Mathematische Logik II

Wilfried Buchholz

Skriptum einer 4-std. Vorlesung im Sommersemester 1993

Mathematisches Institut der Universität München

10 Ordinalzahlarithmetik

Vereinbarung: λ bezeichne im folgenden stets eine Limeszahl.

Definition
1. Eine Klasse $A \subseteq On$ heißt *abgeschlossen*, falls gilt $\forall u(\emptyset \neq u \subseteq A \Rightarrow \sup(u) \in A)$.
2. Eine Funktion $F : On \to On$ heißt *stetig*, falls gilt $\forall u(\emptyset \neq u \subseteq On \Rightarrow F(\sup(u)) = \sup(F[u]))$.
3. $F : On \to On$ heißt *Normalfunktion*, falls F ordnungstreu und stetig ist.

Lemma 10.1
a) $\emptyset \neq u \subseteq On \wedge \sup(u) \notin u \Rightarrow \sup(u) \in Lim$.
b) $\alpha \in Lim \Leftrightarrow \alpha \neq 0 \wedge \sup(\alpha) = \alpha$.
c) α Nachfolgerzahl $\Rightarrow \alpha = \sup(\alpha) + 1 \wedge \sup(\alpha) = \max(\alpha)$.
d) $F : On \to On$ ordnungstreu $\Rightarrow \forall\alpha(\alpha \leq F(\alpha))$.
Beweis :
a) Sei $\emptyset \neq u \subseteq On$ und $\alpha := \sup(u) \notin u$. Offenbar ist dann $\alpha \neq 0$. Bleibt zu zeigen $\forall\beta < \alpha(\beta + 1 < \alpha)$. Sei also $\beta < \alpha$. Dann ist β keine obere Schranke von u, d.h. es existiert ein $\xi \in u$ mit $\beta < \xi$. Wegen $\alpha \notin u$ gilt dann $\beta + 1 \leq \xi < \alpha$.
b) "$\Rightarrow$" $\sup(\alpha) \leq \alpha$ ist trivial. Aus $\sup(\alpha) < \alpha$ würde $\sup(\alpha) + 1 \in \alpha$ und damit $\sup(\alpha) + 1 \leq \sup(\alpha)$ folgen. Widerspruch. "$\Leftarrow$" Aus $\sup(\alpha) = \alpha \neq 0$ folgt $\sup(\alpha) \notin \alpha \neq \emptyset$ und daraus mit a) $\sup(\alpha) \in Lim$.
c) $\alpha = \beta + 1 \Rightarrow \beta = \max(\alpha) \Rightarrow \beta = \sup(\alpha)$.
d) Induktion nach α: $\forall\xi < \alpha(\xi \leq F(\xi)) \Rightarrow \forall\xi < \alpha(\xi < F(\alpha)) \Rightarrow \alpha \leq F(\alpha)$. △

Lemma 10.2. Für jede Funktion $F : On \to On$ gilt:
F Normalfunktion $\Leftrightarrow \forall\alpha(F(\alpha) < F(\alpha + 1)) \wedge \forall\lambda{\in}Lim(F(\lambda) = \sup(F[\lambda]))$.
Beweis :
"$\Rightarrow$" $F(\lambda) = F(\sup(\lambda)) = \sup(F[\lambda])$.
"$\Leftarrow$" 1. Durch Induktion nach α erhalten wir $\forall\beta < \alpha(F(\beta) < F(\alpha))$.
2. Sei $\emptyset \neq u \subseteq On$ und $\alpha := \sup(u)$. Ist $\alpha \in u$, so $F(\alpha) = \sup(F[u])$, da F ordnungstreu. Ist $\alpha \notin u$, so $\alpha \in Lim$ und deshalb $F(\alpha) = \sup(F[\alpha])$. Ferner gilt $u \subseteq \alpha \wedge \forall\xi < \alpha\exists\eta{\in}u(\xi < \eta)$, woraus $\sup(F[\alpha]) = \sup(F[u])$ folgt. △

Lemma 10.3. Für jede Normalfunktion $F : On \to On$ gilt:
a) $F(\alpha) = \sup\{F(\xi + 1) : \xi \in \alpha\}$, für alle $\alpha > 0$.
b) $\lambda \in Lim \Rightarrow F(\lambda) \in Lim$.
c) $\forall\gamma \geq F(0)\exists!\alpha(F(\alpha) \leq \gamma < F(\alpha + 1))$.
d) G Normalfunktion $\Rightarrow F \circ G$ Normalfunktion.
Beweis :
a) Wegen $\forall\xi < \alpha(\xi + 1 \leq \alpha)$ gilt $\gamma := \sup\{F(\xi + 1) : \xi < \alpha\} \leq F(\alpha)$.
Ist $\alpha = \beta + 1$, so $F(\alpha) \in \{F(\xi + 1) : \xi < \alpha\}$ und deshalb $F(\alpha) \leq \gamma$.
Ist $\alpha \in Lim$, so $F(\alpha) = \sup F[\alpha] \leq \sup\{F(\xi + 1) : \xi < \alpha\} = \gamma$.
b) Es ist $0 \leq F(0) < F(\lambda)$. Aus $\gamma < F(\lambda)$ folgt (wegen $F(\lambda) = \sup F[\lambda]$) $\exists\xi < \lambda(\gamma < F(\xi))$ und weiter $\exists\xi(\gamma + 1 \leq F(\xi) < F(\lambda))$.
c) Sei $\gamma \geq F(0)$. Wegen $\gamma \leq F(\gamma) < F(\gamma + 1)$ existiert $\alpha := \min\{\xi : \gamma < F(\xi + 1)\}$. Dann $\gamma < F(\alpha + 1)$. Ist $\alpha = 0$, so $F(\alpha) = F(0) \leq \gamma$. Ist $\alpha > 0$, so $F(\alpha) = \sup\{F(\xi + 1) : \xi < \alpha\}$ und $\forall\xi < \alpha(F(\xi + 1) \leq \gamma)$, also $F(\alpha) \leq \gamma$.
d) $(F \circ G)(\sup(u)) = F(\sup(G[u])) = \sup(F[G[u]]) = \sup((F \circ G)[u])$. △

Lemma 10.4
Ist F die Ordnungsfunktion von $A \subseteq On$, so gilt:
F Normalfunktion $\Leftrightarrow$ A abgeschlossen und unbeschränkt.
Beweis :
1. $\mathrm{dom}(F) = On \Leftrightarrow A \notin V \Leftrightarrow A$ unbeschränkt.
2. Sei jetzt $\mathrm{dom}(F) = On$.
"$\Rightarrow$" Sei $\emptyset \neq u \subseteq A$ und $v := F^{-1}[u]$. Dann $\sup(u) = \sup(F[v]) = F(\sup(v)) \in A$.
"$\Leftarrow$" $\lambda \in Lim \Rightarrow F[\lambda] \subseteq A \Rightarrow \gamma := \sup(F[\lambda]) \in A \Rightarrow \gamma = \min\{x \in A : \forall \xi < \lambda(F(\xi) < x)\} \overset{8.7}{\Rightarrow} \gamma = F(\lambda).\triangle$

Bemerkung:
Die Funktion $\alpha \mapsto \aleph_\alpha$ ist eine Normalfunktion. (Siehe 9.10)

Lemma 10.5
Ist $F : On \to On$ eine Normalfunktion, so ist die Klasse $\{\beta : F(\beta) = \beta\}$ aller Fixpunkte von F abgeschlossen und unbeschränkt. Die Ordnungsfunktion dieser Klasse wird mit F' bezeichnet, und heißt *Ableitung* von F. Es gilt: $F'(0) = \sup_{n\in\omega} F^{(n)}(0)$, $F'(\beta+1) = \sup_{n\in\omega} F^{(n)}(F'(\beta)+1)$.
Beweis :
1. *abgeschlossen:* Sei $\emptyset \neq u \subseteq On$ mit $\forall \eta \in u(F(\eta) = \eta)$, und sei $\beta := \sup(u)$.
Dann $F(\beta) = \sup\{F(\eta) : \eta \in u\} = \sup\{\eta : \eta \in u\} = \beta$.
2. *unbeschränkt:* Für $\gamma \in On$ sei $\gamma^* := \sup_{n\in\omega} F^{(n)}(\gamma)$. Wir zeigen $\gamma^* = \min\{\beta : \gamma \leq \beta = F(\beta)\}$. Daraus folgen dann auch die beiden restlichen Behauptungen. – Wegen $\forall \xi(\xi \leq F(\xi))$ gilt $\gamma \leq \gamma^*$. Für $\beta \in On$ mit $\gamma \leq \beta = F(\beta)$ folgt durch vollständige Induktion $\forall n(F^{(n)}(\gamma) \leq \beta)$, also $\gamma^* \leq \beta$.
Schließlich gilt $F(\gamma^*) = \sup_{n\in\omega} F^{(n+1)}(\gamma) = \gamma^*$. $\triangle$

Lemma
Sind $A, B \subseteq On$ abgeschlossen und unbeschränkt, so auch $A \cap B$.
Beweis :
1. $A \cap B$ abgeschlossen: klar.
2. Sei $\gamma \in On$.
Definition: $\alpha_0 := \beta_0 := \gamma$, $\alpha_{n+1} := \min\{\alpha \in A : \alpha_n, \beta_n < \alpha\}$, $\beta_{n+1} := \min\{\beta \in B : \alpha_n, \beta_n < \beta\}$.
Dann $\alpha^* := \sup\{\alpha_n : 0 < n \in \omega\} \in A$, $\beta^* := \sup\{\beta_n : 0 < n \in \omega\} \in B$ und $\gamma < \alpha^*$.
Ferner gilt $\alpha^* \leq \sup\{\beta_{n+1} : 0 < n \in \omega\} = \beta^*$ und ebenso $\beta^* \leq \alpha^*$, also $\alpha^* = \beta^* \in A \cap B$. $\triangle$

Definition von $\alpha + \beta$ durch transfinite Rekursion nach β
$\alpha + 0 := \alpha$, $\quad \alpha + (\beta+1) := (\alpha+\beta)+1$, $\quad \alpha + \lambda := \sup\{\alpha + \eta : \eta < \lambda\}$.

Genaue Ausführung der transfiniten Rekursion: Sei $R := \{((x,y),(x,z)) : x,y,z \in On \ \& \ y < z\}$ und $G : (On \times On) \times V \to V$, $G((\alpha,0),f) := \alpha$, $G((\alpha,\beta+1),f) := f((\alpha,\beta)) + 1$, $G((\alpha,\lambda),f) := \sup(\mathrm{ran}(f))$.
Dann $\alpha + \beta = F((\alpha,\beta))$ mit $F(x) := G(x, F|x_R)$. [Im zweiten Fall der Definition von G haben hier Gebrauch von folgender *Konvention* gemacht: *Ist f keine Funktion oder $x \notin \mathrm{dom}(f)$, so sei $f(x) := 0$.*]

Abkürzung: $1 := 0'$.
Diese Abkürzung ist verträglich mit dem bisherigen Gebrauch der Zeichenreihe "+1" als Synomym für "$'$", denn es gilt $\alpha' = \alpha + 0'$.

Lemma 10.6

a) Für jedes α ist $\beta \mapsto \alpha + \beta$ die Ordnungsfunktion von $\{\gamma : \gamma \geq \alpha\}$ und folglich eine Normalfunktion.

b) $\beta_0 < \beta_1 \Rightarrow \alpha + \beta_0 < \alpha + \beta_1$

c) $\beta \leq \alpha + \beta$

d) $\forall \gamma \geq \alpha \exists! \beta (\alpha + \beta = \gamma)$

e) $\alpha_0 \leq \alpha_1 \Rightarrow \alpha_0 + \beta \leq \alpha_1 + \beta$

f) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$

g) $\alpha, \beta < \omega \Rightarrow \alpha + \beta = \beta + \alpha < \omega$

h) $0 < k < \omega \Rightarrow k + \omega = \omega < \omega + k$

Beweis :

a)–d) Sei $+_\alpha(\beta) := \alpha + \beta$. Nach 10.2 ist $+_\alpha$ Normalfunktion. Daraus folgt b) und c). Ferner ist $+_\alpha$ die Ordnungsfunktion von $\mathrm{ran}(+_\alpha)$, und $\mathrm{ran}(+_\alpha) \subseteq \{\gamma : \gamma \geq \alpha\}$. Mit 10.3c folgt umgekehrt $\forall \gamma \geq \alpha \exists \beta (\alpha + \beta \leq \gamma < \alpha + (\beta + 1) = (\alpha + \beta) + 1)$, d.h. $\forall \gamma \geq \alpha \exists \beta (\alpha + \beta = \gamma)$.

e) Induktion nach β. f) Induktion nach γ.

g) Mit 9.13b,c folgt durch Induktion nach β: $\alpha, \beta < \omega \Rightarrow \alpha + \beta = \alpha \hat{+} \beta \in \omega$.

h) $\omega \leq k + \omega = \sup\{k + n : n < \omega\} \leq \omega < \omega + k$. $\triangle$

Definition von $\alpha \cdot \beta$ durch transfinite Rekursion nach β

$\alpha \cdot 0 := 0,\ \alpha \cdot (\beta + 1) := (\alpha \cdot \beta) + \alpha,\ \alpha \cdot \lambda := \sup\{\alpha \cdot \eta : \eta < \lambda\}$.

Lemma 10.7

a) Für jedes $\alpha \geq 1$ ist $\beta \mapsto \alpha \cdot \beta$ eine Normalfunktion.

b) $\alpha_0 \leq \alpha_1 \Rightarrow \alpha_0 \cdot \beta \leq \alpha_1 \cdot \beta$

c) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

d) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

e) $0 \cdot \alpha = \alpha \cdot 0 = 0 \ \& \ 1 \cdot \alpha = \alpha \cdot 1 = \alpha$

f) $\alpha, \beta < \omega \Rightarrow \alpha \cdot \beta = \beta \cdot \alpha < \omega$

Definition von α^β durch transfinite Rekursion nach β

$\alpha^0 := 1,\ \alpha^{\beta+1} := \alpha^\beta \cdot \alpha,\ \alpha^\lambda := \sup\{\alpha^\eta : \eta < \lambda\}$.

Lemma 10.8

Für $\alpha \geq 2$ gilt:

a) $\beta \mapsto \alpha^\beta$ ist Normalfunktion.

b) $\alpha \leq \gamma \Rightarrow \alpha^\beta \leq \gamma^\beta$

c) $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$

d) $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$

e) $\beta > \beta_0 > ... > \beta_n \ \& \ \delta_0, ..., \delta_n < \alpha \Rightarrow \alpha^\beta > \alpha^{\beta_0} \cdot \delta_0 + ... + \alpha^{\beta_n} \cdot \delta_n$.

Beweis :

e) Ind. nach n: I.V. $\Rightarrow \alpha^{\beta_0} > \alpha^{\beta_1} \cdot \delta_1 + ... + \alpha^{\beta_n} \cdot \delta_n \Rightarrow a^\beta \geq \alpha^{\beta_0} \cdot \alpha \geq \alpha^{\beta_0} \cdot \delta_0 + \alpha^{\beta_0} > \alpha^{\beta_0} \cdot \delta_0 + ... + \alpha^{\beta_n} \cdot \delta_n$.

$\triangle$

Satz 10.9

a) Zu $\alpha \geq 2$ und $\gamma \geq 1$ existieren eindeutig β, δ, γ_0 mit $0 < \delta < \alpha \ \& \ \gamma_0 < \alpha^\beta \ \& \ \gamma = \alpha^\beta \cdot \delta + \gamma_0$.

b) Zu $\alpha \geq 2$ und $\gamma \geq 1$ existieren eindeutig $\beta_0 > ... > \beta_n$ und $0 < \delta_0, ..., \delta_n < \alpha$ mit
$\gamma = \alpha^{\beta_0} \cdot \delta_0 + ... + \alpha^{\beta_n} \cdot \delta_n$.

Die Darstellung in b) nennt man die *Cantorsche Normalform von γ zur Basis α*.

Beweis :
a) *Eindeutigkeit:* Sei $\gamma = \alpha^\beta \cdot \delta + \gamma_0 = \alpha^{\beta_1} \cdot \delta_1 + \gamma_1$ mit $0 < \delta, \delta_1 < \alpha \ \& \ \gamma_0 < \alpha^\beta \ \& \ \gamma_1 < \alpha^{\beta_1}$. Dann $\alpha^\beta \leq \gamma < \alpha^{\beta+1} \ \& \ \alpha^{\beta_1} \leq \gamma < \alpha^{\beta_1+1}$, also $\beta = \beta_1$. Weiter folgt nun $\alpha^\beta \cdot \delta \leq \gamma < \alpha^\beta \cdot (\delta + 1)$ und $\alpha^\beta \cdot \delta_1 \leq \gamma < \alpha^\beta \cdot (\delta_1 + 1)$, also auch $\delta = \delta_1$. Aus $\alpha^\beta \cdot \delta + \gamma_0 = \alpha^\beta \cdot \delta + \gamma_1$ folgt schließlich $\gamma_0 = \gamma_1$.
Existenz: Nach 10.3c existiert ein β mit $\alpha^\beta \leq \gamma < \alpha^{\beta+1}$, d.h. $\alpha^\beta \cdot 1 \leq \gamma < \alpha^\beta \cdot \alpha$. Wiederum mit 10.3 (im wesentlichen) folgt daraus $\alpha^\beta \cdot \delta \leq \gamma < \alpha^\beta \cdot (\delta + 1) = \alpha^\beta \cdot \delta + \alpha^\beta$ mit $0 < \delta < \alpha$. Nach 10.6 existiert deshalb ein $\gamma_0 < \alpha^\beta$ mit $\gamma = \alpha^\beta \cdot \delta + \gamma_0$.
b) folgt aus a) und 10.8e mittels Induktion nach γ. △

Definition (Additive Hauptzahlen)
$\gamma \in On$ heißt *additive Hauptzahl*, falls $\gamma > 0 \wedge \forall \xi, \eta < \gamma (\xi + \eta < \gamma)$.

$H :=$ Klasse aller additiven Hauptzahlen.

