# Mathematische Logik

Helmut Schwichtenberg

Mathematisches Institut der Universität München
Wintersemester 1994/95

# Vorwort

Das vorliegende Skriptum gibt den Inhalt einer vierstündigen Vorlesung "Mathematische Logik I" wieder, die ich im Wintersemester 1994/95 am Mathematischen Institut der Universität München gehalten habe. Hinzugefügt habe ich einen Anhang, in dem die Vollständigkeit der Minimallogik bezüglich Beth–Strukturen bewiesen wird. An vielen Stellen habe ich mich auf die Bücher von Kleene [8], Enderton [3] und Shoenfield [13] sowie auf das Vorlesungsmanuskript von Buchholz [1] gestützt.

Für ihre Unterstützung bei der Vorbereitung dieser Vorlesung und der Korrektur des Skriptums bedanke ich mich bei Dr. Ulrich Berger und Ralph Matthes.

München, im April 1995

Helmut Schwichtenberg

# Inhalt

**Teil I: Logik erster Stufe**
1.1 Einführung . . . . . 1
1.2 Induktion und Rekursion . . . . . 6
1.3 Syntax . . . . . 10
1.4 Semantik . . . . . 17
1.5 Natürliches Schließen . . . . . 20
1.6 Hilbertkalküle . . . . . 38
1.7 Vollständigkeit . . . . . 40
1.8 Anfänge der Modelltheorie . . . . . 46
1.9 Historische Anmerkungen . . . . . 54

**Teil II: Berechenbarkeit**
2.1 Primitiv rekursive Funktionen . . . . . 55
2.2 Rekursive Funktionen, rekursiv aufzählbare Relationen . . . . . 65
2.3 Kodierung der Logik . . . . . 71
2.4 Herbrand–Gödel–Kleene–rekursive Funktionen . . . . . 79

**Teil III: Metamathematik**
3.1 Undefinierbarkeit des Wahrheitsbegriffs . . . . . 82
3.2 Der Wahrheitsbegriff in formalen Theorien . . . . . 84
3.3 Unentscheidbarkeit, Unvollständigkeit . . . . . 86
3.4 Repräsentierbarkeit . . . . . 89
3.5 Unbeweisbarkeit der Konsistenz . . . . . 95
3.6 Historische Anmerkungen . . . . . 98
Anhang Vollständigkeit der Minimallogik . . . . . 99
Literatur . . . . . 104
Index . . . . . 105

# Teil I: Logik erster Stufe

## 1.1 Einführung

Untersuchungsgegenstand der mathematischen Logik sind mathematische Beweise. Bei diesen Untersuchungen werden einige interessante Aspekte mathematischer Beweise zum Vorschein kommen. So ist es zum Beispiel möglich und sinnvoll, zwischen Existenzbeweisen zu unterscheiden, die das als existent nachgewiesene Objekt tatsächlich liefern, und solchen, die dies nicht tun. Als Beispiel betrachten wir die folgende Aussage.

Es gibt irrationale Zahlen $a, b$ mit $a^b$ rational.

Einen Beweis erhält man wie folgt durch Fallunterscheidung.

*Fall* $\sqrt{2}^{\sqrt{2}}$ ist rational. Man wähle $a = \sqrt{2}$ und $b = \sqrt{2}$. Dann sind $a, b$ irrational, und nach Annahme ist $a^b$ rational.

*Fall* $\sqrt{2}^{\sqrt{2}}$ ist irrational. Man wähle $a = \sqrt{2}^{\sqrt{2}}$ und $b = \sqrt{2}$. Dann sind nach Annahme $a, b$ irrational, und

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$$

ist rational. □

Solange wir nicht entschieden haben, ob $\sqrt{2}^{\sqrt{2}}$ nun rational ist oder nicht, wissen wir nicht, welche Zahlen $a, b$ wir nehmen müssen. Damit haben wir ein Beispiel eines Existenzbeweises, der es nicht erlaubt, das als existent nachgewiesene Objekt tatsächlich anzugeben.

In der mathematischen Logik wollen wir also mathematische Beweise untersuchen. Wir beginnen deshalb mit einer Beschreibung wesentlicher Aspekte der Tätigkeit eines Mathematikers, um einen angemessenen Einstieg in die mathematische Logik zu bekommen.

Der Mathematiker studiert Axiomensysteme. Man unterscheidet zwischen klassischen Axiomensystemen, die ein intendiertes Modell möglichst vollständig beschreiben sollen (etwa die natürlichen Zahlen oder die ebene Geometrie) und modernen Axiomensystemen wie etwa denen für Gruppen, Ringe und Körper, die von vornherein so konzipiert sind, daß sie möglichst viele Modelle besitzen. Die Grundbegriffe der jeweiligen mathematischen Disziplin sind dann durch die Axiome implizit bestimmt. Ausgehend von den Grundbegriffen werden weitere Begriffe definiert, die aber prinzipiell entbehrlich sind. Aus den Axiomen werden dann mittels logischer Schlußregeln die Sätze der Theorie hergeleitet.

Das Studium von Axiomensystemen wird uns auf viele weitere Probleme führen, die nur noch lose mit Axiomensystemen in Verbindung stehen.

Einen mathematischen Satz kann man unter zwei Aspekten betrachten: einerseits teilt er einen Inhalt mit (semantischer Aspekt), andererseits liegt er als Zeichenreihe vor (syntaktischer Aspekt). Der semantische Aspekt scheint auf den ersten Blick viel wichtiger zu sein. Es ist jedoch nötig und in manchen Fällen auch ergiebig, sich auch mit dem syntaktischen Aspekt zu befassen. Jedenfalls gehört dies zu dem beabsichtigten Studium von Axiomensystemen.

Die syntaktische Seite eines Axiomensystems fassen wir in dem Begriff eines *formalen Systems* zusammen. Ein formales System ist bestimmt durch

(1) eine (formale) Sprache,

(2) Axiome und

(3) Schlußregeln.

Als Sprache verwendet man am besten eine künstliche, formale Sprache, um Eindeutigkeit und Einfachheit zu gewährleisten. Eine solche Sprache ist bestimmt durch einen Zeichenvorrat (Alphabet) und daraus gebildete Terme (die Objekte bedeuten) und Formeln (die Aussagen bedeuten). Eine Aussage ist nach Aristoteles ein sprachliches Gebilde, von dem es sinnvoll ist zu sagen, es sei wahr oder falsch. Die Axiome sind dann einfach spezielle Formeln, und die Schlußregeln gestatten den Übergang von gewissen (meist endlich vielen) Prämissen auf eine Konklusion — im allgemeinen unter zusätzlichen Bedingungen.

Wir wollen hier eine Klasse von formalen Systemen beschreiben, die auf der Logik erster Stufe basieren. Sie reichen für die Darstellung der üblichen Axiomensysteme der Mathematik aus. Als erstes wollen wir ihre Sprache einführen. Dazu beginnen wir mit einer informalen Diskussion.

Jede Sprache verwendet Begriffe. In unserem Fall einer Sprache über mathematische Gegenstände können wir es uns relativ einfach machen. Hier kann man zwischen logischen und nichtlogischen Begriffen unterscheiden. Wir behandeln zunächst die nichtlogischen Begriffe. Wir legen einen sogenannten Individuenbereich zugrunde (etwa den Bereich $\mathbb{N}$ der natürlichen Zahlen oder die Trägermenge $G$ einer Gruppe) und verstehen dann unter einem Begriff einfach eine Teilmenge des Individuenbereichs; ein Beispiel ist der Primzahlbegriff. In der Sprache muß dann für jeden relevanten Begriff ein Symbol zu seiner Benennung vorhanden sein, etwa $P$ für den Primzahlbegriff; solche Symbole nennt man Relationssymbole. Es ist notwendig, auch mehrstellige Begriffe zuzulassen, etwa die Kleiner–oder–Gleich–Beziehung $n \leq m$ zwischen natürlichen Zahlen. Die zugehörigen Symbole nennt man Relationssymbole.

Ferner brauchen wir in der Mathematik offenbar Funktionen, etwa die Nachfolgerfunktion und die Addition auf $\mathbb{N}$ oder die Gruppenverknüpfung. In der Sprache muß dann für jede vorkommende Funktion ein Symbol zu ihrer Benennung vorhanden sein, etwa suc für die Nachfolgerfunktion, $+$ für die Addition und $\circ$ für die Gruppenverknüpfung; solche Symbole nennt man Funktionssymbole. Jedes Funktionssymbol hat eine feste Stellenzahl. Ferner brauchen wir offenbar in der Sprache Konstanten für einzelne Individuen (etwa 5,

0). Man kann Konstante als entartete (genauer: nullstellige) Funktionssymbole auffassen. Aus den Funktionssymbolen und den Konstanten kann man Terme aufbauen, etwa $\mathrm{suc}(5)$ oder $5+7$. Mit solchen Termen lassen sich dann atomare Formeln bilden, etwa $P(7)$ (mit der Bedeutung "7 ist eine Primzahl") oder $\mathrm{suc}(5) < 9$.

Aus atomaren Formeln kann man dann mittels logischer Verknüpfungen weitere Formeln zusammensetzen, etwa $2 < 3 \wedge P(7)$. Allgemein ist mit $A$ und $B$ auch die Konjunktion $A \wedge B$ (gelesen "$A$ und $B$") eine Formel.

Man beachte, daß die Wahrheit oder Falschheit von $A \wedge B$ allein von der Wahrheit oder Falschheit von $A$ und von $B$ abhängt, nicht von der Bedeutung dieser Aussagen. Wir nehmen deshalb mit Frege an, daß zwei verschiedene Wahrheitswerte $W$ und $F$ gegeben sind. Man beachte, daß es nicht darauf ankommt, was genau die Wahrheitswerte $W$ und $F$ sind, solange sie nur verschieden sind. Man könnte etwa 1 und 0 wählen. Wir betrachten jetzt Wahrheitsfunktionen $H\colon \{W,F\}^n \to \{W,F\}$. Die Konjunktion $\wedge$ wird dann vollständig durch ihre Wahrheitsfunktion $H_\wedge\colon \{W,F\}^2 \to \{W,F\}$ beschrieben, die durch

$$\begin{aligned} &H_\wedge(W,W) = W,\\ &H_\wedge(W,F) = H_\wedge(F,W) = H_\wedge(F,F) = F \end{aligned}$$

bestimmt ist.

Mit $A$ ist auch die Negation $\neg A$ (gelesen "nicht $A$") eine Formel. Die zugehörige Wahrheitsfunktion $H_\neg\colon \{W,F\} \to \{W,F\}$ ist einstellig und bestimmt durch

$$H_\neg(W) = F, \qquad H_\neg(F) = W.$$

Mit $A$ und $B$ ist auch die Disjunktion $A \vee B$ (gelesen "$A$ oder $B$") eine Formel. Man beachte, daß das "oder" hier im nicht ausschließenden Sinn gemeint ist; dies ist in der Mathematik üblich. Bei klassischer Auffassung ist die Disjunktion $\vee$ vollständig durch ihre Wahrheitsfunktion $H_\vee\colon \{W,F\}^2 \to \{W,F\}$ beschrieben, die durch

$$\begin{aligned} &H_\vee(W,W) = H_\vee(W,F) = H_\vee(F,W) = W,\\ &H_\vee(F,F) = F \end{aligned}$$

bestimmt ist. Man beachte, daß dann $A \vee B$ dasselbe bedeutet wie $\neg(\neg A \wedge \neg B)$, also $\vee$ auch durch $\wedge$ und $\neg$ definiert werden kann. Es gilt nämlich

$$\begin{aligned} &H_\neg(H_\wedge(H_\neg(W), H_\neg(W))) = H_\neg(H_\wedge(F,F)) = H_\neg(F) = W = H_\vee(W,W),\\ &H_\neg(H_\wedge(H_\neg(W), H_\neg(F))) = H_\neg(H_\wedge(F,W)) = H_\neg(F) = W = H_\vee(W,F),\\ &H_\neg(H_\wedge(H_\neg(F), H_\neg(W))) = H_\neg(H_\wedge(W,F)) = H_\neg(F) = W = H_\vee(F,W),\\ &H_\neg(H_\wedge(H_\neg(F), H_\neg(F))) = H_\neg(H_\wedge(W,W)) = H_\neg(W) = F = H_\vee(F,F). \end{aligned}$$

Wir werden auch noch eine konstruktive (oder starke) Auffassung des "oder" besprechen, bei der $\vee$ nicht mehr so definiert werden kann.

Mit $A$ und $B$ ist auch die Implikation $A \to B$ (gelesen "wenn $A$, so $B$" oder "$A$ impliziert $B$") eine Formel. Man beachte, daß wenn–so hier im mathematischen Sinn gemeint ist, d.h. es braucht kein kausaler Zusammenhang zwischen $A$ und $B$ zu bestehen. So ist zum Beispiel $2 < 3 \to P(7)$ wahr. Die Wahrheitsfunktion $H_\to : \{W, F\}^2 \to \{W, F\}$ ist

$$H_\to(W, W) = H_\to(F, W) = H_\to(F, F) = W,$$
$$H_\to(W, F) = F.$$

Schließlich ist mit $A$ und $B$ auch die Äquivalenz $A \leftrightarrow B$ (gelesen "$A$ genau dann, wenn $B$" oder "$A$ äquivalent $B$") eine Formel. Die Wahrheitsfunktion $H_\leftrightarrow : \{W, F\}^2 \to \{W, F\}$ ist

$$H_\leftrightarrow(W, W) = H_\leftrightarrow(F, F) = W,$$
$$H_\leftrightarrow(W, F) = H_\leftrightarrow(F, W) = F.$$

Die Äquivalenz ist offenbar aus $\wedge$ und $\to$ definierbar durch $(A \to B) \wedge (B \to A)$.

Ferner ist es nützlich, noch das Falsum $\bot$ als logische Konstante einzuführen. Es ist bestimmt durch die "nullstellige" Wahrheitsfunktion $H_\bot := F$. Man kann dann etwa die Negation $\neg$ aus der Implikation $\to$ und dem Falsum $\bot$ definieren durch $\neg A :\equiv A \to \bot$, denn es gilt

$$H_\to(W, H_\bot) = H_\to(W, F) = F = H_\neg(W),$$
$$H_\to(F, H_\bot) = H_\to(F, F) = W = H_\neg(F).$$

Um auch allgemeine Aussagen machen zu können — etwa $\forall x(e \circ x = x)$ —, benötigen wir noch Variablen $x, y, z, \ldots$. Dabei stellen wir uns vor, daß die Variablen über die Elemente unseres Individuenbereichs laufen. Der Termbegriff ist dann so zu erweitern, daß auch Variablen darin zugelassen sind.

Mit $A$ ist auch die Allformel $\forall x\, A$ (gelesen "für alle $x$ gilt $A$") eine Formel. Hierbei wird im allgemeinen $A$ eine Formel sein, in der die Variable $x$ vorkommt.

Schließlich ist mit $A$ auch die Existenzformel $\exists x\, A$ (gelesen "es gibt ein $x$ mit $A$") eine Formel. Man beachte, daß bei der üblichen klassischen (oder schwachen) Auffassung des "es gibt" $\exists x\, A$ dasselbe bedeutet wie $\neg\forall x\neg A$, also $\exists$ auch durch $\forall$ und $\neg$ definiert werden kann. Wir werden auch noch eine konstruktive (oder starke) Auffassung des Existenzquantors besprechen, bei der dies nicht mehr der Fall ist.

Man beachte ferner, daß die Verwendung der Quantoren $\forall x$ und $\exists x$ die Unterscheidung zwischen freien und gebundenen Vorkommen von Variablen notwendig macht. So ist etwa in $\forall x(x \leq x + y)$ das zweite und dritte Vorkommen der Variablen $x$ gebunden, aber das einzige Vorkommen der Variablen $y$ frei. Die letzte Formel kann man unter Erhalt ihrer

Bedeutung auch umschreiben in $\forall z(z \leq z + y)$, denn dies ist nur eine Umbenennung der gebundenen Variablen. Ein ähnliches Phänomen ist aus der Analysis bekannt, wo ebenfalls

$$\int_0^1 \sin(xy)\,dx = \int_0^1 \sin(ty)\,dt$$

ist; $x$ bzw. $t$ kommen hier gebunden vor.

Als ein Beispiel einer Formalisierung mathematischer Aussagen betrachten wir die Axiome der Gruppentheorie. Grundbegriffe sind die Gruppenverknüpfung $\circ$ (ein zweistelliges Funktionssymbol), die Einheit $e$ (eine Konstante), die Inversenbildung $^{-1}$ (ein einstelliges Funktionssymbol) und schließlich die Gleichheit $=$ (ein zweistelliges Relationssymbol). Als Axiome haben wir

$$\begin{aligned}
&\forall x \forall y \forall z[x \circ (y \circ z) = (x \circ y) \circ z] \qquad \text{(Assoziativität)},\\
&\forall x[e \circ x = x] \qquad \text{(Linkseinheit)},\\
&\forall x[x^{-1} \circ x = e] \qquad \text{(Linksinverses)}.
\end{aligned}$$

Wir geben noch zwei weitere Beispiele zur Formalisierung mathematischer Aussagen.

Zwei Mengen sind gleich, wenn sie dieselben Elemente haben ($\forall$, für alle Mengen; $\in$, ist ein Element von; $=$, ist gleich).

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

$f$ ist stetig im Punkt $a$ ($f$, einstelliges Funktionssymbol; $a, 0$, reelle Zahlen; $\forall$, für alle reellen Zahlen; $>$, ist größer als; $<$, ist kleiner als; $d(x, y)$, der Abstand von $x$ und $y$).

$$\forall \varepsilon(\varepsilon > 0 \rightarrow \exists \delta[\delta > 0 \wedge \forall x(d(x, a) < \delta \rightarrow d(f(x), f(a)) < \varepsilon)]).$$

## 1.2 Induktion und Rekursion

In der Logik und auch allgemein in der Mathematik hat man oft Anlaß, induktiv definierte Mengen zu betrachten. Dabei handelt es sich um folgende Situation. Gegeben sei eine Menge $U$, das "Universum". Wir wollen dann eine Teilmenge $C \subseteq U$ so definieren, daß alle Elemente einer gegebenen Menge $B$ (die "Basiselemente") in $C$ sind, und ferner $C$ abgeschlossen ist gegen gewisse Erzeugungsfunktionen $f_j$, $j \in J$, jede mit einer Stellenzahl $n_j \geq 1$. $C$ soll schließlich die kleinste Menge mit dieser Eigenschaft darstellen; dadurch ist $C$ eindeutig bestimmt.

*Beispiele.* a. Die Menge $\mathbb{N}$ der natürlichen Zahlen ist die kleinste Teilmenge der Menge $\mathbb{Q}$ der rationalen Zahlen, die 0 enthält und in der mit $x$ stets auch $x+1$ liegt.

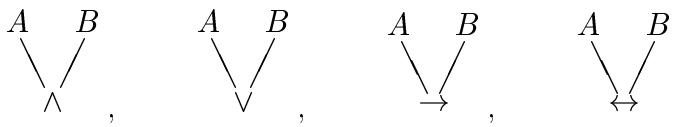
b. Die Menge $\mathbb{Z}$ der ganzen Zahlen ist die kleinste Teilmenge der Menge $\mathbb{Q}$ der rationalen Zahlen, die 0 enthält und in der mit $x$ stets auch $x+1$ und $x-1$ liegen.

c. Sei $X$ eine Menge, deren Elemente wir Aussagensymbole nennen und mit $P, Q, R$ bezeichnen. $U$ sei die Menge aller endlichen beschrifteten Bäume mit beliebigen endlichen Verzweigungen und Beschriftungen aus $X \cup \{\bot, \neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$. Die Menge der aussagenlogischen Formeln über $X$ ist die kleinste Teilmenge von $U$, die

- alle einelementigen Bäume $P$ mit $P \in X$ sowie $\bot$ enthält,
- mit $A$ stets auch

  enthält, und

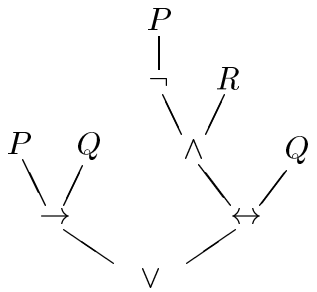
- mit $A$ und $B$ stets auch




  enthält.

Wir schreiben meist $\neg A$, $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ und $(A \leftrightarrow B)$ für die angegebenen beschrifteten Bäume. Offenbar hat jede aussagenlogische Formel einen eindeutig bestimmten Erzeugungsbaum. Beispiel: Die Formel $((P \rightarrow Q) \vee ((\neg P \wedge R) \leftrightarrow Q))$ hat folgenden

Erzeugungsbaum.




Die Anzahl der Basiselemente und auch die Anzahl der Erzeugungsfunktionen kann beliebig, insbesondere auch unendlich sein. Zur Vereinfachung der folgenden Diskussion nehmen wir an, daß wir zwei Basiselemente $a, b$, eine zweistellige Erzeugungsfunktion $f$ und eine einstellige Erzeugungsfunktion $g$ haben.

Es gibt zwei Möglichkeiten zur Darstellung von $C$: man kann $C$ sozusagen "von unten" und "von oben" kommend definieren.

Bei der Definition von $C$ "von unten" definieren wir uns Mengen $C_n$ wie folgt. $C_n$ besteht aus allen Objekten $x$ derart daß es eine endliche Konstruktionsfolge $\langle x_0, \ldots, x_n \rangle$ gibt mit $x_n = x$ und der Eigenschaft daß es für alle $i \leq n$ eine der folgenden Bedingungen erfüllt ist.

- $x_i = a$ oder $x_i = b$,
- $x_i = f(x_j, x_k)$ mit $j, k < i$,
- $x_i = g(x_j)$ mit $j < i$.

Dann setzen wir

$$C_* := \bigcup_n C_n.$$

Zum Beispiel erhält man die Konstruktionsfolge für die Formel $((P \to Q) \vee ((\neg P \wedge R) \leftrightarrow Q))$ durch Linearisierung des oben angegebenen Baums.

Zur Definition von $C$ "von oben" betrachten wir das System $\mathcal{S}$ aller induktiven Teilmengen $D \subseteq U$, die $a, b$ enthalten und gegen $f$ und $g$ abgeschlossen sind, d.h. die mit $x$ und $y$ stets auch $f(x, y)$ und $g(x)$ enthalten. $\mathcal{S}$ ist nicht leer, da zum Beispiel $U$ eine solche Teilmenge ist. Dann setzen wir

$$C^* := \bigcap_{D \in \mathcal{S}} D.$$

**Lemma 2.1.** $C_* = C^*$.

*Beweis.* $\subseteq$. Sei $D \in \mathcal{S}$. Es genügt zu zeigen, daß $C_n \subseteq D$ für alle $n$. Dies folgt sofort durch Induktion über $n$.

$\supseteq$. Es genügt zu zeigen, daß $C_* \in \mathcal{S}$. Dies folgt aber sofort aus den Definitionen. □

Wenn wir zeigen wollen, daß alle Elemente $x$ von $C$ eine Eigenschaft $E$ haben, können wir das folgende, sehr nützliche Induktionsprinzip verwenden.

**Lemma 2.2 (Induktionsprinzip für induktiv definierte Mengen).** *Die Menge $C$ sei induktiv definiert durch zwei Basiselemente $a, b$, eine zweistellige Erzeugungsfunktion $f$ und eine einstellige Erzeugungsfunktion $g$. Wir nehmen folgendes an.*

- *$a, b$ haben die Eigenschaft $E$.*
- *Wenn $x, y$ die Eigenschaft $E$ haben, so auch $f(x, y)$.*
- *Wenn $x$ die Eigenschaft $E$ hat, so auch $g(x)$.*

*Dann haben alle Elemente von $C$ die Eigenschaft $E$.*

*Beweis.* Sei $D$ die Menge aller Elemente von $U$ mit der Eigenschaft $E$. Aufgrund der Annahme ist $D \in \mathcal{S}$, also $C^* \subseteq D$. Das heißt aber, daß alle Elemente von $C = C^*$ die Eigenschaft $E$ haben. □

Man beachte, daß hier nicht verlangt ist, daß jedes Element aus $C$ einen eindeutig bestimmten Erzeugungsbaum besitzt. Ist dies der Fall, so nennt man $C$ *frei erzeugt*. Genauer: $C \subseteq U$ heißt aus $B \subseteq U$ mittels $f: U \times U \to U$ und $g: U \to U$ frei erzeugt, wenn

- $f, g$ injektiv sind und
- $B$ und die Wertebereiche von $f$ und $g$ paarweise disjunkt sind.

In dem Fall, daß $C \subseteq U$ frei erzeugt ist, können wir Funktionen auf $C$ durch *Rekursion* über die Erzeugung von $C$ definieren.

**Rekursionssatz 2.3.** *Die Menge $C \subseteq U$ sei aus $B \subseteq U$ mittels $f: U \times U \to U$ und $g: U \to U$ frei erzeugt. Sei ferner $V$ eine Menge und Funktionen*

$$\begin{aligned} h&: B \to V, \\ F&: V \times V \to V, \\ G&: V \to V \end{aligned}$$

*gegeben. Dann gibt es eine eindeutig bestimmte Funktion*

$$\bar{h}: C \to V$$

*mit folgenden Eigenschaften.*

- *$\bar{h}(x) = h(x)$ für alle $x \in B$.*

- $\bar{h}(f(x,y)) = F(\bar{h}(x), \bar{h}(y))$ *für alle* $x, y \in C$.
- $\bar{h}(g(x)) = G(\bar{h}(x))$ *für alle* $x \in C$.

*Beweis.* Da $C$ frei erzeugt ist, besitzt jedes Element von $C$ einen eindeutig bestimmten Erzeugungsbaum. Längs dieses Erzeugungsbaums konstruiert man mittels $h, F$ und $G$ den Funktionswert $\bar{h}(x)$. Es ist klar, daß $\bar{h}(x)$ eindeutig bestimmt ist. □

Algebraisch formuliert sagt der Rekursionssatz aus, daß sich jede Abbildung $h\colon B \to V$ zu einem eindeutig bestimmten Homomorphismus der Algebra $C$ (mit den Operationen $f$ und $g$) in die Algebra $V$ (mit den Operationen $F$ und $G$) fortsetzen läßt.

*Beispiel.* Auf der Menge der aussagenlogischen Formeln definieren wir eine Funktion $d$ in die natürlichen Zahlen durch

$$\begin{aligned}
&d(P) = 0 \qquad \text{für alle } P \in X \text{ (d.h. } P \text{ Aussagensymbol)},\\
&d(\bot) = 0,\\
&d(\neg A) = d(A) + 1,\\
&d(A \circ B) = \max\{d(A), d(B)\} + 1 \qquad \text{für } \circ \in \{\wedge, \vee, \to, \leftrightarrow\}.
\end{aligned}$$

$d$ ist also die *Tiefe* der aussagenlogischen Formel $A$.

Man beachte, daß der Rekursionssatz falsch wird, wenn wir auf die Voraussetzung der freien Erzeugtheit von $C$ verzichten. Versucht man z.B., auf der aus 0 durch $+1$ und $-1$ definierten Menge $\mathbb{Z} \subseteq \mathbb{Q}$ eine Funktion $\bar{h}$ zu definieren durch

$$\begin{aligned}
&\bar{h}(0) = 0,\\
&\bar{h}(x+1) = \bar{h}(x) + 2,\\
&\bar{h}(x-1) = \bar{h}(x) + 3,
\end{aligned}$$

so erhält man leicht einen Widerspruch (indem man etwa die beiden Darstellungen von 1 durch $0+1$ und $0+1+1-1$ verwendet).

Es sei noch vermerkt, daß man oft allgemeinere Formen der Induktion und der Rekursion verwenden möchte. Beispiele sind etwa Induktion über die Tiefe einer Formel, oder eine rekursive Definition, in der man nicht nur auf die früheren Funktionswerte, sondern auch auf die Rekursionsvariable zurückgreifen möchte. Alle diese Varianten lassen sich mit mehr oder weniger Mühe auf die hier angegebenen Schemata zurückführen.

## 1.3 Syntax

Wir können jetzt die formalen Sprachen definieren, mit denen wir in unseren formalen Systemen arbeiten wollen.

### 1.3.1 Terme und Formeln

Gegeben sei eine abzählbar unendliche Menge von *Variablen* $*_0, *_1, \ldots$, die wir mit $x, y, z$ bezeichnen. Eine *Sprache $\mathcal{L}$ erster Stufe* ist bestimmt durch ihre *Signatur*. Darunter versteht man folgendes.

- Für jede natürliche Zahl $n \geq 0$ eine (eventuell leere) Menge $\mathrm{Rel}_{\mathcal{L}}^{(n)}$ von $n$–stelligen *Relationssymbolen* (oder auch *Prädikatensymbolen*). 0–stellige Relationssymbole heißen *Aussagensymbole*.

- Für jede natürliche Zahl $n \geq 0$ eine (eventuell leere) Menge $\mathrm{Fun}_{\mathcal{L}}^{(n)}$ von $n$–stelligen *Funktionssymbolen*. Die 0–stelligen Funktionssymbole heißen *Konstante*.

Wir setzen voraus, daß die Menge der Variablen und alle Mengen $\mathrm{Rel}_{\mathcal{L}}^{(n)}$ und $\mathrm{Fun}_{\mathcal{L}}^{(n)}$ paarweise disjunkt sind.

Zum Beispiel ist die Sprache $\mathcal{L}_G$ der Gruppentheorie bestimmt durch folgende Signatur. Die Gruppenverknüpfung $\circ$ (ein zweistelliges Funktionssymbol), die Einheit $e$ (eine Konstante), die Inversenbildung $^{-1}$ (ein einstelliges Funktionssymbol) und schließlich die Gleichheit $=$ (ein zweistelliges Relationssymbol).

*$\mathcal{L}$–Terme* werden induktiv wie folgt definiert.

- Jede Variable ist ein $\mathcal{L}$–Term.

- Jede Konstante von $\mathcal{L}$ ist ein $\mathcal{L}$–Term.

- Sind $t_1, \ldots, t_n$ $\mathcal{L}$–Terme und ist $f$ ein $n$–stelliges Funktionssymbol von $\mathcal{L}$ mit $n \geq 1$, so ist $f(t_1, \ldots, t_n)$ ein $\mathcal{L}$–Term.

Mit $\mathrm{Ter}_{\mathcal{L}}$ bezeichnen wir die Menge der $\mathcal{L}$–Terme. Wir fassen hier $\mathcal{L}$–Terme wieder als endliche beschriftete Bäume mit endlichen Verzweigungen auf. Die Menge der $\mathcal{L}$–Terme ist also frei erzeugt, und wir können Funktionen auf $\mathcal{L}$–Termen durch Rekursion über die Erzeugung von $\mathcal{L}$–Termen definieren. Zum Beispiel ist für jeden $\mathcal{L}$–Term $t$ die Menge $\mathrm{vars}(t)$ aller Variablen, die in dem Term auftreten, wie folgt definiert.

- Ist $t$ eine Variable, so ist $\mathrm{vars}(t) := \{t\}$.

- Ist $t$ eine Konstante von $\mathcal{L}$, so ist $\mathrm{vars}(t) := \emptyset$.

- Sind $t_1, \ldots, t_n$ $\mathcal{L}$–Terme und ist $f$ ein $n$–stelliges Funktionssymbol von $\mathcal{L}$, so ist $\mathrm{vars}(f(t_1, \ldots, t_n)) := \mathrm{vars}(t_1) \cup \ldots \cup \mathrm{vars}(t_n)$.

Ist $\mathrm{vars}(t) = \emptyset$, so heißt der Term $t$ *geschlossener Term* oder *Grundterm*.

Zweistellige Funktionssymbole werden meist in *Infix*–Schreibweise verwendet. Man schreibt dann $x+y$ statt $+(x, y)$. Klammern werden so gesetzt, daß sich die Struktur eines Terms eindeutig ergibt. Statt $f(t_1, \ldots, t_n)$ schreiben wir oft auch $ft_1 \ldots t_n$. Terme der Sprache der Gruppentheorie, also $\mathcal{L}_G$–Terme, sind dann zum Beispiel

$$e, \quad x \circ e, \quad (x^{-1} \circ y^{-1})^{-1}.$$

Aus $\mathcal{L}$–Termen erhält man jetzt sehr einfach $\mathcal{L}$–*Primformeln* oder *atomare Formeln* von $\mathcal{L}$: Sind $t_1, \ldots, t_n$ $\mathcal{L}$–Terme und ist $R$ ein $n$–stelliges Relationssymbol von $\mathcal{L}$, so ist $R(t_1, \ldots, t_n)$ eine $\mathcal{L}$–Primformel; ferner ist $\bot$ (gelesen "das Falsche") eine $\mathcal{L}$–Primformel.

Auch zweistellige Relationssymbole werden meist in *Infix*–Schreibweise verwendet. Man schreibt dann $x < y$ statt $< (x, y)$. Klammern werden so gesetzt, daß sich die Struktur einer atomaren Formel eindeutig ergibt. Statt $R(t_1, \ldots, t_n)$ schreiben wir oft $Rt_1 \ldots t_n$.

$\mathcal{L}$–*Formeln* werden aus $\mathcal{L}$–Primformeln wieder induktiv definiert durch

- Jede $\mathcal{L}$–Primformel ist eine $\mathcal{L}$–Formel. Insbesondere ist also $\bot$ eine $\mathcal{L}$–Formel.
- Sind $A$ und $B$ $\mathcal{L}$–Formeln, so auch $A \wedge B$ und $A \to B$.
- Ist $A$ eine $\mathcal{L}$–Formel und $x$ eine Variable, so ist $\forall x\, A$ eine $\mathcal{L}$–Formel.

$\mathcal{L}$–Formeln fassen wir wieder als endliche beschriftete Bäume mit endlichen Verzweigungen auf. Man beachte, daß wir hier unendlich viele Erzeugungsfunktionen verwenden: Für jede Variable $x$ brauchen wir eine Erzeugungsfunktion, die den Übergang von $A$ zu $\forall x\, A$ erlaubt. Die Menge der $\mathcal{L}$–Formeln ist also frei erzeugt, und wir können wieder Funktionen auf $\mathcal{L}$–Formeln durch Rekursion über die Erzeugung von $\mathcal{L}$–Formeln definieren. Zum Beispiel ist für jede $\mathcal{L}$–Formel $A$ die Menge $\mathrm{FV}(A)$ aller in $A$ *freien Variablen* wie folgt definiert.

$$\begin{aligned}
&\mathrm{FV}(R(t_1, \ldots, t_n)) := \mathrm{vars}(t_1) \cup \ldots \cup \mathrm{vars}(t_n),\\
&\mathrm{FV}(\bot) := \emptyset,\\
&\mathrm{FV}(A \wedge B) := \mathrm{FV}(A) \cup \mathrm{FV}(B),\\
&\mathrm{FV}(A \to B) := \mathrm{FV}(A) \cup \mathrm{FV}(B),\\
&\mathrm{FV}(\forall x\, A) := \mathrm{FV}(A) \setminus \{x\}.
\end{aligned}$$

Falls $\mathrm{FV}(A) = \emptyset$, so heißt $A$ *geschlossene Formel* oder *Satz*. Wir schreiben $A[\vec{x}]$, um mitzuteilen, daß alle freien Variablen von $A$ in der Liste $\vec{x}$ enthalten sind.

Wir beschränken uns hier der Einfachheit halber auf die logischen Symbole $\bot$, $\wedge$, $\to$ und $\forall$, da Negation, Disjunktion, Äquivalenz und der Existenzquantor daraus definierbar sind, und zwar wie folgt.

$$\begin{aligned}
&\neg A := A \to \bot,\\
&A \vee B := \neg(\neg A \wedge \neg B),\\
&A \leftrightarrow B := (A \to B) \wedge (B \to A),\\
&\exists x\, A := \neg\forall x\, \neg A.
\end{aligned}$$

Wir schreiben $t \neq s$ für $\neg(t = s)$ und $t \not< s$ für $\neg(t < s)$. Klammern werden so gesetzt, daß sich die Struktur einer Formel eindeutig ergibt. Um Klammern zu sparen, vereinbaren wir folgendes.

1. Der Wirkungsbereich von $\neg$ und $\forall x$ ist so klein wie möglich. Beispiele:

$$\begin{aligned}
\neg A \wedge B \quad &\text{meint} \quad (\neg A) \wedge B, \qquad \text{nicht} \quad \neg(A \wedge B).\\
\forall x\, A \to B \quad &\text{meint} \quad (\forall x\, A) \to B, \quad \text{nicht} \quad \forall x(A \to B).
\end{aligned}$$

2. Der Wirkungsbereich von $\wedge$ und $\vee$ ist so klein wie möglich, unter Berücksichtigung von 1. Beispiel:
$$\neg A \wedge B \to C \quad \text{meint} \quad ((\neg A) \wedge B) \to C.$$

3. Bei wiederholter Anwendung einer Verknüpfung ist stets Rechtsklammerung gemeint. Beispiel:
$$A \to B \to C \quad \text{meint} \quad A \to (B \to C).$$

4. Schreibt man hinter $\forall x$ einen Punkt, so ist der Wirkungsbereich von $\forall x$ ist so groß wie möglich. Beispiel:

$$\forall x.A \to B \quad \text{meint} \quad \forall x(A \to B), \quad \text{nicht} \quad (\forall x\, A) \to B.$$

Als Mitteilungszeichen verwenden wir (auch mit Indizes)

$$\begin{aligned}
&r, s, t \quad \text{für Terme,}\\
&x, y, z \quad \text{für Variablen,}\\
&c \quad \text{für Konstanten,}\\
&P, Q, R \quad \text{für Relationssymbole,}\\
&f, g, h \quad \text{für Funktionssymbole,}\\
&A, B, C, D \quad \text{für Formeln.}
\end{aligned}$$

Im folgenden sei die Sprache $\mathcal{L}$ fest gewählt. Wir lassen deshalb den Bezug auf $\mathcal{L}$ weg und sprechen zum Beispiel kurz von Termen und Formeln statt von $\mathcal{L}$–Termen und $\mathcal{L}$–Formeln.

### 1.3.2 Substitutionen

Eine *Substitution* $\vartheta$ ist eine endliche Menge der Form

$$\vartheta = \{t_1/x_1, \ldots, t_n/x_n\},$$

so daß $t_i \neq x_i$ für $i = 1, \ldots, n$ und $x_1, \ldots, x_n$ paarweise verschieden sind. Ein Element $t_i/x_i$ von $\vartheta$ wird als *Bindung* (von $x_i$ an $t_i$) bezeichnet.

Ist $r$ ein Term und $\vartheta$ die Substitution $\{t_1/x_1, \ldots, t_n/x_n\}$, so verstehen wir unter $r\vartheta$ den Term, den wir erhalten, indem wir in $r$ simultan jedes Vorkommen von $x_i$ durch $t_i$ ersetzen ($i = 1, \ldots, n$). Wir sagen dann, daß $\vartheta$ auf $r$ angewandt wurde und nennen $r\vartheta$ die von $\vartheta$ induzierte *Instanz* von $r$.

Ist $\vartheta$ eine Substitution $\{t_1/x_1, \ldots, t_n/x_n\}$, so bezeichnen wir

$$\mathrm{dom}(\vartheta) := \{x_1, \ldots, x_n\}$$

als den Bereich von $\vartheta$ und

$$\mathrm{ranv}(\vartheta) := \mathrm{vars}(t_1) \cup \ldots \cup \mathrm{vars}(t_n)$$

als die Wertevariablen von $\vartheta$. (Wir schreiben nicht "ran" als Abkürzung, da dies zu Verwechslungen mit dem üblichen Wertebereich einer Funktion führen könnte.) $\vartheta$ heißt *Grundsubstitution*, falls $\{t_1, \ldots, t_n\}$ nur aus geschlossenen Termen besteht; $\vartheta$ heißt *Variablensubstitution*, falls $\{t_1, \ldots, t_n\}$ nur aus Variablen besteht. Ist $\vartheta = \emptyset$, so sprechen wir von der leeren Substitution, die wir mit $\varepsilon$ bezeichnen.

*Beispiel.* Es seien $a$ und $b$ Konstanten sowie $r = f(x, y, g(a))$ und $\vartheta = [b/x, x/y]$. Dann ist $r\vartheta = f(b, x, g(a))$.

Sind $r, t$ Terme und ist $\vartheta = \{t/x\}$ eine Substitution, so bezeichnen wir den Term $r\vartheta$ auch mit $r[t/x]$. Ferner setzen wir $r[x/x] := r$ (um später Fallunterscheidungen zu vermeiden).

Gegeben seien jetzt die Substitutionen

$$\vartheta = \{s_1/x_1, \ldots, s_m/x_m\},$$
$$\sigma = \{t_1/y_1, \ldots, t_n/y_n\}.$$

Dann ist die *Komposition* $\vartheta\sigma$ von $\vartheta$ und $\sigma$ die Substitution, die wir erhalten, indem wir aus der Menge

$$\{s_1\sigma/x_1, \ldots, s_m\sigma/x_m, t_1/y_1, \ldots, t_n/y_n\}$$

alle Bindungen $s_i\sigma/x_i$ streichen, für die $s_i\sigma = x_i$ ist, sowie alle Bindungen $t_j/y_j$, für die $y_j \in \{x_1, \ldots, x_m\}$.

**Lemma 3.1.** *Für Substitutionen $\vartheta, \sigma, \tau$ gilt:*

a. $\vartheta = \sigma \iff r\vartheta = r\sigma$ *für alle Terme* $r$.

b. $\vartheta = \sigma \iff x\vartheta = x\sigma$ *für alle Variablen* $x$.

c. $\vartheta\varepsilon = \varepsilon\vartheta = \vartheta$.

d. $(r\vartheta)\sigma = r(\vartheta\sigma)$ *für alle Terme* $r$.

e. $\vartheta(\sigma\tau) = (\vartheta\sigma)\tau$.

*Beweis.* a–c sind klar; e folgt unmittelbar aus a und d. Wir zeigen nun d. Sei also

$$\vartheta = \{s_1/x_1, \ldots, s_m/x_m\} \qquad \text{und} \qquad \sigma = \{t_1/y_1, \ldots, t_n/y_n\}.$$

Ist $r$ eine Variable $x$, so unterscheiden wir drei Fälle:

*Fall* $x \notin \{x_1, \ldots, x_m\} \cup \{y_1, \ldots, y_n\}$. Dann ist $(x\vartheta)\sigma = x\sigma = x = x(\vartheta\sigma)$.

*Fall* $x \in \{x_1, \ldots, x_m\}$, $x = x_i$. Dann ist $(x\vartheta)\sigma = s_i\sigma = x(\vartheta\sigma)$.

*Fall* $x \in \{y_1, \ldots, y_n\} \setminus \{x_1, \ldots, x_m\}$, $x = y_j$. Dann ist $(x\vartheta)\sigma = x\sigma = t_j = x(\vartheta\sigma)$.

Daraus folgt nun die Behauptung für beliebige Terme $r$ durch eine triviale Induktion nach dem Termaufbau. □

*Bemerkung.* Aufgrund von d und e schreibt man statt $(r\vartheta)\sigma$ oder $r(\vartheta\sigma)$ kurz $r\vartheta\sigma$; ebenso schreibt man statt $\vartheta(\sigma\tau)$ oder $(\vartheta\sigma)\tau$ kurz $\vartheta\sigma\tau$.

Ist $A$ eine Formel und $\vartheta = \{t_1/x_1, \ldots, t_n/x_n\}$ eine Substitution, so kann es bei der simultanen Ersetzung jedes freien Vorkommens von $x_i$ durch $t_i$ in $A$ vorkommen, daß eine Variable aus $t_i$ in den Bindungsbereich eines Quantors in $A$ gerät.

Man kann leicht Beispiele einer Formel $A$ und einer Substitution der Form $\vartheta = \{t_1/x_1, \ldots, t_n/x_n\}$ finden, so daß bei der simultanen Ersetzung jedes freien Vorkommens von $x_i$ durch $t_i$ in $A$ eine Variable aus $t_i$ in den Bindungsbereich eines Quantors in $A$ gerät. Um diese unerwünschte Erscheinung zu vermeiden, müssen wir gegebenenfalls einige gebundene Variablen in $A$ umbenennen. Wir definieren deshalb zunächst die Menge $\mathrm{BV}(A)$ der in $A$ *gebundenen Variablen*.

$$\begin{aligned}
&\mathrm{BV}(R(t_1, \ldots, t_n)) := \emptyset.\\
&\mathrm{BV}(\bot) := \emptyset.\\
&\mathrm{BV}(A \wedge B) := \mathrm{BV}(A) \cup \mathrm{BV}(B).\\
&\mathrm{BV}(A \to B) := \mathrm{BV}(A) \cup \mathrm{BV}(B).\\
&\mathrm{BV}(\forall x\, A) := \mathrm{BV}(A) \cup \{x\}.
\end{aligned}$$

Wir definieren jetzt $A\vartheta$ wie folgt durch Induktion über $A$.

$$R(t_1, \ldots, t_n)\vartheta := R(t_1\vartheta, \ldots, t_n\vartheta).$$

$$\bot\vartheta := \bot.$$
$$(A \wedge B)\vartheta := A\vartheta \wedge B\vartheta.$$
$$(A \to B)\vartheta := A\vartheta \to B\vartheta.$$

Im Fall $\forall x\, A$ bildet man zunächst $\sigma := \vartheta{\restriction}\mathrm{FV}(\forall x\, A)$ und setzt dann

$$(\forall x\, A)\vartheta := \begin{cases} \forall x\, A\sigma, & \text{falls } x \notin \mathrm{ranv}(\sigma) \\ \forall y\, A(\{y/x\}\sigma), & \text{falls } x \in \mathrm{ranv}(\sigma), \end{cases}$$

wobei $y$ eine "neue" Variable ist, etwa die erste Variable echt oberhalb aller Variablen in $\mathrm{ranv}(\sigma) \cup \mathrm{FV}(A) \cup \mathrm{BV}(A)$. Man beachte, daß unter den angegebenen Voraussetzungen $\{y/x\}\sigma = \{y/x\} \cup \sigma$ ist. Diese Definition zeichnet sich dadurch aus, daß nur die unbedingt notwendigen Umbenennungen vorgenommen werden.

