, z)$ *die Prädikate* Q *und* R *mit*

$$Q(\vec{a}, b) \Leftrightarrow (\exists c{<}b)P(\vec{a}, c) \text{ bzw. } R(\vec{a}, b) \Leftrightarrow (\forall c{<}b)P(\vec{a}, c).$$

Beweis. R^+: Es gelte $Q(\vec{a}, b)$, d.h. $P(\vec{a}, c)$ für ein $c < b$. Dann ist $\vdash \alpha(\underline{\vec{a}}, \underline{c}) \wedge \underline{c} < \underline{b}$. Folglich $\vdash (\exists z{<}\underline{b})\alpha(\underline{\vec{a}}, z)$. Zum Beweis von R^- sei $\neg Q(\vec{a}, b)$ und damit $\vdash \neg\alpha(\underline{\vec{a}}, \underline{i})$ für alle $i < b$. Mit C5 Seite 183 ergibt dies $z < \underline{b} \vdash \bigvee_{i<b} z = \underline{i} \vdash \neg\alpha(\underline{\vec{a}}, z)$ und folglich $z < \underline{b} \vdash \neg\alpha(\underline{\vec{a}}, z)$. Daher $\vdash (\forall z{<}\underline{b})\neg\alpha(\underline{\vec{a}}, z) \equiv \neg(\exists z{<}\underline{b})\alpha(\underline{\vec{a}}, z)$, womit R^- gezeigt ist. Für das Prädikat R genügt der Hinweis auf $R(\vec{a}, b) \Leftrightarrow \neg(\exists c{<}b)\neg P(\vec{a}, c)$. ❑

Wegen $(\exists z{\leqslant}y)\alpha\,\frac{z}{y} \equiv (\exists z{<}y)\alpha\,\frac{z}{y} \vee \alpha$ sind nach diesem Lemma mit P auch die durch $(\exists c{\leqslant}b)P(\vec{a}, c)$ und $(\forall c{\leqslant}b)P(\vec{a}, c)$ definierten Prädikate repräsentierbar.

Wir erklären nun den Begriff der repräsentierbaren Funktion nach [TMR]. Man könnte z.B. auch von *funktional repräsentierbar* reden, aber der neue Begriff wird sich alsbald als gleichwertig mit der Repräsentierbarkeit von *graph f* erweisen.

Definition. $f \in \mathbf{F}_n$ heiße repräsentierbar in T (ohne den Zusatz 'in T' meinen wir stets $T = \mathsf{Q}$), wenn für eine gewisse Formel $\varphi(\vec{x}, y)$ und alle $\vec{a} \in \mathbb{N}^n$

$$R^+ : \quad \vdash_T \varphi(\underline{\vec{a}}, \underline{f\vec{a}}), \qquad R^= : \quad \varphi(\underline{\vec{a}}, y) \vdash_T y = \underline{f\vec{a}}.$$

Ist f durch φ repräsentiert, so durch dasselbe φ auch *graph f*. Denn je nachdem ob $(\vec{a}, b) \in \mathit{graph}\, f$ oder nicht, ist $b = f\vec{a}$ oder $b \neq f\vec{a}$ und somit $\vdash_T \varphi(\underline{\vec{a}}, \underline{b})$ nach R^+, bzw. $\vdash_T \neg\varphi(\underline{\vec{a}}, \underline{b})$ nach C2 und $R^=$. Man sieht leicht, daß R^+ und $R^=$ zusammen ersetzt werden können durch die einzige Bedingung $y = \underline{f\vec{a}} \equiv_T \varphi(\underline{\vec{a}}, y)$ für alle $\vec{a}$.

Hat P eine repräsentierende Δ_0-, Σ_1- bzw. Π_1-Formel, heiße P auch Δ_0-, Σ_1- bzw. Π_1-repräsentierbar. Ist P Σ_1- und Π_1-repräsentierbar, heiße P Δ_1-repräsentierbar. Analoge Redeweisen verwenden wir für Funktionen. Satz 4.5 wird zeigen, daß alle irgendwie repräsentierbaren Prädikate immer auch Δ_1-repräsentierbar sind.

Lemma 3.4. (a) *Sei* $P \subseteq \mathbb{N}^{n+1}$ *durch* $\alpha(\vec{x}, y)$ *repräsentiert und* $\forall\vec{a}\,\exists b P(\vec{a}, b)$*. Dann wird* $f\colon \vec{a} \mapsto \mu b[P(\vec{a}, b)]$ *durch* $\varphi(\vec{x}, y) := \alpha(\vec{x}, y) \wedge (\forall z{<}y)\neg\alpha(\vec{x}, z)$ *repräsentiert. Ist* P Δ_1*-repräsentierbar, so ist* f Σ_1*-repräsentierbar.* (b) f *ist repräsentierbar, falls graph f repräsentierbar ist, und insbesondere* Δ_0*-repräsentierbar, falls graph f dies ist.* (c) *Ist* f Σ_1*-repräsentierbar, so ist* f *auch* Π_1*-repräsentierbar.* (d) *Ist* χ_P Σ_1*-repräsentierbar, so ist* P Δ_1*-repräsentierbar.*

Beweis. (a) Die Formel $\varphi(\vec{x}, y)$ repräsentiert nach Lemma 3.3 das durch sie definierte Prädikat und dies ist offenbar *graph f*. Es verbleibt daher der Beweis von

$$R^=_\varphi : \quad \alpha(\underline{\vec{a}}, y) \wedge (\forall z{<}y)\neg\alpha(\underline{\vec{a}}, z) \vdash y = \underline{f\vec{a}}.$$

Sei $b := f\vec{a}$. Dann ist $\underline{b}{<}y \vdash (\exists z{<}y)\alpha(\underline{\vec{a}}, z)$, weil $\vdash \alpha(\underline{\vec{a}}, \underline{b})$. Kontraposition liefert $(\forall z{<}y)\neg\alpha(\underline{\vec{a}}, z) \vdash \underline{b} \not< y$. Nach C5 und R^- gilt $y < \underline{b} \vdash \bigvee_{i<b} y = \underline{i} \vdash \neg\alpha(\underline{\vec{a}}, y)$. Daher

$\alpha(\underline{\vec{a}}, y) \vdash y \not< \underline{b}$. Also $\alpha(\underline{\vec{a}}, y) \wedge (\forall z{<}y)\neg\alpha(\underline{\vec{a}}, y) \vdash y \not< \underline{b} \wedge \underline{b} \not< y \vdash y = \underline{b}$ gemäß C6. Das beweist $R^{=}_{\beta}$. Zum Beweis der Zusatzbehauptung betrachte man einfach nur die Σ_1-Formel $\alpha(\vec{x}, y) \wedge (\forall v{<}y)\neg\alpha'(\vec{x}, v)$, wobei P durch α Σ_1- und durch α' Π_1-repräsentiert wird. (b) ist eine Anwendung von (a) auf $P = \mathit{graph}\, f$, einfach weil $f\vec{a} = \mu b[P(\vec{a}, b)]$. (c): Sei f durch die Σ_1-Formel $\varphi(\vec{x}, y)$ repräsentiert und $z \notin \mathit{var}\,\varphi$. Dann ist die Formel $\varphi'(\vec{x}, y) := \forall z(\varphi(\vec{x}, z) \to y = z)$ sicher Π_1 und f wird auch durch φ' repräsentiert. Denn nach $R^{=}$ ist $\vdash \varphi'(\underline{\vec{a}}, \underline{f\vec{a}})$, und $\vdash \varphi(\underline{\vec{a}}, \underline{f\vec{a}})$ liefert außerdem

$$\varphi'(\underline{\vec{a}}, y) = \forall z(\varphi(\underline{\vec{a}}, z) \to y = z) \vdash \varphi(\underline{\vec{a}}, \underline{f\vec{a}}) \to y = \underline{f\vec{a}} \vdash y = \underline{f\vec{a}}.$$

(d): Sei χ_P durch $\varphi(\vec{x}, y)$ Σ_1-repräsentiert. Dann ist P durch $\varphi(\vec{x}, \underline{1})$ und $\neg\varphi(\vec{x}, 0)$ zugleich Σ_1- und Π_1-repräsentiert wie man leicht verifiziert. ❑

Bemerkung 2. Nach Lemma 3.4(b) ist z.B. die Paarkodierung $\wp$ in Q durch die Δ_0-Formel $\pi(x, y, z) \wedge (\forall u{<}z)\neg\pi(x, y, u)$ repräsentiert; dabei ist $\pi(x, y, z)$ hier die Primformel $(x + y) \cdot \mathtt{S}(x + y) + \underline{2} \cdot x = \underline{2} \cdot z$. Man beachte, in $\mathcal{N}$ wird $\wp$ durch π explizit definiert.

Lemma 3.5. (a) *Sei $P \subseteq \mathbb{N}^k$ durch $\alpha(\vec{y})$ repräsentiert und $g_i \in \mathbf{F}_n$ für $i = 1, \ldots, k$ durch γ_i repräsentiert. Dann wird $Q := P[g_1, \ldots, g_k]$ repräsentiert durch die Formel $\beta(\vec{x}) := \exists\vec{y}\,[\alpha(\vec{y}) \wedge \bigwedge_i \gamma_i(\vec{x}, y_i)]$. Sind die γ_i Σ_1, ist mit P auch Q Δ_1-repräsentierbar,*
(b) *Mit $h \in \mathbf{F}_m$ und $g_1, \ldots, g_m \in \mathbf{F}_n$ ist auch $f = h[g_1, \ldots, g_m]$ repräsentierbar.*

Beweis. (a): Sei $b_i := g_i\vec{a}$, so daß $\vdash \gamma_i(\underline{\vec{a}}, \underline{b_i})$, $i = 1, \ldots, k$, sowie $\vec{b} = (b_1, \ldots, b_k)$, $\underline{\vec{b}} = (\underline{b_1}, \ldots, \underline{b_k})$. Gilt $Q\vec{a}$, also $P\vec{b}$, so ist $\vdash \alpha(\underline{\vec{b}})$. Mithin $\vdash \alpha(\underline{\vec{b}}) \wedge \bigwedge_i \gamma_i(\underline{\vec{a}}, \underline{b_i})$, also $\vdash \beta(\underline{\vec{a}})$. Falls aber $\neg Q\vec{a}$ und damit $\neg P\vec{b}$, so ist $\vdash \neg\alpha(\underline{\vec{b}})$. Mit $R^{=}_{\gamma_i}$ ergibt sich hieraus $\bigwedge_i \gamma_i(\underline{\vec{a}}, y_i) \vdash \bigwedge_i y_i = \underline{b_i} \vdash \neg\alpha(\vec{y})$. Daher $\vdash \forall\vec{y}\,[\bigwedge_i \gamma_i(\underline{\vec{a}}, y_i) \to \neg\alpha(\vec{y})] \equiv \neg\beta(\underline{\vec{a}})$. Sind die γ_i und auch α Σ_1, so auch β. Wird P zugleich durch die Π_1-Formel $\alpha'(\vec{x})$ repräsentiert, so Q durch die Π_1-Formel $\forall\vec{y}[\bigwedge_i \gamma_i(\vec{x}, y_i) \to \alpha'(\vec{y})]$. (b): $\beta(\vec{x}, z)$ repräsentiere h. Wie in (a) zeigt man leicht $\exists\vec{y}[\beta(\vec{y}, z) \wedge \bigwedge_i \gamma_i(\vec{x}, y_i)]$ repräsentiert $h[g_1, \ldots, g_m]$. ❑

Übungen

1. Man zeige, jede Σ_1-Formel ist äquivalent zu einer Σ_1-Formel $\exists y\varphi$, jede Π_1-Formel zu einer Formel $\forall y\varphi$ für eine Δ_0-Formel φ (*Quantorenkompression*).

2. Man zeige, Σ_1 ist abgeschlossen unter beschränkter Quantifizierung. Genauer, definiert $\alpha = \alpha(x, y, \vec{v})$ ein Σ_1-Prädikat, so auch $(\forall y{<}x)\alpha$ und $(\exists y{<}x)\alpha$. Dasselbe zeige man für Π_1. Dies gilt demnach auch für Δ_1.

3. Man zeige, $\alpha(\vec{x}) \wedge y = \underline{1} \vee \neg\alpha(\vec{x}) \wedge y = \underline{0}$ repräsentiert χ_P, falls α P repräsentiert.

4. Man beweise durch „Hineintreiben der Negation“ (Übung 2 in 2.4): jede Δ_0-Formel ist äquivalent zu einer aus Literalen allein mit $\wedge, \vee$ und den beschränkten Quantoren $(\forall x{\leqslant}t)$ und $(\exists x{\leqslant}t)$ aufgebauten Formel.

6.4 Der Repräsentationssatz

Zur Repräsentierbarkeit aller rekursiven oder auch nur aller p.r. Funktionen ist eine repräsentierbare Funktion $g \in \mathbf{F}_2$ hilfreich, die folgendes leistet: Zu jedem n und jeder Zahlenfolge $c_0, \dots, c_n$ existiert eine Zahl c mit $g(c,i) = c_i$ für alle $i \leqslant n$. Kurzum, c läßt sich so wählen, daß die Werte $g(c,0), g(c,1), \dots, g(c,n)$ die vorgegebenen sind. Es gibt nun viele sogar p.r. Funktionen g, die dies leisten. So gilt für $g(c,i) = (c)_i$ und $c = p_0^{1+c_0} \cdot \ldots \cdot p_n^{1+c_n}$ in der Tat $g(c,i) = c_i$, wenn $i \leqslant n$. Nur ist zunächst kein Weg erkennbar, die Repräsentierbarkeit einer solchen Funktion g in Q (oder einer Erweiterung von Q) im Rahmen der Sprache $\mathcal{L}_{ar}$ nachzuweisen. Deswegen hat K. Gödel, der um 1930 mit diesem und ähnlichen Problemen befaßt war, nach den Worten von A. Mostowski „mit Gott telefoniert". Man kennt heute mehrere Möglichkeiten, aber wir folgen der ursprünglichen, die ihren Reiz nicht verloren hat.

Es sei $\boldsymbol{\alpha}(a,b,i) := rest(a : (1 + (1 + i)b))$. Dabei sei $rest(c : d)$ der Rest der Division von c durch d ($\neq 0$), sowie $rest(c : 0) := 0$. Die Funktion $\boldsymbol{\alpha}$ hat die Δ_0-Definition

$$\boldsymbol{\alpha}(a,b,i) = k \;\Leftrightarrow\; (\exists c{\leqslant}a)[a = c(1 + (1 + i)b) + k \;\&\; k < 1 + (1 + i)b]$$

und ist nach Korollar 3.2 und Lemma 3.5(b) Δ_0-repräsentierbar. Dasselbe gilt für die Paarkodierung $\wp$, Bemerkung 2 in **6.3**. Weil $\wp$ bijektiv ist, gibt es gewiß Funktionen $\varkappa_1, \varkappa_2$ mit $\wp(\varkappa_1 k, \varkappa_2 k) = k$ für alle k. Deren explizite Darstellung ist hier unwesentlich. Es wird nur die offenkundige Eigenschaft $\varkappa_1 k, \varkappa_2 k \leqslant k$ benötigt. Die Funktion $\boldsymbol{\beta}\colon (c,i) \mapsto \boldsymbol{\alpha}(\varkappa_1 c, \varkappa_2 c, i)$ heiße die *$\boldsymbol{\beta}$-Funktion*. Auch diese ist Δ_0-definiert, denn weil $\boldsymbol{\beta}(c,i) = k \Leftrightarrow (\exists a{\leqslant}c)(\exists b{\leqslant}c)[\wp(a,b) = c \;\&\; \boldsymbol{\alpha}(a,b,i) = k]$, gewinnen wir wie für $\boldsymbol{\alpha}$ und $\wp$ eine die $\boldsymbol{\beta}$-Funktion repräsentierende Δ_0-Formel $\mathtt{beta} = \mathtt{beta}(x,y,z)$.

Man benötigt folgenden einfachen zahlentheoretischen Satz, um die wesentliche, in Lemma 4.1 formulierte Eigenschaft der $\boldsymbol{\beta}$-Funktion zu erkennen.

Chinesischer Restsatz. *Sei $c_i < d_i$ für $i = 0, \dots, n$ und seien $d_0, \dots, d_n$ paarweise teilerfremd. Dann existiert ein $a \in \mathbb{N}$ mit $rest(a : d_i) = c_i$ für $i = 0, \dots, n$.*

Beweis durch Induktion über n. Für $n = 0$ ist dies klar mit $a = c_0$. Seien nun die Voraussetzungen für $n > 0$ erfüllt. Nach Induktionsannahme ist $rest(a : d_i) = c_i$ für ein a und alle $i < n$. Auch $k := \mathrm{kgV}\{d_\nu | \, \nu{<}n\}$ und d_n sind teilerfremd (Übung 2). Also existieren nach Übung 1 Zahlen $x, y \in \mathbb{N}$ mit $xk + 1 = yd_n$. Multipliziert man beide Seiten mit $c_n(k-1) + a$, folgt $x'k + c_n(k-1) + a = y'd_n$ mit neuen Werten $x', y' \in \mathbb{N}$. Sei $a' := (x'+c_n)k + a = y'd_n + c_n$. Dann ist $rest(a' : d_i) = rest(a : d_i) = c_i$ für alle $i < n$ (weil $d_i \mid k$), aber auch $rest(a' : d_n) = c_n$, denn $c_n < d_n$. ❑

Dieser Beweis ist – anders als die Beweise in vielen Lehrbüchern der Zahlentheorie – konstruktiv und nach PA übertragbar wie **7.1** zeigen wird. In der Mathematischen

Logik kommt es gelegentlich nicht nur darauf an was man beweist, sondern wie man es beweist.

Lemma 4.1 (über die $\boldsymbol{\beta}$-Funktion). *Zu jedem n und jeder Folge $c_0, \ldots, c_n$ gibt es ein c mit $\boldsymbol{\beta}(c, i) = c_i$ für $i = 0, \ldots, n$.*

Beweis. Wir geben Werte a und b mit $\boldsymbol{\alpha}(a, b, i) = c_i$ an. Die Behauptung ist wegen $\boldsymbol{\beta}(\wp(a, b), i) = \boldsymbol{\alpha}(a, b, i)$ dann mit $c = \wp(a, b)$ erfüllt. Sei $m = \max\{n, c_0, \ldots, c_n\}$ und $b := \mathrm{kgV}\{i + 1 \mid i \leqslant m\}$ [5]. Wir behaupten, die Zahlen $d_i := 1 + (1 + i) \cdot b > c_i$ $(i \leqslant n)$ sind paarweise teilerfremd. Denn sei p Primteiler von d_i. Dann ist $p > m$, weil sonst $p \mid b \mid d_i - 1$, im Widerspruch zu $p \mid d_i$. Gilt $p \mid d_i, d_j$ für $i < j \leqslant n$, haben wir $p \mid d_j - d_i = (j - i)b$. Weil wegen $p > m$ aber $p \nmid b$, folgt $p \mid j - i \leqslant n \leqslant m < p$, daher $j - i = 0$. Also sind $d_0, \ldots, d_n$ paarweise teilerfremd. Nach dem Restsatz existiert daher ein a mit $rest(a : d_i) = c_i$ für $i = 0, \ldots, n$, d.h. $\boldsymbol{\alpha}(a, b, i) = c_i$. ❑

Bemerkung 1. Schon an dieser Stelle gewinnt man die interessante Einsicht, daß die Exponentialfunktion $(a, b) \mapsto a^b$ in $\mathcal{N}$ elementar definierbar ist, nämlich durch

$$(*) \qquad \delta_{exp}(x, y, z) := \exists u[\boldsymbol{\beta}(u, 0) = \mathtt{S}0 \wedge (\forall v{<}y)\, \boldsymbol{\beta}(u, \mathtt{S}v) = \boldsymbol{\beta}(u, v) \cdot x \wedge \boldsymbol{\beta}(u, y) = z].$$

Genauer, δ_{exp} ist die *Beschreibung* einer Σ_1-Formel, die durch Elimination der $\boldsymbol{\beta}$-Terme mittels der Formel `beta` unter Benutzung weiterer $\exists$-Quantoren aus $(*)$ entsteht. Man macht sich induktiv über b leicht klar, daß $\mathcal{N} \vDash \delta_{exp}(\underline{a}, \underline{b}, \underline{c}) \Rightarrow a^b = c$. Sei umgekehrt $a^b = c$. Dann garantiert uns Lemma 4.1 ein gesuchtes u mit $\mathcal{N} \vDash \delta_{exp}(\underline{a}, \underline{b}, \underline{c})$: man wähle ein u mit $\boldsymbol{\beta}(u, i) = a^i$ für alle $i \leqslant b$. Diese Argumentation wird in Satz 4.2 verallgemeinert.

Im folgenden Satz sei nur der Übersicht halber $T \supseteq \mathsf{Q}$ angenommen; er gilt genauso, wenn z.B. Q im Sinne von **6.6** in T nur interpretierbar ist, etwa für ZFC. Für viele Anwendungen, z.B. die Herleitung von Unentscheidbarkeitsresultaten und einer vereinfachten Version des 1. Unvollständigkeitssatzes reicht bereits der erste Teil des Satzes aus. Die Verfeinerung im zweiten Teil wird z.B. in Satz 4.5 angewendet.

Satz 4.2 (Repräsentationssatz). *Jede rekursive Funktion f – und damit auch jedes rekursive Prädikat P – ist in in Q und damit in jeder konsistenten Theorie $T \supseteq \mathsf{Q}$ repräsentierbar. f ist sogar Σ_1-repräsentierbar.*

Beweis. Es genügt, eine f in Q repräsentierende Σ_1-Formel anzugeben. Für die Anfangsfunktionen 0, $\mathtt{S}$, I^n_ν leisten dies $\boldsymbol{v}_0 = 0$, $\boldsymbol{v}_1 = \mathtt{S}\boldsymbol{v}_0$ und $\boldsymbol{v}_n = \boldsymbol{v}_\nu$. Sei nun $f = h[g_1, \ldots, g_m]$ und seien $\beta(\vec{y}, z)$ und $\gamma_i(\vec{x}, y_i)$ repräsentierende Σ_1-Formeln für h und die g_i. Dann ist $\varphi(\vec{x}, z) := \exists \vec{y}\,[\bigwedge_i \gamma_i(\vec{x}, y_i) \wedge \beta(\vec{y}, z)]$ eine derartige Formel für f (Lemma 3.5). Nun sei $f = \boldsymbol{Op}(g, h)$ und f, g seien beide Σ_1-repräsentierbar. Erklärt man P durch $P(\vec{a}, b, c) \Leftrightarrow \boldsymbol{\beta}(c, 0) = g\vec{a} \wedge (\forall v{<}b)\boldsymbol{\beta}(c, \mathtt{S}v) = h(\vec{a}, v, \boldsymbol{\beta}(c, v))$, so

[5] Gödel wählt hier $b = m!$. Aber unsere Wahl erleichtert den späteren Beweis des Satzes in PA.

entsteht dieses Prädikate offenbar aus einem Δ_0- und damit Δ_1-definierbaren Prädikat durch Einsetzung Σ_1-definierbarer Funktionen. Also ist P nach Lemma 3.5(a) Δ_1-repräsentierbar. Man sieht sehr einfach, daß $P(\vec{a}, b, c)$ gleichwertig ist mit

$$(*) \quad \boldsymbol{\beta}(c, i) = f(\vec{a}, i) \text{ für alle } i \leqslant b.$$

Nach Lemma 4.1 gibt es zu gegebenen $\vec{a}, b$ eine den Gleichungen $(*)$ genügende Zahl c. Kurzum, $\forall\vec{a}\forall b\exists cP(\vec{a}, b, c)$. Also ist nach Lemma 3.4(a) $\tilde{f} \colon \vec{a} \mapsto \mu cP(\vec{a}, b, c)$ Σ_1-repräsentierbar. Wegen $P(\vec{a}, b, \tilde{f}(\vec{a}, b))$ ist $(*)$ mit $c := \tilde{f}(\vec{a}, b)$ tatsächlich erfüllt. Für $i = b$ ergibt dies $f(\vec{a}, b) = \boldsymbol{\beta}(\tilde{f}(\vec{a}, b), b)$. Als Komposition Σ_1-repräsentierbarer Funktionen ist damit auch f Σ_1-repräsentierbar. Schließlich entstehe f aus g mittels $\boldsymbol{O\mu}$, also $f\vec{a} = \mu b[P(\vec{a}, b)]$, mit $P(\vec{a}, b) \Leftrightarrow g(\vec{a}, b) = 0$; dabei sei g Σ_1-repräsentierbar. Nach Lemma 3.4(c) ist g zugleich auch Π_1-repräsentierbar und P damit sicher Δ_1-repräsentierbar. Dann aber ist f nach Lemma 3.4(a) auch Σ_1-repräsentierbar. ❑

Sei $T \supseteq \mathsf{Q}$ eine Theorie in $\mathcal{L}_{ar}$. Der Gödelzahl von $\varphi \in \mathcal{L}_{ar}$ entspricht in T der Term $\underline{\dot{\varphi}}$, der fortan mit $\ulcorner\varphi\urcorner$ bezeichnet werde und der *Gödelterm* von φ heiße. So ist z.B. $\ulcorner \boldsymbol{v}_0 \boldsymbol{=} 0 \urcorner = \underline{\dot{\boldsymbol{v}}_0 \dot{=} \dot{0}} = \underline{2^{22} \cdot 3^2 \cdot 5^{14}}$. Analog sei $\ulcorner t \urcorner$ für Terme t definiert. Ist T axiomatisierbar, so ist $\ulcorner\Phi\urcorner = \underline{\dot{\Phi}}$ auch für Beweise Φ wohldefiniert. Zum Beispiel ist $\Phi = (\mathtt{S}\boldsymbol{v}_0 \boldsymbol{=} \mathtt{S}\boldsymbol{v}_0)$ ein trivialer Beweis der Länge 1 nach Axiom $\Lambda9$ in **3.6**. Sein Gödelterm ist $\ulcorner\Phi\urcorner = \underline{2^{\dot{\mathtt{S}}\dot{\boldsymbol{v}}_0 \dot{=} \dot{\mathtt{S}}\dot{\boldsymbol{v}}_0 + 1}} = \underline{2^{2^{16} \cdot 3^{22} \cdot 5^2 \cdot 7^{16} \cdot 11^{22} + 1}}$.

Weil bew_T rekursiv ist (Satz 2.4), ist bew_T Σ_1-repräsentierbar gemäß Satz 4.2, sagen wir durch $\mathtt{bew}_T(y, x)$. Nach (4) von Seite 178 ist $\vdash_T \varphi$ äquivalent zu $bew_T(n, \dot{\varphi})$ für ein geeignetes n. Für $\mathtt{bwb}_T(x) := \exists y\, \mathtt{bew}_T(y, x)$ liefert Satz 4.2 damit folgendes

Korollar 4.3. *Es sei $T \supseteq \mathsf{Q}$ axiomatisierbar. Dann gilt $\vdash_T \varphi$ genau dann, wenn $\vdash_T \mathtt{bew}_T(\underline{n}, \ulcorner\varphi\urcorner)$ für ein gewisses n. Aus $\vdash_T \varphi$ folgt daher $\vdash_T \mathtt{bwb}_T(\ulcorner\varphi\urcorner)$.*

Die Umkehrung $\vdash_T \mathtt{bwb}_T(\ulcorner\varphi\urcorner) \Rightarrow \vdash_T \varphi$ muß nicht gelten! Siehe dazu **7.1**. Satz 4.2 hat weitere wichtige Folgerungen. Vor deren Formlierung stellen aber noch eine Methode vor, welche die Churchsche These aus anschaulichen Entscheidbarkeits-Argumenten zu eliminieren erlaubt. Das muß im Prinzip immer gesichert sein, sonst verlöre die These ihre Berechtigung. Diese wird z.B. in Satz 3.5.2 verwendet. Wir formulieren diesen Satz jetzt etwas präziser und beweisen ihn anschließend rigoros.

Satz 4.4. *Eine vollständige axiomatisierbare Theorie T ist rekursiv.*

Beweis. Wegen der angenommenen Vollständigkeit ist

$$f \colon a \mapsto \mu b[a \in \dot{\mathcal{L}}^0 \;\Rightarrow\; bew_T(b, a) \vee bew_T(b, \tilde{\neg}a)]$$

wohldefiniert. Denn bezeichnet $P(a, b)$ das p.r. Prädikat in eckigen Klammern, gilt offenbar $\forall a\exists bP(a, b)$, wobei für $a \notin \dot{\mathcal{L}}^0$ bereits $P(a, 0)$ zutrifft. Gemäß $\boldsymbol{O\mu}$ ist f also rekursiv. Ferner gilt $(*)$ $a \in \dot{T} \Leftrightarrow a \in \dot{\mathcal{L}}^0$ & $bew_T(fa, a)$, was sofort die Rekursivität von T impliziert. Zum Nachweis von $(*)$ sei $a \in \dot{T}$, und damit gewiß $a \in \dot{\mathcal{L}}^0$. Dann gilt für $b = fa$ – das kleinste b mit $bew_T(b,a) \vee bew_T(b, \tilde{\neg} a)$ – sicher das erste Alternativglied, weil wegen der Konsistenz von T überhaupt kein b mit $bew_T(b, \tilde{\neg} a)$ existiert. Also $bew_T(fa, a)$. Die Richtung $\Leftarrow$ in $(*)$ ist offensichtlich. ❑

Dieser Beweis illustriert zugleich den Unterschied zwischen einem p.r. und einem rekursiven Entscheidungsverfahren. Auch wenn X und damit das Prädikat P p.r. sind, muß die dort definierte rekursive Funktion f nicht mehr p.r. sein, denn die Vollständigkeit von T könnte ja auf nichtkonstruktive Weise erschlossen worden sein. Der Gebrauch der Churchschen These in den Beweisen von (i)⇒(ii) und (iii)⇒(ii) im folgenden Satz kann in fast derselben Weise eliminiert werden wie oben, nur ist der Beweis dann etwas weniger anschaulich und seine Lektüre wird erschwert.

Satz 4.5. *Für ein Prädikat $P \subseteq \mathbb{N}^n$ und eine beliebige konsistente axiomatisierbare Theorie $T \supseteq \mathsf{Q}$ sind folgende Eigenschaften äquivalent:*

(i) *P ist repräsentierbar in T,* (ii) *P ist rekursiv,* (iii) *P ist Δ_1.*

Beweis. (i)⇒(ii): P werde in T durch $\alpha(\vec{x})$ repräsentiert. Wir starten bei gegebenem $\vec{a}$ die Aufzählungsmaschine von T und warten, bis $\alpha(\vec{a})$ oder $\neg\alpha(\vec{a})$ erscheint. Also ist P entscheidbar und damit rekursiv. (ii)⇒(i),(iii): Nach Satz 4.2 ist χ_P in T durch eine Σ_1-Formel repräsentiert. Daher ist P gemäß Lemma 3.4(d) Δ_1-repräsentierbar und zugleich wurde $P \in \Delta_1$ gezeigt. (iii)⇒(ii): Sei P definiert durch die Σ_1-Formel $\alpha(\vec{x})$ und durch die Π_1-Formel $\beta(\vec{x})$. Wir starten bei gegebenem $\vec{a}$ die Aufzählungsmaschine für T und warten, bis eine der Σ_1-Aussagen $\alpha(\underline{\vec{a}})$ oder $\neg\beta(\underline{\vec{a}})$ erscheint. Im ersten Falle gilt $P\vec{a}$, im zweiten nicht. Das Verfahren terminiert, denn T ist Σ_1-vollständig nach Satz 3.1. Also ist P entscheidbar und damit rekursiv. ❑

Nach dem Satz sind in jeder konsistenten axiomatischen Erweiterung von Q dieselben Prädikate repräsentierbar, nämlich genau die rekursiven. Ferner besteht Δ_1 danach genau aus den rekursiven, und wie man unter Beachtung von Übung 1 in **6.3** leicht folgert, Σ_1 genau aus den r.a. Prädikaten. Satz 4.5 macht den engen Zusammenhang zwischen Logik und Rekursionstheorie besonders deutlich. Er ist unabhängig von der Churchschen These. Selbst wenn diese irgendwie revidiert werden müßte, würde die ausgezeichnete Rolle der μ-rekursiven Funktionen dadurch nicht angetastet.

Bemerkung 2. Man wünscht sich natürlich ein übersehbares Repräsentantensystem von Formeln, welche die rekursiven Prädikate in hinreichend starken Theorien repräsentieren oder in $\mathcal{N}$ zumindest definieren. Leider kann man ein solches Formelsystem nicht rekursiv aufzählen. Denn angenommen es gibt eine solche Aufzählung. Sei $\alpha_0, \alpha_1, \ldots$ die hieraus entstehende Folge ihrer Glieder aus $\mathcal{L}^1_{ar}$, die in $\mathcal{N}$ dann die rekursiven Mengen definieren. Dann ist auch $\{n \in \mathbb{N} \mid n \notin \alpha_n^{\mathcal{N}}\}$ rekursiv, also etwa durch α_m in $\mathcal{N}$ definiert, so daß $n \in \alpha_m^{\mathcal{N}} \Leftrightarrow n \notin \alpha_n^{\mathcal{N}}$. Das ergibt für $n = m$ aber den Widerspruch $m \in \alpha_m^{\mathcal{N}} \Leftrightarrow m \notin \alpha_m^{\mathcal{N}}$.

In **6.5** und **7.1** benötigen wir noch weitere p.r. Funktionen. $\mathrm{zf}\colon n \mapsto \underline{\dot{n}}$ (Gödelzahl von $\underline{n}$) ist sicher p.r. Denn $\mathrm{zf}\,0 = \dot{0}$ und $\mathrm{zf}\,\mathtt{S}n = \dot{\mathtt{S}} * \mathrm{zf}\,n$. Sei $\mathrm{sb}_x(m,n) = [m]^{\mathrm{zf}\,n}_{\dot{x}}$, sowie $\mathrm{sb}_{\vec{x}} \in \mathbf{F}_{n+1}$ durch $\mathrm{sb}_{\vec{x}}(m,\vec{a}) = \mathrm{sb}_{x_n}(\mathrm{sb}_{x_1,\dots,x_{n-1}}(m,a_1,\dots,a_{n-1}),a_n)$ erklärt, $n>1$. Dabei seien $x_1,\dots,x_n$ beliebige, aber paarweise verschiedene Variablen. Der Bequemlichkeit halber sei $\mathrm{sb}_\emptyset(m) = m$. Sei $\dot{\alpha}\frac{\tilde{\mathrm{t}}}{\tilde{\mathrm{x}}} := (\alpha\frac{\tilde{\mathrm{t}}}{\tilde{\mathrm{x}}})^{\boldsymbol{\cdot}}$ und speziell $\dot{\alpha}_{\vec{x}}(\underline{\vec{a}})$ die Gödelzahl der Aussage $\alpha_{\vec{x}}(\underline{\vec{a}})$. Die Funktionen $\mathrm{sb}_{\vec{x}}$ sind offenbar alle p.r. und es gilt

Satz 4.6. *Für beliebiges* $\alpha \in \mathcal{L}$ *ist* $\mathrm{sb}_{\vec{x}}(\dot{\alpha},\vec{a}) = \dot{\alpha}_{\vec{x}}(\underline{\vec{a}})$ *für alle* $\vec{a} \in \mathbb{N}^n$.

Beweis. Weil $\alpha_{\vec{x}}(\underline{\vec{a}})$ durch schrittweise Ausführung einfacher Substitutionen entsteht ((2) in **2.2**), muß nur $\mathrm{sb}_x(\dot{\alpha},a) = \dot{\alpha}_x(\underline{a})$ für alle a gezeigt werden. Das erfolgt induktiv über α, Übung 4a. Vorher ist $\mathrm{sb}_x(\dot{t},a) = \dot{t}_x(\underline{a})$ zu zeigen. ❑

Beispiele. α sei $\mathtt{S}x = y$. Dann ist $\mathrm{sb}_x(\dot{\alpha},a) = (\mathtt{S}\underline{a} = y)^{\boldsymbol{\cdot}}$ für alle $a \in \mathbb{N}$. Ferner gilt $\mathrm{sb}_{xy}(\dot{\alpha},a,\mathtt{S}a) = (\mathtt{S}\underline{a} = \underline{\mathtt{S}a})^{\boldsymbol{\cdot}} = \tilde{\mathtt{S}}\,\mathrm{zf}\,a \mathrel{\tilde{=}} \mathrm{zf}\,\mathtt{S}a = \tilde{\mathtt{S}}\,\mathrm{zf}\,a = \tilde{\mathtt{S}}\,\mathrm{zf}\,a$, weil $\mathrm{zf}\,\mathtt{S}a = \tilde{\mathtt{S}}\,\mathrm{zf}\,a$. Aber auch $\mathrm{sb}_x(\dot{\alpha}\frac{\mathtt{S}x}{y},a) = \tilde{\mathtt{S}}\,\mathrm{zf}\,a \mathrel{\tilde{=}} \tilde{\mathtt{S}}\,\mathrm{zf}\,a$. Daher ist $\mathrm{sb}_{xy}(\dot{\alpha},a,\mathtt{S}a) = \mathrm{sb}_x(\dot{\alpha}\frac{\mathtt{S}x}{y},a)$.