Lemma 10.10
a) $\alpha \mapsto \omega^\alpha$ ist die Ordnungsfunktion der Klasse H aller additiven Hauptzahlen.
b) $\gamma \in H \ \Leftrightarrow \ \gamma > 0 \wedge \forall \xi < \gamma (\xi + \gamma = \gamma)$.
Beweis :
a) "⇒": Wir zeigen $\omega^\alpha \in H$:
1. $\omega^0 \in H$ ist trivial.
2. $0 < \xi, \eta < \omega^\alpha \ \Rightarrow \ \xi, \eta < \omega^{\beta+1}$ für ein $\beta < \alpha \ \Rightarrow \ \xi, \eta < \omega^\beta \cdot n$ für ein $n < \omega \ \Rightarrow$
$\xi + \eta < \omega^\beta \cdot n + \omega^\beta \cdot n = \omega^\beta \cdot (n + n) < \omega^{\beta+1} \leq \omega^\alpha$.
"⇐": Wir zeigen: $\gamma \notin \{\omega^\alpha : \alpha \in On\} \ \Rightarrow \ \gamma \notin H$.
Sei $1 \leq \gamma \notin \{\omega^\alpha : \alpha \in On\}$. Dann $\gamma = \omega^\beta \cdot n + \gamma_0$ mit $0 < n < \omega \ \& \ \gamma_0 < \omega^\beta$ und $1 < n \vee 0 < \gamma_0$. Für $\eta := \omega^\beta \cdot (n-1) + \gamma_0$ gilt nun $0 < \eta < \omega^\beta \cdot n \leq \gamma$ und $\omega^\beta < \omega^\beta + \eta = \gamma$, d.h. $\gamma \notin H$.
b) "⇒": Sei $\gamma \in H$ und $\xi < \gamma$. Dann $\xi + \gamma = \sup\{\xi + \eta + 1 : \eta < \gamma\} \leq \gamma$.
"⇐": Gelte $\gamma > 0 \ \& \ \forall \xi < \gamma (\xi + \gamma = \gamma)$, und sei $\xi, \eta < \gamma$. Dann $\xi + \eta < \xi + \gamma = \gamma$. △

Definition
$\alpha =_{NF} \alpha_0 + ... + \alpha_n \ :\Leftrightarrow \ \alpha = \alpha_0 + ... + \alpha_n \ \& \ \alpha_0 \geq ... \geq \alpha_n \ \& \ \alpha_0, ..., \alpha_n \in H$.

Lemma 10.11
a) Zu jedem $\alpha > 0$ existiert genau ein Tupel $\alpha_0, ..., \alpha_n$ mit $\alpha =_{NF} \alpha_0 + ... + \alpha_n$.
b) $\alpha =_{NF} \alpha_0 + ... + \alpha_n \ \& \ k < n \ \Rightarrow \ \alpha_0 + ... + \alpha_k < \alpha \ \& \ \alpha_{k+1} + ... + \alpha_n < \alpha$.
Beweis :
a) folgt aus dem Satz über die Cantorsche-Normalform (zur Basis ω) unter Berücksichtigung der Gleichung $\omega^\beta \cdot n = \omega^\beta + ... + \omega^\beta$.
b) 1. $\alpha_0 + \ldots + \alpha_k < \alpha_0 + \ldots + \alpha_{k+1} \leq \alpha$.
2. $\alpha_{k+1} + ... + \alpha_n \leq \alpha_k + ... + \alpha_{n-1} < \alpha_k + ... + \alpha_n \leq \alpha$. △

Definition (Natürliche Summe oder Hessenberg-Summe)
$\alpha \# 0 := 0 \# \alpha := \alpha$.
Für $\alpha =_{NF} \alpha_0 + ... + \alpha_n$ und $\beta =_{NF} \alpha_{n+1} + ... + \alpha_{n+m}$ sei $\alpha \# \beta := \alpha_{p(0)} + ... + \alpha_{p(m+n)}$,
wobei p eine Permutation von $m + n + 1$ mit $\alpha_{p(0)} \geq ... \geq \alpha_{p(m+n)}$.

Lemma 10.12
a) $\alpha\#\beta = \beta\#\alpha$,
b) $(\alpha\#\beta)\#\gamma = \alpha\#(\beta\#\gamma)$,
c) $\alpha_0 \geq ... \geq \alpha_n$ additive Hauptzahlen $\Rightarrow\ \alpha_0 + ... + \alpha_n = \alpha_0\#...\#\alpha_n$,
d) $\beta < \gamma\ \Rightarrow\ \alpha\#\beta < \alpha\#\gamma$,
e) $\alpha, \beta < \omega^\gamma\ \Rightarrow\ \alpha\#\beta < \omega^\gamma$,
f) $\alpha + \beta \leq \alpha\#\beta$.
Beweis :
a),b),c),e) klar.
d) Wegen b), c) reicht es, die Behauptung für $\alpha \in H$ zu beweisen. Dies geschieht durch Induktion nach γ.
Sei $\beta =_{NF} \beta_0 + ... + \beta_n$ und $\gamma =_{NF} \gamma_0 + ... + \gamma_m$. Wegen $\beta < \gamma$ ist dann $\beta_0 \leq \gamma_0$.
Fall 1: $\alpha \geq \gamma_0$. Dann $\alpha\#\beta = \alpha + \beta < \alpha + \gamma = \alpha\#\gamma$.
Fall 2: $\beta_0, \alpha < \gamma_0$. Dann $\alpha\#\beta < \gamma_0 < \alpha\#\gamma$.
Fall 3: $\alpha < \beta_0 = \gamma_0$. Dann $\alpha\#\beta = \beta_0 + (\alpha\#\hat{\beta})\ \ \&\ \ \alpha\#\gamma = \beta_0 + (\alpha\#\hat{\gamma})$ wobei
$\beta_1 + ... + \beta_n = \hat{\beta} < \hat{\gamma} = \gamma_1 + ... + \gamma_m$. Mit I.V. folgt daraus $\alpha\#\beta < \alpha\#\gamma$.
f) 1. Ist $\alpha \in H$, so $\alpha + \beta = \beta \leq \alpha\#\beta$ oder $\alpha + \beta = \alpha\#\beta$.
2. Für beliebiges α folgt die Behauptung aus 1. und b),c), sowie 10.6 . $\triangle$

Multimengen

Definition
Eine *Multimenge* ist eine Funktion M mit $\mathrm{ran}(M) \subseteq \omega \setminus \{0\}$. x heißt *Element der Multimenge* M (geschrieben $x \in' M$), falls $x \in \mathrm{dom}(M)$. Ist M Multimenge und $x \notin \mathrm{dom}(M)$, so sei $M(x) := 0$.
Vereinigung $\sqcup$, *Durchschnitt* $\sqcap$ und *Differenz* $-$ von Multimengen seien wie folgt definiert:
$\mathrm{dom}(M \sqcup N) := \mathrm{dom}(M) \cup \mathrm{dom}(N)$ und $(M \sqcup N)(x) := M(x) + N(x)$,
$\mathrm{dom}(M \sqcap N) := \mathrm{dom}(M) \cap \mathrm{dom}(N)$ und $(M \sqcap N)(x) := \min\{M(x), N(x)\}$,
$\mathrm{dom}(M - N) := \{x \in \mathrm{dom}(M) : N(x) < M(x)\}$ und $(M - N)(x) := M(x) \dot{-} N(x)$.
Eine Multimenge M heißt *endlich*, falls $\mathrm{dom}(M)$ endlich ist.
Jede endliche Multimenge ist also von der Form $\{(x_0, k_0), ..., (x_{n-1}, k_{n-1})\}$ mit $card\{x_0, ..., x_{n-1}\} = n \in \omega$ und $k_0, ..., k_{n-1} \in \omega$.

Bemerkung: Für Multimengen M, N gilt $M = (M \sqcap N) \sqcup (M - N)$.

Sei nun $\prec$ eine Relation. Die durch $\prec$ induzierte *Multimengenordnung* $\prec_{mul}$ ist folgendermaßen definiert:
$N \prec_{mul} M\ :\Leftrightarrow\ N \neq M\ \ \&\ \ \forall x \in' N - M \exists y \in' M - N (x \prec y)$.

Lemma 10.13
Sei $\prec$ eine Relation, und sei $o : V \to On$ mit $\forall x, y (x \prec y \to o(x) < o(y))$.
Für jede endliche Multimenge $M = \{(x_0, k_0), \ldots, (x_{n-1}, k_{n-1})\}$ sei
$o(M) := \omega^{o(x_0)} \cdot k_0 \# \ldots \# \omega^{o(x_{n-1})} \cdot k_{n-1}$.
(Wegen der Kommutativität und Assoziativität von # ist dies eine korrekte Definition.)
Dann gilt für alle endlichen Multimengen M, N:
a) $o(M \sqcup N) = o(M)\#o(N)$,
b) $N \prec_{mul} M\ \Rightarrow\ o(N) < o(M)$.
Beweis :
a) "klar"
b) Nach a) gilt $o(N) = o(M \sqcap N)\#o(N - M)$ und $o(M) = o(M \sqcap N)\#o(M - N)$.
Noch zu zeigen $o(N - M) < o(M - N)$.

Fall 1: $N-M = \emptyset$. Dann $o(N-M) = 0$ und (wegen $N \neq M$) $M-N \neq \emptyset$, also $0 < o(M-N)$.
Fall 2: $N-M \neq \emptyset$. Wegen $N \prec_{mul} M$ ist dann auch $M-N \neq \emptyset$, und für $\alpha := \max\{o(x) : x \in' N-M\}$ und $\beta := \max\{o(x) : x \in' M-N\}$ gilt $\alpha < \beta$. Es folgt $o(N-M) < \omega^{\alpha+1} \leq \omega^{\beta} \leq o(M-N)$. $\triangle$

Korollar
Ist $\prec$ wohlfundiert, so ist $\prec_{mul}$ eingeschränkt auf die Klasse der endlichen Multimengen fundiert.
Beweis :
Mittels $\prec$-Rekursion definieren wir $o(x) := \sup\{o(y) + 1 : y \prec x\}$.
Daraus folgt mit 10.13b die Fundiertheit von $\prec_{mul}$.

11 Ergänzungen zur Vorlesung "Logik I"

Vereinbarungen:
Ist F keine Funktion oder $x \notin \mathrm{dom}(F)$, so sei $F(x) := 0$.
Eine Funktion f mit $\mathrm{dom}(f) = n \in \omega$ schreiben wir auch als $(f(0), ..., f(n-1))$, und nennen sie ein n-Tupel.

1. Transfinite Induktion und Rekursion für beliebige wohlfundierte Relationen
Wir zeigen, daß in Lemma 8.2 und Satz 8.3 auf die Voraussetzung "R transitiv" verzichtet werden kann.

Definition (transitive Hülle einer Relation R)
$R^* := \{(y, x) : \exists(x_0, ..., x_n)[yRx_n \wedge x_nRx_{n-1} \wedge \ldots \wedge x_1Rx_0 = x]\}$.

Lemma 11.1
Für jede Relation R gilt:
a) $R \subseteq R^*$ und R^* ist transitiv.
b) $R \subseteq Q \subseteq V \times V$ & Q transitiv $\Rightarrow$ $R^* \subseteq Q$.
c) $R \in V \Rightarrow R^* \in V$.
d) $\forall x(x_R \in V) \Rightarrow \forall x(x_{R^*} \in V)$.
Beweis :
a) $R \subseteq R^*$ ist trivial. Gelte nun $zRy_mRy_{m-1} \ldots y_1Ry_0 = y$ und $yRx_nRx_{n-1} \ldots x_1Rx_0 = x$.
Dann $zRx_{n+m+1}Rx_{n+m} \ldots x_1Rx_0 = x$ mit $x_{n+i+1} := y_i$.
b) Durch Induktion nach n zeigt man: $yRx_nRx_{n-1} \ldots x_1Rx_0 = x \Rightarrow (y, x) \in Q$.
c) Sei $R \in V$. Dann sind auch $a := \mathrm{dom}(R) \cup \mathrm{ran}(R)$ und $a \times a$ Mengen. Ferner ist $a \times a$ offenbar eine transitive Relation, die R umfaßt. Mit b) folgt also $R^* \subseteq a \times a$ und weiter $R^* \in V$.
d) Sei $a \in V$. Definition: $h_0 := \{a\}$, $h_{n+1} := \bigcup\{x_R : x \in h_n\}$.
Durch Induktion nach n folgt $(x_nRx_{n-1} \ldots x_1Rx_0 \in a \Rightarrow x_n \in h_n)$, und somit $a_{R^*} \subseteq \bigcup_{n\in\omega} h_n \in V$. $\triangle$

Lemma 11.2
Für jede wohlfundierte Relation R gelten die Prinzipien (I) (Existenz minimaler Elemente) und (II) (Induktion über R). (D.h. in 8.2 kann auf die Voraussetzung "R transitiv" verzichtet werden).
Beweis von (I): Gelte $u \in C$.
Fall 1: $\forall y \in u_R(y \notin C)$. Dann fertig.
Fall 2: $\exists y \in u_R(y \in C)$. Dann $a := u_{R^*} \cap C \neq \emptyset$. Da R fundiert ist, existiert ein $c \in a$ mit $\forall y \in c_R(y \notin a)$.
Aus $c \in u_{R^*}$ folgt $c_R \subseteq u_{R^*}$. Somit $c \in C$ und $\forall y \in c_R(y \notin C)$. $\triangle$

Lemma 11.3
Ist R eine wohlfundierte Relation, so auch R^*.

Beweis :
Nach 8.1 (und wegen 11.1d) reicht es, das Induktionsprinzip für R^* zu beweisen.
Gelte (1) $\forall x(x_{R^*} \subseteq C \to x \in C)$. Zu zeigen ist: $\forall x(x \in C)$.
Sei $\bar{C} := \{x : x_{R^*} \subseteq C\}$. Wegen (1) gilt dann (2) $\bar{C} \subseteq C$. Ferner gilt: (3) $\forall x(x_R \subseteq \bar{C} \to x \in \bar{C})$.
Beweis von (3): $x_R \subseteq \bar{C} \overset{(2)}{\Rightarrow} x_R \subseteq C \wedge \forall y \in x_R(y_{R^*} \subseteq C) \Rightarrow x_{R^*} \subseteq C \Rightarrow x \in \bar{C}$.
Aus (2),(3) und 11.2 folgt $\forall x(x \in \bar{C} \subseteq C)$. △

Lemma 11.4
Für jede wohlfundierte Relation R gilt das Prinzip der Rekursion über R.
(D.h. in 8.3 kann auf die Voraussetzung "R transitiv" verzichtet werden.)
Beweis :
Sei R wohlfundiert und $G : A \times V \to V$. Wir definieren $G' : A \times V \to V$, $G'(x, f) := G(x, f|x_R)$. Nach 11.3 und 11.1 ist R^* wohlfundiert und transitiv; und nach 8.3 existiert genau ein $F : A \to V$ mit $F(x) = G'(x, F|x_{R^*})$ für alle $x \in A$. Es gilt aber $G'(x, F|x_{R^*}) = G(x, F|x_R)$. △

Da die Elementrelation $\in$ wohlfundiert ist (aufgrund des Fundierungsaxioms), erhält man als Spezialfall von 11.2 und 11.4 die folgenden Prinzipien der sog. $\in$-Induktion bzw. $\in$-Rekursion:
($\in$-Induktion) $\forall x(x \subseteq C \to x \in C) \to \forall x(x \in C)$
($\in$-Rekursion) Zu $G : V \to V$ existiert genau ein $F : V \to V$ mit $F(x) = G(F|x)$ für alle x.

2. Induktive Definitionen

Sei A eine Menge und $\preceq$ eine reflexive, antisymmetrische und transitive Relation auf A.
Ferner gelte: Jede $\preceq$-Kette $X \subseteq A$ besitzt ein Supremum in A.
Sei $\Phi : A \to A$ monoton bzgl. $\preceq$, d.h. $\forall x, y \in A(y \preceq x \to \Phi(y) \preceq \Phi(x))$.

Definition
$$\mathrm{I}^\alpha_\Phi := \begin{cases} \Phi(\sup_{\xi<\alpha} \mathrm{I}^\xi_\Phi) & \text{falls das sup existiert} \\ \sup(\emptyset) & \text{sonst.} \end{cases}$$

Satz 11.5
a) $\alpha < \beta \Rightarrow \mathrm{I}^\alpha_\Phi \preceq \mathrm{I}^\beta_\Phi$.
b) $\mathrm{I}^{\alpha+1}_\Phi = \Phi(\mathrm{I}^\alpha_\Phi)$.
c) Es existiert ein α mit $\mathrm{I}^\alpha_\Phi = \mathrm{I}^{\alpha+1}_\Phi$.
d) Gilt $\mathrm{I}^\alpha_\Phi = \mathrm{I}^{\alpha+1}_\Phi$, so $\forall \beta \geq \alpha(\mathrm{I}^\alpha_\Phi = \mathrm{I}^\beta_\Phi)$ und $\mathrm{I}^\alpha_\Phi = \min_\preceq\{x \in A : \Phi(x) \preceq x\}$;
insbesondere ist I^α_Φ der $\preceq$-kleinste Fixpunkt von Φ.
Beweis :
a) Induktion nach β: Nach I.V. ist $\{\mathrm{I}^\xi_\Phi : \xi < \beta\}$ eine Kette; also existiert $\sup_{\xi<\beta} \mathrm{I}^\xi_\Phi$ und $\sup_{\xi<\alpha} \mathrm{I}^\xi_\Phi$; und wegen $\alpha < \beta$ gilt $\sup_{\xi<\alpha} \mathrm{I}^\xi_\Phi \preceq \sup_{\xi<\beta} \mathrm{I}^\xi_\Phi$. Mit der Montonie von Φ folgt nun $\mathrm{I}^\alpha_\Phi \preceq \mathrm{I}^\beta_\Phi$.
b) $\mathrm{I}^{\alpha+1}_\Phi = \Phi(\sup_{\xi<\alpha+1} \mathrm{I}^\xi_\Phi) = \Phi(\mathrm{I}^\alpha_\Phi)$.
c) Andernfalls hätten wir $\forall \alpha, \beta(\alpha < \beta \to \mathrm{I}^\alpha_\Phi \prec \mathrm{I}^\beta_\Phi)$, und damit wäre $F : On \to A$, $\alpha \mapsto \mathrm{I}^\alpha_\Phi$ injektiv. Dann könnte aber A keine Menge sein.
d) 1. $\mathrm{I}^\alpha_\Phi = \mathrm{I}^{\alpha+1}_\Phi = \Phi(\mathrm{I}^\alpha_\Phi)$.
2. $\Phi(p) \preceq p \Rightarrow \forall \beta(\mathrm{I}^\beta_\Phi \preceq p)$.
Beweis durch Induktion nach β: $\forall \xi < \beta(\mathrm{I}^\xi_\Phi \preceq p) \Rightarrow \sup_{\xi<\beta} \mathrm{I}^\xi_\Phi \preceq p \Rightarrow \mathrm{I}^\beta_\Phi = \Phi(\sup_{\xi<\beta} \mathrm{I}^\xi_\Phi) \preceq \Phi(p) \preceq p$. △

Korollar
Sei M eine Menge, und $\Phi : \mathrm{Pot}(M) \to \mathrm{Pot}(M)$ monoton bzgl. $\subseteq$. Definition: $\mathrm{I}^\alpha_\Phi := \Phi(\bigcup_{\xi<\alpha} \mathrm{I}^\xi_\Phi)$.
Dann existiert α mit $\Phi(\mathrm{I}^\alpha_\Phi) = \mathrm{I}^\alpha_\Phi$, und für jedes derartige α gilt $\mathrm{I}^\alpha_\Phi = \bigcap\{x \subseteq M : \Phi(x) \subseteq x\}$.