Wir beweisen jetzt einige einfache Eigenschaften von Substitutionen.

**Lemma 3.2.** *a. Gilt $x\vartheta = x\sigma$ für alle $x \in \mathrm{vars}(t)$, so ist $t\vartheta = t\sigma$.*

*b. Gilt $x\vartheta = x\sigma$ für alle $x \in \mathrm{FV}(A)$, so ist $A\vartheta = A\sigma$.*

*Beweis.* a ist klar. b beweisen wir durch Induktion über $A$. Wir behandeln nur den Fall $\forall x\, A$. Sei $\vartheta' := \vartheta{\restriction}\mathrm{FV}(\forall x\, A)$, $\sigma' := \sigma{\restriction}\mathrm{FV}(\forall x\, A)$. Nach Voraussetzung ist $\vartheta' = \sigma'$. Da $(\forall x\, A)\tau$ nur von $x$, $A$ und $\tau{\restriction}\mathrm{FV}(\forall x\, A)$ abhängt, folgt $(\forall x\, A)\vartheta = (\forall x\, A)\sigma$. □

**Lemma 3.3.** *a.* $\mathrm{vars}(t\vartheta) \subseteq [\mathrm{vars}(t) \setminus \mathrm{dom}(\vartheta)] \cup \mathrm{ranv}(\vartheta)$*; ist* $\mathrm{dom}(\vartheta) \subseteq \mathrm{vars}(t)$*, so gilt* $=$*.*

*b.* $\mathrm{FV}(A\vartheta) \subseteq [\mathrm{FV}(A) \setminus \mathrm{dom}(\vartheta)] \cup \mathrm{ranv}(\vartheta)$*; ist* $\mathrm{dom}(\vartheta) \subseteq \mathrm{FV}(A)$*, so gilt* $=$*.*

*Beweis.* a ist klar. b beweisen wir durch Induktion über $A$. Wir behandeln nur den Fall $\forall x\, A$. Sei $\sigma := \vartheta{\restriction}\mathrm{FV}(\forall x\, A)$.

*Unterfall* $x \notin \mathrm{ranv}(\sigma)$. Dann hatten wir definiert $(\forall x\, A)\vartheta = \forall x\, A\sigma$. Man erhält

$$\begin{aligned} \mathrm{FV}(\forall x\, A)\vartheta &= \mathrm{FV}(\forall x\, A\sigma) \\ &= \mathrm{FV}(A\sigma) \setminus \{x\} \\ &= ([\mathrm{FV}(A) \setminus \mathrm{dom}(\sigma)] \cup \mathrm{ranv}(\sigma)) \setminus \{x\} && \text{nach IH} \\ &= [(\mathrm{FV}(A) \setminus \{x\}) \setminus \mathrm{dom}(\sigma)] \cup \mathrm{ranv}(\sigma) && \text{wegen } x \notin \mathrm{ranv}(\sigma) \\ &\subseteq [\mathrm{FV}(\forall x\, A) \setminus \mathrm{dom}(\vartheta)] \cup \mathrm{ranv}(\vartheta) \end{aligned}$$

Im Fall $\mathrm{dom}(\vartheta) \subseteq \mathrm{FV}(\forall x\, A)$ ist $\vartheta = \sigma$ und nach IH das $\subseteq$ ein $=$.

*Unterfall* $x \in \mathrm{ranv}(\sigma)$. Dann hatten wir definiert $(\forall x\, A)\vartheta = \forall x\, A(\{y/x\}\sigma)$ mit $y \notin \mathrm{ranv}(\sigma) \cup \mathrm{FV}(A) \cup \mathrm{BV}(A)$. Man erhält

$$\begin{aligned} \mathrm{FV}(\forall x\, A)\vartheta &= \mathrm{FV}(\forall y\, A(\{y/x\}\sigma)) \\ &= \mathrm{FV}(A(\{y/x\}\sigma)) \setminus \{y\} \\ &\subseteq ([\mathrm{FV}(A) \setminus (\{x\} \cup \mathrm{dom}(\sigma))] \cup \{y\} \cup \mathrm{ranv}(\sigma)) \setminus \{y\} && \text{nach IH} \\ &= [(\mathrm{FV}(A) \setminus \{x\}) \setminus \mathrm{dom}(\sigma)] \cup \mathrm{ranv}(\sigma) && \text{wegen } y \notin \mathrm{ranv}(\sigma) \cup \mathrm{FV}(A) \\ &\subseteq [\mathrm{FV}(\forall x\, A) \setminus \mathrm{dom}(\vartheta)] \cup \mathrm{ranv}(\vartheta) \end{aligned}$$

Im Fall $\mathrm{dom}(\vartheta) \subseteq \mathrm{FV}(\forall x\, A)$ ist wieder $\vartheta = \sigma$ und deshalb das zweite $\subseteq$ ein $=$. Auch das erste $\subseteq$ ist ein $=$, denn im Fall $x \in \mathrm{FV}(A)$ liefert die IH das $=$, und im Fall $x \notin \mathrm{FV}(A)$ hat man

$$\begin{aligned}
\mathrm{FV}(A(\{y/x\}\sigma)) \setminus \{y\} &= \mathrm{FV}(A\sigma) \setminus \{y\} && \text{nach Lemma 3.2b} \\
&= ([\mathrm{FV}(A) \setminus \mathrm{dom}(\sigma)] \cup \mathrm{ranv}(\sigma)) \setminus \{y\} && \text{nach IH} \\
&= [\mathrm{FV}(A) \setminus \mathrm{dom}(\sigma)] \cup \mathrm{ranv}(\sigma) && \text{da } y \notin \mathrm{ranv}(\sigma) \cup \mathrm{FV}(A) \\
&= [\mathrm{FV}(\forall x\, A) \setminus \mathrm{dom}(\sigma)] \cup \mathrm{ranv}(\sigma). && \square
\end{aligned}$$

## 1.4 Semantik

Wir wollen jetzt den Begriff der Bedeutung eines Terms und einer Formel präzisieren. Dazu definieren wir zunächst den Begriff einer $\mathcal{L}$–Struktur und erklären dann, was der Wert eines Terms und die Bedeutung einer Formel in einer solchen $\mathcal{L}$– Struktur sein soll.

$\mathcal{M} = (D, I)$ heißt $\mathcal{L}$–*Prästruktur*, wenn $D$ eine nichtleere Menge ist (die *Trägermenge* oder der *Individuenbereich* von $\mathcal{M}$) und $I$ eine Abbildung (*Interpretation*), die jedem $n$–stelligen Funktionssymbol $f$ von $\mathcal{L}$ eine Funktion

$$I(f)\colon D^n \to D$$

zuordnet. Ist $n = 0$, so ist $I(f)$ ein Element von $D$. $\mathcal{M} = (D, I_0, I_1)$ heißt $\mathcal{L}$–*Struktur*, wenn $(D, I_0)$ eine $\mathcal{L}$–Prästruktur ist und $I_1$ eine Abbildung, die jedem $n$–stelligen Relationssymbol $R$ von $\mathcal{L}$ eine $n$–stellige Relation

$$I_1(R) \subseteq D^n$$

zuordnet. Ist $n = 0$, so ist $I_1(R) \in \{W, F\}$.

Ist $\mathcal{M} = (D, I)$ bzw. $(D, I_0, I_1)$, so schreiben wir oft $|\mathcal{M}|$ für die Trägermenge $D$ von $\mathcal{M}$ sowie $f^{\mathcal{M}}$ und $R^{\mathcal{M}}$ für die Interpretationen $I_0(f)$ und $I_1(R)$ der Funktions– und Relationssymbole.

Eine (Variablen–) *Belegung* oder *Umgebung* in der nichtleeren Menge $D$ ist eine Abbildung von Variablen in $D$. $U$ ordnet also jeder Variablen $x \in \mathrm{dom}(U)$ einen Wert $U(x) \in D$ zu. Wir können deshalb endliche Umgebungen darstellen durch $[a_1/x_1, \ldots, a_n/x_n]$ mit verschiedenen $x_i$. Eine äquivalente Schreibweise ist $[a_1, \ldots, a_n/x_1, \ldots, x_n]$. Sind $U$, $V$ Umgebungen, so sei $U + V$ die Umgebung, die für $x \in \mathrm{dom}(U) \cup \mathrm{dom}(V)$ durch

$$(U + V)(x) := \begin{cases} V(x), & \text{falls } x \in \mathrm{dom}(V); \\ U(x), & \text{sonst} \end{cases}$$

definiert ist. $U + V$ ensteht also durch Überschreiben von $U$ durch $V$. Insbesondere ist

$$(U + [a/x])(y) := \begin{cases} a, & \text{falls } y = x; \\ U(y), & \text{sonst.} \end{cases}$$

Oft schreiben wir $U^a_x$ für $U + [a/x]$.

Seien jetzt eine $\mathcal{L}$–Prästruktur $\mathcal{M}$ und eine Umgebung $U$ in $|\mathcal{M}|$ gegeben. Wir können dann eine homomorphe Fortsetzung $\overline{U}$ von $U$ auf die Menge $\mathrm{Ter}_{\mathcal{L}}$ der $\mathcal{L}$–Terme $t$ mit $\mathrm{vars}(t) \subseteq \mathrm{dom}(U)$ definieren durch

$$\begin{aligned} &\overline{U}(x) := U(x), \\ &\overline{U}(c) := c^{\mathcal{M}}, \\ &\overline{U}(f(t_1, \ldots, t_n)) := f^{\mathcal{M}}(\overline{U}(t_1), \ldots, \overline{U}(t_n)). \end{aligned}$$

Man beachte, daß $\overline{U}$ von $\mathcal{M}$ abhängt, ohne daß dies in der Bezeichnung zum Ausdruck kommt. Wir schreiben deshalb auch $t^{\mathcal{M}}[U]$ für $\overline{U}(t)$.

Für jede $\mathcal{L}$–Struktur $\mathcal{M}$, Umgebung $U$ in $|\mathcal{M}|$ und $\mathcal{L}$–Formel $A$ mit $\mathrm{FV}(A) \subseteq \mathrm{dom}(U)$ definieren wir $\mathcal{M} \models A[U]$ (gelesen: $A$ ist *gültig* in $\mathcal{M}$ unter der Belegung $U$) durch Induktion über $A$.

$$\begin{aligned}
&\mathcal{M} \models (R(t_1, \ldots, t_n))[U] :\Longleftrightarrow \overline{(}U(t_1), \ldots, \overline{U}(t_n)) \in R^{\mathcal{M}}.\\
&\mathcal{M} \not\models \bot[U].\\
&\mathcal{M} \models (A \wedge B)[U] :\Longleftrightarrow \mathcal{M} \models A[U] \text{ und } \mathcal{M} \models B[U].\\
&\mathcal{M} \models (A \to B)[U] :\Longleftrightarrow \text{ wenn } \mathcal{M} \models A[U], \text{ so } \mathcal{M} \models B[U].\\
&\mathcal{M} \models (\forall x\, A)[U] :\Longleftrightarrow \text{ für alle } a \in |\mathcal{M}| \text{ gilt } \mathcal{M} \models A[U^a_x].
\end{aligned}$$

Ist $S$ eine Menge von $\mathcal{L}$–Formeln, so schreiben wir $\mathcal{M} \models S[U]$, wenn für alle $A \in S$ gilt $\mathcal{M} \models A[U]$.

**Koinzidenzlemma 4.1.** *Sei $\mathcal{M}$ eine $\mathcal{L}$–Struktur, $t$ ein $\mathcal{L}$–Term und $A$ eine $\mathcal{L}$–Formel. Ferner seien $U$ und $V$ zwei Umgebungen in $|\mathcal{M}|$.*

a. *Gilt $U(x) = V(x)$ für alle $x \in \mathrm{vars}(t)$, so ist $\overline{U}(t) = \overline{V}(t)$.*

b. *Gilt $U(x) = V(x)$ für alle $x \in \mathrm{FV}(A)$, so ist $\mathcal{M} \models A[U] \iff \mathcal{M} \models A[V]$.*

*Beweis* durch Induktion über Terme bzw. Formeln. □

**Substitutionslemma 4.2.** *Sei $\mathcal{M}$ eine $\mathcal{L}$–Struktur, $t$ ein $\mathcal{L}$–Term und $A$ eine $\mathcal{L}$–Formel. Ferner sei $\vartheta$ eine $\mathcal{L}$–Substitution und $U$ eine Umgebung in $|\mathcal{M}|$. Dann gilt*

a. $\overline{U}(t\vartheta) = \overline{U + (\overline{U} \circ \vartheta)}(t)$.

b. $\mathcal{M} \models A\vartheta[U] \iff \mathcal{M} \models A[U + (\overline{U} \circ \vartheta)]$.

*Beweis.* a. Induktion über $t$. *Fall $x$.* Ist $x \notin \mathrm{dom}(\vartheta)$, so hat man links und rechts $\overline{U}(x)$. Ist $x \in \mathrm{dom}(\vartheta)$, so gilt

$$\overline{U}(x\vartheta) = \overline{U}(\vartheta(x)) = \overline{U + (\overline{U} \circ \vartheta)}(x).$$

Der *Fall $c$* ist klar: links und rechts hat man $c^{\mathcal{M}}$. *Fall $f(t_1, \ldots, t_n)$.* Zur Vereinfachung der Schreibweise nehmen wir $n = 1$ an. Dann ist

$$\begin{aligned}
\overline{U}(f(t)\vartheta) &= f^{\mathcal{M}}(\overline{U}(t\vartheta))\\
&= f^{\mathcal{M}}(\overline{U + (\overline{U} \circ \vartheta)}(t)) \quad \text{nach IH}\\
&= \overline{U + (\overline{U} \circ \vartheta)}(f(t)).
\end{aligned}$$

b. Induktion über $A$. Wir beschränken uns die Fälle einer atomaren Formel und einer Allformel; die restlichen Fälle sind sehr einfach.

*Fall* $R(t_1, \ldots, t_n)$. Zur Vereinfachung nehmen wir $n = 1$ an. Dann gilt

$$\begin{aligned}
\mathcal{M} \models R(t)\vartheta[U] &\iff \mathcal{M} \models R(t\vartheta)[U] \\
&\iff \overline{U}(t\vartheta) \in R^{\mathcal{M}} \\
&\iff \overline{U + (\overline{U} \circ \vartheta)}(t) \in R^{\mathcal{M}} \quad \text{nach a} \\
&\iff \mathcal{M} \models R(t)[U + (\overline{U} \circ \vartheta)].
\end{aligned}$$

*Fall* $\forall x\, A$. Nach Definition der Substitution und dem Koinzidenzlemma können wir oBdA $\mathrm{dom}(\vartheta) \subseteq \mathrm{FV}(\forall x\, A)$ annehmen. *Unterfall* $x \notin \mathrm{ranv}(\vartheta)$. Dann war $(\forall x\, A)\vartheta := \forall x\, A\vartheta$. Man erhält

$$\begin{aligned}
&\mathcal{M} \models (\forall x\, A)\vartheta[U] \\
&\iff \mathcal{M} \models (\forall x\, A\vartheta)[U] \\
&\iff \text{für alle } a \in |\mathcal{M}| \text{ gilt } \mathcal{M} \models A\vartheta[U^a_x] \\
&\iff \text{für alle } a \in |\mathcal{M}| \text{ gilt } \mathcal{M} \models A[U_1] \text{ mit } U_1 := U^a_x + (\overline{U^a_x} \circ \vartheta) \text{ nach IH} \\
&\iff \text{für alle } a \in |\mathcal{M}| \text{ gilt } \mathcal{M} \models A[U_2] \text{ mit } U_2 := \big(U + (\overline{U} \circ \vartheta)\big)^a_x \text{ nach 4.1; siehe unten} \\
&\iff \mathcal{M} \models (\forall x\, A)[U + (\overline{U} \circ \vartheta)].
\end{aligned}$$

Zu zeigen bleibt $U_1(z) = U_2(z)$ für alle $z \in \mathrm{FV}(A)$. Im Fall $z = x$ ist $U_1(z) = a$ wegen $x \notin \mathrm{dom}(\vartheta)$ und ebenfalls $U_2(z) = a$. Im Fall $z \neq x$, $z \in \mathrm{dom}(\vartheta)$ ist

$$U_1(z) = \overline{U^a_x}(\vartheta(z)) = \overline{U}(\vartheta(z))$$

wegen $x \notin \mathrm{ranv}(\vartheta)$ und Lemma 3.3, und ebenfalls $U_2(z) = \overline{U}(\vartheta(z))$. Im Fall $z \neq x$, $z \notin \mathrm{dom}(\vartheta)$ ist $U_1(z) = U^a_x(z) = U(z) = U_2(z)$.

*Unterfall* $x \in \mathrm{ranv}(\vartheta)$. Dann hatten wir $(\forall x\, A)\vartheta := \forall y\, A([y/x]\vartheta)$ definiert mit $y$ minimal neu, d.h. $y \notin \mathrm{ranv}(\vartheta) \cup \mathrm{FV}(A) \cup \mathrm{BV}(A)$. Man erhält

$$\begin{aligned}
&\mathcal{M} \models (\forall x\, A)\vartheta[U] \\
&\iff \mathcal{M} \models (\forall y\, A([y/x]\vartheta))[U] \\
&\iff \text{für alle } b \in |\mathcal{M}| \text{ gilt } \mathcal{M} \models A([y/x]\vartheta)[U^b_y] \\
&\iff \text{für alle } b \in |\mathcal{M}| \text{ gilt } \mathcal{M} \models A[U_1] \text{ mit } U_1 := U^b_y + (\overline{U^b_y} \circ [y/x]\vartheta) \text{ nach IH} \\
&\iff \text{für alle } b \in |\mathcal{M}| \text{ gilt } \mathcal{M} \models A[U_2] \text{ mit } U_2 := \big(U + (\overline{U} \circ \vartheta)\big)^b_x \text{ nach 4.1; siehe unten} \\
&\iff \mathcal{M} \models (\forall x\, A)[U + (\overline{U} \circ \vartheta)].
\end{aligned}$$

Zu zeigen bleibt $U_1(z) = U_2(z)$ für alle $z \in \mathrm{FV}(A)$. Im Fall $z = x$ ist $U_1(z) = b = U_2(z)$. Im Fall $z \neq x$, $z \in \mathrm{dom}(\vartheta)$ ist

$$U_1(z) = \overline{U^b_y}(\vartheta(z)) = \overline{U}(\vartheta(z))$$

wegen $y \notin \mathrm{ranv}(\vartheta)$ und Lemma 3.3, und ebenfalls $U_2(z) = \overline{U}(\vartheta(z))$. Im Fall $z \neq x$, $z \notin \mathrm{dom}(\vartheta)$ ist $U_1(z) = U^b_y(z) = U(z) = U_2(z)$, denn wegen $y \notin \mathrm{FV}(A)$ ist $z \neq y$. □

## 1.5 Natürliches Schließen

Wir wollen jetzt den Begriff einer *logischen Herleitung* einer Formel $A$ definieren. Dazu verwenden wir ein System des "natürlichen Schließens", das von Gerhard Gentzen in [4] eingeführt wurde.

### 1.5.1 Herleitungen, Korrektheit

Wir beginnen mit einigen Beispielen für natürliche Beweise. Gegeben sei also eine Sprache $\mathcal{L}$ erster Stufe. Der Einfachheit halber betrachten wir Beweise in der reinen Logik, d.h. ohne Annahmen über die Funktionen und Prädikate.

$$(A \wedge B \to C) \to (A \to (B \to C)). \tag{1}$$

Gelte $A \wedge B \to C$. Zu zeigen: $A \to (B \to C)$. Gelte also $A$. Zu zeigen: $B \to C$. Gelte also $B$. Zu zeigen: $C$. Wir haben $A \wedge B$, nach den letzten beiden Annahmen. Also auch $C$, nach der ersten Annahme.

$$(A \to (B \to C)) \to (A \wedge B \to C). \tag{2}$$

Gelte $A \to (B \to C)$. Zu zeigen: $A \wedge B \to C$. Gelte also $A \wedge B$. Zu zeigen: $C$. Wir haben $A$, nach der letzten Annahme. Also auch $B \to C$, nach der ersten Annahme. Wir haben $B$, wieder nach der letzten Annahme. Daher auch $C$, nach den letzten beiden Aussagen.

$$\forall x(A \to B) \to (A \to \forall x\, B), \quad \text{falls } x \notin \mathrm{FV}(A). \tag{3}$$

Gelte $\forall x(A \to B)$. Zu zeigen: $A \to \forall x\, B$. Gelte also $A$. Zu zeigen: $\forall x\, B$. Sei $x$ beliebig; man beachte, daß wir bisher keine Annahmen über $x$ gemacht haben. Zu zeigen: $B$. Wir haben $A \to B$, nach der ersten Annahme. Also auch $B$, nach der zweiten Annahme.

$$(A \to \forall x\, B) \to \forall x(A \to B), \quad \text{falls } x \notin \mathrm{FV}(A). \tag{4}$$

Gelte $A \to \forall x\, B$. Zu zeigen: $\forall x(A \to B)$. Sei $x$ beliebig; man beachte, daß wir bisher keine Annahmen über $x$ gemacht haben. Zu zeigen: $A \to B$. Gelte also $A$. Zu zeigen: $B$. Wir haben $\forall x\, B$, nach der ersten und zweiten Annahme. Also auch $B$.

Ein Charakteristikum dieser Beweise ist es, daß Annahmen eingeführt und wieder beseitigt werden: Zu jedem Zeitpunkt im Beweis kennt man die jetzt freien Annahmen.

Wir reservieren das Wort *Beweis* für die Meta–Stufe; eine formale Darstellung eines Beweises nennen wir *Herleitung* oder *Ableitung*.

Eine anschauliche Art, Herleitungen zu definieren, besteht darin, sie als beschriftete Bäume aufzufassen. Die Beschriftungen der inneren Knoten sind Formeln, die der Blätter sind Formeln oder Terme. Die Beschriftungen der Nachfolger eines Knotens $\nu$ sind die *Prämissen* einer Regelanwendung, die Formel am Konten $\nu$ ist ihre *Konklusion*. An der Wurzel des Baums befindet sich die Konklusion der gesamten Herleitung. Im natürlichen Schließen arbeitet man mit *Annahmen*, die an Blättern des Baums stehen; sie können offen oder geschlossen (man sagt auch: *gestrichen*) sein.

Jede dieser Annahmen ist mit einer *Marke* versehen. Als Marken verwenden wir *Annahmenvariablen* $\square_0, \square_1, \ldots$; Mitteilungszeichen für Annahmenvariablen sind $u, v, w$. Die (bisherigen) Variablen nennen wir oft auch *Objektvariablen*, um sie von den Annahmenvariablen zu unterscheiden. Wenn an einer späteren Stellen (d.h. an einem Knoten im Baum unterhalb dieser Annahme) die Abhängigkeit von dieser Annahme beseitigt wird, notieren wir dies durch Angabe der Annahmenvariablen. Da wir dieselbe Annahme auch mehrfach verwenden können (dies war etwa im Beispiel (2) der Fall), darf in einem Baum eine mit $u$ markierte Annahme $A$ (mitgeteilt durch $u\colon A$) auch mehrfach vorkommen. Wir verlangen jedoch, daß verschiedene Annahmeformeln stets verschiedene Marken bekommen.

Einen inneren Knoten im Baum verstanden wir als Resultat eines Übergangs von *Prämissen* zu einer *Konklusion*. Die zulässigen Übergänge werden durch die *Regeln* bestimmt. Die Beschriftung des Knotens enthält dann neben der Konklusion noch den Namen der verwendeten Regel. In manchen Fällen bindet eine Regel eine Annahmenvariable $u$ (und beseitigt damit die Abhängigkeit von allen darüber stehenden, mit $u$ markierten Annahmen $u\colon A$) oder eine Objektvariable $x$ (und beseitigt damit die Abhängigkeit von $x$). Dann wird die abgebundene Annahmen– oder Objektvariable der Beschriftung hinzugefügt.

Die Regeln des natürlichen Schließens gliedern sich in Einführungs– und Beseitigungsregeln. Für die Konjuktion $\wedge$ haben wir eine Einführungsregel $\wedge$I und zwei Beseitigungsregeln $\wedge\mathrm{E_r}$ und $\wedge\mathrm{E_l}$.

$$\frac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ A & B\end{array}}{A \wedge B}\,\wedge\mathrm{I} \qquad \frac{\mathcal{D}}{A \wedge B}\,\wedge\mathrm{E_r} \qquad \frac{\mathcal{D}}{A \wedge B}\,\wedge\mathrm{E_l}$$

Für die Implikation $\rightarrow$ gibt es eine Einführungsregel $\rightarrow$I,$u$ und eine Beseitigungsregel $\rightarrow$E, die man auch *modus ponens* nennt. Die linke Prämisse $A \rightarrow B$ in $\rightarrow$E nennt man *Hauptprämisse*, die rechte Prämisse $A$ *Nebenprämisse*. Man beachte, daß in einer $\rightarrow$I,$u$–Anwendung *alle* darüber stehenden mit $u$ markierten Annahmen $A$ gestrichen werden.

$$\frac{\begin{array}{c}[u\colon A]\\ \mathcal{D}\\ B\end{array}}{A \rightarrow B}\,\rightarrow\mathrm{I},u \qquad \frac{\begin{array}{cc}\mathcal{D}_1 & \mathcal{D}_2\\ A \rightarrow B & A\end{array}}{B}\,\rightarrow\mathrm{E}$$

Für den Allquantor $\forall$ gibt es eine Einführungsregel $\forall$I,$x$ und eine Beseitigungsregel $\forall$E, die als rechte Prämisse den zu substituierenden Term $t$ hat. Die Regel $\forall$I,$x$ unterliegt der

folgenden *Variablenbedingung*: Die Herleitung $\mathcal{D}$ darf keine offenen Annahmen enthalten, in denen $x$ frei vorkommt.

$$\frac{\begin{array}{c}\mathcal{D}\\ A\end{array}}{\forall x\, A}\,\forall \mathrm{I},x \qquad \frac{\begin{array}{cc}\mathcal{D} & \\ \forall x\, A & t\end{array}}{A[t/x]}\,\forall \mathrm{E}$$

*Beispiele.* Wir geben Herleitungen für die oben bewiesenen Formeln (1)–(4) an. Da meist die verwendete Regel durch die an den Knoten stehenden Formeln bestimmt ist, verzichten wir im allgemeinen auf die Angabe der Regel.

$$\dfrac{\dfrac{\dfrac{\dfrac{u\colon A\wedge B\to C \qquad \dfrac{v\colon A \quad w\colon B}{A\wedge B}}{C}}{B\to C}\,w}{A\to(B\to C)}\,v}{(A\wedge B\to C)\to(A\to(B\to C))}\,u \tag{1}$$

$$\dfrac{\dfrac{\dfrac{u\colon A\to(B\to C) \qquad \dfrac{v\colon A\wedge B}{A}}{B\to C} \qquad \dfrac{v\colon A\wedge B}{B}}{C}}{\dfrac{A\wedge B\to C}{(A\to(B\to C))\to(A\wedge B\to C)}\,v}\,u \tag{2}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{u\colon \forall x(A\to B) \quad x}{A\to B} \qquad v\colon A}{B}}{\forall x\, B}\,x}{A\to\forall x\, B}\,v}{\forall x(A\to B)\to(A\to\forall x\, B)}\,u \tag{3}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{u\colon A\to\forall x\, B \quad v\colon A}{\forall x\, B} \qquad x}{B}}{A\to B}\,v}{\forall x(A\to B)}\,x}{(A\to\forall x\, B)\to\forall x(A\to B)}\,u \tag{4}$$

Die angegebenen Regeln definieren die sogenannte *Minimallogik* (genauer: die Minimallogik für die hier zugrunde gelegten Verknüpfungen $\wedge\to\forall$). Wir schreiben deshalb $\vdash_m A$ und nennen $A$ *herleitbar* (in der Minimallogik), wenn es eine Herleitung von $A$ ohne

freie Annahmen gibt. Eine Formel $B$ heißt herleitbar aus den Annahmen $A_1, \ldots, A_n$, wenn es eine Herleitung mit freien Annahmen unter $A_1, \ldots, A_n$ gibt. Sei $S$ eine (endliche oder unendliche) Menge von Formeln. Wir schreiben $S \vdash_m B$, wenn die Formel $B$ aus endlich vielen Annahmen $A_1, \ldots, A_n \in S$ herleitbar ist.

Wir zeigen zunächst, daß unser Herleitungsbegriff *korrekt* ist. Dabei steht $\mathcal{M} \models S[U]$ für $\mathcal{M} \models A[U]$ für alle $A \in S$.

**Korrektheitssatz 5.1.** *Sei $S \vdash_m B$. Ist dann $\mathcal{M}$ eine Struktur und $U$ eine Umgebung in $|\mathcal{M}|$, so gilt*

$$\mathcal{M} \models S[U] \implies \mathcal{M} \models B[U].$$

*Beweis* durch Induktion über Herleitungen. Da die gegebene Herleitung von $B$ nur endlich viele Annahmen frei enthält, können wir oBdA voraussetzen, daß $S = \{A_1, \ldots, A_n\}$.

*Fall* $u\colon B$. Dann ist $B \in S$ und die Behauptung ist klar.

*Fall* $\wedge$I. Gelte $\mathcal{M} \models S[U]$. Zu zeigen ist $\mathcal{M} \models A \wedge B[U]$. Nach IH haben wir $\mathcal{M} \models A[U]$ und $\mathcal{M} \models B[U]$. Die Behauptung folgt aus der Definition von $\models$. Die Fälle $\wedge\mathrm{E}_r$, $\wedge\mathrm{E}_l$ und $\to$E beweist man genauso.

*Fall* $\to$I. Gelte $\mathcal{M} \models S[U]$. Zu zeigen ist $\mathcal{M} \models A \to B[U]$. Gelte also noch $\mathcal{M} \models A[U]$. Zu zeigen ist $\mathcal{M} \models B[U]$. Nach IH (mit $S \cup \{A\}$ statt $S$) gilt dies.

*Fall* $\forall$I,$x$. Gelte $\mathcal{M} \models S[U]$. OBdA mögen alle Formeln $A_1, \ldots, A_n$ in der gegebenen Herleitung von $A$ als freie Annahmen vorkommen. Zu zeigen ist $\mathcal{M} \models \forall x\, A[U]$. Sei also $a \in |\mathcal{M}|$. Zu zeigen ist $\mathcal{M} \models A[U^a_x]$. Da aufgrund der Variablenbedingung für $\forall$I,$x$ die Variable $x$ in keiner der Formeln $A_1, \ldots, A_n$ frei vorkommt, gilt nach dem Koinzidenzlemma 4.1 $\mathcal{M} \models S[U^a_x]$. Die IH (mit $U^a_x$ statt $U$) liefert $\mathcal{M} \models A[U^a_x]$.

*Fall* $\forall$E. Gelte $\mathcal{M} \models S[U]$. Zu zeigen ist $\mathcal{M} \models A[t/x][U]$, d.h. nach dem Substitutionslemma 4.2

$$\mathcal{M} \models A[U^{\overline{U}(t)}_x].$$

Nach IH haben wir $\mathcal{M} \models \forall x\, A[U]$, d.h. für alle $a \in |\mathcal{M}|$ gilt $\mathcal{M} \models A[U^a_x]$. Mit $\overline{U}(t)$ für $a$ folgt die Behauptung. □

Wie sieht es nun mit der Umkehrung aus? Kann man aus der Gültigkeit von $\mathcal{M} \models A[U]$ für alle Strukturen $\mathcal{M}$ und Umgebungen $U$ schließen auf $\vdash_m A$? Die Antwort ist "nein" für unseren gegenwärtigen Herleitungsbegriff, der der Minimallogik entspricht. Ein Gegenbeispiel ist etwa

$$\neg\neg P \to P$$

für ein Aussagensymbol $P$. Offensichtlich gilt $\mathcal{M} \models \neg\neg P \to P$ in jeder $\mathcal{L}$–Struktur $\mathcal{M}$, und andererseits sieht man leicht (unter Verwendung des Korrektheitssatzes 5.1) ein, daß es keine Herleitung der Formel $\neg\neg P \to P$, also $((P \to \bot) \to \bot) \to P$ geben kann. Dies liegt daran, daß das Falsum $\bot$ von keiner Herleitungsregel besonders behandelt wird; es spielt daher (in der Minimallogik) nur die Rolle eines gewöhnlichen Aussagensymbols. Wäre also $((P \to \bot) \to \bot) \to P$ herleitbar, so auch $((P \to Q) \to Q) \to P$. Dies widerspricht aber

dem Korrektheitssatz, denn in der Struktur $\mathcal{M}$ mit $P^{\mathcal{M}} = F$ und $Q^{\mathcal{M}} = W$ haben wir $\mathcal{M} \models (P \to Q) \to Q$ und $\mathcal{M} \not\models P$.

Um dies zu ändern, müssen wir unseren Herleitungsbegriff zu dem der *klassischen Logik* erweitern. Wir können dies am einfachsten dadurch tun, daß wir für jedes Relationssymbol $R$ von $\mathcal{L}$ das *Prinzip des indirekten Beweisens* für $R$ als Annahme zulassen, also die Formel

$$\forall \vec{x}(\neg\neg R\vec{x} \to R\vec{x}); \tag{$\mathrm{Stab}_R$}$$

diese Formel bezeichnet man auch als *Stabilität* von $R$.

Wir nennen die Formel $A$ *klassisch herleitbar* und schreiben $\vdash_c A$, wenn es eine Herleitung von $A$ aus Stabilitätsannahmen $\mathrm{Stab}_R$ gibt. Ebenso nennen wir die Formel $A$ klassisch herleitbar aus $S$ und schreiben $S \vdash_c A$, wenn es eine Herleitung von $A$ aus $S$ und Stabilitätsannahmen $\mathrm{Stab}_R$ gibt.

Wir wollen uns zunächst überlegen, daß man aus solchen Stabilitätsannahmen das Prinzip des indirekten Beweisens für beliebige Formeln herleiten kann.

**Lemma 5.2 (Stabilität).** *Für jede Formel $A$ gilt $\vdash_c \neg\neg A \to A$.*

*Beweis* durch Induktion über $A$. In den konstruierten Herleitungen lassen wir der Kürze halber Anwendungen von $\to$I am Schluß fort.

*Fall $R(\vec{t})$.* Mit $\mathrm{Stab}_R$.

*Fall $\bot$.* Man beachte, daß gilt $\neg\neg\bot \to \bot = ((\bot \to \bot) \to \bot) \to \bot$. Die gesuchte Herleitung ist:

$$\dfrac{v\colon (\bot \to \bot) \to \bot \qquad \dfrac{u\colon \bot}{\bot \to \bot}\, u}{\bot}$$

*Fall $A \wedge B$.* Mit

$$\vdash_m (\neg\neg A \to A) \to (\neg\neg B \to B) \to \neg\neg(A \wedge B) \to A \wedge B.$$

*Fall $A \to B$.* Mit

$$\vdash_m (\neg\neg B \to B) \to \neg\neg(A \to B) \to A \to B.$$

Eine Herleitung ist

$$\dfrac{u\colon \neg\neg B \to B \qquad \dfrac{\dfrac{v\colon \neg\neg(A \to B) \qquad \dfrac{\dfrac{u_1\colon \neg B \qquad \dfrac{u_2\colon A \to B \quad w\colon A}{B}}{\bot}}{\neg(A \to B)}\, u_2}{\bot}}{\neg\neg B}\, u_1}{B}$$

*Fall* $\forall x\, A$. Offenbar genügt es zu zeigen

$$\vdash_m (\neg\neg A \to A) \to \neg\neg\forall x\, A \to A.$$

Eine Herleitung ist

$$\dfrac{u\colon \neg\neg A \to A \qquad \dfrac{\dfrac{v\colon \neg\neg\forall x\, A \qquad \dfrac{\dfrac{\dfrac{u_1\colon \neg A \qquad \dfrac{u_2\colon \forall x\, A \quad x}{A}}{\bot}\, u_2}{\neg\forall x\, A}}{\bot}}{\neg\neg A}\, u_1}{A}$$

□

**Lemma 5.3 (Ex–falso–quodlibet).** *Für jede Formel $A$ gilt $\vdash_c \bot \to A$.*

*Beweis.* Nach dem Stabilitätslemma 5.2 genügt $\vdash_m (\neg\neg A \to A) \to (\bot \to A)$. Dies ergibt sich aus

$$\dfrac{u\colon \neg\neg A \to A \qquad \dfrac{v\colon \bot}{\neg\neg A}\, w}{A}$$

□

*Bemerkung.* Durch geeignete andere Annahmen über das Falsum $\bot$ erhält man aus der Minimallogik die *intuitionistische Logik*. Sie ergibt sich aus *ex–falso–quodlibet*–Annahmen $\forall\vec{x}(\bot \to R\vec{x})$ für jedes Relationssymbol $R$ der Sprache.

**Lemma 5.4 (Fallunterscheidung).** $\vdash_c (A \to B) \wedge (\neg A \to B) \to B$.

*Beweis.*

$$\dfrac{\dfrac{\mathcal{D}_{\mathrm{Stab}}}{\neg\neg B \to B} \qquad \dfrac{\dfrac{w\colon \neg B \qquad \dfrac{\dfrac{u\colon (A \to B) \wedge (\neg A \to B)}{\neg A \to B} \qquad \dfrac{\dfrac{u\colon (A \to B) \wedge (\neg A \to B)}{A \to B} \qquad v\colon A}{B}}{\neg A}\, v}{B}}{\bot}\, w}{\neg\neg B}}{B}$$

wobei $\mathcal{D}_{\mathrm{Stab}}$ nach dem Stabilitätslemma 5.2 bekannt ist. □

**Lemma 5.5 (Allgemeines Umbenennungslemma)**

**a. Ist $z \notin \mathrm{FV}(A) \cup \mathrm{BV}(A)$, so gilt $(A[z/y])[y/x] = A([z/y][y/x])$.**

*b. Ist $y \notin \mathrm{FV}(A)$, so gilt $\vdash_m (A[y/x])[x/y] \leftrightarrow A$.*

*c. Ist $y \notin \mathrm{FV}(A)$, so gilt $\vdash_m \forall x\, A \leftrightarrow \forall y\, A[y/x]$.*

*Beweis.* a. OBdA ist $z \neq y$ und $y \in \mathrm{FV}(A)$. Wir führen den Beweis durch Induktion über $A$ und beschränken uns auf den Fall $\forall u\, A$. Dann ist $z \neq u$ und $y \neq u$, und wir haben $(\forall u\, A[z/y])[y/x] = ((\forall u\, A)[z/y])[y/x] =: LS$; ferner sei $(\forall u\, A)([z/y][y/x]) =: RS$.

*Fall $x \neq z$. Unterfall $x \in \mathrm{FV}(\forall u\, A)$.* Wir können oBdA $x \neq y$ annehmen, denn andernfalls ist $LS = \forall u\, A[z/y] = RS$. Dann haben wir $x \in \mathrm{FV}(\forall u\, A[z/y])$, also $LS = \forall u\, (A[z/y])[y/x]$. Ferner ist $RS = (\forall u\, A)[z, y/y, x] = \forall u\, (A[z, y/y, x]) = \forall u\, A([z/y][y/x])$ und die IH liefert die Behauptung. *Unterfall $x \notin \mathrm{FV}(\forall u\, A)$.* Dann ist $x \neq y$ wegen $y \in \mathrm{FV}(\forall u\, A)$. Wegen $x \neq z$ haben wir $LS = (\forall u\, A)[z/y]$. Ferner ist $RS = (\forall u\, A)([z/y][y/x]) = (\forall u\, A)([z, y/y, x]) = (\forall u\, A)[z/y]$.

*Fall $x = z$.* Folgt aus Lemma 5.5b; direkter Beweis: Es ist $LS = ((\forall u\, A)[z/y])[y/z] = (\forall u\, A[z/y])[y/z] = \forall u\, (A[z/y])[y/z] =_{IH} \forall u\, A([z/y][y/z]) = \forall u\, A[y/z] = \forall u\, A$, und $RS = (\forall u\, A)([z/y][y/z]) = (\forall u\, A)[y/z] = \forall u\, A$.

b. Wir führen den Beweis wieder durch Induktion über die Anzahl der logischen Zeichen in $A$ und beschränken uns auf den Fall $\forall z\, A$. Sei $LS := ((\forall z\, A)[y/x])[x/y]$. Wir können oBdA $x \in \mathrm{FV}(\forall z\, A)$ annehmen, denn andernfalls ist $LS = (\forall z\, A)[x/y] = \forall z\, A$.

*Fall $z \neq y$.* Dann ist $LS = (\forall z\, A[y/x])[x/y] = \forall z\, (A[y/x])[x/y]$ wegen $z \neq x$, und nach IH hat man $\vdash_m (A[y/x])[x/y] \leftrightarrow A$.

*Fall $z = y$.* Dann ist $LS = ((\forall y\, A)[y/x])[x/y] = (\forall u\, A([u/y][y/x]))[x/y]$ mit $u \notin \mathrm{FV}(A) \cup \mathrm{BV}(A)$, $u \neq y$. Nach a erhält man weiter $LS = (\forall u\, ((A[u/y])[y/x]))[x/y] = \forall u\, ((A[u/y])[y/x])[x/y]$ wegen $u \neq x$. Nach der IH für $A[u/y]$ ist wegen $y \notin \mathrm{FV}(A[u/y])$ dies minimallogisch äquivalent zu $\forall u\, A[u/y]$ und damit auch zu $\forall y\, A$, denn aus $\forall u\, A[u/y]$ erhält man zunächst $(A[u/y])[y/u]$, daraus aus der IH für $A$ auch $A$ und schließlich $\forall y\, A$.

c folgt jetzt leicht aus b, wie im Beweis von Lemma 5.5. □

*Bemerkung.* Oft reicht auch schon die folgende, einfacher zu beweisende Aussage:

a. $t[y/x][x/y] = t$, falls $y \notin \mathrm{vars}(t)$.

b. $(A[y/x])[x/y] = A$, falls $y \notin \mathrm{FV}(A) \cup \mathrm{BV}(A)$.

c. $\vdash_m \forall x\, A \leftrightarrow \forall y\, A[y/x]$, falls $y \notin \mathrm{FV}(A) \cup \mathrm{BV}(A)$.

*Beweis.* a ist klar. b zeigt man durch Induktion über $A$. Wir behandeln nur den Fall $\forall z\, A$. OBdA ist $x \in \mathrm{FV}(\forall z\, A)$, also $z \neq x$. Wegen $z \neq y$ folgt $(\forall z\, A)[y/x] = \forall z\, A[y/x]$. Weiter ist $(\forall z\, A[y/x])[x/y] = \forall z(A[y/x])[x/y]$, denn es ist $z \neq x$ und $y \in \mathrm{FV}(\forall z\, A[y/x])$ nach Lemma 3.3b (da $x \in \mathrm{FV}(\forall z\, A)$). Die IH liefert die Behauptung.

c. $\rightarrow$ ist klar. $\leftarrow$. OBdA ist $y \neq x$. Dann ist $x \notin \mathrm{FV}(A[y/x])$ nach Lemma 3.3b.

Ferner erhält man mit Teil b, daß $(A[y/x])[x/y] = A$. Also ist die folgende Herleitung korrekt.

$$\dfrac{\dfrac{\dfrac{\forall y\, A[y/x] \quad x}{(A[y/x])[x/y]}}{\forall x\, A}\, x}{}$$

□

Wir nennen zwei Formeln $A$ und $B$ *äquivalent* in der Minimallogik bzw. in der klassischen Logik, wenn $\vdash_m A \leftrightarrow B$ bzw. $\vdash_c A \leftrightarrow B$.

**Lemma 5.6 (Äquivalenzlemma).** *Für $\vdash \in \{\vdash_m, \vdash_c\}$ gilt folgendes. Ist $\vdash A_1 \leftrightarrow A_2$ und entsteht $B_2$ aus $B_1$ durch Ersetzen eines Teils $A_1$ von $B_1$ durch $A_2$, so gilt auch $\vdash B_1 \leftrightarrow B_2$.*

*Beweis* durch Induktion über $B_1$. Falls ganz $B_1$ ersetzt wird, so ist die Behauptung klar. Andernfalls muß $B_1$ eine zusammengesetzte Formel sein.

*Fall* $C_1 \wedge D_1$. Die Ersetzung finde etwa in $C_1$ statt. Zu zeigen ist dann $\vdash C_1 \wedge D_1 \leftrightarrow C_2 \wedge D_1$. $\rightarrow$:

$$\dfrac{\dfrac{\mathcal{D} \qquad \dfrac{C_1 \wedge D_1}{C_1}}{C_2} \qquad \dfrac{C_1 \wedge D_1}{D_1}}{C_2 \wedge D_1}$$

wobei $\mathcal{D}$ nach IH bekannt ist. $\leftarrow$ beweist man ähnlich.

*Fall* $C_1 \rightarrow D_1$. Falls die Ersetzung in $C_1$ stattfindet, ist zu zeigen $\vdash (C_1 \rightarrow D_1) \leftrightarrow (C_2 \rightarrow D_1)$. $\rightarrow$:

$$\dfrac{\dfrac{C_1 \rightarrow D_1 \qquad \dfrac{\mathcal{D}}{C_2 \rightarrow C_1} \quad \dfrac{}{u{:}\,C_2}}{C_1}}{D_1}\, u$$

wobei wieder $\mathcal{D}$ nach IH bekannt ist. $\leftarrow$ beweist man ähnlich. Falls die Ersetzung in $D_1$ stattfindet, ist zu zeigen $\vdash (C_1 \rightarrow D_1) \leftrightarrow (C_1 \rightarrow D_2)$. $\rightarrow$:

$$\dfrac{\dfrac{D_1 \rightarrow D_2 \qquad \dfrac{\mathcal{D}}{C_1 \rightarrow D_1} \quad \dfrac{}{u{:}\,C_1}}{D_1}}{D_2}\, u$$

wobei wieder $\mathcal{D}$ nach IH bekannt ist. $\leftarrow$ beweist man ähnlich.