Letzeres wird in Übung 4(c) verallgemeinert. Dort schreiben wir wegen der späteren Formalisierung dieser Gleichungen in PA einfach $\vec{x}$ statt $\vec{a}$. Man beachte dabei: in $\mathrm{sb}_{\vec{x}}(\vec{x})$ dient das Index-Tupel $\vec{x}$ nur als Parameter; hingegen bezeichnet $\vec{x}$ in den Klammern das Tupel der Funktionsvariablen.

Übungen

1. Man beweise den im Beweis des Chinesischen Restsatzes benutzten

   Satz von Euklid: *Positive* $a,b \in \mathbb{N}$ *sind teilerfremd (kurz* $a \perp b$*) genau dann, wenn es Zahlen* $x,y \in \mathbb{N}$ *gibt mit* $xa+1 = yb$.

2. Man zeige, $\mathrm{kgV}\{d_\nu \mid \nu{<}n\}$ und d_n sind teilerfremd, falls die Zahlen $d_0,\dots,d_n$ paarweise teilerfremd sind ($n>0$). Zuerst zeige man (a) $p \mid ab \Rightarrow p \mid a \vee p \mid b$ und (b) $p \mid \mathrm{kgV}\{a_\nu \mid \nu{\leqslant}n\}$ impliziert $p \mid a_\nu$ für ein $\nu \leqslant n$.

3. Man gebe eine definierende Σ_1-Formel für die Primzahlaufzählung $n \mapsto p_n$ an.

4. Man beweise für beliebige $\alpha,\beta \in \mathcal{L}_{ar}$ folgende Gleichungen in $\mathbb{N}$:
   (a) $\mathrm{sb}_{\vec{x}}((\alpha \wedge \beta)^{\boldsymbol{\cdot}},\vec{x}) = \mathrm{sb}_{\vec{x}}(\dot{\alpha},\vec{x}) \mathbin{\tilde{\wedge}} \mathrm{sb}_{\vec{x}}(\dot{\beta},\vec{x})$, und analog für $\neg$, $\rightarrow$ und $\forall$.
   (b) $\mathrm{sb}_{\vec{x}}(\dot{\alpha},\vec{x}) = \mathrm{sb}_{\vec{x}'}(\dot{\alpha},\vec{x}')$, mit $\mathit{var}\,\vec{x}' := \mathit{var}\,\vec{x} \cap \mathit{frei}\,\alpha$.
   (c) $\mathrm{sb}_{\vec{x},x}(\dot{\alpha},\vec{x},t) = \mathrm{sb}_{\vec{x}}(\dot{\alpha}\frac{t}{x},\vec{x})$ für $t \in \{y,\mathtt{S}y,0\}$ falls $x \notin \mathit{frei}\,\alpha$ oder $y \in \mathit{var}\,\vec{x}$; sonst ist $\mathrm{sb}_{\vec{x},x}(\dot{\alpha},\vec{x},t) = \mathrm{sb}_{\vec{x},y}(\dot{\alpha}\,\frac{t}{x},\vec{x},y)$. Hierbei sei $y \notin \mathit{gbd}\,\alpha$ und $\mathrm{sb}_{\vec{x},x}$ $(n{+}1)$-stellig. Man denke sich $\vec{x}$ um x ($\notin \mathit{var}\,\vec{x}$) verlängert.

6.5 Die Sätze von Gödel, Tarski, Church

Eine Theorie $T \subseteq \mathcal{L}$ heiße *gödelisierbar*, wenn $\mathcal{L}$ gödelisierbar ist und eine Folge $(\underline{n})_{n\in\mathbb{N}}$ paarweise verschiedener Grundterme entweder vorhanden ist oder in T so definiert werden kann, daß $\mathrm{zf}: n \mapsto \underline{\dot{n}}$ p.r. ist, siehe **6.4**. Dies ist sicher der Fall für jede Theorie $T \supseteq \mathsf{Q}$, aber z.B. auch für ZFC mit wesentlich derselben Folge von Termen, auch *ω-Terme* genannt ($\underline{0}$ sei $\emptyset$ und $\underline{n+1}$ sei $\underline{n}\cup\{\underline{n}\}$). Wie auf Seite 191 sei auch im allgemeinen Falle $\alpha \in \mathcal{L}$ *in T* durch den Gödelterm $\ulcorner\alpha\urcorner = \underline{\dot{\alpha}}$ kodiert. Um bei den folgenden sehr allgemeinen Lemmata eine konkrete Vorstellung zu haben, denke man an $\mathcal{L} = \mathcal{L}_{ar}$ und etwa $T = \mathsf{PA}$.

Eine Aussage γ heiße ein *Fixpunkt von $\alpha(x) \in \mathcal{L}$ in T*, falls $\gamma \equiv_T \alpha(\ulcorner\gamma\urcorner)$, oder gleichwertig, $\vdash_T \gamma \leftrightarrow \alpha(\ulcorner\gamma\urcorner)$. In anschaulicher Formulierung besagt γ dann offenbar „α trifft auf mich zu“. Die Funktion sb_x aus **6.4** ist für beliebig gewähltes x unter recht schwachen Voraussetzungen in T repräsentierbar (Satz 4.2). Daher haben die folgenden beiden Lemmata ein breites Anwendungsspektrum.

Fixpunktlemma. *Sei T gödelisierbar und sei sb_x in T repräsentierbar. Dann gibt es zu jedem $\alpha = \alpha(x) \in \mathcal{L}$ ein $\gamma \in \mathcal{L}^0$ mit*

(1) $\gamma \equiv_T \alpha(\ulcorner\gamma\urcorner)$.

Beweis. Sei $x_1, x_2, y \neq x$ und $\mathtt{sb}(x_1, x_2, y)$ eine sb_x in T repräsentierende Formel, die sich im Prinzip auch effektiv angeben läßt. Für alle Formeln $\varphi = \varphi(x)$ und alle n gilt also $\mathtt{sb}(\ulcorner\varphi\urcorner, \underline{n}, y) \equiv_T y \boldsymbol{=} \ulcorner\varphi(\underline{n})\urcorner$. Für $n = \dot{\varphi}$, also $\underline{n} = \ulcorner\varphi\urcorner$ folgt speziell

(2) $\mathtt{sb}(\ulcorner\varphi\urcorner, \ulcorner\varphi\urcorner, y) \equiv_T y \boldsymbol{=} \ulcorner\varphi(\ulcorner\varphi\urcorner)\urcorner$.

Sei $\beta(x) := \forall y(\mathtt{sb}(x, x, y) \to \alpha\,\frac{y}{x})$. Dann leistet $\gamma := \beta(\ulcorner\beta\urcorner)$ das Verlangte. Denn

$$\begin{array}{rll} \gamma & = & \forall y(\mathtt{sb}(\ulcorner\beta\urcorner, \ulcorner\beta\urcorner, y) \to \alpha\,\frac{y}{x}) \\ & \equiv_T & \forall y(y \boldsymbol{=} \ulcorner\beta(\ulcorner\beta\urcorner)\urcorner \to \alpha\,\frac{y}{x}) \qquad \big((2) \text{ mit } \varphi = \beta(x)\big) \\ & = & \forall y(y \boldsymbol{=} \ulcorner\gamma\urcorner \to \alpha\,\frac{y}{x}) \qquad \big(\text{weil } \gamma = \beta(\ulcorner\beta\urcorner)\big) \\ & \equiv_T & \alpha(\ulcorner\gamma\urcorner). \qquad \square \end{array}$$

Auch das folgende Lemma formuliert ein häufig wiederkehrendes Argument.

Nichtrepräsentierbarkeitslemma. Sei T konsistent und gödelisierbar. Dann ist T (genauer, $\dot{T}$) in T selbst nicht repräsentierbar.

Beweis. Angenommen, T wird durch $\tau(x)$ repräsentiert. Wir zeigen, daß bereits die schwächere Annahme (a) $\nvdash_T \alpha \;\Leftrightarrow\; \vdash_T \neg\tau(\ulcorner\alpha\urcorner)$ zum Widerspruch führt. Denn sei γ Fixpunkt von $\neg\tau(x)$ gemäß (1) oben, also (b) $\vdash_T \gamma \Leftrightarrow\; \vdash_T \neg\tau(\ulcorner\gamma\urcorner)$. Wählt man $\alpha = \gamma$ in (a), ergibt sich mit (b) offenbar der Widerspruch $\nvdash_T \gamma \;\Leftrightarrow\; \vdash_T \gamma$. $\square$

Wir formulieren nun den 1. Gödelschen Unvollständigkeitssatz, und zwar in drei Versionen, von denen die zweite im wesentlichen der originalen entspricht. Von nun an sei der Einfachheit halber $\mathcal{L} \supseteq \mathcal{L}_{ar}$ und $T \supseteq \mathsf{Q}$. Doch gilt alles folgende auch für Theorien T wie z.B. ZFC, in denen Q im Sinne von **6.6** nur interpretierbar ist.

Satz 5.1 (Die populäre Version). *Jede hinreichend starke konsistente rekursiv axiomatisierbare arithmetische Theorie T (genauer, $T \supseteq \mathsf{Q}$) ist unvollständig.*

Beweis. Wäre T vollständig, so nach Satz 3.5.2 auch entscheidbar, also in Q und damit in T repräsentierbar, was das Nichtrepräsentierbarkeitslemma ausschließt. ❑

Dieser Beweis ist, anders als die Beweise der Sätze 5.1′ und 5.1″, nicht konstruktiv. Denn er gestattet nicht, eine Aussage α mit $\nvdash_T \alpha$ und $\nvdash_T \neg\alpha$ explizit anzugeben.

Eine Verschärfung der Konsistenz einer Theorie T in $\mathcal{L}_{ar}$ ist ihre *ω-Konsistenz*, d.h. für alle $\varphi = \varphi(x)$ mit $\vdash_T \exists x\varphi(x)$ ist $\nvdash_T \neg\varphi(\underline{n})$ für mindestens ein n, oder gleichwertig, $(\forall n{\in}\mathbb{N}) \vdash_T \neg\varphi(\underline{n})$ impliziert $\nvdash_T \exists x\varphi(x)$. Ist $\mathcal{N}$ Modell für T, so ist T sicher ω-konsistent; denn die Annahme $\vdash_T \exists x\varphi$ und $\vdash_T \neg\varphi(\underline{n})$ für alle n impliziert den Widerspruch $\mathcal{N} \vDash \exists x\varphi, \forall x\neg\varphi$. Also sind z.B. die Theorien Q und PA aus semantischer Perspektive gewiß ω-konsistent. Die Beweistheorie versucht die nichtfinite Semantik den Betrachtungen fernzuhalten, und es gibt berühmte Konsistenzbeweise von PA, die weit weniger voraussetzen als die Hilfsmittel der Semantik.

Satz 5.1′ (Die Originalversion). *Zu jeder durch ein p.r. Axiomensystem X axiomatisierten ω-konsistenten Theorie $T \supseteq \mathsf{Q}$ gibt es eine Π_1-Aussage α, so daß weder $\vdash_T \alpha$ noch $\vdash_T \neg\alpha$, d.h. α ist unabhängig in T. Es gibt eine p.r. Funktion, die einer X repräsentierenden Formel ein solches α zuordnet.*

Beweis. Sei bew_T in T repräsentiert durch die Σ_1-Formel $\mathtt{bew}_T$, siehe Seite 191. Für $\mathtt{bwb}(x) = \exists y\,\mathtt{bew}_T(y, x)$ gilt dann (a) $\vdash_T \varphi \Rightarrow \vdash_T \mathtt{bwb}(\ulcorner\varphi\urcorner)$ gemäß Korollar 4.3. Sei γ Fixpunkt von $\neg\,\mathtt{bwb}(x)$ nach (1), also (b) $\gamma \equiv_T \neg\,\mathtt{bwb}(\ulcorner\gamma\urcorner)$. Die Annahme $\vdash_T \gamma$ ergibt $\vdash_T \mathtt{bwb}(\ulcorner\gamma\urcorner)$ nach (a), aber $\vdash_T \neg\,\mathtt{bwb}(\ulcorner\gamma\urcorner)$ nach (b), im Widerspruch zur Konsistenz von T. Also $\nvdash_T \gamma$. Angenommen $\vdash_T \neg\gamma$, so daß $\vdash_T \mathtt{bwb}(\ulcorner\gamma\urcorner)$ nach (b), d.h. (c) $\vdash_T \exists y\,\mathtt{bew}(y, \ulcorner\gamma\urcorner)$. Da T konsistent ist, also $\nvdash_T \gamma$, trifft $bew_T(\underline{n}, \dot\gamma)$ für kein n zu; wegen der Repräsentierbarkeit von bew_T ist also $\vdash_T \neg\,\mathtt{bew}(\underline{n}, \ulcorner\gamma\urcorner)$ für alle n. Dies und (c) widersprechen aber der ω-Konsistenz von T. Daher ist auch $\nvdash_T \neg\gamma$. Mit γ ist offenbar auch die Π_1-Aussage $\alpha = \neg\,\mathtt{bwb}(\ulcorner\gamma\urcorner)$ unabhängig in T. Die Behauptung über die p.r. Zuordnung folgt ersichtlich aus der Konstruktion von γ in (1). ❑

Dieser Satz bleibt uneingeschränkt richtig, wenn das Axiomensystem X nur r.a. ist. Denn X kann durch ein rekursives X' ersetzt werden (Übung 1 in **6.2**). Damit ist auch bew_T rekursiv, mithin in T repräsentierbar und nach Satz 4.5 auch Σ_1.

Satz 5.1″ (Rossers Verschärfung von Satz 5.1′). *Die Voraussetzung der ω-Konsistenz in Satz 5.1′ kann zur Konsistenz von T abgeschwächt werden.*

Beweis. Sei T konsistent und $\mathtt{prov}(x) := \exists y[\mathtt{bew}(y,x) \wedge (\forall z{<}y)\neg\,\mathtt{bew}(z,\tilde{\neg}x)]$. Die p.r. Funktion $\tilde{\neg}$ denken wir uns mittels einer sie repräsentierenden Formel hieraus wie üblich eliminiert. $\mathtt{prov}(x)$ besagt wegen der Konsistenz von T im Prinzip dasselbe wie $\mathtt{bwb}(x)$ und hat folgende Fundamentaleigenschaften:

$$\text{(a) } \vdash_T \mathtt{prov}(\ulcorner\alpha\urcorner) \text{ falls } \vdash_T \alpha, \quad \text{(b) } \vdash_T \neg\,\mathtt{prov}(\ulcorner\alpha\urcorner) \text{ falls } \vdash_T \neg\alpha\,^{6)}.$$

Denn sei $\vdash_T \alpha$, also $\vdash_T \mathtt{bew}(\underline{n},\ulcorner\alpha\urcorner)$ für ein n (Korollar 4.3). Wegen $\nvdash_T \neg\alpha$ sagt der Repräsentationssatz $\vdash_T \neg\,\mathtt{bew}(\underline{k},\ulcorner\neg\alpha\urcorner)$ für alle $k < n$. Daher liefert C5 aus **6.3** $\vdash_T (\forall z{<}\underline{n})\neg\,\mathtt{bew}(z,\ulcorner\neg\alpha\urcorner)$. Somit $\vdash_T \mathtt{prov}(\ulcorner\alpha\urcorner)$. Nachweis von (b): Sei $\vdash_T \neg\alpha$, etwa $\vdash_T \mathtt{bew}(\underline{m},\ulcorner\neg\alpha\urcorner)$. Weil $\nvdash_T \alpha$, ist $\vdash_T (\forall y{\leqslant}\underline{m})\neg\,\mathtt{bew}(y,\ulcorner\alpha\urcorner)$ nach C5. Das ergibt $\mathtt{bew}(y,\ulcorner\alpha\urcorner) \vdash_T \underline{m}{<}y$ nach C6. Weil $\underline{m}{<}y \vdash_T (\exists z{<}y)\,\mathtt{bew}(z,\ulcorner\neg\alpha\urcorner)$ (wähle $z = \underline{m}$), folgt $\vdash_T \forall y[\mathtt{bew}(y,\ulcorner\alpha\urcorner) \to (\exists z{<}y)\,\mathtt{bew}(z,\ulcorner\neg\alpha\urcorner)] \equiv \neg\,\mathtt{prov}(\ulcorner\alpha\urcorner)$. Das beweist (b). Sei nun $\gamma \equiv_T \neg\,\mathtt{prov}(\ulcorner\gamma\urcorner)$ gemäß (1). Die Annahme $\vdash_T \neg\gamma$ ergibt dann $\vdash_T \mathtt{prov}(\ulcorner\gamma\urcorner)$ im Widerspruch zu (b). Und die Annahme $\vdash_T \gamma$ führt zum Widerspruch ganz wie in Satz 5.1′. Also gilt in der Tat weder $\vdash_T \gamma$ noch $\vdash_T \neg\gamma$. ❑

$T \subseteq \mathcal{L}^0_{ar}$ heißt *ω-unvollständig*, wenn es ein $\varphi = \varphi(x)$ gibt mit $\vdash_T \varphi(\underline{n})$ für alle n und dennoch $\nvdash_T \forall x\varphi$. Wir zeigen, PA ist auch ω-unvollständig: Sei γ ein Fixpunkt von $\neg\,\mathtt{bwb}_{\mathsf{PA}}(x)$ und $\varphi(x) := \neg\,\mathtt{bew}_{\mathsf{PA}}(x,\ulcorner\gamma\urcorner)$. Weil $\nvdash_{\mathsf{PA}} \gamma$ (siehe den Beweis von Satz 5.1′), ist auch $\nvdash_{\mathsf{PA}} \forall x\varphi$ $(\equiv \neg\exists x\,\mathtt{bew}_{\mathsf{PA}}(x,\ulcorner\gamma\urcorner)) \equiv_{\mathsf{PA}} \gamma)$. Wohl aber ist $\vdash_{\mathsf{PA}} \varphi(\underline{n})$ für alle n wegen der Repräsentierbarkeit von bew_{PA} durch $\mathtt{bew}_{\mathsf{PA}}$. Hier ist φ sogar Π_1.

$\alpha \in \mathcal{L}^0$ heiße *wahr* in einer Struktur $\mathcal{A}$, wenn $\mathcal{A} \vDash \alpha$. Insbesondere heißt $\alpha \in \mathcal{L}^0_{ar}$ *wahr* wenn $\mathcal{N} \vDash \alpha$. Falls es ein $\tau(x) \in \mathcal{L}$ gibt mit $\mathcal{A} \vDash \alpha \;\Leftrightarrow\; \mathcal{A} \vDash \tau(\ulcorner\alpha\urcorner)$ für alle $\alpha \in \mathcal{L}^0$, sagt man *der Wahrheitsbegriff von $\mathcal{A}$ sei in $\mathcal{A}$ definierbar.* Gleichwertig: $Th\mathcal{A}$ ist in $Th\mathcal{A}$ repräsentierbar. Das Nichtrepräsentierbarkeitslemma schließt dies für $\mathcal{A} = \mathcal{N}$ aber aus. Damit erhalten wir

Satz 5.2 (Tarskis Nichtdefinierbarkeitstheorem). *$Th\mathcal{N}$ ist nicht definierbar in $\mathcal{N}$; mit anderen Worten, $Th\mathcal{N}$ ist nicht arithmetisch.*

In diesem Satz hat eine weit entwickelte Theorie über Definierbarkeit in $\mathcal{N}$ ihren Ursprung (siehe auch **6.7**). Er gilt sinngemäß für jeden Gegenstandsbereich $\mathcal{A}$, dessen Sprache gödelisierbar und in dem eine der Funktionen sb_x repräsentierbar ist.

Wir kommen nun zu Unentscheidbarkeitsresultaten. Zuerst wird die in Übung 1 in **3.6** formulierte Behauptung ohne Rückgriff auf die Churchsche These gezeigt.

[6)] Demnach ist speziell $\vdash_T \neg\,\mathtt{prov}(\ulcorner\bot\urcorner)$. Daß letzteres nicht der Fall ist, wenn hier $\mathtt{bwb}$ statt $\mathtt{prov}$ geschrieben wird, ist die Aussage des 2. Gödelschen Unvollständigkeitssatzes 7.2.2. Obwohl also $\mathtt{bew}_T(y,x) \equiv_{\mathcal{N}} \mathtt{prov}(y,x)$, verhalten sich $\mathtt{bwb}$ und $\mathtt{prov}$ innerhalb von T sehr verschieden.

Lemma 5.3. *Jede endliche Erweiterung T' einer entscheidbaren Theorie T ein und derselben Sprache $\mathcal{L}$ ist entscheidbar.*

Beweis. Sei T' Erweiterung von T um $\alpha_0, \dots, \alpha_m$, $\alpha := \bigwedge_{i \leqslant m} \alpha_i$, also $T' = T + \alpha$. Weil $\beta \in T' \Leftrightarrow \alpha \to \beta \in T$, erhalten wir $n \in \dot{T}' \;\Leftrightarrow\; n \in \dot{\mathcal{L}}^0 \;\&\; \dot{\alpha}_0 \tilde{\to} n \in \dot{T}$. Mit $\dot{T}$, $\dot{\mathcal{L}}^0$ und $\tilde{\to}$ ist dann aber auch $\dot{T}'$ rekursiv. ❑

Daß T' derselben Sprache wie T angehört, ist hier wichtig. Eine durch $X \subseteq \mathcal{L}^0$ axiomatisierte entscheidbare Theorie T kann – betrachtet als Theorie in $\mathcal{L}' \supset \mathcal{L}$ mit demselben Axiomensystem X – wegen der hinzukommenden Tautologien von $\mathcal{L}'$ durchaus unentscheidbar sein. Dieses Lemma wird oft so angewendet, daß man aus der Unentscheidbarkeit von T' die von T folgert, siehe etwa Satz 5.5 unten.

$T_0 \subseteq \mathcal{L}_0$ heiße *streng unentscheidbar*, wenn T_0 konsistent ist und jede mit T_0 verträgliche Theorie $T \subseteq \mathcal{L}_0$ unentscheidbar ist. Dann ist sogar jede mit T_0 verträgliche Theorie T einer Sprache $\mathcal{L} \supseteq \mathcal{L}_0$ unentscheidbar, weil andernfalls auch die Theorie $T \cap \mathcal{L}_0$ entscheidbar wäre. Mit T_0 ist jedes konsistente $T_1 \supseteq T_0$ ebenfalls streng unentscheidbar, denn ist T mit T_1 verträglich, dann auch mit T_0. Ferner ist dann auch jede Subtheorie von T_0 in $\mathcal{L}_0$ unentscheidbar, oder T_0 ist *erblich unentscheidbar* in der Terminologie von [TMR]. Je schwächer eine streng unentscheidbare Theorie, um so größer ihr Anwendungsbereich. Das wird noch deutlich werden durch

Satz 5.4. ([TMR]). Q *ist streng unentscheidbar.*

Beweis. Sei $T' := T + \mathsf{Q}$ konsistent. T' ist wegen der endlichen Axiomatisierbarkeit von Q endliche Erweiterung von T. Wäre T entscheidbar, gilt dasselbe nach Lemma 5.3 auch für T'. Also ist T' nach Satz 4.2 in Q und damit in sich selbst repräsentierbar, was das Nichtrepräsentierbarkeitslemma aber ausschließt. ❑

Satz 5.5 (Unentscheidbarkeitssatz von Church). *Die Menge $\mathsf{Taut}_{\mathcal{L}}$ aller tautologischen Aussagen ist für $\mathcal{L} \supseteq \mathcal{L}_{ar}$ unentscheidbar.*

Beweis. $\mathsf{Taut}_{\mathcal{L}}$ ist mit Q sicher verträglich, also unentscheidbar nach Satz 5.4. ❑

Dieses Resultat läßt sich durch Interpretation unschwer auf die Sprache mit einer zweistelligen Relation und damit auf alle Expansionen dieser Sprache übertragen, siehe **6.6**, sowie überhaupt auf alle Sprachen mit Ausnahme derjenigen, die nur einstellige Prädikatensymbole und höchstens ein einstelliges Funktionssymbol enthalten. Für deren Tautologien gibt es tatsächlich auch Entscheidungsverfahren.

Nach Satz 5.4 ist speziell $Th\mathcal{N}$ unentscheidbar. Ebenso jede Subtheorie von $Th\mathcal{N}$, z.B. die Peano-Arithmetik PA, sowie deren Subtheorien und auch alle konsistenten Erweiterungen von PA. Denn diese sind mit Q alle verträglich. $Th\mathcal{N}$ ist nicht einmal axiomatisierbar, weil eine axiomatisierbare vollständige Theorie doch entscheidbar ist. Weitere Folgerungen über unentscheidbare Theorien werden in **6.6** gezogen.

Neben Unentscheidbarkeitsresultaten, die formalisierte Theorien betreffen, lassen sich auf ähnliche Weise auch zahlreiche spezielle Ergebnisse dieser Art gewinnen, etwa negative Lösungen von Wortproblemen aller Art, von Halteproblemen usw. (siehe z.B. [Ob], [Ba]). Von diesen war vielleicht die spektakulärste die Lösung des 10. Hilbertschen Problems: Gibt es einen Algorithmus, welcher für jedes Polynom $p(\vec{x})$ mit ganzzahligen Koeffizienten entscheidet, ob die diophantische Gleichung $p(\vec{x}) = 0$ ganzzahlig lösbar ist? Die Antwort ist nein, wie Matiyasevich 1970 bewies.

Wir skizzieren kurz den Beweisgang. Es genügt zu zeigen, daß es keinen Algorithmus für die Lösbarkeit aller diophantischen Gleichungen in $\mathbb{N}$ gibt. Denn nach einem bekannten Satz von Lagrange ist jede natürliche Zahl Summe von vier Quadraten ganzer Zahlen. Folglich ist $p(\vec{x}) = 0$ in $\mathbb{N}$ genau dann lösbar, wenn in $\mathbb{Z}$ die Gleichung $p(u_1^2 + v_1^2 + w_1^2 + z_1^2, \dots, u_n^2 + v_n^2 + w_n^2 + z_n^2) = 0$ lösbar ist. Könnte man also über die Lösbarkeit diophantischer Gleichungen in $\mathbb{Z}$ entscheiden, so auch über das entsprechende Problem in $\mathbb{N}$. Zum letzteren beachte man zunächst, daß die Frage der Lösbarkeit von $p(\vec{x}) = 0$ in natürlichen Zahlen gleichwertig ist zur Lösbarkeit einer diophantischen Gleichung, d.h. einer Gleichung $s(\vec{x}) = t(\vec{x})$ aus $\mathcal{L}_{ar}$, indem man alle mit einem Minuszeichen versehenen Glieder von $p(x)$ „auf die andere Seite bringt“. Hilberts Problem reduziert sich so offenbar auf die Frage nach einem Entscheidungsalgorithmus für das Problem $\mathcal{N} \vDash \exists\vec{x}\delta(\vec{x})$, wobei $\delta(\vec{x})$ alle diophantischen Gleichungen aus $\mathcal{L}_{ar}$ durchläuft.

Die negative Lösung des Hilbertschen Problems folgt leicht aus dem viel weitergehenden Satz 5.6, der eine überraschende Verbindung zwischen Zahlen- und Rekursionstheorie herstellt und z.B. in [Mat] ausführlich bewiesen wird. Dieser Satz ist ein Paradebeispiel dafür, daß gewisse Fragen zu Ergebnissen führen können, die in ihrer Bedeutung weit über die einer Antwort auf die ursprüngliche Frage hinausreichen.

Satz 5.6. *Ein arithmetisches Prädikat P ist diophantisch dann und nur dann, wenn P rekursiv aufzählbar ist.*

Um den Beweis wenigstens anzudeuten, sei das diophantische Prädikat $P \subseteq \mathbb{N}^n$ definiert durch $P\vec{a} \Leftrightarrow \mathcal{N} \vDash \exists\vec{y}\delta^{\mathcal{N}}(\underline{\vec{a}}, \vec{y})$, mit der Gleichung $\delta(\vec{x}, \vec{y})$. Die definierende Formel für P ist Σ_1, also ist P nach Übung 1 in **6.3** rekursiv aufzählbar. Dies ist sozusagen die triviale Richtung der Behauptung. Die Umkehrung – jedes r.a. Prädikat ist diophantisch – kann ihres Umfangs wegen hier nicht ausgeführt werden. Zahlreiche arithmetische Prädikate und Funktionen müssen durch trickreiche Überlegungen als diophantisch nachgewiesen werden, darunter das dreistellige Prädikat '$a^b = c$', das diesem Nachweis lange widerstanden hatte. Dieser Satz ergibt leicht das

Korollar 5.7. (a) *Das zehnte Hilbertsche Problem hat eine negative Antwort.* (b) *Für jede axiomatisierbare Theorie $T \supseteq \mathsf{Q}$, speziell für $T = \mathsf{PA}$, gibt es eine unlösbare diophantische Gleichung, deren Unlösbarkeit in T unbeweisbar ist.*

Beweis. bwb_{Q} ist nach **6.2** r.a. Gemäß Satz 5.6 existiert daher eine diophantische Gleichung $\delta(x, \vec{y})$ mit $(*)$ $bwb_{\mathsf{Q}}(n) \Leftrightarrow \mathcal{N} \vDash \exists\vec{y}\,\delta(\underline{n}, \vec{y})$. Wir behaupten, schon für die Schar $\exists\vec{y}\,\delta(\underline{n}, \vec{y})$ diophantischer Aussagen $(n = 0, 1, \dots)$ gibt es kein Entscheidungsverfahren. Sonst wäre $\{n \in \mathbb{N} \mid \mathcal{N} \vDash \exists\vec{y}\,\delta(\underline{n}, \vec{y})\}$ rekursiv, und damit gemäß $(*)$ auch bwb_{Q} im Widerspruch zu Satz 5.4. Das beweist (a). Wäre die Unlösbarkeit jeder unlösbaren diophantischen Gleichung $\delta(\vec{x})$ in T beweisbar, so wäre entweder $\vdash_T \neg\exists\vec{x}\delta(\vec{x})$ (falls $\delta(\vec{x})$ unlösbar ist) oder $\vdash_T \exists\vec{x}\delta(\vec{x})$, wegen der Σ_1-Vollständigkeit von T. Weil die Sätze von T r.a. sind, hätte man so eine Entscheidungsprozedur für die Lösbarkeit diophantischer Gleichungen vor sich, im Widerspruch zu (a). ❏

Satz 5.6 kann noch weiter verschärft werden. Der gesamte Beweis ist nämlich in PA ausführbar. Man erhält so folgendes Theorem, dessen Name von **M**atiyasevich, **R**obinson, **D**avis und **P**utnam herrührt, die alle wesentliche Beiträge zur Lösung des 10. Hilbertschen Problems lieferten. Wir werden es seines langwierigen Beweises wegen nicht benutzen, obwohl manches damit vereinfacht werden könnte.

MRDP-Theorem. *Zu jeder Σ_1-Formel α gibt es schon eine $\exists$-Formel α' aus $\mathcal{L}_{ar}$ mit $\alpha \equiv_{\mathsf{PA}} \alpha'$. Dabei ist α' o.B.d.A. von der Gestalt $\exists\vec{x}\, s = t$.*

Bemerkung. Die Fermatsche Vermutung $(*)$ $(\forall x\, y\, z \neq 0)(\forall n{>}2)\, x^n + y^n \neq z^n$ ist eine Π_1-Aussage, weil $(x, y) \mapsto x^y$ nach Satz 4.5 Δ_1 ist. Sie ist also ein Kandidat für eine von PA unabhängige Aussage. Es wäre interessant zu erfahren, ob der kürzlich vorgelegte oder ein anderer Beweis dieser Vermutung auch in PA ausführbar ist. Ein Nachweis, daß dies nicht der Fall ist, wäre kaum weniger sensationell als die Lösung des Problems selbst. Weil PA schon für Π_1-Formeln ω-unvollständig ist (Seite 196), könnte es sogar sein, daß $\vdash_{\mathsf{PA}} (\forall x\forall y\forall z \neq 0)\, x^{\underline{n}} + y^{\underline{n}} \neq z^{\underline{n}}$ für alle $n > 2$, obwohl $(*)$ in PA nicht beweisbar ist.

Übungen

1. Man zeige, eine ω-unvollständige Theorie in $\mathcal{L}_{ar}$ hat eine konsistente, aber ω-inkonsistente Erweiterung.

2. Sei T vollständig. Man zeige die Gleichwertigkeit von

   (i) T ist streng unentscheidbar, (ii) T ist erblich unentscheidbar.

3. Sei Δ eine endliche Liste expliziter Definitionen neuer Symbole mittels derjenigen von $\mathcal{L}$. Man zeige, mit T ist auch $T + \Delta$ entscheidbar (es genügt zu fordern Δ ist r.a., damit $\varphi^{rd} \in \mathcal{L}$ für $\varphi \in T + \Delta$ wohldefiniert ist).

4. Man konstruiere eine rekursive Funktion f mit nichtrekursivem $ran\, f$.

6.6 Übertragung durch Interpretation

Interpretierbarkeit ist ein mächtiges Werkzeug, um nebst modelltheoretischen Eigenschaften auch Unentscheidbarkeits- ebenso wie Entscheidbarkeitsresultate von einer Theorie auf die andere zu übertragen. Wir behandeln die beiden wichtigsten Konzepte, die (relative) Interpretierbarkeit nach Tarski und die Modellinterpretierbarkeit nach Rabin. Alle hier betrachteten Theorien seien konsistent.

Sei $\mathtt{P}$ ein 1-stelliges Prädikatensymbol. Die $\mathtt{P}$-*Relativierte* $\varphi^{\mathtt{P}}$ der Formel φ entsteht aus φ durch Ersetzung aller Subformeln der Gestalt $\forall x\alpha$ durch $\forall x(\mathtt{P}x \to \alpha)$, d.h. $(\forall x\varphi)^{\mathtt{P}} = \forall x(\mathtt{P}x \to \varphi^{\mathtt{P}})$. Hieraus folgt leicht $(\exists x\varphi)^{\mathtt{P}} \equiv \exists x(\mathtt{P}x \wedge \varphi^{\mathtt{P}})$. Für quantorenfreies φ ist definitionsgemäß $\varphi^{\mathtt{P}} = \varphi$.

Beispiel. $(\forall x\exists y\, y = \mathtt{S}x)^{\mathtt{P}} = \forall x[\mathtt{P}x \to \neg\forall y(\mathtt{P}y \to y \neq \mathtt{S}x)]$. Diese Formel ist logisch äquivalent zu $\forall x(\mathtt{P}x \to \exists y(\mathtt{P}y \wedge y = \mathtt{S}x))$ und diese wiederum zu $\forall x(\mathtt{P}x \to \mathtt{PS}x)$.

Definition. $T_0 \subseteq \mathcal{L}_0$ heiße *interpretierbar* in $T \subseteq \mathcal{L}$ (wobei die Signatur von T_0 der Einfachheit halber endlich sei), wenn es eine Liste Δ von in T legitimen expliziten Definitionen der in T nicht vorkommenden Symbole von T_0 und eines neuen Prädikatensymbols $\mathtt{P}$ gibt mit $T_0^{\mathtt{P}} \subseteq T^{\Delta}$. Dabei sei stets $X^{\mathtt{P}} := \{\alpha^{\mathtt{P}} \mid \alpha \in X\}$ und $T^{\Delta} := T + \Delta$, eine Theorie in $\mathcal{L}^{\Delta}$, der Δ-Expansion von $\mathcal{L}$ (Signatur $L_0 \cup L \cup \{\mathtt{P}\}$).

Diese technisch etwas komplizierte Definition soll nur zum Ausdruck bringen, dass die Begriffe von T_0 in T „verstanden werden“ und alles was in T_0 bewiesen werden kann auch in T beweisbar ist. Interpretierbarkeit verallgemeinert den Begriff der Subtheorie: T_0 ist trivial interpretierbar in $T \supseteq T_0$, mit $\Delta = \{\mathtt{P}x \leftrightarrow x = x\}$. In diesem Falle ist $\alpha^{\mathtt{P}}$ zu α logisch äquivalent.