Beispiel:
$M :=$ Menge aller endlichen Zeichenreihen über $\mathcal{L} \cup \mathrm{Var}$.
$\Phi(X) := \mathrm{Var} \cup \{ft_1...t_n : f \in \mathcal{L}\ n\text{-stellig} \ \ \& \ \ t_1, ..., t_n \in X\}$
Dann ist $\mathrm{I}_\Phi^{\omega+1} = \mathrm{I}_\Phi^\omega = \bigcup_{n<\omega} \mathrm{I}_\Phi^n$, und wegen $\Phi(\mathrm{I}_\Phi^\omega) = \mathrm{I}_\Phi^\omega$ gilt:
$t \in \mathrm{I}_\Phi^\omega \ \Leftrightarrow t \in \mathrm{Var}$ oder $t = ft_1...t_n$ mit $t_1, ..., t_n \in \mathrm{I}_\Phi^\omega$.

3. Beweis des Vollständigkeitssatzes für Sprachen $\mathcal{L}$ beliebiger Kardinalität

Satz 2.7 (Vollständigkeitssatz)
Jede konsistente Formelmenge Γ ist erfüllbar.
Beweis :
Sei Γ konsistente Formelmenge. Außerdem setzen wir voraus, daß alle Formeln in Γ geschlossen sind. (Der allgemeine Fall kann mittels Lemma 2.5 leicht auf diesen Fall zurückgeführt werden.)
Definition: $\mathcal{L}_0 := \mathcal{L}, \quad \mathcal{L}_{n+1} := \mathcal{L}_n \cup \{e_{n,\forall xA} : \forall xA \text{ ist } \mathcal{L}_n\text{-Satz}\}, \quad \mathcal{L}' := \bigcup_{n\in\omega} \mathcal{L}_n$.
Hierbei seien die $e_{n,\forall xA}$ jeweils neue Konstanten.
$\Sigma_n := \{A_x(e_{n,\forall xA}) \to \forall xA : \forall xA \text{ ist } \mathcal{L}_n\text{-Satz}\}, \quad \Sigma_\omega := \Gamma \cup \bigcup_{n\in\omega} \Sigma_n$.
Wir haben jetzt zu unterscheiden zwischen Herleitbarkeit in $\mathcal{L}$ und Herleitbarkeit in $\mathcal{L}'$. Allgemein nennen wir die Herleitung $(A_0, ..., A_n)$ eine $\mathcal{L}$-Herleitung, wenn $A_0, ..., A_n$ Formeln der Sprache $\mathcal{L}$ sind.
$\Delta \vdash A \ :\Leftrightarrow$ Es gibt eine $\mathcal{L}$-Herleitung von A aus Δ,
$\Delta \vdash' A \ :\Leftrightarrow$ Es gibt eine $\mathcal{L}'$-Herleitung von A aus Δ.

HS 1: $\Sigma_\omega \vdash' \bot \ \Rightarrow \ \Gamma \vdash \bot$.
Beweis: Nach Voraussetzung existiert eine endliche Teilmenge $\{A_0, ..., A_k\}$ von $\bigcup_{n\in\omega} \Sigma_n$ mit $\Gamma \cup \{A_0, ..., A_k\} \vdash' \bot$. Sei n die kleinste Zahl mit $\{A_0, ..., A_k\} \subseteq \bigcup_{i\le n} \Sigma_i$. Ohne Einschränkung der Allgemeinheit können wir $A_k \in \Sigma_n$ annehmen. Dann gilt $A_k = B_x(e_{n,\forall xB}) \to \forall xB$, wobei $\forall xB$ ein $\mathcal{L}_n$-Satz ist. Nach Definition tritt die Konstante $e_{n,\forall xB}$ in keiner Formel der Menge $\Gamma \cup \{A_0, ..., A_{k-1}, \forall xB\}$ auf. (Die Formeln $A_0, ..., A_k$ seien natürlich paarweise verschieden.) Sei $\Gamma_1 := \Gamma \cup \{A_0, ..., A_{k-1}\}$. Aus $\Gamma \cup \{A_0, ..., A_k\} \vdash' \bot$ folgt mit dem Deduktionstheorem und Lemma 2.5 $\Gamma_1 \vdash' \neg(B \to \forall xB)$. Daraus folgt weiter $\Gamma_1 \vdash' \bot$. [Begründung: $\Gamma_1 \vdash' \neg(B \to \forall xB) \ \Rightarrow \ \Gamma_1 \vdash' B \ \ \& \ \ \Gamma_1 \vdash' \neg\forall xB \ \Rightarrow$
$\Gamma_1 \vdash' \forall xB \ \ \& \ \ \Gamma_1 \vdash' \neg\forall xB$]
Nach k Schritten ergibt sich auf diese Weise $\Gamma \vdash' \bot$. Nun ersetzen wir noch in der Herleitung von $\bot$ aus Γ alle Konstanten $e \in \mathcal{L}' \setminus \mathcal{L}$ durch eine "neue" Variablen, und erhalten so die Behauptung $\Gamma \vdash \bot$.

Nach Voraussetzung und HS 1 ist Σ_ω konsistent. Mit dem Zornschen Lemma folgt daraus die Existenz einer maximal-konsistenten Obermenge $\Sigma' \supseteq \Sigma_\omega$.
Genauer gesagt: Σ' ist eine Menge von $\mathcal{L}'$-Sätzen mit
(0) $\Sigma_\omega \subseteq \Sigma'$,
(i) A $\mathcal{L}'$-Satz $\ \& \ A \notin \Sigma' \ \Rightarrow \ \Sigma' \cup \{A\} \vdash' \bot$,
(ii) $\neg\forall xA \in \Sigma' \ \Rightarrow$ Es existiert eine Konstante e mit $\neg A_x(e) \in \Sigma'$.
[Beweis von (ii): Sei $\forall xA$ ein $\mathcal{L}_n$-Satz mit $\neg\forall xA \in \Sigma'$, und sei $e := e_{n,\forall xA}$.
Dann ist $A_x(e) \to \forall xA \in \Sigma_\omega \subseteq \Sigma'$, und somit gilt $\Sigma' \vdash' \neg\forall xA \to \neg A_x(e)$. Darau folgt $\Sigma' \vdash \neg A_x(e)$ und weiter $\neg A_x(e) \in \Sigma'$ (wegen (i) und der Konsistenz von Σ').]
Σ' ist also eine vollständige Henkin-Theorie, und nach Lemmata 2.6, 1.4 existiert eine $\mathcal{L}'$-Struktur $\mathcal{M}'$ mit $\mathcal{M}' \models \Sigma'$, nämlich das kanonische Modell von Σ'. Wegen $\Gamma \subseteq \Sigma'$ folgt daraus die Behauptung. $\triangle$

4. Abänderung des Kalküls aus Abschnitt 2

Modifikation von Abschnitt 2 der Vorlesung: $(\to 4)$ wird auf Primformeln A eingeschränkt.
Das beeinträchtigt nicht die Beweise von 2.1, 2.2, 2.4.

Neues LEMMA: $\vdash \neg\neg A \to A$, für jede Formel A.
Beweis durch Induktion nach der Länge von A:
Gelte schon $\vdash \neg\neg B \to B$.

1. $A, A \to B \vdash B$
$A, \neg B, A \to B \vdash \bot$
$A, \neg B \vdash \neg(A \to B)$; $\quad \neg(A \to B), \neg\neg(A \to B) \vdash \bot$
$A, \neg B, \neg\neg(A \to B) \vdash \bot$
$A, \neg\neg(A \to B) \vdash \neg\neg B$
$A, \neg\neg(A \to B) \vdash B$

2. $\vdash \forall x B \to B$
$\forall x B \vdash B$; $\quad B, \neg B \vdash \bot$
$\neg B, \forall x B \vdash \bot$
$\neg B \vdash \neg\forall x B$
$\neg\neg\forall x B, \neg B \vdash \bot$
$\neg\neg\forall x B \vdash B$
$\neg\neg\forall x B \vdash \forall x B$.

12 Beweistheoretische Analyse des Axiomensystems Z der Arithmetik

Sei PR die in Abschnitt 4 eingeführte Menge von Funktionszeichen für alle primitiv rekursiven Funktionen. Ist t ein geschlossener PR-Term, so sei $val(t)$ der Wert von t in der Standardstruktur $\mathcal{N}$. ($val(t) := t^{\mathcal{N}}$)
Abkürzung: $E_x(n) := E_x(\underline{n})$ für jeden PR-Ausdruck E und $n \in \mathbb{N}$.

Das **Axiomensystem Z** besteht aus den Allabschlüssen der folgenden PR-Formeln:
$\neg(\mathsf{S}x = \mathbf{0})$,
$\mathsf{S}x = \mathsf{S}y \to x = y$,
$\mathbf{0}^n x_1 ... x_n = \mathbf{0}$,
$\mathsf{I}_i^n x_1 ... x_n = x_i$,
$(\circ h g_1 ... g_m) x_1 ... x_n = h g_1 x_1 ... x_n \ldots g_m x_1 ... x_n$,
$(\mathsf{R}gh) x_1 ... x_n \mathbf{0} = g x_1 ... x_n$,
$(\mathsf{R}gh) x_1 ... x_n \mathsf{S}y = h x_1 ... x_n y (\mathsf{R}gh) x_1 ... x_n y$,
$A_x(\mathbf{0}) \to (\forall x(A \to A_x(\mathsf{S}x)) \to \forall x A)$, für jede PR-Formel A.

Wir fixieren eine Funktion $\Phi : \mathbb{N} \to \mathbb{N}$ mit den folgenden Eigenschaften:
(Φ1) $\forall n(2 \leq \Phi(n) \ \ \& \ \ 2\Phi(n) + 2 \leq \Phi(n+1))$,
(Φ2) Zu jeder (n-st.) primitiv rekursiven Funktion f existiert ein $p \in \mathbb{N}$ mit
$f(a_1, ..., a_n) < \Phi(p + \max\{a_1, ..., a_n\})$ für alle $a_1, ..., a_n \in \mathbb{N}$.
(Eine solche Funktion Φ wird später explizit angegeben.)

Unter Formeln bzw. Termen wollen wir bis auf weiteres stets PR-Formeln bzw. PR-Terme verstehen.

Definition von $\mathrm{rk}(A)$
1. $\mathrm{rk}(A) := 0$, falls A Primformel,
2. $\mathrm{rk}(A \to B) := \max\{\mathrm{rk}(A), \mathrm{rk}(B)\} + 1$,
3. $\mathrm{rk}(\forall x A) := \mathrm{rk}(A) + 1$.
Folgerung: $\mathrm{rk}(A_x(t)) = \mathrm{rk}(A)$.

Mit $\alpha, \beta, \gamma, \delta, \xi, \eta$ bezeichnen wir im folgenden stets Ordinalzahlen $< \varepsilon_0 := \min\{\alpha : \omega^\alpha = \alpha\}$.

Definition von $G(\alpha)$
1. $G(0) := 0$,
2. $G(\omega^\alpha) := G(\alpha) + 1$,
3. $G(\alpha) := G(\alpha_0) + ... + G(\alpha_n)$, falls $\alpha =_{NF} \alpha_0 + ... + \alpha_n$.
Folgerung: $G(\alpha \# \beta) = G(\alpha) + G(\beta)$; insbesondere $G(\alpha + n) = G(\alpha) + n$, für $n < \omega$.

Schreibweise: $G\alpha := G(\alpha)$.

Bemerkung: Für jedes $k \in \mathbb{N}$ gilt $card\{\alpha < \varepsilon_0 : G\alpha < k\} < \omega$.

Beweis durch Induktion nach k:

Sei $U_k := \{\alpha : G\alpha \leq k\}$. Dann gilt $U_0 = \{0\}$ und $U_{k+1} \subseteq \{\omega^\alpha : \alpha \in U_k\} \cup \{\alpha + \beta : \alpha, \beta \in U_k\}$.

Definition (A. Weiermann)

$\beta <_n^1 \alpha \iff \beta < \alpha \ \& \ G\beta \leq \Phi(G\alpha + n)$,

$<_n :=$ transitive Hülle von $<_n^1$.

Folgerung: $\beta <_n^1 \alpha \,\&\, n \leq m \ \Rightarrow \ \beta <_m^1 \alpha$.

Lemma 12.1

a) $\beta <_n^1 \alpha \ \Rightarrow \ \gamma\#\beta <_n^1 \gamma\#\alpha \ \& \ \omega^\beta <_n^1 \omega^\alpha$,

b) $\alpha_0, \alpha_1 <_n^1 \alpha \ \Rightarrow \ \omega^{\alpha_0}\#\omega^{\alpha_1} <_n^1 \omega^\alpha$,

c) $\beta <_n^1 \alpha \ \Rightarrow \ \beta + n + 1 <_0^1 \alpha + n + 1$,

d) $14(n+1) <_n^1 \omega$.

Beweis :

a) $G(\gamma\#\beta) = G\gamma + G\beta \leq G\gamma + \Phi(G\alpha + n) \leq \Phi(G\gamma + G\alpha + n) = \Phi(G(\gamma\#\alpha) + n)$.
$G(\omega^\beta) = G\beta + 1 \leq \Phi(G\alpha + n) + 1 \leq \Phi(G\alpha + 1 + n) = \Phi(G\omega^\alpha + n)$.

b) $G(\omega^{\alpha_0}\#\omega^{\alpha_1}) = G\alpha_0 + 1 + G\alpha_1 + 1 \leq \Phi(G\alpha + n) + \Phi(G\alpha + n) + 2 \leq \Phi(G\alpha + n + 1) = \Phi(G\omega^\alpha + n)$.

c) $G(\beta + n + 1) = G\beta + n + 1 \leq \Phi(G\alpha + n) + n + 1 \leq \Phi(G\alpha + n + 1)$.

d) $G(14(n+1)) = 14(n+1) \leq \Phi(n+2) = \Phi(G\omega + n)$. △

Bemerkung: Die Aussagen von Lemma 12.1 gelten auch für $<_n$ statt $<_n^1$.

[zu b) $\alpha_0, \alpha_1 <_n \alpha \ \Rightarrow \ \alpha_i \leq_n \beta_i <_n^1 \alpha \ \Rightarrow \ \omega^{\alpha_0}\#\omega^{\alpha_1} \leq_n \omega^{\beta_0}\#\omega^{\beta_1} <_n^1 \omega^\alpha$.

zu c) Wir haben $\beta = \gamma_0 <_n^1 \gamma_1 <_n^1 \ldots <_n^1 \gamma_k = \alpha$. Mit c) folgt daraus

$\beta + n + 1 = \gamma_0 + n + 1 <_0^1 \gamma_1 + n + 1 <_0^1 \ldots <_0^1 \gamma_k + n + 1 = \alpha + n + 1$, d.h. $\beta + n + 1 <_0 \alpha + n + 1$.]

Definition

$\mathrm{TRUE}_0 :=$ Menge aller wahren geschlossenen Primformeln.

$\mathrm{FALSE}_0 :=$ Menge aller falschen geschlossenen Primformeln.

(Die einzigen Primformeln der Sprache PR sind Gleichungen.)

Mitteilungszeichen:

Γ für endliche Mengen von geschlossenen Formeln.

Ausdrücke der Form $\Gamma \supset C$ heißen *Sequenzen*.

Schreibweise: A, Γ bzw. Γ, Γ' für $\{A\} \cup \Gamma$ bzw. $\Gamma \cup \Gamma'$.

Definition von $\vdash_m^\alpha \Gamma \supset C$ (für geschlossenes C)

$\vdash_m^\alpha \Gamma \supset C$ gelte genau dann, wenn einer der folgenden Fälle vorliegt:

(Ax) $C \in \mathrm{TRUE}_0$ oder $\Gamma \cap \mathrm{FALSE}_0 \neq \emptyset$,

($\to r$) $C = A \to B \ \& \ \vdash_m^{\alpha_0} A, \Gamma \supset B \ \& \ \alpha_0 <_0 \alpha$,

($\forall r$) $C = \forall x A \ \& \ \vdash_m^{\alpha_n} \Gamma \supset A_x(n) \ \& \ \alpha_n <_n \alpha \ (\forall n \in \mathbb{N})$,

($\to l$) $(A \to B) \in \Gamma \ \& \ \vdash_m^{\alpha_0} \Gamma \supset A \ \& \ \vdash_m^{\alpha_1} B, \Gamma \supset C \ \& \ \alpha_0 + 1, \alpha_1 <_0 \alpha$,

($\forall l$) $\forall x A \in \Gamma \ \& \ \vdash_m^{\alpha_0} A_x(k), \Gamma \supset C \ \& \ \alpha_0 <_0 \alpha \ \& \ k + 1 <_0 \alpha$,

(Cut) $\mathrm{rk}(D) < m \ \& \ \vdash_m^{\alpha_0} \Gamma \supset D \ \& \ \vdash_m^{\alpha_1} D, \Gamma \supset C \ \& \ \alpha_0, \alpha_1 <_0 \alpha$.

Lemma 12.2

a) $\vdash_m^\alpha \Gamma \supset C \;\&\; \Gamma \subseteq \Gamma_1 \;\&\; \alpha \leq_0 \alpha_1 \;\&\; m \leq m_1 \;\Rightarrow \vdash_{m_1}^{\alpha_1} \Gamma_1 \supset C$.

b) $\vdash_m^\alpha A, \Gamma \supset C \;\&\; A \in \mathrm{TRUE}_0 \;\Rightarrow \vdash_m^\alpha \Gamma \supset C$.

c) $\vdash_m^\alpha \Gamma \supset A \;\&\; A \in \mathrm{FALSE}_0 \;\Rightarrow \vdash_m^\alpha \Gamma \supset C$.

d) $\vdash_m^\alpha \neg A, \Gamma \supset C \;\&\; A \in \mathrm{FALSE}_0 \;\Rightarrow \vdash_m^\alpha \Gamma \supset C$.

Beweis durch Induktion nach α:

a),b),c) trivial.

d) Ist $\neg A$ nicht Hauptteil des letzten Schlusses, so folgt die Behauptung sofort aus der I.V. . Andernfalls gilt $\vdash_m^{\alpha_0} \neg A, \Gamma \supset A$ mit $\alpha_0 <_0 \alpha$. Nach I.V. haben wir dann $\vdash_m^{\alpha_0} \Gamma \supset A$, und daraus folgt mit c) $\vdash_m^\alpha \Gamma \supset C$. $\triangle$

Lemma 12.3 (Inversion)

a) $\vdash_m^\alpha \Gamma \supset A \to B \;\Rightarrow \vdash_m^\alpha A, \Gamma \supset B$,

b) $\vdash_m^\alpha \Gamma \supset \forall x A \;\Rightarrow \vdash_m^{\alpha+n+1} \Gamma \supset A_x(n)$, für alle $n \in \mathbb{N}$.

Beweis durch Induktion nach α:

b) (Ax) Gilt $\Gamma \cap \mathrm{FALSE}_0 \neq \emptyset$, so ist die Behauptung trivial.

$(\to l)$ Gelte $B \to C \in \Gamma \;\&\; \vdash_m^{\alpha_0} \Gamma \supset B \;\&\; \vdash_m^{\alpha_1} C, \Gamma \supset \forall x A$ mit $\alpha_0 + 1, \alpha_1 <_0 \alpha$.

Nach I.V. haben wir dann $\vdash_m^{\alpha_1+n+1} C, \Gamma \supset A_x(n)$. Mit $(\to l)$ folgt daraus $\vdash_m^{\alpha+n+1} \Gamma \supset A_x(n)$.