*Fall* $\forall x\, C_1$. Zu zeigen ist $\vdash \forall x\, C_1 \leftrightarrow \forall x\, C_2$. $\rightarrow$:

$$\dfrac{\dfrac{\mathcal{D}}{C_1 \to C_2} \qquad \dfrac{\forall x\, C_1 \quad x}{C_1}}{\dfrac{C_2}{\forall x\, C_2}}$$

wobei wieder $\mathcal{D}$ nach IH bekannt ist. Man beachte, daß $\mathcal{D}$ keine freien Annahmen enthält. $\leftarrow$ beweist man ähnlich. □

### 1.5.2 Herleitungen als Terme

Herleitungen kann man in natürlicher Weise als getypte Terme auffassen. Wir wollen diese Idee zunächst im Fall der reinen Implikationslogik illustrieren.

Als Grundbausteine von Herleitungstermen verwenden wir mit Formeln versehene Annahmenvariable $u\colon A$; $u$ ist wieder eines der Symbole $\square_0, \square_1, \ldots$. Wir verlangen wie bisher, daß verschiedene Annahmeformeln stets verschiedene Marken $u$ haben. Als Mitteilungszeichen für Herleitungsterme verwenden wir $d, e, f$. Oft schreiben wir auch $u^A$ anstelle von $u\colon A$ und $d^A$ anstelle von $d\colon A$.

Herleitungsterme werden aus Annahmenvariablen $u^A$ erzeugt durch *Abstraktion* und *Anwendung*. Ist $d^B$ ein Herleitungsterm, so auch $(\lambda u^A d^B)^{A\to B}$. Sind $d^{A\to B}$ und $e^A$ Herleitungsterme, so auch $(d^{A\to B} e^A)^B$. Die Abstraktion entspricht der Einführungsregel $\to$I,$u$ für die Implikation $\to$, und die Anwendung entpricht der Beseitigungsregel $\to$E.

Die Herleitungsterme der reinen Implikationslogik sind gerade die Terme des *einfach getypten Lambda–Kalküls*.

Die Parallele zwischen Beweisen und Formeln auf der einen Seite und Termen und Typen auf der anderen Seite nennt man üblicherweise die *Formeln–als–Typen*–Idee. Sie hat sich in Untersuchungen im Bereich der mathematischen Logik und der theoretischen Informatik als recht fruchtbar erwiesen.

*Bemerkung.* Man beachte, daß Herleitungsterme und Herleitungen sich eineindeutig entsprechen. Insbesondere enthält jeder Herleitungsterm die volle Information über die zugrunde liegende Herleitung. Man beachte ferner, daß in Herleitungstermen viele Bestandteile überflüssig sind. Wenn man $(\lambda u\, d)^{A\to B}$ schreibt, so ist klar, daß $u$ den Typ $A$ und $d$ den Typ $B$ haben müssen. Ebenso muß in $(d^{A\to B} e)$ der Gesamtterm den Typ $B$ und $e$ den Typ $A$ haben. Wir werden im folgenden häufig solche redundanten Typen weglassen.

Wir geben jetzt eine simultane induktive Definition der *Herleitungsterme* (in der Minimallogik) und der Menge ihrer *freien Annahmen*. Herleitungsterme bezeichnen wir mit $d, e, \ldots$ und die Menge ihrer freien Annahmen mit $\mathrm{FA}(d)$.

(A) $u^A$ ist ein Herleitungsterm, $\mathrm{FA}(u^A) := \{A\}$.

($\wedge$I) Sind $d^A$ und $e^B$ Herleitungsterme, so auch

$$\langle d^A, e^B \rangle^{A \wedge B}.$$

$\mathrm{FA}(\langle d^A, e^B \rangle^{A \wedge B}) := \mathrm{FA}(d^A) \cup \mathrm{FA}(e^B)$.

($\wedge \mathrm{E_r}$) Ist $d^{A_0 \wedge A_1}$ ein Herleitungsterm, so auch

$$\pi_0(d^{A_0 \wedge A_1})^{A_0}.$$

$\mathrm{FA}(\pi_0(d^{A_0 \wedge A_1})^{A_0}) := \mathrm{FA}(d^{A_0 \wedge A_1})$.

($\wedge \mathrm{E_l}$) Ist $d^{A_0 \wedge A_1}$ ein Herleitungsterm, so auch

$$\pi_1(d^{A_0 \wedge A_1})^{A_1}.$$

$\mathrm{FA}(\pi_1(d^{A_0 \wedge A_1})^{A_1}) := \mathrm{FA}(d^{A_0 \wedge A_1})$.

($\to$I) Ist $d^B$ ein Herleitungsterm, so auch

$$(\lambda u^A d^B)^{A \to B}.$$

$\mathrm{FA}((\lambda u^A d^B)^{A \to B}) := \mathrm{FA}(d^B) \setminus \{u^A\}$.

($\to$E) Sind $d^{A \to B}$ und $e^A$ Herleitungsterme, so auch

$$(d^{A \to B} e^A)^B.$$

$\mathrm{FA}((d^{A \to B} e^A)^B) := \mathrm{FA}(d^{A \to B}) \cup \mathrm{FA}(e^A)$.

($\forall$I) Ist $d^A$ ein Herleitungsterm und $x \notin \bigcup\{\mathrm{FV}(B) : u^B \in \mathrm{FA}(d^A)\}$, so auch

$$(\lambda x\, d^A)^{\forall x\, A}.$$

$\mathrm{FA}((\lambda x\, d^A)^{\forall x\, A}) := \mathrm{FA}(d^A)$.

($\forall$E) Ist $d^{\forall x\, A}$ ein Herleitungsterm und $t$ ein Term, so ist

$$(d^{\forall x\, A} t)^{A[t/x]}$$

ein Herleitungsterm. $\mathrm{FA}((d^{\forall x\, A} t)^{A[t/x]}) := \mathrm{FA}(d)$.

Ein Herleitungsterm $d^A$ heißt *geschlossen*, wenn $\mathrm{FA}(d^A) = \emptyset$. Wir schreiben

$$d^B[u_1^{A_1}, \ldots, u_n^{A_n}]$$

um mitzuteilen, daß die freien Annahmen von $d^B$ in der Liste $u_1^{A_1}, \ldots, u_n^{A_n}$ enthalten sind.

**Definition.** *Für jeden Herleitungsterm $d$ definieren wir seine Menge* $\mathrm{FV}(d)$ *von freien (Objekt–) Variablen durch*

$$\begin{aligned}
\mathrm{FV}(u^A) &:= \mathrm{FV}(A).\\
\mathrm{FV}(\langle d^A, e^B\rangle) &:= \mathrm{FV}(d^A) \cup \mathrm{FV}(e^B).\\
\mathrm{FV}(\pi_i(d^{A\wedge B})) &:= \mathrm{FV}(d^{A\wedge B}).\\
\mathrm{FV}(\lambda u^A d^B) &:= \mathrm{FV}(A) \cup \mathrm{FV}(d^B).\\
\mathrm{FV}(d^{A\to B} e^A) &:= \mathrm{FV}(d^{A\to B}) \cup \mathrm{FV}(e^A).\\
\mathrm{FV}(\lambda x\, d^A) &:= \mathrm{FV}(d^A) \setminus \{x\}.\\
\mathrm{FV}(d^{\forall x\, A} t) &:= \mathrm{FV}(d^{\forall x\, A}) \cup \mathrm{vars}(t).
\end{aligned}$$

*Beispiel.* Man betrachte die folgende Herleitung:

$$\frac{\begin{array}{c}u\colon Rx\end{array}}{Rx \to Rx}\, u.$$

Für den zugehörigen Herleitungsterm $d$ gilt dann

$$\begin{aligned}
&d = \lambda u^{R(x)}\, u^{R(x)},\\
&\mathrm{FA}(d) = \emptyset,\\
&\mathrm{FV}(d) = \{x\}.
\end{aligned}$$

Für Herleitungsterme haben wir zwei Arten von Substitutionen: Man kann einen Herleitungsterm $f^A$ für eine Annahmenvariable $u^A$ substituieren, und man kann auch einen Objektterm $t$ für eine Objektvariable $x$ substituieren.

### 1.5.3 Abgeleitete Regeln für Disjunktion und Existenz

Disjunktion und Existenz hatten wir definiert durch

$$\begin{aligned}
A \vee B &:= \neg(\neg A \wedge \neg B),\\
\exists x\, A &:= \neg\forall x\, \neg A.
\end{aligned}$$

Herleitungen von Formeln mit $\vee, \exists$ lassen sich jedoch oft leichter finden, wenn man nicht auf diese Definitionen zurückgeht, sondern direkt mit '*abgeleiteten Regeln*' für $\vee, \exists$ arbeitet. Darunter verstehen wir die folgenden Regeln.

Für die Disjunktion $\vee$ gibt es zwei Einführungsregeln $\vee\mathrm{I_l}$ und $\vee\mathrm{I_r}$, sowie eine Beseitigungsregel $\vee\mathrm{E}$,$uv$.

$$\frac{\begin{array}{c}\mathcal{D}\\ A\end{array}}{A \vee B}\,\vee\mathrm{I_r} \qquad \frac{\begin{array}{c}\mathcal{D}\\ B\end{array}}{A \vee B}\,\vee\mathrm{I_l} \qquad \frac{\begin{array}{ccc}\mathcal{D} & [u\colon A] & [v\colon B]\\ A \vee B & \mathcal{D}_1 & \mathcal{D}_2\\ & C & C\end{array}}{C}\,\vee\mathrm{E},uv$$

Für den Existenzquantor $\exists$ gibt es eine Einführungsregel $\exists$I, die als rechte Prämisse den zu substituierenden Term $t$ hat, und eine Beseitigungsregel $\exists$E,$xu$. Die Regel $\exists$E,$xu$ unterliegt der folgenden *Variablenbedingung*: Die Herleitung $\mathcal{D}_1$ darf keine offenen Annahmen außer $u\colon A$ enthalten, in denen $x$ frei vorkommt, und ferner darf $B$ die Variable $x$ nicht frei enthalten.

$$\dfrac{\begin{array}{c}\mathcal{D}\\ A[t/x]\end{array}\quad t}{\exists x\,A}\,\exists\mathrm{I} \qquad \dfrac{\begin{array}{ccc} & [u\colon A] & \\ \mathcal{D} & \mathcal{D}_1 & \\ \exists x\,A & & B\end{array}}{B}\,\exists\mathrm{E},xu$$

Der doppelte Strich deutet hierbei an, daß es sich nicht um eine primitive Regel unserer Logik handelt, sondern daß man an dieser Stelle einen Herleitungsteil so einsetzen kann, daß eine korrekt gebildete Herleitung entsteht. Dies läßt sich am besten mit Hilfe von Herleitungstermen präzisieren. Wir geben im folgenden für jede der abgeleiteten Regeln den einzusetzenden Herleitungsteil sowie die Definition des zugehörigen Herleitungsterms an.

$\vee\mathrm{I}_\mathrm{r}$ ($\vee\mathrm{I}_\mathrm{r}$ wird entsprechend behandelt):

$$\dfrac{\dfrac{\underline{u\colon \neg A\wedge\neg B}\quad \mathcal{D}}{\dfrac{\neg A\qquad A}{\bot}}}{\neg(\neg A\wedge\neg B)}\,u$$

Der zugehörige Herleitungsterm ist

$$\lambda u^{\neg A\wedge\neg B}.\pi_0 u^{\neg A\wedge\neg B} d^A =: \vee\mathrm{I}_\mathrm{r}(d^A)^{A\vee B}.$$

$\vee\mathrm{E},uv$:

$$\dfrac{\begin{array}{c}\mathcal{D}_{\mathrm{Stab}}\\ \neg\neg C\to C\end{array}\qquad \dfrac{\begin{array}{c}\mathcal{D}\\ \neg(\neg A\wedge\neg B)\end{array}\qquad \dfrac{\dfrac{\underline{w\colon \neg C}\quad C}{\dfrac{\bot}{\neg A}}\,u}{\neg A\wedge\neg B}}{\dfrac{\bot}{\neg\neg C}\,w}}{C}$$

$$\dfrac{\dfrac{\underline{w\colon \neg C}\quad C}{\dfrac{\bot}{\neg B}}\,v}{\neg A\wedge\neg B}$$

$$\dfrac{[u\colon A]}{\mathcal{D}_1}\qquad \dfrac{[v\colon B]}{\mathcal{D}_2}$$

Der zugehörige Herleitungsterm ist

$$\mathrm{Stab}_C\,\lambda w^{\neg C}.d\langle\lambda u^A.w^{\neg C}d_1^C,\lambda v^B.w^{\neg C}d_2^C\rangle =: (\delta u^A,v^B.d^{A\vee B}d_1^C d_2^C)^C.$$

∃I:

$$\dfrac{\dfrac{u\colon \forall x\, \neg A \quad t}{\neg A[t/x]} \qquad \begin{matrix}\mathcal{D}\\ A[t/x]\end{matrix}}{\dfrac{\bot}{\neg\forall x\, \neg A}\, u}$$

Der zugehörige Herleitungsterm ist

$$\lambda u^{\forall x\, \neg A}.utd^{A[t/x]} =: \exists \mathrm{I}(d^{A[t/x]}, t)^{\exists x\, A}.$$

∃E,$xu$:

$$\dfrac{\begin{matrix}\mathcal{D}_{\mathrm{Stab}}\\ \neg\neg B \to B\end{matrix} \qquad \dfrac{\begin{matrix}\mathcal{D}_1\\ \neg\forall x\, \neg A\end{matrix} \qquad \dfrac{\dfrac{\dfrac{[u\colon A]}{\begin{matrix}\mathcal{D}_2\\ v\colon \neg B\end{matrix} \qquad B}}{\bot}\, u}{\neg A}\, x}{\forall x\, \neg A}}{\bot}\, v}{\neg\neg B}}{B}$$

Der zugehörige Herleitungsterm ist

$$\mathrm{Stab}_B \lambda v^{\neg B}.d_1^{\neg\forall x\, \neg A}(\lambda x \lambda u^A.v^{\neg B} d_2^B) =: (\varepsilon x, u^A.d_1^{\exists x\, A} d_2^B)^B.$$

### 1.5.4 Konjunktive und disjunktive Normalform

Im folgenden schreiben wir der Kürze halber $\vdash$ für $\vdash_c$.

**Lemma 5.7 (Assoziativität, Kommutativität und Distributivität von $\wedge$ und $\vee$).**

*a.* $\vdash A \wedge (B \wedge C) \leftrightarrow (A \wedge B) \wedge C$.

*b.* $\vdash A \vee (B \vee C) \leftrightarrow (A \vee B) \vee C$.

*c.* $\vdash A \wedge B \leftrightarrow B \wedge A$.

*d.* $\vdash A \vee B \leftrightarrow B \vee A$.

*e.* $\vdash A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$.

*f.* $\vdash A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$.

*Beweis.* Übung. □

**Lemma 5.8.**

*a. (De–Morgan–Äquivalenzen).*

$$\vdash \neg(A \wedge B) \leftrightarrow \neg A \vee \neg B,$$
$$\vdash \neg(A \vee B) \leftrightarrow \neg A \wedge \neg B.$$

*b. ($\rightarrow$ aus $\neg, \wedge$ bzw. $\neg, \vee$).*

$$\vdash (A \to B) \leftrightarrow \neg(A \wedge \neg B),$$
$$\vdash (A \to B) \leftrightarrow \neg A \vee B.$$

*c. (Tertium non datur).*

$$\vdash A \vee \neg A.$$

*Beweis.* a. Die Behauptung ergibt sich aus der Definition von $\vee$, dem Stabilitätslemma 5.2 und dem Äquivalenzlemma 5.6.

b1. $\rightarrow$.

$$\dfrac{\dfrac{A \wedge \neg B}{\neg B} \quad \dfrac{A \to B \qquad \dfrac{A \wedge \neg B}{A}}{B}}{\bot}$$

$\leftarrow$.

$$\dfrac{\mathcal{D}_{\mathrm{Stab}}}{\dfrac{\neg\neg B \to B \qquad \dfrac{\dfrac{\neg(A \wedge \neg B) \qquad \dfrac{u\colon A \quad v\colon \neg B}{A \wedge \neg B}}{\bot}}{\neg\neg B}}{B}\, u}{A \to B}$$

b2. $\rightarrow$. Hier helfen die abgeleiteten Regeln für $\vee$ nicht und wir müssen auf die Definition von $\vee$ zurückgehen.

$$\dfrac{\dfrac{v\colon \neg\neg A \wedge \neg B}{\neg B} \quad \dfrac{u\colon A \to B \qquad \dfrac{\mathcal{D}_{\mathrm{Stab}} \qquad v\colon \neg\neg A \wedge \neg B}{\neg\neg A \to A \qquad \neg\neg A}}{A}}{B}}{\bot}$$

$\leftarrow$. Hier kann man wieder eine abgeleitete Regel für $\vee$ verwenden; ferner benötigt man das Ex–Falso–Quodlibet–Lemma 5.3.

c ergibt sich sofort aus der Definition von $\vee$:

$$\dfrac{\dfrac{u\colon \neg A \wedge \neg\neg A}{\neg\neg A} \quad \dfrac{u\colon \neg A \wedge \neg\neg A}{\neg A}}{\bot}$$

□

**Satz 5.9 (Konjunktive und disjunktive Normalform).**

a. *Jede Formel ist logisch äquivalent zu einer Formel der Gestalt*

$$\bigwedge_{i=1}^{n} \bigvee_{j=1}^{n_i} A_{ij} \qquad \textit{(konjunktive Normalform),}$$

*wobei die $A_{ij}$ aussagenlogisch unzerlegbare Formeln (d.h. Primformeln oder von der Form $\forall x\, A$) oder Negationen davon sind.*

a. *Jede Formel ist logisch äquivalent zu einer Formel der Gestalt*

$$\bigvee_{i=1}^{n} \bigwedge_{j=1}^{n_i} A_{ij} \qquad \textit{(disjunktive Normalform),}$$

*wobei die $A_{ij}$ aussagenlogisch unzerlegbare Formeln oder Negationen davon sind.*

*Beweis* von a und b gemeinsam durch Induktion über die gegebene Formel, unter Verwendung des Äquivalenzlemmas 5.6.

*Fall* Primformel, $\forall x\, A$. In diesem Fall ist nichts zu zeigen.

*Fall* $A \wedge B$. Für a verwendet man die konjunktive Normalform von $A$ und von $B$. b ergibt sich aus der disjunktiven Normalform von $A$ und von $B$ durch Ausdistribuieren.

*Fall* $A \to B$. Die Behauptung ergibt sich aus $\vdash (A \to B) \leftrightarrow \neg A \vee B$ und den De–Morgan–Äquivalenzen, und zwar für a unter Verwendung der disjunktiven Normalform von $A$ und der konjunktiven Normalform von $B$ und für b unter Verwendung der konjunktiven Normalform von $A$ und der disjunktiven Normalform von $B$, wobei in a noch auszudistribuieren ist. □

Eine konjunktive Normalform von $A$ (die offenbar nicht eindeutig bestimmt ist) nennt man auch eine *Klauselform* von $A$. Da eine Konjunktion genau dann herleitbar ist, wenn dies für jedes Konjunktionsglied gilt, kann man sich also bei der Suche nach Herleitungen von Formeln auf sogenannte Klauseln, also Disjunktionen von aussagenlogisch unzerlegbaren Formeln beschränken. Man beachte, daß die Herstellung etwa der konjunktiven Normalform einer gegebenen Formel im allgemeinen exponentiell viele (in der Länge der Formel) Rechenschritte erfordert, da bei den Disjunktivgesetzen Formeln dupliziert werden.

### 1.5.5 Pränexe Normalform

**Lemma 5.10 (Herausziehen von Quantoren).** *Sei $x$ nicht frei in $A$. Dann gilt*

*a.* $\vdash A \wedge \forall x\, B \leftrightarrow \forall x(A \wedge B)$.

*b.* $\vdash A \wedge \exists x\, B \leftrightarrow \exists x(A \wedge B)$.

*c.* $\vdash (A \to \forall x\, B) \leftrightarrow \forall x(A \to B)$.

*d.* $\vdash (A \to \exists x\, B) \leftrightarrow \exists x(A \to B)$.

*e.* $\vdash (\forall x\, B \to A) \leftrightarrow \exists x(B \to A)$.

*f.* $\vdash (\exists x\, B \to A) \leftrightarrow \forall x(B \to A)$.

*Beweis.* Wir behandeln hier und im folgenden die abgeleiteten Regeln für $\exists$ und $\vee$ wie gewöhnliche Regeln.

a ist sehr leicht zu zeigen. b $\to$.

$$\dfrac{v\colon \exists x\, B \qquad \dfrac{\dfrac{u\colon A \quad u_0\colon B}{A \wedge B}}{\exists x(A \wedge B)}\, x}{\exists x(A \wedge B)}\, x, u_0$$

b $\leftarrow$.

$$\dfrac{\dfrac{u\colon \exists x(A \wedge B) \qquad \dfrac{u_0\colon A \wedge B}{A}}{A}\, x, u_0 \qquad \dfrac{u\colon \exists x(A \wedge B) \qquad \dfrac{\dfrac{u_1\colon A \wedge B}{B}}{\exists x\, B}\, x}{\exists x\, B}\, x, u_1}{A \wedge \exists x\, B}$$

c haben wir in den Beispielen (3) und (4) am Beginn von 1.5.1 bewiesen.

d $\to$. Hier helfen die abgeleiteten Regeln für $\exists$ nicht; wir müssen auf die Definition von $\exists$ zurückgehen. Ferner ist es nützlich, sich an die (klassische) Äquivalenz von $\neg(A \to B)$ mit $A \wedge \neg B$ zu erinnern. Wir führen den Beweis informal, und zwar so daß klar ist, wie man daraus (unter Zuhilfenahme des Äquivalenzlemmas 5.6) eine formale Herleitung gewinnen kann. Gelte also (1) $A \to \neg\forall x\, \neg B$ und (2) $\forall x(A \wedge \neg B)$. Aus (2) erhält man $A$, also aus (1) $\neg\forall x\, \neg B$. Aus (2) erhält man auch $\forall x\, \neg B$, also insgesamt $\bot$, wie gewünscht.

d $\leftarrow$.

$$\dfrac{u\colon \exists x(A \to B) \qquad \dfrac{\dfrac{u_0\colon A \to B \quad u_1\colon A}{B} \qquad x}{\exists x\, B}\, x, u_0}{\dfrac{\exists x\, B}{A \to \exists x\, B}\, u_1}$$

e $\to$. Hier helfen wieder die abgeleiteten Regeln für $\exists$ nicht; wir müssen auf die Definition von $\exists$ zurückgehen. Ferner ist es wieder nützlich, sich an die (klassische) Äquivalenz von $\neg(A \to B)$ mit $B \wedge \neg A$ zu erinnern. Wir führen den Beweis wieder informal. Gelte also (1) $\forall x\, B \to A$ und (2) $\forall x(B \wedge \neg A)$. Aus (2) erhält man $\forall x\, B$, also aus (1) $A$. Aus (2) erhält man auch $\neg A$, also insgesamt $\bot$, wie gewünscht.

e $\leftarrow$.

$$\dfrac{u\colon \exists x(B \to A) \qquad \dfrac{\dfrac{u_1\colon \forall x\, B \quad x}{B}}{A}\, x, u_0}{\dfrac{A}{\forall x\, B \to A}\, u_1}$$

f $\to$.

$$\dfrac{\dfrac{u\colon \exists x\, B \to A \qquad \dfrac{u_0\colon B \quad x}{\exists x\, B}}{A}\, u_0}{\dfrac{B \to A}{\forall x(B \to A)}\, x}$$

f $\leftarrow$.

$$\dfrac{v\colon \exists x\, B \qquad \dfrac{u\colon \forall x(B \to A) \quad x}{B \to A} \qquad u_1\colon B}{A}\, x, u_1$$

□

Eine Formel $A$ heißt *pränex*, wenn

$$A = Q_1 x_1 Q_2 x_2 \ldots Q_n x_n\, B$$

mit $Q_i \in \{\forall, \exists\}$ und $B$ quantorenfrei. $B$ heißt der *Kern* von $A$ und $Q_1 x_1 Q_2 x_2 \ldots Q_n x_n$ das *Präfix* von $A$. Wir zeigen jetzt, daß sich jede Formel in eine *pränexe Normalform* bringen läßt.

**Satz 5.11 (Pränexe Normalform).** *Zu jeder Formel $A$ findet man eine pränexe Formel $A'$ mit*

$$\vdash A \leftrightarrow A'.$$

*Beweis* durch Induktion über $A$.

*Fall* Primformel. In diesem Fall ist nichts zu zeigen.

*Fall* $A \wedge B$. Nach IH haben wir $\vdash A \leftrightarrow A'$ und $\vdash B \leftrightarrow B'$ mit

$$\begin{aligned} A' &= Q_1 x_1 \ldots Q_n x_n \, A_0, \qquad A_0 \text{ quantorenfrei}, \\ B' &= Q_1^* y_1 \ldots Q_m^* y_m \, B_0, \qquad B_0 \text{ quantorenfrei}. \end{aligned}$$

Nach dem Umbenennungslemma 5.5 und dem Äquivalenzlemma 5.6 können wir oBdA annehmen, daß kein $x_i$ in $B'$ und kein $y_j$ in $A'$ vorkommt. Nach dem Lemma 5.10 über das Herausziehen von Quantoren und dem Äquivalenzlemma 5.6 folgt

$$\vdash A \wedge B \leftrightarrow Q_1 x_1 \ldots Q_n x_n Q_1^* y_1 \ldots Q_m^* y_m (A_0 \wedge B_0).$$

*Fall* $A \to B$. Wie eben erhält man

$$\vdash (A \to B) \leftrightarrow \overline{Q}_1 x_1 \ldots \overline{Q}_n x_n Q_1^* y_1 \ldots Q_m^* y_m (A_0 \wedge B_0).$$

wobei $\overline{Q}_i = \forall$, falls $Q_i = \exists$, und $\overline{Q}_i = \exists$, falls $Q_i = \forall$.

*Fall* $\forall x \, A$. Nach IH haben wir $\vdash A \leftrightarrow A'$ mit einem pränexen $A'$. Nach dem Äquivalenzlemma 5.6 folgt

$$\vdash \forall x \, A \leftrightarrow \forall x \, A'. \qquad \square$$

Zur Berechnung der pränexen Normalform ist es nützlich, die folgenden leicht zu beweisenden Äquivalenzen zu verwenden.

**Lemma 5.12.**

$$\begin{aligned} &\vdash \neg \forall x \, B \leftrightarrow \exists x \, \neg B, \\ &\vdash \neg \exists x \, B \leftrightarrow \forall x \, \neg B, \\ &\vdash A \vee \forall x \, B \leftrightarrow \forall x (A \vee B), \qquad \textit{falls } x \notin \mathrm{FV}(A), \\ &\vdash A \vee \exists x \, B \leftrightarrow \exists x (A \vee B), \qquad \textit{falls } x \notin \mathrm{FV}(A). \end{aligned}$$

*Beweis.* Übung. $\square$

## 1.6 Hilbertkalküle

Es gibt viele verschiedene Logikkalküle in der Literatur. Unter einem *Hilbertkalkül* verstehen wir einen Logikkalkül, in dem man nicht die Möglichkeit hat, offene Annahmen zu streichen, also ohne die Regel $\to$I der $\to$–Einführung. Ein derartiges System für die Minimallogik ist etwa das folgende. Axiomenschemata:

$$
\begin{aligned}
&K\colon B \to A \to B,\\
&S\colon (A \to B \to C) \to (A \to B) \to A \to C,\\
&\wedge\text{I–Ax}\colon A \to B \to A \wedge B,\\
&\wedge\text{E}_i\text{–Ax}\colon A_0 \wedge A_1 \to A_i,\\
&\forall\text{I–Ax}\colon \forall x (A \to B) \to (A \to \forall x\, B), \qquad \text{falls } x \notin \mathrm{FV}(A),\\
&\forall\text{E–Ax}\colon \forall x\, A \to A[t/x].
\end{aligned}
$$

Regeln: Nur $\to$E, $\forall$I. Manchmal nennt man $\forall$I die *Generalisierungsregel*. Man beachte, daß wir zusätzlich zu den Axiomen (oder besser Axiomenkonstanten) auch Annahmenvariablen erlauben. Die Variablenbedingung in der Generalisierungsregel bezieht sich nur auf die freien Annahmenvariablen, nicht auf die Axiomenkonstanten.

*Beispiel.* Wir zeigen, daß $A \to A$ im Hilbertkalkül herleitbar ist. Eine Herleitung mit Herleitungsterm $SKK$ ist

$$
\dfrac{\dfrac{(A \to (A \to A) \to A) \to (A \to A \to A) \to A \to A \quad A \to (A \to A) \to A}{(A \to A \to A) \to A \to A} \qquad A \to A \to A}{A \to A}
$$

Wir wollen zeigen, daß dieser Hilbertkalkül äquivalent ist zu dem System des natürlichen Schließens für die Minimallogik, das wir oben eingeführt haben.

Für die nichttriviale Richtung betrachten wir ein Zwischensystem, das die obigen Axiome hat und als Regeln nur $\to$I, $\to$E, $\forall$I.

Wir zeigen zunächst, daß man zu jedem Herleitungsterm $d[\vec{u}\colon \vec{A}]\colon B$ im System des natürlichen Schließens einen Herleitungsterm $d'[\vec{u}\colon \vec{A}]\colon B$ im Zwischensystem finden kann. Dies zeigen wir durch Induktion über $d$.

*Fall* $\langle d_0, d_1 \rangle$. Wähle $\wedge$I–Ax $d_0' d_1'$.

*Fall* $\pi_i(d)$. Wähle $\wedge$E$_i$–Ax $d'$.

*Fall* $dt$. Wähle $\forall$E–Ax $d'$. □

**Satz 6.1 (Deduktionstheorem).** *Für jeden Herleitungsterm $d[u^A, \vec{u}\colon \vec{A}]\colon B$ im Hilbertkalkül findet man einen Herleitungsterm $(\lambda^* u^A\, d)[\vec{u}\colon \vec{A}]\colon A \to B$ wieder im Hilbertkalkül.*

*Beweis* durch Induktion über $d$.

*Fall* $v \neq u$ oder Axiom. Wähle $\lambda^* u^A\, d := Kd$.

*Fall* $u$. Wähle $\lambda^* u^A\, u := SKK$; hierbei hat $S$ wie oben den Typ $S\colon (A \to (A \to A) \to A) \to (A \to A \to A) \to A \to A$.

*Fall* $de$. Wähle $\lambda^* u^A.de := S(\lambda^* u^A\, d)(\lambda^* u^A\, e)$.

*Fall* $\lambda x\, d$. Wähle $\lambda^* u^A(\lambda x\, d) := \forall\text{I–Ax}(\lambda x(\lambda^* u^A\, d))$. □

**Satz 6.2.** *Für jeden Herleitungsterm $d[\vec{u}\colon \vec{A}]\colon B$ im System des natürlichen Schließens findet man eine Herleitung von $B$ aus $\vec{A}$ im Hilbertkalkül.*

*Beweis.* Wir können annehmen, daß $d$ ein Herleitungsterm im Zwischensystem ist. Verwendet wird wieder Induktion über $d$. Der einzig interessante Fall ist der, wo der Herleitungsterm von der Form $(\lambda u^A\, d[u^A, \vec{u}\colon \vec{A}])\colon A \to B$ ist. Nach IH können wir annehmen, daß $d[u^A, \vec{u}\colon \vec{A}]\colon B$ bereits ein Herleitungsterm im Hilbertkalkül ist. Dann liefert uns aber das Deduktionstheorem eine Herleitung $(\lambda^* u^A\, d)[\vec{u}\colon \vec{A}]\colon A \to B$ von $A \to B$ aus $\vec{A}$ im Hilbertkalkül. □

*Bemerkung.* Man betrachte die folgende Variante des Hilbertkalküls. Axiome: Alle Formeln der Gestalt $\forall x_1, \ldots, x_n\, A$, wobei $A$ eine der folgenden Formen hat.

$$
\begin{aligned}
&K\colon B \to A \to B,\\
&S\colon (A \to B \to C) \to (A \to B) \to A \to C,\\
&\wedge\text{I–Ax}\colon A \to B \to A \wedge B,\\
&\wedge\text{E}_i\text{–Ax}\colon A_0 \wedge A_1 \to A_i,\\
&K^{\forall}\colon B \to \forall x\, B, \quad \text{falls } x \notin \mathrm{FV}(B),\\
&S^{\forall}\colon \forall x(B \to C) \to \forall x\, B \to \forall x\, C,\\
&\forall\text{E–Ax}\colon \forall x\, A \to A[t/x].
\end{aligned}
$$

Regeln: Nur $\to$E. Zusätzlich zu den Axiomen sind Annahmenvariablen erlaubt. Durch Modifikation der vorangehenden Überlegung kann man leicht zeigen, daß man zu jedem Herleitungsterm $d[\vec{u}\colon \vec{A}]\colon B$ im System des natürlichen Schließens einen Herleitungsterm $d'[\vec{u}\colon \vec{A}]\colon B$ in dieser Variante des Hilbertkalküls finden kann.

# 1.7 Vollständigkeit

Jetzt können wir die Umkehrung des Korrektheitssatzes 5.1, den sogenannten Vollständigkeitssatz beweisen. Dies wird hier nur für abzählbare Sprachen $\mathcal{L}$ durchgeführt. (Eine Sprache $\mathcal{L}$ heißt abzählbar, wenn in $\mathcal{L}$ höchstens abzählbar viele Relations– und Funktionssymbole vorkommen.) Der Beweis wird jedoch so angesetzt, daß er sich später leicht auf überabzählbare Sprachen übertragen läßt.

Zur Vereinfachung wollen wir uns zunächst überlegen, daß man sich auf das Fragment der Logik ohne $\wedge$ beschränken kann.

**Lemma 7.1 (Elimination von $\wedge$).** *Zu jedem $A$ findet man $A_1, \ldots, A_n$ ohne $\wedge$ so daß $\vdash_m A \leftrightarrow \bigwedge_{i=1}^{n} A_i$.*

*Beweis* durch Induktion über $A$. *Fall* $\bot$. Wähle $n = 0$. *Fall* $R\vec{t}$. Wähle $A_i := R\vec{t}$. *Fall* $A \wedge B$. Nach IH haben wir $A_1, \ldots, A_n$ und $B_1, \ldots, B_m$. Wähle $A_1, \ldots, A_n, B_1, \ldots, B_m$. *Fall* $A \to B$. Nach IH haben wir wieder $A_1, \ldots, A_n$ und $B_1, \ldots, B_m$. Zur Vereinfachung sei etwa $n = 2$ und $m = 3$; den allgemeinen Fall behandelt man ähnlich. Es gilt dann

$$\begin{aligned}\vdash_m &(A_1 \wedge A_2 \to B_1 \wedge B_2 \wedge B_3)\\ &\leftrightarrow (A_1 \to A_2 \to B_1) \wedge (A_1 \to A_2 \to B_2) \wedge (A_1 \to A_2 \to B_3).\end{aligned}$$

*Fall* $\forall x\, A$. Nach IH haben wir wieder $A_1, \ldots, A_n$. Wähle $\forall x\, A_1, \ldots, \forall x\, A_n$, denn es gilt

$$\vdash_m \forall x \bigwedge_{i=1}^{n} A_i \leftrightarrow \bigwedge_{i=1}^{n} \forall x\, A_i. \qquad \square$$

Im Beweis des Vollständigkeitssatzes werden wir das *Königsche Lemma* benutzen. Wir führen zunächst die benötigten Begriffe ein. Ein *Knoten* ist eine endliche Folge $\kappa = \langle k_0, k_1, \ldots, k_{n-1}\rangle$ von natürlichen Zahlen; $n$ heißt die *Länge* $\lg(\kappa)$ von $\kappa$. Wir schreiben $\kappa_1 \leq \kappa_2$, wenn $\kappa_1$ Anfangsstück von $\kappa_2$ ist. Ein *Baum* ist eine gegen Bildung von Anfangsstücken abgeschlossene Menge von Knoten. Ein Baum $B$ heißt *endlich verzweigt*, wenn es zu jedem $\kappa \in B$ nur endlich viele unmittelbare Fortsetzungen in $B$ gibt. Ein Baum $B$ heißt *unbeschränkt*, wenn es zu jedem $n$ einen Knoten $\kappa \in B$ mit $\lg(\kappa) = n$ gibt. Ein *Ast* in einem Baum $B$ ist eine durch $\leq$ linear geordnete, gegen Bildung von Anfangsstücken abgeschlossene Teilmenge von $B$. Jeder unendliche Ast ist bestimmt durch eine Folge $(k_n)_{n\in\mathbb{N}}$ von natürlichen Zahlen, deren endliche Anfangsstücke die Knoten des Astes bilden.

**Lemma 7.2 (König).** *Jeder endlich verzweigte unbeschränkte Baum hat einen unendlichen Ast.*

*Beweis.* Sei $B$ endlich verzweigter unbeschränkter Baum. Wir definieren rekursiv natürliche Zahlen $k_n$ wie folgt: $k_n$ ist das kleinste $k$ so daß $\langle k_0, k_1, \ldots, k_{n-1}, k\rangle$ beliebig lange Fortsetzungen in $B$ hat. $\square$

*Bemerkung.* Ohne die Voraussetzung, daß $B$ endlich verzweigt ist, ist das Königsche Lemma falsch. Ein Gegenbeispiel ist die Menge $B$ aller Knoten $\langle n, 0, \ldots, 0\rangle$ mit $n$ Vorkommen von 0. $B$ ist offenbar unbeschränkt, hat aber keinen unendlichen Ast.

Sei $S \cup \{A\}$ eine Menge von $\mathcal{L}$–Formeln. Wir schreiben $S \models A$ (gelesen: aus $S$ *folgt* $A$), wenn für alle $\mathcal{L}$–Strukturen $\mathcal{M}$ und alle Umgebungen $U$ in $|\mathcal{M}|$ aus $\mathcal{M} \models B[U]$ für alle $B \in S$ folgt $\mathcal{M} \models A[U]$. Im Korrektheitssatz 5.1 hatten wir bewiesen $S \vdash A \implies S \models A$. Jetzt können wir die Umkehrung zeigen.

**Vollständigkeitssatz 7.3.** *Sei $S \cup \{A\}$ eine Menge von $\mathcal{L}$–Formeln. Dann gilt*

$$S \models A \implies S \vdash A.$$

*Beweis.* Wir verwenden ein auf Beth, Hintikka und Schütte zurückgehendes Verfahren. Konstruiert wird ein universeller (also von $S$ und $A$ unabhängiger) Suchbaum. Mit Hilfe dieses universellen Suchbaums erhalten wir dann zu gegebenem $S$ und $A$ entweder eine Herleitung von $A$ aus $S$ in der klassischen Logik oder ein Gegenbeispiel, d.h. ein Modell von $S \cup \{\neg A\}$.

Zur Definition des universellen Suchbaums benötigen wir an gewissen Stellen neue Variablen. Zunächst können wir offenbar annehmen, daß es eine abzählbar unendliche Menge $V$ von Variablen gibt, die weder in $S$ noch in $A$ vorkommen. Sei AllFor die Menge der Allformeln und Ter die Menge der Terme von $\mathcal{L}$. Da $\mathcal{L}$ als abzählbar angenommen wurde, können wir von einer festen Abzählung von AllFor $\times$ Ter ausgehen; wir schreiben $(\forall y\, C, s) \prec (\forall x\, B, t)$, wenn $(\forall y\, C, s)$ vor $(\forall x\, B, t)$ in dieser Abzählung vorkommt. Wir können dann rekursiv eine injektive Abbildung neu: AllFor $\times$ Ter $\to V$ definieren so daß $\mathrm{neu}(\forall x\, B, t)$ in keinem $(\forall y\, C, s)$ vorkommt mit $(\forall y\, C, s) \preceq (\forall x\, B, t)$.

Man beachte zunächst, daß wir aufgrund von Lemma 7.1 annehmen können, daß weder $S$ noch $A$ die Verknüpfung $\wedge$ enthält. Sei noch AtomFor die Menge der atomaren Formeln und ImpFor die Menge der Implikationsformeln von $\mathcal{L}$. Wir betrachten

$$I := \mathrm{AtomFor} \cup \mathrm{ImpFor} \cup (\mathrm{AllFor} \times \mathrm{Ter})$$

als Indexmenge. Für jedes $F \in I$ und jedes $k \in \{0, 1, 2\}$ definieren wir eine endliche Formelmenge $\Delta_k(F)$ durch

$$\Delta_k(B) := \begin{cases} \{\neg B\}, & \text{falls } k = 0, \\ \{B\}, & \text{falls } k \in \{1, 2\}, \end{cases} \qquad \text{für } B \text{ atomar},$$

$$\Delta_k(B \to C) := \begin{cases} \{\neg(B \to C), B, \neg C\}, & \text{falls } k = 0, \\ \{B \to C, \neg B\}, & \text{falls } k = 1, \\ \{B \to C, C\}, & \text{falls } k = 2, \end{cases}$$

$$\Delta_k(\forall x\, B, t) := \begin{cases} \{\neg\forall x\, B, \neg B[y/x]\}, & \text{falls } k = 0 \text{ und } y = \mathrm{neu}(\forall x\, B, t), \\ \{\forall x\, B, B[t/x]\}, & \text{falls } k \in \{1, 2\}. \end{cases}$$

Eine partielle Abbildung $\alpha$ von $I$ in $\{0,1,2\}$ nennen wir einen *Suchpfad* oder kurz *Pfad*. Für jeden Suchpfad $\alpha$ definieren wir eine Formelmenge $\Gamma_\alpha$ durch

$$\Gamma_\alpha := \bigcup_{F \in \mathrm{dom}(\alpha)} \Delta_{\alpha(F)}(F).$$

$\alpha$ heißt *blockiert*, wenn

- $A \in \Gamma_\alpha$ oder $\neg B \in \Gamma_\alpha$ für ein $B \in S$, oder
- $B, \neg B \in \Gamma_\alpha$ für ein $B$, oder
- $\bot \in \Gamma_\alpha$.

*Positiver Hauptfall.* Es gibt ein $I_0 \subseteq_{\mathrm{fin}} I$ so daß alle Suchpfade $\alpha$ durch $I_0$ (d.h. mit $\mathrm{dom}(\alpha) = I_0$) blockiert sind.

Wir zeigen, daß in diesem Fall gilt $S \vdash A$. Dazu denken wir uns $I_0$ so angeordnet, daß hinter allen mit $\prec$ geordneten Elementen aus AllFor $\times$ Ter alle Formeln aus AtomFor und ImpFor kommen. Mit $J$ bezeichnen wir Teilmengen von $I_0$, die Anfangsstücke bzgl. dieser Ordnung bilden. Wir zeigen, daß für jedes solche $J$ und alle $\alpha$ durch $J$ gilt $\Gamma_\alpha \cup S \vdash A$, und zwar durch Induktion über die Anzahl der Elemente in $I_0 \setminus J$. Mit $J = \emptyset$ folgt dann die Behauptung $S \vdash A$.

Im Basisfall ist $J = I_0$. Nach Annahme ist dann $\alpha$ blockiert; deshalb gilt $\Gamma_\alpha \cup S \vdash A$. Im Schritt unterscheiden wir drei Fälle.

*Fall* $\{B\}\dot\cup J$ mit $B$ atomar. Sei $\alpha$ Suchpfad durch $J$. Nach IH gilt $\Gamma_{\alpha[k/B]} \cup S \vdash A$ für jedes $k \in \{0,1,2\}$, also

$$\{\neg B\} \cup \Gamma_\alpha \cup S \vdash A \qquad \text{und} \qquad \{B\} \cup \Gamma_\alpha \cup S \vdash A,$$

und damit

$$\Gamma_\alpha \cup S \vdash (B \to A) \wedge (\neg B \to A).$$

Mit $\vdash (B \to A) \wedge (\neg B \to A) \to A$ (nach dem Fallunterscheidungslemma 5.4) folgt $\Gamma_\alpha \cup S \vdash A$.

*Fall* $\{B \to C\}\dot\cup J$. Sei $\alpha$ Suchpfad durch $J$. Nach IH gilt $\Gamma_{\alpha[k/B\to C]} \cup S \vdash A$ für jedes $k \in \{0,1,2\}$, also

$$\{\neg(B \to C), B, \neg C\} \cup \Gamma_\alpha \cup S \vdash A, \tag{0}$$
$$\{B \to C, \neg B\} \cup \Gamma_\alpha \cup S \vdash A, \tag{1}$$
$$\{B \to C, C\} \cup \Gamma_\alpha \cup S \vdash A. \tag{2}$$

Wegen $\vdash \neg(B \to C) \to B \wedge \neg C$ folgt aus (0)

$$\{\neg(B \to C)\} \cup \Gamma_\alpha \cup S \vdash A. \tag{3}$$

Wegen $\vdash (\neg B \to A) \wedge (C \to A) \to ((B \to C) \to A)$ folgt aus (1) und (2)

$$\{B \to C\} \cup \Gamma_\alpha \cup S \vdash A. \tag{4}$$

Aus (3) und (4) ergibt sich wie eben mit dem Fallunterscheidungslemma $\Gamma_\alpha \cup S \vdash A$.