CA bezeichne die Menge aller sogenannten *Abschlußaxiome* $\exists x\mathtt{P}x$ $\big(\equiv (\exists x\, x = x)^{\mathtt{P}}\big)$, $\mathtt{P}c$ $\big(\equiv (\exists x\, x = c)^{\mathtt{P}}\big)$ und $\forall\vec{x}\,(\bigwedge_{i=i}^{n} \mathtt{P}x_i \to \mathtt{P}f\vec{x})$ $\big(\equiv (\forall\vec{x}\,\exists y\, y = f\vec{x})^{\mathtt{P}}\big)$ für $c, f \in L_0$. Offenbar ist *CA* eine endliche Teilmenge von $T_0^{\mathtt{P}}$ und damit auch von T^{Δ}. Auch ist *CA* ist bis auf Äquivalenz eine Menge der Gestalt $E^{\mathtt{P}}$ für ein endliches $E \subseteq \mathit{Taut}_{\mathcal{L}_0}$. Die *CA*-Axiome garantieren, daß für jedes $\mathcal{B} \vDash T^{\Delta}$ eine $\mathcal{L}_0$-Struktur $\mathcal{A} = \mathcal{B}_{\Delta}$ mit dem Träger $A = \mathtt{P}^{\mathcal{B}}$ und den auf A eingeschränkten, durch Δ definierten Relationen und Operationen wohldefiniert ist. $\mathcal{A}$ ist Substruktur des $\mathcal{L}_0$-Redukts von $\mathcal{B}$.

Lemma 6.1. *Sei $\mathcal{B} \vDash CA$. Dann gilt $\mathcal{B}_{\Delta} \vDash \alpha \Leftrightarrow \mathcal{B} \vDash \alpha^{\mathtt{P}}$, für alle Aussagen $\alpha \in \mathcal{L}_0^0$.*

Beweis. Sei $\mathcal{A} := \mathcal{B}_{\Delta}$. Induktiv über $\varphi \in \mathcal{L}_0$ zeigen wir $(\mathcal{A}, w) \vDash \varphi \Leftrightarrow (\mathcal{B}, w) \vDash \varphi^{\mathtt{P}}$, für beliebiges $w\colon \mathit{Var} \to A$, wovon das Lemma nur der Spezialfall $\varphi \in \mathcal{L}_0^0$ ist. Die Behauptung ist klar für Primformeln α wegen $\alpha^{\mathtt{P}} = \alpha$. Die Induktionsschritte über $\wedge, \neg$ verlaufen routinemäßig und der Induktionsschritt über $\forall$ ergibt sich wie folgt:

$$\begin{aligned}(\mathcal{A},w)\vDash\forall x\varphi &\Leftrightarrow (\mathcal{A},w_x^a)\vDash\varphi \text{ für alle } a\in A\\ &\Leftrightarrow (\mathcal{B},w_x^a)\vDash\varphi^{\mathsf{P}} \text{ für alle } a\in A \quad \text{(Induktionsannahme)}\\ &\Leftrightarrow (\mathcal{B},w_x^a)\vDash \mathsf{P}x\to\varphi^{\mathsf{P}} \text{ für alle } a\in B \quad (\text{weil } A=\mathsf{P}^{\mathcal{B}})\\ &\Leftrightarrow (\mathcal{B},w)\vDash\forall x(\mathsf{P}x\to\varphi^{\mathsf{P}})=(\forall x\varphi)^{\mathsf{P}}. \quad \square\end{aligned}$$

Ist T_0 durch X_0 axiomatisiert, genügt es in obiger Definition statt $T_0^{\mathsf{P}}\subseteq T^{\Delta}$ nur $X_0^{\mathsf{P}}\cup CA\subseteq T^{\Delta}$ zu fordern. Dies ist sehr wichtig und folgt unmittelbar aus

$$(*)\qquad X\vdash\alpha\Rightarrow X^{\mathsf{P}}\cup CA\vdash\alpha^{\mathsf{P}}, \text{ für alle } X,\alpha\subseteq\mathcal{L}_0^0.$$

Zum Nachweis von $(*)$ sei $X\vdash\alpha$ und $\mathcal{B}\vDash X^{\mathsf{P}}, CA$, also $\mathcal{B}_\Delta\vDash X$ nach dem Lemma, daher $\mathcal{B}_\Delta\vDash\alpha$ und somit $\mathcal{B}\vDash\alpha^{\mathsf{P}}$. Weil $\mathcal{B}$ beliebig war, ist $X^{\mathsf{P}}\cup CA\vdash\alpha^{\mathsf{P}}$.

Satz 6.2. *Ist T_0 in T interpretierbar, so ist mit T_0 auch T streng unentscheidbar.*

Beweis. Sei T_1 $(\subseteq\mathcal{L})$ mit T verträglich. Dann ist mit $T+T_1$ auch die Theorie $(T+T_1)^{\Delta}$ konsistent. Nun ist $S:=\{\alpha\in\mathcal{L}_0^0\mid\alpha^{\mathsf{P}}\in T_1^{\Delta}+CA\}$ eine Theorie; denn $S\vdash\alpha$ impliziert $T_1^{\Delta}+CA\supseteq S^{\mathsf{P}}\cup CA\vdash\alpha^{\mathsf{P}}$ nach $(*)$ und folglich $\alpha^{\mathsf{P}}\in T_1^{\Delta}+CA$. Mit $\mathcal{B}\vDash(T+T_1)^{\Delta}\supseteq T^{\Delta},T_1^{\Delta},CA$ ist wegen $T_0^{\mathsf{P}}\subseteq T^{\Delta}$ gewiß auch $\mathcal{B}\vDash T_0^{\mathsf{P}},S^{\mathsf{P}}$. Mithin $\mathcal{B}_\Delta\vDash T_0,S$ nach dem Lemma, d.h. S ist mit T_0 verträglich, also unentscheidbar. Wäre T_1 entscheidbar, dann auch T_1^{Δ} (Übung 3 in **6.5**), daher auch $T_1^{\Delta}+CA$ (Lemma 5.3) und folglich also auch S. Dies aber ist ein Widerspruch. $\square$

Beispiel. Q ist in der Theorie T_d der diskret geordneten Ringe interpretierbar, d.h. der geordneten Ringe $\mathcal{R}=(R,0,+,\times,<)$ mit kleinstem positiven Element e, das aber kein Einselement von $\mathcal{R}$ sein muß. Man wähle folgende Definitionen für $\mathsf{P},\mathsf{S},\cdot$:

$$\mathsf{P}x\leftrightarrow x\geqslant 0\wedge x\times e=e\times x\wedge\forall y\exists z\; z\times e=y\times x,$$

$$y=\mathsf{S}x\leftrightarrow y=x+e,\quad z=x\cdot y\leftrightarrow z\times e=x\times y\vee\forall u(u\times e\neq x\times y\wedge z=x).$$

Aus diesen Formeln ist e wegen $x=e\leftrightarrow 0<x\wedge\forall y(0<y\to x\leqslant y)$ eliminierbar. $0,+$ bleiben unverändert. Mit etwas geduldigem Rechnen beweist man in T_d^{Δ} alle auf P relativierten Axiome von Q und auch sämtliche Abschlußaxiome.

Damit erweist sich T_d als streng unentscheidbar. Q ist zwar nicht direkt interpretierbar in der Theorie T_R der Ringe oder der Theorie T_K der Körper, wohl aber in einer gewissen endlichen Erweiterung von T_K (Julia Robinson), womit deren Subtheorien T_K und T_R sich als unentscheidbar erweisen. Dasselbe gilt auch für die Gruppentheorie T_G (Tarski). Keine dieser Theorien ist jedoch streng unentscheidbar. Sie haben sämtlich entscheidbare mathematisch hochinteressante Erweiterungen, etwa die entscheidbare Theorie der abelschen Gruppen (Wanda Szmielew).

Q und sogar PA sind auch in ZFC interpretierbar: sei $\mathsf{P}x\leftrightarrow x\in\omega$, und $\mathsf{S},+,\cdot$ werden so erklärt, daß ihre Einschränkungen auf ω mit den wie üblich definierten Operationen übereinstimmen. Insbesondere S durch $y=\mathsf{S}x\leftrightarrow y=x\cup\{x\}$. Damit ergibt sich sofort die Unentscheidbarkeit und nebenher auch die Unvollständigkeit von ZFC – die Konsistenz von ZFC natürlich vorausgesetzt. Q ist auch in bemerkenswert schwachen Subtheorien von ZFC interpretierbar, etwa in der Theorie $T_\in$ mit folgenden drei Axiomen in $\mathcal{L}_\in$ [7], einem extrem schwachen Fragment dieser Art, das wie Q dann auch streng unentscheidbar ist:

$$
\begin{array}{ll}
\exists x \forall y\, y \notin x & (\emptyset \text{ existiert}),\\
\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \to x = y) & (\text{Extensionalität}),\\
\forall x \forall y \exists z \forall u (u \in z \leftrightarrow u \in x \vee u = y) & (x \cup \{y\} \text{ existiert}).
\end{array}
$$

Damit ist auch die Menge der Tautologien in einer binären Relation unentscheidbar, sogar ohne Gleichheit in der Sprache, denn $=$ läßt sich in $T_\in$ vermittels der expliziten Definition $x = y \leftrightarrow \forall z (z \in x \leftrightarrow z \in y)$ offenbar eliminieren.

Q ist offenbar trivial interpretierbar in $Th\mathcal{N}$, und $Th\mathcal{N}$ wiederum in $Th\mathcal{Z}$ mit $\mathcal{Z} = (\mathbb{Z}, 0, 1, +, \cdot)$. Dies ergibt sich aus dem Satz von Lagrange. Also ist $Th\mathcal{Z}$ streng, und damit jede Subtheorie schlechthin unentscheidbar, z.B. die Theorie der kommutativen Ringe. $Th\mathcal{N}$ und $Th\mathcal{Z}$ sind gleich kompliziert, denn $Th\mathcal{Z}$ ist (auf unterschiedliche Weisen) auch in $Th\mathcal{N}$ interpretierbar, z.B. indem nichtnegative ganze Zahlen durch die geraden, negative durch die ungeraden natürlichen Zahlen vertreten werden. Bemerkenswert ist auch die wechselseitige Interpretierbarkeit von PA und $\mathsf{ZFC}_{\mathrm{fin}}$. Dies ist die Theorie der endlichen Mengen; sie entsteht aus ZFC durch Ersetzung des Unendlichkeitsaxioms durch das Axiom ‘alle Mengen sind endlich’.

Wir erläutern jetzt eine strengere Form der Interpretierbarkeit, lassen der Einfachheit halber aber gewisse Feinheiten weg. Seien $\boldsymbol{K}_0$ und $\boldsymbol{K}$ Klassen von $\mathcal{L}_0$- bzw. $\mathcal{L}$-Strukturen. In **2.5** wurde erklärt $Th\boldsymbol{K} = \{\alpha \in \mathcal{L}^0 \mid \boldsymbol{K} \vDash \alpha\}$. Sei Δ eine Definitionsliste der $\mathcal{L}_0$-Symbole und eines Prädikatensymbols P, sowie $\mathcal{L}^\Delta$, CA und $\mathcal{B}_\Delta$ für $\mathcal{B} \vDash CA$ definiert wie vorhin. $\mathcal{A}^\Delta$ bezeichne die Δ-Expansion von $\mathcal{A} \in \boldsymbol{K}$, so daß $\mathcal{A}$ das $\mathcal{L}$-Redukt von $\mathcal{A}^\Delta$ ist. Schließlich sei $\boldsymbol{K}_\gamma := \{\mathcal{A}^\Delta \mid \mathcal{A} \in \boldsymbol{K},\ \mathcal{A}^\Delta \vDash \gamma\}$ für eine Aussage γ aus $\mathcal{L}^\Delta$. Zu jeder Aussage $\beta \in \mathcal{L}^\Delta$ läßt sich wie in **2.6** beschrieben eine Reduzierte $\beta^{rd} \in \mathcal{L}$ effektiv konstruieren derart, daß

(0) $\mathcal{A}^\Delta \vDash \beta \;\Leftrightarrow\; \mathcal{A} \vDash \beta^{rd}$, für alle $\mathcal{A} \in \boldsymbol{K}$.

Definition. $\boldsymbol{K}_0$ heiße *modellinterpretierbar* in $\boldsymbol{K}$ (oder auch $Th\boldsymbol{K}_0$ in $Th\boldsymbol{K}$), wenn für eine passende Definitionsliste Δ und eine passende Aussage $\gamma \in \mathcal{L}^\Delta$

(1) $\boldsymbol{K}_\gamma \vDash CA$ und $\mathcal{B}_\Delta \in \boldsymbol{K}_0$ für alle $\mathcal{B} \in \boldsymbol{K}_\gamma$,

(2) Für jedes $\mathcal{A} \in \boldsymbol{K}_0$ gibt es ein $\mathcal{B} \in \boldsymbol{K}_\gamma$ mit $\mathcal{A} \simeq \mathcal{B}_\Delta$.

Satz 6.3. *Sei $\boldsymbol{K}_0$ modellinterpretierbar in $\boldsymbol{K}$. Dann ist mit der Theorie $Th\boldsymbol{K}_0$ auch die Theorie $Th\boldsymbol{K}$ unentscheidbar.*

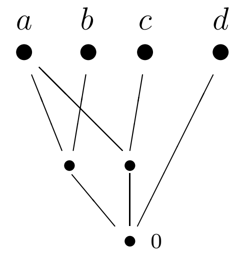
[7] Behauptet in [TMR]. Der langwierige Beweis wird ausgeführt in [Mo, S. 283-290].

Beweis. Es genügt zu zeigen $(*)$ $\boldsymbol{K}_0 \vDash \alpha \;\Leftrightarrow\; \boldsymbol{K} \vDash \gamma^{rd} \to \alpha^{\mathtt{P}\,rd}$. Denn ein Entscheidungsverfahren für $Th\boldsymbol{K}$ hätte wegen $(*)$ ein solches für $Th\boldsymbol{K}_0$ zur Folge. $\Rightarrow$: Sei $\boldsymbol{K}_0 \vDash \alpha$, $\mathcal{A} \in \boldsymbol{K}$ und $\mathcal{A} \vDash \gamma^{rd}$, also $\mathcal{A}^{\Delta} \vDash \gamma$ nach (0), d.h. $\mathcal{B} := \mathcal{A}^{\Delta} \in \boldsymbol{K}_{\gamma}$. Nach (1) ist $\mathcal{B}_{\Delta} \in \boldsymbol{K}_0$, also $\mathcal{B}_{\Delta} \vDash \alpha$, d.h. $\mathcal{B} \vDash \alpha^{\mathtt{P}}$ nach Lemma 6.1, daher $\mathcal{A} \vDash \alpha^{\mathtt{P}\,rd}$. Das zeigt $\boldsymbol{K} \vDash \gamma^{rd} \to \alpha^{\mathtt{P}\,rd}$. $\Leftarrow$ folgt indirekt: Sei $\boldsymbol{K}_0 \nvDash \alpha$, etwa $\mathcal{A} \in \boldsymbol{K}_0$, $\mathcal{A} \nvDash \alpha$. Sei $\mathcal{B} \in \boldsymbol{K}_{\gamma}$ gemäß (2) gewählt, also $\mathcal{B} \vDash \gamma$ und $\mathcal{B}_{\Delta} \simeq \mathcal{A} \nvDash \alpha$. Daher $\mathcal{B} \nvDash \alpha^{\mathtt{P}}$ (Lemma 6.1). Somit $\mathcal{B} \nvDash \gamma \to \alpha^{\mathtt{P}}$, d.h. $\mathcal{B}' \nvDash \gamma^{rd} \to \alpha^{\mathtt{P}\,rd}$ für das $\mathcal{L}$-Redukt $\mathcal{B}'$ $(\in \boldsymbol{K})$ von $\mathcal{B}$. ❑

Beispiel. Sei $\boldsymbol{K}_0$ die Klasse aller Graphen (A, R) und $\boldsymbol{K}$ die Klasse aller einfachen Graphen (B, S), d.h. S ist irreflexiv und symmetrisch. Wir zeigen, $\boldsymbol{K}_0$ ist in $\boldsymbol{K}$ modellinterpretierbar, d.h. beliebige Graphen können durch einfache vollständig kodiert werden. Die Figur zeigt links ein $\mathcal{A} \in \boldsymbol{K}_0$ mit aRa, aRb, bRa und bRc,

und rechts den $\mathcal{A}$ gemäß (2) entsprechenden einfachen Graphen $\mathcal{B}$ mit $\mathcal{A} \simeq \mathcal{B}_{\Delta}$, die „Kodierungs-Struktur“ von $\mathcal{A}$. Grob gesagt, wurden zu A neue Punkte so hinzugefügt, daß $\mathcal{A}$ durch $\mathcal{B}$ vollständig beschrieben wird. Dick gezeichnete Punkte in $\mathcal{B}$ vertreten die Punkte aus A. Es sind dies genau die Punkte aus $\mathtt{P}^{\mathcal{B}}$. Sie heißen der Anschaulichkeit halber „alte“ Punkte. Alle übrigen Punkte aus B heißen die „neuen“ Punkte. Die explizite Definition von $\mathtt{P}$ lautet entsprechend der Figur $\mathcal{B}$ informell '$\mathtt{P}x \;\Leftrightarrow\; x$ ist zu zwei oder drei Endpunkten benachbart' (Endpunkte sind solche, in denen nur eine Kante endet). Die zu zwei Endpunkten benachbarten alten Punkte kennzeichnen die irreflexen, die zu drei Endpunkten benachbarten die reflexiven Punkte von $\mathcal{A}$. Führt in $\mathcal{A}$ eine Kante von x nach y so wird in $\mathcal{B}$ ein neuer Punkt zwischen x und y gesetzt, wobei für Richtungsanzeige ein weiterer Punkt benutzt wird, der offenbar dann entbehrlich ist, wenn zugleich auch eine Kante von y nach x zurückführt. Informell lautet die Definition für R dann '$xRy \;\Leftrightarrow\; x, y \in \mathtt{P}^{\mathcal{B}}$ und entweder $x = y$ und x ist zu drei Endpunkten benachbart, oder es gibt genau einen neuen Punkt z mit $xSzSy$, oder es gibt genau zwei neue Punkte u, v mit $xSuSvSy$ und uSy'. Und γ lautet '$\mathtt{P}^{\mathcal{B}} \neq \emptyset$ und jeder neue Punkt ist entweder Endpunkt oder zu einem oder zwei alten Punkten benachbart'. Es liegt auf der Hand, daß mit diesen Definitionen von $\mathtt{P}$ und R und diesem γ die Bedingungen (1) und (2) erfüllt sind. Man beachte, CA enthält hier lediglich die Formel $\exists x \mathtt{P}x$.

Im Beispiel ist $Th\boldsymbol{K}_0$ die logische Theorie einer binären Relation, die wie schon festgestellt unentscheidbar ist. Demnach ist auch die Theorie aller einfachen Graphen unentscheidbar. Dies kann man nun wieder nutzen, um die Theorie SL der Halbverbände als unentscheidbar nachzuweisen. Daraus folgt nach Satz 5.4 dasselbe für die Theorie SG der Halbgruppen, denn SL ist endliche Erweiterung von SG. Analog zum letzten Beispiel genügt es, für einen einfachen Graphen (A, S) den Kodierungshalbverband $(B, \circ)$ anzugeben. Die Figur links zeigt das Ordnungsdiagramm von B für $A = \{a, b, c, d\}$ und $S = \{\{a, b\}\{ac\}\}$, S verstanden als Kantenmenge, siehe **1.5**. Die alten Punkte sind gerade die maximalen Punkte von B. Nach Konstruktion hat B ein kleinstes Element 0 und ist von der Länge 3, d.h. es gibt bzgl. $<$ höchstens drei aufeinanderfolgende Punkte in B. Das muß die geforderte Aussage γ jetzt zum Ausdruck bringen. Diese Interpretationsmethode ist sehr flexibel. Sie macht z.B. hinreichend deutlich, daß die Theorie der Halbverbände nicht weniger kompliziert ist als die aller gerichteten Graphen schlechthin.



Dieselbe Konstruktion zeigt, daß auch die Theorie der *endlichen* einfachen Graphen in der Theorie der endlichen Halbverbände modellinterpretierbar ist. Weil erstere unentscheibare ist – für eine Beweisskizze siehe z.B. [RZ] – gilt dies auch für die Theorie FSG der endlichen Halbgruppen. Setzt man über die maximalen Elemente der Figur noch ein Einselement, entstehen jeweils endliche Verbände. Also ist auch deren Theorie unentscheidbar. Das gilt auch für die Theorie der Klasse FPO aller endlichen partiellen Ordnungen, denn man braucht zur Beschreibung von (A, S) nur die partielle Ordnung von B.

Auch positive Resultate sind übertragbar. Viele Theorien sind z.B. in der Theorie der Bäume interpretierbar (siehe [KR]), insbesondere in der monadischen Theorie 2. Stufe der Bäume. Die Entscheidbarkeit der letzteren ist besonders weittragend. Für Einzelheiten und Literaturhinweise sei etwa auf [Ba, C2] verwiesen.

Übungen

1. Man zeige (informell), PA ist interpretierbar in ZFC.

2. Man zeige, ist T_1 in T_2 modellinterpretierbar, so ist T_1 in einer gewissen endlichen Erweiterung von T_2 (relativ) interpretierbar.

3. Man zeige, FPO ist modellinterpretierbar in der Klasse FDL aller endlichen distributiven Verbände. Mit $Th\,\mathsf{FPO}$ ist also auch $Th\,\mathsf{FDL}$ unentscheidbar. Diese Übung ist weitaus schwieriger als die obige Konstruktion: Man identifiziere die Elemente von $(E, <) \in \mathsf{FPO}$ mit den $\cap$-irreduziblen Elementen von $\mathcal{A} \in \mathsf{FDL}$ und benutze, daß die (partielle) Ordnung der $\cap$-irreduziblen Elemente von $\mathcal{A} \in \mathsf{FDL}$ die Struktur von $\mathcal{A}$ vollständig bestimmt und deren Ordnung auch beliebig vorgeschrieben werden kann.

6.7 Die arithmetische Hierarchie

Wir wollen abschließend noch etwas mehr über die Komplexität von Prädikaten von $\mathbb{N}$ sagen, speziell von Teilmengen. Die Menge der Gödelzahlen aller in $\mathcal{N}$ gültigen Aussagen ist Beispiel einer recht einfach definierten nichtarithmetischen Teilmenge von $\mathbb{N}$; sie besitzt nach Satz 5.2 keine Definition in $\mathcal{L}_{ar}$ [8]. Aber auch relativ einfach definierte arithmetische Mengen und Prädikate können rekursionstheoretisch hochgradig kompliziert sein. Es ist nützlich, diese nach der Komplexität der definierenden Formeln zu klassifizieren. Das Resultat ist die *arithmetische Hierarchie*, auch die *Kleene-Mostowski-Hierarchie der 1. Stufe* genannt. Die folgende Erklärung setzt die Definition der in **6.3** mittels der Δ_0-Formeln definierten Σ_1- und Π_1-Formeln und der Σ_1-, Π_1- und Δ_1-Prädikate in natürlicher Weise fort.

Definition. Eine Σ_{n+1}-Formel sei eine solche der Gestalt $\exists\vec{x}\alpha(\vec{x},\vec{y})$, wobei α eine Π_n-Formel ($\in \mathcal{L}_{ar}$) ist; analog heiße $\forall\vec{x}\beta(\vec{x},\vec{y})$ eine Π_{n+1}-Formel, falls β eine Σ_n-Formel ist. Dabei seien $\vec{x},\vec{y}$ beliebige Variablentupel, möglicherweise auch leer. Ein Σ_n-*Prädikat* bzw. Π_n-*Prädikat* ist ein durch eine Σ_n-Formel bzw. eine Π_n-Formel definiertes arithmetisches Prädikat P. Ist P zugleich Σ_n und Π_n (d.h. ein Σ_n- und ein Π_n-Prädikat), heißt P ein Δ_n-Prädikat oder kurz P *ist* Δ_n. Es bezeichnen Σ_n, Π_n und Δ_n die Mengen der Σ_n-, Π_n- bzw. der Δ_n-Prädikate, so daß $\Delta_n = \Sigma_n \cap \Pi_n$.

Eine Σ_n-Formel ist also eine pränexe Formel mit n abwechselnden Quantorenblöcken, deren Kern eine Δ_0-Formel ist. Es ist bequem, die Σ_n- und Π_n-Formeln unter logischer Äquivalenz abzuschließen und sich folgender Redeweise zu bedienen: α *ist* Σ_n oder Π_n. Dies soll heißen, α ist zu einer *originalen* Σ_n- bzw. Π_n-Formel äquivalent. Weil $\exists\vec{x}\varphi \equiv \forall\vec{x}\varphi \equiv \varphi$ für $var\,\vec{x} \cap var\,\varphi = \emptyset$, ist jede Σ_n- oder Π_n-Formel sowohl Σ_{n+1} als auch Π_{n+1}. Also ist $\Sigma_n, \Pi_n \subseteq \Delta_{n+1}$. Damit ergibt sich das folgende Inklusionsdiagramm, wobei wir an dieser Stelle nur erwähnen, daß alle durch Striche symbolisierten Inklusionen echte sind:

$$\begin{array}{ccccccccccc}
 & & & & \Sigma_1 & & & & \Sigma_2 & & & & \Sigma_3 & & \\
 & & & / & & \backslash & & / & & \backslash & & / & & & \\
\Delta_0 & — & \Delta_1 & & & & \Delta_2 & & & & \Delta_3 & & & & \cdots \\
 & & & \backslash & & / & & \backslash & & / & & \backslash & & & \\
 & & & & \Pi_1 & & & & \Pi_2 & & & & \Pi_3 & &
\end{array}$$

Σ_1-, Π_1- und Δ_1-Prädikate sind uns schon begegnet. So sind Lösbarkeitsbehauptungen diophantischer Gleichungen Σ_1, und Unlösbarkeitsbehauptungen demnach Π_1.

---

[8] Sie ist erst in der Arithmetik 2. Stufe definierbar, die nebst Zahlenvariablen auch solche für Mengen natürlicher Zahlen hat. Für eine „approximative" elementare Definition siehe Übung 3.

Weiter unten geben wir ein Beispiel eines Π_2-Prädikats. Σ_n-definierbare Funktionen sind immer auch Δ_n, wie eine leichte Verallgemeinerung von Lemma 3.4 zeigt. Man vereinbart als bloße Redeweise, daß Σ_n- bzw. Π_n-*Aussagen* 0-stellige Σ_n- bzw. Π_n-Prädikate definieren. In diesem Sinne ist z.B. die Konsistenz von PA ein Π_1-Prädikat.

Jede Formel ist zu einer Σ_n- oder einer Π_n-Formel für passendes n äquivalent; man braucht sie ja nur in pränexe Normalform zu bringen und die Quantoren zu Blöcken mit gleichen Quantoren zusammenzufassen. Bei neueren Untersuchungen betrachtet man z.B. oft auch Δ_0- oder Σ_n- oder Π_n-*Induktion*, d.h. man schränkt das Induktionsschema IS auf die jeweiligen Formelklassen ein. Ein wichtiges Beispiel ist $I\Delta_0$.

Wie in **6.4** schon gezeigt wurde, sind die Σ_1-Prädikate die rekursiv aufzählbaren, die Π_1- Prädikate sind deren Komplemente, und die Δ_1-Prädikate sind genau die rekursiven. Damit haben wir eine rein rekursionstheoretische Veranschaulichung von Σ_1, Π_1 und Δ_1 vor uns. Das unterstreicht die Bedeutung der arithmetischen Hierarchie, die im übrigen ziemlich stabil ist gegenüber leichten Veränderungen der Definition von Δ_0. Wegen Satz 5.6 könnte man z.B. mit einem Δ_0 starten, das aus allen in $\mathcal{N}$ polynomial (oder gleichwertig, quantorenfrei) definierbaren Relationen besteht. In einigen Darstellungen wird ein System von Formeln effektiv aufgezählt (und mit Δ_0 bezeichnet), durch welche bereits alle p.r. Prädikate in $\mathcal{N}$ definiert werden. **7.1** wird zeigen, wie sich ein solches System von Formeln gewinnen läßt. Zwischen diesen und den Δ_0-Formeln liegen noch viele r.a. Formelklassen, deren zugehörige Prädikate rekursiv sind und die für Theorie und Praxis der Berechenbarkeit bedeutsam sind, z.B. die in der Kapitel-Einleitung erwähnte Klasse der elementaren Funktionen.

Allerdings läßt sich nach Bemerkung 2 in **6.4** kein Formelsystem in $\mathcal{L}_{ar}$ effektiv aufzählen, durch das bereits alle rekursiven, d.h. alle Δ_1-Prädikate definiert werden, so daß die Definition der arithmetischen Hierarchie nicht in übersehbarer Weise mit einer repräsentativen „Menge von Δ_1-Formeln“ beginnen kann.

Ähnlich wie für den Fall $n = 1$ zeigt man, daß eine Konjunktion oder Disjunktion von Σ_n-Formeln wieder zu einer solchen äquivalent ist, und Analoges gilt für Π_n-Formeln. Auch ist die Negation einer Σ_n-Formel zu einer Π_n-Formel äquivalent und umgekehrt. Denn dies ist richtig für $n = 1$, womit der Induktionsanfang einer leicht ausführbaren Induktion über n bereits klar ist. Das Komplement eines Σ_n-Prädikats ist daher ein Π_n-Prädikat und umgekehrt. Daraus folgt leicht, daß Δ_n unter allen erwähnten Operationen abgeschlossen ist.

Durch Quantorenkompression (Übung 1 in **6.3**) erhält man noch eine etwas einfachere Darstellung der Quantorenblöcke. Es lassen sich die abwechselnd aufeinanderfolgenden $\exists$- und $\forall$-Blöcke zu jeweils einem Quantor zusammenziehen:

Satz 7.1. *Jedes Σ_n-Prädikat ist durch eine Formel der Gestalt $\exists x_1 \forall x_2 \cdots Q_n x_n \alpha$ mit einer Δ_0-Formel α definiert; dabei ist Q_n der $\forall$- bzw. der $\exists$-Quantor, je nachdem ob n gerade oder ungerade ist. Entsprechend ist ein Π_n-Prädikat durch eine Formel der Gestalt $\forall x_1 \exists x_2 \cdots Q_n x_n \alpha$ definiert.*

Beweis. Für Σ_1-Prädikate und Π_1-Prädikate zeigt dies Übung 1 in **6.3**. Für den allgemeinen Fall beachte man $Q\vec{x}\varphi \equiv_{\mathcal{N}} Qy(Qx_1{<}y)\dots(Qx_n{<}y)\varphi$. Dabei ist Q der $\forall$- oder $\exists$-Quantor. Es genügt daher zu zeigen, daß die Klassen Σ_n und Π_n unter beschränkter Quantifizierung abgeschlossen sind. Dies behauptet Übung 1. ❑

Häufig wird auch die Paarkodierung verwendet um Quantoren zu komprimieren. Es ist nicht immer einfach, die genaue Position eines vorgegebenen Prädikats in der arithmetischen Hierarchie zu bestimmen. Besser gesagt, dies erfordert wie jedes anspruchsvolle Spiel hinreichendes Training. Es ist z.B. nicht schwer zu sehen, daß die ω-Konsistenz der Form nach Π_3 ist. Aber erst Satz 7.5.2 wird zeigen, daß sie *echt* Π_3 ist, d.h. nicht Σ_n, Π_n oder Δ_n für $n < 3$. Der Übersichtlichkeit halber benutzen wir im folgenden einfacheren Beispiel an einer Stelle die Churchsche These, die jedoch mit etwas Rekursionstheorie in erprobter Weise wieder eliminiert werden kann.

Beispiel. Sei $\mathcal{L}_r$ die Menge der $\alpha \in \mathcal{L}^1_{ar}$, welche in Q die rekursiven Teilmengen von $\mathbb{N}$ repräsentieren. Dazu gehören z.B. alle Δ_0-Formeln aus $\mathcal{L}^1_{ar}$. Weil $\mathbb{N}$ und $\emptyset$ rekursiv sind, gehören zu $\mathcal{L}_r$ auch alle Aussagen α aus $\mathsf{Q}^* := \mathsf{Q} \cup \{\alpha \mid \neg\alpha \in \mathsf{Q}\}$. Denn die $\alpha \in \mathsf{Q}$ repräsentieren trivialerweise $\mathbb{N}$ und die α mit $\neg\alpha \in \mathsf{Q}$ gerade $\emptyset$. Offenbar ist $\mathsf{Q}^* = \mathcal{L}_r \cap \mathcal{L}^0_{ar}$. Wir zeigen nun, $\mathcal{L}_r$ ist arithmetisch; genauer, eine echte Π_2-Menge, also weder rekursiv noch rekursiv aufzählbar. Gemäß Definition ist

$$\alpha \in \mathcal{L}_r \Leftrightarrow \alpha \in \mathcal{L}^1_{ar} \;\&\; \forall n \exists \Phi[\Phi \text{ ist Beweis für } \alpha(\underline{n}) \text{ oder für } \neg\alpha(\underline{n})].$$

Daraus gewinnt man unschwer eine Definition von $\dot{\mathcal{L}}_r$ durch eine Π_2-Formel $\varphi(x)$. In der Tat, sei das p.r. Prädikat '$a \in \dot{\mathcal{L}}^1_{ar}$' etwa durch die Σ_1-Formel $\lambda_1(x)$ definiert. Mit $\mathrm{sb} = \mathrm{sb}_{\boldsymbol{v}_0}$ setze man dann

$$\varphi(x,y) := \lambda_1(x) \wedge \forall y \exists u[\mathtt{bew}_{\mathsf{Q}}(u, \mathrm{sb}(x,y)) \vee \mathtt{bew}_{\mathsf{Q}}(u, \tilde{\neg}\,\mathrm{sb}(u,y))],$$

genauer, die Reduzierte dieser Formel in $\mathcal{L}_{ar}$ nach Elimination der vorkommenden p.r. Funktionsterme mit weiteren $\exists$-Quantoren innerhalb der eckigen Klammern. φ beschreibt also eine Σ_1-Formel. Damit ist $\forall y \varphi(x,y)$ Π_2, d.h. $\dot{\mathcal{L}}_r$ ist eine Π_2-Menge. Sie ist nicht Σ_1, weil $\mathcal{L}_r$ nach Bemerkung 2 in **6.4** nicht r.a. ist. Sie ist aber auch nicht Π_1. Angenommen dies sei der Fall. Dann ist $\mathsf{Q}^* = \mathcal{L}_r \cap \mathcal{L}^0_{ar}$ ebenfalls Π_1, denn $\mathcal{L}_r$ ist Δ_1. Nun ist Q^* sicher r.a. und damit Σ_1, also ist Q^* nach Satz 4.5 rekursiv. Wir erhalten daraus aber ein Entscheidungsverfahren für Q, also einen Widerspruch: Sei $\alpha \in \mathcal{L}^0_{ar}$ gegeben. Ist $\alpha \notin \mathsf{Q}^*$, so auch $\alpha \notin \mathsf{Q}$; ist $\alpha \in \mathsf{Q}^*$, setzen wir die Aufzählungsmaschine für Q in Aktion und warten, bis α oder $\neg\alpha$ erscheint.

In Vorbereitung auf **7.1** zeigen wir abschließend, daß die Σ_1-Formeln in nicht zu schwachen Theorien durch spezielle Formeln vertreten werden können. In Teil (a) von Satz 7.2 unten könnte PA auch durch die schwächere Theorie N ersetzt werden.

Definition. *Modifizierte* Σ_1-Formeln seien wie folgt erklärt:

(i) $\mathtt{S}x = y$, $x+y=z$ und $x\cdot y=z$ sind modifizierte Σ_1-Formeln, wobei x,y,z paarweise verschiedene Variablen bezeichnen,

(ii) Mit α,β sind auch $\alpha\wedge\beta$, $\alpha\vee\beta$, $\alpha\,\frac{0}{x}$ und $\alpha\,\frac{y}{x}$ ($y\notin gbd\,\alpha$, Primterm-Substitution) modifizierte Σ_1-Formeln, sowie $\exists x\alpha$ und $(\forall x{<}y)\alpha$ für $y\notin var\,\alpha$.