(Cut) und $(\forall l)$: analog zu $(\to l)$.

$(\forall r)$ Gelte $\vdash_m^{\alpha_n} \Gamma \supset A_x(n) \;\&\; \alpha_n <_n \alpha$ für alle $n \in \mathbb{N}$. Nach 12.1c ist dann $\alpha_n <_0 \alpha + n + 1$, und folglich $\vdash_m^{\alpha+n+1} \Gamma \supset A_x(n)$. $\triangle$

Lemma 12.4 (Reduktion)

$\mathrm{rk}(D) \leq m \;\&\; \vdash_m^\alpha \Gamma \supset D \;\&\; \vdash_m^\beta D, \Gamma \supset C \;\Rightarrow \vdash_m^{\alpha \# \beta} \Gamma \supset C$.

Beweis durch Induktion nach β:

1. Gelte $\vdash_m^\beta D, \Gamma \supset C$ gemäß (Ax).

1.1. $D \in \mathrm{FALSE}_0$: Dann folgt die Behauptung aus $\vdash_m^\alpha \Gamma \supset D$ mittels Lemma 12.2a,c.

1.2. $D \notin \mathrm{FALSE}_0$: Dann gilt auch die Behauptung gemäß (Ax).

2. Sei $A \to B \in D, \Gamma$ und gelte $\vdash_m^{\beta_0} D, \Gamma \supset A \;\&\; \vdash_m^{\beta_1} B, D, \Gamma \supset C \;\&\; \beta_0 + 1, \beta_1 <_0 \beta$. Mit I.V. erhalten wir (1) $\vdash_m^{\alpha \# \beta_0} \Gamma \supset A$, (2) $\vdash_m^{\alpha \# \beta_1} B, \Gamma \supset C$. Ist $A \to B \in \Gamma$, so folgt daraus die Behauptung mittels $(\to l)$.

Sei jetzt $A \to B = D$. Dann liefert das Inversionslemma: (3) $\vdash_m^\alpha A, \Gamma \supset B$.

Aus (1) und (3) folgt mit einem Schnitt (i.e. einer Anwendung von (Cut)): $\vdash_m^{\alpha \# \beta_0 + 1} \Gamma \supset B$.
Mit (2) und einem weiteren Schnitt folgt dann die Behauptung.

4. Sei $\forall x A \in D, \Gamma$ und gelte $\vdash_m^{\beta_0} A_x(k), D, \Gamma \supset C \;\&\; \beta_0, k + 1 <_0 \beta$.

Mit I.V. erhalten wir (1) $\vdash_m^{\alpha \# \beta_0} A_x(k), \Gamma \supset C$.
Ist $\forall x A \in \Gamma$, so folgt die Behauptung aus (1) mittels $(\forall l)$.

Ist $\forall x A = D$, so liefert das Inversionslemma (2) $\vdash_m^{\alpha \# (k+1)} \Gamma \supset A_x(k)$,
und die Behauptung folgt aus (1) und (2) mittels (Cut).

5. Gilt $\vdash_m^\beta D, \Gamma \supset C$ nach $(\to r)$ oder $(\forall r)$ oder (Cut), so folgt die Behauptung unmittelbar aus der I.V. (vergl. jeweils den ersten Unterfall von 3. bzw. 4.). $\triangle$

Lemma 12.5 (Schnittelimination)

$\vdash_{m+1}^\alpha \Gamma \supset C \;\Rightarrow \vdash_m^{\omega^\alpha} \Gamma \supset C.$

Beweis durch Induktion nach α:

Gelte $\vdash_{m+1}^{\alpha_0} \Gamma \supset D \;\&\; \vdash_{m+1}^{\alpha_1} D, \Gamma \supset C \;\&\; \mathrm{rk}(D) \leq m \;\&\; \alpha_0, \alpha_1 <_0 \alpha.$

Nach I.V. haben wir dann $\vdash_m^{\omega^{\alpha_0}} \Gamma \supset D$ und $\vdash_m^{\omega^{\alpha_1}} D, \Gamma \supset C.$

Mit dem Reduktionslemma folgt $\vdash_m^{\omega^{\alpha_0} \# \omega^{\alpha_1}} \Gamma \supset C$ und daraus $\vdash_m^{\omega^\alpha} \Gamma \supset C$, denn $\omega^{\alpha_0} \# \omega^{\alpha_1} <_0 \omega^\alpha$.

In allen anderen Fällen folgt die Behauptung unmittelbar aus der I.V. $\triangle$

Definition

$\mathrm{K}(0) := 0$ und $\mathrm{K}(\alpha) := \max\{\mathrm{K}(\beta) + 1 : \beta <_0^1 \alpha\}$ für $\alpha > 0$.

Folgerungen:

(1) $\forall m \in \mathbb{N}(\mathrm{K}(m) = m)$

(2) $\beta <_0 \alpha \;\Rightarrow\; \mathrm{K}(\beta) < \mathrm{K}(\alpha).$

(3) $\mathrm{K}(\alpha) = \max\{k : \exists(\alpha_0, ..., \alpha_k)[\alpha_k <_0^1 \ldots <_0^1 \alpha_0 = \alpha]\}.$

Lemma 12.6 (Collapsing)

$\vdash_0^\alpha \forall x \neg A \supset \bot \;\&\; \mathrm{rk}(A) = 0 \;\Rightarrow$ Es existiert ein $k < \mathrm{K}(\alpha)$ mit $A_x(k) \in \mathrm{TRUE}_0$.

Beweis :

Nach Voraussetzung existieren $\alpha_0 <_0 \alpha$ und $k + 1 <_0 \alpha$ mit $\vdash_0^{\alpha_0} \forall x \neg A, \neg A_x(k) \supset \bot$.

Fall 1: $A_x(k) \in \mathrm{TRUE}_0$. Dann $k = \mathrm{K}(k) < \mathrm{K}(\alpha)$ und wir sind fertig.

Fall 2: $A_x(k) \in \mathrm{FALSE}_0$. Dann folgt mit Lemma 12.2d $\vdash_0^{\alpha_0} \forall x \neg A \supset \bot$ und daraus nach I.V. die Behauptung, denn $(\alpha_0 <_0 \alpha \;\Rightarrow\; \mathrm{K}(\alpha_0) < \mathrm{K}(\alpha))$. $\triangle$

Korollar

Gilt $\vdash_0^\alpha \supset \forall x \exists y A(x, y)$, wobei A Primformel,

so gibt es zu jedem $n \in \mathbb{N}$ ein $k < \mathrm{K}(\alpha + n + 1)$ mit $A(n, k) \in \mathrm{TRUE}_0$.

Beweis :

Vorauss.& Inversion $\Rightarrow \vdash_0^{\alpha+n+1} \supset \neg\forall y \neg A(n, y) \;\Rightarrow \vdash_0^{\alpha+n+1} \forall y \neg A(n, y) \supset \bot \overset{12.6}{\Rightarrow}$ Beh. $\triangle$

EINBETTUNG

Definition

$A \sim A' \;:\Leftrightarrow$ Es gibt eine Formel D, paarweise verschiedene Variablen $x_1, ..., x_n$ und geschlossene Terme $t_1, t_1', \ldots, t_n, t_n'$ mit $val(t_i) = val(t_i')$ $(i = 1, ..., n)$ und $A = D_{x_1,...,x_n}(t_1, ..., t_n),\; A' = D_{x_1,...,x_n}(t_1', ..., t_n').$

Lemma 12.7 (Tautologie-Lemma)

Für geschlossene Formeln A, B, C, C' bzw. $\forall x A$, $\forall x B$ gilt:

a) $C \sim C' \;\Rightarrow \vdash_0^{\omega \cdot \mathrm{rk}(C)} C \supset C'.$

b) $\vdash_0^{\omega \cdot (k+1)} (C \to (A \to B)), C \to A, C \supset B, \quad$ wobei $k := \max\{\mathrm{rk}(A), \mathrm{rk}(B), \mathrm{rk}(C)\}.$

c) $\vdash_0^\omega \neg\neg A \supset A$, falls A Primformel.

d) $\vdash_0^{\omega \cdot (k+1)} \forall x(A \to B), \forall x A \supset \forall x B, \quad$ wobei $k := \max\{\mathrm{rk}(A), \mathrm{rk}(B)\}.$

Beweis :

a) 1. Ist C eine Primformel, so gilt entweder $C, C' \in \mathrm{TRUE}_0$ oder $C, C' \in \mathrm{FALSE}_0$. Folglich $\vdash_0^0 C \supset C'$.

2. Sei $C = \forall x A$ und $k := \mathrm{rk}(A)$. Dann $C' = \forall x A'$ mit $A \sim A'$, und nach I.V. gilt $\vdash_0^{\omega \cdot k} A_x(n) \supset A'_x(n)$ für alle $n \in \mathbb{N}$. Mit $(\forall l)$ folgt $\vdash_0^{\omega \cdot k + n + 2} \forall x A \supset A'_x(n)$ für alle $n \in \mathbb{N}$. Wegen $\omega \cdot k + n + 2 <_n \omega \cdot (k+1)$ folgt daraus $\vdash_0^{\omega \cdot (k+1)} \forall x A \supset \forall x A'$.

3. Sei $C = A \to B$, $C' = A' \to B'$ und $k := \max\{\mathrm{rk}(A), \mathrm{rk}(B)\}$.

Nach I.V. gilt $\vdash_0^{\omega \cdot k} A' \supset A \ \ \& \ \ \vdash_0^{\omega \cdot k} B \supset B'$.

Mit $(\to l)$ bzw. $(\to r)$ folgt daraus erst $\vdash_0^{\omega \cdot k + 2} A', A \to B \supset B'$, und dann $\vdash_0^{\omega \cdot (k+1)} C \supset C'$.

b)

$\vdash_0^{\omega \cdot k} A \supset A \ \mid \ \vdash_0^{\omega \cdot k} B \supset B$

$\vdash_0^{\omega \cdot k + 2} A \to B, A \supset B \ \mid \ \vdash_0^{\omega \cdot k} C \supset C$

$\vdash_0^{\omega \cdot k + 4} A, C \to (A \to B), C \supset B \ \mid \ \vdash_0^{\omega \cdot k} C \supset C$

$\vdash_0^{\omega \cdot (k+1)} C \to A, C \to (A \to B), C \supset B$

c) Für $A \in \mathrm{TRUE}_0$ ist die Behauptung trivial.

Für $A \in \mathrm{FALSE}_0$ haben wir:

$\vdash_0^0 A \supset \bot$

$\vdash_0^1 \supset \neg A \ \mid \ \vdash_0^0 \bot \supset A$

$\vdash_0^\omega \neg A \to \bot \supset A$

d) $\vdash_0^{\omega \cdot k} A(n) \supset A(n) \ \mid \ \vdash_0^{\omega \cdot k} B(n) \supset B(n)$

$\vdash_0^{\omega \cdot k + 2} A(n) \to B(n), A(n) \supset B(n)$

$\vdash_0^{\omega \cdot k + n + 3} \forall x (A \to B), A(n) \supset B(n)$

$\vdash_0^{\omega \cdot k + n + 4} \forall x (A \to B), \forall x A \supset B(n), \ \text{für alle } n$

$\vdash_0^{\omega \cdot (k+1)} \forall x (A \to B), \forall x A \supset \forall x B.$ $\triangle$

Lemma 12.8 (Induktionslemma)

Sei $\mathrm{FV}(A) \subseteq \{x\}$ und $k := \mathrm{rk}(A)$. Dann gilt $\vdash_0^{\omega \cdot (k+1)} A(0), \forall x (A(x) \to A(\mathsf{S}x)) \supset \forall x A(x)$.

Beweis :

Durch Induktion nach n zeigen wir: $\vdash_0^{\omega \cdot k + 3n} A(0), \forall x (A(x) \to A(\mathsf{S}x)) \supset A(n)$.

1. Für $n = 0$ folgt die Behauptung aus dem Tautologie-Lemma.

2. $\vdash_0^{\omega \cdot k + 3n} A(0), \forall x (A(x) \to A(\mathsf{S}x)) \supset A(n) \ \mid \ \vdash_0^{\omega \cdot k} A(\mathsf{S}n) \supset A(\mathsf{S}n)$,

$\vdash_0^{\omega \cdot k + 3n + 2} A(0), \forall x (A(x) \to A(\mathsf{S}x)), (A(n) \to A(\mathsf{S}n)) \supset A(\mathsf{S}n)$,

$\vdash_0^{\omega \cdot k + 3n + 3} A(0), \forall x (A \to A(\mathsf{S}x)) \supset A(\mathsf{S}n)$. $\triangle$

Abkürzung:

A^0 bezeichne die Formel, die man erhält, wenn in A jede freie Variable durch die Konstante 0 ersetzt wird.

Satz 12.9 (Einbettungssatz)

$\mathrm{Z} \vdash C \ \Rightarrow$ Es gibt $k, m \in \mathbb{N}$ mit $\vdash_m^{\omega \cdot k} \supset C^0$.

Beweis durch Induktion nach der Herleitung von C:

1. C wurde aus A und $A \to C$ erschlossen. Nach I.V. gibt es dann k, m mit $\vdash_m^{\omega \cdot k} \supset A^0$ und $\vdash_m^{\omega \cdot k} \supset A^0 \to C^0$. Aus letzterem folgt $\vdash_m^{\omega \cdot k} A^0 \supset C^0$. Wir können auch noch $\mathrm{rk}(A) < m$ annehmen. Dann folgt mit einem Schnitt $\vdash_m^{\omega \cdot (k+1)} \supset C^0$.

2. $C^0 = \forall y_1 ... \forall y_p (\forall x A \to A_x(t))$. Sei $k_0 := \mathrm{rk}(A)$ und $\mathrm{FV}(A_x(t)) = \{x_1, ..., x_l\}$.

Abkürzung:

Für $\vec{n} = (n_1, ..., n_l)$, $\alpha \in On$, E Ausdruck sei $\alpha + \vec{n} = \alpha + \max\{n_1, ..., n_l\}$ und $E(\vec{n}) := E_{x_1,...,x_l}(n_1, ..., n_l)$.

Es ex. $k > k_0$ mit $val(t(\vec{n})) + 1 < \Phi(k + \vec{n})$ $(\forall \vec{n} \in \mathbb{N}^l)$. Folglich $val(t(\vec{n})) + 1 <_0 \omega \cdot k + \vec{n}$ $(\forall \vec{n} \in \mathbb{N}^l)$.

Wir beweisen: $\vdash_0^{\omega \cdot (k+1) + \vec{n}} \supset (\forall x A \to A_x(t))(\vec{n})$, für alle $\vec{n} \in \mathbb{N}^l$.

Daraus folgt dann mit dem unten stehenden Hilfssatz: $\vdash_0^{\omega \cdot (k+p+1)} \supset C^0$.

Sei also $\vec{n} \in \mathbb{N}^l$ gegeben, und sei $(\forall x A)(\vec{n}) = \forall x B$. Dann $B_x(t(\vec{n})) = A_x(t)(\vec{n})$. Nach Lemma 12.7a gilt also $\vdash_0^{\omega \cdot k_0} B_x(j) \supset A_x(t)(\vec{n})$, wobei $j := val(t(\vec{n}))$. Mit $j + 1 <_0 \omega \cdot k + \vec{n}$ folgt nun $\vdash_0^{\omega \cdot k + \vec{n}} \forall x B \supset A_x(t)(\vec{n})$, und weiter $\vdash_0^{\omega \cdot (k+1) + \vec{n}} \supset (\forall x A \to A_x(t))(\vec{n})$.

3. Andernfalls ist $C^0 = \forall y_1 ... \forall y_p A$, und es gibt ein k, so daß $\vdash_0^{\omega \cdot k} \supset A'$ für jede geschlossene Instanz A' von A (siehe u.a. Lemmata 12.7, 12.8). Daraus folgt $\vdash_0^{\omega \cdot (k+p)} \supset \forall y_1 ... y_p A$.

Abkürzung: $\vdash^{\alpha,*} \supset A \ :\Leftrightarrow\ \forall \vec{n} [\vdash_0^{\alpha + \vec{n}} \supset A_{\vec{x}}(\vec{n})]$, wobei $\mathrm{FV}(A) = \{\vec{x}\}$.

Hilfssatz: $\alpha \in Lim \ \&\ \vdash^{\alpha,*} \supset A \ \Rightarrow \vdash^{\alpha + \omega,*} \supset \forall y A$.

Beweis: Sei $\mathrm{FV}(\forall y A) = \{\vec{x}\}$, und $\vec{n}$ gegeben.

$\vdash^{\alpha,*} \supset A \ \Rightarrow \vdash_0^{\alpha + \max\{k, \vec{n}\}} \supset A_{\vec{x}}(\vec{n})_y(k)$, für alle $\vec{n}, k \ \Rightarrow \vdash_0^{\alpha + \omega + \vec{n}} \supset (\forall y A)_{\vec{x}}(\vec{n})$, denn

$\alpha + \max\{k, \vec{n}\} <_k \alpha + \omega + \vec{n}$ und $(\forall y A)_{\vec{x}}(\vec{n}) = \forall y\, A_{\vec{x}}(\vec{n})$. $\triangle$

ZWISCHENRESULTAT

Sei A eine Primformel mit $\mathrm{FV}(A) \subseteq \{x, y\}$. Dann gilt:

$\mathrm{Z} \vdash \forall x \exists y A \implies \exists \alpha < \varepsilon_0 \forall n \exists k < \mathrm{K}(\alpha + n + 1)[\, A(n, k)$ wahr $]$.

Beweis: 12.9, 12.5, 12.6.

DIE HARDY-HIERARCHIE

Definition (Fundamentalfolgen)

1. $0[n] := 1[n] := 0$.
2. $\omega^{\alpha+1}[n] := \omega^\alpha \cdot (n + 1)$.
3. $\omega^\lambda[n] := \omega^{\lambda[n]}$, für $\lambda \in Lim$.
4. $\alpha[n] := \alpha_0 + ... + \alpha_{k-1} + \alpha_k[n]$, falls $\alpha =_{NF} \alpha_0 + ... + \alpha_k$.

Folgerung: $(\alpha + 1)[n] = \alpha$.