*Fall* $\{(\forall x\, B, t)\} \dot\cup J$ mit $J \subseteq \mathrm{AllFor} \times \mathrm{Ter}$ und $(\forall x\, B, t) \succ (\forall y\, C, s)$ für alle $(\forall y\, C, s) \in J$. Sei $\alpha$ Suchpfad durch $J$. Nach IH gilt $\Gamma_{\alpha[k/(\forall x\, B, t)]} \cup S \vdash A$ für jedes $k \in \{0, 1, 2\}$, also

$$\{\neg \forall x\, B, \neg B[y/x]\} \cup \Gamma_\alpha \cup S \vdash A,$$
$$\{\forall x\, B, B[t/x]\} \cup \Gamma_\alpha \cup S \vdash A,$$

wobei $y$ nicht in $\forall x\, B$, $\Gamma_\alpha$, $S$ und $A$ vorkommt. Mit

$$\vdash (\forall x\, B \to A) \to \forall y(\neg \forall x\, B \to \neg B[y/x] \to A) \to A$$

für $y$ nicht in $\forall x\, B$, $A$ ergibt sich wieder mit dem Fallunterscheidungslemma $\Gamma_\alpha \cup S \vdash A$.

*Negativer Hauptfall.* Für jedes $I_0 \subseteq_{\mathrm{fin}} I$ gibt es einen nicht blockierten Suchpfad $\alpha$ durch $I_0$.

Wir zeigen, daß es dann einen nicht blockierten Suchpfad $\alpha$ durch ganz $I$ gibt. Aus $\alpha$ werden wir ein Gegenbeispiel zur Voraussetzung des Satzes erhalten.

Da wir $\mathcal{L}$ als abzählbar vorausgesetzt hatten, ist auch $I$ abzählbar und kann in der Form $I = \{ F_n \mid n \in \mathbb{N} \}$ mit $F_n \neq F_m$ für $n \neq m$ geschrieben werden. Sei

$$B := \{ \kappa \mid \exists \alpha(\alpha \text{ nicht blockiert } \wedge \forall i(i < \lg(\kappa) \to F_i \in \mathrm{dom}(\alpha) \wedge \kappa(i) = \alpha(F_i))) \}.$$

Offenbar ist $B$ ein Baum, d.h. abgeschlossen gegen Bildung von Anfangsstücken. Ferner ist $B$ endlich verzweigt, da stets $\alpha(F) \in \{0, 1, 2\}$ gilt. Schließlich ist $B$ unbeschränkt aufgrund der Annahme im negativen Hauptfall. Nach dem Königschen Lemma 7.2 gibt es also einen etwa durch $(k_n)_{n \in \mathbb{N}}$ bestimmten unendlichen Ast in $B$. Setzt man $\alpha(F_n) := k_n$, so ist $\alpha$ ein nicht blockierter Suchpfad durch ganz $I$.

Mit Hilfe des gefundenen (von $S$ und $A$ abhängigen) nicht blockierten Suchpfades $\alpha$ und der durch $\alpha$ bestimmten Formelmenge

$$\Gamma_\alpha = \bigcup_{F \in I} \Delta_{\alpha(F)}(F)$$

können wir jetzt das gesuchte Gegenbeispiel zur Voraussetzung des Vollständigkeitssatzes konstruieren. Zunächst notieren wir einige Eigenschaften von $\Gamma_\alpha$, die sofort aus der Definition folgen.

(a) Für jede Formel $B$ gilt entweder $B \in \Gamma_\alpha$ oder $\neg B \in \Gamma_\alpha$.

(b) $\bot \notin \Gamma_\alpha$.

(c) $A \notin \Gamma_\alpha$, und $S \subseteq \Gamma_\alpha$.

(d) Wenn $\neg(B \to C) \in \Gamma_\alpha$, so ist $B \in \Gamma_\alpha$ und $\neg C \in \Gamma_\alpha$.

(e) Wenn $B \to C \in \Gamma_\alpha$, so ist $\neg B \in \Gamma_\alpha$ oder $C \in \Gamma_\alpha$.

(f) Wenn $\neg\forall x\, B \in \Gamma_\alpha$, so ist $\neg B[y/x] \in \Gamma_\alpha$ für ein $y$.

(g) Wenn $\forall x\, B \in \Gamma_\alpha$, so ist $B[t/x] \in \Gamma_\alpha$ für alle Terme $t$.

Wir definieren jetzt eine $\mathcal{L}$–Struktur $\mathcal{M}$ durch

$$\mathcal{M} := (\mathrm{Ter}_\mathcal{L}, I_0, I_1),$$

wobei

$$\begin{aligned} I_0(f)(t_1, \ldots, t_n) &:= f(t_1, \ldots, t_n), \\ I_1(R) &:= \{\, (t_1, \ldots, t_n) \mid R(t_1, \ldots, t_n) \in \Gamma_\alpha \,\}. \end{aligned}$$

Man kann nun zeigen

$$\mathcal{M} \models B[\mathrm{id}] \iff B \in \Gamma_\alpha. \qquad (*)$$

Den Beweis führen wir durch Induktion über die Anzahl der logischen Zeichen $\to, \forall$ in $B$. Zu beachten ist, daß bei unserer kanonischen Definition von $I_0(f)$ gilt $\overline{\mathrm{id}}(t) = t$ für alle $\mathcal{L}$–Terme $t$. Wir schreiben $\mathcal{M} \models B$ für $\mathcal{M} \models B[\mathrm{id}]$.

*Fall* $R(\vec{t})$. $\mathcal{M} \models R(\vec{t})$ bedeutet nach Definition von $\mathcal{M}$, daß $R(\vec{t}) \in \Gamma_\alpha$.

*Fall* $\bot$. Nach (b) ist $\bot \notin \Gamma_\alpha$.

*Fall* $B \to C$. $\Longrightarrow$. Gelte $\mathcal{M} \models B \to C$. Zu zeigen ist $B \to C \in \Gamma_\alpha$. Nach (a) genügt $\neg(B \to C) \notin \Gamma_\alpha$. Nehmen wir also an, daß $\neg(B \to C) \in \Gamma_\alpha$. Nach (d) gilt dann $B \in \Gamma_\alpha$ und $\neg C \in \Gamma_\alpha$, also nach (a) $C \notin \Gamma_\alpha$. Nach IH folgt $\mathcal{M} \models B$ und $\mathcal{M} \not\models C$ im Widerspruch zur Voraussetzung $\mathcal{M} \models B \to C$.

$\Longleftarrow$. Gelte $B \to C \in \Gamma_\alpha$. Zu zeigen ist $\mathcal{M} \models B \to C$. Sei also $\mathcal{M} \models B$. Zu zeigen ist $\mathcal{M} \models C$. Nach IH haben wir $B \in \Gamma_\alpha$, also nach (e) und (a) $C \in \Gamma_\alpha$, also nach IH $\mathcal{M} \models C$.

*Fall* $\forall x\, B$. $\Longrightarrow$. Gelte $\mathcal{M} \models \forall x\, B$. Zu zeigen ist $\forall x\, B \in \Gamma_\alpha$. Nach (a) genügt $\neg\forall x\, B \notin \Gamma_\alpha$. Nehmen wir also an, daß $\neg\forall x\, B \in \Gamma_\alpha$. Nach (f) ist dann $\neg B[y/x] \in \Gamma_\alpha$ für ein $y$, also nach (a) und der IH $\mathcal{M} \not\models B[y/x][\mathrm{id}]$, also nach dem Substitutionslemma 4.2 $\mathcal{M} \not\models B[\mathrm{id}^y_x]$ im Widerspruch zur Annahme $\mathcal{M} \models \forall x\, B[\mathrm{id}]$.

$\Longleftarrow$. Sei $\forall x\, B \in \Gamma_\alpha$. Zu zeigen ist $\mathcal{M} \models \forall x\, B[\mathrm{id}]$. Sei also $t \in \mathrm{Ter}_\mathcal{L}$ beliebig. Zu zeigen ist $\mathcal{M} \models B[\mathrm{id}^t_x]$, also $\mathcal{M} \models B[t/x][\mathrm{id}]$ nach dem Substitutionslemma 4.2. Aus (g) folgt aber $B[t/x] \in \Gamma_\alpha$, also nach der IH für $B[t/x]$ auch $\mathcal{M} \models B[t/x][\mathrm{id}]$.

Jetzt können wir den Beweis des Vollständigkeitssatzes abschließen. Wegen (c) ist $A \notin \Gamma_\alpha$ und $S \subseteq \Gamma_\alpha$, also $\mathcal{M} \not\models A[\mathrm{id}]$ und $\mathcal{M} \models B[\mathrm{id}]$ für alle $B \in S$, d.h. $\mathcal{M}$ und id bilden ein Gegenbeispiel zur Voraussetzung $S \models A$ des Vollständigkeitssatzes. $\square$

Der Vollständigkeitssatz gilt ebenfalls für überabzählbare Sprachen $\mathcal{L}$; ein Beweis dafür wird später gegeben, wenn wir das dafür benötigte Zornsche Lemma behandelt haben.

Wir notieren noch einige einfache, aber wichtige Folgerungen aus dem Vollständigkeitssatz bzw. aus seinem Beweis. Eine Menge $S$ von $\mathcal{L}$–Formeln heißt *konsistent*, wenn $S \nvdash \bot$; $S$ heißt *erfüllbar*, wenn es eine $\mathcal{L}$–Struktur $\mathcal{M}$ und eine Umgebung $U$ in $|\mathcal{M}|$ gibt mit $\mathcal{M} \models B[U]$ für alle $B \in S$.

**Satz 7.4 (Erfüllbarkeitssatz).** *Jede konsistente Menge von $\mathcal{L}$–Formeln ist erfüllbar.*

*Beweis.* Aus $S \nvdash \bot$ folgt $S \not\models \bot$ nach dem Vollständigkeitssatz. Wäre nun $S$ nicht erfüllbar, so würde $S \models \bot$ gelten. □

**Satz 7.5 (Kompaktheitssatz).** *Sei $S$ eine Menge von $\mathcal{L}$–Formeln. Ist jede endliche Teilmenge von $S$ erfüllbar, so auch $S$ selbst.*

*Beweis.* Andernfalls gilt $S \models \bot$, also nach dem Vollständigkeitssatz $S \vdash \bot$, also auch $S_0 \vdash \bot$ für eine endliche Teilmenge $S_0 \subseteq S$, also $S_0 \models \bot$ im Widerspruch zu Voraussetzung, daß $S_0$ ein Modell besitzt. □

**Satz 7.6 (Löwenheim, Skolem).** *Sei $\mathcal{L}$ abzählbar und $S$ eine Menge von $\mathcal{L}$–Formeln. Wenn $S$ erfüllbar ist, so auch durch eine $\mathcal{L}$–Struktur mit der abzählbaren Trägermenge* $\mathrm{Ter}_{\mathcal{L}}$.

*Beweis.* Wir verwenden den Beweis des Vollständigkeitssatzes mit $A = \bot$. Er liefert entweder $S \vdash \bot$ oder ein Modell von $S \cup \{\neg\bot\}$, dessen Trägermenge $\mathrm{Ter}_{\mathcal{L}}$ ist. $S \vdash \bot$ kann aber aufgrund der Voraussetzung nicht gelten. □

*Bemerkung.* Man zeigt leicht: a. $\vdash \neg(B \to C) \to B \wedge \neg C$,

b. $\vdash (\neg B \to A) \wedge (C \to A) \to ((B \to C) \to A)$,

c. $\vdash (\forall x\, B \to A) \to \forall y(\neg\forall x\, B \to \neg B[y/x] \to A) \to A$ für $y \notin \mathrm{FV}(B) \cup \mathrm{FV}(A)$.

# 1.8 Anfänge der Modelltheorie

In diesem Abschnitt wollen wir wie in der Modelltheorie üblich auch überabzählbare Sprachen $\mathcal{L}$ zulassen. Wie bereits erwähnt, gilt der Vollständigkeitssatz und seine in 1.7 angagabenen Folgerungen ebenfalls für überabzählbare Sprachen; ein Beweis dafür wird später gegeben, wenn wir das dafür benötigte Zornsche Lemma behandelt haben.

Für jede Formelmenge $S$ sei $L(S)$ die Menge aller in $S$ vorkommenden Funktions– und Relationssymbole. Ist $\mathcal{L}$ eine Teilsprache von $\mathcal{L}'$, $\mathcal{M}$ eine $\mathcal{L}$–Struktur und $\mathcal{M}'$ eine $\mathcal{L}'$–Struktur, so nennt man $\mathcal{M}'$ eine *Expansion* von $\mathcal{M}$ (und $\mathcal{M}$ ein *Redukt* von $\mathcal{M}'$), wenn

$$\begin{aligned} &|\mathcal{M}| = |\mathcal{M}'|, \\ &f^{\mathcal{M}} = f^{\mathcal{M}'} \quad \text{für alle } f \in \mathrm{Fun}_{\mathcal{L}}, \\ &R^{\mathcal{M}} = R^{\mathcal{M}'} \quad \text{für alle } R \in \mathrm{Rel}_{\mathcal{L}}. \end{aligned}$$

Das (eindeutig bestimmte) $\mathcal{L}$–Redukt von $\mathcal{M}'$ wird mit $\mathcal{M}'\restriction\mathcal{L}$ bezeichnet. Ist $\mathcal{M}'$ eine Expansion von $\mathcal{M}$ und $U$ eine Umgebung in $|\mathcal{M}|$, so gilt offenbar $t^{\mathcal{M}}[U] = t^{\mathcal{M}'}[U]$ für jeden $\mathcal{L}$–Term $t$ und $\mathcal{M} \models A[U]$ genau dann, wenn $\mathcal{M}' \models A[U]$ für jede $\mathcal{L}$–Formel $A$. Die Gültigkeit von $S \models A$ hängt deshalb nicht von der zugrunde gelegten Sprache $\mathcal{L}$ ab, solange nur $L(S \cup \{A\}) \subseteq \mathcal{L}$ (genauer $\subseteq \mathrm{Fun}_{\mathcal{L}} \cup \mathrm{Rel}_{\mathcal{L}}$) ist. Wegen des Vollständigkeitssatzes $S \models A \iff S \vdash A$ gilt dasselbe auch für $S \vdash A$.

Wir wollen uns jetzt mit den *Gleichheitsaxiomen* befassen. Wir setzen deshalb in diesem Kapitel voraus, daß die Sprache $\mathcal{L}$ stets ein zweistelliges Relationssymbol $=$ enthält. Die Menge $\mathrm{Eq}_{\mathcal{L}}$ der $\mathcal{L}$–Gleichheitsaxiome besteht dann aus den Allabschlüssen von

$$\begin{aligned} &x = x \qquad \text{(Reflexivität)}, \\ &x = y \to y = x \qquad \text{(Symmetrie)}, \\ &x = y \wedge y = z \to x = z \qquad \text{(Transitivität)}, \\ &x_1 = y_1 \wedge \ldots \wedge x_n = y_n \to f x_1 \ldots x_n = f y_1 \ldots y_n \quad \text{für alle } f \in \mathrm{Fun}_{\mathcal{L}}^{(n)}, \\ &x_1 = y_1 \wedge \ldots \wedge x_n = y_n \wedge R x_1 \ldots x_n \to R y_1 \ldots y_n \quad \text{für alle } R \in \mathrm{Rel}_{\mathcal{L}}^{(n)}. \end{aligned}$$

**Lemma 8.1 (Gleichheitslemma).** *a.* $\mathrm{Eq}_{\mathcal{L}} \vdash t = s \to r[t] = r[s]$.

*b.* $\mathrm{Eq}_{\mathcal{L}} \vdash t = s \wedge A[t] \to A[s]$.

*Beweis.* a. Induktion über $r$. b. Induktion über die Anzahl der logischen Zeichen in $A$. Wir beschränken uns auf den Fall $\forall z\, A$ und führen den Beweis informal. Gelte also $t_1 = t_2$ und $(\forall z\, A)[t_1/x]$. Zu zeigen ist $(\forall z\, A)[t_2/x]$. OBdA sei $x \in \mathrm{FV}(\forall z\, A)$. Wähle ein $y$ mit $y \notin \mathrm{FV}(A) \cup \mathrm{BV}(A)$, $y \neq x$ und $y \notin \mathrm{vars}(t_1) \cup \mathrm{vars}(t_2)$. Dann ist nach Lemma 5.5

$$\vdash_m \forall z\, A \leftrightarrow \forall y\, A[y/z],$$

also auch

$$\vdash_m (\forall z\, A)[t_i/x] \leftrightarrow (\forall y\, A[y/z])[t_i/x],$$

also nach Definition der Substitution auch

$$\vdash_m (\forall z\, A)[t_i/x] \leftrightarrow \forall y\, (A[y/z])[t_i/x].$$

Man verwende jetzt die IH für $A[y/z]$. □

Eine $\mathcal{L}$–Struktur $\mathcal{M}$ erfüllt die Gleichheitsaxiome genau dann, wenn $=^{\mathcal{M}}$ eine Kongruenzrelation ist (also eine Äquivalenzrelation, die mit den Funktionen und Relationen von $\mathcal{M}$ verträglich ist). In diesem Kapitel setzen wir voraus, daß alle betrachteten $\mathcal{L}$–Strukturen $\mathcal{M}$ die Gleichheitsaxiome erfüllen. Man kann dann die *Quotientenstruktur* $\mathcal{M}/{=^{\mathcal{M}}}$ bilden, deren Trägermenge aus den Kongruenzklassen besteht. Wir nennen ein $\mathcal{M}$ *unendlich* (*abzählbar*, *n–elementig*), wenn $\mathcal{M}/{=^{\mathcal{M}}}$ unendlich (abzählbar, $n$–elementig) ist.

Unter einem *Axiomensystem* $S$ verstehen wir eine Menge geschlossener Formeln mit $\mathrm{Eq}_{L(S)} \subseteq S$. Ein *Modell* eines Axiomensystems $S$ ist eine $\mathcal{L}$–Struktur $\mathcal{M}$ mit $L(S) \subseteq \mathcal{L}$ und $\mathcal{M} \models S$. Für Mengen $S$ geschlossener Formeln schreiben wir

$$\mathrm{Mod}_{\mathcal{L}}(S) := \{\, \mathcal{M} \mid \mathcal{M} \text{ ist } \mathcal{L}\text{–Struktur und } \mathcal{M} \models S \cup \mathrm{Eq}_{\mathcal{L}} \,\}.$$

Offenbar ist $S$ genau dann erfüllbar, wenn $S$ ein Modell besitzt.

**Satz 8.2.** *Hat ein Axiomensystem beliebig große endliche Modelle, so hat es auch ein unendliches Modell.*

*Beweis.* Angenommen, $S$ ist ein solches Axiomensystem. Seien $x_0, x_1, x_2, \ldots$ verschiedene Variable und

$$S' := S \cup \{\, x_i \neq x_j \mid i, j \in \mathbb{N} \text{ mit } i < j \,\}.$$

Nach Annahme ist jede endliche Teilmenge von $S'$ erfüllbar, also nach dem Kompaktheitssatz 7.5 auch $S'$. Wir haben also $\mathcal{M}$ und $U$ mit $\mathcal{M} \models S'[U]$ und damit $U(x_i) \neq^{\mathcal{M}} U(x_j)$ für $i < j$. Also ist $\mathcal{M}$ unendlich. □

Mit $\overline{\mathcal{L}}$ bezeichnen wir die Menge aller geschlossenen $\mathcal{L}$–Formeln. Unter einer *Theorie* $T$ verstehen wir ein gegen $\vdash$ abgeschlossenes Axiomensystem, also $\mathrm{Eq}_{L(T)} \subseteq T$ und

$$T = \{\, A \in \overline{L(T)} \mid T \vdash A \,\}.$$

Eine Theorie $T$ heißt *vollständig*, wenn für jede Formel $A \in \overline{L(T)}$ gilt $T \vdash A$ oder $T \vdash \neg A$. Für jede $\mathcal{L}$–Struktur $\mathcal{M}$ (die die Gleichheitsaxiome erfüllt) bildet die Menge aller geschlossenen $\mathcal{L}$-Formeln $A$ mit $\mathcal{M} \models A$ offenbar eine Theorie; sie heißt die *Theorie von* $\mathcal{M}$ und wird mit $\mathrm{Th}(\mathcal{M})$ bezeichnet. Zwei $\mathcal{L}$–Strukturen $\mathcal{M}$ und $\mathcal{M}'$ heißen *elementar äquivalent* (geschrieben $\mathcal{M} \equiv \mathcal{M}'$), wenn $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{M}')$ ist. Zwei $\mathcal{L}$–Strukturen $\mathcal{M}$ und $\mathcal{M}'$ heißen *isomorph* (geschrieben $\mathcal{M} \cong \mathcal{M}'$), wenn es eine Abbildung $\pi\colon |\mathcal{M}| \to |\mathcal{M}'|$ gibt, die eine Bijektion zwischen $|\mathcal{M}/{=^{\mathcal{M}}}|$ und $|\mathcal{M}'/{=^{\mathcal{M}'}}|$ induziert, also

$$(\forall a, b \in |\mathcal{M}|)(a =^{\mathcal{M}} b \iff \pi(a) =^{\mathcal{M}'} \pi(b)),$$
$$(\forall a' \in |\mathcal{M}'|)(\exists a \in |\mathcal{M}|)(\pi(a) =^{\mathcal{M}'} a'),$$

so daß für alle $a_1, \ldots, a_n \in |\mathcal{M}|$ gilt

$$\begin{aligned} \pi(f^{\mathcal{M}}(a_1, \ldots, a_n)) &=^{\mathcal{M}'} f^{\mathcal{M}'}(\pi(a_1), \ldots, \pi(a_n)) \qquad \text{für alle } f \in \mathrm{Fun}_{\mathcal{L}}^{(n)}, \\ R^{\mathcal{M}}(a_1, \ldots, a_n) &\iff R^{\mathcal{M}'}(\pi(a_1), \ldots, \pi(a_n)) \qquad \text{für alle } R \in \mathrm{Rel}_{\mathcal{L}}^{(n)}. \end{aligned}$$

Unmittelbar durch Induktion über $t$ bzw. $A$ zeigt man:

**Lemma 8.3.** *Seien $U, V$ Umgebungen in $|\mathcal{M}|$ mit $\mathrm{dom}(U) = \mathrm{dom}(V)$ und $U(x) =^{\mathcal{M}} V(x)$ für alle $x \in \mathrm{dom}(U)$. Dann gilt*

a. $t^{\mathcal{M}}[U] =^{\mathcal{M}} t^{\mathcal{M}}[V]$ *falls* $\mathrm{vars}(t) \subseteq \mathrm{dom}(U)$ *und*

b. $\mathcal{M} \models A[U] \iff \mathcal{M} \models A[V]$ *falls* $\mathrm{FV}(A) \subseteq \mathrm{dom}(U)$. □

**Lemma 8.4.** a. $\mathrm{Th}(\mathcal{M})$ *ist vollständig.*

b. *Ist $S$ ein Axiomensystem mit $L(S) \subseteq \mathcal{L}$, so ist*

$$\{\, A \in \overline{\mathcal{L}} \mid S \vdash A \,\} = \bigcap \{\, \mathrm{Th}(\mathcal{M}) \mid \mathcal{M} \in \mathrm{Mod}_{\mathcal{L}}(S) \,\}.$$

c. $\mathcal{M} \equiv \mathcal{M}' \iff \mathcal{M} \models \mathrm{Th}(\mathcal{M}')$.

d. *Ist $\mathcal{L}$ abzählbar, so existiert zu jeder $\mathcal{L}$–Struktur $\mathcal{M}$ eine abzählbare $\mathcal{L}$–Struktur $\mathcal{M}'$ mit $\mathcal{M} \equiv \mathcal{M}'$.*

*Beweis.* a. Sei $\mathcal{M}$ eine $\mathcal{L}$–Struktur und $A \in \overline{\mathcal{L}}$. Dann gilt $\mathcal{M} \models A$ oder $\mathcal{M} \models \neg A$, also $\mathrm{Th}(\mathcal{M}) \vdash A$ oder $\mathrm{Th}(\mathcal{M}) \vdash \neg A$.

b. Für alle $A \in \overline{\mathcal{L}}$ hat man

$$\begin{aligned} S \vdash A &\iff S \models A \\ &\iff \text{für alle } \mathcal{L}\text{–Strukturen } \mathcal{M} \text{ gilt } (\mathcal{M} \models S \implies \mathcal{M} \models A) \\ &\iff \text{für alle } \mathcal{L}\text{–Strukturen } \mathcal{M} \text{ gilt } (\mathcal{M} \in \mathrm{Mod}_{\mathcal{L}}(S) \implies A \in \mathrm{Th}(\mathcal{M})) \\ &\iff A \in \bigcap \{\, \mathrm{Th}(\mathcal{M}) \mid \mathcal{M} \in \mathrm{Mod}_{\mathcal{L}}(S) \,\}. \end{aligned}$$

c. $\Longrightarrow$. Gelte $\mathcal{M} \equiv \mathcal{M}'$ und $A \in \mathrm{Th}(\mathcal{M}')$. Dann folgt $\mathcal{M}' \models A$, also $\mathcal{M} \models A$.

$\Longleftarrow$. Gelte $\mathcal{M} \models \mathrm{Th}(\mathcal{M}')$. Offenbar ist dann $\mathrm{Th}(\mathcal{M}') \subseteq \mathrm{Th}(\mathcal{M})$. Zum Beweis der umgekehrten Inklusion sei $A \in \mathrm{Th}(\mathcal{M})$. Wäre $A \notin \mathrm{Th}(\mathcal{M}')$, so hätte man nach a auch $\neg A \in \mathrm{Th}(\mathcal{M}')$, also $\mathcal{M} \models \neg A$ im Widerspruch zu $A \in \mathrm{Th}(\mathcal{M})$.

d. Sei $\mathcal{L}$ abzählbar und $\mathcal{M}$ eine $\mathcal{L}$–Struktur. Dann ist $\mathrm{Th}(\mathcal{M})$ erfüllbar, besitzt also nach dem Satz 7.6 von Löwenheim und Skolem auch eine erfüllende $\mathcal{L}$–Struktur $\mathcal{M}'$ mit der abzählbaren Trägermenge $\mathrm{Ter}_{\mathcal{L}}$. Nach c ist $\mathcal{M} \equiv \mathcal{M}'$. □

**Satz 8.5.** *Es sei $T$ eine Theorie und $\mathcal{L} = L(T)$. Dann sind folgende Aussagen äquivalent.*

a. *$T$ ist vollständig.*

b. *Für jedes Modell $\mathcal{M} \in \mathrm{Mod}_{\mathcal{L}}(T)$ gilt $\mathrm{Th}(\mathcal{M}) = T$.*

c. *Je zwei Modelle $\mathcal{M}, \mathcal{M}' \in \mathrm{Mod}_{\mathcal{L}}(T)$ sind elementar äquivalent.*

*Beweis.* a $\Longrightarrow$ b. Sei $T$ vollständig und $\mathcal{M} \in \mathrm{Mod}_{\mathcal{L}}(T)$. Dann gilt $\mathcal{M} \models T$, also $T \subseteq \mathrm{Th}(\mathcal{M})$. Sei nun umgekehrt $A \in \mathrm{Th}(\mathcal{M})$. Dann folgt $\neg A \notin \mathrm{Th}(\mathcal{M})$, also $\neg A \notin T$ und damit $A \in T$.

b $\Longrightarrow$ c ist klar.

c $\Longrightarrow$ a. Sei $A \in \overline{\mathcal{L}}$ und $T \not\vdash A$. Dann existiert ein Modell $\mathcal{M}_0$ von $T \cup \{\neg A\}$. Sei nun $\mathcal{M} \in \mathrm{Mod}_{\mathcal{L}}(T)$ beliebig. Nach c ist $\mathcal{M} \equiv \mathcal{M}_0$, also $\mathcal{M} \models \neg A$. Damit haben wir $T \vdash \neg A$.□

**Satz 8.6.** *Ist $\pi$ ein Isomorphismus von $\mathcal{M}$ auf $\mathcal{M}'$, so gilt für alle Terme $t$ und Formeln $A$ und für jede genügend große Umgebung $U$ in $|\mathcal{M}|$*

a. *$\pi(t^{\mathcal{M}}[U]) =^{\mathcal{M}'} t^{\mathcal{M}'}[\pi \circ U]$ und*

b. *$\mathcal{M} \models A[U] \iff \mathcal{M}' \models A[\pi \circ U]$.*

*Insbesondere hat man also $\mathcal{M} \cong \mathcal{M}' \implies \mathcal{M} \equiv \mathcal{M}'$.*

*Beweis.* a. Induktion über $t$. Zur Vereinfachung der Schreibweise behandeln wir nur den Fall einstelliger Funktionssymbole.

$\pi(x^{\mathcal{M}}[U]) = \pi(U(x)) = x^{\mathcal{M}'}[\pi \circ U]$

$\pi(c^{\mathcal{M}}[U]) = \pi(c^{\mathcal{M}}) =^{\mathcal{M}'} c^{\mathcal{M}'}$

$\pi(f(t)^{\mathcal{M}}[U]) = \pi(f^{\mathcal{M}}(t^{\mathcal{M}}[U])) =^{\mathcal{M}'} f^{\mathcal{M}'}(\pi(t^{\mathcal{M}}[U])) =^{\mathcal{M}'} f^{\mathcal{M}'}(t^{\mathcal{M}'}[\pi \circ U]) = f(t)^{\mathcal{M}'}[\pi \circ U]$

b. Induktion über $A$. Wir behandeln nur den Fall einstelliger Relationssymbole und den Fall $\forall x\, A$.

$$\begin{aligned}
\mathcal{M} \models R(t)[U] &\iff R^{\mathcal{M}}(t^{\mathcal{M}}[U]) \\
&\iff R^{\mathcal{M}'}(\pi(t^{\mathcal{M}}[U])) \\
&\iff R^{\mathcal{M}'}(t^{\mathcal{M}'}[\pi \circ U]) \\
&\iff \mathcal{M}' \models R(t)[\pi \circ U],
\end{aligned}$$

$$\begin{aligned}
\mathcal{M} \models \forall x\, A[U] &\iff \text{für alle } a \in |\mathcal{M}| \text{ gilt } \mathcal{M} \models A[U^a_x] \\
&\iff \text{für alle } a \in |\mathcal{M}| \text{ gilt } \mathcal{M}' \models A[\pi \circ U^a_x] \\
&\iff \text{für alle } a \in |\mathcal{M}| \text{ gilt } \mathcal{M}' \models A[(\pi \circ U)^{\pi(a)}_x] \\
&\iff \text{für alle } a' \in |\mathcal{M}'| \text{ gilt } \mathcal{M}' \models A[(\pi \circ U)^{a'}_x] \quad \text{nach 8.3} \\
&\iff \mathcal{M}' \models \forall x\, A[\pi \circ U] \qquad \square.
\end{aligned}$$

**Satz 8.7.** *Zu jeder unendlichen Struktur $\mathcal{M}$ gibt es eine elementar äquivalente Struktur $\mathcal{M}_0$, die nicht isomorph zu $\mathcal{M}$ ist.*

*Beweis.* OBdA sei $=^{\mathcal{M}}$ die Gleichheit auf $M := |\mathcal{M}|$. Mit $\mathcal{P}(M)$ bezeichnen wir die Potenzmenge von $M$. Zu jedem $\alpha \in \mathcal{P}(M)$ wählen wir eine neue Konstante $c_\alpha$. In der Sprache $\mathcal{L}' := \mathcal{L} \cup \{ c_\alpha \mid \alpha \in \mathcal{P}(M) \}$ betrachten wir das Axiomensystem

$$S := \mathrm{Th}(\mathcal{M}) \cup \{ c_\alpha \neq c_\beta \mid \alpha, \beta \in \mathcal{P}(M) \text{ und } \alpha \neq \beta \} \cup \mathrm{Eq}_{\mathcal{L}'}.$$

Jede endliche Teilmenge von $S$ ist erfüllbar durch eine geeignete Expansion von $\mathcal{M}$. Also ist nach dem Kompaktheitssatz 7.5 auch $S$ erfüllbar, etwa durch $\mathcal{M}_0'$. Sei $\mathcal{M}_0 := M_0' \restriction \mathcal{L}$. OBdA sei $=^{\mathcal{M}_0}$ die Gleichheit auf $|\mathcal{M}_0|$. $\mathcal{M}_0$ ist nicht isomorph zu $\mathcal{M}$, denn andernfalls hätte man eine Injektion von $\mathcal{P}(M)$ in $M$ und damit einen Widerspruch. □

*Bemerkung.* Nach Satz 8.7 ist es nicht möglich, eine unendliche Struktur durch ein Axiomensystem erster Stufe bis auf Isomorphie zu charakterisieren. Verläßt man jedoch die Logik erster Stufe und erlaubt auch die Quantifikation über Mengen $X$, so kann man etwa die folgenden *Peano–Axiome* anschreiben:

$$\begin{aligned}
&\forall n(Sn \neq 0),\\
&\forall n \forall m(Sn = Sm \to n = m),\\
&\forall X(0 \in X \wedge \forall n(n \in X \to Sn \in X) \to \forall n(n \in X)).
\end{aligned}$$

Man kann zeigen, daß $(\mathbb{N}, 0, S)$ bis auf Isomorphie das einzige Modell der Peano–Axiome ist. Eine Struktur, die elementar äquivalent, aber nicht isomorph zu $\mathcal{N} := (\mathbb{N}, 0, S)$ ist, heißt ein *Nichtstandardmodell* der natürlichen Zahlen. In jedem Nichtstandardmodell der natürlichen Zahlen gilt das Prinzip der vollständigen Induktion nicht für alle Mengen $X \subseteq \mathbb{N}$. Entsprechend heißt eine Struktur, die elementar äquivalent, aber nicht isomorph zu $(\mathbb{R}, 0, 1, +, \cdot, <)$ ist, ein Nichtstandardmodell der reellen Zahlen. In jedem Nichtstandardmodell der reellen Zahlen gilt das Vollständigkeitsaxiom

$$\forall X(\emptyset \neq X \text{ beschränkt} \to \exists y(y = \sup(X)))$$

nicht für alle Mengen $X \subseteq \mathbb{R}$.

**Satz 8.8.** *Es gibt abzählbare Nichtstandardmodelle der natürlichen Zahlen.*

*Beweis.* Sei

$$S := \mathrm{Th}(\mathcal{N}) \cup \{ x \neq \underline{n} \mid n \in \mathbb{N} \},$$

wobei $\underline{0} := 0$ und $\underline{n+1} := S\underline{n}$. Offenbar ist jede endliche Teilmenge von $S$ erfüllbar, also nach dem Kompaktheitssatz 7.5 auch $S$. Nach dem Satz 7.6 von Löwenheim und Skolem haben wir dann ein höchstens abzählbares $\mathcal{M}$ und eine Umgebung $U$ mit $\mathcal{M} \models S[U]$. Wegen $\mathcal{M} \models \mathrm{Th}(\mathcal{N})$ ist $\mathcal{M} \equiv \mathcal{N}$; daraus folgt insbesondere, daß $\mathcal{M}$ abzählbar ist. Weiter ist $U(x) \neq^{\mathcal{M}} \underline{n}^{\mathcal{M}}$ für alle $n \in \mathbb{N}$, also $\mathcal{M} \not\cong \mathcal{N}$. □

Wir wollen jetzt einige Anwendungen auf aus der Mathematik bekannte Axiomensysteme diskutieren.

Die Axiome der *Körpertheorie* sind (außer den Gleichheitsaxiomen) die Allabschlüsse von

$$\begin{aligned}
&x + (y + z) = (x + y) + z,\\
&0 + x = x,\\
&(-x) + x = 0,\\
&x + y = y + x,\\
&x \cdot (y \cdot z) = (x \cdot y) \cdot z,\\
&1 \cdot x = x,\\
&x \neq 0 \to x^{-1} \cdot x = 1,\\
&x \cdot y = y \cdot x,\\
&(x + y) \cdot z = (x \cdot z) + (y \cdot z),\\
&1 \neq 0.
\end{aligned}$$

*Körper* sind also genau die Modelle dieses Axiomensystems.

In der Theorie der *geordneten Körper* hat man zusätzlich ein zweistelliges Relationssymbol $<$ und als Axiome die Allabschlüsse von

$$\begin{aligned}
&x \not< x,\\
&x < y \wedge y < z \to x < z,\\
&x < y \vee x = y \vee y < x,\\
&x < y \to x + z < y + z,\\
&0 < x \wedge 0 < y \to 0 < x \cdot y.
\end{aligned}$$

*Geordnete Körper* sind genau die Modelle dieses erweiterten Axiomensystems. Ein geordneter Körper heißt *archimedisch geordnet*, wenn es zu jedem Körperelement $a$ eine natürliche Zahl $n$ gibt, so daß $a$ kleiner ist als das $n$–fache der Eins im Körper.

**Satz 8.9.** *Zu jedem archimedisch geordneten Körper gibt es einen elementar äquivalenten geordneten Körper, der nicht archimedisch geordnet ist.*

*Beweis.* Sei $\mathcal{K}$ ein archimedisch geordneter Körper, $x$ eine Variable und

$$S := \mathrm{Th}(\mathcal{K}) \cup \{\, \underline{n} < x \mid n \in \mathbb{N} \,\}.$$

Offenbar ist jede endliche Teilmenge von $S$ erfüllbar, also nach dem Kompaktheitssatz 7.5 auch $S$. Wir haben also $\mathcal{M}$ und $U$ mit $\mathcal{M} \models S[U]$. Wegen $\mathcal{M} \models \mathrm{Th}(\mathcal{K})$ ist $\mathcal{M} \equiv \mathcal{K}$ und damit $\mathcal{M}$ ein geordneter Körper. Weiter ist $1^{\mathcal{M}} \cdot n <^{\mathcal{M}} U(x)$ für alle $n \in \mathbb{N}$, also $\mathcal{M}$ nicht archimedisch geordnet. □

Eine Klasse $\mathcal{S}$ von $\mathcal{L}$–Strukturen heißt (*endlich*) *axiomatisierbar*, wenn es ein (endliches) Axiomensystem $S$ gibt mit $\mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(S)$. Offenbar ist $\mathcal{S}$ endlich axiomatisierbar genau dann, wenn $\mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(\{A\})$ für ein $A$. Gibt es zu jedem $\mathcal{M} \in \mathcal{S}$ ein elementar äquivalentes $\mathcal{M}' \notin \mathcal{S}$, so kann $\mathcal{S}$ offensichtlich nicht axiomatisierbar sein. Aus Satz 8.9 folgt also, daß die Klasse der archimedisch geordneten Körper nicht axiomatisierbar ist. Ebenso folgt, daß die Klasse der geordneten Körper, die nicht archimedisch geordnet sind, nicht axiomatisierbar ist.

**Lemma 8.10.** *Sei $\mathcal{S}$ eine Klasse von $\mathcal{L}$–Strukturen und $S$ ein Axiomensystem.*

a. *$\mathcal{S}$ ist endlich axiomatisierbar genau dann, wenn $\mathcal{S}$ und das Komplement von $\mathcal{S}$ axiomatisierbar sind.*

b. *Ist $\mathrm{Mod}_{\mathcal{L}}(S)$ endlich axiomatisierbar, so gibt es ein endliches $S_0 \subseteq S$ mit $\mathrm{Mod}_{\mathcal{L}}(S_0) = \mathrm{Mod}_{\mathcal{L}}(S)$.*

*Beweis.* a. Mit $1 - \mathcal{S}$ bezeichnen wir das Komplement von $\mathcal{S}$. $\Longrightarrow$. Sei $\mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(\{A\})$. Dann gilt $\mathcal{M} \in 1 - \mathcal{S} \iff \mathcal{M} \models \neg A$, also $1 - \mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(\{\neg A\})$. $\Longleftarrow$. Sei $\mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(S_1)$ und $1 - \mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(S_2)$. Dann ist $S_1 \cup S_2$ nicht erfüllbar, es gibt also ein endliches $S \subseteq S_1$ so daß $S \cup S_2$ nicht erfüllbar ist. Man erhält

$$\mathcal{M} \in \mathcal{S} \implies \mathcal{M} \models S \implies \mathcal{M} \not\models S_2 \implies \mathcal{M} \notin 1 - \mathcal{S} \implies \mathcal{M} \in \mathcal{S},$$

also $\mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(S)$.

b. Sei $\mathrm{Mod}_{\mathcal{L}}(S) = \mathrm{Mod}_{\mathcal{L}}(\{A\})$. Dann gilt $S \models A$, also auch $S_0 \models A$ für ein endliches $S_0 \subseteq S$. Man erhält

$$\mathcal{M} \models S \implies \mathcal{M} \models S_0 \implies \mathcal{M} \models A \implies \mathcal{M} \models S,$$

also $\mathrm{Mod}_{\mathcal{L}}(S_0) = \mathrm{Mod}_{\mathcal{L}}(S)$. □

Zum Abschluß dieses Kapitels behandeln wir als Beispiel einer vollständigen Theorie noch die Theorie *DO* der dichten linearen Ordnungen ohne Endpunkte. Die Axiome der Theorie *DO* sind (außer den Gleichheitsaxiomen) die Allabschlüsse von

$$\begin{aligned}
&x \not< x,\\
&x < y \wedge y < z \to x < z,\\
&x < y \vee x = y \vee y < x,\\
&x < y \to \exists z\,(x < z \wedge z < y),\\
&\exists y\,(x < y),\\
&\exists y\,(y < x).
\end{aligned}$$

**Lemma 8.11.** *Jedes abzählbare Modell von DO ist isomorph zur Struktur $(\mathbb{Q}, <)$ der rationalen Zahlen.*

*Beweis.* Sei $\mathcal{M} = (M, \prec)$ ein abzählbares Modell von *DO*; wir können annehmen, daß $=^{\mathcal{M}}$ die Gleichheit auf $M$ ist. Sei $M = \{\, b_n \mid n \in \mathbb{N} \,\}$ und $\mathbb{Q} = \{\, a_n \mid n \in \mathbb{N} \,\}$, wobei wir

$a_n \neq a_m$ und $b_n \neq b_m$ für $n < m$ annehmen können. Wir definieren rekursiv Funktionen $f_n \subseteq \mathbb{Q} \times M$ wie folgt. Sei $f_0 := \{(a_0, b_0)\}$. Angenommen, wir haben $f_n$ schon konstruiert.

*Fall* $n + 1 = 2m$. Sei $j$ minimal so daß $b_j \notin \mathrm{ran}(f_n)$. Wähle $a_i \notin \mathrm{dom}(f_n)$ so daß für alle $a \in \mathrm{dom}(f_n)$ gilt $a_i < a \leftrightarrow b_j < f_n(a)$; ein solches $a_i$ existiert, da $\mathcal{M}$ und $(\mathbb{Q}, <)$ Modelle von $DO$ sind. Setze $f_{n+1} := f_n \cup \{(a_i, b_j)\}$.

Den *Fall* $n + 1 = 2m + 1$ behandelt man ähnlich. Sei $i$ minimal so daß $a_i \notin \mathrm{dom}(f_n)$. Wähle $b_j \notin \mathrm{ran}(f_n)$ so daß für alle $a \in \mathrm{dom}(f_n)$ gilt $a_i < a \leftrightarrow b_j < f_n(a)$; ein solches $b_j$ existiert, da $\mathcal{M}$ und $(\mathbb{Q}, <)$ Modelle von $DO$ sind. Setze $f_{n+1} := f_n \cup \{(a_i, b_j)\}$.

Nach Konstruktion ist $\{b_0, \ldots, b_m\} \subseteq \mathrm{ran}(f_{2m})$ und $\{a_0, \ldots, a_{m+1}\} \subseteq \mathrm{dom}(f_{2m+1})$ und schließlich $f := \bigcup_n f_n$ ein Isomorphismus von $(\mathbb{Q}, <)$ auf $\mathcal{M}$. □

**Satz 8.12.** *Die Theorie $DO$ ist vollständig, und es gilt $DO = \mathrm{Th}(\mathbb{Q}, <)$.*

*Beweis.* Da offenbar $(\mathbb{Q}, <)$ Modell von $DO$ ist, gengt es nach Satz 8.5 zu zeigen, daß für jedes Modell $\mathcal{M}$ von $DO$ gilt $\mathcal{M} \equiv (\mathbb{Q}, <)$. Sei also $\mathcal{M}$ Modell von $DO$. Nach Lemma 8.4d existiert ein abzählbares $\mathcal{M}'$ mit $\mathcal{M} \equiv \mathcal{M}'$. Nach dem vorangehenden Satz ist $\mathcal{M}' \cong (\mathbb{Q}, <$ ), also $\mathcal{M} \equiv \mathcal{M}' \equiv (\mathbb{Q}, <)$. □

Ein weiteres Beispiel einer vollständigen Theorie ist die Theorie der algebraisch abgeschlossenen Körper. Hierfür und für viele weitere Gegenstände der Modelltheorie sei verwiesen auf die Literatur; ein gutes und umfassendes Buch über Modelltheorie ist Chang–Keisler[2].

## 1.9 Historische Anmerkungen

Der Gödelsche Vollständigkeitssatz wurde zuerst von Gödel [5] für abzählbare Sprachen, und im allgemeinen Fall von Malzew [10] bewiesen. Der Satz von Löwenheim und Skolem wurde bereits vor dem Vollständigkeitssatz bewiesen von Löwenheim [9] und Skolem [14]. Die Sätze 8.3–8.5 stammen von Robinson [12].

# Teil II: Berechenbarkeit

## 2.1 Primitiv rekursive Funktionen

Wir beschränken uns auf die Diskussion der Berechenbarkeit von Funktionen $F\colon \mathbb{N}^n \to \mathbb{N}$. Eine solche Funktion soll *berechenbar* (im intuitiven Sinn) heißen, wenn es einen Algorithmus gibt, der für jedes Argumentetupel $a_1, \ldots, a_n$ terminiert und den Funktionswert $f(a_1, \ldots, a_n)$ liefert. In diesem Kapitel behandeln wir besonders einfache berechenbare Funktionen, nämlich die von Hilbert eingeführten sogenannten primitiv rekursiven Funktionen, die aus einfachen Ausgangsfunktionen durch Komposition (oder Einsetzung) und primitive Rekursion erzeugt werden können. Obwohl diese Definitionsschemata recht speziell sind, wird sich zeigen, daß nahezu alle in der Mathematik verwendeten zahlentheoretischen Funktionen primitiv rekursiv sind. Insbesondere werden wir in Kapitel 2.3 Terme, Formeln und Herleitungen durch natürliche Zahlen kodieren und zeigen, daß die charakteristischen Funktionen der entsprechenden Mengen von Kodenummern primitiv rekursiv sind.