Satz 7.2. (a) *Jede originale* Σ_1*-Formel ist in* PA *zu einer modifizierten* Σ_1*-Formel äquivalent.* (b) *Jede modifizierte* Σ_1*-Formel ist modulo* PA *eine* Σ_1*-Formel.*

Beweis. (a): Es genügt offenbar, dies für alle Δ_0-Formeln zu beweisen, denn auch die Menge aller modifizierten Σ_1-Formeln ist unter $\exists$-Quantifikation abgeschlossen. Weil $s=t \equiv \exists x(x=s\wedge x=t)$ mit $x\notin var\,s,t$ genügt es, Primformeln der Gestalt $x=t$ zu betrachten. Wir beweisen (a) für Formeln $x=t$ durch Terminduktion. Ist t ein Primterm, ergibt sich die Behauptung offensichtlich aus $x=0 \equiv (x=y)\,\frac{0}{y}$, sowie $x=y \equiv_{\mathsf{PA}} (x+z=y)\,\frac{0}{z}$. Induktion über $\mathtt{S},+,\cdot$ folgt aus $x=\mathtt{S}t \equiv \exists y(x=\mathtt{S}y\wedge y=t)$, $x=s+t \equiv \exists yz(x=y+z\wedge y=s\wedge z=t)$, und ganz analog verläuft der Beweis für $\cdot$. $x\neq y \equiv_{\mathsf{PA}} \exists uz(\mathtt{S}u=z\wedge(x+z=y\vee y+z=x))$ und $s\neq t \equiv \exists yz(x\neq y\wedge x=s\wedge y=t)$ zeigen, daß (a) für alle Literale gilt. Nach Übung 4 in **6.3** genügt es daher, die Induktionsschritte über $\wedge,\vee,(\forall x{\leqslant}t)$ und $(\exists x{\leqslant}t)$ auszuführen. Für $\wedge,\vee$ ist dies klar. Im übrigen beachte man $(\forall x{\leqslant}t)\alpha \equiv_{\mathsf{PA}} \exists y(y=t\wedge(\forall x{<}y)\alpha\wedge\alpha\,\frac{y}{x})$ mit $y\notin var\,\alpha$, sowie $(\exists x{\leqslant}t)\alpha \equiv_{\mathsf{PA}} \exists xyz(x+y=z\wedge z=t\wedge\alpha)$ mit $y,z\notin var\,\alpha,t$. (b) erfordert lediglich den Nachweis, daß für eine Σ_1-Formel $\exists z\varphi$ auch die Formel $(\forall x{<}y)\exists z\varphi$ zu einer Σ_1-Formel in PA äquivalent ist. Dieser Nachweis ist leicht, denn das Schrankenschema (Übung 3(c) Seite 86) zeigt $(\forall y{<}x)\exists z\varphi \equiv_{\mathsf{PA}} \exists u(\forall y{<}x)(\exists z{<}u)\varphi$. ❑

Übungen

1. Man zeige (induktiv über n) Σ_n, Π_n und damit auch Δ_n sind abgeschlossen unter beschränkter Quantifizierung (eine beschränkt quantifizierte Σ_n-Formel ist aber zu einer Σ_n-Formel i.a. nicht nicht mehr logisch äquivalent).

2. Man bestätige $\Delta_0\subset\Delta_1\subset\Sigma_1,\Pi_1$, womit gezeigt ist, daß diese vier Klassen arithmetischer Prädikate paarweise verschieden sind.

3. Es sei $Tr_n = \{\alpha\in\mathcal{L}^0_{ar}\mid\mathcal{N}\vDash\alpha \;\&\; \mathrm{qr}\,\alpha\leqslant n\}$, so daß $Th\mathcal{N} = \bigcup_{n\in\mathbb{N}} Tr_n$. Nach Satz 5.2 ist $Th\mathcal{N}$ selbst nicht arithmetisch. Man beweise, Tr_n ist für jedes n arithmetisch; genauer, Tr_n ist höchstens Δ_{n+1}. In diesem Sinne darf man sagen, $Th\mathcal{N}$ sei arithmetisch approximierbar.

Kapitel 7

Zur Theorie der Selbstreferenz

Vorliegendes Kapitel kann nur einen Einblick in eine im letzten Viertel des 20. Jahrhunderts weit entwickelte Theorie geben. Wir beweisen den zweiten Unvollständigkeitssatz von Gödel, Löbs Theorem und andere mit der Selbstreferenz zusammenhängende Ergebnisse. Einige weiterführende Resultate werden anhand von geeigneten Anwendungen nur erläutert. Mit Selbstreferenz ist grob gesagt die Möglichkeit gemeint, in einer Theorie T über T selbst oder verwandte Theorien zu reden. Diese Thematik ist insgesamt von hohem erkenntnistheoretischen Wert.

Der Nachweis der sogenannten Ableitungsbedingungen für PA und andere Theorien in **7.1** ist der Berg, den zunächst erstiegen werden muß. Wer sich jedoch mit einem Überfliegen von **7.1** zufriedengibt, kann gleich in **7.2** beginnen; von dort ab sind nur Früchte zu ernten. Allerdings entgeht einem dabei ein wirkliches Abenteuer, die Verschmelzung von Logik und Zahlentheorie bei der Analyse von PA.

Schon Gödel hat versucht, den Begriff 'beweisbar' durch einen modalen Operator im Rahmen des Modalsystems S4 zu interpretieren. Dieser Ansatz widerspiegelt seine eigenen Resultate aber nicht adäquat. Erst nachdem die Modallogik nach 1970 einen hinreichend hohen Entwicklungsstand erreicht hatte, konnte ein entsprechendes Programm erfolgreich ausgeführt werden. Als geeignetes Instrument hat sich dafür ein mit G (oder GL) bezeichnete Modallogik erwiesen. Deren in **7.3** vorgestellte Kripke-Semantik ist ein handliches Werkzeug zur Entscheidung über die Zugehörigkeit modaler Formeln zu G, so daß dieses Modalsystem gut beherrschbar ist.

Ein Hauptresultat der modallogischen Behandlung der Selbstreferenz ist der Solovaysche Vollständigkeitssatz 4.2. Glücklicherweise gehört dieser Satz ebenso wie die Vollständigkeit der Kripke-Semantik für G zu jener Art von Hilfsmitteln, die man bequem anwenden kann, ohne ihre Beweise im Detail zu kennen. Es gibt einige Erweiterungen von G, die für die Analyse anderer Begriffe oder ihren Vergleich nützlich sind, z.B. die in **7.5** behandelte bimodale Expansion von G oder die Interpretierbarkeitslogik, siehe [Vi]. Einen umfassenden Überblick gibt [Bu, Chapter VII].

7.1 Die Ableitungsbedingungen

Der zweite Unvollständigkeitssatz 2.2 besagt etwas vereinfacht, daß für eine hinreichend strenge konsistente axiomatisierbare Theorie $T \subseteq \mathcal{L}$ nicht $\vdash_T \mathtt{Con}_T$ gelten kann, wobei $\mathtt{Con}_T$ eine Aussage ist, welche die Konsistenz von T in $\mathcal{L}$ zum Ausdruck bringt. In populärer Formulierung: *Ist T konsistent, so ist dies im Rahmen von T nicht beweisbar.* Darüber hinaus ist die kursiv gesetzte Aussage unter gewissen Bedingungen in T schon formulierbar und dort auch beweisbar.

Diese Bedingungen sind die sogenannten *Ableitungsbedingungen* $D1$ - $D3$ unten, die durchaus ein eigenes Interesse verdienen. Ihre Formulierung setzt die Gödelisierbarkeit von T voraus, was die Auszeichnung einer Folge $\underline{0}, \underline{1}, \ldots$ von Grundtermen einschließt, siehe Seite 194. $\mathtt{bew}_T(y,x)$ sei wie in **6.5** eine Σ_1–Formel, die das rekursive Prädikat bew_T in T repräsentiere. $\mathtt{bwb}_T(\ulcorner\alpha\urcorner)$ $(= \exists y\, \mathtt{bew}_T(y, \ulcorner\alpha\urcorner))$ werde durch $\Box\alpha$ abgekürzt und gelesen als 'box α' oder 'beweisbar α', weil es sich um die Formalisierung des Sachverhalts '$\vdash_T \alpha$' in T handelt. $\Box\alpha$ ist stets eine Aussage, auch wenn α freie Variablen enthält. Später wird gelegentlich auch $\Box(x)$ für $\mathtt{bwb}_T(x)$ geschrieben. In **7.4** wird $\Box$ überdies als modallogischer Operator in Erscheinung treten.

Wir erklären ferner $\Diamond\alpha := \neg\Box\neg\alpha$ für $\alpha \in \mathcal{L}^0$. Diese Aussage darf man lesen als α *ist verträglich mit T*, denn sie ist die Formalisierung von '$\nvdash_T \neg\alpha$', oder gleichwertig '$T + \alpha$ ist konsistent'. Schließlich wird $\mathtt{Con}_T$ in natürlicher Weise durch

$$\mathtt{Con}_T := \neg\Box\bot \;\big(= \neg\, \mathtt{bwb}_T(\ulcorner\bot\urcorner)\big)$$

definiert. Dabei sei $\bot$ eine beliebige Kontradiktion, etwa $0 \neq 0$, wobei hier 0 dasselbe bedeute wie $\underline{0}$. Es wird sich gleich herausstellen, daß $\mathtt{Con}_T$ modulo T unabhängig ist von der Wahl von $\bot$. Die erwähnten Ableitungsbedingungen lauten wie folgt:

$$D1\colon \vdash_T \alpha \Rightarrow\ \vdash_T \Box\alpha, \qquad D2\colon \vdash_T \Box\alpha \wedge \Box(\alpha \to \beta) \to \Box\beta, \qquad D3\colon \vdash_T \Box\alpha \to \Box\Box\alpha.$$

Dabei durchlaufen α, β alle Aussagen aus $\mathcal{L}^0$. Oft formuliert man $D2$ auch in der gleichwertigen Form $\Box(\alpha \to \beta) \vdash_T \Box\alpha \to \Box\beta$ oder $D3$ in der Form $\Box\alpha \vdash_T \Box\Box\alpha$. Die Ableitungsbedingungen stammen in der angegebenen Gestalt von Löb, wurden in etwas anderer Gestalt aber schon in [HB] formuliert.

Eine unmittelbare Folgerung aus $D1, D2$ ist $D0$: $\alpha \vdash_T \beta \ \Rightarrow\ \Box\alpha \vdash_T \Box\beta$. Denn $\alpha \vdash_T \beta \ \Rightarrow \vdash_T \alpha \to \beta \ \Rightarrow \vdash_T \Box(\alpha \to \beta) \ \Rightarrow \vdash_T \Box\alpha \to \Box\beta$. Daraus folgt sofort, daß „unter $\Box$" äquivalent ersetzt werden kann. Die Wahl von $\bot$ in $\mathtt{Con}_T$ ist also frei.

Bemerkung 1. Jeder nur $d1$: $\vdash_T \alpha \ \Rightarrow \vdash_T \partial\alpha$ und $d2$: $\partial(\alpha \to \beta) \vdash_T \partial\alpha \to \partial\beta$ erfüllende Operator $\partial\colon \mathcal{L} \to \mathcal{L}$ erfüllt demnach immer auch $d0$: $\alpha \vdash_T \beta \ \Rightarrow\ \partial\alpha \vdash_T \partial\beta$. Er erfüllt zudem $d\wedge$: $\partial(\alpha \wedge \beta) \equiv_T \partial\alpha \wedge \partial\beta$. Denn $\alpha \wedge \beta \vdash_T \alpha, \beta$, also $\partial(\alpha \wedge \beta) \vdash_T \partial\alpha, \partial\beta \vdash_T \partial\alpha \wedge \partial\beta$ nach $d0$. Ähnlich folgt $\partial\alpha \wedge \partial\beta \vdash_T \partial(\alpha \wedge \beta)$ mit $d0$, $d2$ leicht aus $\alpha \vdash_T \beta \to \alpha \wedge \beta$. Aus $d0$ schließt man unmittelbar auf $d00$: $\alpha \equiv_T \beta \Rightarrow \partial\alpha \equiv_T \partial\beta$.

Während $D2$ und $D3$ Aussagen(schemata) in T darstellen, ist $D1$ metatheoretischer Natur. $D1$ folgt unmittelbar aus der Repräsentierbarkeit von bew_T und gilt daher schon für relativ schwache Theorien wie z.B. $T = \mathsf{Q}$. Die Umkehrung von $D1$,

$$D1^*:\quad \vdash_T \Box\alpha \;\Rightarrow \vdash_T \alpha, \text{ für alle } \alpha \in \mathcal{L}^0$$

muß nicht richtig sein, gilt aber für alle ω-konsistenten axiomatischen Erweiterungen $T \supseteq \mathsf{Q}$ wie z.B. $T = \mathsf{PA}$. Denn aus $\nvdash_T \alpha$ folgt $\vdash_T \neg\,\mathtt{bew}_T(\underline{n}, \ulcorner\alpha\urcorner)$ für alle n nach Satz 6.4.2, also $\nvdash_T \exists y\,\mathtt{bew}_T(y, \ulcorner\alpha\urcorner) = \Box\alpha$ wegen der ω-Konsistenz von T.

Anders als $D1$ sind $D2$ und $D3$ nicht so billig zu haben. T muß direkt oder indirekt (via Gödelisierung) über das Beweisen in T reden können. $D3$ ist nichts anderes als *die in T formalisierte Bedingung* $D1$, während $D2$ den Sachverhalt

$$(0)\qquad bwb_T(\dot\alpha)\ \&\ bwb_T((\alpha\to\beta)^{\boldsymbol{\cdot}}) \Rightarrow bwb_T(\dot\beta)\quad \text{(siehe (7) Seite 178).}$$

in der Theorie T reflektiert. Wir behaupten nun, $D2$ ist eine Konsequenz von

$$(1)\quad \vdash_T \mathtt{bew}_T(u,x) \wedge \mathtt{bew}_T(v, x \mathbin{\tilde{\to}} y) \to \mathtt{bew}_T(u * v * \langle y\rangle, y).$$

Dabei müssen die in (1) auftretenden p.r. Funktionen in T natürlich definiert sein, was bloße Repräsentierbarkeit erheblich verschärft: $f \in \mathbf{F}_n$ heiße *definierbar in T* (bzgl. einer gegebenen Termfolge $(\underline{n})_{n\in\mathbb{N}}$), wenn es eine Formel $\delta(\vec{x}, y) \in \mathcal{L}$ gibt mit

$$\text{(a)}\ \vdash_T \delta(\underline{\vec{a}}, \underline{f\vec{a}}) \text{ für alle } \vec{a} \in \mathbb{N}^n, \qquad \text{(b)}\ \vdash_T \forall\vec{x}\,\exists! y\,\delta(\vec{x}, y).$$

Daher kann f mit einem ebenfalls mit f bezeichneten Symbol in T definitorisch eingeführt werden, also $\vdash_T y = f\vec{x} \leftrightarrow \delta(\vec{x}, y)$. Dabei unterscheiden wir von nun an nicht mehr zwischen T und definitorischen Erweiterungen von T. Damit erhält man leicht $\vdash_T f\underline{\vec{a}} = \underline{f\vec{a}}$, etwa $\vdash_T \underline{a \mathbin{\tilde{\to}} b} = \underline{a} \mathbin{\tilde{\to}} \underline{b}$. Mit $\ulcorner\alpha\urcorner$, $\ulcorner\beta\urcorner$ für x, y liefert (1) dann

$$\mathtt{bew}_T(u, \ulcorner\alpha\urcorner) \wedge \mathtt{bew}_T(v, \ulcorner\alpha\to\beta\urcorner) \vdash_T \mathtt{bew}_T(u * v * \langle\ulcorner\beta\urcorner\rangle, \ulcorner\beta\urcorner)$$

(weil $\ulcorner\alpha\to\beta\urcorner = \underline{\dot\alpha \mathbin{\tilde{\to}} \dot\beta} = \underline{\dot\alpha} \mathbin{\tilde{\to}} \underline{\dot\beta} = \ulcorner\alpha\urcorner \mathbin{\tilde{\to}} \ulcorner\beta\urcorner$). Partikularisierung liefert schließlich $D2$. Die eigentliche Arbeit – der Nachweis von (1) – steht aber noch aus.

Der Übersicht halber begrenzen wir alle folgenden Ausführungen auf die Theorien ZFC und PA, die bei fast allen grundlagentheoretischen Fragestellungen im Blickpunkt des Interesses stehen. ZFC wird nur kurz diskutiert, weil der Nachweis von $D2$, $D3$ hier ungleich einfacher ist als für PA. So ist (1) und damit $D2$ deshalb klar, weil der naive Beweis von (0) für $T = \mathsf{ZFC}$ unschwer *in* ZFC formalisiert werden kann. Das schließt die Definierbarkeit aller dort erscheinenden arithmetischen Funktionen natürlich ein. Diese wurden in **6.1** aber definiert – setze z.B. $a * b = \emptyset$ falls nicht $a, b \in \omega$. Man gödelisiert $\mathcal{L}_\in$ nach dem Muster von **6.2** durch eine Primzahlexponenten-Kodierung, obwohl man dazu eigentlich nicht genötigt ist, weil in ZFC über üblich definierte endliche Folgen und damit über $\mathcal{L}_\in$-Formeln nahezu direkt geredet werden kann. Dies geschieht nur, um die Kohärenz mit den

Ausführungen in **6.2** zu wahren. Eine Formel $\varphi \in \mathcal{L}_\in$ wird so zum ω-Term $\ulcorner\varphi\urcorner$ in ZFC. $\mathcal{L}_{ar}$-Formeln identifizieren wir mit ihren Relativierten auf ω, den *arithmetischen* Formeln von $\mathcal{L}_\in$ wie z.B. $\mathtt{bew}_{\mathsf{ZFC}}(y,x)$ und $\mathtt{bwb}_{\mathsf{ZFC}}$ $\big(= (\exists y \in \omega)\,\mathtt{bew}_{\mathsf{ZFC}}(y,x)\big)$.

Sicher wird bew_{ZFC} nach Satz 6.4.2 in ZFC durch $\mathtt{bew}_{\mathsf{ZFC}}$ repräsentiert. Dieser Satz ist wie jeder Satz in diesem Buch ein Satz *in* ZFC. Damit ist der auf diesem beruhende Beweis von $D1$ (bishin zu Korollar 6.4.3) in ZFC gewiß ausführbar – denn wir haben ihn ja ausgeführt, wenn auch nur informell – und $D3$ ist bewiesen. Die Ableitungsbedingungen für ZFC folgen grob gesagt einfach daraus, daß die gewohnte Mathematik, speziell das Material von Kapitel **6** in ZFC formalisierbar ist.

Bei alledem braucht man keine typisch mengentheoretischen Konstruktionen wie z.B. ordinale Rekursion; man benötigt nur einfache kombinatorische Fakten. Das deutet darauf hin, daß die Beweise auch in hinreichend strengen arithmetischen Theorien ausführbar sind. Die Kodierung der $\mathcal{L}_{ar}$-Formeln in PA durch ihre Gödelterme wie auf Seite 191 ist nicht das Problem. Nur liegt z.B. die Definierbarkeit der Funktionen aus (1) und anderer relevanter Funktionen in PA nicht auf der Hand [1)]. Unser erstes Etappenziel ist daher der Nachweis, daß alle bisher in Erscheinung getretenen p.r. Funktionen sogar in folgendem Sinne beweisbar rekursiv sind:

Definition. Eine n-stellige rekursive Funktion f heiße Σ_1-*definierbar in* PA oder kurz *beweisbar rekursiv*, wenn es eine Σ_1-Formel $\delta_f(\vec{x}, y)$ gibt mit

(2) (a) $\mathcal{N} \vDash \delta_f(\underline{\vec{a}}, \underline{f\vec{a}})$ für alle $\vec{a} \in \mathbb{N}^n$, (b) $\vdash_{\mathsf{PA}} \forall\vec{x}\,\exists! y\,\delta_f(\vec{x}, y)$.

Wegen der Σ_1-Vollständigkeit von PA ist (a) gleichwertig mit $\vdash_{\mathsf{PA}} \delta_f(\underline{\vec{a}}, \underline{f\vec{a}})$, so daß f durch δ_f in PA tatsächlich explizit definiert wird. Wir zeigen dies sogleich für *alle* p.r. Funktionen, und zudem die Beweisbarkeit der entsprechenden Rekursionsgleichungen. Danach kann man in PA mit diesen Funktionen umgehen, als wären sie von Anfang an in der Sprache vorhanden. Erst diese grundlegende Tatsache rechtfertigt eine Identifikation der elementaren Zahlentheorie und Kombinatorik mit PA.

$D3$ erfordert darüber hinaus weitergehende Vorbereitungen. Wegen ihres Umfangs werden auch in guten Lehrbüchern nicht alle Beweisschritte dargeboten. Aber alle nachfolgend nur beschriebenen Beweisschritte können vom Leser mit ausreichender Geduld unschwer explizit ausgeführt werden. Man könnte sich das Leben durch die leider auch nicht einfach beweisbare gegenseitige Interpretierbarkeit von PA und $\mathsf{ZFC_{fin}}$ (Seite 202) erleichtern. Dann käme man weitgehend ohne Kodierung aus.

[1)] Gödel gab in [Go2] eine Liste von 45 p.r. Funktionen an, deren letzte χ_{bew} war. Er betrachtet dort in Anlehnung an [WR] eine arithmetische Theorie höherer Stufe. Daß Gödels Sätze auch in einer Arithmetik 1. Stufe gelten, wurde in [HB] erstmals nachgewiesen. Wie stark PA wirklich ist äußert sich unter anderem auch darin, daß in PA wesentliche Resultate der Metamathematik, etwa die relative Konsistenz von ZFC zu ZF bewiesen werden können.

Für einige Funktionen, darunter die $\boldsymbol{\beta}$-Funktion, ist deren Σ_1-Definierbarkeit in PA direkt beweisbar, Übung 1. Aber schon um die Definition der Exponentialfunktion in $\mathcal{N}$ durch δ_{exp} aus der Bemerkung 1 in **6.4** auch in PA als legitim zu erkennen, müssen Lemma 6.4.1 über die $\boldsymbol{\beta}$-Funktion und damit auch der Chinesische Restsatz *im Rahmen von* PA bewiesen werden. Schon die Formulierbarkeit dieser Aussagen in $\mathcal{L}_{ar}$ liegt nicht auf der Hand. Zwecks Überwindung dieser Hürde mögen vorübergehend c, d einstellige beweisbar rekursive Funktionen bezeichnen, die noch von weiteren Parametern abhängen dürfen. Ein solches c bestimmt für gegebenes n die Zahlenfolge $c_0, \ldots, c_n$ mit $c_\nu := c(\nu)$ für $\nu \leqslant n$. Mit der definierbaren Relation $\perp$ der Teilerfremdheit ist der Chinesische Restsatz in PA provisorisch dann wie folgt formulierbar: Für beliebige c, d wie oben verabredet gilt

$$(3)\ \vdash_{\mathsf{PA}} \forall n[(\forall n, i, j \leqslant n)(c_\nu < d_\nu \land (i \neq j \to d_i \perp d_j)) \to \exists a (\forall \nu \leqslant n)\, rest(a : d_\nu) = c_\nu]$$ [2].

Um den Beweis des Restsatzes auf Seite 189 in einen solchen von (3) zu verwandeln, benötigen wir für gegebenes beweisbar rekursives d den Term $\mathrm{kgV}\{d_\nu | \nu \leqslant n\}$. Dieser ist in PA Σ_1-definierbar weil d dies ist und Teilbarkeit Δ_0 ist, und zwar durch

$$\delta_f(x, y) := (\forall \nu \leqslant x) d_\nu \,|\, y \land (\forall z < y)(\exists \nu \leqslant x)\, d_\nu \nmid z \qquad (f : n \mapsto \mathrm{kgV}\{d_\nu | \nu \leqslant n\}).$$

Genauer, $\delta_f(x, y)$ beschreibt eine Σ_1-Formel, ähnlich wie δ_{exp} auf Seite 190. Weil $\mathcal{N} \vDash \delta_f(\underline{n}, \underline{\mathrm{kgV}\{d_\nu | \nu \leqslant n\}})$ für jedes n, gilt 2(a). Für $\beta(x, y) := (\forall \nu \leqslant x) d_\nu \,|\, y$ ergibt das Schema der Minimimalzahl (Übung 3 in **3.3**) sofort $\vdash_{\mathsf{PA}} \exists! y \delta_f(x, y)$, wenn zuvor nur $\vdash_{\mathsf{PA}} \exists y \beta(x, y)$ bewiesen wurde ('endlich viele Zahlen haben ein gemeinsames Vielfaches'). Das erfolgt induktiv über x. Klar ist $\vdash_{\mathsf{PA}} \exists y \beta(0, y)$. Den Beweis des Induktionsschritts $\exists y \beta(x, y) \vdash_{\mathsf{PA}} \exists y' \beta(\mathtt{S}x, y')$ führen wir informell: Sei $d_\nu \,|\, y$ für alle $\nu \leqslant x$. Dann gilt sicher $d_\nu \,|\, y \cdot d_{\mathtt{S}x}$ für alle $\nu \leqslant \mathtt{S}x$, d.h. $y' = y \cdot d_{\mathtt{S}x}$ ist eine geeignete Wahl. Also $\exists y' \beta(\mathtt{S}x, y')$. Das beweist 2(b). Damit erhält man schließlich den Beweis von (3), indem man konsequent dem Beweis des Restsatzes in **6.4** folgt, und mit der Schreibweise $\boldsymbol{\beta} st$ für $\boldsymbol{\beta}(s, t)$ alsdann folgende Version von Lemma 6.4.1:

$$(4)\quad \vdash_{\mathsf{PA}} \forall v \exists u (\forall \nu \leqslant v)\, c_\nu = \boldsymbol{\beta} u \nu, \quad \text{für jede beweisbar rekursive Funktion } c.$$

Satz 1.1. *Jede p.r. Funktion f ist beweisbar rekursiv. Darüber hinaus sind im Falle $f = \boldsymbol{Op}(g, h)$ auch die Rekursionsgleichungen für f in* PA *beweisbar.*

Beweis. Für die Anfangsfunktionen und $+, \cdot$ sind $\boldsymbol{v}_0 = 0$, $\boldsymbol{v}_1 = \mathtt{S}\boldsymbol{v}_0$, $\boldsymbol{v}_n = \boldsymbol{v}_\nu$, sowie $\boldsymbol{v}_2 = \boldsymbol{v}_0 + \boldsymbol{v}_1$ und $\boldsymbol{v}_2 = \boldsymbol{v}_0 \cdot \boldsymbol{v}_1$ definierende Σ_1-Formeln. (2) ist hier offensichtlich. Für $f = h[g_1, \ldots, g_m]$ sei $\delta_f(\vec{x}, y)$ die Formel $y = h(g_1\vec{x}, \ldots, g_m\vec{x})$ – genauer, deren Reduzierte $\exists \vec{y}\, (\bigwedge_i \delta_{g_i}(\vec{x}, y_i) \land \delta_h(\vec{y}, y))$ in $\mathcal{L}_{ar}$ – und auch hier ist (2) offensichtlich.

[2] Aus suggestiven Gründen bezeichnen jetzt gelegentlich auch $n, \nu, \ldots$ Variablen von $\mathcal{L}_{ar}$. Im Restsatz in **6.4** wird über endliche Zahlenfolgen quantifiziert. Dies kann in PA erst geschehen, *nachdem nachgewiesen wurde*, daß PA über endliche Zahlenfolgen zu reden imstande ist, daher die Benennung *provisorisch.* Die jetzigen Betrachtungen dienen u.a. diesem Ziel.

Etwas Geschick verlangt nur die Definition von δ_f für $f = \boldsymbol{Op}(g,h)$. Beachtet man, daß für die $\boldsymbol{\beta}$-Funktion die Formel `beta` aus **6.4** das Verlangte leistet, sei

$$(5)\quad \delta_f(\vec{x},y,z) := \exists u[\underbrace{\boldsymbol{\beta}u0 = g\vec{x} \wedge (\forall v{<}y)\boldsymbol{\beta}u\mathtt{S}v = h(\vec{x},v,\boldsymbol{\beta}uv) \wedge \boldsymbol{\beta}uy = z}_{\gamma(u,\vec{x},y,z)}].$$

Die Bedingung 2(a) $\mathcal{N} \vDash \delta_f(\underline{\vec{a}},\underline{b},\underline{f\vec{a}})$ überprüft man leicht durch (Meta-)Induktion über das Rekursionsargument b. Wir konzentrieren uns hier auf den Nachweis von 2(b). Die Eindeutigkeit folgt aus $\vdash_{\mathsf{PA}} \gamma(u,\vec{x},y,z) \wedge \gamma(u',\vec{x},y,z') \to z = z'$, was sich mit dem Blick auf (5) leicht induktiv über y ergibt. Auch $\vdash_{\mathsf{PA}} \exists z\delta_f(\vec{x},y,z)$ folgt induktiv über y. Für $y = 0$ beachte man $\vdash_{\mathsf{PA}} \exists u\boldsymbol{\beta}u0 = g\vec{x}$ gemäß (4); man nehme hier z.B. $c\colon v \to w$, definiert durch die Formel $v = 0 \wedge w = g\vec{x} \vee v \neq 0 \wedge w = 0$. Den Induktionsschritt $(*)$ $\exists z\delta_f(\vec{x},y,z) \vdash_{\mathsf{PA}} \exists z'\delta(\vec{x},\mathtt{S}y,z')$ beweisen wir wieder informell. Angenommen $\gamma(u,\vec{x},y,z)$, oder gleichwertig $\gamma(u,\vec{x},y,\boldsymbol{\beta}uy)$. Dann ist das durch

$$\varphi(v,w,u,\vec{x},y) := v \neq \mathtt{S}y \wedge w = \boldsymbol{\beta}uv \vee v = \mathtt{S}y \wedge w = h(\vec{x},v,\boldsymbol{\beta}uy)$$

definierte $c\colon v \mapsto w$ mit den Parametern $u,\vec{x},y$ beweisbar rekursiv. Nach (4) mit $\mathtt{S}y$ für v gibt es ein u' mit $\boldsymbol{\beta}u'v = c_v = \boldsymbol{\beta}uv$ für $v \leqslant y$ und $\boldsymbol{\beta}u'\mathtt{S}y = h(\vec{x},y,\boldsymbol{\beta}uz)$. Mit diesem u' und $z' = \boldsymbol{\beta}u'\mathtt{S}y$ erhält man dann $\gamma(u,\vec{x},\mathtt{S}y,z')$. und damit $\exists z'\delta_f(\vec{x},\mathtt{S}y,z')$. Das beweist $(*)$ und damit 2(b). Schließlich zeigen wir für $f = \boldsymbol{Op}(g,h)$ noch

$$\text{(a)} \vdash_{\mathsf{PA}} f(\vec{x},0) = g\vec{x}, \quad \text{(b)} \vdash_{\mathsf{PA}} f(\vec{x},\mathtt{S}y) = h(\vec{x},y,f(\vec{x},y)).$$

(a) gilt nach 2(b), weil (5) unschwer $\vdash_{\mathsf{PA}} \delta_f(\vec{x},0,g\vec{x})$ ergibt. Zum Nachweis von (b) zeigt man induktiv über y zuerst leicht $\gamma(u,\vec{x},y,z) \vdash_{\mathsf{PA}} (\forall v{\leqslant}y)f(\vec{x},\mathtt{S}v) = \boldsymbol{\beta}u\mathtt{S}v$. Hieraus ergibt sich $\gamma(u,\vec{x},y,z) \vdash_{\mathsf{PA}} \varphi := (\forall v{\leqslant}y)f(\vec{x},\mathtt{S}v) = h(\vec{x},v,f(\vec{x},v))$. Weil aber $\vdash_{\mathsf{PA}} \exists z\gamma(u,\vec{x},y,z)$, erhalten wir $\vdash_{\mathsf{PA}} \varphi$, was (b) offensichtlich umfaßt. ❑

Damit ist unser erstes Etappenziel erreicht. Wegen der Definierbarkeit ihrer charakteristischen Funktionen lassen sich die auf Seite 178 formulierten Eigenschaften der Prädikate bew_{PA} und bwb_{PA} nun auch im Rahmen von PA beweisen. Dazu sind nur die in der dortigen Bemerkung formulierten Eigenschaften von $*, \ell, \ldots$ auch in PA zu beweisen. Das ist ein kleines, dem Leser überlassenes Extraprogramm mit Einschluß des Beweises der eindeutigen Primzerlegung. Damit ist (1) für $T = \mathsf{PA}$ endlich bewiesen. (1) impliziert $D2$ und mit $\Box = \mathtt{bwb}_{\mathsf{PA}}$ darüber hinaus offenbar

$$(6)\quad \Box(x \,\tilde{\to}\, y) \vdash_{\mathsf{PA}} \Box(x) \to \Box(y).$$ [3]

Bemerkung 2. Nun lassen sich auch die formalisierten Gleichungen der Übung 4 in **6.4** in PA beweisen. (b) lautet nun z.B. $\vdash_{\mathsf{PA}} \mathrm{sb}_{\vec{x}}(\ulcorner\alpha\urcorner,\vec{x}) = \mathrm{sb}_{\vec{x}'}(\ulcorner\alpha\urcorner,\vec{x}\,')$ mit $\mathit{var}\,\vec{x}\,' = \mathit{frei}\,\alpha$. Damit ist $\vdash_{\mathsf{PA}} \mathrm{sb}_{\vec{x}}(\ulcorner\alpha\urcorner,\vec{x}) = \ulcorner\alpha\urcorner$ für $\alpha \in \mathcal{L}^0_{ar}$. (c) verdeutliche man sich an einem Sonderfall: $\mathrm{sb}_{xy}(\dot{\alpha},a,\mathtt{S}a) = \mathrm{sb}_x((\alpha\,\frac{\mathtt{S}x}{y})^{\cdot},a)$, formalisiert: $\mathrm{sb}_{x,y}(\ulcorner\alpha\urcorner,x,y)\,\frac{\mathtt{S}x}{y} = \mathrm{sb}_x(\ulcorner\alpha\,\frac{\mathtt{S}x}{y}\urcorner,x)$. Für den Spezialfall im Beispiel Seite 193 benötigt man dazu lediglich $\vdash_{\mathsf{PA}} \text{zf}\,\mathtt{S}x = \tilde{\mathtt{S}}\,\text{zf}\,x$.

[3] $\Box$ könnte hier sogar $\mathtt{bwb}_T$ für eine beliebige axiomatisierbare gödelisierbare Theorie bedeuten.

Nunmehr sind wir für den Beweis von $D3$ gerüstet. Nützlich hierfür ist folgende

Definition. Für $\varphi = \varphi(\vec{x})$ sei $\square[\varphi] := \square(\mathrm{sb}_{\vec{x}}(\ulcorner\varphi\urcorner, \vec{x}))$ $\big(= \mathtt{bwb}_{\mathsf{PA}}(\mathrm{sb}_{\vec{x}}(\ulcorner\varphi\urcorner, \vec{x}))\big)$.

Nach Bemerkung 2 ist $\vdash_{\mathsf{PA}} \mathrm{sb}_{\vec{x}}(\ulcorner\varphi\urcorner, \vec{x}) = \mathrm{sb}_{\vec{x}'}(\ulcorner\varphi\urcorner, \vec{x}')$ mit $var\,\vec{x}' = frei\,\varphi$. Daher darf man o.B.d.A. von $frei\,\square[\varphi] = frei\,\varphi$ ausgehen. Für Aussagen α darf $\square[\alpha]$ mit $\square\alpha$ identifiziert werden, weil $\vdash_{\mathsf{PA}} \mathrm{sb}_{\vec{x}}(\ulcorner\alpha\urcorner, \vec{x}) = \ulcorner\alpha\urcorner$. Durch $\vdash_{\mathsf{PA}} \square[\varphi]$, gleichwertig $\vdash_{\mathsf{PA}} \forall\vec{x}\,\square[\varphi]$, wird in PA der Sachverhalt '$\vdash_{\mathsf{PA}} \varphi(\underline{\vec{a}})$ für alle $\vec{a}$', also die Existenz einer *Schar von Beweisen* in einer einzigen Aussage formuliert. Dies kann wegen der ω-Unvollständigkeit von PA weniger sein als $\vdash_{\mathsf{PA}} \square\varphi$ (oder gleichwertig $\vdash_{\mathsf{PA}} \square\forall\vec{x}\varphi$).