Lemma 12.10

a) $\alpha \in Lim \ \Rightarrow\ \forall n(\alpha[n] < \alpha[n + 1]) \ \&\ \alpha = \sup\{\alpha[n] : n \in \mathbb{N}\}$

b) $\alpha > 0 \ \Rightarrow\ G\alpha[0] < G\alpha$

c) $\alpha[n] < \beta < \alpha \ \Rightarrow\ \alpha[n] \leq \beta[0]$

d) $\alpha[n] < \beta < \alpha \ \Rightarrow\ G\alpha[n] < G\beta$

e) $\beta < \alpha \ \Rightarrow\ \beta \leq \alpha[G\beta]$

Beweis :
a),b) klar.
c) Sei $\beta =_{NF} \beta_0 + ... + \beta_k$.
1. Gelte $\omega^\alpha \cdot (n+1) < \beta < \omega^{\alpha+1}$. Dann $k > n$ und $\beta_0 = ... = \beta_n = \omega^\alpha$.
Es folgt $\omega^\alpha \cdot (n+1) \leq \beta_0 + ... + \beta_{k-1} + \beta_k[0] = \beta[0]$.
2. Gelte $\omega^{\lambda[n]} < \beta < \omega^\lambda$ und $\lambda \in Lim$. Dann $\omega^{\lambda[n]} \leq \beta_0 = \omega^\gamma < \omega^\lambda$.
Ist $k = 0$, so $\lambda[n] < \gamma < \lambda$ und deshalb (nach I.V.) $\lambda[n] \leq \gamma[0]$. Es folgt $\omega^{\lambda[n]} \leq \omega^{\gamma[0]} = \omega^\gamma[0] = \beta[0]$.
Ist $k > 0$, so $\omega^{\lambda[n]} \leq \beta_0 + ... + \beta_{k-1} + \beta_k[0] = \beta[0]$.
3. Gelte $\alpha =_{NF} \alpha_0 + ... + \alpha_m$, $m > 0$ und $a[n] = \alpha_0 + ... + \alpha_{m-1} + \alpha_m[n] < \beta < \alpha$. Dann
$m \leq k$, $\alpha_m[n] < \beta_m < \alpha_m$ und $\alpha_i = \beta_i$ für $i < m$. Mit I.V. folgt $\alpha_m[n] \leq \beta_m[0]$ und weiter
$\alpha[n] \leq \beta_0 + ... + \beta_{m-1} + \beta_m[0] \leq \beta_0 + ... + \beta_{k-1} + \beta_k[0] = \beta[0]$.
d) Nach c) ist $\alpha[n] = \beta[0]...[0]$. Mit b) folgt daraus die Behauptung.
e) Sei $\alpha \in Lim$. Wegen a),d) gilt dann $\forall n(n \leq G\alpha[n])$, insbesondere $G\beta \leq G\alpha[G\beta]$. Mit d) folgt daraus die Behauptung. △

Definition (Die Hardy-Hierarchie)
$H_0(n) := n$, $H_\alpha(n) := H_{\alpha[n]}(n+1)$, falls $\alpha > 0$.

Lemma 12.11
a) $H_\alpha(n) < H_\alpha(n+1)$,
b) $\beta < \alpha \ \& \ G\beta \leq n \ \Rightarrow \ H_\beta(n+1) \leq H_\alpha(n)$,
c) $\alpha > 0 \ \Rightarrow \ H_\alpha(n) = n + \min\{l : \alpha[n][n+1]\dots[n+l-1] = 0\}$,
d) $\alpha[m] < \beta < \alpha \ \Rightarrow \ H_{\alpha[m]}(n) < H_\beta(n)$.
Beweis :
a) Induktion nach α:
Fall 1: $\alpha = \beta + 1$. Dann $H_\alpha(n) = H_\beta(n+1) \overset{\text{I.V.}}{<} H_\beta(n+2) = H_\alpha(n+1)$.
Fall 2: $\alpha \in Lim$. Nach 12.10a,c existiert dann ein $k \geq 2$ mit $\alpha[n] = \alpha[n+1][n+2]\dots[n+k]$.
Es folgt: $H_\alpha(n+1) = H_{\alpha[n+1]\dots[n+k]}(n+k+1) = H_{\alpha[n]}(n+k+1) \overset{\text{I.V.}}{>} H_{\alpha[n]}(n+1) = H_\alpha(n)$.
b) Induktion nach α:
Ist $\alpha = \beta + 1$, so $H_\beta(n+1) = H_\alpha(n)$. Ist $\alpha = \alpha_0 + 1$ mit $\beta < \alpha_0$, so
$H_\beta(n+1) \overset{\text{I.V.}}{\leq} H_{\alpha_0}(n) \overset{\text{a)}}{<} H_{\alpha_0}(n+1) = H_\alpha(n)$.
Sei jetzt $\alpha \in Lim$. Dann $G\beta \leq n \leq G\alpha[n]$ und somit $\beta \leq \alpha[n]$ nach 12.10d. Ist $\beta = \alpha[n]$, so
$H_\beta(n+1) = H_\alpha(n)$. Ist $\beta < \alpha[n]$, so gilt [nach I.V. und a)] $H_\beta(n+1) < H_\beta(n+2) \leq H_{\alpha[n]}(n+1) = H_\alpha(n)$.
c) Sei $\alpha > 0$. Dann existiert ein $l > 0$ mit $\alpha > \alpha[n] > \alpha[n][n+1] > \dots > \alpha[n][n+1]...[n+l-1] = 0$ und
$H_\alpha(n) = H_{\alpha[n]}(n+1) = H_{\alpha[n][n+1]}(n+2) = H_{\alpha[n][n+1]\dots[n+l-1]}(n+l) = n+l$.
d) Nach 12.10a,c existiert ein kleinstes k mit $\alpha[m] = \beta[n]\dots[n+k]$. Für dieses k gilt nun
$H_{\alpha[m]}(n) < H_{\alpha[m]}(n+k+1) = H_{\beta[n]\dots[n+k]}(n+k+1) = H_\beta(n)$. △

Abkürzung
$NF(\alpha,\beta) \ :\Leftrightarrow \ \alpha = 0 \vee \beta = 0 \vee [\,\alpha =_{NF} \alpha_0 + ... + \alpha_n \wedge \beta =_{NF} \beta_0 + ... + \beta_m \text{ mit } \alpha_n \geq \beta_0\,]$.
Folgerung: $NF(\alpha,\beta) \ \& \ \beta > 0 \ \Rightarrow \ (\alpha+\beta)[n] = \alpha + \beta[n] \ \& \ NF(\alpha,\beta[n])$

Lemma 12.12
a) $NF(\alpha,\beta) \ \Rightarrow \ H_{\alpha+\beta} = H_\alpha \circ H_\beta$.
b) $H_\alpha(n) < H_{\omega^\alpha}(n)$.

Beweis : a) Sei $\beta > 0$. Dann $H_{\alpha+\beta}(n) = H_{\alpha+\beta[n]}(n+1) = H_\alpha(H_{\beta[n]}(n+1)) = H_\alpha(H_\beta(n))$.
b) Induktion nach α unter Verwendung von a) im Nachfolgerfall. $\triangle$

Definition (Die schnell wachsende Hierarchie)
$F_\alpha := H_{\omega^\alpha}$

Lemma 12.13
(F1) $F_0(n) = n+1$
(F2) $F_{\alpha+1}(n) = F_\alpha^{(n+1)}(n+1)$
(F3) $F_\lambda(n) = F_{\lambda[n]}(n+1)$
(F4) $n < F_\alpha(n) < F_{\alpha+1}(n)$
(F5) $F_\alpha^{(2)}(n+1) < F_{\alpha+1}(n+1)$ & $F_\alpha^{(2)}(n) < F_{\alpha+2}(n)$
(F6) $\beta < \alpha$ & $G\beta < n \Rightarrow F_\beta(n) < F_\alpha(n)$.
(F7) $F_\omega(0) = 4$ & $2 \cdot F_\omega(n) + 2 \le F_\omega(n+1)$.
Beweis :
1. $H_{\omega^0}(n) = H_0(n+1) = n+1$.
2. $H_{\omega^{\alpha+1}}(n) = H_{\omega^\alpha \cdot (n+1)}(n+1) = H_{\omega^\alpha}^{(n+1)}(n+1)$.
3. $H_{\omega^\lambda}(n) = H_{\omega^{\lambda[n]}}(n+1) = H_{\omega^{\lambda[n]}}(n+1)$.
4. $n < F_\alpha(n)$ folgt durch Induktion nach α. $F_\alpha(n) < F_\alpha(n+1) \le F_\alpha^{(n+1)}(n+1) = F_{\alpha+1}(n)$.
5. $F_{\alpha+1}(n+1) = F_\alpha^{(n+2)}(n+2) \ge F_\alpha^{(2)}(n+2)\ .\ F_\alpha^{(2)}(0) < F_\alpha^{(2)}(2) = F_{\alpha+1}(1) = F_{\alpha+2}(0)$.
6. $\beta < \alpha$ & $G\beta < n \Rightarrow \omega^\beta < \omega^\alpha$ & $G\omega^\beta \le n \Rightarrow H_{\omega^\beta}(n) < H_{\omega^\alpha}(n)$. (Siehe 12.11.)
7. $F_\omega(0) = F_1(1) = F_0^{(2)}(2) = 4$. — $F_1(n) = F_0^{(n+1)}(n+1) = n+1+n+1$.
$F_\omega(n) \cdot 2 + 2 = F_1(F_\omega(n)) = F_1(F_{n+1}(n+1)) \le F_{n+1}^{(2)}(n+1) < F_{n+2}(n+2) = F_\omega(n+1)$. $\triangle$

Abkürzungen:
1. Für $\vec{a} = (a_1, ..., a_n)$ sei $|\vec{a}| := \max\{a_1, ..., a_n\}$.
2. Für $h : \mathbb{N}^n \to \mathbb{N}$ und $f : \mathbb{N} \to \mathbb{N}$ sei: $h \le f \ :\Leftrightarrow \forall \vec{a} \in \mathbb{N}^n [\, h(\vec{a}) \le f(|\vec{a}|)\,]$.

Lemma 12.14
a) $h, g_1, ..., g_m \le F_\gamma \Rightarrow (\circ h g_1 ... g_m) \le F_\gamma \circ F_\gamma \le F_{\gamma+2}$.
b) $h, g \le F_\gamma \Rightarrow (\mathsf{R}gh) \le F_{\gamma+1}$
c) Zu jeder primitiv rekursiven Funktion f existiert ein $k < \omega$ mit $f \le F_k$.
d) $k < \omega \Rightarrow F_k \le F_{\alpha+k}$.
Beweis :
a) $h(g_1(\vec{a}), ..., g_m(\vec{a})) \le F_\gamma(\max\{g_1(\vec{a}), ..., g_m(\vec{a})\}) \le F_\gamma(F_\gamma(|\vec{a}|)) \overset{(F5)}{\le} F_{\gamma+2}(|\vec{a}|)$.
b) Sei $f := (\mathsf{R}gh)$. Durch Induktion nach b beweisen wir: $(*)$ $f(\vec{a}, b) \le F_\gamma^{(b+1)}(|\vec{a}|)$.
$f(\vec{a}, 0) = g(\vec{a}) \le F_\gamma(|\vec{a}|)$. $f(\vec{a}, b+1) = h(\vec{a}, b, f(\vec{a}, b)) \le F_\gamma(|\vec{a}, b, f(\vec{a}, b)|) \le F_\gamma(F_\gamma^{(b+1)}(|\vec{a}|)) = F_\gamma^{(b+2)}(|\vec{a}|)$.
Mit $(*)$ folgt nun $f(\vec{a}, b) \le F_\gamma^{(|\vec{a}, b|+1)}(|\vec{a}, b| + 1) = F_{\gamma+1}(|\vec{a}, b|)$.
c) folgt aus a) und b).
d) Induktion nach k: 1. $F_0(n) = n+1 \le F_\alpha(n)$.
2. $F_\beta \le F_\gamma \Rightarrow F_{\beta+1}(n) = F_\beta^{(n+1)}(n+1) \le F_\gamma^{(n+1)}(n+1) = F_{\gamma+1}(n)$. $\triangle$

Lemma 12.15
Seien α, γ, $(\delta_{n,k})_{n,k \in \mathbb{N}}$ gegeben, so daß gilt:
(V1) $\gamma + \omega + \alpha = \alpha$,
(V2) $\forall n [\, \delta_{n,0} \le \alpha$ & $G\delta_{n,0} \le F_\gamma(n)\,]$,

(V3) $\forall n,k[\,\delta_{n,k}\neq 0 \;\Rightarrow\; \delta_{n,k+1}<\delta_{n,k}\,]$,
(V4) $\forall n,k[\,G\delta_{n,k+1}\leq F_\gamma(G\delta_{n,k})\,]$.
Dann existiert ein $p<\omega$ mit $\forall n\geq p[\,\min\{k:\;\delta_{n,k}=0\}<F^{(2)}_\alpha(n)\,]$.
Beweis :
Aus (V2) und (V4) folgt
(1) $G\delta_{n,k}\leq F^{(k+1)}_\gamma(n)\quad(\forall n,k)$.
Nach Lemma 12.14 existiert ein $m<\omega$, so daß
(2) $G\gamma+l+F^{(k+3)}_\gamma(n)+2\leq F_{\gamma+m}(\max\{l,n,k\})\quad(\forall l,n,k)$.
Abk.: $\beta:=\gamma+m,\quad \alpha(n,0):=\beta+\alpha,\ \alpha(n,k+1):=\beta+\delta_{n,k+1},\quad g(n,k):=G\beta+F^{(k+2)}_\gamma(n)+2$.
Dann gilt
(3) $g(n,k+1)\overset{(2)}{\leq} F_\beta(\max\{m,k,n\})<F_\beta(g(n,k))$,
(4) $G\alpha(n,k+1)+1\overset{(1)}{<} g(n,k)$,
(5) $\delta_{n,k}\neq 0\;\Rightarrow\; F_{\alpha(n,k+1)}(g(n,k+1))<F_{\alpha(n,k)}(g(n,k))$.
Beweis von (5): $\delta_{n,k}\neq 0\;\Rightarrow\;\delta_{n,k+1}<\delta_{n,k}\;\Rightarrow\;\alpha(n,k+1)<\alpha(n,k)\;\Rightarrow\;F_{\alpha(n,k+1)}(g(n,k+1))\overset{(3)}{<}$
$F_{\alpha(n,k+1)}F_\beta(g(n,k))\overset{(F6)}{\leq}F^{(2)}_{\alpha(n,k+1)}(g(n,k))\overset{(F5)}{<}F_{\alpha(n,k+1)+1}(g(n,k))\overset{(F6),(4)}{\leq}F_{\alpha(n,k)}(g(n,k))$.
Aus (5) folgt: $\min\{k:\;\delta_{n,k}=0\}\leq F_{\alpha(n,0)}(g(n,0))$. $\qquad[\,n_k<\ldots<n_0\;\Rightarrow\;n_k+k\leq n_0\,]$.
Für $n>G\beta$ gilt ferner: $F_{\alpha(n,0)}(g(n,0))\overset{(V1)}{=}F_\alpha(g(n,0))\overset{(3)}{\leq}F_\alpha(F_\beta(n))\overset{(F6)}{<}F_\alpha(F_\alpha(n))$. △

Von jetzt an sei $\Phi:=F_\omega$.

Lemma 12.16
$\alpha_0,\omega^2<\alpha\;\Rightarrow\;\exists p\forall n\geq p[\,\mathrm{K}(\alpha_0+n+1)<F_\alpha(n)\,]$.
Beweis :
Offenbar existiert eine Familie $(\delta_{n,k})_{n,k\in\mathbb{N}}$ mit $\forall n[\,\delta_{n,0}=\alpha_0+n+1\,]$ und $\forall n,k[\,\delta_{n,k}\neq 0\;\Rightarrow\;\delta_{n,k+1}<^1_0\delta_{n,k}\,]$ und $\forall n[\,\mathrm{K}(\alpha_0+n+1)=\min\{k:\;\delta_{n,k}=0\}\,]$.
Ferner existiert ein $\gamma=\omega+l$ mit $\forall n[\,G\delta_{n,0}\leq F_\gamma(n)\,]$. Wegen $\Phi=F_\omega$ gilt dann
auch $\forall n,k[\,G\delta_{n,k+1}\leq F_\gamma(G\delta_{n,k})\,]$. Nach Lemma 12.15 existiert also ein p mit
$\forall n\geq p[\,\min\{k:\;\delta_{n,k}=0\}<F^{(2)}_\beta(n)\,]$, wobei $\beta:=\max\{\alpha_0,\omega^2\}$. Aus (F5) und (F6) folgt $F^{(2)}_\beta(n)<F_\alpha(n)$
für alle hinreichend großen n. △

Definition $\quad\omega_0:=1,\ \ \omega_{n+1}:=\omega^{\omega_n}$.

Satz 12.17
Ist A eine Primformel mit $\mathrm{FV}(A)\subseteq\{x,y\}$, so gilt:
$\mathrm{Z}\vdash\forall x\exists y A\;\Rightarrow\;\exists p\forall n\geq p\exists k<H_{\omega_p}(n)[\,A(n,k)$ wahr $\,]$.
Beweis :
Wie weiter oben gezeigt, gibt es ein $\alpha_0<\varepsilon_0$ mit $\forall n\exists k<\mathrm{K}(\alpha_0+n+1)[\,A(n,k)$ wahr $\,]$. Weiter existiert ein m mit $\alpha_0,\omega^2<\omega_m$. Nach Lemma 12.16 existiert ein $p>m$, so daß $\forall n\geq p[\,\mathrm{K}(\alpha_0+n+1)<F_{\omega_m}(n)\,]$.
Mit 12.12 b) folgt $F_{\omega_m}\leq H_{\omega_p}$. △

Bemerkung:
Sei f primitiv rekursiv, so daß $f(m,n,k)=0\;\Leftrightarrow\;k>n\,\&\,\omega_m[n]\ldots[k-1]=0$.
Die Formel $\forall z\forall x\exists y(fzxy=0)$ ist wahr aber nicht beweisbar in Z.
[Beweis der Unbeweisbarkeit: $\vdash\forall z\forall x\exists y(fzxy=0)\;\Rightarrow\vdash\forall x\exists y(fxxy=0)\;\Rightarrow$
$\exists p\forall n\geq p\exists k<H_{\omega_p}(n)\,f(n,n,k)=0$. Nach 12.11c gilt aber $H_{\omega_p}(n)=\min\{k:\;f(p,n,k)=0\}$.]

Durch Formalisierung der transfiniten Induktion bis ω_m kann man zeigen:
$Z \vdash \forall x \exists y (f\underline{m}xy = 0)$, für jedes $m \in \mathbb{N}$.

13 Ein Unabhängigkeitsresultat (Goodstein-Folgen)

Definition
$\mathcal{S}(m,b)$ werde durch folgenden Algorithmus berechnet: Man entwickle m "vollständig" zur Basis b und ersetze in der so gewonnenen Darstellung b durch $b+1$; der Zahlenwert des neuen Ausdrucks sei $\mathcal{S}(m,b)$.
$\mathrm{GS}(a,0) := \mathrm{GS}(a,1) := a$, $\mathrm{GS}(a,n+1) := \mathcal{S}(\mathrm{GS}(a,n),n+1) \dot{-} 1$ für $n \geq 1$.
Die Folge $(\mathrm{GS}(a,n))_{n\in\mathbb{N}}$ (wobei $a \in \mathbb{N}$) heißt *Goodstein-Folge* von a. Wir werden zeigen, daß jede Goodstein-Folge terminiert (d.h. $\forall a \exists n. \mathrm{GS}(a,n) = 0$), und, daß diese Tatsache nicht in Z beweisbar ist.

Definition
$\mathrm{G}_n(0) := 0$, $\mathrm{G}_n(\alpha+1) := \mathrm{G}_n(\alpha) + 1$, $\mathrm{G}_n(\lambda) := \mathrm{G}_n(\lambda[n])$.
$\mathrm{P}_n(0) := 0$, $\mathrm{P}_n(\alpha+1) := \alpha$, $\mathrm{P}_n(\lambda) := \mathrm{P}_n(\lambda[n])$.