Wir definieren induktiv für jedes $n \in \mathbb{N}$ eine Menge $\mathrm{PR}^n$ von $n$–stelligen Funktionssymbolen.

1. $0^n \in \mathrm{PR}^n$ $(n \geq 0)$, $\mathrm{suc} \in \mathrm{PR}^1$, $I_i^n \in \mathrm{PR}^n$ $(1 \leq i \leq n)$.
2. Sind $g_1, \ldots, g_m \in \mathrm{PR}^n$, $h \in \mathrm{PR}^m$ und $m, n \geq 1$, so ist $(\circ h g_1 \ldots g_m) \in \mathrm{PR}^n$.
3. Ist $g \in \mathrm{PR}^n$ und $h \in \mathrm{PR}^{n+2}$, so ist $(Rgh) \in \mathrm{PR}^{n+1}$.

Wir setzen $\mathrm{PR} := \bigcup_{n\in\mathbb{N}} \mathrm{PR}^n$ und $0 := 0^0$.

Zu der durch PR gegebenen Sprache definieren wir eine Standardstruktur $\mathcal{N}$ wie folgt. Es ist $|\mathcal{N}| := \mathbb{N}$ und

$$
\begin{aligned}
&(0^n)^{\mathcal{N}}(a_1, \ldots, a_n) := 0,\\
&\mathrm{suc}^{\mathcal{N}}(a) := a + 1,\\
&(I_i^n)^{\mathcal{N}}(a_1, \ldots, a_n) := a_i,\\
&(\circ h g_1 \ldots g_m)^{\mathcal{N}}(\vec{a}) := h^{\mathcal{N}}(g_1^{\mathcal{N}}(\vec{a}), \ldots, g_m^{\mathcal{N}}(\vec{a})),\\
&(Rgh)^{\mathcal{N}}(0, \vec{b}) := g^{\mathcal{N}}(\vec{b}),\\
&(Rgh)^{\mathcal{N}}(a+1, \vec{b}) := h^{\mathcal{N}}(a, (Rgh)^{\mathcal{N}}(a, \vec{b}), \vec{b}).
\end{aligned}
$$

Eine Funktion $F\colon \mathbb{N}^n \to \mathbb{N}$ heißt *primitiv rekursiv*, wenn es ein $f \in \mathrm{PR}^n$ gibt mit $F = f^{\mathcal{N}}$. Eine Relation $R \subseteq \mathbb{N}^n$ heißt primitiv rekursiv, wenn ihre *charakteristische Funktion* $1_R$ primitiv rekursiv ist, wobei

$$
1_R(\vec{a}) := \begin{cases} 1, & \text{falls } \vec{a} \in R;\\ 0, & \text{sonst.} \end{cases}
$$

Wir wollen zunächst zeigen, daß die Menge der primitiv rekursiven Funktionen gegen *explizite Definitionen* abgeschlossen ist. Dazu definieren wir für jeden PR–Term $t$ und verschiedene Variablen $x_1, \ldots, x_n$ mit $\mathrm{vars}(t) \subseteq \{x_1, \ldots, x_n\}$ ein $n$–stelliges Funktionssymbol $\lambda x_1, \ldots, x_n\, t$ wie folgt.

$$\begin{aligned}
&\lambda x_1, \ldots, x_n\, 0 := 0^n,\\
&\lambda x_1, \ldots, x_n\, x_i := I_i^n,\\
&\lambda x_1, \ldots, x_n.ht_1 \ldots t_m := (\circ h g_1 \ldots g_m), \quad \text{wobei } g_i := \lambda x_1, \ldots, x_n\, t_i.
\end{aligned}$$

**Lemma 1.1.** *Für jeden* PR*–Term $t$ und verschiedene Variablen $x_1, \ldots, x_n$ mit* $\mathrm{vars}(t) \subseteq \{x_1, \ldots, x_n\}$ *gilt*

$$(\lambda x_1, \ldots, x_n\, t)^{\mathcal{N}}(a_1, \ldots, a_n) = t^{\mathcal{N}}[a_1, \ldots, a_n/x_1, \ldots, x_n].$$

*Beweis* durch Induktion über $t$. Wir schreiben $t^{\mathcal{N}}[\vec{a}]$ für $t^{\mathcal{N}}[a_1, \ldots, a_n/x_1, \ldots, x_n]$.

$$\begin{aligned}
(\lambda \vec{x}\, 0)^{\mathcal{N}}(\vec{a}) &= (0^n)^{\mathcal{N}}(\vec{a}) = 0 = 0^{\mathcal{N}}[\vec{a}].\\
(\lambda \vec{x}\, x_i)^{\mathcal{N}}(\vec{a}) &= (I_i^n)^{\mathcal{N}}(\vec{a}) = a_i = x_i^{\mathcal{N}}[\vec{a}].
\end{aligned}$$

Sei $t = ht_1 \ldots t_m$ und $g_i := \lambda x_1, \ldots, x_n\, t_i$. Dann ist

$$\begin{aligned}
(\lambda \vec{x}\, t)^{\mathcal{N}}(\vec{a}) &= (\circ h g_1 \ldots g_m)^{\mathcal{N}}(\vec{a})\\
&= h^{\mathcal{N}}(g_1^{\mathcal{N}}(\vec{a}), \ldots, g_m^{\mathcal{N}}(\vec{a}))\\
&= h^{\mathcal{N}}(t_1^{\mathcal{N}}[\vec{a}], \ldots, t_m^{\mathcal{N}}[\vec{a}]) \quad \text{nach IH}\\
&= t^{\mathcal{N}}[\vec{a}].
\end{aligned}$$

□

Wir verwenden $a, b, c, i, j, k, \ell, m, n$ als Mitteilungszeichen für natürliche Zahlen. Ist $f \in \mathrm{PR}^n$, so bezeichnen wir die Funktion $f^{\mathcal{N}}\colon \mathbb{N}^n \to \mathbb{N}$ ebenfalls kurz mit $f$; in diesem Sinn ist $\mathrm{PR}^n$ die Menge der $n$–stelligen und PR die Menge aller primitiv rekursiven Funktionen. PR ist also die kleinste Funktionenmenge, die die *Ausgangsfunktionen* $0^n, I_i^n, \mathrm{suc}$ enthält und abgeschlossen ist gegen *Komposition* (oder *Einsetzung*) $\circ$ und *primitive Rekursion* $R$.

*Beispiele* für primitiv rekursive Funktionen. Setzt man $\tilde{+} := RI_1^1(\lambda x, y, z.\mathrm{suc}(y))$, so ist

$$\begin{aligned}
\tilde{+}(0, b) &= b,\\
\tilde{+}(a+1, b) &= \mathrm{suc}(\tilde{+}(a, b)),
\end{aligned}$$

und setzt man $\tilde{\cdot} := R0^1(\lambda x, y, z.\tilde{+}yz)$, so ist

$$\begin{aligned}
\tilde{\cdot}(0, b) &= 0,\\
\tilde{\cdot}(a+1, b) &= \tilde{+}(\tilde{\cdot}(a, b), b).
\end{aligned}$$

Es gilt also $\tilde{+}(a,b) = a+b$ und $\tilde{\cdot}(a,b) = a \cdot b$; wir schreiben deshalb $+, \cdot$ für $\tilde{+}, \tilde{\cdot}$. Weiter sei $\mathrm{pd} := R0(\lambda x, y\, x)$ und $\dot{-} := RI_1^1(\lambda x, y, z.\mathrm{pd}(y))$. Dann gilt

$$\begin{aligned} &\mathrm{pd}(0) = 0, \\ &\mathrm{pd}(a+1) = a \end{aligned}$$

und

$$\begin{aligned} &b \dot{-} 0 = b, \\ &b \dot{-} (a+1) = \mathrm{pd}(b \dot{-} a), \end{aligned}$$

wobei wir für $\dot{-}$ die übliche Infixschreibweise verwendet haben. Es ist also

$$b \dot{-} a = \begin{cases} 0, & \text{falls } b \leq a; \\ b-a, & \text{sonst.} \end{cases}$$

Für $f \in \mathrm{PR}^{n+1}$ sei $\sum f := R0^n(\lambda x, y, \vec{z}\,(y + f(x, \vec{z})))$, also

$$\begin{aligned} &\left(\sum f\right)(0, \vec{b}) = 0, \\ &\left(\sum f\right)(a+1, \vec{b}) = \left(\sum f\right)(a, \vec{b}) + f(a, \vec{b}). \end{aligned}$$

In Anlehnung an die übliche mathematische Terminologie schreiben wir $\sum_{i<a} f(i, \vec{b})$ für $(\sum f)(a, \vec{b})$. Ähnlich setzen wir $\prod f := R(\circ\mathrm{suc}0^n)\lambda x, y, \vec{z}\,(y \cdot f(x, \vec{z}))$, also $(\prod f)(a, \vec{b}) = \prod_{x<a} f(x, \vec{b})$. Wir schreiben auch $\sum_{i \leq a} f(i, \vec{b})$ für $\sum_{i<\mathrm{suc}(a)} f(i, \vec{b})$ und entsprechend bei Produkten.

Man beachte, daß eine Relation $R \subseteq \mathbb{N}^n$ genau dann primitiv rekursiv ist, wenn es ein $f \in \mathrm{PR}^n$ gibt mit $R = \{\, \vec{a} \in \mathbb{N}^n \mid f(\vec{a}) = 0 \,\}$; zum Beweis beachte man $1_R(\vec{a}) = 1 \dot{-} f(\vec{a})$ bzw. setze $f(\vec{a}) = 1 \dot{-} 1_R(\vec{a})$.

Um neben Termen auch Formeln betrachten zu können, nehmen wir im folgenden an, daß die Sprache PR noch das Gleichheitssymbol $=$ enthält, und daß $=^{\mathcal{N}}$ in der Standardstruktur $\mathcal{N}$ die Gleichheit auf $\mathbb{N}$ ist. Wir schreiben $s < t$ für $\mathrm{suc}(s) \dot{-} t = 0$; offenbar gilt dann

$$\mathcal{N} \models (s < t)[U] \iff s^{\mathcal{N}}[U] < t^{\mathcal{N}}[U].$$

Eine Relation $R \subseteq \mathbb{N}^n$ heißt *definierbar* durch eine Formel $A[x_1, \ldots, x_n]$ der Sprache PR, wenn

$$R = \{\, (a_1, \ldots, a_n) \in \mathbb{N}^n \mid \mathcal{N} \models A[a_1, \ldots, a_n / x_1, \ldots, x_n] \,\}.$$

Offenbar sind genau die primitiv rekursiven Relationen durch atomare PR–Formeln definierbar. Wir wollen jetzt zeigen, daß dasselbe auch für eine reichere Formelmenge der Fall ist, nämlich für die sogenannten $\Delta_0$–Formeln der Sprache PR.

Wir setzen im Fall $x \notin \mathrm{vars}(t)$

$$\begin{aligned} &\forall x < t\, A := \forall x\, (x < t \to A), \\ &\exists x < t\, A := \neg \forall x\, (x < t \to \neg A), \\ &\forall x \leq t\, A := \forall x < \mathrm{suc}(t)\, A, \\ &\exists x \leq t\, A := \exists x < \mathrm{suc}(t)\, A. \end{aligned}$$

Man beachte, daß $\exists x < t\, A$ logisch äquivalent ist zu $\exists x\,(x < t \wedge A)$. $\Delta_0$–*Formeln* werden induktiv definiert durch

- Jede PR–Primformel ist eine $\Delta_0$–Formel; insbesondere ist also $\bot$ eine $\Delta_0$–Formel.
- Sind $A$ und $B$ $\Delta_0$–Formeln, so auch $\neg A$, $A \wedge B$ und $A \vee B$.
- Ist $A$ eine $\Delta_0$–Formel und $t$ ein PR–Term mit $x \notin \mathrm{vars}(t)$, so ist auch $\forall x < t\, A$ eine $\Delta_0$–Formel.

Es folgt, daß mit $A$ im Fall $x \notin \mathrm{vars}(t)$ auch $\exists x < t\, A$ eine $\Delta_0$–Formel ist.

**Lemma 1.2.** *Ist $A$ eine $\Delta_0$–Formel mit $\mathrm{FV}(A) \subseteq \{x_1, \ldots, x_n\}$, so ist die Relation*

$$\{\, (a_1, \ldots, a_n) \in \mathbb{N}^n \mid \mathcal{N} \models A[a_1, \ldots, a_n / x_1, \ldots, x_n] \,\}$$

*primitiv rekursiv.*

*Beweis.* Wir definieren für jede $\Delta_0$–Formel $A$ einen PR–Term $r_A$ mit $\mathrm{vars}(r_A) = \mathrm{FV}(A)$ so daß für jede $\mathcal{N}$–Umgebung $U$ gilt $r_A^{\mathcal{N}}[U] = 0 \iff \mathcal{N} \models A[U]$.

$$\begin{aligned}
&r_\bot := \mathrm{suc}(0),\\
&r_{s=t} := (s \dot{-} t) + (t \dot{-} s),\\
&r_{\neg A} := 1 \dot{-} r_A,\\
&r_{A \wedge B} := 1 \dot{-} (1 \dot{-} r_A) \cdot (1 \dot{-} r_B),\\
&r_{A \vee B} := r_A \cdot r_B,\\
&r_{\forall x < t\, A} := \Big(\sum f\Big)\, t\vec{y} \quad \text{mit } f = \lambda x, \vec{y}\, r_A \text{ und } \mathrm{FV}(\forall x < t\, A) = \{\vec{y}\}.
\end{aligned}$$

□

Es folgt, daß die Menge aller primitiv rekursiven Relationen abgeschlossen ist gegen $\cap, \cup, \setminus$, beschränkte Quantifikation sowie gegen die Einsetzung von primitiv rekursiven Funktionen.

**Lemma 1.3.** *Sind $f_1, \ldots, f_{k+1} \in \mathrm{PR}^n$ und sind $R_1, \ldots, R_k \subseteq \mathbb{N}^n$ paarweise disjunkte primitiv rekursive Relationen, so ist auch die wie folgt definierte Funktion $f\colon \mathbb{N}^n \to \mathbb{N}$ primitiv rekursiv.*

$$f(\vec{a}) := \begin{cases} f_1(\vec{a}), & \text{falls } R_1(\vec{a});\\ \vdots & \vdots\\ f_k(\vec{a}), & \text{falls } R_k(\vec{a});\\ f_{k+1}(\vec{a}), & \text{sonst.} \end{cases}$$

*Beweis.* Sei $R_{k+1} := \mathbb{N}^n \setminus (R_1 \cup \cdots \cup R_k)$. Dann ist

$$f = \lambda \vec{x}. f_1(\vec{x}) \cdot 1_{R_1}(\vec{x}) + \cdots + f_k(\vec{x}) \cdot 1_{R_k}(\vec{x}) + f_{k+1}(\vec{x}) \cdot 1_{R_{k+1}}(\vec{x}).$$

□

Der *beschränkte $\mu$–Operator* macht aus jedem $g\colon \mathbb{N}^{n+1} \to \mathbb{N}$ ein $\overline{\mu}g\colon \mathbb{N}^n \to \mathbb{N}$, das wie folgt definiert ist.

$$(\overline{\mu}g)(a,\vec{b}) := \begin{cases} \min\{\, i \mid g(i,\vec{b}) = 0 \,\}, & \text{falls } \exists i < a\,(g(i,\vec{b}) = 0); \\ a, & \text{sonst.} \end{cases}$$

Wir schreiben auch $\mu i < a\,(g(i,\vec{b}) = 0)$ für $(\overline{\mu}g)(a,\vec{b})$ und $\mu i \leq a\,(g(i,\vec{b}) = 0)$ für $\mu i < \mathrm{suc}(a)\,(g(i,\vec{b}) = 0)$.

**Lemma 1.4.** *Mit $g\colon \mathbb{N}^{n+1} \to \mathbb{N}$ ist auch $\overline{\mu}g$ primitiv rekursiv.*

*Beweis.* Sei

$$h(c,\vec{b}) := \begin{cases} c, & \text{falls } g(c,\vec{b}) = 0 \text{ und } \forall i < c\,(g(i,\vec{b}) \neq 0); \\ 0, & \text{sonst.} \end{cases}$$

$h$ ist nach den Lemmata 1.2 und 1.3 primitiv rekursiv, und wir haben

$$\mu i < a\,(g(i,\vec{b}) = 0) = \begin{cases} \sum_{i<a} h(i,\vec{b}), & \text{falls } \exists i < a\,(g(i,\vec{b}) = 0); \\ a, & \text{sonst.} \end{cases}$$ □

*Beispiele* für primitiv rekursive Funktionen und Relationen.

$$\begin{aligned}
b^a &:= \prod_{i<a} b, \\
a! &:= \prod_{i<a} (i+1), \\
a|b &:\leftrightarrow \exists x \leq b\,(b = a \cdot x), \\
\lfloor a/b \rfloor &:= \mu x \leq a\,(a < b \cdot (x+1)), \\
r(a,b) &:= \mu x \leq a \exists y \leq a\,(a = by + x), \\
\mathrm{Pr}(a) &:\leftrightarrow a \geq 2 \wedge \forall x \leq a\,(x|a \to x = 1 \vee x = a), \\
q(a) &:= \mu x \leq a! + 1\,(x > a \wedge \mathrm{Pr}(x)), \\
p_i &:= \mu x \leq 2^{2^i} \left( \sum_{y \leq x} 1_{\mathrm{Pr}}(y) = i + 1 \right).
\end{aligned}$$

Die Abschätzung $p_i \leq 2^{2^i}$ für die $i$–te Primzahl $p_i$ beweist man durch Induktion über $i$: Für $i = 0$ ist dies klar, und für $i \geq 1$ erhält man

$$p_i \leq p_0 p_1 \cdots p_{i-1} + 1 = 2^{2^0} 2^{2^1} \cdots 2^{2^{i-1}} + 1 = 2^{2^i - 1} + 1 < 2^{2^i}.$$

Man kann die Eindeutigkeit der Darstellung natürlicher Zahlen als Primzahlpotenzprodukt verwenden, um eine endliche Folge $a_0, a_1, \ldots, a_{n-1}$ natürlicher Zahlen durch

$$a := \prod_{i<n} p_i^{a_i}$$

zu kodieren; dies nennt man die *Primzahlpotenzkodierung*. Die $i$–te Komponente der durch $a$ kodierten Folge kann man aus $a$ und $i$ ablesen durch

$$\exp(i,a) := \mu x \leq a\,(p_i^{x+1} \not| a).$$

Offenbar ist exp und für jedes feste $n$ die Funktion $(a_0,\ldots,a_{n-1}) \mapsto \prod_{i<n} p_i^{a_i}$ primitiv rekursiv.

Bei der Primzahlpotenzkodierung wird das Zahlenpaar $a,b$ durch $2^a 3^b$ kodiert. Dieses exponentielle Wachstum einer Paarkodierungsfunktion ist aber nicht notwendig, denn man kann $\mathbb{N}\times\mathbb{N}$ auch wie folgt abzählen.

$$\begin{array}{llllll}
\vdots & & & & & \\
10 & & & & & \\
6 & \ldots & & & & \\
3 & 7 & \ldots & & & \\
1 & 4 & 8 & \ldots & & \\
0 & 2 & 5 & 9 & \ldots &
\end{array}$$

An der Stelle $(0,b)$ steht offenbar die Summe der Längen der vorangehenden Diagonalen, und auf der nächsten Diagonalen bleibt $a+b$ konstant. Nennt man die an der Stelle $(a,b)$ eingetragene Zahl $\pi(a,b)$, so ergibt sich

$$\begin{aligned}
\pi(a,b) &= \left(\sum_{i\leq a+b} i\right) + a \\
&= \frac{1}{2}(a+b)(a+b+1) + a.
\end{aligned}$$

Offenbar ist $\pi\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ bijektiv. Ferner gilt $a,b \leq \pi(a,b)$ und im Fall $\pi(a,b)\neq 0$ auch $a < \pi(a,b)$. Setzt man

$$\begin{aligned}
\pi_1(c) &:= \mu x \leq c \exists y \leq c\,(\pi(x,y) = c), \\
\pi_2(c) &:= \mu y \leq c \exists x \leq c\,(\pi(x,y) = c),
\end{aligned}$$

so folgt unmittelbar $\pi_i(c) \leq c$ für $i \in \{1,2\}$ und

$$\begin{aligned}
\pi_1(\pi(a,b)) &= a, \\
\pi_2(\pi(a,b)) &= b, \\
\pi(\pi_1(c),\pi_2(c)) &= c.
\end{aligned}$$

Ferner sind $\pi, \pi_1, \pi_2$ aufgrund ihrer Definitionen primitiv rekursiv.

Mit Hilfe der *Paarfunktion* $\pi$ kann man jetzt leicht (wie etwa in der Programmsprache Lisp oder Scheme) eine andere Kodierung von endlichen Folgen natürlicher Zahlen definieren. Wir setzen

$$\begin{aligned}&\langle\rangle := 0,\\ &\langle a_0, a_1, \ldots, a_n\rangle := \pi(a_0, \langle a_1, \ldots, a_n\rangle) + 1.\end{aligned}$$

Offenbar läßt sich dann jede Zahl $a$ eindeutig in der Form $a = \langle a_0, a_1, \ldots, a_{n-1}\rangle$ darstellen. Aus $a$ lassen sich die Bestandteile dieser Darstellung wieder ablesen durch die folgenden Funktionen.

$$\begin{aligned}&\mathrm{hd}(a) := \pi_1(a \dot{-} 1) \quad \text{hd steht für 'head',}\\ &\mathrm{tl}(a) := \pi_2(a \dot{-} 1) \quad \text{tl steht für 'tail',}\\ &\tau(a, 0) := a,\\ &\tau(a, k+1) := \mathrm{tl}(\tau(a, k)).\end{aligned}$$

Man beachte, daß für $\tau(a, k) \neq 0$ gilt $\tau(a, k+1) < \tau(a, k)$.

$$\begin{aligned}&\mathrm{lh}(a) := \mu k \leq a(\tau(a, k) = 0),\\ &(a)_i := \begin{cases}\mathrm{hd}(\tau(a, i)), & \text{falls } i < \mathrm{lh}(a);\\ 0, & \text{sonst.}\end{cases}\end{aligned}$$

Es folgt $\mathrm{lh}(a) \leq a$ und $(a)_i \leq a$; für $i < \mathrm{lh}(a)$ gilt sogar $(a)_i < a$, denn dann ist

$$(a)_i = \mathrm{hd}(\tau(a, i)) < \tau(a, i) \leq a.$$

Offenbar sind die Funktionen $(a_0, \ldots, a_n) \mapsto \langle a_0, \ldots, a_n\rangle$ für jedes feste $n$, sowie $\mathrm{hd}, \mathrm{tl}, \tau, \mathrm{lh}$ und $(a, i) \mapsto (a)_i$ primitiv rekursiv. Wir schreiben $(a)_{i,j}$ für $((a)_i)_j$ und $(a)_{i,j,k}$ für $(((a)_i)_j)_k$.

**Lemma 1.5.**

$$\begin{aligned}&\mathrm{hd}(\langle a_0, a_1, \ldots, a_n\rangle) = a_0,\\ &\mathrm{tl}(\langle a_0, a_1, \ldots, a_n\rangle) = \langle a_1, \ldots, a_n\rangle,\\ &\tau(\langle a_0, \ldots, a_k, \ldots, a_n\rangle, k) = \langle a_k, \ldots, a_n\rangle,\\ &\mathrm{lh}(\langle a_0, \ldots, a_{n-1}\rangle) = n,\\ &(\langle a_0, \ldots, a_{n-1}\rangle)_i = a_i \quad \textit{für } i < n.\end{aligned}$$

□

Wir werden beide Kodierungen von endlichen Folgen natürlicher Zahlen nebeneinander verwenden. Ein Vorteil der Primzahlpotenzkodierung liegt darin, daß man die bekannte Produktschreibweise verwenden kann. Dies nutzen wir aus in dem folgenden Beweis, daß die Menge der primitiv rekursiven Funktionen abgeschlossen ist gegen *Wertverlaufsrekursion*. Für jedes $f\colon \mathbb{N}^{n+1} \to \mathbb{N}$ definieren wir seine *Wertverlaufsfunktion* $\overline{f}$ durch

$$\overline{f}(a, \vec{b}) := \prod_{i<a} p_i^{f(i,\vec{b})}.$$

Es folgt, daß mit $f$ auch $\overline{f}$ primitiv rekursiv ist.

**Lemma 1.6 (Wertverlaufsrekursion).** *Mit $g$ ist auch die durch*

$$f(a,\vec{b}) := g(a,\overline{f}(a,\vec{b}),\vec{b})$$

*definierte Funktion $f$ primitiv rekursiv.*

*Beweis.* Es gilt

$$\begin{aligned}\overline{f}(0,\vec{b}) &= 1,\\ \overline{f}(a+1,\vec{b}) &= \overline{f}(a,\vec{b})\cdot p_a^{g(a,\overline{f}(a,\vec{b}),\vec{b})}.\end{aligned}$$

Also ist mit $g$ auch $\overline{f}$ primitiv rekursiv, und deshalb wegen $f(a,\vec{b}) = \exp(a,\overline{f}(a+1,\vec{b}))$ auch $f$. □

Wir zeigen jetzt, daß die Menge der primitiv rekursiven Funktionen auch gegen primitive Rekursion mit Einsetzungen in Parameterstellen abgeschlossen ist; dies wurde zuerst von R. Péter bewiesen (s. etwa [11]). Zur Vorbereitung beweisen wir ein Lemma über primitive Rekursion mit Abstieg bezüglich einer "Maßzahl" $h(a,\vec{b})$. Dieses Lemma werden wir später als Lemma 1.10 noch wesentlich verschärfen können.

**Lemma 1.7.** *Alle $i$ mit $h(i,\vec{b}) < c$ seien abschätzbar durch $i < h'(c,\vec{b})$. Es gelte*

$$\begin{aligned}&f(0,\vec{b}) = g_1(\vec{b}),\\ &f(a,\vec{b}) = g_2(a, f(t_1(a,\vec{b}),\vec{b}),\ldots,f(t_k(a,\vec{b}),\vec{b}),\vec{b}) \quad \textit{falls } a>0,\\ &h(t_j(a,\vec{b}),\vec{b}) < h(a,\vec{b}) \quad \textit{für } 1\le j\le k, \textit{ falls } a>0.\end{aligned}$$

*Dann ist mit $g_1, g_2, t_1, \ldots, t_k, h$ und $h'$ auch $f$ primitiv rekursiv.*

*Beweis.* Zur Vereinfachung lassen wir die Parameter $\vec{b}$ weg. Sei

$$\tilde{f}(c) := \prod_{h(i)<c} p_i^{f(i)}.$$

Dann gilt offenbar $f(a) = \exp(a,\tilde{f}(h(a)+1))$ und

$$\begin{aligned}\tilde{f}(0) &= 1,\\ \tilde{f}(c+1) &= \tilde{f}(c)\cdot\prod_{h(i)=c} p_i^{f(i)}\\ &= \tilde{f}(c)\cdot\left(\prod_{\substack{0<i<h'(c+1)\\ h(i)=c}} p_i^{g_2(i,\exp(t_1(i),\tilde{f}(c)),\ldots,\exp(t_k(i),\tilde{f}(c)))}\right)\cdot\begin{cases} p_0^{g_1}, & \text{falls } h(0)=c,\\ 1, & \text{sonst.}\end{cases}\end{aligned}$$

Sind $g_1, g_2, t_1, \ldots, t_k, h, h'$ primitiv rekursiv, so ist offenbar auch $\tilde{f}$ und damit auch $f$ primitiv rekursiv. □

**Satz 1.8 (Primitive Rekursion mit Einsetzungen in Parameterstellen).** *Sei*

$$f(0,b,\vec{c}) = g_1(b,\vec{c}),$$
$$f(a+1,b,\vec{c}) = g_2(a, f(a,h_1(a,b,\vec{c}),\vec{c}),\ldots,f(a,h_k(a,b,\vec{c}),\vec{c}),b,\vec{c}).$$

*Dann ist mit $g_1, g_2, h_1, \ldots, h_k$ auch $f$ primitiv rekursiv.*

*Beweis.* Zur Vereinfachung lassen wir die Parameter $\vec{c}$ weg. Sei

$$\hat{h}(a,b) := \left( \max_{\substack{i\le a, j\le b \\ 1\le \ell\le k}} h_\ell(i,j) \right) + b + 1$$

und

$$h^*(0,a,b) := b,$$
$$h^*(c+1,a,b) := \hat{h}(a,h^*(c,a,b)).$$

Dann sind mit $h_1,\ldots,h_k$ auch $\hat{h}, h^*$ primitiv rekursiv. Man beachte hier, daß mit $g$ auch $\max_{i<a} g(i,\vec{b})$ primitiv rekursiv ist. Ferner zeigt man leicht durch Induktion über $c$

$$h^*(c+1,a,b) = h^*(c,a,\hat{h}(a,b)),$$
$$h^*(c,a,b) \ge \max(c,b).$$

Wir verwenden jetzt Lemma 1.7 mit $h(\pi(a,b)) := h^*(a,a,b)$. Sei also $h(x) < c$. Dann folgt

$$c > h^*(\pi_1(x),\pi_1(x),\pi_2(x)) \ge \max(\pi_1(x),\pi_2(x)) \ge \pi_i(x),$$

also

$$x = \pi(\pi_1(x),\pi_2(x)) < \pi(c,c) =: h'(c).$$

Sei jetzt

$$\tilde{f}(\pi(0,b)) = g_1(b),$$
$$\tilde{f}(\pi(a+1,b)) = g_2(a,\tilde{f}(\pi(a,h_1(a,b))),\ldots,\tilde{f}(\pi(a,h_k(a,b))),b).$$

Dann gilt offenbar $f(a,b) = \tilde{f}(\pi(a,b))$. Ferner hat man

$$h(\pi(a\dot{-}1,h_\ell(a\dot{-}1,b))) < h(\pi(a,b)) \quad \text{für } 1\le\ell\le k \text{ und } a>0,$$

denn es gilt

$$\begin{aligned} h(\pi(a\dot{-}1,h_\ell(a\dot{-}1,b))) &= h^*(a\dot{-}1,a\dot{-}1,h_\ell(a\dot{-}1,b)) \\ &< h^*(a\dot{-}1,a\dot{-}1,\hat{h}(a\dot{-}1,b)) \\ &= h^*(a,a\dot{-}1,b) \\ &\le h^*(a,a,b) \\ &= h(\pi(a,b)). \end{aligned}$$

Für $a=0$ und $b>0$ kann man $t_j(\pi(0,b)) := 0$ setzen, denn dann ist $h(t_j(\pi(0,b))) = h(0) < h(\pi(0,b))$. Damit ergibt sich die Behauptung aus Lemma 1.7. □

Wir zeigen schließlich noch, daß auch die Wertverlaufsrekursion mit Einsetzungen in Parameterstellen nicht aus den primitiv rekursiven Funktionen hinausführt.

**Folgerung 1.9.** *Mit $g, h_1, \ldots, h_k$ ist auch die durch*

$$f(a,b,\vec{c}) := g(a, \overline{f}(a, h_1(a,b,\vec{c}),\vec{c}), \ldots, \overline{f}(a, h_k(a,b,\vec{c}),\vec{c}), b, \vec{c})$$

*definierte Funktion $f$ primitiv rekursiv.*

*Beweis.* Es gilt

$$\begin{aligned}
&\overline{f}(0,b,\vec{c}) = 1,\\
&\overline{f}(a+1,b,\vec{c}) = \overline{f}(a,b,\vec{c}) \cdot p_a^{g(a,\overline{f}(a,h_1(a,b,\vec{c}),\vec{c}),\ldots,\overline{f}(a,h_k(a,b,\vec{c}),\vec{c}),b,\vec{c})}.
\end{aligned}$$

Also ist mit $g$ auch $\overline{f}$ primitiv rekursiv, und deshalb wegen $f(a,\vec{c}) = \exp(a, \overline{f}(a+1,\vec{c}))$ auch $f$. □

Jetzt können wir Lemma 1.7 wie folgt verschärfen.

**Lemma 1.10 (Primitive Rekursion nach einer Maßzahl).** *Es gelte*

$$\begin{aligned}
&f(0,\vec{b}) = g_1(\vec{b}),\\
&f(a,\vec{b}) = g_2(a, f(t_1(a,\vec{b}),\vec{b}), \ldots, f(t_k(a,\vec{b}),\vec{b}),\vec{b}) \quad \textit{falls } a > 0,\\
&h(t_j(a,\vec{b}),\vec{b}) < h(a,\vec{b}) \quad \textit{für } 1 \le j \le k, \textit{ falls } a > 0.
\end{aligned}$$

*Dann ist mit $g_1, g_2, t_1, \ldots, t_k$ und $h$ auch $f$ primitiv rekursiv.*

*Beweis.* Zur Vereinfachung lassen wir die Parameter $\vec{b}$ weg. Es gilt $f(a) = f^*(h(a), a)$ mit folgendem $f^*$:

$$f^*(c,a) := \begin{cases} g_2(a, f^*(h(t_1(a)),t_1(a)), \ldots, f^*(h(t_k(a)),t_k(a))), & \text{falls } c = h(a) \text{ und } a > 0;\\ g_1, & \text{sonst.}\end{cases}$$

$f^*$ ist primitiv rekursiv nach Folgerung 1.9. □

## 2.2 Rekursive Funktionen, rekursiv aufzählbare Relationen

Aus den primitiv rekursiven Relationen erhält man durch Projektion die rekursiv aufzählbaren Relationen und daraus die rekursiven Funktionen als die Menge der Funktionen mit rekursiv aufzählbaren Graphen. Es wird sich zeigen, daß dieser Begriff einer rekursiven Funktion eine Präzisierung des intuitiven Begriffs der berechenbaren Funktion ist (Churchsche These).

Eine Relation $R \subseteq \mathbb{N}^n$ heißt *rekursiv aufzählbar*, wenn es eine primitiv rekursive Relation $Q \subseteq \mathbb{N}^{n+1}$ gibt mit

$$R = \{\, (a_1, \ldots, a_n) \mid \exists b\, (b, a_1, \ldots, a_n) \in Q \,\}.$$

Insbesondere ist deshalb jede primitiv rekursive Relation rekursiv aufzählbar.

**Lemma 2.1.** *Eine nichtleere Menge $M \subseteq \mathbb{N}$ ist rekursiv aufzählbar genau dann, wenn es ein $f \in \mathrm{PR}^1$ gibt mit $M = \mathrm{ran}(f)$.*

*Beweis.* $\Longrightarrow$. Sei $M \subseteq \mathbb{N}$ rekursiv aufzählbar, also $M = \{\, c \mid \exists b\, (b, c) \in Q \,\}$. Nach Annahme ist $M \neq \emptyset$, es gibt also ein $a_0 \in M$. Setze

$$f(a) := \begin{cases} \pi_2(a), & \text{falls } (\pi_1(a), \pi_2(a)) \in Q; \\ a_0, & \text{sonst.} \end{cases}$$

Dann ist $M = \mathrm{ran}(f)$, und nach Lemma 1.3 gilt $f \in \mathrm{PR}^1$.

$\Longleftarrow$. Sei $M = \mathrm{ran}(f)$ für ein $f \in \mathrm{PR}^1$. Dann ist $M = \{\, c \mid \exists b\, f(b) = c \,\}$ und deshalb rekursiv aufzählbar. □

Unter denselben Annahmen, unter denen wir in Kapitel 2.1 $\Delta_0$–Formeln eingeführt hatten, definieren wir jetzt induktiv den Begriff einer $\Sigma_1$–*Formel* der Sprache PR.

- Jede PR–Primformel und jede negierte PR–Primformel ist eine $\Sigma_1$–Formel.
- Sind $A$ und $B$ $\Sigma_1$–Formeln, so auch $A \wedge B$ und $A \vee B$.
- Ist $A$ eine $\Sigma_1$–Formel und $t$ ein PR–Term mit $x \notin \mathrm{vars}(t)$, so ist $\forall x < t\, A$ eine $\Sigma_1$–Formel.
- Ist $A$ eine $\Sigma_1$–Formel, so ist $\exists x\, A$ eine $\Sigma_1$–Formel.

Offenbar ist jede $\Delta_0$–Formel logisch äquivalent zu einer $\Sigma_1$–Formel und jede rekursiv aufzählbare Relation definierbar durch eine $\Sigma_1$–Formel. Auch die Umkehrung ist richtig:

**Lemma 2.2.** *Ist $A$ eine $\Sigma_1$–Formel mit $\mathrm{FV}(A) \subseteq \{x_1, \ldots, x_n\}$, so ist die Relation*

$$\{\, (a_1, \ldots, a_n) \in \mathbb{N}^n \mid \mathcal{N} \models A[a_1, \ldots, a_n / x_1, \ldots, x_n] \,\}$$

*rekursiv aufzählbar.*

*Beweis.* Eine $\Sigma_1$–Formel $A$ heiße *strikt*, wenn sie von der Form $\exists x\, A$ mit einer $\Delta_0$–Formel $A$ ist. Wir konstruieren zu jeder $\Sigma_1$–Formel $A$ eine strikte $\Sigma_1$–Formel $A'$ mit $\mathrm{FV}(A) = \mathrm{FV}(A')$ und $\mathcal{N} \models \forall (A \leftrightarrow A')$, und zwar durch Rekursion über die Definition der $\Sigma_1$–Formeln. Daraus folgt offenbar die Behauptung. Ist $A$ eine PR–Primformel oder negierte PR–Primformel, so setze man $A' := \exists z\, A$ mit $z \notin \mathrm{FV}(A)$. In den restlichen Fällen sei $A' = \exists x\, \tilde{A}$ und $B' = \exists y\, \tilde{B}$ mit $\Delta_0$–Formeln $\tilde{A}$ und $\tilde{B}$. Wir setzen

$$\begin{aligned}
(A \vee B)' &:= \exists z\, (\tilde{A}[z/x] \vee \tilde{B}[z/y]),\\
(A \wedge B)' &:= \exists z\, (\tilde{A}[\pi_1 z/x] \wedge \tilde{B}[\pi_2 z/y]),\\
(\forall y < t\, A)' &:= \exists z \forall y < t\, \exists x < z\, \tilde{A},\\
(\exists y\, A)' &:= \exists z\, \tilde{A}[\pi_1 z, \pi_2 z/x, y]
\end{aligned}$$

wobei $z \notin \mathrm{FV}(\tilde{A}) \cup \mathrm{FV}(\tilde{B})$ bzw. $z \notin \mathrm{FV}(\tilde{A}) \cup \mathrm{vars}(t)$. □

Es folgt, daß die Menge aller rekursiv aufzählbaren Relationen abgeschlossen ist gegen $\cap, \cup$, beschränkte Allquantifikation, unbeschränkte Existenzquantifikation (oder Projektion) sowie gegen die Einsetzung von primitiv rekursiven Funktionen.

Eine Funktion $f\colon \mathbb{N}^n \to \mathbb{N}$ heißt *rekursiv*, wenn ihr Graph

$$G_f := \{\, (a_1, \ldots, a_n, b) \mid f(a_1, \ldots, a_n) = b \,\}$$

rekursiv aufzählbar ist. Eine Relation $R \subseteq \mathbb{N}^n$ heißt *rekursiv*, wenn ihre charakteristische Funktion $1_R$ rekursiv ist. Hieraus ergibt sich, daß jede primitiv rekursive Relation auch rekursiv ist.

**Lemma 2.3.** *Eine Relation $R \subseteq \mathbb{N}^n$ ist rekursiv genau dann, wenn $R$ und ihr Komplement $\mathbb{N}^n \setminus R$ rekursiv aufzählbar sind.*

*Beweis.* $\Longrightarrow$. Sei $R$ rekursiv, also $1_R$ rekursiv, also

$$G_{1_R} = \{\, (\vec{a}, 1) \mid \vec{a} \in R \,\} \cup \{\, (\vec{a}, 0) \mid \vec{a} \in \mathbb{N}^n \setminus R \,\}$$

rekursiv aufzählbar. Dann sind

$$R = \{\, \vec{a} \mid (\vec{a}, 1) \in G_{1_R} \,\}$$

und

$$\mathbb{N}^n \setminus R = \{\, \vec{a} \mid (\vec{a}, 0) \in G_{1_R} \,\}$$

rekursiv aufzählbar nach Lemma 2.2.

$\Longleftarrow$. Seien $R$ und $\mathbb{N}^n \setminus R$ rekursiv aufzählbar. Dann gibt es $\Sigma_1$–Formeln $A$ und $A'$ mit

$$R = \{\, \vec{a} \mid \mathcal{N} \models A[\vec{a}] \,\},$$
$$\mathbb{N}^n \setminus R = \{\, \vec{a} \mid \mathcal{N} \models A'[\vec{a}] \,\}.$$

Zu zeigen ist, daß die charakteristische Funktion $1_R$ rekursiv ist, also, daß ihr Graph $G_{1_R}$ rekursiv aufzählbar ist. Es gilt

$$\begin{aligned} G_{1_R} &= \{\, (\vec{a}, b) \mid 1_R(\vec{a}) = b \,\} \\ &= \{\, (\vec{a}, b) \mid (\vec{a} \in R \text{ und } b = 1) \text{ oder } (\vec{a} \in \mathbb{N}^n \setminus R \text{ und } b = 0) \,\} \\ &= \{\, (\vec{a}, b) \mid \mathcal{N} \models ((A \wedge y = 1) \vee (A' \wedge y = 0))[\vec{a}, b] \,\}. \end{aligned}$$

Damit ist gezeigt, daß $G_{1_R}$ durch eine $\Sigma_1$–Formel definierbar und deshalb rekursiv aufzählbar ist. □

**Folgerung 2.4.** *Für jede rekursive Funktion $f$ ist ihr Graph $G_f$ rekursiv.*

*Beweis.* Sei $f\colon \mathbb{N}^n \to \mathbb{N}$ rekursiv. Es genügt zu zeigen, daß $\mathbb{N}^{n+1} \setminus G_f$ rekursiv aufzählbar ist. Dies folgt aber aus

$$\mathbb{N}^{n+1} \setminus G_f = \{\, (\vec{a}, b) \mid \exists c\, (c \neq b \wedge (\vec{a}, c) \in G_f) \,\}.$$ □

Sei $\mathcal{F}$ die kleinste Menge von Funktionen mit den folgenden Eigenschaften. Wir schreiben $\mathcal{F}^n$ für die Teilmenge der $n$–stelligen Funktionen in $\mathcal{F}$.

a. $0^n \in \mathcal{F}^n$ $(n \geq 0)$, suc $\in \mathcal{F}^1$, $I_i^n \in \mathcal{F}^n$ $(1 \leq i \leq n)$.

b. Sind $g_1, \ldots, g_m \in \mathcal{F}^n$, $h \in \mathcal{F}^m$ und $m, n \geq 1$, so ist $(\circ h g_1 \ldots g_m) \in \mathcal{F}^n$.

c. Ist $g \in \mathcal{F}^n$ und $h \in \mathcal{F}^{n+2}$, so ist $(Rgh) \in \mathcal{F}^{n+1}$.

d. Ist $g \in \mathcal{F}^{n+1}$ und gilt $\forall \vec{a} \exists i\, g(i, \vec{a}) = 0$, so ist die durch

$$(\mu g)(\vec{a}) := \min\{\, i \mid g(i, \vec{a}) = 0 \,\}$$

definierte Funktion $\mu g$ in $\mathcal{F}^n$ (*unbeschränkter $\mu$–Operator*). Wir schreiben meist $\mu i\, (g(i, \vec{a}) = 0)$ für $(\mu g)(\vec{a})$.

Die Funktionen in $\mathcal{F}$ nennen wir auch $\mu$–rekursiv.

**Satz 2.5.** *$\mathcal{F}$ ist die Menge der rekursiven Funktionen.*

*Beweis.* Wir zeigen zunächst durch Induktion über die Definition von $\mathcal{F}$, daß jedes $f \in \mathcal{F}$ rekursiv ist. Dazu konstruieren wir zu jedem $f \in \mathcal{F}^n$ eine $\Sigma_1$–Formel $A_f[x_1, \ldots, x_n, y]$ so daß $f(\vec{a}) = b$ genau dann, wenn $\mathcal{N} \models A_f[\vec{a}, b]$. Für die Ausgangsfunktionen ist dies trivial. *Fall* $f = (\circ h g_1 \ldots g_m)$.

$$A_f := \exists z_1, \ldots, z_m \left( \bigwedge_{i=1}^{m} A_{g_i}[\vec{x}, z_i] \wedge A_h[z_1, \ldots, z_m, y] \right).$$

*Fall* $f = (Rgh)$.

$$A_f[x, \vec{x}, y] := \exists z \; (lh(z) = x + 1 \wedge A_g[\vec{x}, (z)_0] \wedge \forall i < x \, A_h[i, (z)_i, \vec{x}, (z)_{i+1}] \wedge y = (z)_x) .$$

*Fall* $f = (\mu g)$.

$$A_f := A_g[y, \vec{x}, 0] \wedge \forall i < y \exists z \, A_g[i, \vec{x}, \mathrm{suc}(z)].$$

Sei nun umgekehrt $f$ rekursiv, also $G_f$ rekursiv aufzählbar. Zu zeigen ist $f \in \mathcal{F}$. Nach dem Beweis von Lemma 2.2 ist $G_f$ durch eine strikte $\Sigma_1$–Formel definierbar. Es gibt also eine $\Delta_0$–Formel $A$ so daß

$$G_f = \{ \, (\vec{a}, b) \mid \mathcal{N} \models (\exists y \, A)[\vec{a}, b] \, \}.$$

Nach Lemma 1.2 ist

$$R = \{ \, (i, \vec{a}) \mid \mathcal{N} \models A[\vec{a}, \pi_1(i), \pi_2(i)] \, \}$$

primitiv rekursiv. Es gibt also eine primitiv rekursive Funktion $g$ mit $R = \{ \, (i, \vec{a}) \mid g(i, \vec{a}) = 0 \, \}$. Nach Konstruktion gilt $\forall \vec{a} \exists i \, (g(i, \vec{a}) = 0)$ und $f(\vec{a}) = \pi_1(\mu i \, (g(i, \vec{a}) = 0))$. Also ist $f \in \mathcal{F}$, da $g, \pi_1 \in \mathrm{PR} \subseteq \mathcal{F}$. □

Wir wollen jetzt noch den Zusammenhang zwischen den Begriffen einer rekursiven bzw. rekursiv aufzählbaren Relation und einer rekursiven Funktion einerseits und den intuitiven Begriffen der Entscheidbarkeit und der Aufzählbarkeit einer Relation und der Berechenbarkeit einer Funktion herstellen. Der Einfachheit halber beschränken wir uns wieder auf Funktionen und Relationen über den natürlichen Zahlen. Zunächst geben wir eine informale Definition der erwähnten intuitiven Begriffe, wobei wir auch *partielle Funktionen* zulassen, also Funktionen $f\colon \mathrm{dom}(f) \to \mathbb{N}$ mit $\mathrm{dom}(f) \subseteq \mathbb{N}^n$. Eine Funktion heißt *total*, wenn sie auf ganz $\mathbb{N}^n$ definiert ist.