Beispiel. Sei $\varphi(x, y) = \mathtt{S}x = y$. Wir zeigen $\varphi \vdash_{\mathsf{PA}} \square[\varphi]$, gleichwertig $\vdash_{\mathsf{PA}} (\square[\varphi])\,\frac{\mathtt{S}x}{y}$, wobei o.B.d.A. $x, y \notin gbd\,\square(x)$. Weil $\vdash_{\mathsf{PA}} \mathrm{sb}_{x,y}(\ulcorner\varphi\urcorner, x, \mathtt{S}x) = \mathrm{sb}_x(\ulcorner\varphi\,\frac{\mathtt{S}x}{y}\urcorner, x)$ (Bemerkung 2), genügt es $\vdash_{\mathsf{PA}} \square[\mathtt{S}x = \mathtt{S}x]$ zu verifizieren. Dies reflektiert in PA 'für beliebiges n ist $\vdash_{\mathsf{PA}} \mathtt{S}\underline{n} = \mathtt{S}\underline{n}$'. Wir begründen $\vdash_{\mathsf{PA}} \square[\alpha]$ für $\alpha(x) := \mathtt{S}x = \mathtt{S}x$ im Detail: Man betrachte die p.r. Funktion $\tilde{\alpha}\colon n \mapsto \mathrm{sb}_x(\dot{\alpha}, n)$ (die Gödelzahl von $\alpha(\underline{n})$). Nach Axiom $\Lambda 9$ ist $\langle\tilde{\alpha}(n)\rangle$ ein simpler arithmetisierter Beweis für $\tilde{\alpha}(n)$. In PA formalisiert: $\vdash_{\mathsf{PA}} \mathtt{bew}_{\mathsf{PA}}(\langle\tilde{\alpha}(x)\rangle, \tilde{\alpha}(x))$. Das ergibt $\vdash_{\mathsf{PA}} \exists y\, \mathtt{bew}_{\mathsf{PA}}(y, \tilde{\alpha}(x)) = \square(\tilde{\alpha}(x)) = \square[\alpha]$.

Es gelten folgende Verallgemeinerungen von $D1, D2$ für $\alpha = \alpha(\vec{x})$ und $\beta = \beta(\vec{x})$:

(7) (a) $\vdash_{\mathsf{PA}} \alpha \;\Rightarrow\; \vdash_{\mathsf{PA}} \square[\alpha]$; (b) $\square[\alpha \to \beta] \vdash_{\mathsf{PA}} \square[\alpha] \to \square[\beta]$.

Denn sei $\vdash_{\mathsf{PA}} \alpha$, so daß auch $\vdash_{\mathsf{PA}} \square\alpha$. Nun liefert ein Beweis für α ähnlich wie im Beispiel für jedes $\vec{a} \in \mathbb{N}^n$ in p.r. Weise leicht einen solchen für $\alpha_{\vec{x}}(\underline{\vec{a}})$. Allgemein formuliert $\square(u) \vdash_{\mathsf{PA}} \square(\mathrm{sb}_{\vec{x}}(u, \vec{x}))$. Das ergibt mit $\ulcorner\alpha\urcorner$ für u wegen $\vdash_{\mathsf{PA}} \square\alpha$ dann $\vdash_{\mathsf{PA}} \square(\mathrm{sb}_{\vec{x}}(\ulcorner\alpha\urcorner, \vec{x}))$ $(= \square[\alpha])$. (b) folgt aus (6) mit $\mathrm{sb}_{\vec{x}}(\ulcorner\alpha\urcorner, \vec{x}), \mathrm{sb}_{\vec{x}}(\ulcorner\beta\urcorner, \vec{x})$ für x, y. Man beachte nur $\vdash_{\mathsf{PA}} \mathrm{sb}_{\vec{x}}(\ulcorner\alpha \to \beta\urcorner, \vec{x}) = \mathrm{sb}_{\vec{x}}(\ulcorner\alpha\urcorner, \vec{x}) \mathbin{\tilde{\to}} \mathrm{sb}_{\vec{x}}(\ulcorner\beta\urcorner, \vec{x})$ nach Übung 4 in **6.4**. Die nach PA übertragene Gleichung (c) dieser Übung ergibt ferner

(8) $\square[\alpha]\,\frac{t}{x} \equiv_{\mathsf{PA}} \square[\alpha\,\frac{t}{x}]$ $(t \in \{0, y, \mathtt{S}y\}$ mit $y \notin gbd\,\alpha)$.

Die Einschränkung in (8) ist unerheblich, aber der Beweis wäre schwieriger und wir benötigen nur (8). $D3$ ist nun lediglich ein Sonderfall der Schlüsselbehauptung

(9) $\varphi \vdash_{\mathsf{PA}} \square[\varphi]$ für alle Σ_1-Formeln φ (die *beweisbare* Σ_1-*Vollständigkeit*).

Denn wählt man in (9) für φ die Σ_1-Aussage $\square\alpha$ für beliebig vorgegebenes $\alpha \in \mathcal{L}^0_{ar}$, ergibt sich $\square\alpha \vdash_{\mathsf{PA}} \square[\square\alpha] = \square\square\alpha$, und $D3$ ist bewiesen. Man erhält (9) durch eine Anwendung des folgenden Satzes, weil der Operator $\partial\colon \alpha \mapsto \square[\alpha]$ nach (7), (8) und wegen $frei\,\alpha = frei\,\square[\alpha]$ die Voraussetzungen des Satzes erfüllt.

Satz 1.2. *Sei $\partial\colon \mathcal{L}_{ar} \to \mathcal{L}_{ar}$ ein Operator mit $frei\,\partial\alpha \subseteq frei\,\alpha$ und den Eigenschaften*

$$d1\colon \vdash_{\mathsf{PA}} \alpha \;\Rightarrow\; \vdash_{\mathsf{PA}} \partial\alpha, \qquad d2\colon \partial(\alpha \to \beta) \vdash_{\mathsf{PA}} \partial\alpha \to \partial\beta,$$
$$ds\colon (\partial\alpha)\tfrac{t}{x} \equiv_{\mathsf{PA}} \partial(\alpha\tfrac{t}{x}) \quad (t \in \{0, y, \mathtt{S}y\},\; y \notin gbd\,\alpha).$$

Dann gilt $\varphi \vdash_{\mathsf{PA}} \partial\varphi$ für alle Σ_1-Formeln φ aus $\mathcal{L}_{ar}$.

Beweis. ∂ erfüllt nach Bemerkung 1 auch $d0$, $d00$ und $d\wedge$. Es genügt nach Satz 6.7.2, die Behauptung für modifizierte Σ_1-Formeln zu beweisen. Sei φ zuerst die Formel $\mathtt{S}x = y$. Hier ist $\varphi \vdash_{\mathsf{PA}} \partial\varphi$ gleichwertig mit $\vdash_{\mathsf{PA}} \partial\varphi\,\frac{\mathtt{S}x}{y}$ $(= (\partial\varphi)\frac{\mathtt{S}x}{y})$, und dies nach ds mit $\vdash_{\mathsf{PA}} \partial\,\mathtt{S}x = \mathtt{S}x$ was nach $d1$ gilt. Ähnlich folgt $y = z \vdash_{\mathsf{PA}} \partial\, y = z$. Das wird für den Induktionsbeweis von $\vdash_{\mathsf{PA}} \forall yz(\varphi \to \partial\varphi)$ mit $\varphi := x + y = z$ über x in PA benötigt. $\varphi\,\frac{0}{x} \vdash_{\mathsf{PA}} y = z \vdash_{\mathsf{PA}} \partial(y = z) \vdash_{\mathsf{PA}} \partial(\varphi\frac{0}{x}) \vdash_{\mathsf{PA}} \partial\varphi\,\frac{0}{x}$ und damit $\vdash_{\mathsf{PA}} (\varphi \to \partial\varphi)\frac{0}{x}$. Weil $\varphi\,\frac{\mathtt{S}y}{y} \equiv_{\mathsf{PA}} \varphi\,\frac{\mathtt{S}x}{x}$, ist wegen $d00, ds$ auch $\partial\varphi\,\frac{\mathtt{S}y}{y} \equiv_{\mathsf{PA}} \partial\varphi\,\frac{\mathtt{S}x}{x}$. Das liefert den Induktionsschritt, denn $\forall yz(\varphi \to \partial\varphi) \vdash \varphi\,\frac{\mathtt{S}y}{y} \to \partial\varphi\,\frac{\mathtt{S}y}{y} \vdash_{\mathsf{PA}} \varphi\,\frac{\mathtt{S}x}{x} \to \partial\varphi\,\frac{\mathtt{S}x}{x} = (\varphi \to \partial\varphi)\frac{\mathtt{S}x}{x}$.

Die Formel $x \cdot y = z$ überlassen wir dem Leser. Die Schritte über $\wedge, \vee, \exists$ sind einfach: $\alpha\wedge\beta \vdash_{\mathsf{PA}} \alpha, \beta \vdash_{\mathsf{PA}} \partial\alpha\wedge\partial\beta \vdash_{\mathsf{PA}} \partial(\alpha\wedge\beta)$ nach $d\wedge$. Bei $\vee$ ist $\alpha \vdash_{\mathsf{PA}} \partial\alpha \vdash_{\mathsf{PA}} \partial(\alpha\vee\beta)$ zu beachten, analog für β. Ferner ist wegen $\alpha \vdash_{\mathsf{PA}} \exists x\alpha$ auch $\alpha \vdash_{\mathsf{PA}} \partial\alpha \vdash_{\mathsf{PA}} \partial\exists x\alpha$, und weil $x \notin \mathit{frei}\,\partial\exists x\alpha$, folgt $\exists x\alpha \vdash_{\mathsf{PA}} \partial\exists x\alpha$ nach $d0$. Auch der Schritt über die Primterm-Substitution ist einfach: $\alpha \vdash_{\mathsf{PA}} \partial\alpha$ liefert $\alpha\,\frac{t}{x} \vdash_{\mathsf{PA}} \partial\alpha\,\frac{t}{x} \vdash_{\mathsf{PA}} \partial(\alpha\frac{t}{x})$.

Es verbleibt der Schritt über die beschränkte Quantifizierung. Sei $\alpha \vdash_{\mathsf{PA}} \partial\alpha$ und $y \notin \mathit{var}\,\alpha$. Wir zeigen $\varphi \vdash_{\mathsf{PA}} \partial\varphi$ für $\varphi := (\forall x{<}y)\alpha$ induktiv über y. Wegen $\vdash_{\mathsf{PA}} \varphi\frac{0}{y}$ ist $\vdash_{\mathsf{PA}} \partial(\varphi\frac{0}{y}) \vdash_{\mathsf{PA}} \partial\varphi\,\frac{0}{y}$ nach $d1, ds$ und erst recht $\varphi\frac{0}{y} \vdash_{\mathsf{PA}} \partial\varphi\,\frac{0}{y}$ (Induktionsanfang). Nun ist $\varphi\frac{\mathtt{S}y}{y} \equiv_{\mathsf{PA}} \varphi \wedge \alpha\,\frac{y}{x}$, und $\alpha \vdash_{\mathsf{PA}} \partial\alpha$ liefert $\alpha\,\frac{y}{x} \vdash_{\mathsf{PA}} \partial\alpha\,\frac{y}{x} \vdash_{\mathsf{PA}} \partial(\alpha\frac{y}{x})$. Das ergibt $\varphi\,\frac{\mathtt{S}y}{y} \wedge(\varphi \to \partial\varphi) \vdash_{\mathsf{PA}} \varphi\wedge\alpha\frac{y}{x} \wedge(\varphi \to \partial\varphi) \vdash_{\mathsf{PA}} \partial\varphi\wedge\partial(\alpha\frac{y}{x}) \vdash_{\mathsf{PA}} \partial(\varphi\wedge\alpha\frac{y}{x}) \vdash_{\mathsf{PA}} \partial(\varphi\frac{\mathtt{S}y}{y})$, also $\varphi \to \partial\varphi \vdash_{\mathsf{PA}} \varphi\frac{\mathtt{S}y}{y} \to \partial(\varphi\frac{\mathtt{S}y}{y})$ was zum Induktionsschritt gleichwertig ist. ❑

Bemerkung 3. $D1$ - $D3$ sind noch für erheblich schwächere Theorien als PA beweisbar, z.B. für die sogenannte *Elementare Arithmetik* $\mathsf{EA} = I\Delta_0 + \forall xy\exists z\delta_{exp}(x, y, z)$. Hier sei δ_{exp} gemäß Bemerkung 1 Seite 186 als Δ_0-Formel verstanden. Für eine äquivalente Formulierung von EA siehe auch [FS]. Bemerkenswerterweise sind die in EA beweisbar rekursiven Funktionen genau die elementaren (für einen expliziten Nachweis siehe [Si]). Höchst bemerkenswert ist auch ein Resultat aus [Be3]. Erweitert man EA um das Π_2-Induktionsschema ohne Parameter, so sind in dieser Theorie genau die p.r. Funktionen beweisbar rekursiv.

Übungen

1. Man beweise in PA mit den üblichen Rechengesetzen (Übung 2 Seite 86) $\forall xy\exists!z\,\underline{2}z = (x + y)^2 + \underline{3}x + y$ und $\forall xy\exists!z(y = z = 0 \vee \exists v\, x = y \cdot v + z \wedge z < y)$ (Definierbarkeit von Paar- und *rest*-Funktion), sowie $\vdash_{\mathsf{PA}} \forall xy\exists!z\,\mathtt{beta}(x, y, z)$.

2. Man beweise in PA (a) $(\forall a{>}1)\exists p(\mathsf{prim}\,p\wedge p\,|\,a)$, (b) den Satz von Euklid, **6.4**.

3. $(\forall k{\geqslant}\underline{2})\exists un(k = \prod_{\nu\leqslant n} p_i^{\boldsymbol{\beta}u\nu} \wedge \boldsymbol{\beta}un \neq 0)$ ist eine Formalisierung der Primfaktorzerlegung. Man beweise diese in PA und darüber hinaus deren Eindeutigkeit.

4. Sei $T' = T + \alpha$ und T erfülle $D1$ - $D4$. Man zeige (a) $\vdash_T \Box_{T'}\varphi \leftrightarrow \Box_T(\alpha \to \varphi)$ (das formalisierte Deduktionstheorem), (b) $D1$ - $D4$ gelten auch für T'.

7.2 Die Theoreme von Gödel und Löb

Wir werden nun die Früchte der Bemühungen in **7.1** ernten. Solange nichts anderes vereinbart wird, bezeichne T eine beliebige axiomatische Theorie in einer gödelisierten Sprache $\mathcal{L}$, welche nebst dem Fixpunktlemma aus **6.5** die Ableitungsbedingungen $D1$ - $D3$ aus **7.1** erfüllt. Wir richten unser Augenmerk sogleich auf die Eindeutigkeitsaussage in Lemma 2.1(b) unten. Danach kann bis auf Äquivalenz in T höchstens $\Box\alpha \to \alpha$ Fixpunkt der Formel $\Box(x) \to \alpha$ sein. Der Beweis von Satz 2.2 wird zeigen, daß auch $\neg\Box(x)$ bis auf T-Äquivalenz nur einen Fixpunkt hat. Dahinter verbirgt sich nach Korollar 4.6 eine ganz allgemeine Tatsache.

Lemma 2.1. *Sei T wie oben vereinbart und α, γ Aussagen aus $\mathcal{L}^0$ derart, daß*

$$(\star) \qquad \gamma \equiv_T \Box\gamma \to \alpha.$$

Dann gelten (a) $\Box\gamma \equiv_T \Box\alpha$, *sowie* (b) $\gamma \equiv_T \Box\alpha \to \alpha$.

Beweis. $(\star)$ liefert $\Box\gamma \vdash_T \Box(\Box\gamma \to \alpha) \vdash_T \Box\Box\gamma \to \Box\alpha$ mit $D0, D2$. Nach $D3$ ist aber $\Box\gamma \vdash_T \Box\Box\gamma$, also $\Box\gamma \vdash_T \Box\alpha$. Weil $\alpha \vdash_T \Box\gamma \to \alpha \vdash_T \gamma$ nach $(\star)$, folgt $\alpha \vdash_T \gamma$ und wegen $D0$ daher auch $\Box\alpha \vdash_T \Box\gamma$. Das beweist (a). Ersetzung von $\Box\gamma$ durch $\Box\alpha$ in $(\star)$ gemäß (a) ergibt (b). ❏

Satz 2.2 (Zweiter Unvollständigkeitssatz). PA *erfüllt nebst dem Fixpunktlemma auch $D1$ - $D3$. Jede Theorie T dieser Art hat die folgenden Eigenschaften:*

(1) *Ist T konsistent, so ist $\nvdash_T \mathtt{Con}_T$,*

(2) $\vdash_T \mathtt{Con}_T \to \neg\Box\, \mathtt{Con}_T$.

Beweis. Der Beweis von $D1$ - $D3$ für PA war Gegenstand von **7.1**. (1) folgt leicht aus (2). Denn angenommen $\vdash_T \mathtt{Con}_T$. Dann ist $\vdash_T \Box\,\mathtt{Con}_T$ nach $D1$ und $\vdash_T \neg\Box\,\mathtt{Con}_T$ nach (2), daher ist T inkonsistent. Das beweist (1). Zum Nachweis von (2) sei γ ein Fixpunkt von $\neg\,\mathtt{bwb}_T(x)$, also (c) $\gamma \equiv_T \neg\Box\gamma$. Mit Lemma 2.1(b) für $\alpha = \bot$ folgt $\gamma \equiv_T \Box\bot \to \bot \equiv \neg\Box\bot = \mathtt{Con}_T$. Dies liefert $\mathtt{Con}_T \equiv_T \neg\Box\,\mathtt{Con}_T$ nach (c). Eine Hälfte hiervon ist die Behauptung (2). ❏

Keine noch so starke konsistente Theorie kann demnach ihre eigene Konsistenz beweisen. Speziell gilt $\nvdash_{\mathsf{PA}} \mathtt{Con}_{\mathsf{PA}}$. Der Beweis zeigt ferner, daß $\mathtt{Con}_T$ modulo T der einzige Fixpunkt von $\neg\,\mathtt{bwb}_T$ ist. Er zeigt darüber hinaus

(3) $\mathtt{Con}_T \equiv_T \neg\Box\,\mathtt{Con}_T$.

Das verschärft (2) aber nur leicht. Denn $\neg\Box\,\mathtt{Con}_T \vdash_T \mathtt{Con}_T$ ist ein Sonderfall von

(4) $\neg\Box\alpha \vdash_T \mathtt{Con}_T$ (gleichwertig $\neg\,\mathtt{Con}_T \vdash_T \Box\alpha$), für jedes $\alpha \in \mathcal{L}$.

Dies folgt wegen $\bot \vdash_T \alpha$ und $\neg\,\mathtt{Con}_T \equiv \Box\bot$ bereits mit $D0$ und reflektiert in T den Sachverhalt 'Ist T inkonsistent, so ist jede Formel beweisbar'. Nach (1) und (3) ist $\nvdash_{\mathsf{PA}} \neg\Box\,\mathtt{Con}_{\mathsf{PA}}$, obwohl 'in PA ist $\mathtt{Con}_{\mathsf{PA}}$ unbeweisbar' wegen (1) wahr ist.

Alle diese Behauptungen gelten unabhängig vom „Wahrheitsgehalt" der Sätze von T. Eine Folge des 2. Unvollständigkeitssatzes ist nämlich die Existenz konsistenter arithmetischer Theorien $T \supseteq \mathsf{PA}$, die nebst (in $\mathcal{N}$) wahren auch falsche Behauptungen beweisen; mit anderen Worten, in denen Wahrheiten und Unwahrheiten friedlich miteinander leben. Solche „Traumtheorien" sind überaus reichhaltig und umfassen die gewöhnliche Zahlentheorie. Eine solche ist speziell $\mathsf{PA}^{\bot} := \mathsf{PA} + \neg\,\mathtt{Con}_{\mathsf{PA}}$, denn *die Unbeweisbarkeit von* $\mathtt{Con}_{\mathsf{PA}}$ *in* PA *ist gleichwertig mit der Konsistenz von* $\mathsf{PA}^{\bot}$. Die kursiv hervorgehobene Aussage ist in PA sogar beweisbar. In der Tat, nach dem Deduktionstheorem ist $\vdash_{\mathsf{PA}+\alpha} \bot \;\Leftrightarrow\; \vdash_{\mathsf{PA}} \alpha \to \bot \equiv \neg\alpha$, und dies läßt sich auch *in* PA verifizieren, d.h. $\vdash_{\mathsf{PA}} \Box_{\mathsf{PA}+\alpha}\bot \leftrightarrow \Box\neg\alpha$ (Übung 4(a) in **7.1**), oder gleichwertig

(5) $\mathtt{Con}_{\mathsf{PA}+\alpha} \equiv_{\mathsf{PA}} \neg\Box\neg\alpha$; allgemeiner $\mathtt{Con}_{T+\alpha} \equiv_T \neg\Box\neg\alpha$.

Für $\alpha = \mathtt{Con}_{\mathsf{PA}}$ ergibt dies $\mathtt{Con}_{\mathsf{PA}^{\bot}} = \neg\Box\neg\neg\,\mathtt{Con}_{\mathsf{PA}} \equiv \neg\Box\,\mathtt{Con}_{\mathsf{PA}}$, und mit (3) folgt

(6) $\mathtt{Con}_{\mathsf{PA}} \equiv_{\mathsf{PA}} \mathtt{Con}_{\mathsf{PA}^{\bot}}$.

Zusammengefaßt: die konsistente Theorie $\mathsf{PA}^{\bot}$ umfaßt einerseits die uns vertraute Zahlentheorie, beweist aber die gewiß falsche Aussage $\mathtt{bwb}_{\mathsf{PA}}(\ulcorner 0 \neq 0 \urcorner)$. Mehr noch, weil $\vdash_{\mathsf{PA}^{\bot}} \neg\,\mathtt{Con}_{\mathsf{PA}}$, beweist diese Theorie nach (6) sogar ihre eigene Inkonsistenz, obwohl sie doch konsistent ist. Wir lernen hieraus, daß mit einer konsistenten Theorie T nicht notwendig auch $T^+ := T + \mathtt{Con}_T$ konsistent sein muß. Die Konsistenz von T kann in T sozusagen eine andere Bedeutung haben als von außen gesehen, ähnlich wie die Bedeutungen von 'abzählbar' divergieren, je nachdem ob man sich in ZFC befindet oder auf ZFC blickt. Man kann auch sagen, $\mathsf{PA}^{\bot}$ belügt uns mit der Behauptung $\neg\,\mathtt{Con}_{\mathsf{PA}^{\bot}}$. Womit uns $\mathsf{PA}^{\bot}$ u.a. noch belügt wird Satz 2.4 zeigen.

Wir diskutieren nun das neben (3) berühmteste Beispiel einer selbstbezüglichen Aussage. Offenbar behauptet ein Fixpunkt α von $\mathtt{bwb}_T$ gerade seine eigene Beweisbarkeit, also $\alpha \equiv_T \Box\alpha$. Ein triviales Beispiel ist $\alpha = \top$, denn mit $\vdash_T \top$ ist auch $\vdash_T \Box\top$, also $\top \equiv_T \Box\top$. Es wird sich wiederum zeigen, daß $\top$ modulo T einziger Fixpunkt von $\mathtt{bwb}_T(x)$ ist. Ein Satz kann also seine eigene Beweisbarkeit nur dann behaupten, wenn er tatsächlich beweisbar ist. $\vdash_T \alpha$ folgt sogar schon aus $\vdash_T \Box\alpha \to \alpha$. Damit gilt das Letztere nicht für jedes α, obwohl man etwa für $T = \mathsf{PA}$ die Beweisbarkeit von $\Box\alpha \to \alpha$ für alle $\alpha \in \mathcal{L}^0$ durchaus erwarten könnte, weil diese Aussagen wahr sind.

Satz 2.3 (Löbs Theorem). *T erfülle $D1$ - $D3$ und das Fixpunktlemma. Dann hat T die Eigenschaften*

$D4$: $\vdash_T \Box(\Box\alpha \to \alpha) \to \Box\alpha$, $\qquad D4^\circ$: $\vdash_T \Box\alpha \to \alpha \;\Rightarrow\; \vdash_T \alpha \qquad (\alpha \in \mathcal{L}^0)$.

Beweis. Sei γ ein Fixpunkt von $\Box(x) \to \alpha$ gemäß Fixpunktlemma, $\gamma \equiv_T \Box\gamma \to \alpha$. Also $\gamma \equiv_T \Box\alpha \to \alpha$ nach Lemma 2.1(b). Hieraus folgt $\Box\gamma \equiv_T \Box(\Box\alpha \to \alpha)$ nach $D0$. Lemma 2.1(a) besagt $\Box\gamma \equiv_T \Box\alpha$, also $\Box\alpha \equiv_T \Box(\Box\alpha \to \alpha)$. Eine Hälfte hiervon ist $D4$. Nachweis von $D4°$: Es gelte $\vdash_T \Box\alpha \to \alpha$. Dann ist $\vdash_T \Box(\Box\alpha \to \alpha)$ nach $D1$. Mit $D4$ folgt hieraus $\vdash_T \Box\alpha$, und $\vdash_T \Box\alpha \to \alpha$ liefert alsdann $\vdash_T \alpha$. ❑

$D4$ ist die in T formalisierte Version von $D4°$. Eine von vielen Anwendungen des Satzes ist folgender Kurzbeweis des Gödelschen Resultats (1). Für $\alpha = \bot$ ergibt $D4°$ $\nvdash_T \bot \Rightarrow \nvdash_T \Box\bot \to \bot \equiv \mathtt{Con}_T$. Analog folgt (2) sofort aus $D4$ durch Kontraposition.

Anders als $\mathsf{PA}^\bot$ geht $\mathsf{PA}^+ = \mathsf{PA} + \mathtt{Con}_{\mathsf{PA}}$ mit der Wahrheit konform. Leider weiß man nicht genau, was $\mathtt{Con}_{\mathsf{PA}}$ zahlentheoretisch oder kombinatorisch bedeutet. Das weiß man aber von einer von Paris und Harrington entdeckten und in ZFC beweisbaren arithmetischen Aussage α mit $\vdash_{\mathsf{PA}} \alpha \to \mathtt{Con}_{\mathsf{PA}}$, die nach (1) in PA nicht beweisbar sein kann. Inzwischen kennt man mehrere derartige Aussagen, die alle kombinatorisch gefärbt sind. Ein populäres Beispiel einer derartigen Aussage ist der

Satz von Goodstein. *Jede Goodstein-Folge endet mit* 0.

Darunter sei eine Zahlenfolge $(a_n)_{n\in\mathbb{N}}$ mit beliebig vorgegebenem a_0 verstanden, so daß sich a_{n+1} aus a_n wie folgt ergibt: Sei $b_n = n + 2$, also $b_0 = 2$. Man stelle a_n für $b := b_n$ in b-adischer Basis dar, so daß für ein gewisses k

$$(*) \qquad a_n = \textstyle\sum_{i\leqslant k} b^{k-i} c_i, \ \text{mit } 0 \leqslant c_i < b.$$

Dabei werden auch die Exponenten $k-i$ in b-adischer Darstellung geschrieben, auch die Exponenten der Exponenten, usw. Nun ersetze man b überall durch $b + 1$ und subtrahiere von der so entstehenden Zahl die Zahl 1. Das Ergebnis heißt dann a_{n+1}. Die Tabelle unten enthält ein Beispiel, beginnend mit $a_0 = 11$. Schon a_5 hat den Wert 134 217 728. Wie man an diesem Beispiel sieht, wächst a_n zunächst enorm an und es ist kaum glaubhaft, daß diese Folge mit 0 endet. Der Beweis hierfür ist nicht einmal schwierig. Man schätzt a_n nach oben ab durch eine Ordinalzahl ξ_n, die aus a_n grob gesagt dadurch entsteht, daß man die Basis b in $(*)$ durch ω ersetzt. Solange $a_{n+1} \neq 0$, gilt dann $\xi_{n+1} < \xi_n$. Da es keine unendlichen echt fallenden Folgen von Ordinalzahlen gibt, muß a_n schließlich mit 0 enden. Siehe hierzu auch [HP].

$a_0 = 11 = 2^{2+1} + 2 + 1$	$2 \rightsquigarrow 3$	$3^{3+1} + 3 + 1 = 85$
$a_1 = 84 = 3^{3+1} + 3$	$3 \rightsquigarrow 4$	$4^{4+1} + 4 = 1028$
$a_2 = 1027 = 4^{4+1} + 3$	$4 \rightsquigarrow 5$	$5^{5+1} + 3 = 15\,628$
$a_3 = 15\,627 = 5^{5+1} + 2$	$5 \rightsquigarrow 6$	$6^{6+1} + 2 = 279\,938$
$a_4 = 279\,937 = 6^{6+1} + 1$	$6 \rightsquigarrow 7$	$7^{7+1} + 1 = 5\,764\,802$

Viele metatheoretische Eigenschaften können durch Benutzung des Beweisoperators $\Box$ in T ausgedrückt werden, oft durch Aussagenschemata. Hier einige Beispiele, die hilfreich sind um die Reichweite von $\neg\,\mathtt{Con}_T$ zu erfassen. Keines dieser Schemata trifft nach Satz 6.5.1′ von außen gesehen auf T zu. α durchläuft jeweils alle Aussagen.

SyVo :	$\Box\alpha \vee \Box\neg\alpha$	(syntaktische Vollständigkeit),
SeVo :	$\alpha \to \Box\alpha$	(semantische Vollständigkeit),
ω-Vo :	$\forall x\Box[\varphi(x)] \to \Box\forall x\varphi(x)$	(ω-Vollständigkeit).

Satz 2.4. *Folgende Eigenschaften sind in einer Theorie T mit den eingangs genannten Eigenschaften äquivalent:*

(i) $\neg\,\mathtt{Con}_T$, (ii) SyVo, (iii) SeVo, (iv) ω-Vo.

Beweis. Nach (4) sind (i)⇒(ii),(iii),(iv) klar. (ii)⇒(i): Nach dem formalisierten Rosserschen Theorem (siehe **7.4**) ist $\mathtt{Con}_T \vdash_T \neg\Box\alpha, \neg\Box\neg\alpha$ für ein α. Das ergibt $\Box\alpha \vee \Box\neg\alpha \vdash_T \neg\,\mathtt{Con}_T$. (iii)⇒(i): Nach SeVo ist $\mathtt{Con}_T \vdash_T \Box\,\mathtt{Con}_T$, Satz 2.2 sagt aber $\mathtt{Con}_T \vdash_T \neg\Box\,\mathtt{Con}_T$, also $\vdash_T \neg\,\mathtt{Con}_T$. (iv)⇒(i): Es ist $\neg\,\mathtt{bew}_T(x,\bot) \vdash_T \Box[\neg\,\mathtt{bew}_T(x,\bot)]$ gemäß (9) in **7.1**, also $\mathtt{Con}_T = \forall x\neg\,\mathtt{bew}_T(x,\bot) \vdash_T \forall x\Box[\neg\,\mathtt{bew}_T(x,\bot)]$. Mit ω-Vo und (2) also $\mathtt{Con}_T \vdash_T \Box\forall x\neg\,\mathtt{bew}(x,\bot) = \Box\,\mathtt{Con}_T \vdash_T \neg\,\mathtt{Con}_T$. Folglich $\vdash_T \neg\,\mathtt{Con}_T$. ❑

Bemerkung. Auch $\mathtt{Con}_T$ ist in T mit anderen Eigenschaften äquivalent, etwa mit dem Schema $\Box\alpha \to \alpha$ für Π_1-Aussagen α *lokales* Π_1*-Reflektionsprinzip*, sowie mit dem *uniformen* Π_1*-Reflektionsprinzip* $\forall x\Box[\alpha(x)] \to \forall x\alpha(x)$ für Π_1-Formeln α, siehe z.B. [Ba, D1]. Sowohl der Satz von Paris-Harrington als auch der von Goodstein sind in PA zur uniformen Σ_1-Reflektion äquivalent, siehe etwa [Ba, D8].

Wir erklären induktiv $T^0 = T$ und $T^{n+1} = T^n + \mathtt{Con}_{T^n}$. Diese *$n$-fach iterierte Konsistenzerweiterung* hat nach Übung 3 die Darstellung $T^n = T + \neg\Box^n\bot$; dabei ist $\Box = \mathtt{bwb}_T$, $\Box^0\alpha = \alpha$ und $\Box^{n+1}\alpha = \Box\Box^n\alpha$. Es sei $T^\omega := \bigcup_{n\in\omega} T^n$. Da $T^n \subseteq T^{n+1}$, ist T^ω konsistent genau dann, wenn alle T^n konsistent sind, d.h. $\nvdash_T \Box^n\bot$ für alle n. Beispiel 2(a) in **7.3** wird zeigen $\mathsf{PA} \subset \mathsf{PA}^1 \subset \mathsf{PA}^2 \subset \dots$ Wie $\mathsf{PA}^1 = \mathsf{PA} + \mathtt{Con}_{\mathsf{PA}}$, geht auch PA^ω mit der Wahrheit konform, was kritisch beleuchtet allerdings nur heißt, daß PA^ω relativ konsistent ist zu ZFC, d.h. $\vdash_{\mathsf{ZFC}} \mathtt{Con}_{\mathsf{PA}^\omega}$. Hier das (in ZFC zu formalisierende) Argument: Wäre $\vdash_{\mathsf{PA}^\omega} \bot$, so folgt schon $\vdash_{\mathsf{PA}^n} \bot$ für ein n und mithin $\vdash_{\mathsf{PA}} \neg\Box^n\bot \to \bot \equiv \Box^n\bot$. Dies aber ist unmöglich, wie eine wiederholte Anwendung von $D1^*$ auf Seite 211 zeigt.

Übungen

1. Man beweise $D4^\circ$ für T durch Anwendung von Satz 2.2 auf $T' = T + \neg\alpha$.
2. Man zeige mit dem Löbschen Theorem, $\mathtt{Con}_{\mathsf{PA}} \to \Diamond\,\mathtt{Con}_{\mathsf{PA}}$ ist in PA unbeweisbar (wohl aber wahr).
3. Man beweise $T^n = T + \neg\Box^n\bot$ und $\mathtt{Con}_{T^n} \equiv_T \neg\Box^{n+1}\bot$. Dabei sei $\Box = \Box_T$.
4. Man beweise $\vdash_{\mathsf{ZFC}} \Box_{\mathsf{PA}}\alpha \to \alpha$ für jede arithmetische Aussage $\alpha \in \mathcal{L}^0_\in$.

7.3 Die Modallogik G

In **7.2** wurde Prädikatenlogik kaum benötigt. Daher überrascht nicht, daß sich viele der dortigen Resultate aussagenlogisch, genauer, in einem sogenannten modalen Aussagenkalkül gewinnen lassen. Dieser enthalte nebst $\wedge, \neg$ auch das Falsumsymbol $\bot$, sowie einen weiteren einstelligen Junktor $\Box$, der den Beweisoperator interpretieren soll. Wir definieren zuerst eine aussagenlogische Sprache $\mathcal{F}_\Box$, deren Formeln durch H, G, F bezeichnet werden mögen: (a) Die Aussagenvariablen $p_1, p_2, \ldots$ und $\bot$ gehören zu $\mathcal{F}_\Box$. (b) Mit $H, G \in \mathcal{F}_\Box$ sind auch $(H \wedge G), \neg H, \Box H \in \mathcal{F}_\Box$. Weitere Formeln gibt es in diesem Zusammenhang nicht. $H \vee G$, $H \to G$, $H \leftrightarrow G$ und $\top$ seien wie üblich definiert. Ferner sei $\Box^0 H = H$ und $\Box^{n+1} H = \Box\Box^n H$, sowie $\Diamond H := \neg\Box\neg H$.