Lemma 13.1
a) $\mathrm{G}_n(\alpha+\beta) = \mathrm{G}_n(\alpha) + \mathrm{G}_n(\beta)$, falls $NF(\alpha,\beta)$.
b) $\mathrm{G}_n(\omega^\alpha) = (n+1)^{\mathrm{G}_n(\alpha)}$.
c) $\mathrm{G}_n(\mathrm{P}_n(\alpha)) = \mathrm{G}_n(\alpha) \dot{-} 1$.
Beweis :
a) $\mathrm{G}_n(\alpha+0) = \mathrm{G}_n(\alpha) + 0 = \mathrm{G}_n(\alpha) + \mathrm{G}_n(0)$; $\mathrm{G}_n(\alpha+\beta+1) = \mathrm{G}_n(\alpha+\beta) + 1 = \mathrm{G}_n(\alpha) + \mathrm{G}_n(\beta) + 1 = \mathrm{G}_n(\alpha) + \mathrm{G}_n(\beta+1)$; $\mathrm{G}_n(\alpha+\lambda) = \mathrm{G}_n(\alpha+\lambda[n]) = \mathrm{G}_n(\alpha) + \mathrm{G}_n(\lambda[n]) = \mathrm{G}_n(\alpha) + \mathrm{G}_n(\lambda)$.
b) $\mathrm{G}_n(\omega^0) = 1 = (n+1)^{\mathrm{G}_n(0)}$; $\mathrm{G}_n(\omega^\lambda) = \mathrm{G}_n(\omega^{\lambda[n]}) = (n+1)^{\mathrm{G}_n(\lambda[n])} = (n+1)^{\mathrm{G}_n(\lambda)}$;
$\mathrm{G}_n(\omega^{\alpha+1}) = \mathrm{G}_n(\omega^\alpha \cdot (n+1)) = \mathrm{G}_n(\omega^\alpha) \cdot (n+1) = (n+1)^{\mathrm{G}_n(\alpha)} \cdot (n+1) = (n+1)^{\mathrm{G}_n(\alpha)+1} = (n+1)^{\mathrm{G}_n(\alpha+1)}$.
c) $\mathrm{G}_n(\mathrm{P}_n(0)) = \mathrm{G}_n(0) = 0 = \mathrm{G}_n(0) \dot{-} 1$; $\mathrm{G}_n(\mathrm{P}_n(\alpha+1)) = \mathrm{G}_n(\alpha) = \mathrm{G}_n(\alpha+1) \dot{-} 1$;
$\mathrm{G}_n(\mathrm{P}_n(\lambda)) = \mathrm{G}_n(\mathrm{P}_n(\lambda[n])) = \mathrm{G}_n(\lambda[n]) \dot{-} 1 = \mathrm{G}_n(\lambda) \dot{-} 1$. △

Induktive Definition von Mengen $\mathrm{M}_n \subseteq \varepsilon_0$
1. $0 \in \mathrm{M}_n$.
2. $\alpha_0, ..., \alpha_k \in \mathrm{M}_n \ \&\ n_0, ..., n_k \in \{1, ..., n\} \ \&\ \alpha_k < ... < \alpha_0 \ \Rightarrow\ \omega^{\alpha_0} \cdot n_0 + ... + \omega^{\alpha_k} \cdot n_k \in \mathrm{M}_n$.

Lemma 13.2
a) $\alpha, \beta \in \mathrm{M}_n \ \&\ \alpha < \beta \ \Rightarrow\ \mathrm{G}_n(\alpha) < \mathrm{G}_n(\beta)$.
b) $\alpha \in \mathrm{M}_n \ \Rightarrow\ \mathcal{S}(\mathrm{G}_n(\alpha), n+1) = \mathrm{G}_{n+1}(\alpha) \ \&\ \mathcal{S}(\mathrm{G}_n(\alpha), n+1) \dot{-} 1 = \mathrm{G}_{n+1}(\mathrm{P}_{n+1}(\alpha))$.
c) $n \geq 1 \ \Rightarrow\ \forall a \in \mathbb{N} \exists! \alpha \in \mathrm{M}_n (a = \mathrm{G}_n(\alpha))$.
Beweis :
a) Induktion nach β:
Sei $\alpha = \omega^{\alpha_0} \cdot n_0 + ... + \omega^{\alpha_k} \cdot n_k$ mit $\alpha_k < ... < \alpha_0$, und $\beta = \omega^{\beta_0} \cdot m_0 + ... + \omega^{\beta_l} \cdot m_l$ mit $\beta_l < ... < \beta_0$.
Wegen $\alpha < \beta$ gilt dann $\alpha_0 \leq \beta_0$.
1. $\alpha_0 < \beta_0$: Nach I.V. haben wir dann $\mathrm{G}_n(\alpha_k) < ... < \mathrm{G}_n(\alpha_0) < \mathrm{G}_n(\beta_0)$.
Daraus folgt $\mathrm{G}_n\alpha = \sum_{i\leq k} (n+1)^{\mathrm{G}_n(\alpha_i)} \cdot n_i < (n+1)^{\mathrm{G}_n(\alpha_0)+1} \leq (n+1)^{\mathrm{G}_n(\beta_0)} \leq \mathrm{G}_n(\beta)$.
2. $\alpha_0 = \beta_0$: Dann existieren $\tilde{\alpha} < \tilde{\beta} < \beta$ mit $\alpha = \omega^{\alpha_0} + \tilde{\alpha}$, $\beta = \omega^{\alpha_0} + \tilde{\beta}$, $\mathrm{G}_n(\alpha) = \mathrm{G}_n(\omega^{\alpha_0}) + \mathrm{G}_n(\tilde{\alpha})$, $\mathrm{G}_n(\beta) = \mathrm{G}_n(\omega^{\alpha_0}) + \mathrm{G}_n(\tilde{\beta})$; und nach I.V. ist $\mathrm{G}_n(\tilde{\alpha}) < \mathrm{G}_n(\tilde{\beta})$.
b) Die erste Gleichung folgt aus 13.1a,b und 13.2a; die zweite Gleichung folgt aus der ersten und 13.1c.
[Beweis von $\mathcal{S}(\mathrm{G}_n(\alpha), n+1) = \mathrm{G}_{n+1}(\alpha)$ durch Induktion nach α: Sei $0 < \alpha \in \mathrm{M}_n$, und
$\omega^{\alpha_0} \cdot n_0 + ... + \omega^{\alpha_k} \cdot n_k$ die Cantor-Normalform von α zur Basis ω. Sei $a_i := \mathrm{G}_n(\alpha_i)$ und $b_i := \mathrm{G}_{n+1}(\alpha_i)$.

Mit 13.1a,b und I.V. folgt $\mathcal{S}(\mathrm{G}_n(\alpha), n+1) = \mathcal{S}(\sum_{i\le k}(n+1)^{a_i}\cdot n_i, n+1) = \sum_{i\le k}(n+2)^{\mathcal{S}(a_i,n+1)}\cdot n_i = \sum_{i\le k}(n+2)^{b_i}\cdot n_i = \mathrm{G}_{n+1}(\alpha)$.]

c) Man nehme die vollständige Entwicklung von a zur Basis $n+1$ und ersetze darin $n+1$ durch ω; das liefert ein $\alpha \in \mathrm{M}_n$ mit $\mathrm{G}_n(\alpha) = a$. Die Eindeutigkeit folgt aus 13.2a. (Beim Beweis von $\mathrm{G}_n(\alpha) = a$ wird 13.2a ebenfalls verwendet.)

[Beweis der Existenz von α durch Induktion nach a. Sei $a > 0$. Dann $a = \sum_{i\le k}(n+1)^{a_i}\cdot n_i$ mit $a_k < ... < a_0 < a$ und $n_0, ..., n_k \in \{1, ..., n\}$. Nach I.V. existieren $\alpha_0, ..., \alpha_k \in \mathrm{M}_n$ mit $\mathrm{G}_n(\alpha_i) = a_i$. Mit a) folgt $\alpha_k < ... < \alpha_0$, also $\alpha := \omega^{\alpha_0}\cdot n_0 + ... + \omega^{\alpha_k}\cdot n_k \in \mathrm{M}_n$ und (nach 13.1a,b) $\mathrm{G}_n(\alpha) = a$.] $\triangle$

Lemma 13.3

a) $\mathrm{P}_n(\alpha+\beta) = \alpha + \mathrm{P}_n(\beta)$, falls $NF(\alpha,\beta)$.

b) $\mathrm{P}_n(\omega^\alpha) = \mathrm{P}_n(\omega^{\mathrm{P}_n(\alpha)}\cdot(n+1)) = \omega^{\mathrm{P}_n(\alpha)}\cdot n + \mathrm{P}_n(\omega^{\mathrm{P}_n(\alpha)})$, falls $\alpha > 0$.

c) $\alpha \in \mathrm{M}_n \;\Rightarrow\; \mathrm{P}_n(\alpha) \in \mathrm{M}_n$.

Beweis :

a) klar.

b) Es muß nur die erste Gleichung bewiesen werden; die zweite folgt aus a). — Induktion nach α:

1. $\mathrm{P}_n(\omega^{\alpha+1}) = \mathrm{P}_n(\omega^\alpha\cdot(n+1)) \;\&\; \alpha = \mathrm{P}_n(\alpha+1)$.

2. $\mathrm{P}_n(\omega^\lambda) = \mathrm{P}_n(\omega^{\lambda[n]}) = \mathrm{P}_n(\omega^{\mathrm{P}_n(\lambda[n])}\cdot(n+1)) = \mathrm{P}_n(\omega^{\mathrm{P}_n(\lambda)}\cdot(n+1))$.

c) Induktion nach α:

1. Sei $\alpha = \alpha_0 + \omega^\beta$ mit $\alpha_0 > 0 \,\&\, NF(\alpha_0, \omega^\beta)$. Dann auch $\alpha_0, \omega^\beta \in \mathrm{M}_n$ und nach I.V. $\mathrm{P}_n(\omega^\beta) \in \mathrm{M}_n$.
Aus $\alpha_0, \mathrm{P}_n(\omega^\beta) \in \mathrm{M}_n \;\&\; NF(\alpha_0,\omega^\beta) \;\&\; \mathrm{P}_n(\omega^\beta) < \omega^\beta$ folgt $\alpha_0 + \mathrm{P}_n(\omega^\beta) \in \mathrm{M}_n$.
Nach a) ist $\mathrm{P}_n(\alpha) = \alpha_0 + \mathrm{P}_n(\omega^\beta)$.

2. Sei $\alpha = \omega^\beta \;\&\; \beta \neq 0$. Dann $\beta \in \mathrm{M}_n$, und nach b) gilt $\mathrm{P}_n(\omega^\beta) = \omega^{\mathrm{P}_n(\beta)}\cdot n + \mathrm{P}_n(\omega^{\mathrm{P}_n(\beta)})$. Mit I.V. folgt $\mathrm{P}_n(\beta) \in \mathrm{M}_n$ und weiter $\omega^{\mathrm{P}_n\beta} \in \mathrm{M}_n$. Wegen $\omega^{\mathrm{P}_n(\beta)} < \alpha$ folgt daraus nach I.V. $\mathrm{P}_n(\omega^{\mathrm{P}_n(\beta)}) \in \mathrm{M}_n$. Mit $\mathrm{P}_n(\omega^{\mathrm{P}_n(\beta)}) < \omega^{\mathrm{P}_n(\beta)}$ folgt weiter $\omega^{\mathrm{P}_n(\beta)}\cdot n + \mathrm{P}_n(\omega^{\mathrm{P}_n(\beta)}) \in \mathrm{M}_n$. $\triangle$

Lemma 13.4

$\alpha \in \mathrm{M}_1 \;\&\; n \ge 1 \;\Rightarrow\; \mathrm{GS}(\mathrm{G}_1(\alpha), n) = \mathrm{G}_n(\mathrm{P}_n ... \mathrm{P}_2(\alpha))$.

Beweis :

Sei $a := \mathrm{G}_1(\alpha)$. Nach 13.3c gilt $\mathrm{P}_n ... \mathrm{P}_2(\alpha) \in \mathrm{M}_n$ für alle $n \ge 1$.

$\mathrm{GS}(a,1) = a = \mathrm{G}_1(\alpha)$.

$\mathrm{GS}(a, n+1) \overset{\mathrm{Def}}{=} \mathcal{S}(\mathrm{GS}(a,n), n+1) \dot{-} 1 \overset{\mathrm{IV}}{=} \mathcal{S}(\mathrm{G}_n(\mathrm{P}_n ... \mathrm{P}_2(\alpha)), n+1) \dot{-} 1 \overset{13.2\mathrm{b}}{=} \mathrm{G}_{n+1}(\mathrm{P}_{n+1}\mathrm{P}_n ... \mathrm{P}_2(\alpha))$. $\triangle$

Korollar $\quad \forall a \in \mathbb{N} \exists n.\, \mathrm{GS}(a,n) = 0$.

Beweis : Sei $a \in \mathbb{N}$. Nach 13.2c existiert ein $\alpha \in \mathrm{M}_1$ mit $\mathrm{G}_1(\alpha) = a$. Wegen $\forall \beta > 0 \forall n(\mathrm{P}_n(\beta) < \beta)$ existiert ein n mit $\mathrm{P}_n ... \mathrm{P}_2(\alpha) = 0$. Es folgt $\mathrm{GS}(a,n) = \mathrm{GS}(\mathrm{G}_1(\alpha), n) = \mathrm{G}_n(0) = 0$. $\triangle$

Definition

$h_0(n) := n, \quad h_{\alpha+1}(n) := h_\alpha(n+1), \quad h_\lambda(n) := h_{\lambda[n]}(n)$.

Lemma 13.5 $\quad H_\alpha(n) \le h_\alpha(n+1)$.

Beweis :

1. $\alpha = \beta + 1$: $H_\alpha(n) = H_\beta(n+1) \overset{\mathrm{I.V.}}{\le} h_\beta(n+2) = h_\alpha(n+1)$.

2. $\alpha \in Lim$: $H_\alpha(n) = H_{\alpha[n]}(n+1) \overset{12.10\mathrm{c},12.11\mathrm{d}}{\le} H_{\alpha[n+1][n]}(n+1) = H_{\alpha[n+1]}(n) \overset{\mathrm{I.V.}}{\le} h_{\alpha[n+1]}(n+1) = h_\alpha(n+1)$. $\triangle$

Lemma 13.6
a) $\alpha > 0 \;\Rightarrow\; h_\alpha(n) = h_{\mathrm{P}_n(\alpha)}(n+1)$.
b) $h_\alpha(n) = \min\{k \geq n : \mathrm{P}_{k-1}...\mathrm{P}_n(\alpha) = 0\}$.
Beweis :
a) Induktion nach α:
1. $\alpha = \beta + 1$: $h_\alpha(n) = h_\beta(n+1) = h_{\mathrm{P}_n(\alpha)}(n+1)$.
2. $\alpha \in Lim$: $h_\alpha(n) = h_{\alpha[n]}(n) \overset{\text{I.V.}}{=} h_{\mathrm{P}_n(\alpha[n])}(n+1) = h_{\mathrm{P}_n(\alpha)}(n+1)$.
b) Für $k = \min\{i \geq n : \mathrm{P}_{i-1}...\mathrm{P}_n(\alpha) = 0\}$ gilt offenbar
$h_\alpha(n) = h_{\mathrm{P}_n(\alpha)}(n+1) = h_{\mathrm{P}_{n+1}\mathrm{P}_n(\alpha)}(n+2) = \ldots = h_{\mathrm{P}_{k-1}...\mathrm{P}_n(\alpha)}(k) = h_0(k) = k$. △

Satz 13.7
$\mathrm{Z} \nvdash \forall x \exists y[\mathrm{GS}(x,y) = 0]$.
Beweis :
Sei $e(0) := 1,\ e(m+1) := 2^{e(m)}$. — Annahme: $\vdash \forall x \exists y[\mathrm{GS}(x,y) = 0]$.
$\Rightarrow \vdash \forall x \exists y[\mathrm{GS}(e(x)+x, y) = 0] \;\Rightarrow\; \exists p \forall m \geq p \exists n < H_{\omega_p}(m).\, \mathrm{GS}(e(m)+m, n) = 0 \;\Rightarrow$
$\Rightarrow\; \exists p(\, \min\{n : \mathrm{GS}(e(p)+p, n) = 0\} < H_{\omega_p}(p)\,)$.
$\mathrm{GS}(e(p)+p, n) = 0 \;\Leftrightarrow\; \mathrm{GS}(\mathrm{G}_1(\omega_p + p), n) = 0 \overset{13.4}{\Leftrightarrow} \mathrm{G}_n(\mathrm{P}_n...\mathrm{P}_2(\omega_p + p)) = 0 \;\Leftrightarrow\; \mathrm{P}_n...\mathrm{P}_2(\omega_p + p) = 0$.
Mit 13.5 und 13.6b folgt: $H_{\omega_p+p}(1) \leq h_{\omega_p+p}(2) = \min\{n \geq 2 : \mathrm{P}_{n-1}...\mathrm{P}_2(\omega_p + p) = 0\} =$
$= \min\{n : \mathrm{GS}(e(p)+p, n-1) = 0\} \leq H_{\omega_p}(p) = H_{\omega_p+p}(0) < H_{\omega_p+p}(1)$. *Widerspruch.* △

14 Elementare Rekursionstheorie

Definition
Eine *n-stellige partielle Funktion* ist eine Funktion f mit $\mathrm{dom}(f) \subseteq \mathbb{N}^n$ und $\mathrm{ran}(f) \subseteq \mathbb{N}$.
Schreibweise: $f : \mathbb{N}^n \overset{\text{part}}{\longrightarrow} \mathbb{N}$.

Wir legen hier den mengentheoretischen Funktionsbegriff aus Abschnitt 7 zugrunde, wonach eine Funktion identisch mit ihrem Graph ist. Für jede n-stellige partielle Funktion f gilt also $f \subseteq \mathbb{N}^n \times \mathbb{N}$.

Für partielle Funktionen f, g definieren wir:
$f(\vec{a}) \simeq b \;:\Leftrightarrow\; \vec{a} \in \mathrm{dom}(f)\,\&\, f(\vec{a}) = b \quad (\Leftrightarrow\; (\vec{a}, b) \in f\,)$.
$f(\vec{a}) \simeq g(\vec{c}) \;:\Leftrightarrow\; [\vec{a} \in \mathrm{dom}(f)\,\&\, \vec{c} \in \mathrm{dom}(g)\,\&\, f(\vec{a}) = g(\vec{c})]$ oder $[\vec{a} \notin \mathrm{dom}(f)\,\&\, \vec{c} \notin \mathrm{dom}(g)]$.