Eine Relation $R \subseteq \mathbb{N}^n$ heißt *entscheidbar*, wenn es einen Algorithmus gibt, der für jedes Argumentetupel $\vec{a}$ terminiert und entscheidet, ob $\vec{a}$ zu $R$ gehört oder nicht. Eine Relation $R \subseteq \mathbb{N}^n$ heißt *aufzählbar* (oder positiv berechenbar), wenn es einen Algorithmus gibt, der für jedes Argumentetupel $\vec{a}$ genau dann terminiert, wenn $\vec{a}$ zu $R$ gehört. Eine Funktion $f\colon \mathrm{dom}(f) \to \mathbb{N}$ mit $\mathrm{dom}(f) \subseteq \mathbb{N}^n$ heißt *berechenbar*, wenn es einen Algorithmus gibt, der für jedes Argumentetupel $\vec{a}$ folgendes leistet.

a. Der Algorithmus terminiert auf $\vec{a}$ genau dann, wenn $\vec{a} \in \mathrm{dom}(f)$.

b. Für jedes $\vec{a} \in \mathrm{dom}(f)$ liefert der Algorithmus bei Eingabe von $\vec{a}$ den Wert $f(\vec{a})$.

Zunächst notieren wir einige einfache Eigenschaften entscheidbarer und aufzählbarer Relationen und berechenbarer Funktionen.

**Lemma 2.6.** *Eine Funktion $f$ ist berechenbar genau dann, wenn ihr Graph $G_f$ aufzählbar ist.*

*Beweis.* 1. Sei $f$ berechenbar. Einen Algorithmus, der für jedes Argumentetupel $(\vec{a}, b)$ genau dann terminiert, wenn $(\vec{a}, b)$ zu $G_f$ gehört, erhält man wie folgt. Man berechne $f(\vec{a})$ mittels des gegebenen Algorithmus für $f$. Man breche ab genau dann, wenn die Berechnung terminiert und den Wert $b$ ergibt.

2. Sei $G_f$ aufzählbar. Einen Algorithmus zur Berechnung von $f$ erhält man wie folgt. Gegeben sei ein Argumentetupel $\vec{a}$. Man zähle alle Tupel $(\vec{c}, b)$ in $G_f$ auf. Sobald dabei ein Tupel $(\vec{c}, b)$ mit $\vec{c} = \vec{a}$ auftaucht, breche man ab und gebe $b$ aus. □

**Lemma 2.7.** *Eine Relation $R \subseteq \mathbb{N}^n$ ist entscheidbar genau dann, wenn sowohl sie selbst als auch ihr Komplement $\mathbb{N}^n \setminus R$ aufzählbar sind.*

*Beweis.* Übungsaufgabe. □

Das folgende Lemma gibt einige einfache Charakterisierungen des Begriffs der Aufzählbarkeit.

**Lemma 2.8.** *Für Relationen $R \subseteq \mathbb{N}^n$ sind folgende Bedingungen äquivalent.*

a. *$R$ ist aufzählbar.*

b. *$R$ ist Definitionsbereich einer berechenbaren Funktion.*

c. *$R$ ist Projektion einer entscheidbaren Relation $Q \subseteq \mathbb{N}^{n+1}$.*

*Beweis.* Übungsaufgabe. □

**Churchsche These.**

a. *Eine Relation $R \subseteq \mathbb{N}^n$ ist entscheidbar genau dann, wenn sie rekursiv ist.*

b. *Eine Relation $R \subseteq \mathbb{N}^n$ ist aufzählbar (oder positiv berechenbar) genau dann, wenn sie rekursiv aufzählbar ist.*

c. *Eine totale Funktion $f\colon \mathbb{N}^n \to \mathbb{N}$ ist berechenbar genau dann, wenn sie rekursiv ist.*

Die *Churchsche These* kann man aus prinzipiellen Gründen nicht mathematisch beweisen, da sie Begriffe verwendet, die nur intuitiv, aber nicht mathematisch präzise erklärt

sind. Es besteht jedoch allgemeine Übereinstimmung darüber, daß die Churchsche These zutrifft. Diese Übereinstimmung beruht im wesentlichen auf Erfahrung: es ist keine im intuitiven Sinn berechenbare totale Funktion bekannt, die nicht rekursiv wäre.

## 2.3 Kodierung der Logik

Gegeben sei eine abzählbare Sprache $\mathcal{L}$ erster Stufe. In injektiver Weise sei jedem $R \in \mathrm{Rel}_{\mathcal{L}}^{(n)}$ eine *Symbolnummer* $\mathrm{SN}(R)$ von der Form $\langle 1, n, i\rangle$ und jedem $f \in \mathrm{Fun}_{\mathcal{L}}^{(n)}$ eine Symbolnummer $\mathrm{SN}(f)$ von der Form $\langle 2, n, j\rangle$ zugeordnet. Wir nennen $\mathcal{L}$ *primitiv rekursiv präsentiert*, wenn

$$\mathrm{Symb}_{\mathcal{L}} := \bigcup_{n\in\mathbb{N}} \{\, \mathrm{SN}(R) \mid R \in \mathrm{Rel}_{\mathcal{L}}^{(n)} \,\} \cup \bigcup_{n\in\mathbb{N}} \{\, \mathrm{SN}(f) \mid f \in \mathrm{Fun}_{\mathcal{L}}^{(n)} \,\}$$

primitiv rekursiv ist. Insbesondere ist also jede Sprache mit endlich vielen Relations– und Funktionssymbolen primitiv rekursiv präsentiert. Für jede im folgenden betrachtete Sprache $\mathcal{L}$ nehmen wir an, daß sie primitiv rekursiv präsentiert ist.

Ferner sei $\mathrm{SN}(\bot) := \langle 3, 0\rangle$, $\mathrm{SN}(\wedge) := \langle 3, 1\rangle$, $\mathrm{SN}(\to) := \langle 3, 2\rangle$ und $\mathrm{SN}(\forall) := \langle 3, 3\rangle$. Schließlich ordnen wir der $i$–ten Variablen $*_i$ die Symbolnummer $\mathrm{SN}(*_i) := \langle 0, i\rangle$ zu.

Für jeden $\mathcal{L}$–Term $t$ definieren wir rekursiv seine *Kodenummer* (oder *Gödelnummer*) $\ulcorner t \urcorner$ durch

$$\begin{aligned}
&\ulcorner x \urcorner := \langle \mathrm{SN}(x)\rangle,\\
&\ulcorner c \urcorner := \langle \mathrm{SN}(c)\rangle,\\
&\ulcorner f t_1 \dots t_n \urcorner := \langle \mathrm{SN}(f), \ulcorner t_1 \urcorner, \dots, \ulcorner t_n \urcorner\rangle.
\end{aligned}$$

Ebenso definieren wir rekursiv für jede $\mathcal{L}$–Formel $A$ ihre Kodenummer $\ulcorner A \urcorner$ durch

$$\begin{aligned}
&\ulcorner R t_1 \dots t_n \urcorner := \langle \mathrm{SN}(R), \ulcorner t_1 \urcorner, \dots, \ulcorner t_n \urcorner\rangle,\\
&\ulcorner \bot \urcorner := \langle \mathrm{SN}(\bot)\rangle,\\
&\ulcorner A \wedge B \urcorner := \langle \mathrm{SN}(\wedge), \ulcorner A \urcorner, \ulcorner B \urcorner\rangle,\\
&\ulcorner A \to B \urcorner := \langle \mathrm{SN}(\to), \ulcorner A \urcorner, \ulcorner B \urcorner\rangle,\\
&\ulcorner \forall x\, A \urcorner := \langle \mathrm{SN}(\forall), \ulcorner x \urcorner, \ulcorner A \urcorner\rangle.
\end{aligned}$$

Sei $\mathrm{Var} := \{\, \langle\langle 0, i\rangle\rangle \mid i \in \mathbb{N} \,\}$. Var ist offenbar primitiv rekursiv, und es gilt $a \in \mathrm{Var}$ genau dann, wenn $a = \ulcorner x \urcorner$ für eine Variable $x$. Ferner definieren wir $\mathrm{Ter} \subseteq \mathbb{N}$ wie folgt durch Wertverlaufsrekursion.

$$\begin{aligned}
a \in \mathrm{Ter} :\leftrightarrow\ & a \in \mathrm{Var}\\
&\vee ((a)_0 \in \mathrm{Symb}_{\mathcal{L}} \wedge (a)_{0,0} = 2 \wedge \mathrm{lh}(a) = (a)_{0,1} + 1 \wedge \forall i_{0<i<\mathrm{lh}(a)}\, (a)_i \in \mathrm{Ter}).
\end{aligned}$$

Also ist Ter primitiv rekursiv, und es gilt $a \in \mathrm{Ter}$ genau dann, wenn $a = \ulcorner t \urcorner$ für einen Term $t$. Weiter sei $\mathrm{For} \subseteq \mathbb{N}$ definiert durch

$$\begin{aligned}
a \in \mathrm{For} :\leftrightarrow\ & ((a)_0 \in \mathrm{Symb}_{\mathcal{L}} \wedge (a)_{0,0} = 1 \wedge \mathrm{lh}(a) = (a)_{0,1} + 1 \wedge \forall i_{0<i<\mathrm{lh}(a)}\, (a)_i \in \mathrm{Ter})\\
&\vee a = \langle \mathrm{SN}(\bot)\rangle\\
&\vee (a = \langle \mathrm{SN}(\wedge), (a)_1, (a)_2\rangle \wedge (a)_1 \in \mathrm{For} \wedge (a)_2 \in \mathrm{For})\\
&\vee (a = \langle \mathrm{SN}(\to), (a)_1, (a)_2\rangle \wedge (a)_1 \in \mathrm{For} \wedge (a)_2 \in \mathrm{For})\\
&\vee (a = \langle \mathrm{SN}(\forall), (a)_1, (a)_2\rangle \wedge (a)_1 \in \mathrm{Var} \wedge (a)_2 \in \mathrm{For}).
\end{aligned}$$

Wieder ist For primitiv rekursiv, und es gilt $a \in \mathrm{For}$ genau dann, wenn $a = \ulcorner A \urcorner$ für eine Formel $A$. Für eine Menge $S$ von Formeln setzen wir $\ulcorner S \urcorner := \{ \ulcorner A \urcorner \mid A \in S \}$. Sei weiter $\mathrm{vars} \subseteq \mathbb{N} \times \mathbb{N}$ definiert durch

$$\mathrm{vars}(n,a) :\leftrightarrow (a \in \mathrm{Var} \wedge n = a) \vee ((a)_0 \in \mathrm{Symb}_{\mathcal{L}} \wedge \exists i_{0<i<\mathrm{lh}(a)}\, \mathrm{vars}(n,(a)_i)).$$

vars ist primitiv rekursiv, und es gilt $\mathrm{vars}(\ulcorner x \urcorner, \ulcorner t \urcorner)$ genau dann, wenn $x \in \mathrm{vars}(t)$. Entsprechend definieren wir

$$\begin{aligned}\mathrm{FV}(n,a) :\leftrightarrow & ((a)_0 \in \mathrm{Symb}_{\mathcal{L}} \wedge \exists i_{0<i<\mathrm{lh}(a)}\, \mathrm{vars}(n,(a)_i)) \\ & \vee ((a)_0 = \mathrm{SN}(\wedge) \wedge (\mathrm{FV}(n,(a)_1) \vee \mathrm{FV}(n,(a)_2))) \\ & \vee ((a)_0 = \mathrm{SN}(\rightarrow) \wedge (\mathrm{FV}(n,(a)_1) \vee \mathrm{FV}(n,(a)_2))) \\ & \vee ((a)_0 = \mathrm{SN}(\forall) \wedge n \neq (a)_1 \wedge \mathrm{FV}(n,(a)_2)).\end{aligned}$$

Dann ist FV primitiv rekursiv, und es gilt $\mathrm{FV}(\ulcorner x \urcorner, \ulcorner A \urcorner)$ genau dann, wenn $x \in \mathrm{FV}(A)$.

Eine Substitution $\{t_1/x_1, \ldots, t_n/x_n\}$ kann man kodieren durch die Zahl

$$\langle \langle \ulcorner x_1 \urcorner, \ulcorner t_1 \urcorner \rangle, \ldots, \langle \ulcorner x_n \urcorner, \ulcorner t_n \urcorner \rangle \rangle$$

und natürlich auch durch viele andere Zahlen, da es auf die Reihenfolge der $\langle \ulcorner x_i \urcorner, \ulcorner t_i \urcorner \rangle$ nicht ankommt. Wir verwenden $\ulcorner \vartheta \urcorner$ zur Mitteilung einer solchen Kodenummer der Substitution $\vartheta$. Mit $\mathrm{substval}(a,0) := a$ und im Fall $\ell > 0$

$$\mathrm{substval}(a,\ell) := \begin{cases} (\ell)_{0,1}, & \text{falls } a = (\ell)_{0,0}; \\ \mathrm{substval}(a, \mathrm{tl}(\ell)), & \text{sonst} \end{cases}$$

ist offenbar substval primitiv rekursiv und es gilt $\mathrm{substval}(\ulcorner x \urcorner, \ulcorner \vartheta \urcorner) = \ulcorner x\vartheta \urcorner$. Weiter sei $\mathrm{restrict}(0,a) := 0$ und im Fall $\ell > 0$

$$\mathrm{restrict}(\ell,a) := \begin{cases} \langle (\ell)_0 \rangle * \mathrm{restrict}(\mathrm{tl}(\ell),a), & \text{falls } \mathrm{FV}((\ell)_{0,0},a); \\ \mathrm{restrict}(\mathrm{tl}(\ell),a), & \text{sonst.} \end{cases}$$

Dann ist restrict primitiv rekursiv und $\mathrm{restrict}(\ulcorner \vartheta \urcorner, \ulcorner A \urcorner)$ kodiert $\vartheta \restriction \mathrm{FV}(A)$. $\mathrm{Ranv}(n,\ell)$ definieren wir durch Rekursion über $n$; aus der Definition ergibt sich unmittelbar, daß Ranv primitiv rekursiv ist. $\mathrm{Ranv}(n,0)$ sei falsch und im Fall $\ell > 0$ setzen wir

$$\mathrm{Ranv}(n,\ell) :\leftrightarrow \mathrm{vars}(n,(\ell)_{0,1}) \vee \mathrm{Ranv}(n,\mathrm{tl}(\ell)).$$

Es gilt $\mathrm{Ranv}(\ulcorner x \urcorner, \ulcorner \vartheta \urcorner) \leftrightarrow x \in \mathrm{ranv}(\vartheta)$.

Zur Definition von $A\vartheta$ benötigen wir im $\forall$–Fall gegebenenfalls eine neue Variable. Dafür definieren wir $\mathrm{newvar}(0)$ beliebig und für $a > 0$

$$\mathrm{newvar}(a) := \begin{cases} \langle \langle 0, (a)_{0,1} + 1 \rangle \rangle, & \text{falls } a \in \mathrm{Var}; \\ \langle \langle 0, \max_{0<i<\mathrm{lh}(a)}(\mathrm{newvar}((a)_i))_{0,1} \rangle \rangle, & \text{falls } (a)_0 \in \mathrm{Symb}_{\mathcal{L}}; \\ \langle \langle 0, \max((\mathrm{newvar}((a)_1))_{0,1}, (\mathrm{newvar}((a)_2))_{0,1}) \rangle \rangle, & \text{falls } (a)_0 \in \{\mathrm{SN}(\wedge), \mathrm{SN}(\rightarrow)\}; \\ \langle \langle 0, \max((a)_{1,0,1} + 1, (\mathrm{newvar}((a)_2))_{0,1}) \rangle \rangle, & \text{falls } (a)_0 = \mathrm{SN}(\forall). \end{cases}$$

Dann ist newvar primitiv rekursiv, und newvar($\ulcorner t \urcorner$) ist $\ulcorner y \urcorner$ für die kleinste Variable echt oberhalb aller Variablen in vars($t$), und newvar($\ulcorner A \urcorner$) ist $\ulcorner y \urcorner$ für die kleinste Variable echt oberhalb aller Variablen in $\mathrm{FV}(A) \cup \mathrm{BV}(A)$. Weiter sei $\mathrm{newranv}(0) := \langle\langle 0, 0\rangle\rangle$ und für $\ell > 0$

$$\mathrm{newranv}(\ell) := \max(\mathrm{newvar}((\ell)_{0,1}), \mathrm{newranv}(\mathrm{tl}(\ell))).$$

Dann ist newranv primitiv rekursiv, und newranv($\ulcorner \vartheta \urcorner$) ist die kleinste Variable echt oberhalb aller Wertevariablen von $\vartheta$.

Wir definieren $\mathrm{sub}(a, \ell)$ wie folgt durch Rekursion über $a$. Im Fall $a \in \mathrm{Var}$ sei

$$\mathrm{sub}(a, \ell) := \mathrm{substval}(a, \ell).$$

Im Fall $(a)_0 = \mathrm{SN}(\forall)$ sei $k := \mathrm{restrict}(\ell, a)$ und

$$\mathrm{sub}(a, \ell) := \begin{cases} \langle \mathrm{SN}(\forall), (a)_1, \mathrm{sub}((a)_2, k)\rangle, & \text{falls } \neg\mathrm{Ranv}((a)_1, k); \\ \langle \mathrm{SN}(\forall), b, \mathrm{sub}((a)_2, \langle\langle (a)_1, b\rangle\rangle * k)\rangle, & \text{falls } \mathrm{Ranv}((a)_1, k), \end{cases}$$

wobei $b := \max(\mathrm{newranv}(k), \mathrm{newvar}((a)_2))$. Sonst sei

$$\mathrm{sub}(a, \ell) := \langle (a)_0, \mathrm{sub}((a)_1, \ell), \ldots, \mathrm{sub}((a)_{\mathrm{lh}(a)-1}, \ell)\rangle.$$

**Lemma 3.1.** *a.* $\mathrm{sub}(\ulcorner t \urcorner, \ulcorner \vartheta \urcorner) = \ulcorner t\vartheta \urcorner$.

*b.* $\mathrm{sub}(\ulcorner A \urcorner, \ulcorner \vartheta \urcorner) = \ulcorner A\vartheta \urcorner$.

*c. Die Funktion* sub *ist primitiv rekursiv.*

*Beweis.* a. Induktion über $t$. b. Induktion über $A$. Im Fall $\forall x\, A$ beachte man, daß in der Definition von $(\forall x\, A)\vartheta$ in Kapitel 1.3 die Komposition $\{y/x\}\sigma$ keine Streichung von Bindungen erfordert.

c. Es gilt $\mathrm{sub}(a, \ell) = g(a, \overline{\mathrm{sub}}(a, \ell), \overline{\mathrm{sub}}(a, \mathrm{restrict}(\ell, a)), \overline{\mathrm{sub}}(a, h_1(a, \ell)), \ell)$ mit

$$b(a, \ell) := \max(\mathrm{newranv}(\mathrm{restrict}(\ell, a)), \mathrm{newvar}((a)_2)),$$
$$h_1(a, \ell) := \langle\langle (a)_1, b(a, \ell)\rangle\rangle * \mathrm{restrict}(\ell, a).$$

Hierbei ist

$$g(a, d_0, d_1, d_2, \ell) := \begin{cases} \mathrm{substval}(a, \ell), & \text{falls } a \in \mathrm{Var}; \\ \langle \mathrm{SN}(\forall), (a)_1, \exp((a)_2, d_1)\rangle, & \text{falls } (a)_0 = \mathrm{SN}(\forall) \text{ und } \neg\mathrm{Ranv}((a)_1, \mathrm{restrict}(\ell, a)); \\ \langle \mathrm{SN}(\forall), b(a, \ell), \exp((a)_2, d_2)\rangle, & \text{falls } (a)_0 = \mathrm{SN}(\forall) \text{ und } \mathrm{Ranv}((a)_1, \mathrm{restrict}(\ell, a)); \\ h(a, d_0, \mathrm{lh}(a) \dot{-} 1), & \text{sonst.} \end{cases}$$

Ferner ist $h$ primitiv rekursiv definiert durch

$$h(a, d, 0) := \langle (a)_0\rangle,$$
$$h(a, d, n+1) := h(a, d, n) * \langle \exp((a)_{n+1}, d)\rangle. \qquad \square$$

In der bisherigen Darstellung von natürlichen Herleitungen findet man die an einem Knoten freien Annahmen, indem man den darüberliegenden Teil des Baums durchmustert. Mit mehr Schreibaufwand verbunden, aber hier und in anderen theoretischen Überlegungen manchmal nützlich ist eine alternative Darstellung, in der man an jedem Knoten noch die dort freien Annahmen hinzuschreibt. Es genügt, dies in der Form einer Multimenge der Annahmeformeln zu tun.

Unter einer *Sequenz* $\Gamma \Rightarrow A$ verstehen wir ein Paar aus einer Multimenge $\Gamma = \{\{A_1, \ldots, A_n\}\}$ von Formeln und einer Formel $A$. Wir definieren $\vdash_m \Gamma \Rightarrow A$ induktiv durch die folgenden Regeln. Eine Annahme kann man einführen durch

$$\Gamma \Rightarrow A, \quad \text{falls } A \text{ in } \Gamma.$$

Für die Konjuktion $\wedge$ haben wir eine Einführungsregel $\wedge$I und zwei Beseitigungsregeln $\wedge\mathrm{E_l}$ und $\wedge\mathrm{E_r}$.

$$\frac{\Gamma \Rightarrow A \quad \Delta \Rightarrow B}{\Gamma, \Delta \Rightarrow A \wedge B}\wedge\mathrm{I} \qquad \frac{\Gamma \Rightarrow A \wedge B}{\Gamma \Rightarrow A}\wedge\mathrm{E_r} \qquad \frac{\Gamma \Rightarrow A \wedge B}{\Gamma \Rightarrow B}\wedge\mathrm{E_l}$$

$\Gamma, \Delta$ bezeichnet hier die Multimengenvereinigung. Für die Implikation $\rightarrow$ gibt es eine Einführungsregel $\rightarrow$I (hier ohne Erwähnung einer Annahmevariablen $u$) und eine Beseitigungsregel $\rightarrow$E.

$$\frac{\Gamma \Rightarrow B}{\Delta \Rightarrow A \rightarrow B}\rightarrow\mathrm{I} \qquad \frac{\Gamma \Rightarrow A \rightarrow B \quad \Delta \Rightarrow A}{\Gamma, \Delta \Rightarrow B}\rightarrow\mathrm{E}$$

Dabei soll in $\rightarrow$I die Multimenge $\Delta$ aus $\Gamma$ durch Streichen einiger Vorkommen von $A$ entstehen. Für den Allquantor $\forall$ gibt es eine Einführungsregel $\forall$I und eine Beseitigungsregel $\forall$E, die wir hier ohne den zu substituierenden Term $t$ als rechte Prämisse formulieren.

$$\frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow \forall x\, A}\forall\mathrm{I} \qquad \frac{\Gamma \Rightarrow \forall x\, A}{\Gamma \Rightarrow A[t/x]}\forall\mathrm{E}$$

In $\forall$I muß wieder die Variablenbedingung erfüllt sein: für alle $B$ in $\Gamma$ muß gelten $x \notin \mathrm{FV}(B)$.

**Lemma 3.2.**

a. *Wenn* $\vdash_m \{\{A_1, \ldots, A_n\}\} \Rightarrow A$, *so gibt es für alle (nicht notwendig verschiedenen)* $u_1, \ldots, u_n$ *mit* $u_i = u_j \rightarrow A_i = A_j$ *einen Herleitungsterm* $d[u_1^{A_1}, \ldots, u_n^{A_n}]^A$.

b. *Zu jedem Herleitungsterm* $d[u_1^{A_1}, \ldots, u_n^{A_n}]^A$ *findet man Vielfachheiten* $k_1, \ldots, k_n \geq 0$ *so daß* $\vdash_m \{\{A_1^{k_1}, \ldots, A_n^{k_n}\}\} \Rightarrow A$; *hierbei bedeutet* $A^k$ *ein k–faches Vorkommen von* $A$.

*Beweis.* a. Gelte $\vdash_m \{\{A_1, \ldots, A_n\}\} \Rightarrow A$. Wir führen den Beweis durch Induktion über $\vdash_m$. *Fall* Annahmeaxiom. Sei etwa $A = A_i$. Wähle $d = u_i$.

*Fall* $\rightarrow$I. OBdA hat man

$$\frac{\{\{A_1, \ldots, A_n, A, \ldots, A\}\} \Rightarrow B}{\{\{A_1, \ldots, A_n\}\} \Rightarrow A \rightarrow B}\rightarrow\mathrm{I}.$$

Seien $u_1, \ldots, u_n$ gegeben mit $u_i = u_j \to A_i = A_j$. Man wähle ein neues $u$. Nach IH existiert ein $d^B$ mit $\mathrm{FA}(d^B) \subseteq \{u_1^{A_1}, \ldots, u_n^{A_n}, u^A\}$. Dann ist $(\lambda u^A\, d^B)^{A\to B}$ ein Herleitungsterm mit freien Annahmen unter $u_1^{A_1}, \ldots, u_n^{A_n}$.

*Fall* $\to$E. Gegeben sind Herleitungen von

$$\{\{A_1, \ldots, A_n\}\} \Rightarrow A \to B \quad \text{und} \quad \{\{A_{n+1}, \ldots, A_{n+m}\}\} \Rightarrow A.$$

Seien $u_1, \ldots, u_{n+m}$ gegeben mit $u_i = u_j \to A_i = A_j$. Nach IH haben wir Herleitungsterme

$$d[u_1^{A_1}, \ldots, u_n^{A_n}]^{A\to B} \quad \text{und} \quad e[u_{n+1}^{A_{n+1}}, \ldots, u_{n+m}^{A_{n+m}}]^A.$$

Dann ist aber auch

$$(de)[u_1^{A_1}, \ldots, u_{n+m}^{A_{n+m}}]^B$$

ein Herleitungsterm.

Die restlichen Fälle behandelt man ähnlich.

b. Gegeben sei ein Herleitungsterm $d[u_1^{A_1}, \ldots, u_n^{A_n}]^A$. Wir führen den Beweis durch Induktion über $d$. *Fall* $u^A$. Dann ist $\vdash_m \{\{A\}\} \Rightarrow A$.

*Fall* $\to$I, also $(\lambda u^A\, d^B)^{A\to B}$. Sei $\mathrm{FA}(d^B) \subseteq \{u_1^{A_1}, \ldots, u_n^{A_n}, u^A\}$ mit $u_1, \ldots, u_n, u$ verschieden. Nach IH hat man

$$\vdash_m \{\{A_1^{k_1}, \ldots, A_n^{k_n}, A^k\}\} \Rightarrow B.$$

Mit der Regel $\to$I folgt

$$\vdash_m \{\{A_1^{k_1}, \ldots, A_n^{k_n}\}\} \Rightarrow A \to B.$$

*Fall* $\to$E. Gegeben ist $(d^{A\to B} e^A)[u_1^{A_1}, \ldots, u_n^{A_n}]^B$. Nach IH hat man

$$\vdash_m \{\{A_1^{k_1}, \ldots, A_n^{k_n}\}\} \Rightarrow A \to B \quad \text{und} \quad \{\{A_1^{\ell_1}, \ldots, A_n^{\ell_n}\}\} \Rightarrow A.$$

Mit der Regel $\to$E folgt

$$\{\{A_1^{k_1+\ell_1}, \ldots, A_n^{k_n \ell_n}\}\} \Rightarrow B.$$

Die restlichen Fälle behandelt man ähnlich. □

Die Multimenge $\{\{A_1, \ldots, A_n\}\}$ kann man durch $\langle \ulcorner A_1 \urcorner, \ldots, \ulcorner A_n \urcorner \rangle$ kodieren. Wie bei Substitutionen hat auch hier dieselbe Multimenge i.a. mehrere Kodenummern. Wir verwenden $\ulcorner \Gamma \urcorner$ zur Mitteilung einer Kodenummer der Multimenge $\Gamma$. Die Verkettungsfunktion $*$ entspricht offenbar der Multimengenvereinigung. Zur Behandlung der $\to$I–Regel benötigen wir noch die wie folgt definierten Funktionen msm (für 'multisetminus') und msrm (für 'multisetremove'). Es sei $\mathrm{msrm}(0, b) := 0$, und für $a > 0$ setzen wir

$$\mathrm{msrm}(a, b) := \begin{cases} \mathrm{tl}(a), & \text{falls } \mathrm{hd}(a) = b; \\ \langle \mathrm{hd}(a) \rangle * \mathrm{msrm}(\mathrm{tl}(a), b), & \text{sonst.} \end{cases}$$

Dann kodiert offenbar $\mathrm{msrm}(\ulcorner\Gamma\urcorner, \ulcorner A\urcorner)$ diejenige Multimenge, die aus $\Gamma$ durch Entfernen eines Vorkommens von $A$ entsteht, falls $A$ in $\Gamma$ vorkommt, und $\Gamma$ sonst.

Weiter sei $\mathrm{msm}(a,0) := a$, und für $b > 0$ sei $\mathrm{msm}(a,b) := \mathrm{msrm}(\mathrm{msm}(a,\mathrm{tl}(b)),\mathrm{hd}(b))$. $\mathrm{msm}(\ulcorner\Gamma\urcorner, \ulcorner\Delta\urcorner)$ kodiert dann die Multimenge, die aus $\Gamma$ durch Entfernen aller Elemente aus $\Delta$ entsteht. Ferner sei die Relation $\mathrm{mseq}(a,b)$ definiert durch $\mathrm{msm}(a,b) = 0 \wedge \mathrm{msm}(b,a) = 0$. Offenbar gilt dann $\mathrm{mseq}(\ulcorner\Gamma\urcorner, \ulcorner\Delta\urcorner)$ genau dann, wenn $\Gamma$ und $\Delta$ als Multimengen gleich sind. Wir schreiben kurz $a =_m b$ für $\mathrm{mseq}(a,b)$.

Eine Sequenz $\Gamma \Rightarrow A$ kodieren wir durch $\langle \ulcorner\Gamma\urcorner, \ulcorner A\urcorner\rangle$. Solche Kodifikate bezeichnen wir mit $\ulcorner\Gamma \Rightarrow A\urcorner$. Eine Herleitung oder genauer eine Konstruktionsfolge (siehe Kapitel 1.2) für die induktive Definition von $\vdash_m$ kodieren wir durch $\langle \ulcorner\Gamma_0 \Rightarrow A_0\urcorner, \ldots, \ulcorner\Gamma_n \Rightarrow A_n\urcorner\rangle$.

Wir definieren jetzt

$$
\begin{aligned}
&\mathrm{Herl}_m(d) :\leftrightarrow \forall i < \mathrm{lh}(d)(\\
&(\mathrm{Ann}) \quad (\forall m < \mathrm{lh}((d)_{i,0})\,\mathrm{For}((d)_{i,0,m}) \wedge \exists n < \mathrm{lh}((d)_{i,0})\,((d)_{i,1} = (d)_{i,0,n}))\\
&(\wedge\mathrm{I}) \quad \vee\, \exists j,k < i\,((d)_{i,1} = \langle \mathrm{SN}(\wedge), (d)_{j,1}, (d)_{k,1}\rangle \wedge (d)_{i,0} =_m (d)_{j,0} * (d)_{k,0})\\
&(\wedge\mathrm{E_r}) \quad \vee\, \exists j < i\,((d)_{j,1} = \langle \mathrm{SN}(\wedge), (d)_{i,1}, (d)_{j,1,2}\rangle \wedge (d)_{i,0} =_m (d)_{j,0})\\
&(\wedge\mathrm{E_l}) \quad \vee\, \exists j < i\,((d)_{j,1} = \langle \mathrm{SN}(\wedge), (d)_{j,1,1}, (d)_{i,1}\rangle \wedge (d)_{i,0} =_m (d)_{j,0})\\
&(\to\mathrm{I}) \quad \vee\, \exists j < i\,((d)_{i,1} = \langle \mathrm{SN}(\to), (d)_{i,1,1}, (d)_{j,1}\rangle \wedge \mathrm{For}((d)_{i,1,1})\\
&\qquad\qquad \wedge\, \mathrm{msm}((d)_{i,0}, (d)_{j,0}) = 0\\
&\qquad\qquad \wedge\, \forall n < \mathrm{lh}(\mathrm{msm}((d)_{j,0}, (d)_{i,0}))\,((\mathrm{msm}((d)_{j,0}, (d)_{i,0}))_n = (d)_{i,1,1}))\\
&(\to\mathrm{E}) \quad \vee\, \exists j,k < i\,((d)_{j,1} = \langle \mathrm{SN}(\to), (d)_{k,1}, (d)_{i,1}\rangle \wedge (d)_{i,0} =_m (d)_{j,0} * (d)_{k,0})\\
&(\forall\mathrm{I}) \quad \vee\, \exists j < i\,((d)_{i,1} = \langle \mathrm{SN}(\forall), (d)_{i,1,1}, (d)_{j,1}\rangle \wedge \mathrm{Var}((d)_{i,1,1}) \wedge (d)_{i,0} =_m (d)_{j,0}\\
&\qquad\qquad \wedge\, \forall n < \mathrm{lh}((d)_{i,0})\,\neg\mathrm{FV}((d)_{i,1,1}, (d)_{i,0,n}))\\
&(\forall\mathrm{E}) \quad \vee\, \exists j < i\,((d)_{j,1,0} = \mathrm{SN}(\forall) \wedge (d)_{i,0} =_m (d)_{j,0}\\
&\qquad\qquad \wedge\, ((d)_{i,1} = (d)_{j,1,2} \vee \exists n < (d)_{i,1}(\mathrm{Ter}(n) \wedge (d)_{i,1} = \mathrm{sub}((d)_{j,1,2}, \langle\langle (d)_{j,1,1}, n\rangle\rangle))))).
\end{aligned}
$$

**Lemma 3.3.** *a.* $\mathrm{Herl}_m(d)$ *gilt genau dann, wenn* $d$ *eine Herleitung kodiert.*

*b.* $\mathrm{Herl}_m$ *ist primitiv rekursiv.*

*Beweis.* a. $\Longrightarrow$. Gelte $\mathrm{Herl}_m(d)$. Man sieht dann leicht durch Induktion über $i$, daß für jedes $i < \mathrm{lh}(d)$ gilt $(d)_{i,0} = \ulcorner\Gamma\urcorner$ und $(d)_{i,1} = \ulcorner A\urcorner$ mit $\vdash_m \Gamma \Rightarrow A$.

$\Longleftarrow$. $d$ kodiere eine Herleitung, etwa $d = \langle \ulcorner\Gamma_0 \Rightarrow A_0\urcorner, \ldots, \ulcorner\Gamma_n \Rightarrow A_n\urcorner\rangle$. Durch Induktion über $n$ und Fallunterscheidung nach der zuletzt angewandten Regel zeigt man leicht, daß dann $\mathrm{Herl}_m(d)$ gilt.

b. Die primitive Rekursivität von $\mathrm{Herl}_m$ folgt unmittelbar aus der Definition. □

Eine Menge $S$ von Formeln heißt *rekursiv* (*primitiv rekursiv*, *rekursiv aufzählbar*), wenn $\ulcorner S\urcorner := \{\, \ulcorner A\urcorner \mid A \in S \,\}$ rekursiv (primitiv rekursiv, rekursiv aufzählbar) ist. Um auch die klassische Logik behandeln zu können, zeigen wir jetzt, daß die Menge $\mathrm{Stabax}_{\mathcal{L}}$

primitiv rekursiv ist, also die Menge der Formeln

$$\forall x_1, \ldots, x_n \, (\neg\neg R x_1 \ldots x_n \to R x_1 \ldots x_n). \tag{1}$$

mit $R \in \mathrm{Rel}_{\mathcal{L}}^{(n)}$. Offenbar können wir hier annehmen, daß $x_1, \ldots, x_n$ die ersten $n$ Variablen $*_0, \ldots, *_{n-1}$ sind. Wir definieren deshalb zunächst

$$\begin{aligned} &\mathrm{app}(a, 0) := \langle a \rangle, \\ &\mathrm{app}(a, n+1) := \mathrm{app}(a, n) * \langle\langle 0, n \rangle\rangle\rangle. \end{aligned}$$

Dann ist app primitiv rekursiv und wir haben $\mathrm{app}(\mathrm{SN}(R), n) = \ulcorner R *_0 \ldots *_{n-1} \urcorner$ und auch $\mathrm{app}(\mathrm{SN}(f), n) = \ulcorner f *_0 \ldots *_{n-1} \urcorner$. Weiter definieren wir

$$\begin{aligned} &\mathrm{gen}(0, a) := a, \\ &\mathrm{gen}(n+1, a) := \mathrm{gen}(n, \langle \mathrm{SN}(\forall), \langle\langle 0, n \rangle\rangle, a \rangle). \end{aligned}$$

Dann ist gen primitiv rekursiv und es gilt $\mathrm{gen}(n, \ulcorner A \urcorner) = \ulcorner \forall *_0 \ldots \forall *_{n-1} \; A \urcorner$. Setzt man noch $a \dot{\to} b := \langle \mathrm{SN}(\to), a, b \rangle$ und $\dot{\neg} a := a \dot{\to} \ulcorner \bot \urcorner$, so gilt

$$\begin{aligned} &\ulcorner \mathrm{Stabax}_{\mathcal{L}} \urcorner(a) \\ &\leftrightarrow \exists k < a \, (\mathrm{Symb}_{\mathcal{L}}(k) \wedge (k)_0 = 1 \wedge a = \mathrm{gen}((k)_1, \dot{\neg}\dot{\neg}\mathrm{app}(k, (k)_1) \dot{\to} \mathrm{app}(k, (k)_1))). \end{aligned}$$

Offenbar ist $\ulcorner \mathrm{Stabax}_{\mathcal{L}} \urcorner$ primitiv rekursiv.

Weiter zeigen wir, daß auch die Menge $\mathrm{Eq}_{\mathcal{L}}$ der $\mathcal{L}$–Gleichheitsaxiome primitiv rekursiv ist; hierbei setzen wir natürlich voraus, daß unsere primitiv rekursiv präsentierte Sprache $\mathcal{L}$ das Gleichheitssymbol $=$ enthält. Zum Beweis konstruiert man primitiv rekursive Hilfsfunktionen $\mathrm{app}_g, \mathrm{app}_u$ und $h$ mit

$$\begin{aligned} &\mathrm{app}_g(\mathrm{SN}(R), n) = \ulcorner R *_0 *_2 *_4 \ldots *_{2n-2} \urcorner, \qquad \mathrm{app}_g(\mathrm{SN}(f), n) = \ulcorner f *_0 *_2 *_4 \ldots *_{2n-2} \urcorner, \\ &\mathrm{app}_u(\mathrm{SN}(R), n) = \ulcorner R *_1 *_3 *_5 \ldots *_{2n-1} \urcorner, \qquad \mathrm{app}_u(\mathrm{SN}(f), n) = \ulcorner f *_1 *_3 *_5 \ldots *_{2n-1} \urcorner, \\ &h(n) = \ulcorner *_0 = *_1 \wedge *_2 = *_3 \wedge \cdots \wedge *_{2n-2} = *_{2n-1} \urcorner. \end{aligned}$$

Setzt man noch $a \dot{=} b := \langle \mathrm{SN}(=), a, b \rangle$ und $a \dot{\wedge} b := \langle \mathrm{SN}(\wedge), a, b \rangle$, so gilt

$$\begin{aligned} a \in \ulcorner \mathrm{Eq}_{\mathcal{L}} \urcorner \leftrightarrow a = {} & \ulcorner \forall *_0 \, (*_0 = *_0) \urcorner \\ & \vee a = \ulcorner \forall *_0, *_1 \, (*_0 = *_1 \to *_1 = *_0) \urcorner \\ & \vee a = \ulcorner \forall *_0, *_1, *_2 \, (*_0 = *_1 \wedge *_1 = *_2 \to *_0 = *_2) \urcorner \\ & \vee \exists k, n < a (\mathrm{Symb}_{\mathcal{L}}(k) \wedge (k)_0 = 1 \wedge (k)_1 = n > 0 \\ & \qquad \wedge a = \mathrm{gen}(2n, h(n) \dot{\wedge} \mathrm{app}_g(k, n) \dot{\to} \mathrm{app}_u(k, n))) \\ & \vee \exists k, n < a (\mathrm{Symb}_{\mathcal{L}}(k) \wedge (k)_0 = 2 \wedge (k)_1 = n > 0 \\ & \qquad \wedge a = \mathrm{gen}(2n, h(n) \dot{\to} \mathrm{app}_g(k, n) \dot{=} \mathrm{app}_u(k, n))). \end{aligned}$$

Offenbar ist $\ulcorner \mathrm{Eq}_{\mathcal{L}} \urcorner$ primitiv rekursiv.

Sei jetzt $\mathcal{L}$ eine primitiv rekursiv präsentierte Sprache mit $=$ in $\mathcal{L}$. Eine Theorie $T$ mit $L(T) \subseteq \mathcal{L}$ heißt *(primitiv) rekursiv axiomatisierbar*, wenn es eine (primitiv) rekursive Menge $S$ geschlossener $\mathcal{L}$–Formeln gibt so daß $T = \{ A \in \overline{\mathcal{L}} \mid S \cup \mathrm{Eq}_{\mathcal{L}} \vdash_c A \}$.

**Satz 3.4.** *Für Theorien $T$ mit $L(T) \subseteq \mathcal{L}$ sind die folgenden Aussagen äquivalent.*

a. *$T$ ist rekursiv axiomatisierbar.*

b. *$T$ ist primitiv rekursiv axiomatisierbar.*

c. *$T$ ist rekursiv aufzählbar.*

*Beweis.* c $\Longrightarrow$ b. Sei $\ulcorner T \urcorner$ rekursiv aufzählbar. Nach Lemma 2.1 existiert dann ein $f \in \mathrm{PR}^1$ mit $\ulcorner T \urcorner = \mathrm{ran}(f)$. Sei $f(n) = \ulcorner A_n \urcorner$. Wir definieren ein primitiv rekursives $g$ mit $g(n) = \ulcorner A_0 \wedge \cdots \wedge A_n \urcorner$ durch

$$\begin{aligned} g(0) &:= f(0), \\ g(n+1) &:= \langle \mathrm{SN}(\wedge), g(n), f(n+1) \rangle. \end{aligned}$$

Für $S := \{ A_0 \wedge \cdots \wedge A_n \mid n \in \mathbb{N} \}$ ist $\ulcorner S \urcorner = \mathrm{ran}(g)$, und diese Menge ist primitiv rekursiv wegen $a \in \mathrm{ran}(g) \leftrightarrow \exists n < a\, (a = g(n))$. $T$ ist also primitiv rekursiv axiomatisierbar, denn offenbar gilt $T = \{ A \in \overline{\mathcal{L}} \mid S \cup \mathrm{Eq}_{\mathcal{L}} \vdash_c A \}$.

b $\Longrightarrow$ a ist klar.

a $\Longrightarrow$ c. Sei $T$ axiomatisiert durch $S$ mit $\ulcorner S \urcorner$ rekursiv. Dann gilt

$$\begin{aligned} & a \in \ulcorner T \urcorner \\ & \leftrightarrow \exists d \exists c < d\, (\mathrm{Herl}_m(d) \wedge (d)_{\mathrm{lh}(d) \dot{-} 1} = \langle c, a \rangle \wedge \forall i < \mathrm{lh}(c)\, ((c)_i \in \ulcorner \mathrm{Stabax} \urcorner \cup \ulcorner \mathrm{Eq} \urcorner \cup \ulcorner S \urcorner)). \end{aligned}$$

Also ist $\ulcorner T \urcorner$ rekursiv aufzählbar. □

Eine Theorie $T$ in unserer primitiv rekursiv präsentierten Sprache $\mathcal{L}$ heißt *axiomatisiert*, wenn sie durch ein rekursiv aufzählbares Axiomensystem $\mathrm{Ax}_T$ gegeben ist. Nach Satz 3.4 können wir dann sogar annehmen, daß $\mathrm{Ax}_T$ primitiv rekursiv ist. Für solche axiomatisierten Theorien definieren wir $\mathrm{Abl}_T \subseteq \mathbb{N} \times \mathbb{N}$ durch

$$\begin{aligned} & \mathrm{Abl}_T(d, a) \\ & :\leftrightarrow \mathrm{Herl}_m(d) \wedge \exists c < d((d)_{\mathrm{lh}(d) \dot{-} 1} = \langle c, a \rangle \wedge \forall i < \mathrm{lh}(c)\, ((c)_i \in \ulcorner \mathrm{Stabax} \urcorner \cup \ulcorner \mathrm{Eq} \urcorner \cup \ulcorner \mathrm{Ax}_T \urcorner)). \end{aligned}$$

Offenbar ist $\mathrm{Abl}_T$ primitiv rekursiv und es gilt $\mathrm{Abl}_T(d, a)$ genau dann, wenn $d$ eine Herleitung einer Sequenz $\Gamma \Rightarrow A$ kodiert mit $a = \ulcorner A \urcorner$ und $\Gamma$ zusammengesetzt ist aus Stabilitätsaxiomen, Gleichheitsaxiomen und Formeln aus $\mathrm{Ax}_T$.