Sei G die Menge der Formeln von $\mathcal{F}_\Box$, die man mit Substitutionen $\sigma\colon \mathcal{F}_\Box \to \mathcal{F}_\Box$, dem Modus Ponens MP und der „Box-Regel" MN: $H/\Box H$ ableiten kann aus den Tautologien der 2-wertigen Aussagenlogik, vermehrt um die modalen Axiome

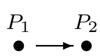
$$\Box(p \to q) \to \Box p \to \Box q, \quad \Box p \to \Box\Box p, \quad \Box(\Box p \to p) \to \Box p \ (\textit{Löbs Axiom}).$$

Auf das Axiom $\Box p \to \Box\Box p$ könnte im Prinzip verzichtet werden; es ist aus den übrigen Axiomen beweisbar, siehe [Boo] oder [Ra1]. Für $H \in \mathsf{G}$ schreiben wir meistens $\vdash_{\mathsf{G}} H$ (gelesen: G *beweist* H). Die Regel MN entspricht offenbar der Bedingung $D1$. Das erste Axiom von G gibt $D2$ wieder, das mittlere $D3$, und das letzte entspricht $D4$. Eine Beschreibung der Beziehung zwischen G und PA gibt **7.4**. Zunächst geht es nur um das formale System G und seine nachfolgend erläuterte Kripke-Semantik. Wir beschränken uns hier ganz auf endliche Kripke-Strukturen für G, kurz G-Strukturen genannt, und beginnen ohne lange Vorrede mit folgender

Definition. Eine G-*Struktur* sei eine endliche irreflexive Halbordnung $(g, <)$. Eine *Belegung* sei eine Abbildung w, die jeder Variablen p eine Teilmenge wp von g zuordnet. Die von w abhängige Relation $P \Vdash H$ zwischen Punkten $P \in g$ und Formeln $H \in \mathcal{F}_\Box$ (gelesen: P *akzeptiert* H) wird induktiv erklärt durch

$$\begin{array}{lll} P \Vdash p \ \Leftrightarrow\ P \in wp, & P \nVdash \bot, & P \Vdash H \wedge G \ \Leftrightarrow\ P \Vdash H, G, \\ P \Vdash \neg H \ \Leftrightarrow\ P \nVdash H, & P \Vdash \Box H \ \Leftrightarrow\ P' \Vdash H \text{ für alle } P' > P. & \end{array}$$

Die letzte Klausel ergibt offensichtlich $P \Vdash \Diamond H \ \Leftrightarrow\ P' \Vdash H$ für ein gewisses $P' > P$. Falls $P \Vdash H$ für alle $P \in g$, alle Belegungen w und alle G-Strukturen g, schreibt man $\vDash_{\mathsf{G}} H$ und sagt H *sei* G-*gültig*. Die G-Struktur rechts aus den Punkten P_1, P_2 mit $P_1 < P_2$ zeigt $\nvDash_{\mathsf{G}} p \to \Box p$. Unter der Belegung w mit $wp = \{P_1\}$ ist zwar $P_1 \Vdash p$, nicht aber $P_1 \Vdash \Box p$, weil $P_2 \nVdash p$. Auch ist z.B. $P_2 \Vdash \Box H$ für alle H weil es kein $P > P_2$ gibt. Damit ist $P_2 \nVdash \Diamond\neg p$, wohl aber $P_1 \Vdash \Diamond\neg p$. Es stehe $H \equiv_{\mathsf{G}} H'$ für $\vDash_{\mathsf{G}} H \leftrightarrow H'$. Dies ist eine Kongruenz in $\mathcal{F}_\Box$, welche die logische Äquivalenz der Formeln ohne $\Box$ konservativ erweitert. So gilt z.B. $\neg\Box H \equiv_{\mathsf{G}} \Diamond\neg H$.



Beispiele. (a) Obwohl stets $P \nVdash \bot$, gilt $P \Vdash \Box\bot$ für maximale Punkte P einer G-Struktur g, d.h. es gibt kein $P' > P$. Auch $\Box\neg\Box\bot$ wird nur genau an den maximalen Punkten von g akzeptiert. Daher ist $\Box\neg\Box\bot \equiv_{\mathsf{G}} \Box\bot$, also $\neg\Box\bot \equiv_{\mathsf{G}} \Diamond\Box\bot$. Dies reflektiert in G den zweiten Unvollständigkeitssatz. Siehe Beispiel 1 in **7.4**.

(b) Sei $\{P_0, \dots, P_n\}$ die G-Struktur mit $P_n < \dots < P_0$. Induktion über n zeigt leicht $P_n \Vdash \Box^m\bot$ für $m > n$, jedoch $P_n \nVdash \Box^n\bot$. Daher auch $P_n \nVdash \Box^{n+1}\bot \to \Box^n\bot$. Folglich $\nvDash_{\mathsf{G}} \Box^{n+1}\bot \to \Box^n\bot$ $(\equiv_{\mathsf{G}} \neg\Box^n\bot \to \neg\Box^{n+1}\bot)$ für jedes n. Erst recht also $\nvDash_{\mathsf{G}} \Box^n\bot$.

(c) $\vDash_{\mathsf{G}} \Box(\Box p \to p) \to \Box p$. Denn seien g und $P \in g$ beliebig. Ist $P \nVdash \Box p$, gibt es – weil g endlich ist – ein $Q > P$ mit $Q \nVdash p$ und $Q' \Vdash p$ für alle $Q' > Q$, also $Q \Vdash \Box p$. Das zeigt $Q \nVdash \Box p \to p$ und daher $P \nVdash \Box(\Box p \to p)$. Folglich $P \Vdash \Box(\Box p \to p) \to \Box p$, was die Behauptung offenbar beweist. Ebenso einfach verifiziert man $\vDash_{\mathsf{G}} \Box p \to \Box\Box p$ mit der Transitivität von $<$. Ganz leicht ist der Beweis von $\vDash_{\mathsf{G}} \Box(p \to q) \to \Box p \to \Box q$.

(d) Für $R_n := \bigwedge_{i=1}^n (\Box p_i \to p_i)$ ist $\vDash_{\mathsf{G}} \neg\Box^{n+1}\bot \to \Diamond R_n$. Denn sei $P \Vdash \neg\Box^{n+1}\top$. Dann muß eine Kette $P = P_0 < \dots < P_{n+1}$ in g existieren. Ein Konjunktionsglied von R_n wird aber von höchstens einem der $n+1$ Punkte $P_1, \dots, P_{n+1}$ nicht akzeptiert, wie man leicht einsieht. Also $P_i \Vdash R_n$ für wenigstens ein $i > 0$. Folglich $P \Vdash \Diamond R_n$. Die Formel R_n ist sehr wichtig für unseren Beweis von Satz 6.1 auf Seite 228.

Induktion in $\vdash_{\mathsf{G}}$ zeigt $\vdash_{\mathsf{G}} H \Rightarrow \vDash_{\mathsf{G}} H$. Beispiel (c) ist ein Teil des Induktionsanfangs. Bei MN schließe man indirekt: mit $P \nVdash \Box H$ folgt $P' \nVdash H$ für ein $P' > P$. Etwas mehr Anstrengung kostet der Nachweis von $\vDash_{\mathsf{G}} H \Rightarrow \vdash_{\mathsf{G}} H$ in folgendem Satz, den wir ohne Beweis benutzen werden. Danach kann $\vdash_{\mathsf{G}} H$ durch den Nachweis von $\vDash_{\mathsf{G}} H$ auch bestätigt werden. Die besondere Bedeutung des Satzes und seines Korollars wird erst klar durch Satz 4.2. Für einen Beweis des Satzes siehe [Boo], [Ra1], oder auch [Kr] mit sehr allgemeinen Kriterien der endlichen Modelleigenschaft, die auf alle in diesem Kapitel betrachteten Modallogiken zutreffen.

Satz 3.1 (Vollständigkeit der Kripke-Semantik für G). $\vdash_{\mathsf{G}} H \;\Leftrightarrow\; \vDash_{\mathsf{G}} H$.

Die in G beweisbaren Formeln sind damit rekursiv aufzählbar. Aber auch die dort widerlegbaren Formeln; denn G ist endlich axiomatisierbar und die G-Strukturen sind sicher aufzählbar. Damit ergibt sich in völliger Analogie zu Übung 3 in **3.6** das

Korollar 3.2. G *ist entscheidbar.*

Bemerkung. Sei $\mathcal{F}^0_\Box$ die Menge der variablenfreien Formeln. $\mathsf{G}^0 := \mathsf{G} \cap \mathcal{F}^0_\Box$ ist ein wichtiges Fragment von G. Dessen interessanteste Formeln sind die $\neg\Box^n\bot$ $(\equiv_{\mathsf{G}} \Diamond^n\top)$. Denn diese bilden eine Boolesche Basis für G^0. Das sieht man leicht, indem man zeigt G^0 ist vollständig bzgl. aller linearen G-Strukturen und den Basissatz 5.2.3 entsprechend anpaßt. Zwei lineare G-Strukturen, die dieselben „Basisformeln“ $\Box^n\bot$ erfüllen, sind entweder beide endlich und bereits isomorph, oder beide sind unendlich und ununterscheidbar bzgl. aller $H \in \mathcal{F}^0_\Box$.

7.4 Modale Behandlung der Selbstreferenz

Sei T eine Theorie in $\mathcal{L}$ wie in **7.2**. Eine Abbildung $\imath\colon p_i \mapsto \alpha_i$ ($\in \mathcal{L}^0$), *Einsetzung* genannt, liefert zu jedem H eine $\mathcal{L}$-Aussage $H^\imath$, indem $\imath$ durch $\bot^\imath = \bot$, $(\neg H)^\imath = \neg H^\imath$, $(H \wedge G)^\imath = H^\imath \wedge G^\imath$ und $(\Box H)^\imath = \Box H^\imath$ ($= \mathtt{bwb}_T(\ulcorner H^\imath \urcorner)$) auf ganz $\mathcal{F}_\Box$ fortgesetzt wird. $H^\imath$ entsteht aus $H = H(p_1, \ldots, p_n)$ einfach durch Ersetzung der p_ν durch die α_ν, $H^\imath = H(\alpha_1, \ldots, \alpha_n)$. So ist z.B. $(\Box p \wedge \neg\Box\bot)^\imath = \Box\alpha \wedge \neg\Box\bot$, falls $p^\imath = \alpha$. Das folgende Lemma zeigt $\vdash_{\mathsf{G}}$ ist „korrekt“ für $\vdash_T$. Allein dies erleichtert Beweise über selbstbezügliche Aussagen, die Ausrechnung von Fixpunkten usw. erheblich.

Lemma 4.1. *Für jedes H mit $\vdash_{\mathsf{G}} H$ und jede Einsetzung $\imath$ in $\mathcal{L}$ gilt $\vdash_T H^\imath$.*

Beweis durch Induktion über $\vdash_{\mathsf{G}} H$. Für eine aussagenlogische Tautologie H ist $H^\imath \in \mathit{Taut}_L \subseteq T$. Ist H eines der modalen Axiome von G, gilt $\vdash_T H^\imath$ nach $D2$, $D3$ bzw. $D4$. Ist $\vdash_{\mathsf{G}} H$ und $\sigma\colon \mathcal{F}_\Box \to \mathcal{F}_\Box$ eine Substitution, gilt $\vdash_T H^{\sigma\imath}$, weil $H^{\sigma\imath} = H^{\imath'}$ mit $\imath' : p \mapsto p^{\sigma\imath}$ und $\vdash_T H^{\imath'}$ gemäß Induktionsannahme. Wurde MN verwendet, gilt also $\vdash_T H^\imath$ nach Induktionsannahme, folgt mit $D1$ sicher auch $\vdash_T \Box H^\imath = (\Box H)^\imath$. Für den Schritt über MP beachte man $(F \to G)^\imath = F^\imath \to G^\imath$. ❑

Beispiel 1. (a) Wir beweisen (3) und damit (2) aus **7.2**. Gemäß Lemma 4.1 und Satz 3.1 genügt zu zeigen $\vDash_{\mathsf{G}} \neg\Box\bot \leftrightarrow \neg\Box\neg\Box\bot$, was nach Beispiel (a) aus **7.3** richtig ist. (b) Man sieht leicht $\vDash_{\mathsf{G}} \Box(p \leftrightarrow \Diamond p) \to \Box\neg p$. Also $\vdash_{\mathsf{PA}} \Box(\alpha \leftrightarrow \Diamond\alpha) \to \Box\neg\alpha$. Das sagt in PA ‘Eine Aussage, die ihre eigene Konsistenz mit PA behauptet ist mit PA unverträglich’. Obwohl dies im ersten Moment wenig plausibel erscheint, ist hiervon auch die Umkehrung richtig und in PA beweisbar. Denn $\vDash_{\mathsf{G}} \Box\neg p \to \Box(p \leftrightarrow \Diamond p)$.

Wir erläutern nun einige Fakten, die die bisherigen Ausführungen in interessanter Weise ergänzen. Für PA und verwandte Theorien gilt auch die Umkehrung von Lemma 4.1. Mit anderen Worten, die Ableitungsbedingungen und Löbs Theorem enthalten bereits alles Wissenswerte über selbstreferierende Aussagenschemata. Für die subtilen Beweise der Sätze 4.2, 4.4 und 4.5 verweisen wir auf [Boo].

Satz 4.2 (Solovays Vollständigkeitssatz). *Für beliebiges $H \in \mathcal{F}_\Box$ gilt $\vdash_{\mathsf{G}} H$ (oder gleichwertig $\vDash_{\mathsf{G}} H$) genau dann, wenn $\vdash_{\mathsf{PA}} H^\imath$ für alle Einsetzungen $\imath$.*

Beispiel 2. (a) $\nvdash_{\mathsf{PA}} \neg\Box^n\bot \to \neg\Box^{n+1}\bot$. Denn $\nvDash_{\mathsf{G}} \neg\Box^n\bot \to \neg\Box^{n+1}\bot$, Beispiel (b) in **7.3**. Das beweist $\mathsf{PA} \subset \mathsf{PA}^1 \subset \mathsf{PA}^2 \subset \ldots$, was $\nvdash_{\mathsf{PA}} \neg\Box^{n+1}\bot$ für alle n einschließt. (b) Man zeigt leicht $\nvDash_{\mathsf{G}} \neg\Box\bot \to \Box\neg\Box\bot$. Daher $\nvdash_{\mathsf{PA}} \mathtt{Con}_{\mathsf{PA}} \to \Box\,\mathtt{Con}_{\mathsf{PA}}$ nach Satz 4.2. (c) $\mathsf{PA}_n := \mathsf{PA} + \Box^{n+1}\bot$ ist konsistent nach (a), aber ω-inkonsistent; andernfalls ergibt $D1^*$ Seite 211 $\vdash_{\mathsf{PA}_n} \Box^{n+1}\bot \Rightarrow \vdash_{\mathsf{PA}_n} \Box^n\bot \Rightarrow \ldots \Rightarrow \vdash_{\mathsf{PA}_n} \bot$, im Widerspruch zur Konsistenz von PA_n. Weil $\vdash_{\mathsf{PA}} \Box^n\bot \to \Box^{n+1}\bot$ gemäß $D3$, gilt $\mathsf{PA}_n \supseteq \mathsf{PA}_{n+1}$, und weil $\mathsf{PA}_n \neq \mathsf{PA}_{n+1}$ wegen $\nvDash_{\mathsf{G}} \Box^{n+1}\bot \to \Box^n\bot$, ist $\mathsf{PA}^\bot = \mathsf{PA}_0 \supset \mathsf{PA}_1 \supset \ldots \supset \mathsf{PA}$.

Infolge der Entscheidbarkeit von G ist Satz 4.2 ein sehr effizientes Instrument zur Entscheidung über die Beweisbarkeit selbstbezüglicher Aussagenschemata. Weil z.B. $\nvdash_{\mathsf{G}} \Box p \to p$, muß es ein $\alpha \in \mathcal{L}^0_{ar}$ mit $\nvdash_{\mathsf{PA}} \Box\alpha \to \alpha$ geben. Ein Beispiel ist $\alpha = \bot$.

Viele andere Theorien haben dieselbe Beweislogik wie PA. Dabei heiße eine modale Aussagenlogik M allgemein die *Beweislogik* für T, wenn das Analogon von Satz 4.2 bzgl. T und M gilt. Für spezielle Theorien kann die Beweislogik allerdings auch eine echte Erweiterung von G sein. So hat z.B. die ω-inkonsistente Theorie PA_n aus Beispiel 2(d) gerade die Beweislogik $\mathsf{G}_n := \mathsf{G} + \Box^n\bot$, die kleinste gegenüber allen Regeln von G abgeschlossene Erweiterung von G mit dem Zusatzaxiom $\Box^n\bot$. Das ist eine direkte Folge von Satz 4.2 für PA, Übung 1. Andere Erweiterungen von G kommen nach folgendem Satz von A. Visser als Beweislogiken nicht in Frage.

Satz 4.3. *T sei mindestens so stark wie* PA. *Dann gelten*

(a) *Ist T^ω konsistent, so ist* G *die Beweislogik von T* (Beweis erfolgt in **7.6**),

(b) *Ist $\vdash_{T^\omega} \bot$ und n minimal mit $\vdash_{T^n} \bot$, so ist* G_n *die Beweislogik von T.*

Es lassen sich nun auch die Formeln $H \in \mathcal{F}_\Box$ mit $\mathcal{N} \vDash H^\imath$ für alle Einsetzungen $\imath$ in $\mathcal{L}_{ar}$ überraschenderweise recht einfach charakterisieren. Offenbar gehören dazu alle $H \in \mathsf{G}$. Aber z.B. gehört dazu auch $\Box p \to p$, weil $\mathcal{N} \vDash \Box\alpha \to \alpha$ für alle $\alpha \in \mathcal{L}^0_{ar}$.

Sei GS ($\supseteq \mathsf{G}$) die Menge $H \in \mathcal{F}_\Box$, die sich aus denen von $\mathsf{G} \cup \{\Box p \to p\}$ mittels Substitution und alleiniger Anwendung von MP, also ohne Box-Regel gewinnen lassen. Induktion über die Erzeugung von GS zeigt $H \in \mathsf{GS} \Rightarrow \mathcal{N} \vDash H^\imath$, für alle Einsetzungen $\imath$. Auch hier gilt nach [So] wieder die Umkehrung:

Satz 4.4. *$H \in$* GS *genau dann, wenn $\mathcal{N} \vDash H^\imath$ für alle Einsetzungen $\imath$.*

Auch GS ist entscheidbar, denn man zeigt unschwer $H \in \mathsf{GS} \Leftrightarrow H^* \in \mathsf{G}$, wobei

$$H^* := [\textstyle\bigwedge_{\Box G \in Sf^\Box H}(\Box G \to G)] \to H.$$

Hier ist $Sf^\Box H$ die Menge der Subformeln von H der Gestalt $\Box G$. Nach Satz 4.4 sind viele, die Beziehungen zwischen *beweisbar* und *wahr* betreffende Fragen effektiv entscheidbar. So ist z.B. $H(p) := \neg\Box(\neg\Box\bot \to \neg\Box p \wedge \neg\Box\neg p) \notin \mathsf{GS}$ leicht zu bestätigen. Aufgrund von Satz 4.4 ist also $\mathcal{N} \vDash \neg H(\alpha) \equiv \Box(\neg\Box\bot \to \neg\Box\alpha \wedge \neg\Box\neg\alpha)$ für ein gewisses $\alpha \in \mathcal{L}^0_{ar}$. Dies bedeutet: Für eine gewisse Aussage α ist *in* PA *beweisbar*, daß die Konsistenz von PA die Unabhängigkeit von α impliziert. Genau dies besagt der im Rahmen von PA formulierte Satz von Rosser. Nach [Be1] kann $\Box$ in den $H \in \mathsf{GS}$ in Satz 4.4 auch $\mathtt{bwb}_T$ für eine beliebige axiomatisierbare Theorie T mit $\mathsf{PA} \subseteq T \subseteq Th\mathcal{N}$ bedeuten; beweist T hingegen falsche Sätze, (wie z.B. $\mathsf{PA}^\bot$), kann GS vollkommen übersehbar neu definiert werden und ist stets entscheidbar.

Eine in H vorkommende Variable p heiße *modalisiert in H*, wenn p nur im Wirkungsbereich eines $\Box$-Operators steht, wie z.B. in $\neg\Box p$ und $\Box(p \to q)$, nicht aber in $\Box p \to p$. Ein weiterer hochinteressanter Satz ist

Satz 4.5 (Fixpunktsatz von DeJongh/Sambin). *Sei p modalisiert in $H(p,\vec{q})$, $\vec{q}=(q_1,\dots,q_n)$, $n\geqslant 0$. Dann gibt es ein $F=F(\vec{q})\in\mathcal{F}_\Box$ mit* (a) $F\equiv_{\mathsf{G}} H(F,\vec{q})$. *Ferner gilt* (b) $\vdash_{\mathsf{G}} \bigwedge_{i=1,2}[(p_i\leftrightarrow H(p_i,\vec{q}))\wedge\Box(p_i\leftrightarrow H(p_i,\vec{q}))]\rightarrow(p_1\leftrightarrow p_2)$.

Dieser Satz ergibt für alle $D1$ - $D4$ erfüllende Theorien T leicht das

Korollar 4.6. *Sei p modalisiert in $H=H(p,\vec{q})$ und T erfülle $D1$-$D4$. Dann gibt es ein $F=F(\vec{q})\in\mathcal{F}_\Box$ mit $F(\vec{\alpha})\equiv_T H(F(\vec{\alpha}),\vec{\alpha})$ für alle $\vec{\alpha}=(\alpha_1,\dots,\alpha_n)$, $\alpha_i\in\mathcal{L}^0$. Bis auf Äquivalenz in T existiert zu jedem $\vec{\alpha}$ nur genau ein $\beta\in\mathcal{L}^0$ mit $\beta\equiv_T H(\beta,\vec{\alpha})$.*

Beweis. Sei F gemäß Satz 4.5 beliebig gewählt. Dann gilt $F(\vec{\alpha})\equiv_T H(F(\vec{\alpha}),\vec{\alpha})$ nach Lemma 4.1, mit $\vec{q}^{\,\imath}=\vec{\alpha}$. Zum Nachweis der Eindeutigkeit sei $\beta_i\equiv_T H(\beta_i,\vec{\alpha})$ für $i=1,2$. Das ergibt $\vdash_T (\beta_i\leftrightarrow H(\beta_i,\vec{\alpha}))\wedge\Box(\beta_i\leftrightarrow H(\beta_i,\vec{\alpha}))$ mit $D1$. Einsetzung von $\beta_i,\vec{\alpha}$ für p_i bzw. $\vec{q}$ in Satz 4.5(b) liefert nach Lemma 4.1 dann $\beta_1\equiv_T\beta_2$. ❑

Beispiel 3. (a) Für $H=\neg\Box p$ ist $n=0$, sowie $F=\neg\Box\bot$ eine „Lösung“ von (a) in Satz 4.5, weil $\neg\Box\bot\equiv_{\mathsf{G}}\neg\Box(\neg\Box\bot)$. Nach dem Korollar ist $\mathtt{Con}_T=\neg\Box\bot$ einziger Fixpunkt von $\neg\,\mathtt{bwb}_T$ modulo T. (b) Für $H(p,q)=\Box p\rightarrow q$ ist $F=\Box q\rightarrow q$ eine Lösung von $F\equiv_{\mathsf{G}} H(F,q)$. Das Korollar besagt $\Box\alpha\rightarrow\alpha$ ist der einzige Fixpunkt von $\mathtt{bwb}_T(x)\rightarrow\alpha$ modulo T. Genau dies ist die Aussage von Lemma 2.1.

Viele Spezialfälle des Korollars repräsentieren ältere Resultate über Selbstreferenz von Gödel, Löb, Rogers, Jeroslow und Kreisel, die – modallogisch formuliert – Fixpunkte p von $\neg\Box p$, $\Box p$, $\neg\Box\neg p$, $\Box\neg p$, $\Box p\rightarrow q$ und $\Box(p\rightarrow q)$ betreffen. Der Reihe nach sind dies $\neg\Box\bot$, $\top$, $\bot$, $\Box\bot$, $\Box q\rightarrow q$ bzw. $\Box q$. Für diese Formeln erhält man übrigens Fixpunkte nach einem ganz einfachen Rezept, denn sie haben alle die Gestalt

$$H(p,\vec{q})=G\,\frac{\Box H'}{p}\qquad (p \text{ in } G(p,\vec{q}) \textit{ nicht} \text{ modalisiert, } H'(p,\vec{q}) \text{ passend gewählt}).$$

Dann nämlich ist $F=H\,\frac{G(\top,\vec{q})}{p}$ Fixpunkt von H, wie sich nachrechnen läßt. Für $H=\neg\Box p=\neg p\,\frac{\Box p}{p}$ etwa ist $G=\neg p$. Daher ist $F=\neg\Box p\,\frac{\neg\top}{p}=\neg\Box\neg\top\equiv_{\mathsf{G}}\neg\Box\bot$. Für $H=\Box p\rightarrow q$ ist $G=p\rightarrow q$, daher $F=(p\rightarrow q)\frac{\Box(\top\rightarrow q)}{p}=\Box(\top\rightarrow q)\rightarrow q\equiv_{\mathsf{G}}\Box q\rightarrow q$. Für Kreisels Formel $\Box(p\rightarrow q)$ ist $G=p$, also $F=p\frac{\Box(\top\rightarrow q)}{p}=\Box(\top\rightarrow q)\equiv_{\mathsf{G}}\Box q$.

Übungen

1. Man beweise, die Theorie PA_n aus Beispiel 2(c) hat die Beweislogik G_n.

2. Man zeige $\mathsf{PA}^n+\neg\,\mathtt{Con}_{\mathsf{PA}^n}$ ist identisch mit $\mathsf{PA}+\Box^{n+1}\bot\wedge\neg\Box^n\bot$ ($\Box=\Box_{\mathsf{PA}}$) und hat nach Satz 4.3 daher die Beweislogik $\mathsf{G}_0=\mathsf{G}+\Box\bot$. Dasselbe zeige man für $T:=\mathsf{PA}+\Box(\Box\,\mathtt{Con}_{\mathsf{PA}}\vee\Box\neg\,\mathtt{Con}_{\mathsf{PA}})\wedge\neg(\Box\,\mathtt{Con}_{\mathsf{PA}}\vee\Box\neg\,\mathtt{Con}_{\mathsf{PA}})$.

3. (Mostowskis Theorem). Sei $T\supseteq\mathsf{PA}$ axiomatisierbar und $T\vDash\mathcal{N}$. Man zeige, es gibt über T zwei relativ zueinander unabhängige (Σ_1-)Aussagen α,β, d.h. α, $\neg\alpha$, $\alpha\rightarrow\beta$, $\alpha\rightarrow\neg\beta$, $\neg\alpha\rightarrow\beta$, $\neg\alpha\rightarrow\neg\beta$ sind unbeweisbar in T.

7.5 Eine bimodale Beweislogik für PA

Nach einer Bemerkung von Hilbert läßt sich das Unvollständigkeitsphänomen durch Benutzung der sogenannten *ω-Regel* ρ_ω : $\dfrac{X \vdash \varphi(\underline{n}) \text{ für alle } n}{X \vdash \forall x\varphi}$ sozusagen gewaltsam aus der Welt schaffen. ρ_ω hat unendlich viele Prämissen und es ist einfach, mittels ρ_ω jede in $\mathcal{N}$ gültige Aussage α aus den Axiomen von PA (sogar denen von Q) herzuleiten. Denn dies ist wegen der Σ_1-Vollständigkeit von Q sicher möglich für Primaussagen und deren Negationen; jede andere Aussage läßt sich aus diesen bis auf Äquivalenz mit $\wedge, \vee, \forall, \exists$ erzeugen und die Induktionsschritte über diese Junktoren sind einfach. Beim $\forall$-Schritt verwendet man gerade ρ_ω. Der uneingeschänkte Gebrauch der infinitären Regel ρ_ω widerspricht jedoch Hilberts eigenen Intentionen einer finiten Grundlegung der Mathematik. Schränkt man ρ_ω aber auf eine *einmalige* Anwendung beim Beweis von α ein, d.h. definiert man $\mathit{1bwb}_{\mathsf{PA}}(\alpha)$ durch

$$\mathit{1bwb}_{\mathsf{PA}}(\alpha) := (\exists\varphi{\in}\mathcal{L}^1_{ar})[\forall n\, \mathit{bwb}_{\mathsf{PA}}(\varphi(\underline{n})) \wedge \mathit{bwb}_{\mathsf{PA}}(\forall \boldsymbol{v}_0\varphi \to \alpha)].$$

so ist dieses Prädikat immerhin arithmetisch; genauer, es ist Σ_3 wegen des in $\mathit{bwb}_{\mathsf{PA}}$ noch verborgenen $\exists$-Quantors. Im Sinne der Bemerkung 1 in **6.2** unterscheiden wir dabei nicht mehr zwischen α und $\dot\alpha$; wir lesen $\mathit{1bwb}_{\mathsf{PA}}(\alpha)$ als 'α ist 1-beweisbar'. Mit $\mathit{bwb}_{\mathsf{PA}}(\alpha)$ ist gewiß auch $\mathit{1bwb}_{\mathsf{PA}}(\alpha)$ (man wähle $\varphi = \alpha$). Dies läßt sich auch in PA beweisen: $\vdash_{\mathsf{PA}} \Box\alpha \to \boxed{1}\alpha$, für jedes $\alpha \in \mathcal{L}^0_{ar}$. Die Umkehrung gilt nicht. Denn sicher ist $\nvdash_{\mathsf{PA}} \mathtt{Con}_{\mathsf{PA}}$, doch ist $\mathtt{Con}_{\mathsf{PA}}$ leicht 1-beweisbar: mit $\varphi(\boldsymbol{v}_0) := \neg\,\mathtt{bew}_{\mathsf{PA}}(\boldsymbol{v}_0, \bot)$ ist $\vdash_{\mathsf{PA}} \varphi(\underline{n})$ für jedes n, und $\vdash_{\mathsf{PA}} \forall\boldsymbol{v}_0\varphi \to \mathtt{Con}_{\mathsf{PA}}$ ist wegen $\forall\boldsymbol{v}_0\varphi \equiv \mathtt{Con}_{\mathsf{PA}}$ trivial.

Sei $\mathtt{1bwb}(z)$ die $\mathit{1bwb}_{\mathsf{PA}}$ definierende Σ_3-Formel, $\boxed{1}\alpha := \mathtt{1bwb}(\ulcorner\alpha\urcorner)$ und $\langle 1\rangle\alpha := \neg\,\boxed{1}\neg\alpha$. Für $\alpha \in \mathcal{L}^0_{ar}$ darf man $\Box\alpha$ bekanntlich lesen als '$\mathsf{PA} + \neg\alpha$ ist inkonsistent', $\boxed{1}\alpha$ nach Lemma 5.1 hingegen als '$\mathsf{PA} + \neg\alpha$ ist ω-inkonsistent'. $\langle 1\rangle\top$ ($\equiv \neg\,\boxed{1}\bot$) meint demnach '$\mathsf{PA}$ ($= \mathsf{PA} + \neg\bot$) ist ω-konsistent'. Dies erklärt das Interesse an dem Operator $\boxed{1}$.

Sei $\Omega := \{\forall x\varphi \mid \varphi \in \mathcal{L}^1_{ar},\ \vdash_{\mathsf{PA}} \varphi(\underline{n}) \text{ für alle } n\}$ mit $x = \boldsymbol{v}_0$. Wie Satz 5.2 zeigen wird, ist PA^Ω echt Σ_3, also nicht mehr rekursiv axiomatisierbar. Wir zeigen zuerst

Lemma 5.1. *Folgende Eigenschaften sind für beliebiges $\alpha \in \mathcal{L}^0_{ar}$ gleichwertig:*

(i) $\mathit{1bwb}_{\mathsf{PA}}(\alpha)$, (ii) $\vdash_{\mathsf{PA}^\Omega} \alpha$, (iii) $\mathsf{PA} + \neg\alpha$ *ist ω-inkonsistent.*

Beweis. (i)⇒(ii) folgt unmittelbar aus den Definitionen. (ii)⇒(iii): Sei $\vdash_{\mathsf{PA}^\Omega} \alpha$. Nun ist Ω modulo PA konjunktiv abgeschlossen. Also gibt es nach dem Deduktionstheorem ein $\forall x\varphi(x) \in \Omega$ mit $\vdash_{\mathsf{PA}} \forall x\varphi \to \alpha$ und $\vdash_{\mathsf{PA}} \varphi(\underline{n})$ für alle n. Weil dann offenbar $\vdash_{\mathsf{PA}+\neg\alpha} \exists x\neg\varphi$, ist $\mathsf{PA} + \neg\alpha$ ω-inkonsistent. (iii)⇒(i): Sei etwa $\vdash_{\mathsf{PA}+\neg\alpha} \beta(\underline{n})$ für alle n, sowie $\vdash_{\mathsf{PA}+\neg\alpha} \exists x\neg\beta(x)$, folglich $\vdash_{\mathsf{PA}} \forall x\beta \to \alpha$. Mit $\varphi(x) := \neg\alpha \to \beta(x)$ ist dann $\vdash_{\mathsf{PA}} \varphi(\underline{n})$ für alle n und weil $\forall x\varphi \equiv \alpha \vee \forall x\beta \vdash_{\mathsf{PA}} \alpha$, ist auch $\vdash_{\mathsf{PA}} \forall x\varphi \to \alpha$. Daher ist α 1-beweisbar. ❑

Satz 5.2. *Alle in $\mathcal{N}$ gültigen Σ_3-Aussagen sind 1-beweisbar. Für jedes derartige α ist sogar $\vdash_{\mathsf{PA}} \alpha \rightarrow \boxed{1}\alpha$ (die 1-beweisbare Σ_3-Vollständigkeit von* PA*).*

Beweis. Sei $\mathcal{N} \vDash \alpha = \exists x \forall y \gamma(x, y)$ und $\gamma(x, y)$ Σ_1. Dann gibt es ein m derart, daß $\mathcal{N} \vDash \gamma(\underline{m}, \underline{n})$ für alle n. Daher $\vdash_{\mathsf{PA}} \gamma(\underline{m}, \underline{n})$ für alle n, wegen der Σ_1-Vollständigkeit von PA. Also $\forall y \gamma(\underline{m}, y) \in \Omega$ und mithin $\vdash_{\mathsf{PA}^\Omega} \exists x \forall y \gamma$, oder gleichwertig *1bwb*$_{\mathsf{PA}}(\alpha)$ nach Lemma 5.1. Diese Argumentation ist wegen der beweisbaren Σ_1-Vollständigkeit von PA in PA nachvollziehbar, so daß auch $\alpha \vdash_{\mathsf{PA}} \boxed{1}\alpha$. ❑

$D1$-$D4$ gelten auch für den Operator $\boxed{1} : \mathcal{L}^0_{ar} \rightarrow \mathcal{L}^0_{ar}$. In der Tat, $D1$ trifft zu wegen $\vdash_{\mathsf{PA}} \alpha \Rightarrow \vdash_{\mathsf{PA}} \Box\alpha \Rightarrow \vdash_{\mathsf{PA}} \boxed{1}\alpha$. $D2$ formalisiert '$\vdash_{\mathsf{PA}^\Omega} \alpha, \alpha \rightarrow \beta \ \Rightarrow \vdash_{\mathsf{PA}^\Omega} \beta$' nach Lemma 5.1, und $D3$ ist eine Anwendung von Satz 5.2 auf die Σ_3-Aussage $\boxed{1}\alpha$. In **7.2** wurden für den Beweis von $D4$ nebst dem Fixpunktlemma nur $D1$ - $D3$ benutzt. Also gilt auch $D4$. Damit überträgt sich fast alles aus **7.2** auf $\boxed{1}$, speziell der Gödelsche Satz 2.2, der jetzt die Formulierung $\nvdash_{\mathsf{PA}} \neg \boxed{1}\bot$ ($\equiv \Diamond_1\top$) annimmt. Demnach ist die ω-Konsistenz von PA auch mit den erweiterten Mitteln nicht beweisbar. Ferner kann diese nach Satz 5.2 nicht Σ_3 sein. Sie ist der Form nach Π_3 und daher echt Π_3.

Nebst $\Box\alpha \rightarrow \boxed{1}\alpha$ gibt es weitere interessante Interaktionen zwischen $\Box$ und $\boxed{1}$. So ist $\vdash_{\mathsf{PA}} \neg\Box\alpha \rightarrow \boxed{1}\neg\Box\alpha$ für alle $\alpha \in \mathcal{L}^0_{ar}$, die Formalisierung von 'wenn $\nvdash_{\mathsf{PA}} \alpha$ so ist $\neg\Box\alpha$ 1-beweisbar' in PA. Dies ist richtig; denn $\nvdash_{\mathsf{PA}} \alpha$ impliziert $\vdash_{\mathsf{PA}} \varphi(\underline{n})$ für alle n mit $\varphi(x) := \neg\, \mathtt{bew}_{\mathsf{PA}}(x, \ulcorner\alpha\urcorner)$ und sicher ist $\vdash_{\mathsf{PA}} \forall x \varphi \rightarrow \neg\Box\alpha$, also ist $\neg\Box\alpha$ 1-beweisbar. Hingegen ist $\vdash_{\mathsf{PA}} \neg\Box\alpha \rightarrow \Box\neg\Box\alpha$ i.a. falsch, siehe Beispiel (c) auf Seite 223.

Die Sprache der nunmehr definierten bimodalen Aussagenlogik GD entstehe aus $\mathcal{F}_\Box$ durch Aufnahme eines weiteren Junktors $\boxed{1}$, der syntaktisch wie $\Box$ zu handhaben ist. Axiome von GD seien die von G, formuliert für $\Box$ und auch für $\boxed{1}$, zuzüglich

$$\Box p \rightarrow \boxed{1}p, \quad \neg\Box p \rightarrow \boxed{1}\neg\Box p.$$

Die Regeln von GD seien dieselben wie für G. Einsetzungen $\imath$ nach $\mathcal{L}^0_{ar}$ seien definiert wie in **7.4**, mit der Zusatzklausel $(\boxed{1}H)^\imath = \boxed{1}H^\imath \ \big(= \mathit{1bwb}_{\mathsf{PA}}(\ulcorner H^\imath \urcorner)\big)$. Nach obigen Ausführungen sind die Axiome und Regeln von GD korrekt, was eine (die leichtere) Hälfte des folgenden bemerkenswerten *Satzes von Dzhaparidze* (1985) beweist:

Satz 5.3. $\vdash_{\mathsf{GD}} H \ \Leftrightarrow \vdash_{\mathsf{PA}} H^\imath$ *für alle Einsetzungen $\imath$. Auch* GD *ist entscheidbar.*

Durch GD werden also die Interaktionen zwischen *bwb*$_{\mathsf{PA}}$ und *1bwb*$_{\mathsf{PA}}$ vollkommen erfaßt. Ferner überträgt sich auch Satz 4.5. Allerdings hat GD keine adäquate Kripke-Semantik mehr, was das Entscheidungsverfahren kompliziert gestaltet. Diesbezüglich und für Literaturangaben sei jedoch auf [Boo] und [Be3] verwiesen.