Definition der Operationen $\circ$, R, μ für partielle Funktionen:
1. Für $h : \mathbb{N}^m \overset{\text{part}}{\longrightarrow} \mathbb{N}$ und $g_1, ..., g_m : \mathbb{N}^n \overset{\text{part}}{\longrightarrow} \mathbb{N}$ sei $(\circ h g_1 ... g_m) : \mathbb{N}^n \overset{\text{part}}{\longrightarrow} \mathbb{N}$ definiert durch:
   $(\circ h g_1 ... g_m)(\vec{a}) \simeq b \;\Leftrightarrow\; \exists b_1 \ldots \exists b_m[h(b_1, ..., b_m) = b\,\&\, g_1(\vec{a}) = b_1\,\&\, \ldots\,\&\, g_m(\vec{a}) = b_m]$.
2. Für $g : \mathbb{N}^n \overset{\text{part}}{\longrightarrow} \mathbb{N}$ und $h : \mathbb{N}^{n+2} \overset{\text{part}}{\longrightarrow} \mathbb{N}$ sei $(\mathsf{R}gh) : \mathbb{N}^{n+1} \overset{\text{part}}{\longrightarrow} \mathbb{N}$ definiert durch:
   $(\mathsf{R}gh)(\vec{a}, 0) \simeq g(\vec{a})$,
   $(\mathsf{R}gh)(\vec{a}, k+1) \simeq b \;\Leftrightarrow\; \exists c[\,(\mathsf{R}gh)(\vec{a}, k) \simeq c\,\&\, h(\vec{a}, k, c) \simeq b\,]$.
3. Für $g : \mathbb{N}^{n+1} \overset{\text{part}}{\longrightarrow} \mathbb{N}$ sei $(\mu g) : \mathbb{N}^n \overset{\text{part}}{\longrightarrow} \mathbb{N}$ definiert durch:
   $(\mu g)(\vec{a}) \simeq b \;\Leftrightarrow\; g(\vec{a}, b) \simeq 0\,\&\, \forall i < b \exists c[c \neq 0\,\&\, g(\vec{a}, i) \simeq c]$.

Abkürzung:
Für $R \subseteq \mathbb{N}^{n+1}$ und $\vec{a} \in \mathbb{N}^n$ sei:
$\mu y.R(\vec{a}, y) := \begin{cases} \min\{k : (\vec{a}, k) \in R\} & \text{falls } \exists k\,(\vec{a}, k) \in R \\ \text{undefiniert} & \text{sonst} \end{cases}$
Anders gesagt, $\vec{a} \mapsto \mu y.R(\vec{a}, y)$ bezeichnet die partielle Funktion (μg) mit $g(\vec{a}, b) := 1 \dot{-} \mathbf{1}_R(\vec{a}, b)$.

Definition
Sei $f : \mathbb{N}^n \xrightarrow{\text{part}} \mathbb{N}$.
f heißt *partiell-rekursiv* $:\Leftrightarrow$ f ist rekursiv aufzählbar.
f heißt *total* $:\Leftrightarrow$ $\text{dom}(f) = \mathbb{N}^n$.

Bemerkung:
Eine Funktion $f : \mathbb{N}^n \xrightarrow{\text{part}} \mathbb{N}$ ist genau dann rekursiv, wenn sie partiell-rekursiv und total ist.

Satz 14.1
Die Menge aller partiell-rekursiven Funktionen ist die kleinste Funktionenmenge $\mathcal{P} = \bigcup_{n\in\mathbb{N}} \mathcal{P}^n$, für die gilt:
1. $\mathbf{0}^n, \mathsf{S}, \mathsf{I}_i^n \in \mathcal{P}$,
2. $h \in \mathcal{P}^m \ \&\ g_1, ..., g_m \in \mathcal{P}^n \ \&\ m, n \geq 1 \ \Rightarrow\ (\circ h g_1 ... g_m) \in \mathcal{P}^n$,
3. $g \in \mathcal{P}^n \ \&\ h \in \mathcal{P}^{n+2} \ \Rightarrow\ (\mathsf{R} g h) \in \mathcal{P}^{n+1}$,
4. $g \in \mathcal{P}^{n+1} \ \Rightarrow\ (\mu g) \in \mathcal{P}^n$.
Beweis : klar. (Vergl. Beweis von 4.15.)

Korollar
Ist $R \subseteq \mathbb{N}^{n+1}$ rekursiv, so ist die durch $f(\vec{a}) :\simeq \mu y.R(\vec{a}, y)$ definierte Funktion f partiell-rekursiv.

Churchsche These
Eine Funktion $f : \mathbb{N}^n \xrightarrow{\text{part}} \mathbb{N}$ ist genau dann im intuitiven Sinn berechenbar, wenn sie partiell-rekursiv ist.

Lemma 14.2
Eine Relation $Q \subseteq \mathbb{N}^n$ ist genau dann rekursiv aufzählbar, wenn sie Definitionsbereich einer n-st. partiell-rekursiven Funktion ist.
Beweis :
1. Sei Q rekursiv aufzählbar. Dann gibt es ein primitiv rekursives g mit $Q = \{\vec{a} : \exists b\, g(\vec{a}, b) = 0\}$, also $Q = \text{dom}((\mu g))$ und (μg) partiell-rekursiv.
2. Ist f partiell-rekursiv, so ist f rekursiv aufzählbar, und folglich auch $\text{dom}(f) = \{\vec{a} : \exists b\, (\vec{a}, b) \in f\}$ rekursiv aufzählbar. $\triangle$

Satz 14.3 (Kleenesches Normalform-Theorem)
Es gibt eine primitiv rekursive Funktion U und zu jedem $n \geq 1$ eine n-st. primitiv rekursive Relation T^n, so daß für $\{e\}^n(\vec{a}) :\simeq U(\mu y.\mathsf{T}^n(e, \vec{a}, y))$ gilt:
$\{\{e\}^n : e \in \mathbb{N}\}$ = Menge aller n-st. partiell-rekursiven Funktionen.
Die Relationen T^n $(n \geq 1)$ heißen *Kleenesche T-Prädikate*.
Beweis :
Definition: $Sb_0(e) := e$, $Sb_{n+1}(e, a_1, ..., a_{n+1}) := Sb_n(\mathsf{Sub}(\ulcorner \underline{a_{n+1}} \urcorner, \ulcorner v_{n+1} \urcorner, e), a_1, ..., a_n)$.
Offenbar gilt: $Sb_n(\ulcorner A \urcorner, a_1, ..., a_n) = \ulcorner A_{v_1,...,v_n}(\underline{a_1}, ..., \underline{a_n}) \urcorner$.
Definition:
$\mathsf{T}^n(e, a_1, ..., a_n, c) \ :\Leftrightarrow\ (Sb_{n+2}(e, \pi_1\pi_2(c), \pi_1(c), a_1, ..., a_n), \pi_2\pi_2(c)) \in \mathsf{Bew}_{\mathrm{Z}_0}$,
$U(c) := \pi_1(c)$,
$\{e\}^n(\vec{a}) :\simeq U(\mu y.\mathsf{T}^n(e, \vec{a}, y))$.
Offenbar sind U, T^n primitiv rekursiv. Daraus folgt sofort, daß für jedes $n \geq 1$ die Funktion $(e, \vec{a}) \mapsto \{e\}^n(\vec{a})$ partiell-rekursiv ist. Natürlich ist dann für alle $e \in \mathbb{N}$, $n \geq 1$ auch die Funktion $\{e\}^n$ partiell-rekursiv.
Sei jetzt $f : \mathbb{N}^n \xrightarrow{\text{part}} \mathbb{N}$ partiell-rekursiv. Dann gibt es eine $(n+2)$-st. (primitiv) rekursive Relation R mit $f = \{(\vec{a}, b) : \exists k\, R(k, b, \vec{a})\}$. Nach Satz 6.6 ist R in Z_0 repräsentierbar, und folglich gibt es eine

$(n{+}2)$-st. arithmetische Formel A mit $R = \{(k,b,\vec{a}) : \mathrm{Z}_0 \vdash A(\underline{k},\underline{b},\underline{\vec{a}})\}$. Sei $e := \ulcorner A \urcorner$. Dann gilt:
$f(\vec{a}) \simeq b \;\Leftrightarrow$
$\exists k,d[\,(\ulcorner A(\underline{k},\underline{b},\underline{\vec{a}})\urcorner, d) \in \mathsf{Bew}_{\mathrm{Z}_0}\,] \;\Leftrightarrow$
$\exists k,d[\,(Sb_{n+2}(e,k,b,\vec{a}),d) \in \mathsf{Bew}_{\mathrm{Z}_0}\,] \;\Leftrightarrow$
$\exists c[\,b = \pi_1(c) \;\&\; (Sb_{n+2}(e,\pi_1\pi_2(c),\pi_1(c),\vec{a}),\pi_2\pi_2(c)) \in \mathsf{Bew}_{\mathrm{Z}_0}\,] \;\Leftrightarrow$
$\exists c[\,b = U(c) \;\&\; \mathsf{T}^n(e,\vec{a},c)\,]$.
Daraus folgt $\mathrm{dom}(f) \subseteq \mathrm{dom}(\{e\}^n)$ und $(\,\{e\}^n(\vec{a}) \simeq b \;\Rightarrow\; f(\vec{a}) \simeq b\,)$, also $f = \{e\}^n$. $\triangle$

Bemerkung: Die $(n{+}1)$-st. Funktion $(e,\vec{a}) \mapsto \{e\}^n(\vec{a})$ ist partiell-rekursiv.

Abkürzung: $W_e^n := \mathrm{dom}(\{e\}^n) \quad (= \{\vec{a} \in \mathbb{N}^n : \exists c\, \mathsf{T}^n(e,\vec{a},c)\})$.

Bemerkung:
Nach 14.2 und 14.3 gilt: $\{W_e^n : e \in \mathbb{N}\}$ = Menge aller n-st. rekursiv aufzählbaren Relationen.

Satz 14.4 (Unlösbarkeit des Halteproblems)
$K := \{e \in \mathbb{N} : e \in W_e^1\}$ ist rekursiv aufzählbar aber nicht rekursiv.
Beweis :
1. K ist rekursiv aufzählbar, da $(e \in W_e^1 \;\Leftrightarrow\; \exists c\, \mathsf{T}^1(e,e,c))$ und T^1 prim. rekursiv.
2. *Annahme*: K rekursiv. Dann ist auch $\mathbb{N} \setminus K$ rekursiv (aufzählbar), und nach 14.3 existiert ein e_0 mit $\mathbb{N} \setminus K = W_{e_0}^1$. Es folgt: $e_0 \in K \;\Leftrightarrow\; e_0 \in W_{e_0}^1 \;\Leftrightarrow\; e_0 \notin K$. *Widerspruch.* $\triangle$

Bemerkung:
Intuitiv betrachtet hat T^n folgende Bedeutung:

$$\mathsf{T}^n(e,\vec{a},\pi(b,k)) \iff \left\{\begin{array}{l} e \text{ ist Nummer eines Programms, das angesetzt auf die} \\ \text{Eingabe } \vec{a} \text{ nach } k \text{ Schritten das Resultat } b \text{ liefert.} \end{array}\right.$$

Dann ist K die Menge aller Programmnummern e für die gilt *'das Programm mit Nummer e terminiert bei Eingabe e'.*

Satz 14.5 (s-m-n Theorem)
Zu $m,n \geq 1$ gibt es eine $(m{+}1)$-st. primitiv rekursive Funktion $\mathbf{s}_n^m$, so daß
für alle $e,c \in \mathbb{N}$, $\vec{a} \in \mathbb{N}^n$, $\vec{b} \in \mathbb{N}^m$ gilt:
a) $\mathsf{T}^{n+m}(e,\vec{a},\vec{b},c) \iff \mathsf{T}^n(\mathbf{s}_n^m(e,\vec{b}),\vec{a},c)$,
b) $\{e\}^{n+m}(\vec{a},\vec{b}) \simeq \{\mathbf{s}_n^m(e,\vec{b})\}^n(\vec{a})$.
Beweis :
Sei $\mathbf{s}_n^0(e) := e$ und $\mathbf{s}_n^{m+1}(e,b_1,...,b_{m+1}) := \mathbf{s}_n^m(\mathsf{Sub}(\ulcorner \underline{b_{m+1}} \urcorner, \ulcorner v_{n+m+3} \urcorner, e), b_1,...,b_m)$.
Wir beweisen $(*)$ $Sb_{n+m+2}(e,i,j,\vec{a},\vec{b}) = Sb_{n+2}(\mathbf{s}_n^m(e,\vec{b}),i,j,\vec{a})$.Daraus folgt dann sofort a) und b).
Beweis von $(*)$ durch Induktion nach m:
1. $m = 0$: trivial.
2. $Sb_{n+m+3}(e,i,j,\vec{a},\vec{b},b_{m+1}) \overset{\mathrm{Def}}{=} Sb_{n+m+2}(\mathsf{Sub}(\ulcorner \underline{b_{m+1}} \urcorner, \ulcorner v_{n+m+3} \urcorner, e), i,j,\vec{a},\vec{b}) \overset{\mathrm{IV}}{=}$
$Sb_{n+2}(\mathbf{s}_n^m(\mathsf{Sub}(\ulcorner \underline{b_{m+1}} \urcorner, \ulcorner v_{n+m+3} \urcorner, e),\vec{b}),i,j,\vec{a}) \overset{\mathrm{Def}}{=} Sb_{n+2}(\mathbf{s}_n^{m+1}(e,\vec{b},b_{m+1}),i,j,\vec{a})$. $\triangle$

Satz 14.6 (Rekursionstheorem)
Zu jeder $(n{+}1)$-st. partiell-rekursiven Funktion g existiert ein $e \in \mathbb{N}$ mit $\{e\}^n(\vec{a}) \simeq g(e,\vec{a})$ für alle $\vec{a} \in \mathbb{N}^n$.
Beweis :
Nach 14.3 existiert ein k mit $\{k\}^{n+1}(\vec{a},e) \simeq g(\mathbf{s}_n^1(e,e),\vec{a})$, für alle $\vec{a},e$. — Sei $e := \mathbf{s}_n^1(k,k)$.
Dann $\{e\}^n(\vec{a}) \simeq \{\mathbf{s}_n^1(k,k)\}^n(\vec{a}) \overset{14.5}{\simeq} \{k\}^{n+1}(\vec{a},k) \simeq g(\mathbf{s}_n^1(k,k),\vec{a}) \simeq g(e,\vec{a})$. $\triangle$

Korollar
Zu jedem $n \geq 1$ und jeder 1-st. rekursiven Funktion f existiert ein $e \in \mathbb{N}$ mit $\{f(e)\}^n = \{e\}^n$.

Beweis : Setze $g(e,\vec{a}) :\simeq \{f(e)\}^n(\vec{a})$ und wende 14.6 an. $\triangle$

Beispiel zum Rekursions-Theorem

Die Ackermann-Funktion $\mathcal{A} : \mathbb{N}^2 \to \mathbb{N}$ ist definiert durch

$$\mathcal{A}(m,k) := \begin{cases} k+1 & \text{falls } m = 0 \\ \mathcal{A}(m\dot{-}1, 1) & \text{falls } m > 0 \,\&\, k = 0 \\ \mathcal{A}(m\dot{-}1, \mathcal{A}(m, k\dot{-}1)) & \text{sonst} \end{cases}$$

Definition einer partiell-rekursiven Funktion g:

$$g(e,m,k) :\simeq \begin{cases} k+1 & \text{falls } m = 0 \\ \{e\}^2(m\dot{-}1, 1) & \text{falls } m > 0 \,\&\, k = 0 \\ \{e\}^2(m\dot{-}1, \{e\}^2(m, k\dot{-}1)) & \text{sonst} \end{cases}$$

Nach dem Rekursions-Theorem existiert ein e mit $\{e\}^2(m,k) \simeq g(e,m,k)$ für alle m,k.
Durch Hauptinduktion nach m und Nebeninduktion nach k zeigt man $\{e\}^2(m,k) \simeq \mathcal{A}(m,k)$. Folglich ist $\mathcal{A}$ rekursiv.

Beispiel zum s-m-n Theorem

Behauptung:
Es gibt eine prim. rek. Funktion h mit $\{h(b,u)\}^1(0) = b$ und $\{h(b,u)\}^1(\langle i\rangle * c) \simeq \{\{u\}^1(i)\}^1(c)$.
Beweis:
Def.: $\langle a_0,...,a_{n-1}\rangle * \langle b_0,...,b_{m-1}\rangle := \langle a_0,...,a_{n-1},b_0,...,b_{m-1}\rangle$.
Sei $f \in \mathrm{PR}$ mit $a = \langle (a)_0\rangle * f(a)$ für alle $a \in \mathbb{N}$. Sei ferner $e \in \mathbb{N}$, so daß

$$\{e\}^3(a,b,u) \simeq \begin{cases} b & \text{falls } a = 0 \\ \{\{u\}^1((a)_0)\}^1(f(a)) & \text{sonst} \end{cases}.$$

Für $h(b,u) := \mathbf{s}^2_1(e,b,u)$ gilt dann:
$\{h(b,u)\}^1(0) \simeq \{e\}^3(0,b,u) \simeq b$,
$\{h(b,u)\}^1(\langle i\rangle * c) \simeq \{e\}^3(\langle i\rangle * c, b, u) \simeq \{\{u\}^1(i)\}^1(c)$.

Satz 14.7 (Rice)
Für jede Menge $\mathcal{F}$ n-st. partiell-rekursiver Funktionen mit $\emptyset \neq \mathcal{F} \neq \{\{e\}^n : e \in \mathbb{N}\}$ ist die Menge $\{e \in \mathbb{N} : \{e\}^n \in \mathcal{F}\}$ nicht rekursiv.
Beweis :
Nach Voraussetzung existieren $e_0, e_1 \in \mathbb{N}$ mit $\{e_0\}^n \notin \mathcal{F}$ und $\{e_1\}^n \in \mathcal{F}$. Sei $R \subseteq \mathbb{N}$ irgendeine rekursive Menge. Wir zeigen $R \neq \{e : \{e\}^n \in \mathcal{F}\}$.

Sei $g : \mathbb{N}^{n+1} \xrightarrow{\text{part}} \mathbb{N}$, $g(e,a) :\simeq \begin{cases} \{e_0\}^n(a) & \text{falls } e \in R \\ \{e_1\}^n(a) & \text{falls } e \notin R \end{cases}$.

Nach dem Rekursionstheorem existiert ein e mit $\forall a \in \mathbb{N}^n(\{e\}^n(a) \simeq g(e,a))$.
Es folgt:
$e \in R \Rightarrow \forall a(\{e\}^n(a) \simeq g(e,a) \simeq \{e_0\}^n(a)) \Rightarrow \{e\}^n = \{e_0\}^n \Rightarrow \{e\}^n \notin \mathcal{F}$.
$e \notin R \Rightarrow \forall a(\{e\}^n(a) \simeq g(e,a) \simeq \{e_1\}^n(a)) \Rightarrow \{e\}^n = \{e_1\}^n \Rightarrow \{e\}^n \in \mathcal{F}$. $\triangle$

Beweisbar rekursive Funktionen

Definition
Eine rekursive Funktion $f : \mathbb{N}^n \to \mathbb{N}$ heißt *beweisbar rekursiv in* Z, falls es prim. rek. Funktionen U_f und T_f gibt, so daß
(i) $\mathrm{Z} \vdash \forall \vec{x} \exists y\, T_f \vec{x} y = 0$,
(ii) $f = U_f \circ (\mu T_f)$.