Eine Theorie $T$ heißt *konsistent*, wenn es eine geschlossene Formel $A$ gibt mit $A \notin T$; andernfalls heißt $T$ *inkonsistent*.

**Folgerung 3.5.** *Jede axiomatisierte vollständige Theorie $T$ ist rekursiv.*

*Beweis.* Ist $T$ inkonsistent, so ist $\ulcorner T \urcorner$ rekursiv. Andernfalls folgt aus der Vollständigkeit von $T$

$$a \in \mathbb{N} \setminus \ulcorner T \urcorner \leftrightarrow a \notin \mathrm{For} \vee \exists b < a\, FV(b, a) \vee \dot{\neg} a \in \ulcorner T \urcorner.$$

Also ist mit $\ulcorner T \urcorner$ auch $\mathbb{N} \setminus \ulcorner T \urcorner$ rekursiv aufzählbar und damit nach Lemma 2.3 $\ulcorner T \urcorner$ rekursiv. □

# 2.4 Herbrand–Gödel–Kleene–rekursive Funktionen

Wir geben in diesem Kapitel eine weitere, auf Herbrand, Gödel und Kleene zurückgehende Charakterisierung der rekursiven Funktionen. Diese Charakterisierung verwendet logische Herleitungen aus Gleichungssystemen und stellt deshalb eine Verbindung zwischen den Teilen I und II dieser Vorlesung dar. Als Anwendung beweisen wir die Existenz einer rekursiv aufzählbaren, aber nicht rekursiven Relation.

Unter einem *Gleichungssystem* verstehen wir eine endliche Menge von generalisierten Gleichungen, also von Formeln der Gestalt $\forall x_1, \ldots, x_n(t[x_1, \ldots, x_n] = s[x_1, \ldots, x_n])$. Wir setzen in diesem Abschnitt stets voraus, daß $0, \mathrm{suc}$ in der Sprache vorhanden sind.

Eine Funktion $f\colon \mathbb{N}^n \to \mathbb{N}$ heißt *Herbrand–Gödel–Kleene–rekursiv* (oder kurz: *HGK–rekursiv*), wenn es ein Gleichungssystem $E_f$ mit einem ausgezeichneten Funktionssymbol $\hat{f}$ gibt so daß für alle $a_1, \ldots, a_n, b \in \mathbb{N}$ gilt

$$f(a_1, \ldots, a_n) = b \quad \text{genau dann, wenn} \quad E_f \cup \mathrm{Eq} \vdash \hat{f}(\underline{a_1}, \ldots, \underline{a_n}) = \underline{b}.$$

**Satz 4.1.** *Jede $\mu$–rekursive Funktion ist HGK–rekursiv.*

*Beweis.* Durch Rekursion über die induktive Definition der $\mu$–rekursiven Funktionen $f$ konstruieren wir ein Gleichungssystem $E_f$ mit einem ausgezeichneten Funktionssymbol $\hat{f}$ so daß

1. $E_f$ nur die Funktionssymbole $0, \mathrm{suc}, \hat{\cdot}, \hat{q}$ sowie $\hat{g}, \widehat{\prod g}$ für jede in der Definition von $f$ vorkommende Funktion $g$ enthält,

2. $E_f$ in $\mathbb{N}$ gültig ist, wenn man 0 durch die Zahl 0, suc durch die Nachfolgerfunktion, $\hat{\cdot}$ durch die Multiplikation, $\hat{q}$ durch $q(\mathrm{suc}(a), 0, b) := b$ und beliebig sonst, jedes $\hat{g}$ durch $g$ und jedes $\widehat{\prod g}$ durch $b, \vec{a} \mapsto \prod_{c<b} g(c, \vec{a})$ interpretiert, und

3. für alle $a_1, \ldots, a_n, b \in \mathbb{N}$ gilt

$$f(a_1, \ldots, a_n) = b \quad \text{genau dann, wenn} \quad E_f \cup \mathrm{Eq} \vdash \hat{f}(\underline{a_1}, \ldots, \underline{a_n}) = \underline{b}.$$

Die Gültigkeit von 1–3 ergibt sich jeweils unmittelbar aus der im folgenden angegebenen Konstruktion, wobei man zum Beweis von $3 \Longleftarrow$ verwendet, daß 2 zutrifft. Bei Gleichungen lassen wir der Kürze halber die Generalisierungen immer weg.

*Fall* $0^n$. Wähle $\widehat{0^n}(x_1, \ldots, x_n) = 0$.

*Fall* suc. Wähle $\widehat{\mathrm{suc}}(x) = \mathrm{suc}(x)$.

*Fall* $I_i^n$. Wähle $\widehat{I_i^n}(x_1,\ldots,x_n) = x_i$.

*Fall* $(\circ h g_1 \ldots g_m)$. Nach IH haben wir $E_h, E_{g_1}, \ldots, E_{g_m}$ mit ausgezeichneten Funktionssymbolen $\hat{g_1}, \ldots, \hat{g_m}$. Wähle $E_h \cup E_{g_1} \cup \cdots \cup E_{g_m}$ zusammen mit der Generalisierung von

$$\hat{f}(x_1,\ldots,x_n) = \hat{h}(\hat{g_1}(x_1,\ldots,x_n),\ldots,\hat{g_m}(x_1,\ldots,x_n)).$$

*Fall* $(Rgh)$. Nach IH haben wir $E_g, E_h$ mit ausgezeichneten Funktionssymbolen $\hat{g}, \hat{h}$. Wähle $E_g \cup E_h$ zusammen mit den Generalisierungen von

$$\begin{aligned}
&\hat{f}(0, y_1,\ldots,y_n) = \hat{g}(y_1,\ldots,y_n),\\
&\hat{f}(\mathrm{suc}(x), y_1,\ldots,y_n) = \hat{h}(x, \hat{f}(x, y_1,\ldots,y_n), y_1,\ldots,y_n).
\end{aligned}$$

*Fall* $(\mu g)$. Nach IH haben wir $E_g$ mit ausgezeichnetem Funktionssymbol $\hat{g}$. Wähle $E_g$ zusammen mit den Generalisierungen von

$$\begin{aligned}
&\widehat{\Big(\prod g\Big)}(0, x_1,\ldots,x_n) = 1,\\
&\widehat{\Big(\prod g\Big)}(\mathrm{suc}(y), x_1,\ldots,x_n) = \hat{\cdot}\Big(\widehat{\Big(\prod g\Big)}(y, x_1,\ldots,x_n), \hat{g}(y, x_1,\ldots,x_n)\Big),\\
&\hat{q}(\mathrm{suc}(x), 0, y) = y,\\
&\hat{f}(x_1,\ldots,x_n) = \hat{q}\Big(\widehat{\Big(\prod g\Big)}(y, x_1,\ldots,x_n), \widehat{\Big(\prod g\Big)}(\mathrm{suc}(y), x_1,\ldots,x_n), y\Big). \qquad \square
\end{aligned}$$

Zum Beweis der Umkehrung definieren wir für jedes $n$ eine primitiv rekursive Relation $T_n \subseteq \mathbb{N}^{n+2}$ so daß für jedes Gleichungssystem $E$ mit ausgezeichnetem Funktionssymbol $\hat{f}$ mit Symbolnummer $\mathrm{SN}(\hat{f}) = \langle 2, n, 0\rangle$ gilt $T_n(\ulcorner E\urcorner, a_1,\ldots,a_n,d)$ genau dann, wenn $d$ eine Herleitung einer Sequenz $\Gamma \Rightarrow \hat{f}(\underline{a_1},\ldots,\underline{a_n}) = \underline{b}$ kodiert, wobei $\Gamma$ aus Stabilitätsaxiomen, Gleichheitsaxiomen und Elementen aus $E$ besteht. Ferner definieren wir eine primitiv rekursive Funktion $U\colon \mathbb{N} \to \mathbb{N}$, die aus einem solchen $d$ die Zahl $b$ abliest. Wir setzen

$$\begin{aligned}
T_n(e, a_1,\ldots,a_n,d) :\leftrightarrow\ & \mathrm{Herl}_m(d) \wedge \exists c, a, b < d(\\
& (d)_{\mathrm{lh}(d)\dot{-}1} = \langle c, a\rangle\\
& \wedge a = \langle \mathrm{SN}(=), \langle\langle 2, n, 0\rangle, \ulcorner\underline{a_1}\urcorner, \ldots, \ulcorner\underline{a_n}\urcorner\rangle, \ulcorner\underline{b}\urcorner\rangle\\
& \wedge \forall i < \mathrm{lh}(c)((c)_i \in \ulcorner\mathrm{Stabax}\urcorner \cup \ulcorner\mathrm{Eq}\urcorner \vee \exists j < \mathrm{lh}(e)((c)_i = (e)_j)))\\
U(d) :=\ & \mathrm{dec}((d)_{\mathrm{lh}(d)\dot{-}1,1,2}),
\end{aligned}$$

wobei dec eine primitiv rekursive Funktion ist mit $\mathrm{dec}(\ulcorner\underline{b}\urcorner) = b$; dec definieren wir durch $\mathrm{dec}(0) := 0$ und für $a > 0$

$$\mathrm{dec}(a) := \begin{cases} \mathrm{dec}((a)_1) + 1, & \text{falls } (a)_0 = \mathrm{SN}(\mathrm{suc});\\ 0, & \text{sonst.}\end{cases}$$

Nach Konstruktion sind $T_n$ und $U$ primitiv rekursiv und haben die verlangten Eigenschaften. Deshalb gilt offenbar folgender Satz.

**Satz 4.2 (Kleenesches Normalformentheorem).** *Zu jeder HGK–rekursiven $n$–stelligen Funktion $f$ gibt es ein $e \in \mathbb{N}$ so daß folgendes gilt.*

a. $\forall a_1, \ldots, a_n \exists d\, T_n(e, a_1, \ldots, a_n, d)$

b. $f(a_1, \ldots, a_n) = U(\mu d\, T_n(e, a_1, \ldots, a_n, d))$ □

Insbesondere ergibt sich hieraus, daß jede $\mu$–rekursive Funktion mit einem geeigneten $e$ in der angegebenen Form definiert werden kann, wobei der $\mu$–Operator nur einmal angewandt wird. Dies erklärt den Namen "Normalformentheorem".

**Folgerung 4.3.** *Jede HGK–rekursive Funktion ist $\mu$–rekursiv.* □

Wir kommen nun noch einmal auf den Fall $(\mu g)$ mit $g$ $\mu$–rekursiv zurück, aber jetzt ohne vorauszusetzen, daß $\forall \vec{a} \exists i\, g(i, \vec{a}) = 0$. Sei $E$ das oben im Fall $(\mu g)$ angegebene Gleichungssystem. Dann gilt: (1) Wenn $\exists i\, g(i, \vec{a}) = 0$, so ist $E \cup \mathrm{Eq} \vdash \hat{f}(\underline{a_1}, \ldots, \underline{a_n}) = \underline{i}$ für das kleinste $i$ mit $g(i, \vec{a}) = 0$. (2) Gilt $E \cup \mathrm{Eq} \vdash \hat{f}(\underline{a_1}, \ldots, \underline{a_n}) = \underline{i}$, so ist $g(i, \vec{a}) = 0$ und für $j < i$ ist $g(j, \vec{a}) = 0$. Daraus ergibt sich aufgrund der Definition von $T_n$:

**Satz 4.4 (Kleenesches Aufzählungstheorem).** *Zu jeder rekursiven Relation $R \subseteq \mathbb{N}^{n+1}$ findet man eine Zahl $e$ so daß für alle $a_1, \ldots, a_n \in \mathbb{N}$ gilt*

$$\exists b\, R(b, a_1, \ldots, a_n) \leftrightarrow \exists d\, T_n(e, a_1, \ldots, a_n, d). \qquad \square$$

Die Relationen $\{\, (a_1, \ldots, a_n) \mid \exists d\, T_n(e, a_1, \ldots, a_n, d) \,\}$ durchlaufen also für $e = 0, 1, \ldots$ genau die $n$–stelligen rekursiv aufzählbaren Relationen. Sei jetzt $n = 1$. Mit dem Cantorschen Diagonalargument folgt dann, daß $\{\, a \mid \neg \exists d\, T_1(a, a, d) \,\}$ *nicht* rekursiv aufzählbar sein kann. Andernfalls gäbe es nämlich ein $e$ so daß für alle $a$ gilt

$$\neg \exists d\, T_1(a, a, d) \leftrightarrow \exists d\, T_1(e, a, d),$$

und durch Einsetzung von $e$ für $a$ erhielte man einen Widerspruch. Da nach Lemma 2.3 eine rekursiv aufzählbare Relation genau dann rekursiv ist, wenn ihr Komplement rekursiv aufzählbar ist, erhalten wir:

**Satz 4.5.** $\{\, a \mid \exists d\, T_1(a, a, d) \,\}$ *ist rekursiv aufzählbar, aber nicht rekursiv.* □

Setzt man die Churchsche These voraus, so haben wir damit ein erstes Beispiel eines *unentscheidbaren Problems* gefunden: Es kann keinen Algorithmus geben, der für ein beliebiges $a \in \mathbb{N}$ stets terminiert und entscheidet, ob es ein $d \in \mathbb{N}$ gibt so daß die primitiv rekursive Relation $T_1(a, a, d)$ besteht.

# Teil III: Metamathematik

## 3.1 Undefinierbarkeit des Wahrheitsbegriffs

Sei $\mathcal{M}$ eine $\mathcal{L}$–Struktur. Eine Relation $R \subseteq |\mathcal{M}|^n$ heißt in $\mathcal{M}$ *definierbar*, wenn es eine $\mathcal{L}$–Formel $A[x_1, \ldots, x_n]$ gibt so daß

$$R = \{\, (a_1, \ldots, a_n) \in |\mathcal{M}|^n \mid \mathcal{M} \models A[a_1, \ldots, a_n / x_1, \ldots, x_n] \,\}.$$

Wir wollen in diesem Kapitel annehmen, daß $|\mathcal{M}| = \mathbb{N}$ und $0 \in \mathrm{Fun}^{(0)}_{\mathcal{L}}$, $\mathrm{suc} \in \mathrm{Fun}^{(1)}_{\mathcal{L}}$ mit $0^{\mathcal{M}} = 0$ und $\mathrm{suc}^{\mathcal{M}}(a) = a + 1$. Dann kann man für jedes $a \in \mathbb{N}$ die *Ziffer* $\underline{a} \in \mathrm{Ter}_{\mathcal{L}}$ definieren durch $\underline{0} := 0$ und $\underline{n+1} := \mathrm{suc}(\underline{n})$. Man beachte auch, daß in diesem Fall die Definierbarkeit von $R \subseteq \mathbb{N}^n$ durch $A[x_1, \ldots, x_n]$ äquivalent ist zu

$$R = \{\, (a_1, \ldots, a_n) \in \mathbb{N}^n \mid \mathcal{M} \models A[\underline{a_1}, \ldots, \underline{a_n}] \,\}.$$

Sei weiter $\mathcal{L}$ eine primitiv rekursiv präsentierte Sprache. Wir werden in diesem Kapitel stets voraussetzen, jede primitiv rekursive Relation in $\mathcal{M}$ definierbar ist. Ein Beispiel für eine solche Situation ist die in Kapitel II.2.1 eingeführte Standardstruktur $\mathcal{N}$ zur Sprache PR. Eine Menge $S$ von Formeln heißt *definierbar* in $\mathcal{M}$, wenn $\ulcorner S \urcorner := \{\, \ulcorner A \urcorner \mid A \in S \,\}$ in $\mathcal{M}$ definierbar ist.

Wir zeigen, daß bereits aus diesen recht schwachen Voraussetzungen folgt, daß der *Wahrheitsbegriff* von $\mathcal{M}$, genauer die Menge $\mathrm{Th}(\mathcal{M})$ aller in $\mathcal{M}$ gültigen geschlossenen Formeln, nicht in $\mathcal{M}$ definierbar ist. Da aus der vorausgesetzten Definierbarkeit aller primitiv rekursiven Relationen in $\mathcal{M}$ sofort folgt, daß auch alle rekursiven aufzählbaren Relationen in $\mathcal{M}$ definierbar sind, erhält man hieraus mit der Churchschen These, daß der Wahrheitsbegriff von $\mathcal{M}$ nicht aufzählbar sein kann und folglich insbesondere unentscheidbar ist.

Zum Beweis benötigen wir das folgende Fixpunktlemma, das wir im nächsten Kapitel noch verallgemeinern werden.

**Lemma 1.1 (Semantisches Fixpunktlemma).** *Ist jede primitiv rekursive Relation in $\mathcal{M}$ definierbar, so findet man zu jeder $\mathcal{L}$–Formel $B[z]$ eine geschlossene $\mathcal{L}$–Formel $A$ mit*

$$\mathcal{M} \models A \quad \textit{genau dann, wenn} \quad \mathcal{M} \models B[\ulcorner A \urcorner].$$

*Beweis.* Wir definieren eine primitiv rekursive Funktion $s$ durch

$$s(b, k) := \mathrm{sub}(b, \langle\langle \ulcorner z \urcorner, \ulcorner \underline{k} \urcorner \rangle\rangle).$$

$z$ ist hierbei die spezielle, durch $B[z]$ vorgegebene Variable, etwa $*_0$. Dann gilt für jede Formel $C[z]$

$$s(\ulcorner C \urcorner, k) = \mathrm{sub}(\ulcorner C \urcorner, \ulcorner z \urcorner, \ulcorner \underline{k} \urcorner) = \ulcorner C[\underline{k}] \urcorner,$$

also insbesondere

$$s(\ulcorner C\urcorner, \ulcorner C\urcorner) = \ulcorner C[\underline{\ulcorner C\urcorner}]\urcorner.$$

Nach Annahme ist der Graph $G_s$ von $s$ definierbar in $\mathcal{M}$, etwa durch $A_s[x_1, x_2, x_3]$. Setze

$$\begin{aligned} C &:= \exists x\,(B[x] \wedge A_s[z, z, x]), \\ A &:= C[\underline{\ulcorner C\urcorner}], \end{aligned}$$

also

$$A = \exists x\,(B[x] \wedge A_s[\underline{\ulcorner C\urcorner}, \underline{\ulcorner C\urcorner}, x]).$$

Damit gilt

$$\begin{aligned} \mathcal{M} \models A \quad &\text{genau dann, wenn} \quad \exists a \in \mathbb{N}\,(\mathcal{M} \models B[a] \text{ und } a = \ulcorner C[\underline{\ulcorner C\urcorner}]\urcorner) \\ &\text{genau dann, wenn} \quad \mathcal{M} \models B[\ulcorner A\urcorner]. \end{aligned}$$

□

**Satz 1.2.** *Ist jede primitiv rekursive Relation in $\mathcal{M}$ definierbar, so ist* $\mathrm{Th}(\mathcal{M})$ *in $\mathcal{M}$ undefinierbar, insbesondere also nicht rekursiv aufzählbar.*

*Beweis.* Nehmen wir also an, $\ulcorner \mathrm{Th}(\mathcal{M})\urcorner$ wäre definierbar durch $B_W[z]$. Dann gilt für alle geschlossenen Formeln $A$

$$\mathcal{M} \models A \quad \text{genau dann, wenn} \quad \mathcal{M} \models B_W[\ulcorner A\urcorner].$$

Wir betrachten nun die Formel $\neg B_W[z]$ und wählen uns nach dem Fixpunktlemma 1.1 eine geschlossene $\mathcal{L}$–Formel $A$ mit

$$\mathcal{M} \models A \quad \text{genau dann, wenn} \quad \mathcal{M} \models \neg B_W[\ulcorner A\urcorner].$$

Dies widerspricht aber der obigen Äquivalenz.

Bereits oben hatten wir bemerkt, daß alle rekursiv aufzählbaren Relationen in $\mathcal{M}$ definierbar sind und deshalb folgt, daß $\ulcorner \mathrm{Th}(\mathcal{M})\urcorner$ nicht rekursiv aufzählbar ist. □

## 3.2 Der Wahrheitsbegriff in formalen Theorien

Wir wollen jetzt den Begriff der Herleitbarkeit ins Spiel bringen, der im vorangehenden Kapitel nicht vorkam. Genauer wollen wir die Überlegungen dort übertragen auf die Situation, wo wir an die Stelle der Definierbarkeit in $\mathcal{M}$ die "Repräsentierbarkeit" innerhalb einer formalen Theorie setzen. Es wird sich zeigen, daß wir zu ganz entsprechenden Resultaten kommen, die sich jetzt aber nicht mehr auf den semantisch definierten Wahrheitsbegriff in einer Struktur $\mathcal{M}$ beziehen, sondern auf die syntaktisch bestimmten Sätze einer formalen Theorie.

Sei im folgenden $\mathcal{L}$ wieder eine primitiv rekursiv präsentierte Sprache mit $0, \mathrm{suc}, =$ in $\mathcal{L}$ und $T$ eine Theorie mit $\mathrm{Eq}_{\mathcal{L}} \subseteq T$. Wir nennen eine Relation $R \subseteq \mathbb{N}^n$ *repräsentierbar* in $T$, wenn es eine Formel $A[x_1, \ldots, x_n]$ gibt mit

$$T \vdash A[\underline{a_1}, \ldots, \underline{a_n}], \quad \text{falls } (a_1, \ldots, a_n) \in R,$$
$$T \vdash \neg A[\underline{a_1}, \ldots, \underline{a_n}], \quad \text{falls } (a_1, \ldots, a_n) \notin R.$$

Eine Funktion $f\colon \mathbb{N}^n \to \mathbb{N}$ heißt *repräsentierbar* in $T$, wenn es eine Formel $A[x_1, \ldots, x_n, y]$ gibt, die den Graphen $G_f \subseteq \mathbb{N}^{n+1}$ repräsentiert, also die

$$T \vdash A[\underline{a_1}, \ldots, \underline{a_n}, \underline{f(a_1, \ldots, a_n)}], \tag{1}$$
$$T \vdash \neg A[\underline{a_1}, \ldots, \underline{a_n}, \underline{c}], \quad \text{falls } c \neq f(a_1, \ldots, a_n) \tag{2}$$

erfüllt, und für die zusätzlich gilt

$$T \vdash A[\underline{a_1}, \ldots, \underline{a_n}, y] \wedge A[\underline{a_1}, \ldots, \underline{a_n}, z] \to y = z \quad \text{für alle } a_1, \ldots, a_n \in \mathbb{N}. \tag{3}$$

Man beachte, daß für den Fall $T \vdash \underline{b} \neq \underline{c}$ für $b < c$ die Bedingung (2) aus (1) und (3) folgt.

**Lemma 2.1.** *Ist die charakteristische Funktion $1_R$ einer Relation $R \subseteq \mathbb{N}^n$ in $T$ repräsentierbar, so auch die Relation $R$ selbst.*

*Beweis.* OBdA sei $n = 1$. Sei $A[x, y]$ eine $1_R$ repräsentierende Formel. Wir zeigen, daß dann $A[x, \underline{1}]$ die Relation $R$ repräsentiert. Sei also zunächst $a \in R$. Dann ist $1_R(a) = 1$, also $(a, 1) \in G_{1_R}$, also $T \vdash A[\underline{a}, \underline{1}]$. Sei nun $a \notin R$. Dann ist $1_R(a) = 0$, also $(a, 1) \notin G_{1_R}$, also $T \vdash \neg A[\underline{a}, \underline{1}]$. □

**Lemma 2.2 (Fixpunktlemma).** *Sind alle primitiv rekursiven Funktionen in $T$ repräsentierbar, so findet man zu jeder Formel $B[z]$ eine geschlossene Formel $A$ mit*

$$T \vdash A \leftrightarrow B[\underline{\ulcorner A \urcorner}].$$

*Beweis.* Sei $A_s[x_1, x_2, x_3]$ eine die primitiv rekursive Funktion $s(b,k) := \mathrm{sub}(b, \langle\langle \ulcorner z \urcorner, \ulcorner \underline{k} \urcorner\rangle\rangle)$ repräsentierende Formel. Setze

$$C := \exists x\,(B[x] \wedge A_s[z,z,x]),$$
$$A := C[\underline{\ulcorner C \urcorner}],$$

also

$$A = \exists x\,(B[x] \wedge A_s[\underline{\ulcorner C \urcorner}, \underline{\ulcorner C \urcorner}, x]).$$

Wegen $s(\ulcorner C \urcorner, \ulcorner C \urcorner) = \ulcorner C[\underline{\ulcorner C \urcorner}] \urcorner = \ulcorner A \urcorner$ ist in $T$ herleitbar

$$A_s[\underline{\ulcorner C \urcorner}, \underline{\ulcorner C \urcorner}, x] \leftrightarrow x = \underline{\ulcorner A \urcorner},$$

also nach Definition von $A$ auch

$$A \leftrightarrow \exists x\,(B[x] \wedge x = \underline{\ulcorner A \urcorner})$$

und damit

$$A \leftrightarrow B[\underline{\ulcorner A \urcorner}].$$ □

Mit $T = \mathrm{Th}(\mathcal{M})$ ergibt sich das obige (semantische) Fixpunktlemma 1.1 als Spezialfall.

**Satz 2.3.** *Sei $T$ eine konsistente Theorie, in der alle primitiv rekursiven Funktionen repräsentierbar sind. Dann kann es keine Formel $B[z]$ geben so daß für alle geschlossenen Formeln $A$ gilt*

$$T \vdash A \leftrightarrow B[\underline{\ulcorner A \urcorner}].$$

*Beweis.* Angenommen, wir hätten so ein $B[z]$. Wir betrachten nun die Formel $\neg B[z]$ und wählen nach dem Fixpunktlemma 2.2 eine geschlossene Formel $A$ mit

$$T \vdash A \leftrightarrow \neg B[\underline{\ulcorner A \urcorner}].$$

Für dieses $A$ hätte man also $T \vdash A \leftrightarrow \neg A$ im Widerspruch zur Konsistenz von $T$. □

Mit $T = \mathrm{Th}(\mathcal{M})$ ergibt sich wieder der obige Satz 1.2 als Spezialfall.

## 3.3 Unentscheidbarkeit, Unvollständigkeit

In diesem Kapitel betrachten wir eine konsistente formale Theorie, in der alle rekursiven Funktionen repräsentierbar sind. Dies ist eine sehr schwache Voraussetzung, wie wir im nächsten Kapitel zeigen werden. Sie ist erfüllt, sobald die Theorie ein gewisses Minimum an Arithmetik zu beweisen gestattet.

Wir zeigen, daß eine solche Theorie notwendigerweise unentscheidbar ist. Weiter zeigen wir den ersten Gödelschen Unvollständigkeitssatz, der aussagt, daß eine axiomatisierte derartige Theorie immer unvollständig sein muß. Diesen Satz beweisen wir dann noch in einer von J.B. Rosser verschärften Form, in der eine geschlossene Formel $A$ angegeben wird, so daß weder $A$ noch $\neg A$ in der Theorie beweisbar ist.

In diesem Kapitel sei $\mathcal{L}$ wieder eine primitiv rekursiv präsentierte Sprache mit $0, \mathrm{suc}, =$ in $\mathcal{L}$ und $T$ eine Theorie mit $\mathrm{Eq}_{\mathcal{L}} \subseteq T$.

**Satz 3.1 (Unentscheidbarkeit).** *Ist $T$ eine konsistente Theorie, in der alle rekursiven Funktionen repräsentierbar sind, so ist $T$ nicht rekursiv.*

*Beweis.* Nehmen wir an, $T$ ist rekursiv. Nach Voraussetzung ist dann $\ulcorner T \urcorner$ durch eine Formel $B[z]$ in $T$ repräsentierbar. Wir wählen nach dem Fixpunktlemma 2.2 eine geschlossene Formel $A$ mit

$$T \vdash A \leftrightarrow \neg B[\underline{\ulcorner A \urcorner}]$$

und zeigen (1) $T \nvdash A$ und (2) $T \vdash A$; dies ist der gewünschte Widerspruch.

Zu (1). Gelte $T \vdash A$. Dann ist $A \in T$, also $\ulcorner A \urcorner \in \ulcorner T \urcorner$ und damit $T \vdash B[\underline{\ulcorner A \urcorner}]$ (da ja $B[z]$ die Menge $\ulcorner T \urcorner$ in $T$ repräsentiert). Es folgt $T \vdash \neg A$ nach Wahl von $A$ und damit ein Widerspruch zur Konsistenz von $T$.

Zu (2). Nach (1) wissen wir $T \nvdash A$. Daher ist $A \notin T$, also $\ulcorner A \urcorner \notin \ulcorner T \urcorner$ und damit $T \vdash \neg B[\underline{\ulcorner A \urcorner}]$. Es folgt $T \vdash A$ nach Wahl von $A$. □

**Satz 3.2 (Erster Gödelscher Unvollständigkeitssatz).** *Jede axiomatisierte konsistente Theorie, in der alle rekursiven Funktionen repräsentierbar sind, ist unvollständig.*

*Beweis.* Folgerung II.3.5 und Satz 3.1. □

Wie oben schon erwähnt, wollen wir jetzt unter Verwendung einer Idee von J.B. Rosser den Unvollständigkeitssatz in dem Sinn verschärfen, daß wir tatsächlich eine geschlossene Formel $A$ angegeben, so daß weder $A$ noch $\neg A$ in der Theorie beweisbar ist.

**Satz 3.3 (Gödel–Rosser).** *Sei $T$ eine axiomatisierte konsistente $\mathcal{L}$–Theorie mit $0, \mathrm{suc}, =$ in $\mathcal{L}$ und $\mathrm{Eq}_{\mathcal{L}} \subseteq T$. Ferner gebe es eine Formel $K[x, y]$ — geschrieben $x < y$ — so daß*

$$T \vdash \forall x\,(x < \underline{n} \rightarrow x = \underline{0} \vee \cdots \vee x = \underline{n-1}), \qquad (*)$$

$$T \vdash \forall x\,(x = \underline{0} \vee \cdots \vee x = \underline{n} \vee \underline{n} < x). \qquad (**)$$

*Ferner sei jede primitiv rekursive Funktion in $T$ repräsentierbar. Dann findet man eine geschlossene Formel $A$ so daß weder $A$ noch $\neg A$ in $T$ beweisbar ist.*

*Beweis.* Wir definieren zunächst $\mathrm{Wdl}_T \subseteq \mathbb{N} \times \mathbb{N}$ durch

$$\mathrm{Wdl}_T(d, a) :\leftrightarrow \mathrm{Abl}_T(d, \dot{\neg} a).$$

Dann ist $\mathrm{Wdl}_T$ primitiv rekursiv, und es gilt $\mathrm{Wdl}_T(d, a)$ genau dann, wenn $d$ eine Widerlegung von $a$ in $T$ ist, d.h. wenn $d$ eine Herleitung einer Sequenz $\Gamma \Rightarrow \neg A$ kodiert mit $a = \ulcorner \neg A \urcorner$ und $\Gamma$ zusammengesetzt aus Stabilitätsaxiomen und Formeln aus $\mathrm{Ax}_T$. Seien $B_{\mathrm{Abl}_T}[x_1, x_2]$ und $B_{\mathrm{Wdl}_T}[x_1, x_2]$ repräsentierende Formeln zu $\mathrm{Abl}_T$ und $\mathrm{Wdl}_T$. Man wähle nun nach dem Fixpunktlemma 2.2 eine geschlossene Formel $A$ mit

$$T \vdash A \leftrightarrow \forall x \, (B_{\mathrm{Abl}_T}[x, \underline{\ulcorner A \urcorner}] \to \exists y \, (y < x \wedge B_{\mathrm{Wdl}_T}[y, \underline{\ulcorner A \urcorner}])).$$

$A$ drückt also seine eigene Unbeweisbarkeit aus, und zwar in der (auf Rosser zurückgehenden) Form "Zu jedem Beweis von mir gibt es einen kürzeren Beweis meiner Negation".

Wir zeigen (1) $T \nvdash A$ und (2) $T \nvdash \neg A$. Zu (1). Gelte $T \vdash A$. Man wähle ein $n$ mit

$$\mathrm{Abl}_T(n, \ulcorner A \urcorner).$$

Dann gilt auch

$$\text{nicht } \mathrm{Wdl}_T(m, \ulcorner A \urcorner) \quad \text{für alle } m,$$

da $T$ konsistent ist. Folglich haben wir

$$\begin{aligned} &T \vdash B_{\mathrm{Abl}_T}[\underline{n}, \underline{\ulcorner A \urcorner}], \\ &T \vdash \neg B_{\mathrm{Wdl}_T}[\underline{m}, \underline{\ulcorner A \urcorner}] \quad \text{für alle } m. \end{aligned}$$

Daraus folgt

$$T \vdash B_{\mathrm{Abl}_T}[\underline{n}, \underline{\ulcorner A \urcorner}] \wedge \forall y \, (y < \underline{n} \to \neg B_{\mathrm{Wdl}_T}[y, \underline{\ulcorner A \urcorner}]),$$

denn wir haben $T \vdash \forall x \, (x < \underline{n} \to x = \underline{0} \vee \cdots \vee x = \underline{n-1})$ vorausgesetzt. Also gilt

$$\begin{aligned} &T \vdash \exists x \, (B_{\mathrm{Abl}_T}[x, \underline{\ulcorner A \urcorner}] \wedge \forall y \, (y < x \to \neg B_{\mathrm{Wdl}_T}[y, \underline{\ulcorner A \urcorner}])), \\ &T \vdash \neg A. \end{aligned}$$

Dies ist ein Widerspruch zur Konsistenz von $T$.

Zu (2). Gelte $T \vdash \neg A$. Man wähle ein $n$ mit

$$\mathrm{Wdl}_T(n, \ulcorner A \urcorner).$$

Dann gilt auch

$$\text{nicht } \mathrm{Abl}_T(m, \ulcorner A \urcorner) \quad \text{für alle } m,$$

da $T$ konsistent ist. Folglich haben wir

$$T \vdash B_{\mathrm{Wdl}_T}[\underline{n}, \underline{\ulcorner A \urcorner}],$$
$$T \vdash \neg B_{\mathrm{Abl}_T}[\underline{m}, \underline{\ulcorner A \urcorner}] \quad \text{für alle } m.$$

Daraus erhält man aber

$$T \vdash \forall x\,(B_{\mathrm{Abl}_T}[x, \underline{\ulcorner A \urcorner}] \to \exists y\,(y < x \wedge B_{\mathrm{Wdl}_T}[y, \underline{\ulcorner A \urcorner}])),$$

wie man durch Fallunterscheidung nach $x$ mit Hilfe der Voraussetzung $T \vdash \forall x\,(x = \underline{0} \vee \cdots \vee x = \underline{n} \vee \underline{n} < x)$ leicht beweist. Also gilt

$$T \vdash A.$$

Dies ist wieder ein Widerspruch zur Konsistenz von $T$. □

Schließlich wollen wir noch eine Variante dieses Satzes formulieren, in der wir nicht mehr davon ausgehen, daß die Theorie $T$ nur etwas über Zahlen aussagt.

**Satz 3.4 (Gödel–Rosser).** *Sei $T$ eine axiomatisierte konsistente $\mathcal{L}$–Theorie mit $0, \mathrm{suc}, =$ in $\mathcal{L}$ und $\mathrm{Eq}_{\mathcal{L}} \subseteq T$. Ferner gebe es Formeln $N[x]$ und $K[x, y]$ — geschrieben $Nx$ bzw. $x < y$ — so daß $T \vdash N0$, $T \vdash \forall x \in N\, N[\mathrm{suc}(x)]$ und*

$$T \vdash \forall x \in N\,(x < \underline{n} \to x = \underline{0} \vee \cdots \vee x = \underline{n-1}), \qquad (*)$$
$$T \vdash \forall x \in N\,(x = \underline{0} \vee \cdots \vee x = \underline{n} \vee \underline{n} < x). \qquad (**)$$

*Hierbei steht $\forall x \in N\, A$ für $\forall x\,(Nx \to A)$. Ferner sei jede primitiv rekursive Funktion in $T$ repräsentierbar. Dann findet man eine geschlossene Formel $A$ so daß weder $A$ noch $\neg A$ in $T$ beweisbar ist.*

*Beweis.* Wie für den Satz 3.3; man muß lediglich die auftretenden Quantoren auf $N$ relativieren. □

## 3.4 Repräsentierbarkeit

Wir zeigen in diesem Kapitel, daß schon recht einfache formale Theorien die Eigenschaft besitzen, daß in ihnen jede rekursive Funktion repräsentierbar ist. Als Hilfsmittel für den Beweis zeigen wir zunächst, daß die Menge der rekursiven Funktionen auch ohne das Schema der primitiven Rekursion alleine durch Komposition und den unbeschränkten $\mu$–Operator aus einfachen Ausgangsfunktionen erzeugt werden kann.

Wir definieren die Menge $\mathcal{G}$ der *$\mu$–rekursiven* Funktionen als die kleinste Menge von Funktionen mit den folgenden Eigenschaften. Wir schreiben $\mathcal{G}^n$ für die Teilmenge der $n$–stelligen Funktionen in $\mathcal{G}$.

a. $0^n \in \mathcal{G}^n$ $(n \geq 0)$, $\mathrm{suc} \in \mathcal{G}^1$, $I_i^n \in \mathcal{G}^n$ $(1 \leq i \leq n)$, $+, \cdot, 1_< \in \mathcal{G}^2$.

b. Sind $g_1, \ldots, g_m \in \mathcal{G}^n$, $h \in \mathcal{G}^m$ und $m, n \geq 1$, so ist $(\circ h g_1 \ldots g_m) \in \mathcal{G}^n$.

c. Ist $g \in \mathcal{G}^{n+1}$ und gilt $\forall \vec{a} \exists i\, (g(i, \vec{a}) = 0)$, so ist $\mu g$ in $\mathcal{G}^n$.

**Lemma 4.1.** *Die Funktionen $\dot{-}$ sowie $\pi, \pi_1, \pi_2$ sind $\mu$–rekursiv.*

*Beweis.* $a \dot{-} b = \mu i\, (a < i + b + 1)$. Es war $\pi(a, b) = \frac{1}{2}(a + b)(a + b + 1) + a$. Zum Beweis von $\pi \in \mathcal{G}$ genügt es offenbar, ein $h \in \mathcal{G}$ zu finden mit $h(2c) = c$. Eine solche Funktion ist $h(d) := \mu i\, (d < 2i + 1)$.

Wir zeigen jetzt $\pi_1 \in \mathcal{G}^1$. Dazu beachte man, daß

$$2\pi(a, b) = (a + b)(a + b + 1) + 2a. \tag{1}$$

Nun gilt

$$(a + b)(a + b + 1) \leq (a + b)(a + b + 1) + 2a < (a + b + 1)(a + b + 2).$$

Setzt man also

$$g(c) := \mu i\, (2c < (i + 1)(i + 2)),$$

so ist $g(\pi(a, b)) = a + b$. Wegen (1) können wir also aus $c := \pi(a, b)$ die Zahl $2a$ gewinnen als $2c - g(c)(g(c) + 1)$. Damit gilt

$$\pi_1(c) = h(2c \dot{-} g(c)(g(c) + 1))$$

und wir haben $\pi_1 \in \mathcal{G}$ gezeigt.

$\pi_2 \in \mathcal{G}$ folgt jetzt aus $\pi_2(c) = g(c) \dot{-} \pi_1(c)$. □

**Lemma 4.2 (Gödel).** *Die im Beweis definierte $\mu$–rekursive Funktion $\beta$ hat folgende Eigenschaft. Zu beliebigen $a_0, \ldots, a_{n-1}$ findet man ein $c$ mit $\beta(c,i) = a_i$ für alle $i < n$.*

*Beweis.* Sei

$$a := \max_{i<n} \pi(a_i, i).$$

Man beachte zunächst, daß alle $1 + ka!$ für $k \leq a$ relativ prim sind. Hätten nämlich $1 + ia!$ und $1 + ja!$ mit $i < j \leq a$ einen gemeinsamen Primteiler $p$, so wäre $p|(j-i)a!$, also auch $p|a!$ und damit $p|1$, was nicht sein kann.

Wir setzen jetzt

$$\begin{aligned} b &:= a!, \\ d &:= \prod_{i<n} (1 + \pi(a_i, i)a!). \end{aligned}$$

Aus $b$ und $d$ kann man zu gegebenem $i < n$ die Zahl $a_i$ wie folgt wiedergewinnen. Man betrachte das kleinste $x$ mit

$$1 + \pi(x, i)b|d.$$

Offenbar ist $a_i$ ein solches $x$. Würde nun ein $x < a_i$ die Bedingung auch erfüllen, so wäre wegen $\pi(x,i) < a$ und der Tatsache, daß alle $1 + ka!$ für $k \leq a$ relativ prim sind, $\pi(x,i) = \pi(a_j, j)$ für ein $j < n$ nach Konstruktion von $d$, also $x = a_j$ und $i = j$ im Widerspruch zu $x < a_i$.

Wir können also definieren

$$\beta(c,i) := \pi_2(\mu y\,[(1 + \pi(\pi_1(y), i) \cdot \pi_1(c)) \cdot \pi_2(y) \geq \pi_2(c)]).$$

Diese Funktion heißt *Gödelsche $\beta$–Funktion.* $\beta$ ist $\mu$–rekursiv, denn für jedes $c, i$ existiert offenbar ein solches $y$. Für $c := \pi(b,d)$ ist dann $\pi(a_i, \lceil d/1 + \pi(a_i,i)b \rceil)$ das kleinste solche $y$ und wir haben $\beta(c,i) = a_i$. □

**Satz 4.3.** *Die Menge der $\mu$–rekursiven Funktionen ist abgeschlossen unter primitiver Rekursion.*

*Beweis.* Sei $g \in \mathcal{G}^n$, $h \in \mathcal{G}^{n+2}$ und $f = (Rgh)$. Nach dem vorangehenden Lemma findet man zu gegebenen $a, \vec{b}$ ein $c$ mit $\beta(c,i) = f(i, \vec{b})$ für alle $i \leq a$, also

$$\begin{aligned} &\beta(c,0) = g(\vec{b}), \\ &\beta(c,i+1) = h(i, \beta(c,i), \vec{b}) \quad \text{für alle } i < a. \end{aligned}$$

Setze

$$\begin{aligned} |a-b| &:= (a \dot{-} b) + (b \dot{-} a), \\ h_1(a, \vec{b}, c) &:= \mu i\,((a \dot{-} i)(1 \dot{-} |h(i, \beta(c,i), \vec{b}) - \beta(c, i+1)|) = 0), \\ h_2(a, \vec{b}, c) &:= |g(\vec{b}) - \beta(c,0)| + (a \dot{-} h_1(a, \vec{b}, c)). \end{aligned}$$

Dann ist offenbar $h_2 \in \mathcal{G}$ und $h_2(a, \vec{b}, c) = 0$ ist äquivalent zu der Gültigkeit der obigen Gleichungen für $\beta$. Insbesondere gibt es zu jedem $a, \vec{b}$ ein $c$ mit $h_2(a, \vec{b}, c) = 0$. Daher gilt

$$f(a, \vec{b}) = \beta(\mu c\,(h_2(a, \vec{b}, c) = 0), a)$$

und $f$ ist deshalb $\mu$–rekursiv. □

**Satz 4.4.** *Sei $T$ eine $\mathcal{L}$–Theorie mit $0, \mathrm{suc}, =$ in $\mathcal{L}$ und $\mathrm{Eq}_{\mathcal{L}} \subseteq T$. Ferner gebe es Formeln $N[x]$ und $K[x, y]$ — geschrieben $Nx$ bzw. $x < y$ — so daß $T \vdash N0$, $T \vdash \forall x \in N\, N[\mathrm{suc}(x)]$ und folgendes gilt.*

a. *Für alle $a, b \in \mathbb{N}$ gilt*

$$T \vdash \mathrm{suc}(\underline{a}) \neq 0,$$
$$T \vdash \mathrm{suc}(\underline{a}) = \mathrm{suc}(\underline{b}) \to \underline{a} = \underline{b}.$$

b. *Die Funktionen $+$ und $\cdot$ sind in $T$ repräsentierbar.*

c. *(i) $T \vdash \forall x \in N\,(x \not< 0)$,*

*(ii) $T \vdash \forall x \in N\,(x < \mathrm{suc}(\underline{b}) \to x < \underline{b} \vee x = \underline{b})$ für alle $b \in \mathbb{N}$,*

*(iii) $T \vdash \forall x \in N\,(x < \underline{b} \vee x = \underline{b} \vee \underline{b} < x)$ für alle $b \in \mathbb{N}$.*

*Hierbei steht wieder $\forall x \in N\, A$ für $\forall x\,(Nx \to A)$. Dann erfüllt $T$ die Voraussetzungen von Satz 3.4, also des (auf $N$ relativierten) Satzes von Gödel–Rosser. Genauer gilt für alle $a \in \mathbb{N}$*

$$T \vdash \forall x \in N\,(x < \underline{a} \to x = \underline{0} \vee \cdots \vee x = \underline{a-1}), \qquad (*)$$
$$T \vdash \forall x \in N\,(x = \underline{0} \vee \cdots \vee x = \underline{a} \vee \underline{a} < x), \qquad (**)$$

*und jede rekursive Funktion ist in $T$ repräsentierbar.*

*Beweis.* Wir zeigen zunächst, daß die Formel $x = y$ die Gleichheit und die Formel $x < y$ die Kleinerbeziehung in $T$ repräsentiert. Aus a folgt sofort $T \vdash \underline{a} \neq \underline{b}$ für $a \neq b$. Gelte nun $a \not< b$. Wir zeigen $T \vdash \underline{a} \not< \underline{b}$ durch Induktion nach $b$. $T \vdash \underline{a} \not< 0$ folgt aus c(i). Im Schritt haben wir $a \not< b+1$, also $a \not< b$ und $a \neq b$, also nach IH und der obigen Bemerkung $T \vdash \underline{a} \not< \underline{b}$ und $T \vdash \underline{a} \neq \underline{b}$, also nach c(ii) $T \vdash \underline{a} \not< \mathrm{suc}(\underline{b})$. Sei jetzt $a < b$. Dann gilt $T \vdash \underline{a} \neq \underline{b}$ und $T \vdash \underline{b} \not< \underline{a}$, also nach c(iii) $T \vdash \underline{a} < \underline{b}$.