Zur Übung empfehlen wir $\boxed{1}(\Box p \rightarrow p)$ aus den Axiomen von GD zu beweisen. Also $\vdash_{\mathsf{PA}} \boxed{1}(\Box\alpha \rightarrow \alpha)$ für *jedes* $\alpha \in \mathcal{L}^0_{ar}$, während $\vdash_{\mathsf{PA}} \Box(\Box\alpha \rightarrow \alpha)$ nur im Falle $\vdash_{\mathsf{PA}} \alpha$ richtig ist. *Vorsicht*: GD erweitert G konservativ, also $\nvdash_{\mathsf{GD}} \Box p \rightarrow p$.

7.6 Modale Operatoren in ZFC

Betrachtungen über Selbstreferenz in ZFC oder ZF sind etwas komplizierter, weil es keine übergeordnete Theorie mehr gibt. Ist ZFC konsistent – wovon wir ausgehen – so ist $\mathtt{Con}_{\mathsf{ZFC}}$ arithmetisch wahr (in $\mathcal{N}$ gültig), aber in ZFC nicht mehr beweisbar. Es liegt daher nahe, gleich $\mathsf{ZFC}^+ := \mathsf{ZFC} + \mathtt{Con}_{\mathsf{ZFC}}$ zu betrachten. Denn wir wollen doch, daß die Mengentheorie möglichst viele plausible Tatsachen erfaßt, aus denen sich vielleicht interessante mengentheoretische Einsichten ergeben.

Wie aber **7.2** lehrt, garantiert die bloße Konsistenzannahme von ZFC noch nicht, daß ZFC^+ tatsächlich konsistent ist. Der zweite Unvollständigkeitssatz verbietet zwar $\vdash_{\mathsf{ZFC}} \mathtt{Con}_{\mathsf{ZFC}}$, nicht aber $\vdash_{\mathsf{ZFC}} \neg\,\mathtt{Con}_{\mathsf{ZFC}}$. Dies hieße, ZFC ginge so weit über gesicherte Erfahrungen mit endlichen Mengen hinaus, daß ihre im eigenen Rahmen formulierte Konsistenz ihren äußerlichen Sinn verlöre. Gewisse Existenzannahmen über große Kardinalzahlen, die unschwer die Konsistenz von ZFC^+ implizieren, müßten dann ad acta gelegt werden. Und man müßte in Kauf nehmen, daß ZFC dann nebst wahren auch äußerlich falsche arithmetische Sätze beweist wie etwa $\neg\,\mathtt{Con}_{\mathsf{ZFC}}$.

Selbst wenn $\nvdash_{\mathsf{ZFC}} \neg\,\mathtt{Con}_{\mathsf{ZFC}}$, könnte immer noch eine der Aussagen aus der Folge $\Box\neg\,\mathtt{Con}_{\mathsf{ZFC}}, \Box\Box\neg\,\mathtt{Con}_{\mathsf{ZFC}}, \dots$ in ZFC beweisbar sein. Dies wird erst ausgeschlossen durch die Konsistenzannahme der ω-iterierten Konsistenzerweiterung ZFC^ω (siehe Seite 220), so daß G nach Satz 4.3 die Beweislogik von ZFC wäre. Diese Konsistenzannahme ist mit letzterem sogar äquivalent. Das ist ein Spezialfall des folgenden Satzes, worin $Rf_T = \{\Box\alpha \to \alpha \mid \alpha \in \mathcal{L}^0\}$ das lokale Reflektionsprinzip bezeichne. Auch Satz 4.3(a) ist ein Korollar des Satzes, denn $(\forall n{\in}\mathbb{N}) \nvdash_T \Box^{n+1}\bot$ ist gleichwertig mit der Konsistenz von T^ω. Die Äquivalenz (i) $\Leftrightarrow$ (ii) ist rein beweistheoretischer Natur und heißt auch *Goryachev's Theorem*, siehe hierzu [Be2].

Satz 6.1. *Für eine hinreichend ausdrucksstarke Theorie* T [4)] *sind äquivalent*

(i) T^ω *ist konsistent,* (ii) $T + Rf_T$ *ist konsistent,* (iii) G *ist die Beweislogik von* T.

Beweis. (i)$\Rightarrow$(ii) indirekt: Sei $T + Rf_T$ inkonsistent. Dann gibt es $\alpha_0, \dots, \alpha_n$ mit $\vdash_T \neg\varphi$ für $\varphi = \bigwedge_{i\leqslant n}(\Box\alpha_i \to \alpha_i)$, also auch $\vdash_T \neg\Diamond\varphi$ $(\equiv_T \Box\neg\varphi)$. Weil $\vdash_{T^\omega} \neg\Box^{n+1}\bot$, ist nach Beispiel (d) in **7.3** und Lemma 4.1 dann auch $\vdash_{T^\omega} \Diamond R_n^\imath$ mit $\imath\colon p_i \mapsto \alpha_i$. Offenbar ist $R_n^\imath = \varphi$, also $\vdash_{T^\omega} \Diamond\varphi$. Folglich ist T^ω inkonsistent. (ii)$\Rightarrow$(iii): Der Beweis von Satz 4.2 für PA wie z.B. präsentiert in [Boo], verläuft für T genauso; denn nur an einer Stelle wird PA überschritten: es wird genutzt daß $\mathcal{N} \vDash Rf_{\mathsf{PA}}$. Die Existenz eines entsprechenden T-Modells ist aber gemäß (ii) gewährleistet. (iii)$\Rightarrow$(i): $\nvdash_{\mathsf{G}} \Box^{n+1}\bot$, also $\nvdash_T \Box^{n+1}\bot \equiv_T \neg\,\mathtt{Con}_{T^n}$ für alle n. Daher ist T^ω konsistent. ❏

[4)] Das heiße hier die Ausführbarkeit der PA nicht überschreitenden Beweisschritte im Solovayschen Satz 4.2 in T, was noch nicht die Beweisbarkeit des Satzes selbst bedeutet.

Bemerkung. Für $T = \mathsf{ZFC}$ möglicherweise naheliegender als (i) oder (ii) ist die Annahme (A) ZFC *ist* ω*-konsistent*, d.h. $\vdash_{\mathsf{ZFC}} \alpha_x(\underline{n})$ für alle n impliziert $\nvdash_{\mathsf{ZFC}} (\exists x{\in}\omega)\neg\alpha$ für $\alpha \in \mathcal{L}_\in$. Die ω-Konsistenz hat $D1^*$ Seite 211 zur Folge, was seinerseits (i) in Satz 6.1 impliziert und damit (iii): G ist die Beweislogik von ZFC. Hier wurde Goryachev's Theorem verwendet. Wir erwähnen, daß auch ohne dieses Theorem die Konsistenz von $\mathsf{ZFC} + Rf_{\mathsf{ZFC}}$ und damit (iii) direkt aus der Annahme (A) folgt. Man beweist nämlich unschwer folgendes

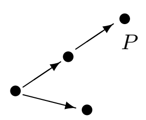
Lemma. *Ist* ZFC ω*-konsistent, so existiert ein Modell* $\mathcal{V} \vDash \mathsf{ZFC}$ *mit* $\mathcal{V} \vDash Rf_{\mathsf{ZFC}}$.

Beweis. Sei $\Omega := \{(\forall x \in \omega)\alpha \mid \alpha = \alpha(x), \vdash_{\mathsf{ZFC}} \alpha(\underline{n}) \text{ für alle } n\}$. Dann ist $\mathsf{ZFC} + \Omega$ konsistent. Andernfalls folgt $\vdash_{\mathsf{ZFC}} \neg(\forall x \in \omega)\alpha \equiv (\exists x \in \omega)\neg\alpha$ für ein $(\forall x \in \omega)\alpha$ aus Ω wegen der konjunktiven Abgeschlossenheit von Ω, im Widerspruch zu (A). Für $\mathcal{V} \vDash \mathsf{ZFC} + \Omega$ ist auch $\mathcal{V} \vDash Rf_{\mathsf{ZFC}}$. Denn sei $\mathcal{V} \nvDash \alpha$, also $\nvdash_{\mathsf{ZFC}} \alpha$ und mithin $\vdash_{\mathsf{ZFC}} \neg\,\mathtt{bew}_{\mathsf{ZFC}}(\underline{n}, \ulcorner\alpha\urcorner)$ für alle n. Das bedeutet $(\forall y \in \omega)\neg\,\mathtt{bew}_{\mathsf{ZFC}}(y, \ulcorner\alpha\urcorner) \in \Omega$, was offenbar $\mathcal{V} \nvDash \Box\alpha$ zur Folge hat.

Wir interpretieren nunmehr den Modaloperator $\Box$ nicht mehr durch 'beweisbar in ZFC' oder gleichwertig, 'gültig in allen ZFC-Modellen', sondern durch die Gültigkeit in gewissen ausgezeichneten Modellklassen. Für die nachfolgend nicht erklärten Begriffe verweisen wir z.B. auf [Ku]. Besonders nützlich sind *transitive* Modelle. Dies sei ein ZFC-Modell $\mathcal{V} = (V, \in^{\mathcal{V}})$, so daß V *transitiv* ist, d.h. $a \in b \in V \Rightarrow a \in V$. Dabei sei $\in$ die gewöhnliche $\in$-Relation und $\in^{\mathcal{V}}$ deren Einschränkung auf V. Wir verstehen hier V als naive Menge unserer Metatheorie die gleichfalls ZFC sei und schreiben einfach V für $\mathcal{V}$. Wie jede Menge, hat auch V einen ordinalen Rang, der mit ρV bezeichnet sei. Für $U \in V$ ist immer $\rho U < \rho V$. Für die hier bewiesene Hälfte des Satzes 6.3, die Korrektheit, verwenden wir

Lemma 6.2. ([JK]) *Es seien* V, W *transitive Modelle von* ZFC *mit* $\rho V < \rho W$ *und* $V \vDash \alpha$. *Dann gilt in* W *die Aussage* '*es gibt ein transitives Modell* U *mit* $U \vDash \alpha$' [5)].

Gi entstehe aus G durch Erweiterung um das Axiom $\Box(\Box p \to \Box q) \vee \Box(\Box q \to p)$. In demselben Sinne, wie G bzgl. aller endlichen Halbordnungen vollständig ist, ist Gi vollständig bzgl. aller *Präferenzordnungen*. Es sei dies eine endliche Halbordnung $(g, <)$, für die ein $h\colon g \to \mathbb{N}$ existiert mit $P < Q \Leftrightarrow hP < hQ$, für alle $P, Q \in g$. Das liefert die endliche Modelleigenschaft und Entscheidbarkeit von Gi.



Die Figur zeigt eine irreflexive Halbordnung, die keine Präferenzordnung ist und in der das hinzugefügte Axiom mit $w(p) = \{P\}$ und $w(q) = \emptyset$ leicht widerlegt werden kann. Es gehört demnach nicht zu G, so daß $\mathsf{Gi} \supset \mathsf{G}$.

Einsetzungen $\imath\colon \mathcal{F}_\Box \to \mathcal{L}^0_\in$ seien analog erklärt wie in **7.4**, wieder mit der Klausel $(\Box H)^\imath = \Box H^\imath$, wobei $\Box\alpha$ für $\alpha \in \mathcal{L}^0_\in$ jetzt bedeute 'α gilt in allen transitiven

[5)] In transitiven Modellen W ist die Aussage in ' ' (die mit etwas Kodierung in $\mathcal{L}_\in$ leicht formulierbar ist) absolut und daher gleichwertig mit der Existenz eines transitiven Modells $U \in W$ mit $U \vDash \alpha$. Die Existenz eines transitiven Modells folgt noch nicht aus der bloßen Konsistenz von ZFC. Aber die hier bewiesene Richtung von Satz 6.3 benötigt die Existenz transitiver Modelle nicht.

Modellen V', genauer die Formalisierung dieser Eigenschaft in $\mathcal{L}_\in$. Es besagt dann $\Diamond\alpha$ ($= \neg\Box\neg\alpha$) offenbar '$V \vDash \alpha$ für ein gewisses transitives V'.

Satz 6.3. $\vdash_{\mathsf{Gi}} H \;\Leftrightarrow\; \vdash_{\mathsf{ZFC}} H^\imath$ *für alle Einsetzungen* $\imath$.

Wir beweisen hier nur die Richtung $\Rightarrow$, also die Korrektheit. Was die Axiome von Gi betrifft, so genügt wegen der in **7.3** erwähnten Beweisbarkeit von $\Box p \to \Box\Box p$ aus den übrigen Axiomen von G offenbar der Nachweis von

$$\text{(A) } \Box(\alpha \to \beta) \land \Box\alpha \vdash_{\mathsf{ZFC}} \Box\beta, \quad \text{(B) } \Box(\Box\alpha \to \alpha) \vdash_{\mathsf{ZFC}} \Box\alpha,$$

$$\text{(C) } \vdash_{\mathsf{ZFC}} \Box(\Box\alpha \to \Box\beta) \lor \Box(\Box\beta \to \alpha), \text{ für alle } \alpha, \beta \in \mathcal{L}^0_\in.$$

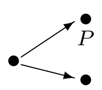
(A) ist trivial, denn die Menge der in allen transitiven Modellen gültigen Aussagen ist sicher MP-abgeschlossen. (B) ist gleichwertig mit (B$'$) $\Diamond\neg\alpha \vdash_{\mathsf{ZFC}} \Diamond(\Box\alpha \land \neg\alpha)$. Hier der Beweis: Wenn es ein transitives Modell V gibt mit $V \vDash \neg\alpha$, dann auch ein derartiges V mit minimalem Rang ρV. Wir behaupten $V \vDash \Box\alpha$. Andernfalls wäre $V \vDash \Diamond\neg\alpha$, also gibt es ein transitives $U \in V$ mit $U \vDash \neg\alpha$ und $\rho U < \rho V$, im Widerspruch zur Wahl von V. Das zeigt $V \vDash \Box\alpha \land \neg\alpha$ und damit (B$'$). Wir beweisen (C) indirekt. Angenommen es existieren transitive Modelle V, W und α, β mit

(a) $V \vDash$ 'α gilt in jedem transitiven Modell und $\neg\beta$ gilt in einem solchen Modell',

(b) $W \vDash$ 'β gilt in allen transitiven Modellen, (c) $W \vDash \neg\alpha$.

Hieraus folgt zuerst $\rho W < \rho V$. Denn sei $U \in V$ ein transitives Modell für $\neg\beta$ nach (a). Wäre $\rho V \leqslant \rho W$, so auch $\rho U < \rho W$. Also gilt nach Lemma 6.2 $W \vDash$ 'es gibt ein transitives Modell für $\neg\beta$', im Widerspruch zu (b). Nun ist $W \vDash \neg\alpha$ nach (c) und $\rho W < \rho V$. In V gilt also 'es gibt ein transitives Modell für $\neg\alpha$' nach dem Lemma, im Widerspruch zu (a). Das beweist (C). Für die Substitutionsregel folgt die Korrektheit wie für G. Auch MN ist trivial korrekt, denn wenn $\vdash_{\mathsf{ZFC}} \alpha$, so gilt α natürlich in allen transitiven Modellen.

Eine andere interessante modelltheoretische Interpretation von $\Box\alpha$ ist 'α gilt in allen V_κ'. Hier durchläuft κ alle unerreichbaren Kardinalzahlen. Unter der Annahme, daß es genügend viele solcher κ gibt, ist $\mathsf{Gj} := \mathsf{G} + \Box(\Box p \land p \to q) \lor \Box(\Box q \to p)$ nach [So] die adäquate Modallogik für diese Interpretation von $\Box$. Diese auch mit $\mathsf{G.3}$ bezeichnete Logik ist vollständig bzgl. aller endlichen linearen Ordnungen. Diese



sind sicher Gi-Strukturen, also $\mathsf{Gi} \subseteq \mathsf{Gj}$. Die Figur zeigt eine Gi-Struktur, auf dem das Zusatzaxiom mit $wp = \{P\}$ und $wq = \emptyset$ leicht widerlegt werden kann. Folglich $\mathsf{Gi} \subset \mathsf{Gj}$. Aus der endlichen Modelleigenschaft folgt wie üblich auch die Entscheidbarkeit von Gj. Wir empfehlen dem Leser abschließend, den Korrektheitsbeweis von Gj für diese Interpretation von $\Box$ auszuführen; er ist dem obigen ähnlich. Man nutzt hier nur, daß V_κ ein transitives Modell ist, sowie $V_\kappa \in V_\lambda$ oder $V_\lambda \in V_\kappa$ für beliebige unerreichbare Kardinalzahlen $\kappa \neq \lambda$.

Lösungshinweise zu den Übungen

Abschnitt 1.1

1. Jedes lineare $f \in \boldsymbol{B}_n$ hat eine *eindeutige* Darstellung der angegebenen Art. Daher ist 2^{n+1} (= Anzahl der $(n+1)$-gliedrigen Folgen aus $0, 1$) die gesuchte Anzahl.

2. Für $\xi \notin \mathcal{F}$ genügt $\mathcal{F}\backslash\{\neg\xi\}$ den Bedingungen der Formeldefinition. Also $\neg\xi \notin \mathcal{F}$.

3. Induktion über α zeigt: Ist ξ echter Anfang von α oder α echter Anfang von ξ, so ist ξ keine Formel.

4. Sei etwa $(\alpha \circ \beta) = (\alpha' \circ' \beta')$. Wäre $\alpha \neq \alpha'$, so wäre α echter Anfang von α' oder umgekehrt. Das ist unmöglich nach Übung 3.

Abschnitt 1.2

2. $\neg p \equiv p + 1,\ 1 \equiv p + \neg p,\ p \leftrightarrow q \equiv p + \neg q$ und $p + q \equiv p \leftrightarrow \neg q$.

3. (a) Induktion über α zeigt $\alpha^{(n)}$ ist monoton, weil mit $f, g \in B$ auch $\vec{x} \mapsto f\vec{x} \circ g\vec{x}$ mononton ist. (b) Induktionsschritt über Stellenzahl: mit $f \in \boldsymbol{B}_{n+1}$ sind auch $f_k \colon \vec{x} \to f(\vec{x}, k)$ monoton, $k = 0, 1$. Werden f_0, f_1 durch α_0 bzw. α_1 repräsentiert, so f durch die Formel $\alpha_0 \vee \alpha_1 \wedge p_{n+1}$.

4. Sei f nicht durch eine Formel in $\{\wedge, \vee, 0, 1\}$ repräsentierbar. Dann ist f nicht monoton. Passende Einsetzung von Konstanten in f liefert die Negation.

Abschnitt 1.3

1. MP ergibt leicht $p \to q \to r,\ p \to q,\ p \vDash r$. Durch 3-malige Anwendung von (D) folgt hieraus $\vDash (p \to q \to r) \to (p \to q) \to (p \to r)$.

4. Sei $X^{\vdash} \vdash \alpha$, also $X \vdash X^{\vdash} \vdash \alpha$. Das ergibt $X \vdash \alpha$ nach (T).

5. $\vdash_0 \subseteq \vdash$: Sei $X \vdash_0 \alpha$, also $X_0 \vdash \alpha$ für ein endliches $X_0 \subseteq X$. Dann folgt $X \vdash \alpha$ nach (M).

Abschnitt 1.4

1. $X \cup \{\neg\alpha \mid \alpha \in Y\} \vdash \bot \Rightarrow X \cup \{\neg\alpha_0, \ldots, \neg\alpha_n\} \vdash \bot$, für gewisse $\alpha_0, \ldots, \alpha_n \in Y$. Das ergibt $X \vdash (\bigwedge_{i \leqslant n} \neg\alpha_i) \to \bot \equiv \bigvee_{i \leqslant n} a_i$.

2. Lemma 4.4 wie folgt ergänzen: $X \vdash \alpha \vee \beta \Leftrightarrow X \vdash \alpha$ oder $X \vdash \beta$.

3. Sei $X \nvdash \varphi$, $X \vdash' \varphi$ und $Y \supseteq X \cup \{\neg\varphi\}$ maximal konsistent in $\vdash$, sowie σ definiert durch $p^\sigma = \top$ für $p \in Y$ und $p^\sigma = \bot$ sonst. Simultane Induktion über $\alpha, \neg\alpha$ zeigt $\alpha \in Y \Rightarrow \vdash \alpha^\sigma$ und $\alpha \notin Y \Rightarrow \vdash \neg\alpha^\sigma$. Folglich $\vdash \neg\varphi^\sigma$. Daher $\vdash' \neg\varphi^\sigma$ und so $X^\sigma \vdash' \neg\varphi^\sigma$. Wegen $X \vdash' \varphi$ ist auch $X^\sigma \vdash' \varphi^\sigma$. Daher $\vdash' \alpha$ für alle α nach $(\neg 1)$.

4. Unter allen Konsequenzen mit den Eigenschaften $(\wedge 1)$ - $(\neg)$ gibt es eine kleinste, sagen wir $\vdash$, und diese ist finitär (Übung 5 in **1.3**). Wegen $\vdash \subseteq \vDash$ und weil $\vdash$ nach Übung 3 maximal ist, kann nur $\vdash = \vDash$ gelten.

Abschnitt 1.5

1. Man muß den Formeln unter Beispiel 1 nur die Formeln $\{p_{ab} \mid a \leqslant_0 b\}$ hinzufügen.

2. Sei U trivial, $K \subseteq I$ koendlich, $K \notin U$, also $E = I \setminus K \in U$. Für jede Zerlegung $E = E_0 \cup E_1$ ist $E_0 \in U$ oder $E_1 \in U$. So erschließe man $\{i_0\} \in U$ für ein $i_0 \in I$.

Abschnitt 1.6

2. Kalküle mit MP als einziger Regel und A1,A2 unter den Axiomen erfüllen das Deduktionstheorem (Beweis wie Lemma 6.3). Für maximal konsistentes X beweist man $X \vdash \alpha \rightarrow \beta \Leftrightarrow$ wenn $X \vdash \alpha$ so $X \vdash \beta$.

3. Man wende das Lemma von Zorn an auf $H = \{Y \supseteq X \mid Y \nvdash \alpha\}$.

4. Sei $X \nvdash \alpha_0$ und X o.B.d.A. α_0-maximal (Übung 3). Definiert man $w \vDash X$ durch $w \vDash p \Leftrightarrow p \in X$, so gilt: $X \vDash \alpha \rightarrow \beta \Leftrightarrow (X \vdash \alpha \Rightarrow X \vdash \beta)$.

Abschnitt 2.1

1. Es gibt 10 wesentlich 2-stellige Boolesche Funktionen f. Die Menge der entsprechenden 10 Gruppoide $(\{0,1\}, f)$ zerfällt in 5 Paare isomorpher Algebren.

4. Man ordne dem Element $a \in 2^I$ die Teilmenge $I_a = \{i \in I \mid a_i = 1\} \subseteq I$ zu.

Abschnitt 2.2

2. (a): Übung 2 in **1.1**, (b): $\mathcal{L} \setminus \{(\alpha \wedge \xi)\}$ erfüllt (F1), (F2), (F3).

3. Induktion über t. Klar für Primterme oder falls ζ erster Buchstabe von t ist. Sonst ist $t = ft_1 \cdots t_n$ und ζ kommt in der Zeichenfolge $t_1 \cdots t_n$ vor, also in einem t_i und ist erster Buchstabe eines Subterms in t_i gemäß Induktionsannahme.

Abschnitt 2.3

1. Sei $\mathcal{M}^{cd}_{xy} \vDash \varphi \wedge \varphi\,\frac{y}{x}$ mit $c \neq d$. Dann gilt $\mathcal{M}^{a}_{x} \vDash \exists y(\varphi\,\frac{y}{x} \wedge x \neq y)$ für alle $a \in A$.

2. Kontraposition von Übung 1 zeigt $\exists x \forall y((\varphi\,\frac{y}{x} \to x = y) \vDash \forall xy(\varphi \wedge \varphi\,\frac{y}{x} \to x = y)$.

3. Nach Satz 3.1 und Satz 3.5 ist $\mathcal{A} \vDash \alpha(x)\,[a] \;\Leftrightarrow\; \mathcal{A}' \vDash \alpha(x)\,[a] \;\Leftrightarrow\; \mathcal{A}' \vDash \alpha\frac{\boldsymbol{a}}{x}$.

4. (b): $\exists_n \wedge \neg\exists_m$ ist für $n \leqslant m$ äquivalent zu $\bigvee_{k=n}^{m} \exists_{=k}$, für $n > m$ zu $\exists_{=0}$ $(\equiv \bot)$.

Abschnitt 2.4

1. $\alpha \equiv \beta \;\Rightarrow\; \vDash \forall\vec{x}\,(\alpha \leftrightarrow \beta) \;\Rightarrow\; \vDash (\alpha \leftrightarrow \beta)\,\frac{\tilde{t}}{\tilde{x}}\; \big(= \alpha\,\frac{\tilde{t}}{\tilde{x}} \leftrightarrow \beta\,\frac{\tilde{t}}{\tilde{x}}\big)$.

2. $\neg\forall x(x \lhd y \to \alpha) \equiv \exists x \neg(x \lhd y \to \alpha) \equiv \exists x(x \lhd y \wedge \neg\alpha)$ (Ersetzungstheorem).

3. O.B.d.A. ist $\alpha \equiv \forall\vec{y}\alpha'(\vec{x},\vec{y})$ und $\beta \equiv \forall\vec{z}\beta'(\vec{x},\vec{z})$ mit disjunkten Tupeln $\vec{x}$, $\vec{y}$, $\vec{z}$.

Abschnitt 2.5

2. Beachte $S \vDash \varphi \to \beta \;\Leftrightarrow\; S, \varphi \vDash \beta$ und (e) Seite 62.

3. Beweise zuerst $T_\alpha := \{\beta \in \mathcal{L}^0 \mid T, \alpha \vdash \beta\}$ ist eine Theorie und dann $T_\alpha = T + \alpha$.

Abschnitt 2.6

1. Man folge dem Beweis von Satz 6.1 (beachte $\varphi(\vec{t}\,) = y \equiv_{T_f} \delta_f(\vec{t}, y))$. Für den „nur dann"-Teil beachte man $(y = f\vec{x} \leftrightarrow \delta(\vec{x}, y))^\forall \vDash \forall\vec{x}\,\exists! y\delta(\vec{x}, y)$.

2. In $(\mathbb{N}, 0, 1, \mathtt{S}, +, \cdot)$ gelten $x = 0 \;\leftrightarrow\; x + x = x$, $x = 1 \;\leftrightarrow\; x \neq 0 \wedge x \cdot x = x$, sowie $y = \mathtt{S}x \leftrightarrow y = x + 1$ $\big(\equiv \exists z(y = x + z \wedge z + z \neq z \wedge z \cdot z = z)\big)$.

3. Sei $xy = xz = e$ ($\circ$, $\vDash$ werden nicht geschrieben) und ein y' mit $yy' = e$ gewählt. Dann ist $x = x(yy') = (xy)y' = y'$. Also $yx = e$ wegen $yy' = e$, $y' = x$. Analog folgt $zx = e$. Daher $y = z$, denn $y = y(xz) = (yx)z = ez = (zx)z = z(xz) = ze = z$.

4. Wäre $<$ definierbar, wäre $<$ unter jedem Automorphismus von $(\mathbb{Z}, 0, +)$ invariant. Das ist nicht der Fall für den Automorphismus $n \mapsto -n$ (Methode von Padoa).

Abschnitt 3.1

1. Sei $X \vdash \alpha\,\frac{t}{x}$. Dann ist $X, \forall x\neg\alpha \vdash \alpha\,\frac{t}{x}, \neg\alpha\,\frac{t}{x}$. Daher $X, \forall x\neg\alpha \vdash \exists x\alpha$. Gewiß ist auch $X, \neg\forall x\neg\alpha \vdash \exists x\alpha$. Also $X \vdash \exists x\alpha$ nach ($\neg$2).

2. Sei $\alpha' := \alpha\,\frac{y}{x}$, $u \notin \operatorname{var}\alpha$, $u \neq y$. Dann ist $\forall x\alpha \vdash \alpha'\,\frac{u}{y}$ $(= \alpha\,\frac{u}{x})$ nach ($\forall$1). Also $\forall x\alpha \vdash \forall y\alpha'$ $(= \forall y\alpha\,\frac{y}{x})$ nach ($\forall$2).

Abschnitt 3.2

1. (i)⇒(ii): Satz 2.6. Beachte $\mathcal{M} \vdash \varphi$ oder $\mathcal{M} \vdash \neg\varphi$ für beliebige Formeln φ.

2. Träger eines solchen $\mathcal{M}$ sei die Termmenge $\mathcal{T}$ einer Henkin-Erweiterung $Y \supseteq X$, indem auf die Faktorisierung von $\mathcal{T}$ in Lemma 2.5 verzichtet wird.

3. Satz 2.7 und der Endlichkeitssatz für $\vdash$.

Abschnitt 3.3

1. Siehe die Beweise dieser Behauptungen in **6.3**.

2. $\vdash_{\mathsf{PA}} \forall z[\forall x\forall y(x + (y + z) = (x + y) + z)]$ folgt induktiv über z. Zum Nachweis von $\vdash_{\mathsf{PA}} \forall xy\, x + y = y + x$ benötigt man $\vdash_{\mathsf{PA}} \forall xy\, x + \mathtt{S}y = \mathtt{S}x + y$.

3. (a): Es genügt zu zeigen $\forall x(\varphi \to \alpha) \vdash_{\mathsf{PA}} \alpha$ mit $\varphi := (\forall z{<}x)\alpha\,\frac{z}{x}$. Wie im Text von Übung 1 schon bemerkt wurde, gilt $z{<}\mathtt{S}x \equiv_{\mathsf{PA}} z{<}x \vee z = x$. Das ergibt $\varphi, \forall x(\varphi \to \alpha) \vdash_{\mathsf{PA}} \varphi \wedge \alpha \vdash_{\mathsf{PA}} (\forall z{<}\mathtt{S}x)\alpha\frac{z}{x}$. Daher $\forall x(\varphi \to \alpha) \vdash_{\mathsf{PA}} \forall x(\varphi \to \varphi\frac{\mathtt{S}x}{x})$. Trivial ist $\vdash_{\mathsf{PA}} \varphi\,\frac{0}{x}$. Mit IS also $\forall x(\varphi \to \alpha) \vdash_{\mathsf{PA}} \forall x\varphi \vdash_{\mathsf{PA}} \forall x\alpha$. (b): Folgt aus (a) durch Kontraposition. (c): Für $\varphi := (\forall y{<}x)\exists z\alpha \to \exists u(\forall y{<}x)(\exists z{<}u)\alpha$ gilt $\vdash_{\mathsf{PA}} \varphi\,\frac{0}{x}$ und man beweist unschwer $\varphi \vdash_{\mathsf{PA}} \varphi\,\frac{\mathtt{S}x}{x}$. Dies liefert die Behauptung gemäß IS.

Abschnitt 3.4

1. $X = T \cup \{\boldsymbol{v}_i \neq \boldsymbol{v}_j \mid i \neq j\}$ ist erfüllbar, weil jede endliche Teilmenge dies ist.

2. $X = Th\mathcal{A} \cup \{\boldsymbol{v}_{n+1} < \boldsymbol{v}_n \mid n \in \mathbb{N}\}$ hat Modell mit unendlich absteigender Kette.

4. Sei $u \in Var$. Folgende Formelmenge (mit Symbolen $\boldsymbol{a}$ für die $a \in V$) ist konsistent:
$$Th(V, \in^V) \cup \{\boldsymbol{a} \in \boldsymbol{b} \mid a, b \in V,\ a \in^V b\} \cup \{\boldsymbol{a} \notin \boldsymbol{b} \mid a, b \in V,\ a \notin^V b\} \cup \{\boldsymbol{a} \in u \mid a \in V\}.$$

Abschnitt 3.5

1. $\beta \in T' \Leftrightarrow \alpha \to \beta \in T$.

2. (ii)⇒(iii): Ist $T + \{\alpha_i \mid i \in \mathbb{N}\}$ nichtendliche Erweiterung, kann $\bigwedge_{i \leqslant n} \alpha_i \nvdash_T \alpha_n$ angenommen werden. Sei T_n Vervollständigung von $T + \bigwedge_{i \leqslant n} \alpha_i + \neg\alpha_n$. Dann ist $T_m \neq T_n$. (iii)⇒(i): Annahme $T + \alpha_0, T + \alpha_1, \dots$ sei eine unendliche Folge paarweise verschiedener Vervollständigungen von T. Dann ist $T + \{\neg\alpha_n \mid n \in \mathbb{N}\}$ eine unendliche Erweiterung von T, weil $T + \bigwedge_{\nu \leqslant n} \neg\alpha_\nu \nvDash \neg\alpha_{n+1}$.

3. $\alpha \in T \Leftrightarrow \alpha \in T_i$ für alle $i \leqslant n$; dabei seien $T_0, \dots, T_n$ alle Vervollständigungen von T. Diese sind sämtlich axiomatisierbar, also entscheidbar.

Abschnitt 3.6

1. $x = y \nvDash \forall x\, x = y$. Wegen $\vdash\, \subseteq\, \vDash$ daher auch $x = y \nvdash \forall x\, x = y$.

2. (a): Seien $(\varphi_n)_{n\in\mathbb{N}}$ und $(\mathcal{A}_n)_{n\in\mathbb{N}}$ effektive Aufzählungen aller Aussagen bzw. aller endlichen T-Modelle. Man notiere im n-ten Schritt alle φ_i für $i \leqslant n$ mit $\mathcal{A}_n \vDash \varphi_i$.
(b): Seien $(\alpha_n)_{n\in\mathbb{N}}$ und $(\beta_n)_{n\in\mathbb{N}}$ effektive Aufzählungen der in T beweisbaren bzw. widerlegbaren Aussagen. Jedes $\alpha \in \mathcal{L}^0$ kommt in genau einer dieser Folgen vor.

3. Auch Bedingung (ii) aus Übung 2 ist erfüllt, weil nur endliche viele Axiome in einer endlichen Struktur auf ihre Gültigkeit getestet werden müssen.

Abschnitt 3.7

1. Für **H**: Sei h Homomorphismus: $ht^{\mathcal{A},w} = t^{\beta,hw}$ mit $x^{hw} = hx^w$. Für **S** siehe (3) in **2.3**. Für **P**: Sei $\mathcal{B} = \prod_{i\in I} \mathcal{A}_i$. Dann ist $t^{\mathcal{B},w} = (t^{\mathcal{A}_i,w_i})_{i\in I}$ mit $x^w = (x^{w_i})_{i\in I}$.

2. In $\mathcal{L}^1_Q$ ist $\alpha_{\text{üa}} := \mho x\, x = x$ eine Aussage mit $\mathcal{A} \vDash \alpha_{\text{üa}} \;\Leftrightarrow\;$ *A ist überabzählbar*. In $\mathcal{L}_{II}$ formalisiere man die Aussage 'es gibt eine lückenlose Ordnung ohne größtes Element'. Eine solche ist immer überabzählbar, wie G. Cantor bewies.

3. Sei α die Konjunktion aller Axiome für geordnete Körper unter Einschluß des in $\mathcal{L}_{II}$ leicht formulierbaren Stetigkeitsaxioms Seite 86. Diese legt den Körper der reellen Zahlen bis auf Isomorphie eindeutig fest. Sei ferner β die in $\mathcal{L}_{II}$ ebenfalls leicht formulierbare Aussage 'Jede überabzählbare Teilmenge des Trägers $\mathbb{R}$ ist zu $\mathbb{R}$ gleichmächtig'. Es gibt eine $\gamma := \alpha \wedge \beta$ erfüllende $\mathcal{L}_{II}$-Struktur genau dann, wenn CH gilt. Andernfalls ist $\neg\gamma$ eine Tautologie.

Abschnitt 4.1

1. Sei $\mathcal{B} = \prod_{i\in I} \mathcal{A}_i$. Es genügt, $(\star)$ $\mathcal{A}_i \vDash \alpha\ [w_i] \Leftrightarrow \beta \vDash \alpha\ [w]$ mit $x^w = (x^{w_i})_{i\in I}$ induktiv für Basis-Hornformeln zu beweisen. Beachte dabei $t^{\mathcal{B},w} = (t^{\mathcal{A}_i,w_i})_{i\in I}$. $(\star)$ ergibt leicht die Induktionsschritte über $\wedge, \forall, \exists$.

3. Eine Menge positiver Hornformeln hat stets ein 1-elementiges Modell.

Abschnitt 4.2

1. Für $w_1 \vDash p_1, p_3, \neg p_2$ und $w_2 \vDash p_2, p_3, \neg p_1$ ist $w_1 \vDash \mathcal{P}$ und $w_2 \vDash \mathcal{P}$, aber es gibt keine Belegung $w \leqslant w_1, w_2$ mit $w \vDash \mathcal{P}$.

2. Für beliebiges $w \vDash \mathcal{P}$ folgt $w \vDash p_{m,n,m+n}$ induktiv über n, also $w_{\mathcal{P}} \leqslant w$.

3. (a) Resolutionssatz. (b) $w_{\mathcal{P}} \vDash \neg p_{n,m,k}$ für $k \neq n + m$.

Abschnitt 4.3

2. $\Rightarrow$: Annahme $x_i \in var\, t_j$. Dann $x_i^\sigma = t_j \neq t_j^\sigma = x_i^{\sigma^2}$.

3. Sei ω Unifikator von $K_0 \cup K_1$, also $K_0^\omega = K_1^\omega$. Sei $x^{\omega'} = x^{\rho\omega}$ für $x \in var\, K_0$ und $x^{\omega'} = x^\omega$ sonst. Dann ist $K_0^{\rho\omega'} = K_0^{\rho^2\omega} = K_0^\omega$ (beachte $\rho^2 = \iota$), sowie $K_1^{\omega'} = K^\omega$.

Abschnitt 4.4

1. Seien K_0, K_1 zerlegt wie in der Definition von UR und sei ρ ein Separator von K_0, K_1, sowie ω' definiert wie im Hinweis zu Übung 3 in **4.3**.

2. Man vereinige $\mathcal{P}_g$ und $\mathcal{P}_h$ und füge dem Resultat noch folgende Klauseln hinzu: $r_f(\vec{x}, 0, u) :- r_g(\vec{x}, u)$ und $r_f(\vec{x}, Sy, u) :- r_f(\vec{x}, y, v), r_h(\vec{x}, y, v, u)$.

3. Man füge den Programmen noch $r_f\vec{x}u :- r_{g_1}\vec{x}y_1, \ldots, r_{g_m}\vec{x}y_m, r_h\vec{y}u$ hinzu.

Abschnitt 5.1

3. Seien $a, b, c \in \mathbb{R}$ mit $a < b, c$. Die lineare Funktion $x \mapsto \frac{a-c}{a-b} \cdot x + \frac{c-b}{a-b} \cdot a$ vermittelt einen Automorphismus des (reellen) Intervalls $[a, b]$ auf das Intervall $[a, c]$.

4. O.B.d.A. sei $A \cap B = \emptyset$. Es genügt zu zeigen $D_{el}\mathcal{A} \cup D_{el}\mathcal{B}$ ist konsistent.

5. (a): $\{t^\mathcal{A} \mid t \in \mathcal{T}_E\}$ ist abgeschlossen gegenüber allen $f^\mathcal{A}$, ist also identisch mit dem Träger von $\mathcal{A}$. (b): $\mathcal{B} \vDash T + D_E\mathcal{A}$ läßt sich zu einem $\mathcal{B}' \vDash T + D\mathcal{A}$ expandieren: Für $a \in A \setminus E$ mit $a = t^\mathcal{A}$ und $t \in \mathcal{T}_E$ gemäß (a) sei $a^{\mathcal{B}'} = t^\mathcal{B}$ $(= t^\mathcal{A})$.

Abschnitt 5.2

2. IS auf $\alpha(x_n) = \forall x_0 \cdots x_{n-1}(\bigwedge_{i<n} \mathtt{S}x_i = x_{i+1} \to x_n \neq x_0)$ anwenden.

3. Sei $a \in G \vDash T$ und $\frac{a}{n}$ das Element mit $n\frac{a}{n} = a$, sowie $\frac{m}{n}\colon a \mapsto m\frac{a}{n}$ für $\frac{m}{n} \in \mathbb{Q}$. Dadurch wird G zur Vektorgruppe eines $\mathbb{Q}$-Vektorraums.

4. (b): Behauptung zuerst für beliebige Konjunktion aus den α_i und ihren Negationen beweisen. Beachte $\alpha_i \wedge \alpha_j \equiv_T \bot$ für $i \neq j$ und $\vdash_T \bigvee_{i \leqslant m} \alpha_i$.

Abschnitt 5.3

1 $(\mathcal{A}, \vec{a}) \sim_k (\mathcal{B}, \vec{b}) \Leftrightarrow a_i \mapsto b_i$ $(i = 1, \ldots, n)$ ist partieller Isomorphismus.

2. In Runde 1 spiele II beliebig, danach gemäß den Gewinnstrategien für Modelle von SO_{01} bzw. SO_{10} in den beiden Zerlegungshälften.

3. Falls I mit $a \in A$ beginnt und rechts und links von a mindestens 2^{n-1} Elemente verbleiben, wähle II entsprechend. Sonst mit Elementen derselben Distanz vom linken bzw. rechten Randelement antworten.

4. Fallunterscheidung ob $\mathcal{A} \vDash \mathsf{SO}$ unendlich oder endlich ist. Im ersten Falle folgt die Behauptung aus der Vollständigkeit aller Theorien $\mathsf{SO}_{ij} \cup \{\exists_i \mid i > 0\}$.

Abschnitt 5.4

1. Jeder Halbverband $(A, \cap)$ ist durch $a \mapsto \{x \in A \mid x \leqslant a\}$ in den Mengenhalbverband $(\mathfrak{P}A, \cap)$ einbettbar. Dabei sei $\leqslant$ die Halbordnung von $(A, \cap)$, Seite 39.

3. Sei A geordnet. Ersetzt man jedes $a \in A$ durch ein Exemplar von $(\mathbb{Z}, <)$ bzw. von $(\mathbb{Q}, <)$, so entsteht eine diskrete Ordnung bzw. eine dichte Ordnung $B \supseteq \mathcal{A}$.

4. Sei $\mathcal{A}_0 \vDash T_0$. Wähle $\mathcal{A}_1$ mit $\mathcal{A}_0 \subseteq \mathcal{A}_1 \vDash T_1$, $\mathcal{A}_2$ mit $\mathcal{A}_1 \subseteq \mathcal{A}_2 \vDash T_0$ usw. Das ergibt eine Kette $\mathcal{A}_0 \subseteq \mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \dots$ mit $\mathcal{A}_{2i} \vDash T_0$, $\mathcal{A}_{2i+1} \vDash T_1$. Dann ist $\bigcup_{i\in\mathbb{N}} \mathcal{A}_{2i} = \bigcup_{i\in\mathbb{N}} \mathcal{A}_{2i+1} \vDash T$. Also sind T, T_i modellverträglich.

5. Die Vereinigung S einer Kette von mit T modellverträglichen induktiven Theorien ist wieder induktiv. S hat denselben $\forall$-Teil wie T, ist mit T also auch modellverträglich. Also gibt es nach dem Zornschen Lemma eine maximale, und nach Übung 4 damit auch eine größte Theorie dieser Art.

Abschnitt 5.5

1. Für $i \neq 0$ oder $j \neq 0$ besitzt DO_{ij} Modelle $\mathcal{A} \subseteq \mathcal{B}$ mit $\mathcal{A} \not\preccurlyeq \mathcal{B}$.

2. (a) Lindströms Kriterium. T ist $\aleph_1$-kategorisch, denn ein T-Modell kann als $\mathbb{Q}$-Vektorraum verstanden werden. (b) Jedes T_0-Modell G ist in ein T-Modell H einbettbar; man gewinnt ein solches H, indem auf der Menge aller Paare $\frac{a}{n}$ mit $a \in G$ und $n \in \mathbb{Z}\setminus\{0\}$ eine geeignete Äquivalenzrelation definiert wird.

3. Eindeutigkeit folgt ähnlich wie die der Modellvervollständigung.

4. Der algebraische Abschluß $\overline{\mathcal{F}_p}$ des Primkörpers $\mathcal{F}_p$ der Charakteristik p hat die Darstellung $\overline{\mathcal{F}_p} = \bigcup_{n\geqslant 1} \mathcal{F}_{p^n}$, wobei $\mathcal{F}_{p^n}$ den endlichen Körper aus p^n Elementen bezeichnet. Ferner gilt eine in allen a.a. Körpern mit Primzahlcharakteristik gültige Aussage bereits in allen a.a. Körpern.

Abschnitt 5.6

1. Seien $\mathcal{A}, \mathcal{B} \vDash \mathsf{ZG}_0$, $\mathcal{A} \subseteq \mathcal{B}$. Dann auch $\mathcal{A}', \mathcal{B}'$, denn das Prädikat $m|$ hat in ZG eine $\forall$- und eine $\exists$-Definition. Also $\mathcal{A}' \subseteq_{ec} \mathcal{B}'$, mithin $\mathcal{A} \subseteq_{ec} \mathcal{B}$.

2. Induktiv über quantorenfreies $\varphi = \varphi(x)$ ergibt sich: für jedes $\mathcal{A} \vDash \mathsf{RCF}^\circ$ ist $\varphi^{\mathcal{A}}$ oder $(\neg\varphi)^{\mathcal{A}}$ endlich, was für $\alpha(x)$ nicht der Fall ist.

4. Die Gruppe $2\mathbb{Z}$ ist Substruktur der geordneten Gruppe $\mathbb{Z}$, aber nicht $2\mathbb{Z} \preccurlyeq \mathbb{Z}$.

Abschnitt 5.7

1. Sei $\{\mathcal{A}_i \mid i \in I\} = \{\mathcal{A}_0, \dots, \mathcal{A}_n\}$ und $I_\nu = \{i \in I \mid \mathcal{A}_i = \mathcal{A}_\nu\}$, also $I = I_0 \cup \dots \cup I_n$. Damit gehört genau eines der I_ν zu F (Induktion über n).

3. Behauptung indirekt beweisen. Seien I, J_α, F definiert wie in Korollar **7.3**, sowie $\mathcal{A}_i \in \boldsymbol{K}$ und $w_i\colon AV \to A_i$ derart, daß $w_i\alpha \in D^{\mathcal{A}_i}$ für $\alpha \in i$, $w_i\varphi \notin D^{\mathcal{A}_i}$, $\mathcal{C} := \prod_{i\in I}^F \mathcal{A}_i$ $(\in \boldsymbol{K})$ und $w = (w_i)_{i\in I}$. Dann ist $wX \subseteq D^{\mathcal{C}}$, also $X \nvDash_{\mathcal{C}} \varphi$.

4. O.B.d.A. ist $\mathcal{A} = \mathit{2}$ und $\mathit{2} \subseteq \mathcal{B} \subseteq \mathit{2}^I$ für gewisses I nach dem Stoneschen Repräsentationssatz (siehe **2.1**). $\mathit{2} \vDash \alpha \Rightarrow \mathit{2}^I \vDash \alpha \Rightarrow \mathcal{B} \vDash \alpha$ nach Satz 7.2.

Abschnitt 6.1

1. $\Rightarrow$: $\chi_{\mathrm{graph}\,f} = \sigma|f\vec{a} - b|$. $\Leftarrow$: $f\vec{a} = \mu b[f\vec{a} = b]$.

2. $b \in \mathit{ran}\, f \;\Leftrightarrow\; (\exists a{\leqslant}b) fa = b$ und Übung 1.

3. *Injektivität*: Sei $\wp(a,b) = \wp(a',b')$. Wäre $a+b < a'+b'$, so $a+b+1 \leqslant a'+b'$, also $\wp(a,b) \leqslant \frac{1}{2}(a'+b')^2 + a < \frac{1}{2}(a'+b')(a'+b'+1) \leqslant \wp(a',b')$. Also $a+b = a'+b'$. Dann aber $a = a'$, und daher auch $b = b'$. *Surjektivität*: Sei $c \in \mathbb{N}$ und d die größte Zahl mit $\frac{d(d+1)}{2} = 1 + 2 + \ldots + d \leqslant c$, sowie $a := c - \frac{d(d+1)}{2}$. Es ist $a \leqslant d$, so daß $b := d - a \in \mathbb{N}$. Dann gilt $\wp(a,b) = c$.

4. $\Rightarrow$: Sei $M = \{b \in \mathbb{N} \mid \exists a Rab\}$, R rekursiv, $c \in M$ fest gewählt. Sei $fn = b$, falls $(\exists a{\leqslant}n)\, n = \wp(a,b)$ & Rab, und $fn = c$ im anderen Falle. Dann gilt $M = \mathit{ran}\, f$. $\Leftarrow$: $M = \{b \in \mathbb{N} \mid (\exists a \in \mathbb{N}) fa = b\}$ und Übung 1.

Abschnitt 6.2

1. Es sei $\alpha_0, \alpha_1, \ldots$ eine rekursive Aufzählung von X. Nach Übung 2 in **6.1** ist dann $\{\beta_n \mid n \in \mathbb{N}\}$ mit $\beta_n = \underbrace{\alpha_n \wedge \ldots \wedge \alpha_n}_{n}$ rekursiv und gewiß ein Axiomensystem für T.

3. (a): Sei $\Phi_n = (\varphi_0, \dots, \varphi_n)$ ein Beweis von $\varphi = \varphi_n$ in $T + \alpha$. Angenommen es sind Beweise Φ'_k für $\alpha \to \varphi_k$ zu $\Phi_i = (\varphi_0, \dots, \varphi_i)$ für alle $i < n$ schon konstruiert. Man definiere einen Beweis Φ'_n für $\alpha \to \varphi$ durch p.r. Fallunterscheidung nach den Fällen $\varphi = \alpha$, $\varphi \in X \cup \Lambda$ (X ein Axiomensystem für T) und φ resultiert aus φ_k und φ_m mit MP ($k, m < n$). Siehe den Beweis von Lemma 1.6.3.

4. Zeige dies zuerst für Gleichungen. Konstruiere in p.r. Weise zu jedem t eine Normalform $\mathrm{Nf}(t) = \underline{a_0} + \sum_{1 \leqslant \nu \leqslant n} \underline{a_\nu} \cdot \boldsymbol{v}_0^{k_0^\nu} \cdot \ldots \cdot \boldsymbol{v}_n^{k_n^\nu}$ mit $\mathcal{N} \vDash t_1 = t_2 \;\Leftrightarrow\; \mathrm{Nf}(t_1) = \mathrm{Nf}(t_2)$.

Abschnitt 6.3

1. $\exists\vec{x}\alpha \equiv_{\mathcal{N}} \exists y(\exists x_1{\leqslant}y)\dots(\exists x_n{\leqslant}y)\alpha$ mit $y \notin \mathit{var}\,\alpha$. Für eine Belegung $\vec{a}$ von $\vec{x}$ belege y mit $\max\{a_1, \dots, a_n\} + 1$. Analog $\forall\vec{x}\alpha \equiv_{\mathcal{N}} \forall y(\forall x_1{\leqslant}y)\dots(\forall x_n{\leqslant}y)\alpha$

2. $(\forall y{<}x)\exists z\alpha \equiv_{\mathsf{PA}} \exists u(\forall y{<}x)(\exists z{<}u)\alpha$, siehe Übung 3(c) in **3.3**.

Abschnitt 6.4

1. $\Leftarrow$: Sei $xa + 1 = yb$ und $p|a$, p Primzahl. Dann $p\nmid b$ weil sonst $p|yb - xa = 1$. $\Rightarrow$: $<$-Induktion über $s = a + b$. Richtig für $s \leqslant 2$ (d.h. $a = b = 1$) mit $x = 0$, $y = 1$. Sei $s > 2$. Dann ist $a \neq b$, etwa $a > b$, also auch $a - b \perp b$. Da $(a-b)+b < s$, gibt es $x, y' \in \mathbb{N}$ mit $x(a - b) + 1 = y'b$. Also $xa + 1 = yb$ mit $y = x + y'$.

2. (a): $p\nmid a \;\Rightarrow\; a \perp p \;\Rightarrow\; \exists xy\, xa + 1 = yp \;\Rightarrow\; \exists xy\, b = yp - xab \;\Rightarrow\; p|b$. (b): folgt aus (a) weil $\mathrm{kgV}\{a_\nu | \nu{<}n\} | \mathrm{kgV}\{a_\nu | \nu{\leqslant}n\}$ (Division mit Rest).

3. $$\exists u[\mathtt{beta}\, u0 = \underline{2} \wedge (\forall v{<}x)(\exists\, w, w'{\leqslant}y)(\mathtt{beta}\, uvw \wedge \mathtt{beta}\, u\mathrm{S}vw' \\ \wedge\, w < w' \wedge \mathsf{prim}\, w' \wedge (\forall z{<}w')(\mathsf{prim}\, z \to z{\leqslant}w) \wedge \mathtt{beta}\, uxy].$$

4. (a): Zeige dies zuerst für x anstatt für $\vec{x}$. (b): Es genügt zu zeigen $\mathrm{sb}_x(\dot{\varphi}) = \dot{\varphi}$ for $x \notin \mathit{frei}\,\varphi$. Beachte $\mathrm{sb}_x((\forall x\alpha)^{\boldsymbol{\cdot}}, x) = (\forall x\alpha)^{\boldsymbol{\cdot}}$ für Aussagen α.

Abschnitt 6.5

2. (ii)$\Rightarrow$(i): Ist T vollständig und $T' + T$ konsistent, so ist $T' \subseteq T$.

3. Das ist trivial, falls $T + \Delta$ inkonsistent ist. Andernfalls sei $\varkappa$ die Konjunktion aller $\forall\vec{x}\,\exists!y\alpha(\vec{x}, y)$, α durchläuft die definierenden Formeln für Operationen aus Δ. Mit T ist $T + \varkappa$ entscheidbar. Ferner ist $\vdash_{T+\Delta} \alpha \;\Leftrightarrow \vdash_{T+\varkappa} \alpha^{rd}$.

4. Q ist rekursiv aufzählbar aber nicht rekursiv. Beachte Übung 1 in **6.1**.

Abschnitt 6.7

1. Hinweis zu Übung 1 in **6.3** führt auch im Induktionsschritt zum Ziel.

2. Δ_0 ist r.a. aber Δ_1 nicht (Bemerkung 2 in **6.3**). $\dot{\mathsf{Q}}$ ist Σ_1 aber nicht Δ_1.

3. Man beweise nacheinander (a) $\{\pi \in \mathcal{L}_{ar} \,|\, \pi$ Primformel und $\mathcal{N} \vDash \pi\}$ ist rekursiv und daher Δ_1, (b) Ist X ($\subseteq \mathcal{L}^0_{ar}$) Δ_n und Y die Menge der Boolschen Kombinationen von X so ist mit $\{\alpha \in X \,|\, \mathcal{N} \vDash \alpha\}$ auch $\{\beta \in Y \,|\, \mathcal{N} \vDash \beta\}$ Δ_n. Man beachte ferner $\{\alpha \in \mathcal{L}^0_{ar} \,|\, \mathrm{qr}\,\alpha = n\}$ ist Δ_1 und $\mathcal{N} \vDash \forall x\varphi \;\Leftrightarrow\; \mathcal{N} \vDash \alpha_x(\underline{n})$ für alle n.

Abschnitt 7.1

1. $\vdash_{\mathsf{PA}} \exists z\varphi(x,y,z)$ mit $\varphi := \underline{2}z = (x+y)^2 + \underline{3}x + y$ induktiv über y beweisen.

2. (a): <-Induktion. (b): Hinweis zu Übung 1 in **6.4** in PA formalisieren.

4. Für $\Box_{T+\alpha}\varphi \vdash_T \Box_T(\alpha \to \varphi)$ nutze man Übung 3 in **6.2**.

Abschnitt 7.2

1. $\vdash_T \Box\alpha \to \alpha \Rightarrow \vdash_T \neg\Box\alpha \Rightarrow \vdash_{T'} \mathtt{Con}_{T'}$, weil nach (5) $\mathtt{Con}_{T'} \equiv_T \neg\Box\neg\neg\alpha \equiv_T \neg\Box\alpha$. Damit ist T' nach Satz 2.2 inkonsistent, also $\vdash_T \alpha$.

3. Induktionsannahme $T^n = T + \neg\Box^n\bot$ und $\mathtt{Con}_T \equiv_T \neg\Box^{n+1}\bot$. Wegen $\Box^n\bot \vdash_T \Box^{n+1}\bot$ also $\neg\Box^{n+1}\bot \vdash_T \neg\Box^n\bot$. Somit $T^{n+1} = (T + \neg\Box^n\bot) + \neg\Box^{n+1}\bot \equiv_T T + \neg\Box^{n+1}\bot$. Ferner ist nach (5) in **7.2** $\mathtt{Con}_{T^{n+1}} \equiv_T \neg\Box(\neg\neg\Box^n\bot) \equiv \neg\Box^{n+1}\bot$.

4. Für jede (nicht formalisierte) arithmetische Aussage A ist der Satz 'Wenn A in PA beweisbar ist, so A' in ZFC beweisbar (man beachte PA ist interpretierbar in ZFC, siehe **6.6**). Formalisiert: $\vdash_{\mathsf{ZFC}} \Box_{\mathsf{PA}}\alpha \to \alpha$; dabei sei A durch α formalisiert.

Abschnitt 7.4

1. Man beweist zuerst $\mathsf{G}_n = \{H \in \mathcal{F}_\Box \,|\, \vdash_{\mathsf{G}} \Box^{n+1}\bot \to H\}$. Damit ist
$$\begin{aligned} \vdash_{\mathsf{G}_n} H \;\Leftrightarrow \vdash_{\mathsf{G}} \Box^{n+1}\bot \to H &\Leftrightarrow \vdash_{\mathsf{PA}} (\Box^{n+1}\bot \to H)^\imath \text{ für alle } \imath && \text{(Satz 4.2)}\\ &\Leftrightarrow \vdash_{\mathsf{PA}} \Box^{n+1}\bot \to H^\imath \text{ für alle } \imath && \text{(Eigenschaft von } \imath)\\ &\Leftrightarrow \vdash_{\mathsf{PA}_n} H^\imath \text{ für alle } \imath && (\mathsf{PA}_n = \mathsf{PA} + \Box^n\bot). \end{aligned}$$

2. Sei $\mathsf{PA}^n_\bot := \mathsf{PA}^n + \neg\,\mathtt{Con}_{\mathsf{PA}^n}$. Nach (6) in **7.2** ist $\mathtt{Con}_{\mathsf{PA}^n_\bot} \equiv_{\mathsf{PA}} \mathtt{Con}_{\mathsf{PA}}$. Nach Übung 2 in **7.2** daher $\mathsf{PA}^n_\bot = (\mathsf{PA} + \neg\Box^n\bot) + \neg\neg\Box^{n+1}\bot = \mathsf{PA} + \neg\Box^n\bot \wedge \Box^{n+1}\bot$. Ferner haben wir $\Box\,\mathtt{Con}_{\mathsf{PA}} \vee \Box\neg\,\mathtt{Con}_{\mathsf{PA}} \equiv_{\mathsf{PA}} \Box\bot \vee \Box^2\bot \equiv_{\mathsf{PA}} \Box^2\bot$. Also $T = \mathsf{PA} + \Box^3\bot \wedge \neg\Box^2\bot = \mathsf{PA}^2_\bot$.

3. $\nvdash_{\mathsf{G}^*} \neg[\neg\Box(p \to q) \wedge \neg\Box(\neg p \to q) \wedge \neg\Box(p \to \neg q) \wedge \neg\Box(\neg p \to \neg q)]$ und Satz 4.4.

Literatur

[As] G. Asser, *Einführung in die mathematische Logik*, Teil III, Teubner 1981.

[Ba] J. Barwise (Herausgeber), *Handbook of Mathematical Logic*, North-Holland 1977.

[BD] A. Berarducci, P. D'Aquino, Δ_0*-complexity of* $y = \prod_{i \leqslant n} F(i)$, Ann. Pure Appl. Logic 75 (1995), 49-56.

[Be1] L.D. Beklemishev, *On the classification of propositional provability logics*, in L. Beklemishev, M. Pentus, N. Vereshchagin, Provability, Complexity and Grammars, AMS Translations Ser.2 vol 192 (1999) 1-56.

[Be2] ——— *Iterated local reflection versus iterated consistency*, Ann. Pure Appl. Logic 75 (1995), 25-48.

[Be3] ——— *Bimodal Logics for Extensions of Arithmetical Theories*, Journ. Symb. Logic 61 (1996), 91-124.

[Be4] ——— *Parameter free Induction and Reflection*, in *Computational Logic and Proof Theory*, LN Comp. Science 1289, Springer 1997.

[BM] J. Bell, M. Machover, *A Course in Mathematical Logic*, North-Holland 1977.

[BF] J. Barwise, S. Feferman (Herausgeber), *Model-Theoretic Logics*, Springer 1985.

[BP] P. Benacerraf, H. Putnam (Editor), *Philosophy of Mathematics, Selected Readings*, 2. Aufl. Cambridge Univ. Press 1993.

[Bi] G. Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Phil. Soc. 50 (1935), 433 - 455.

[BGG] E. Börger, E. Grädel, J. Gurevich, *The classical decision problem*, Springer 1997.

[Boo] G. Boolos, *The Logic of Provability*, Cambridge Univ. Press 1993.

[BJ] G. Boolos, R. Jeffrey, *Computability and Logic*, 3. Aufl. Cambridge Univ. Press 1992.

[Bue] S. Buechler, *Essential Stability Theory*, Springer 1996.

[Bu] S.R. Buss (Hrsg.), *Handbook of Proof Theory*, Elsevier 1998.

[Ca] G. Cantor, *Gesammelte Abhandlungen*, Springer 1980.

[CK] C.C. Chang, H.J. Keisler, *Model Theory*, 3. Aufl. North-Holland 1990.

[Ch] A. Church, *A Note on the Entscheidungsproblem*, Jour. Symb. Logic 1 (1936), 40-41.

[Da] D. van Dalen, *Logic and Structure*, 2. Aufl. Springer 1983.

[De] R. Dedekind, *Was sind und was sollen die Zahlen?*, (Braunschweig 1888), Vieweg 1969.

[Do] K. Doets *From Logic to Logical Programming*, MIT-Press 1994.

[Eb] H. Ebbinghaus, *Einführung in die Mengenlehre*, B.I. Verlag 1994.

[EFT] H. Ebbinghaus, J. Flum, W. Thomas, *Einführung in die Mathematische Logik*, B.I. Verlag 1992.

[En] H. Enderton, *A Mathematical Introduction to Logic*, Acad. Press 1972.

[Fe1] W. Felscher, *Berechenbarkeit*, Springer 1993.

[Fe2] W. Felscher, *Lectures on Mathematical Logic, Vol. 1-3*, Gordon & Breach 2000.

[Fr] G. Frege, *Begriffsschrift*, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens (Halle 1879), Olms 1971.

[FS] H. Friedman, M. Sheard, *Elementary descent Recursion and Proof Theory*, Arch. Pure & Appl. Logic 71 (1995), 1-47.

[GJ] M.R. Garey, D.S. Johnson, *Computers and Intractability*, A Guide to the Theory of NP-Completeness, Freeman 1979.

[Ge] G. Gentzen, *Untersuchungen über das logische Schließen*, Mathematische Zeitschrift 39 (1934/35), 176-210, 405-431.

[Go1] K. Gödel, *Die Vollständigkeit der Axiome des logischen Funktionenkalküls*, Monatshefte Math. u. Physik 37 (1930), 349 - 360, oder *Collected Works* I.

[Go2] ———, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik 38 (1931).

[Go3] ———, *Collected Works*, Oxford Univ. Press, Vol. I 1986, Vol. II 1990, Vol. III 1995.

[GH] H. Goltz, H. Herre, *Grundlagen der logischen Programmierung*, Akademieverlag 1989.

[Gor] S.N. Goryachev, *On the Interpretability of some Extensions of Arithmetic*, Math. Notes 40 (1986), 561-572.

[Gr] G. Grätzer, *Universal Algebra*, 2. Aufl. Springer 1979.

[HP] P. Hajek, P. Pudlak, *Metamathematics of First-order Arithmetic*, Springer 1993.

[Hej] J. Heijenoort, *From Frege to Gödel*, Harvard Univ. Press 1967.

[Hei] L. Heindorf, *Elementare Beweistheorie*, B.I. Verlag 1994.

[He] L. Henkin, *The Completeness of the First-order Functional Calculus*, Journ. Symb. Logic 14 (1949), 159 - 166.

[Her] J. Herbrand, *Recherches sur la théorie de la démonstration*, siehe [Hej].

[HR] H. Herre, W. Rautenberg, *Das Basistheorem und einige Anwendungen in der Modelltheorie,* Wiss. Zeitsch. Humboldt-Univ. 19 (1970), 575-577.

[HeR] B. Herrmann, W. Rautenberg, *Finite Replacement and Hilbert-style Axiomatizability,* Zeitsch. Math. Log. Grundl. Math. 38 (1982), 327-344.

[HB] D. Hilbert, P. Bernays, *Grundlagen der Mathematik*, Band I Springer 1934, Band II Springer 1939.

[Ho] W. Hodges, *Model Theory*, Cambridge Univ. Press 1993.

[Id] P. Idziak, *A Characterization of Finitely Decidable Congruence Modular Varieties*, Trans. Am. Math. Soc. 349 (1997), 903-934.

[Ig] K. Ignatiev, *On Strong Provability Predicates*, Journ. Symb. Logic 58 (1993), 249-290.

[Ih] T. Ihringer, *Allgemeine Algebra*, Teubner 1988.

[JK] R. Jensen, C.Karp, *Primitive recursive Set Theory*, in *Axiomatic Set Theory*, AMS 1971, 143-167.

[Ka] R. Kaye, *Models of Peano Arithmetic*, Clarendon Press 1991.

[Ke] H.J. Keisler, *Logic with the Quantifier "there exist uncountably many"*, Ann. Pure Appl. Logic 1 (1970), 1-93.

[Kl] S. Kleene, *Introduction to Metamathematics*, Wolters-Noordhoff 1988.

[KR] I. Korec, W. Rautenberg, *Model Interpretability into Trees and Applications*, Arch. Math. Logik 17 (1976), 97 -104.

[Kr] M. Kracht, *Tools and Technique in Modal Logic*, Elsevier (Studies in Locic 142), 1999.

[KK] G. Kreisel, J. Krivine, *Modelltheorie*, Springer 1972.

[Kra] J. Krajiček, *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Cambridge University Press 1995.

[Ku] K. Kunen, *Set Theory. An Introduction to Independence Proofs*, North-Holland 1980.

[Li] P. Lindström, *On Extensions of Elementary Logic*, Theoria 35 (1969), 1-11.

[Ll] J.W. Lloyd, *Foundations of Logic Programming*, Springer 1987.

[Lo] M. Löb, *Solution of a Problem of Leon Henkin*, Journ. Symb. Logic 20 (1955), 115-118.

[Ma] J. Malitz, *Introduction to Mathematical Logic*, Springer 1979.

[Mal] I. Malcev, *The Metamathematics of Algebraic Systems*, North-Holland 1971.

[Mat] Y. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press 1993.

[Me] E. Mendelson, *Introduction to Mathematical Logic*, Van Nostrand 1979.

[Mo] D. Monk, *Mathematical Logic*, Springer 1976.

[ML] G. Müller, W. Lenski (Herausgeber) *The Ω-Bibliography of Mathematical Logic*, Springer 1987.

[MV] R. McKenzie, M. Valeriote, *The Structure of Decidable Locally Finite Varieties*, Progress in Math. 79, Birkhäuser 1989.

[Ob] A. Oberschelp, *Rekursionstheorie,* B.I. Verlag 1993.

[WP] J. Paris, A. Wilkie, *On the Scheme of Induction for Bounded Arithmetic Formulas,* Ann. of Pure & Appl. Logic 35 (1987), 261-302.

[Po] W. Pohlers, *Proof Theory – An Introduction*, Springer Lecture Notes 1407 (1989).

[Pr] A. Prestel, *Einführung in die Mathematische Logik und Modelltheorie*, Vieweg 1986.

[RS] H. Rasiowa, R. Sikorski, *The Mathematics of Metamathematics*, Polish Scientific Publ. 1968.

[RZ] W. RAUTENBERG, M.ZIEGLER *Recursive Inseparability in Graph Theory,* Notices Am. Math. Soc. 22 (1975).

[Ra1] W. RAUTENBERG, *Klassische und Nichtklassische Aussagenlogik*, Vieweg 1979.

[Ra2] ———, *Elementare Grundlagen der Analysis,* B.I. Verlag 1993.

[Ri] M. RICHTER, *Logikkalküle*, Teubner 1978.

[Ro1] A. ROBINSON, *Introduction to Model Theory and to the Metamathematics of Algebra*, North-Holland 1974.

[Ro2] A. ROBINSON, *Non-Standard Analysis*, North-Holland 1970.

[Ro] J. ROBINSON, *A Machine-oriented Logic based on the Resolution Principle*, Journ. Ass. Comp. Machinery 12 (1965), 23-41.

[Rog] H. ROGERS, *Theory of Recursive Functions and Effective Computability*, 2. Aufl. MIT Press 1988.

[Ros] J.B. ROSSER, *Extensions of some Theorems of Gödel and Church*, Journ. Symb. Logic 1 (1936), 115-118.

[Rot] P. ROTHMALER, *Einführung in die Modelltheorie*, Spectrum Akad. Verlag, 1995.

[Sa] G. SACKS, *Saturated Model Theory*, Benjamin Reading 1972.

[Sam] G. SAMBIN, *An Effective Fixed Point Theorem in Intuitionistic Diagonalizable Algebras*, Studia Logica 35 (1976), 345-361.

[Scho] U. SCHÖNING, *Logik für Informatiker*, B.I. Verlag 1992.

[Se] A. SELMAN *Completeness of Calculi for Axiomatically Defined Classes*, Algebra Universalis 2 (1972), 20-32.

[Sh] S. SHELAH *Classification Theory and the Number of Nonisomorphic Models*, North-Holland 1978.

[Shoe] J. SHOENFIELD, *Mathematical Logic*, Addison-Wesley 1967.

[Si] W. SIEG, *Herbrand Analyses*, Arch Math. Logic 30 (1991), 409 -441.

[Sm] C. SMORYNSKI, *Diagonalization and Self-Reference*, Clarendon Press 1994.

[So] R. SOLOVAY, *Provability Interpretation of Modal Logic*, Israel Jour. Math. 25(1976), 287-304.

[Tan] K. TANAKA, *Reverse Mathematics and Subsystems of Second Order Arithmetic*, AMS Sugaku Expositions **5**, 1992.

[Ta1] A. Tarski, *Der Wahrheitsbegriff in den formalisierten Sprachen*, Studia Philosophica 1 (1936), siehe auch [Ta3].

[Ta2] ———, *A Decision Method for Elementary Algebra and Geometry*, Berkeley 1948, 1951, Paris 1967.

[Ta3] ———, *Logic, Semantics and Metamathematics*, Clarendon Press 1956.

[TMR] A. Tarski, A. Mostowski, R.M. Robinson, *Undecidable Theories*, North-Holland 1971.

[TS] A. Troelstra, H. Schwichtenberg, *Basic Proof Theory*, Cambridge Univ. Press 1996.

[Tu] A. Turing, *On Computable Numbers, with an Application to the Entscheidungsproblem*, Proceedings of the London Mathematical Society 42 (1936/37) und 43 (1937).

[TW] P. Tuschik, H. Wolter, *Einführung in die Mathematische Logik*, B.I. Verlag 1994.

[Vi] A. Visser, *An Overview of Interpretability Logic*, *Advances in Modal Logic 1996*, Lecture Notes CSLI (Hrsg. M. Kracht et al.), Stanford 1998.

[Wa] F. Wagner, *Simple Theories*, Kluwer 2000.

[Wae] B. van der Waerden, *Algebra I*, Springer 1964.

[WR] A. Whitehead, B. Russell, *Principia Mathematica,* Cambridge Univ. Press 1910.

[Wi] A. Wilkie, *Model Completeness Results for Expansions of the Ordered Field of Real Numbers...,* Journ. Am. Math. Soc. 9 (1996), 1051-1094.

[Zi] M. Ziegler, *Model Theory of Moduls*, Ann. Pure Appl. Logic 26 (1984), 149-213.

Stichwortverzeichnis

Symbolverzeichnis