$(*)$ ergibt sich jetzt leicht durch Induktion über $a$. Die Basis folgt aus c(i), und der Schritt aus der IH und c(ii). $(**)$ ergibt sich aus c(iii) unmittelbar mit $(*)$.

Wir zeigen jetzt durch Induktion über die Definition der $\mu$–rekursiven Funktionen, daß jede $\mu$–rekursive (und damit nach Satz 4.3 auch jede rekursive) Funktion in $T$ repräsentierbar ist. Man beachte hierbei, daß wegen $T \vdash \underline{a} \neq \underline{b}$ für $a \neq b$ die Bedingung (2) in der Definition der Repräsentierbarkeit einer Funktion nicht mehr überprüft werden muß.

Die *Ausgangsfunktionen* $0^n$, suc und $I_i^n$ werden offenbar durch die Formeln $0 = y$, $\mathrm{suc}(x) = y$ und $x_i = y$ repräsentiert. $+$ und $\cdot$ sind nach Voraussetzung b in $T$ repräsentierbar. Wir zeigen noch, daß die Funktion $1_<$ in $T$ durch

$$A := (x_1 < x_2 \wedge y = 1) \vee (x_1 \not< x_2 \wedge y = 0)$$

repräsentiert wird. Gelte also $a_1 < a_2$. Dann ist $T \vdash \underline{a_1} < \underline{a_2}$, also $T \vdash A[\underline{a_1}, \underline{a_2}, 1]$. Sei jetzt $a_1 \not< a_2$. Dann ist $T \vdash \underline{a_1} \not< \underline{a_2}$, also $T \vdash A[\underline{a_1}, \underline{a_2}, 0]$. Ferner ist $A[x_1, x_2, y] \wedge A[x_1, x_2, z] \to y = z$ schon logisch aus den Gleichheitsaxiomen herleitbar (Fallunterscheidung nach $x_1 < x_2$).

*Fall* $(\circ h g_1 \dots g_m)$. OBdA seien $g_1, \dots, g_m$ einstellig. Nach IH haben wir repräsentierende Formeln $A_{g_i}[x, y_i]$ und $A_h[\vec{y}, z]$. Wir setzen

$$A_f := \exists \vec{y}\, (A_{g_1}[x, y_1] \wedge \dots \wedge A_{g_m}[x, y_m] \wedge A_h[\vec{y}, z]).$$

Gelte $f(a) = c$. Offenbar haben wir dann $T \vdash A_f[\underline{a}, \underline{c}]$. Zu zeigen bleibt $T \vdash A_f[\underline{a}, z_1] \wedge A_f[\underline{a}, z_2] \to z_1 = z_2$. Wir führen den Beweis wieder informal. Nach Definition von $A_f$ haben wir $y_{11}, \dots, y_{1m}$ und $y_{21}, \dots, y_{2m}$. Die IH für $g_i$ liefert $y_{1i} = y_{2i} = \underline{g_i(a)}$. Mit der IH für $h$ ergibt sich $z_1 = z_2$.

*Fall* $(\mu g)$. OBdA sei $g$ zweistellig, also $f(a) = \mu i\, (g(i, a) = 0)$, wobei $\forall a \exists i\, (g(i, a) = 0)$. Nach IH haben wir eine repräsentierende Formel $A_g[y, x, z]$. Sei

$$A_f[x, y] := A_g[y, x, 0] \wedge \forall v < y \exists w\, (w \neq 0 \wedge A_g[v, x, w]).$$

Wir zeigen zunächst (1) aus der Definition der Repräsentierbarkeit. Gelte also $f(a) = b$. Zu zeigen ist $T \vdash A_f[\underline{a}, \underline{b}]$. Aufgrund der Gestalt von $A_f$ folgt dies aber sofort mit $T \vdash v < \underline{b} \to v = \underline{0} \vee \dots \vee v = \underline{b-1}$ aus der IH für $g$. Wir zeigen jetzt noch (3) aus der Definition der Repräsentierbarkeit. Gegeben sei also $a$; setze $b := f(a)$. Es genügt zu zeigen $T \vdash A_f[\underline{a}, y] \to y = \underline{b}$. Den Beweis führen wir wieder informal. Gelte also $A_f[\underline{a}, y]$. Nach Voraussetzung c(iii) genügt es, $y \not< \underline{b}$ und $\underline{b} \not< y$ zu zeigen. Nehmen wir also zunächst $y < \underline{b}$ an. Nach $(*)$ folgt $y = \underline{i}$ für ein $i < b$ im Widerspruch zu $A_g[y, \underline{a}, 0]$. Nehmen wir jetzt $\underline{b} < y$ an. Aus $A_f[\underline{a}, y]$ folgt dann $\exists w\, (w \neq 0 \wedge A_g[\underline{b}, \underline{a}, w])$ im Widerspruch zu $A_g[\underline{b}, \underline{a}, 0]$. □

Wir wollen jetzt noch eine spezielle und besonders einfache arithmetische Theorie betrachten. Sei $\mathcal{L}_1$ die durch 0, suc, $+$, $\cdot$ und $=$ bestimmte Sprache und $Z_1$ die durch $\mathrm{Eq}_{\mathcal{L}_1}$ und die Generalisierungen der folgenden Axiome bestimmte Theorie.

$$\mathrm{suc}(x) \neq 0, \tag{$Z_1 1$}$$
$$\mathrm{suc}(x) = \mathrm{suc}(y) \to x = y, \tag{$Z_1 2$}$$
$$x + 0 = x, \tag{$Z_1 3$}$$
$$x + \mathrm{suc}(y) = \mathrm{suc}(x + y), \tag{$Z_1 4$}$$
$$x \cdot 0 = 0, \tag{$Z_1 5$}$$
$$x \cdot \mathrm{suc}(y) = x \cdot y + x, \tag{$Z_1 6$}$$
$$\exists z\, (x + \mathrm{suc}(z) = y) \vee x = y \vee \exists z\, (y + \mathrm{suc}(z) = x). \tag{$Z_1 7$}$$

**Satz 4.5.** *Jede Theorie $T$ mit $T \supseteq Z_1$ erfüllt die Voraussetzungen des Satzes 3.3 von Gödel–Rosser. Bzgl. $K[x,y] := \exists z\,(x + \mathrm{suc}(z) = y)$ ist sogar jede rekursive Funktion in $T$ repräsentierbar.*

*Beweis.* Wir zeigen, daß $T$ mit $N[x] := (x = x)$ und $K[x,y] := \exists z\,(x + \mathrm{suc}(z) = y)$ die Bedingungen von Satz 4.4 erfüllt. Für a ist dies klar. Für b können wir $x + y = z$ und $x \cdot y = z$ als repräsentierende Formeln wählen. Für c(i) ist zu zeigen $\neg\exists z\,(x + \mathrm{suc}(z) = 0)$. Dies folgt aber aus $(Z_1 4)$ und $(Z_1 1)$. Zum Beweis von c(ii) benötigen wir als Hilfsaussage

$$x = 0 \vee \exists y\,(x = \mathrm{suc}(y)), \qquad (*)$$

deren Beweis wir unten nachtragen. Gelte also $x + \mathrm{suc}(z) = \mathrm{suc}(\underline{b})$, also auch $\mathrm{suc}(x + z) = \mathrm{suc}(\underline{b})$ und damit $x + z = \underline{b}$. Wir verwenden jetzt $(*)$ für $z$. Im Fall $z = 0$ folgt $x = \underline{b}$, und im Fall $\exists y\,(z = \mathrm{suc}(y))$ haben wir $\exists y\,(x + \mathrm{suc}(y) = \underline{b})$. Damit ist c(ii) bewiesen. c(iii) folgt sofort aus $(Z_1 7)$.

Zum Beweis von $(*)$ verwenden wir ebenfalls $(Z_1 7)$ und vergleichen $x$ mit 0. Es genügt offenbar, den Fall $\exists z\,(x + \mathrm{suc}(z) = 0)$ auszuschließen. Er besagt aber $\mathrm{suc}(x + z) = 0$ und widerspricht deshalb $(Z_1 1)$. □

**Folgerung 4.6 (Starke Unentscheidbarkeit von $Z_1$).** *Jede konsistente Theorie $T$ mit $T \supseteq Z_1$ ist nicht rekursiv.*

*Beweis.* Sätze 4.5 und 3.1. □

**Folgerung 4.7 (Unentscheidbarkeit der Prädikatenlogik).** *Sei $\mathcal{L}_1$ die durch* 0, suc, $+$, $\cdot$ *und* $=$ *bestimmte Sprache. Dann ist die Menge der in der klassischen Logik herleitbaren $\mathcal{L}_1$–Formeln nicht rekursiv.*

*Beweis.* Andernfalls wäre auch $Z_1$ rekursiv, denn eine Formel $A$ ist herleitbar in $Z_1$ genau dann, wenn die Implikation aus der Konjunktion der endlich vielen $Z_1$–Axiome und der Gleichheitsaxiome in der klassischen Logik herleitbar ist. □

In II.2.1 hatten wir $\Sigma_1$–Formeln der formalen Sprache PR definiert, ausgehend von eventuell negierten PR–Primformeln. Wir wollen jetzt einen entsprechenden Begriff für die durch 0, suc, $+$, $\cdot$ und $=$ bestimmte Sprache $\mathcal{L}_1$ definieren, und zwar so daß immer noch genau die rekursiv aufzählbaren Relationen durch $\Sigma_1$–Formeln definierbar sind. In Anbetracht der stark verringerten sprachlichen Ausdrucksmittel ist es jetzt sinnvoll, nur ganz spezielle atomare und negiert atomare Formeln zuzulassen. $\Sigma_1$–*Formeln* der Sprache $\mathcal{L}_1$ werden wie folgt induktiv definiert.

- Für alle Variablen $x, y, z$ sind $x = y$, $x \neq y$, $0 = x$, $\mathrm{suc}(x) = y$, $x + y = z$ und $x \cdot y = z$ $\Sigma_1$–Formeln der Sprache $\mathcal{L}_1$.
- Mit $A$ und $B$ sind auch $A \wedge B$ und $A \vee B$ $\Sigma_1$–Formeln der Sprache $\mathcal{L}_1$.
- Mit $A$ ist auch $\forall x < y\,A$ eine $\Sigma_1$–Formel der Sprache $\mathcal{L}_1$, falls $y$ von $x$ verschieden ist.

- Mit $A$ ist auch $\exists x\, A$ eine $\Sigma_1$–Formel der Sprache $\mathcal{L}_1$.

Damit jede $\Sigma_1$–Formel der Sprache $\mathcal{L}_1$ auch wirklich eine $\mathcal{L}_1$–Formel ist, verstehen wir $\forall x < y\, A$ als Abkürzung für $\forall x\, (\exists z\, (x + \mathrm{suc}(z) = y) \to A)$.

**Satz 4.8.** *Jede rekursive Funktion ist in $Z_1$ repräsentierbar durch eine $\Sigma_1$–Formel der Sprache $\mathcal{L}_1$.*

*Beweis.* Dies ergibt sich sofort durch Inspektion des Beweises von Satz 4.4. Man hat lediglich zu beachten, daß schon aufgrund der Gleichheitsaxiome $\exists z\, (x + \mathrm{suc}(z) = y)$ mit $\exists z \exists w\, (\mathrm{suc}(z) = w \wedge x + w = y)$ und $A[0]$ mit $\exists x\, (x = 0 \wedge A)$ äquivalent sind. □

$\mathcal{L}_1$–Formeln heißen auch *arithmetische* Formeln. Eine Relation $R \subseteq \mathbb{N}^n$ heißt *arithmetisch*, wenn sie im *Standardmodell* $\mathcal{N}_1$ der Sprache $\mathcal{L}_1$ definierbar ist.

**Folgerung 4.9.** *a. Jede primitiv rekursive Relation ist arithmetisch.*

*b.* $\mathrm{Th}(\mathcal{N}_1)$ *ist nicht arithmetisch, insbesondere also auch nicht rekursiv aufzählbar.*

*Beweis.* a folgt aus Satz 4.5 (mit Lemma 2.1), und b aus Satz 1.2 □.

## 3.5 Unbeweisbarkeit der Konsistenz

Wir haben oben im Satz 3.3 von Gödel–Rosser gesehen, wie man zu jeder axiomatisierten konsistenten Theorie $T$, die gewisse schwache Voraussetzungen erfüllt, einen geschlossenen Satz $A$ konstruieren kann so daß weder $A$ noch $\neg A$ in $T$ beweisbar ist. Die inhaltliche Bedeutung dieses Satzes $A$ war "Zu jedem Beweis von mir gibt es einen kürzeren Beweis meiner Negation". Da also $A$ keinen Beweis besitzt, ist insbesondere $A$ wahr. Wir haben also einen wahren, aber in $T$ unbeweisbaren Satz gefunden.

Diese Aussage wollen wir jetzt noch verschärfen, indem wir zeigen, daß ein besonders interessanter wahrer Satz in $T$ unbeweisbar ist, nämlich der Satz $\mathrm{Wf}_T$, der die Konsistenz (oder *Widerspruchsfreiheit*) von $T$ besagt. Dies ist der sogenannte zweite Unvollständigkeitssatz von Gödel [6].

Wir werden diesen Satz hier in einer von Löb angegebenen verschärften Form beweisen. Zunächst zeigen wir eine Hilfsaussage.

**Lemma 5.1.** *Sei $A[x_1, \ldots, x_n]$ eine $\Sigma_1$–Formel der durch $0$, suc, $+$, $\cdot$ und $=$ bestimmten Sprache $\mathcal{L}_1$. Gilt dann $\mathcal{N}_1 \models A[a_1, \ldots, a_n]$ für das Standardmodell $\mathcal{N}_1$ von $\mathcal{L}_1$, so folgt $Z_1 \vdash A[\underline{a_1}, \ldots, \underline{a_n}]$.*

*Beweis* durch Induktion über die $\Sigma_1$–Formeln der Sprache $\mathcal{L}_1$. Die *Anfangsfälle* hatten wir zu Beginn des Beweises von Satz 4.4 erledigt bzw. ergeben sich (für $x + y = z$ und $x \cdot y = z$) aus den Rekursionsgleichungen für $+$ und $\cdot$ in $(Z_1 3)$–$(Z_1 6)$.

*Fälle* $A \wedge B$, $A \vee B$. Die Behauptung folgt sofort aus der IH.

*Fall* $\forall x < y\, A[x, y, z_1, \ldots, z_n]$; oBdA sei $n = 1$. Gelte also $\mathcal{N}_1 \models (\forall x < y\, A)[b, c]$. Dann folgt $\mathcal{N}_1 \models A[i, b, c]$ für jedes $i < b$ und deshalb nach IH $Z_1 \vdash A[\underline{i}, \underline{b}, \underline{c}]$. Nun gilt nach Satz 4.5

$$Z_1 \vdash \forall x\, (\exists z\, (x + \mathrm{suc}(z) = \underline{b}) \to x = \underline{0} \vee \cdots \vee x = \underline{b - 1}),$$

also

$$Z_1 \vdash \forall x < \underline{b}\, A[\underline{b}, \underline{c}].$$

*Fall* $\exists x\, A[x, y_1, \ldots, y_n]$; oBdA sei $n = 1$. Gelte also $\mathcal{N}_1 \models (\exists x\, A)[b]$. Dann ist $\mathcal{N}_1 \models A[a, b]$ für ein $a \in \mathbb{N}$, also nach IH $Z_1 \vdash A[\underline{a}, \underline{b}]$ und deshalb $Z_1 \vdash (\exists x\, A)[\underline{b}]$. □

Sei $T$ eine axiomatisierte konsistente Theorie mit $T \supseteq Z_1$. Sei $B_{\mathrm{Abl}_T}$ wie in Kapitel 3.3 eine $\mathcal{L}_1$–Formel, die die primitiv rekursive Relation $\mathrm{Abl}_T \subseteq \mathbb{N} \times \mathbb{N}$ in $Z_1$ repräsentiert. Wir definieren dann $\mathcal{L}_1$–Formeln $\mathrm{Thm}_T[x]$ und $\mathrm{Wf}_T$ durch

$$\mathrm{Thm}_T[x] := \exists y\, B_{\mathrm{Abl}_T}[y, x],$$
$$\mathrm{Wf}_T := \neg \exists y\, B_{\mathrm{Abl}_T}[y, \underline{\ulcorner \bot \urcorner}].$$

$\mathrm{Thm}_T[x]$ definiert also in $\mathcal{N}_1$ die Menge der in $T$ beweisbaren Formeln, und es gilt $\mathcal{N}_1 \models \mathrm{Wf}_T$ genau dann, wenn $T$ konsistent ist. Wir betrachten die folgenden beiden *Ableitbarkeitsbedingungen* für $T$.

$$T \vdash A \to \mathrm{Thm}_T[\underline{\ulcorner A \urcorner}] \quad \text{für } A \text{ geschlossene } \Sigma_1\text{–Formel der Sprache } \mathcal{L}_1, \tag{AB1}$$

$$T \vdash \mathrm{Thm}_T[\underline{\ulcorner A \to B \urcorner}] \wedge \mathrm{Thm}_T[\underline{\ulcorner A \urcorner}] \to \mathrm{Thm}_T[\underline{\ulcorner B \urcorner}]. \tag{AB2}$$

(AB1) sagt aus, daß Lemma 5.1 (oder genauer die Aussage, daß jede in $\mathcal{N}_1$ gültige geschlossene $\Sigma_1$–Formel der Sprache $\mathcal{L}_1$ in $T$ liegt) nicht nur wahr, sondern sogar in $T$ beweisbar ist.

**Satz 5.2 (Gödel–Löb).** *Sei $T$ eine axiomatisierte konsistente Erweiterung von $Z_1$, die die Ableitbarkeitsbedingungen (AB1) und (AB2) erfüllt. Gilt dann $T \vdash \mathrm{Thm}_T[\underline{\ulcorner C \urcorner}] \to C$ für eine geschlossene $\mathcal{L}_1$–Formel $C$, so gilt schon $T \vdash C$.*

*Beweis.* Gelte $T \vdash \mathrm{Thm}_T[\underline{\ulcorner C \urcorner}] \to C$. Wähle $A$ nach dem Fixpunktlemma 2.2 so daß

$$Z_1 \vdash A \leftrightarrow (\mathrm{Thm}_T[\underline{\ulcorner A \urcorner}] \to C). \tag{$*$}$$

Zu zeigen ist $T \vdash C$. Wir führen den Beweis informal, müssen jedoch zeigen, daß alle Schlüssen innerhalb von $T$ durchführbar sind. Zunächst zeigen wir

$$\mathrm{Thm}_T[\underline{\ulcorner A \urcorner}] \to C. \tag{1}$$

Gelte also

$$\mathrm{Thm}_T[\underline{\ulcorner A \urcorner}].$$

Nach (AB1) folgt

$$\mathrm{Thm}_T[\underline{\ulcorner \mathrm{Thm}_T[\underline{\ulcorner A \urcorner}] \urcorner}].$$

Wegen $(*)$ ist die geschlossene $\Sigma_1$–Formel $\mathrm{Thm}_T[\underline{\ulcorner A \to (\mathrm{Thm}_T[\underline{\ulcorner A \urcorner}] \to C) \urcorner}]$ wahr (in $\mathcal{N}_1$), und nach Lemma 5.1 können wir sie auch in $Z_1$ beweisen. Also

$$\mathrm{Thm}_T[\underline{\ulcorner A \to (\mathrm{Thm}_T[\underline{\ulcorner A \urcorner}] \to C) \urcorner}].$$

Zweimalige Anwendung von (AB2) ergibt

$$\mathrm{Thm}_T[\underline{\ulcorner C \urcorner}]$$

und damit nach Voraussetzung $C$. Damit ist (1) bewiesen.

Aus (1) erhält man jetzt $A$, nach $(*)$.

Wir verlassen nun den informalen, innerhalb von $T$ durchführbaren Beweis und stellen fest, daß wir $T \vdash A$ gezeigt haben. Also ist die geschlossene $\Sigma_1$–Formel $\mathrm{Thm}_T[\underline{\ulcorner A \urcorner}]$ wahr (in $\mathcal{N}_1$) und damit nach Lemma 5.1 auch in $T$ beweisbar. Da andererseits auch (1) in $T$ beweisbar war, ist auch $C$ in $T$ beweisbar. Damit haben wir $T \vdash C$ gezeigt. □

**Folgerung 5.3 (Zweiter Gödelscher Unvollständigkeitssatz).** *Sei $T$ eine axiomatisierte konsistente Erweiterung von $Z_1$, die die Ableitbarkeitsbedingungen (AB1) und (AB2) erfüllt. Dann gilt $T \nvdash \mathrm{Wf}_T$.*

*Beweis.* Setze $C := \bot$ in Satz 5.2. □

**Folgerung 5.4.** *Sei $T$ eine axiomatisierte konsistente Erweiterung von $Z_1$, die die Ableitbarkeitsbedingungen (AB1) und (AB2) erfüllt. Dann ist das Reflexionsschema*

$$\mathrm{Thm}_T[\underline{\ulcorner C \urcorner}] \to C \quad \textit{mit } C \textit{ geschlossene } \mathcal{L}_1\textit{–Formel}$$

*unbeweisbar in $T$.*

*Beweis.* Man wähle in Satz 5.2 ein $C$ mit $T \nvdash C$, etwa $C = \bot$. □

Ein wichtiges Beispiel einer axiomatisierten konsistenten Erweiterung von $Z_1$, die die Ableitbarkeitsbedingungen (AB1) und (AB2) erfüllt, ist die *Peano–Zahlentheorie $Z$* (oft auch mit PA bezeichnet). Die Sprache von $Z$ ist wieder $\mathcal{L}_1$ (also gegeben durch 0, suc, $+$, $\cdot$ und $=$), und die Axiome sind neben $\mathrm{Eq}_{\mathcal{L}_1}$ die ersten sechs $Z_1$–Axiome und zusätzlich das *Induktionsschema*

$$A[0] \wedge \forall x\,(A \to A[\mathrm{suc}(x)]) \to \forall x\,A.$$

## 3.6 Historische Anmerkungen

Die Unentscheidbarkeit der Prädikatenlogik wurde zuerst von Church gezeigt. Die Grundidee dieses Beweises ist jedoch schon in Gödels Arbeit [6] enthalten.

In dem Buch Grundlagen der Mathematik von Hilbert und Bernays [7] findet man eine ausführliche Darstellung der Unentscheidbarkeitsbeweise, und zwar für einen zahlentheoretischen Formalismus $Z_{00}$ in [7, Seite 433] und damit auch für die Prädikatenlogik (siehe [7, Seite 434]).

# Anhang Vollständigkeit der Minimallogik

Zur Minimallogik paßt der Begriff eines Beth–Modells, wieder in dem Sinn, daß

$$\Vdash A \iff \vdash A.$$

Wir betrachten hier Beth–Modelle der Einfachheit halber nur über dem vollen binären Baum, d.h. der Menge $T_{01}$ aller 0–1–Folgen (Knoten) $k$. Die leere Folge bezeichnen wir mit $\langle\rangle$.

**Definition.** *$\mathcal{M} = (M, I_0, I_1)$ heißt $\mathcal{L}$–Beth–Struktur, wenn $(M, I_0)$ eine $\mathcal{L}$–Prästruktur ist und $I_1$ eine Abbildung, die jedem $n$–stelligen Relationssymbol $R$ von $\mathcal{L}$ und jedem Knoten $k \in T_{01}$ eine $n$–stellige Relation*

$$I_1(R, k) \subseteq M^n$$

*zuordnet, so daß folgende Monotonie–Eigenschaft gilt:*

$$k \leq k' \implies I_1(R, k) \subseteq I_1(R, k').$$

*Ist $n = 0$, so ist $I_1(R, k) \in \{\text{wahr}, \text{falsch}\}$ und die verlangte Monotonieeigenschaft ist*

$$k \leq k', I_1(R, k) = \text{wahr} \implies I_1(R, k') = \text{wahr}.$$

Von $I_1(\bot, k)$ wird also *nichts* verlangt; das Falsum spielt in der Minimallogik die Rolle eines gewöhnlichen Aussagensymbols.

$\mathcal{M}_U(t)$ wird wie bei klassischen Modellen erklärt. An die Stelle der Modellbeziehung $\mathcal{M} \models A[U]$ tritt bei Beth–Strukturen jedoch die *Erzwingungbeziehung*

$$\mathcal{M}, k \Vdash A[U]$$

Wir geben jetzt eine induktive Definition von $\mathcal{M}, k \Vdash A[U]$.

1. $\mathcal{M}, k \Vdash R(t_1, \ldots, t_m)[U]$
   $\iff \exists n \geq \lg(k) \underbrace{\forall k' \geq k}_{\lg(k')=n} (\mathcal{M}_U(t_1), \ldots, \mathcal{M}_U(t_m)) \in I_1(R, k')$ (bzw. $I_1(R, k')$ ist wahr).
2. $\mathcal{M}, k \Vdash (A \to B)[U] \iff \forall k' \geq k. \mathcal{M}, k' \Vdash A[U] \implies \mathcal{M}, k' \Vdash B[U]$.
3. $\mathcal{M}, k \Vdash (\forall x\, A)[U] \iff \forall m \in |\mathcal{M}|\ \mathcal{M}, k \Vdash A[U(\frac{m}{x})]$.

Aus der Definition folgt sofort

$$k \leq k', \mathcal{M}, k \Vdash A[U] \implies \mathcal{M}, k' \Vdash A[U].$$

Wir schreiben $\mathcal{M} \Vdash A[U]$ für $\mathcal{M}, \langle\rangle \Vdash A[U]$. und $\mathcal{M} \Vdash \Gamma[U]$, wenn $\mathcal{M} \Vdash A[U]$ für alle $A \in \Gamma$.

Die Begriffe der Gültigkeit und Erfüllbarkeit lassen sich in naheliegender Weise auf Beth–Strukturen übertragen. Wir schreiben $\Gamma \Vdash A$ für

$$\forall \mathcal{M}, k, W(\mathcal{M}, k \Vdash \Gamma[U] \implies \mathcal{M}, k \Vdash A[U]).$$

Wie üblich beweist man das Koinzidenzlemma und das Substitutionslemma. Daraus erhält man:

**Satz A.1 (Korrektheitssatz für Beth–Strukturen).** $\Gamma \vdash_m A \implies \Gamma \Vdash A$.

Beweis durch Induktion über Herleitungen. □

**Lemma A.2.**

$$(\exists n \geq \lg(k) \underbrace{\forall k' \geq k}_{\lg(k')=n} \mathcal{M}, k' \Vdash A[U]) \implies \mathcal{M}, k \Vdash A[U]$$

Beweis durch Induktion über $A$. Wir schreiben kurz $k \Vdash A$ für $\mathcal{M}, k \Vdash A[U]$.

Fall 1. Primformel $R(t_1, \ldots, t_m)$. Zur Vereinfachung der Schreibweise nehmen wir $m = 1$ an, betrachten also $R(t)$. Gelte

$$\exists n \geq \lg(k) \underbrace{\forall k' \geq k}_{\lg(k')=n} k' \Vdash R(t),$$

also nach Definition

$$\exists n \geq lg(k) \underbrace{\forall k' \geq k}_{\lg(k')=n} \exists m \geq \lg(k') \underbrace{\forall k'' \geq k'}_{\lg(k'')=m} \mathcal{M}_U(r) \in I_1(R, k'').$$

Da $T_{01}$ binär ist, gilt

$$\exists m \geq \lg(k) \underbrace{\forall k' \geq k}_{\lg(k')=m} \mathcal{M}_U(r) \in I_1(R, k'),$$

also $k \Vdash R(t)$.

Fall 2. $A \to B$. Gelte

$$k' \Vdash A \to B$$

für alle $k' \geq k$ mit $\lg(k') = n$. Zu zeigen ist

$$\forall l \geq k.l \Vdash A \implies l \Vdash B.$$

Sei also $l \geq k$ und gelte $l \Vdash A$. Zu zeigen ist $l \Vdash B$. Wir verwenden die IH für $B$ mit $m := \max(n, \lg(l))$. Sei also $l' \geq l$ und $\lg(l') = m$. Es genügt zu zeigen

$$l' \Vdash B.$$

Ist $\lg(l') = \lg(l)$, so ist $l' = l$ und wir sind fertig. Ist $\lg(l') = n > \lg(l)$, so ist $l'$ eine Fortsetzung von $l$ und damit von $k$ der Länge $n$ und wir haben $l' \Vdash A \to B$ nach Annahme. Ferner haben wir $l' \Vdash A$, da $l' \geq l$ und $l \Vdash A$. Damit folgt wieder $l' \Vdash B$.

Fall 3. $\forall x\, A$. Trivial. □

Eine $\mathcal{L}$–Beth–Struktur $\mathcal{M}$ heißt $\mathcal{L}$–Beth–Struktur *für die intuitionistische Logik*, wenn für jedes Relationssymbol $R$ von $\mathcal{L}$ gilt $\mathcal{M} \Vdash \mathrm{Efq}_R$.

Wir wollen jetzt die Vollständigkeit der Minimallogik beweisen.

Wir beschränken uns hier auf eine *abzählbare* Sprache $\mathcal{L}$ der Prädikatenlogik erster Stufe; das soll heißen, daß in $\mathcal{L}$ höchstens abzählbar viele Relations– und Funktionssymbole vorkommen.

Für eine beliebige (oBdA geschlossene) $\mathcal{L}$–Formel $A$ wollen wir zeigen, daß $A$ genau dann in der Minimallogik herleitbar ist, wenn $A$ in allen $\mathcal{L}$–Beth–Strukturen gültig ist. Wir können sogar eine feste "universelle" $\mathcal{L}$–Beth–Struktur $\mathcal{U}$ angeben mit der Eigenschaft, daß $\vdash_m A$ äquivalent ist zu $\mathcal{U} \Vdash A$.

Zur Definition von $\mathcal{U}$ gehen wir aus von einer festen Aufzählung

$$A_0, A_1, A_2, \ldots$$

aller $\mathcal{L}$–Formeln, in der jede Formel unendlich oft vorkommen möge. Wir ordnen zunächst jedem Knoten $k$ des vollen binären Baums $T_{01}$ eine endliche Formelmenge $\Gamma_k$ zu, und zwar durch Induktion über die Länge von $k$. Sei also $\Gamma_{\langle\rangle} := \emptyset$. Wir nehmen jetzt an, daß für einen Knoten $k$ mit $lg(k) = n$ die Menge $\Gamma_k$ schon definiert ist, und definieren $\Gamma_{k0}$ und $\Gamma_{k1}$ wie folgt.

Zunächst sei aber noch eine Schreibweise eingeführt: In diesem Abschnitt schreiben wir $\Gamma \vdash A$ statt $\Gamma \vdash_m A$. Ferner soll $\Gamma \vdash_n A$ mit $n \in \mathbb{N}$ bedeuten, daß es eine Herleitung von $A$ aus $\Gamma$ der Länge (= Anzahl sämtlicher Symbole) $\leq n$ gibt.

*Fall* 1. $\Gamma_k \nvdash_n A_n$. Dann setzen wir

$$\Gamma_{k0} := \Gamma_k \quad \text{und} \quad \Gamma_{k1} := \Gamma_k \cup \{A_n\}.$$

*Fall* 2. $\Gamma_k \vdash_n A_n$. Dann setzen wir

$$\Gamma_{k0} := \Gamma_{k1} := \Gamma_k \cup \{A_n\}.$$

Offenbar folgt aus $k \leq k'$, daß $\Gamma_k \subseteq \Gamma_{k'}$.

**Definition der universellen Beth–Struktur $\mathcal{U}$.** $\mathcal{U} = (\mathrm{Ter}_{\mathcal{L}}, I_0, I_1)$ *mit*

$$I_0(f)(t_1, \ldots, t_n) := f t_1 \ldots t_n,$$

$$(t_1, \ldots, t_n) \in I_1(R, k) :\Longleftrightarrow R(t_1, \ldots, t_n) \in \Gamma_k.$$

Dabei ist $\mathrm{Ter}_{\mathcal{L}}$ die Menge aller $\mathcal{L}$–Terme. Man beachte, daß aus der Definition von $I_0$ offenbar $\mathcal{U}_{\mathrm{id}}(r) = r$ für alle $\mathcal{L}$–Terme $r$ folgt.

**Lemma A.3.** *Sei $n \geq \lg(k)$. Dann gilt*

$$\underbrace{\forall k' \geq k}_{\lg(k')=n} \Gamma_{k'} \vdash A \implies \Gamma_k \vdash A.$$

*Beweis.* Es genügt zu zeigen

$$\Gamma_{k0} \vdash A, \Gamma_{k1} \vdash A \implies \Gamma_k \vdash A.$$

Entsprechend der Definition der $\Gamma_k$ unterscheiden wir zwei Fälle. Im Fall 1 gilt $\Gamma_{k0} = \Gamma_k$ und wir sind sofort fertig. Im Fall 2, also wenn $\Gamma_k \vdash_n A_n$, haben wir $\Gamma_{k0} = \Gamma_k \cup \{A_n\} \vdash A$. Wegen $\Gamma_k \vdash A_n$ folgt $\Gamma_k \vdash A$, was zu zeigen war. □

**Lemma A.4.** $\Gamma_k \vdash A \Rightarrow \exists n \geq \lg(k) \underbrace{\forall k' \geq k}_{\lg(k')=n} A \in \Gamma_{k'}$.

*Beweis.* Wähle $n \geq \lg(k)$ mit $A = A_n$ und $\Gamma_k \vdash_n A_n$. Für alle $k' \geq k$ mit $\lg(k') = n + 1$ gilt dann $A_n \in \Gamma_{k'}$ (wegen Fall 2). □

**Satz A.5.** $\Gamma_k \vdash A \iff \mathcal{U}, k \Vdash A[\mathrm{id}]$.

*Beweis* durch Induktion über $A$. Für $\mathcal{U}, k \Vdash A[\mathrm{id}]$ schreiben wir kurz $k \Vdash A$.

*Fall* 1. $R(t_1, \ldots, t_n)$. Wir formen die Aussage

$$\Gamma_k \vdash R(t_1, \ldots, t_n)$$

äquivalent um. Zunächst erhalten wir

$$\exists n \geq \lg(k) \underbrace{\forall k' \geq k}_{\lg(k')=n} R(t_1 \ldots t_n) \in \Gamma_{k'}$$

wegen Lemma A.3 und Lemma A.4. Daraus ergibt sich

$$\exists n \geq \lg(k) \underbrace{\forall k' \geq k}_{\lg(k')=n} (t_1, \ldots, t_n) \in I_1(R, k')$$

nach Definition von $\mathcal{U}$. Wegen $\mathcal{U}_{\mathrm{id}}(r) = r$ ist dies nach Definition der Erzwingungsbeziehung für Beth–Strukturen äquivalent zu

$$k \Vdash R(t_1 \ldots t_n).$$

*Fall* 2. $A \to B$. $\Longrightarrow$. Gelte

$$\Gamma_k \vdash A \to B.$$

Zu zeigen ist $k \Vdash A \to B$, also

$$\forall k' \geq k . k' \Vdash A \implies k' \Vdash B.$$

Sei also $k' \geq k$ und gelte $k' \Vdash A$. Nach IH folgt $\Gamma_{k'} \vdash A$ und damit wegen $\Gamma_k \vdash A \to B$ auch $\Gamma_{k'} \vdash B$. Wieder nach der IH folgt $k' \Vdash B$, was zu zeigen war.

$\Longleftarrow$. Gelte $k \Vdash A \to B$, also

$$\forall k' \geq k . k' \Vdash A \implies k' \Vdash B.$$

Zu zeigen ist $\Gamma_k \vdash A \to B$. Wir verwenden Lemma A.3 mit einem $n \geq \lg(k)$ derart daß $A = A_n$. Sei also $k' \geq k$ mit $\lg(k') = n$ beliebig gewählt. Zu zeigen ist dann $\Gamma_{k'} \vdash A \to B$. Im Fall $\Gamma_{k'} \vdash_n A_n$ erhalten wir $k' \Vdash A$ nach IH, also $k' \Vdash B$ nach Annahme, also $\Gamma_{k'} \vdash B$ wieder nach IH und damit $\Gamma_{k'} \vdash A \to B$. Im Fall $\Gamma_{k'} \nvdash A_n$ ist nach Definition $\Gamma_{k'1} = \Gamma_{k'} \cup \{A\}$. Damit erhalten wir $\Gamma_{k'1} \vdash A$, also $k'1 \Vdash A$ nach IH, also $k'1 \Vdash B$ nach Annahme, also $\Gamma_{k'1} \vdash B$ wieder nach IH. Wegen $\Gamma_{k'1} = \Gamma_{k'} \cup \{A\}$ folgt daraus auch in diesem Fall $\Gamma_{k'} \vdash A \to B$.

*Fall* 3. $\forall x\, A$. Wir formen die Aussage

$$\Gamma_k \vdash \forall x\, A$$

äquivalent um. Zunächst erhalten wir

$$\forall r \in \mathrm{Ter}_{\mathcal{L}} \Gamma_k \vdash A_x[r].$$

Aus der IH ergibt sich

$$\forall r \in \mathrm{Ter}_{\mathcal{L}} k \Vdash A_x[r],$$

also nach dem Substitutionslemma

$$\forall r \in \mathrm{Ter}_{\mathcal{L}} k \Vdash A[\mathrm{id}(\frac{r}{x})]$$

wegen $U_{\mathrm{id}}(r) = r$, und damit nach Definition der Erzwingungsbeziehung

$$k \Vdash \forall x\, A. \qquad \square$$

Als Folgerung erhalten wir den

**Satz A.5 (Vollständigkeitssatz für die Minimallogik).** *Für jede geschlossene Formel $A$ sind äquivalent (1) $\vdash_m A$, (2) $\Vdash A$ und (3) $\mathcal{U} \Vdash A$.* $\square$

# Literatur


[1] Wilfried Buchholz. Mathematische Logik. Vorlesungsskript, Mathematisches Institut der LMU, WS 92/93.

[2] C.C. Chang and H.J. Keisler. *Model Theory*, volume 73 of *Studies in Logic and the Foundations of Mathematics*. North–Holland, Amsterdam, 1973.

[3] Herbert B. Enderton. *A Mathematical Introduction to Logic*. Academic Press, New York, 1972.

[4] Gerhard Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1934.

[5] Kurt Gödel. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatshefte für Mathematik und Physik*, 37:349–360, 1930.

[6] Kurt Gödel. Über formal unentscheidbare Sätze der *principia mathematica* und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38:173–198, 1931.

[7] David Hilbert and Paul Bernays. *Grundlagen der Mathematik II*, volume 50 of *Grundlehren der mathematischen Wissenschaften*. Springer–Verlag, Berlin, second edition, 1970.

[8] Stephen C. Kleene. *Introduction to Metamathematics*. D. van Nostrand Comp., New York, 1952.

[9] L. Löwenheim. Über Möglichkeiten im Relativkalkül. *Mathematische Annalen*, 76:447–470, 1915.

[10] A. Malzew. Untersuchungen aus dem Gebiete der mathematischen Logik. *Rec. Math. N. S.*, 1:323–336, 1936.

[11] Rosza Péter. *Recursive Functions*. Academic Press, New York, 1967.

[12] Abraham Robinson. *On the Metamathematics of Algebra*. North–Holland, Amsterdam, 1951.

[13] Joseph R. Shoenfield. *Mathematical Logic*. Addison–Wesley Publ. Comp., Reading, Massachusetts, 1967.

[14] T. Skolem. Logisch–kombinatorische Untersuchungen über die Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze nebst einem Theorem über dichte Mengen. *Skrifter utgitt av Videnkapsselskapet i Kristiania, I, Mat. Naturv. Kl.*, 4:36 pp., 1920.

[15] Rolf Socher-Ambrosius. *Deduktionssysteme*. BI–Wissenschafts–Verlag, Mannheim, 1994.

# Index

# Index

$\Delta_0$–Formel, 58
$\Sigma_1$–Formel, 65
    der Sprache $\mathcal{L}_1$, 93
    strikte, 66
$\mu$–Operator
    beschränkter, 59
    unbeschränkter, 67
$n$–elementig, 47
Äquivalenz, 4
äquivalent, 27

abgeleitete Regel, 30
Ableitbarkeitsbedingungen, 96
Ableitung, 20
Abstraktion, 28
abzählbar, 47
Allformel, 4
Alphabet, 2
Annahme, 21
    geschlossene, 21
    offene, 21
Annahmenvariablen, 21
Anwendung, 28
Aristoteles, 2
arithmetisch, 94
Ast, 40

Ausgangsfunktionen, 56
Aussage, 2
Aussagensymbol, 6, 10
Axiom, 2
Axiomensystem, 47

Baum, 40
    beschrifteter, 6
    endlich verzweigter, 40
    unbeschränkter, 40
Belegung, 17
Beseitigungsregel, 21
Beweis, 20
Bindung, 13
blockiert, 42

Cantorsches Diagonalargument, 81
Churchsche These, 69

De–Morgan–Äquivalenzen, 33
Deduktionstheorem, 38
Definition
    explizite, 56
Disjunktion, 3

Einführungsregel, 21
einfach getypter Lambda–Kalkül, 28
Einsetzung, 56
elementar äquivalent, 47
endlich axiomatisierbar, 52
erfüllbar, 45
Erzeugungsbaum, 6

Erzeugungsfunktion, 6
ex–falso–quodlibet, 25
Existenzformel, 4
Expansion, 46

Falsum, 4
Folgerungsbeziehung, 41
formales System, 2
Formel, 2, 11
    arithmetische, 94
    atomare, 11
    aussagenlogisch unzerlegbare, 34
    aussagenlogische, 6
    geschlossene, 11
    pränexe, 36
Formelmenge
    definierbare, 82
    primitiv rekursive, 76
    rekursiv aufzählbare, 76
    rekursive, 76
Formeln
    als Typen, 28
Frege, 3
frei erzeugt, 8
Funktion
    $\mu$–rekursive, 67, 89
    berechenbare, 55, 68
    charakteristische, 55
    HGK–rekursive, 79
    partielle, 68

primitiv rekursive, 55
rekursive, 66
totale, 68
Funktionssymbol, 2, 10

Gödelnummer, 71
Gödelsche $\beta$–Funktion, 90
Gültigkeit, 18
genau dann wenn, 4
Generalisierungsregel, 38
Gleichheitsaxiome, 46
Gleichungssystem, 79
Grundsubstitution, 13
Grundterm, 11
Gruppentheorie, 5

Hauptprämisse, 21
herleitbar, 22
Herleitung, 20
Hilbertkalkül, 38
Homomorphismus, 9

Implikation, 4
Implikationslogik, 28
Individuenbereich, 2, 17
Induktionsschema, 97
induktiv, 7
Infix, 11
Instanz, 13
Interpretation, 17
isomorph, 47

Königsches Lemma, 40
Körper, 51
    archimedisch geordneter, 51
    geordneter, 51
Kern, 36
Klammerkonventionen, 12
Klauselform, 34
Kleenesches $T$–Prädikat, 80
Kleenesches Aufzählungstheorem, 81
Kleenesches Normalformentheorem, 81
Knoten, 40
Kodenummer, 71
Komposition, 13, 56
Kongruenzrelation, 47
Konjunktion, 3
Konklusion, 2, 21
konsistent, 45
Konstante, 2, 10
korrekt, 23

Länge, 40
Logik
    intuitionistische, 25
    klassische, 24
    Minimal–, 22

Marke, 21
Minimallogik, 22
Modell, 47
modus ponens, 21

Nebenprämisse, 21

Negation, 3
Nichtstandardmodell, 50

Objektvariablen, 21
oder, 3

Paarfunktion, 61
Peano–Axiome, 50
Peano–Zahlentheorie, 97
Pfad, 42
Prädikatensymbol, 10
Präfix, 36
Prämisse, 2, 21
Pränexe Normalform, 36
Prästruktur, 17
Primformel, 11
Primzahlpotenzkodierung, 60
Prinzip des indirekten Beweisens, 24

Quantor, 4
Quotientenstruktur, 47

Redukt, 46
Regel, 21
Rekursion, 8
    primitive, 56
Relation
    arithmetische, 94
    aufzählbare, 68
    definierbare, 57, 82
    entscheidbare, 68
    primitiv rekursive, 55

rekursiv aufzählbare, 65
rekursive, 66
Relationssymbol, 2, 10
repräsentierbar, 84

Satz, 11
Schlußregel, 2
Semantik, 2
Sequenz, 74
Signatur, 10
Sprache
primitiv rekursiv präsentierte, 71
Sprache erster Stufe, 10
Stabilität, 24
Standardmodell, 94
Struktur, 17
Substitution, 13
Suchpfad, 42
Symbolnummer, 71
Syntax, 2

Term, 2, 3, 10
geschlossener, 11
Tertium non datur, 33
Theorie, 47
axiomatisierte, 78
inkonsistente, 78
konsistente, 78
primitiv rekursiv axiomatisierbare, 77
rekursiv axiomatisierbare, 77
vollständige, 47

von $\mathcal{M}$, 47
Tiefe, 9
Trägermenge, 17

Umbenennung, 5
Umgebung, 17
und, 3
unendlich, 47
Unvollständigkeitssatz
erster, 86

Variable, 4, 10
freie, 4, 11, 30
gebundene, 4, 14
Variablenbedingung, 22, 31, 74
Variablensubstitution, 13

Wahrheitsbegriff, 82
Wahrheitsfunktion, 3
Wahrheitswert, 3
wenn–so, 4
Wertverlaufsfunktion, 61
Wertverlaufsrekursion, 61
Widerspruchsfreiheit, 95

Ziffer, 82