Lemma 14.8
Eine rekursive Funktion $f : \mathbb{N}^n \to \mathbb{N}$ ist genau dann *beweisbar rekursiv in* Z, wenn es eine Σ_1-Formel $A(\vec{x}, y)$ (der Sprache PR) gibt, so daß
(i)' $\mathrm{Z} \vdash \forall \vec{x} \exists y\, A(\vec{x}, y)$,
(ii)' $\forall \vec{a}, b(\, f(\vec{a}) = b \Leftrightarrow \mathcal{N} \models A[\vec{a}, b])$.
Beweis :
I. Sei f beweisbar rekursiv. $A(x, y) := \exists z(T_f(x, z) = 0 \wedge \forall u{<}z(T_f xu \neq 0) \wedge y = U_f z)$.
(i)' $\mathrm{Z} \vdash \forall x \exists y(T_f xy = 0) \Rightarrow \mathrm{Z} \vdash \forall x \exists z(T_f xz = 0 \wedge \forall u{<}z(T_f xu \neq 0)) \Rightarrow \mathrm{Z} \vdash \forall x \exists y A(x, y)$.
(ii)' klar.
II. Gelte $\mathrm{Z} \vdash \forall x \exists y A(x, y)$ und $\forall a, b(f(a) = b \Leftrightarrow \mathcal{N} \models A[a, b])$.
Es existiert eine prim. rek. Funktion g mit $\mathrm{Z} \vdash A(x, y) \leftrightarrow \exists z(gxyz = 0)$. Sei $T_f(e, b) := g(e, \pi_1 b, \pi_2 b)$.
(i) $\mathrm{Z} \vdash \forall x \exists y A(x, y) \Rightarrow \mathrm{Z} \vdash \forall x \exists y \exists z(gxyz = 0) \Rightarrow \mathrm{Z} \vdash \forall x \exists y(T_f xy = 0)$.
(ii) $c = \min\{k : T_f(a, k) = 0\} \Rightarrow g(a, \pi_1(c), \pi_2(c)) = 0 \Rightarrow \mathcal{N} \models A[a, \pi_1(c)] \Rightarrow f(a) = \pi_1(c)$. △

Bemerkung:
Nach Satz 12.17 gibt es zu jeder in Z beweisbar rekursiven Funktion $f : \mathbb{N} \to \mathbb{N}$ ein $\alpha < \varepsilon_0$ mit $f \leq H_\alpha$.
Daraus folgt u.a., daß die Funktion H_{ε_0} (i.e. $n \mapsto H_{\omega_n}(n+1)$) nicht beweisbar rekursiv in Z ist.
Umgekehrt kann gezeigt werden, daß jedes H_α ($\alpha < \varepsilon_0$) beweisbar rekursiv ist.
Zusammenfassend erhält man folgende Charakterisierung der beweisbar rekursiven Funktionen von Z:
$f : \mathbb{N} \to \mathbb{N}$ ist genau dann beweisbar rekursiv in Z, wenn es $g \in \mathrm{PR}$ und $\alpha < \varepsilon_0$ mit
$f(n) = g(n, H_\alpha(n)) \quad (\forall n \in \mathbb{N})$ gibt.

DIE TURINGMASCHINE

Die historisch älteste abstrakte Rechenmaschine ist die nach dem englischen Logiker A.M. Turing benannte *Turingmaschine*. In ihr wird das Rechnen mit Bleistift und Papier idealisiert. Wir wollen zunächst eine anschauliche Beschreibung der Turingmaschine geben. Der Speicher der Maschine besteht aus einem nach beiden Seiten hin unendlichen Band, das in einzelne Felder unterteilt ist, und einem Schreib-Lese-Kopf. Dieser steht auf einem der Felder des Bandes, dem Arbeitsfeld. Die Turingmaschine kann nun die folgenden Befehle ausführen:
– Ein Zeichen a eines vorgegebenen endlichen Alphabets Σ auf das Arbeitsfeld drucken.
– Das Arbeitsfeld löschen (oder anders gesagt: das Leerzeichen 0 drucken).
– Den Schreib-Lese-Kopf um ein Feld nach links bzw. rechts bewegen.
– Testen, ob das Zeichen auf dem Arbeitsfeld mit einem bestimmten Zeichen $z \in \Sigma \cup \{0\}$ übereinstimmt.

Definitionen
Σ sei ein im folgenden festes Alphabet mit $\Sigma \cap \{0, \mathsf{L}, \mathsf{R}\} = \emptyset$.
$\Sigma_0 := \Sigma \cup \{0\}, \quad \Sigma_1 := \Sigma \cup \{0, \mathsf{L}, \mathsf{R}\}$.
$\Sigma^\# := \{\varphi : \varphi : \mathsf{Z} \to \Sigma_0 \ \ \& \ \ \{i \in \mathsf{Z} : \varphi(i) \neq 0\}$ endlich $\}$, wobei $\mathsf{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
(Die Elemente von $\Sigma^\#$ heißen *Bandinschriften*.)
Eine *Turingprogramm* ist eine Funktion $P : n \times \Sigma_0 \to (n{+}1) \times \Sigma_1$.
$n{+}1 = \{0, ..., n\}$ heißt *Zustandsmenge* von P.
$l(P) := n$ heißt die *Länge* von P.
0 heißt *Anfangszustand* von P.
$stop(P) := n$ heißt *Endzustand* von P.

Zu P wird eine *Zustandsübergangsfunktion* $\delta_P : \mathbb{N} \times \Sigma^\# \to \mathbb{N} \times \Sigma^\#$ wie folgt definiert:

1. Ist $i \geq n$, so $\delta_P(i, \varphi) := (i, \varphi)$.
2. Sei $i < n$ und $P(i, \varphi(0)) = (j, x) \in (n{+}1) \times \Sigma_1$.
   Dann $\delta_P(i, \varphi) := (j, \psi)$, wobei $\psi \in \Sigma^\#$ folgendermaßen definiert sei:

2.1. $x \in \Sigma_0$: $\psi(0) := x$ und $\psi(i) := \varphi(i)$ für $i \neq 0$.
2.2. $x = \mathsf{R}$: $\psi(i) := \varphi(i{+}1)$.
2.3. $x = \mathsf{L}$: $\psi(i) := \varphi(i{-}1)$.

Definition der Funktion $[P] : \Sigma^\# \stackrel{\text{part}}{\longrightarrow} \Sigma^\#$ für jedes Turingprogramm P

$[P](\varphi) \simeq \psi \;:\Leftrightarrow$ Es existiert ein k mit $\delta_P^{(k)}(0, \varphi) = (\mathit{stop}(P), \psi)$.

Definition

Σ enthalte das Symbol 1.

Für $a_1, ..., a_n \in \mathbb{N}$ bezeichne $\varphi_{a_1,...,a_n}$ die folgende Bandinschrift φ:

$$\varphi(i) := \begin{cases} 1 & \text{falls } i = a_1 + ... + a_k + k + j \text{ mit } 0 \leq k < n \text{ und } 1 \leq j \leq a_{k+1} \\ 0 & \text{sonst} \end{cases}$$

Für jedes Turing-Programm P und $n \geq 1$ sei

$f_P^n : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$, $f_P^n(a_1, ..., a_n) :\simeq \mathit{out}([P](\varphi_{a_1,...,a_n}))$, wobei $\mathit{out}(\psi) := \min\{i \geq 0 : \psi(i+1) = 0\}$.

Definition

$f : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ heißt *Turing-berechenbar*, falls es ein Turing-Programm P mit $f = f_P^n$ gibt.

Satz

Für $f : \mathbb{N}^n \stackrel{\text{part}}{\longrightarrow} \mathbb{N}$ gilt:

f Turing-berechenbar $\Leftrightarrow$ f partiell-rekursiv.

15 Der 2. Gödelsche Unvollständigkeitssatz

Zur Vermeidung von Mißverständnissen werden wir in diesem Abschnitt die Gleichheit zwischen Zeichenreihen (Termen, Formeln) mit dem Symbol $\equiv$ ausdrücken. Eine Formel der Sprache PR heißt *wahr* (bzw. *falsch*), wenn sie geschlossen ist und im Standardmodell gilt (bzw. nicht gilt). Unter einer Σ_1-Formel verstehen wir jetzt (im Gegensatz zu Abschnitt 5) eine PR-Formel der Gestalt $\exists x A$, wobei A Primformel ist.

Lemma 15.1

Für jedes $f \in \mathrm{PR}^n$ und alle $a_1, ..., a_n \in \mathbb{N}$ gilt: $f(a_1, ..., a_n) = b \;\Rightarrow\; \mathrm{Z} \vdash f\underline{a_1}...\underline{a_n} = \underline{b}$.

Beweis durch Induktion nach dem Aufbau von f:

1. $\mathsf{S}(a) = b \;\Rightarrow\; \mathsf{S}\underline{a} \equiv \underline{b} \;\Rightarrow\; \mathrm{Z} \vdash \mathsf{S}\underline{a} = \underline{b}$.
2. $\mathbf{0}^n(a_1, ..., a_n) = b \;\Rightarrow\; 0 = b \;\Rightarrow\; \mathrm{Z} \vdash \mathbf{0}^n\underline{a_1}...\underline{a_n} = \underline{b}$.
3. $\mathsf{I}_i^n(a_1, ..., a_n) = b \;\Rightarrow\; a_i = b \;\Rightarrow\; \mathrm{Z} \vdash \mathsf{I}_i^n\underline{a_1}...\underline{a_n} = \underline{b}$.
4. $f = (\circ h g_1 ... g_m)$ und $f(a) = b$:
   Dann $h(b_1, ..., b_m) = b$ mit $b_1 := g_1(a), \ldots, b_m := g_m(a)$, und nach I.V. gilt
   $\mathrm{Z} \vdash h\underline{b_1}...\underline{b_m} = \underline{b} \wedge g_1\underline{a} = \underline{b_1} \wedge \ldots \wedge g_m\underline{a} = \underline{b_m}$. Daraus folgt $\mathrm{Z} \vdash f\underline{a} = hg_1\underline{a}...g_m\underline{a} = h\underline{b_1}...\underline{b_m} = \underline{b}$.
5. $f = (\mathsf{R}gh)$: Nebeninduktion nach dem letzten Argument von f.
   5.1. $f(a, 0) = b \;\Rightarrow\; g(a) = b \stackrel{\text{I.V.}}{\Rightarrow} \mathrm{Z} \vdash f\underline{a}0 = g\underline{a} = \underline{b}$.
   5.2. Sei $f(a, c{+}1) = b$. Dann gilt $h(a, c, d) = b$ mit $d := f(a, c)$. Mit I.V. bzw. N.I.V. folgt daraus
   $\mathrm{Z} \vdash h\underline{a}\,\underline{c}\,\underline{d} = \underline{b}$ und $\mathrm{Z} \vdash f\underline{a}\,\underline{c} = \underline{d}$, also $\mathrm{Z} \vdash f\underline{a}\,\underline{c{+}1} = f\underline{a}\mathsf{S}\underline{c} = h\underline{a}\,\underline{c}\,f\underline{a}\,\underline{c} = \underline{b}$. $\triangle$

Korollar

a) Ist t ein PR-Term mit $\mathrm{FV}(t) \subseteq \{x_1, ..., x_n\}$, so gilt für alle $a_1, ..., a_n \in \mathbb{N}$:
$t^{\mathcal{N}}_{x_1,...,x_n}[a_1, ..., a_n] = b \;\Rightarrow\; \mathrm{Z} \vdash t_{x_1,...,x_n}(\underline{a_1}, ..., \underline{a_n}) = \underline{b}$.

b) $\mathrm{Z} \vdash A$, für jede wahre PR-Primformel A.

c) $\mathrm{Z} \vdash C$, für jeden wahren Σ_1-Satz C.

Voraussetzungen, Abkürzungen, Definitionen

Sei $(\mathcal{L}, SN)$ eine primitiv rekursiv repräsentierte Sprache (vergl. Abschnitt 5) mit $\mathrm{PR} \subseteq \mathcal{L}$. Wie in Abschnitt 5, sei jedem $\mathcal{L}$-Ausdruck E eine Gödelnummer $\ulcorner E \urcorner$ zugeordnet.

Mit "Term" bzw. "Formel" ist im folgenden stets "$\mathcal{L}$-Term" bzw. "$\mathcal{L}$-Formel" gemeint.

Für $q \in \mathcal{L} \cup \mathrm{VAR} \cup \{\bot, \to, \forall, =\}$ sei $\hat{q} :\equiv \underline{SN(q)}$.

Für PR-Terme $t_1, ..., t_{n-1}$ sei der PR-Terme $\langle t_0, ..., t_{n-1}\rangle$ wie folgt definiert:

$\langle\rangle :\equiv 0, \qquad \langle t_0, ..., t_n\rangle :\equiv \mathsf{S}\pi\langle t_0, ..., t_{n-1}\rangle t_n$.

Es sei $\nu \in \mathrm{PR}^1$ mit $\mathrm{Z} \vdash \nu 0 = \underline{\ulcorner 0 \urcorner} \wedge \nu\mathsf{S}x = \langle\hat{\mathsf{S}}, \nu x\rangle$.

(Es gilt also $\nu(n) = \ulcorner \underline{n} \urcorner$ für alle $n \in \mathbb{N}$.)

Definition

Eine Formel heiße *einfach*, wenn sie aus Primformeln und geschlossenen Formeln der Gestalt $\forall x A$ mittels $\to$ aufgebaut ist. Terme und einfache Formeln nennen wir *einfache Ausdrücke*.

Konvention: Im folgenden schreiben wir $\ulcorner E \urcorner$ statt $\underline{\ulcorner E \urcorner}$

Mitteilungszeichen: q bezeichne stets ein Symbol aus $\mathcal{L} \cup \{\bot, \to, =\}$.

Satz 15.2

(S1) $\mathrm{Z} \vdash \mathsf{Sub}y\ulcorner x \urcorner\ulcorner E \urcorner = \ulcorner \theta \urcorner$, falls E ein $\mathcal{L}$-Ausdruck mit $x \notin \mathrm{FV}(E)$

(S2) $\mathrm{Z} \vdash \mathsf{Sub}y\ulcorner x \urcorner\ulcorner x \urcorner = y$,

(S3) $\mathrm{Z} \vdash \mathsf{Sub}y\ulcorner x \urcorner\langle\hat{q}, z_1, ..., z_n\rangle = \langle\hat{q}, \mathsf{Sub}y\ulcorner x \urcorner z_1, \ldots, \mathsf{Sub}y\ulcorner x \urcorner z_n\rangle$, wobei $n = \#(q)$.

Ohne Beweis.

Definition eines PR-Terms $[E]^U$ für jeden einfachen Ausdruck E und jede endliche Variablenmenge U

1. $[x]^U :\equiv \begin{cases} \nu x & \text{falls } x \in U \\ \ulcorner x \urcorner & \text{sonst} \end{cases}$, 2. $[qE_1...E_n]^U :\equiv \langle\hat{q}, [E_1]^U, ..., [E_n]^U\rangle$, 3. $[\forall x A]^U :\equiv \ulcorner \forall x A \urcorner$

Definition $[E] :\equiv [E]^U$ mit $U := \mathrm{FV}(E)$.

Bemerkung: $[x] \equiv \nu x$ und $[qE_1...E_n] \equiv \langle\hat{q}, [E_1], ..., [E_n]\rangle$.

Lemma 15.3

a) $\mathrm{Z} \vdash [E]^{\emptyset} = \ulcorner E \urcorner$, falls E einfach.

b) $\mathrm{Z} \vdash [t] = \nu t \to [E_y(t)] = [E]_y(t)$, falls E einfach.

c) $\mathrm{Z} \vdash [0] = \nu 0 \wedge [\mathsf{S}x] = \nu\mathsf{S}x \wedge [x] = \nu x$.

Beweis :

a) Induktion nach dem Aufbau von E: 1. $[x]^{\emptyset} \equiv \ulcorner x \urcorner$.

2. Sei $E \equiv qE_1...E_n$. Nach 15.1 bzw. I.V. gilt dann $\vdash \langle\hat{q}, \ulcorner E_1 \urcorner, ..., \ulcorner E_n \urcorner\rangle = \ulcorner E \urcorner$ und $\vdash [E_i]^{\emptyset} = \ulcorner E_i \urcorner$.

Es folgt $\vdash [E]^{\emptyset} = \langle\hat{q}, [E_1]^{\emptyset}, ..., [E_n]^{\emptyset}\rangle = \ulcorner E \urcorner$.

3. Für $E \equiv \forall x A$ ist die Beh. trivial.

b) Induktion nach dem Aufbau von E (klar).

c) $\vdash [0] = \langle\hat{0}\rangle = \ulcorner 0 \urcorner = \nu 0$ und $\vdash [\mathsf{S}x] = \langle\hat{\mathsf{S}}, [x]\rangle = \langle\hat{\mathsf{S}}, \nu x\rangle = \nu\mathsf{S}x$. $\triangle$

Lemma 15.4

a) $\mathrm{Z} \vdash \mathsf{Sub} y^{\ulcorner} x^{\urcorner} \nu z = \nu z$,

b) $\mathrm{Z} \vdash \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [E]^U = [E]^{U \cup \{x\}}$.

Beweis :

a) $\vdash \mathsf{Sub} y^{\ulcorner} x^{\urcorner} \nu 0 = \mathsf{Sub} y^{\ulcorner} x^{\urcorner} {}^{\ulcorner} 0^{\urcorner} = {}^{\ulcorner} 0^{\urcorner} = \nu 0$. $\vdash \mathsf{Sub} y^{\ulcorner} x^{\urcorner} \nu \mathsf{S} z = \mathsf{Sub} y^{\ulcorner} x^{\urcorner} \langle \hat{\mathsf{S}}, \nu z \rangle = \langle \hat{\mathsf{S}}, \mathsf{Sub} y^{\ulcorner} x^{\urcorner} \nu z \rangle = \langle \hat{\mathsf{S}}, \nu z \rangle = \nu \mathsf{S} z$.

b) Abkürzung: $U' := U \cup \{x\}$

1. $E \equiv y \in U$: $\vdash \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [E]^U = \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} \nu y = \nu y = [E]^{U'}$.
2. $E \equiv x \notin U$: $\vdash \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [E]^U = \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} {}^{\ulcorner} x^{\urcorner} = \nu x = [E]^{U'}$.
3. $E \equiv y \notin U'$: $\vdash \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [E]^U = \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} {}^{\ulcorner} y^{\urcorner} = {}^{\ulcorner} y^{\urcorner} = [E]^{U'}$.
4. $E \equiv q E_1 ... E_n$: $\vdash \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [E]^U = \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} \langle \hat{q}, [E_1]^U, ..., [E_n]^U \rangle = \langle \hat{q}, \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [E_1]^U, ..., \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [E_n]^U \rangle$
$= \langle \hat{q}, [E_1]^{U'}, ..., [E_n]^{U'} \rangle = [E]^{U'}$.
5. $E \equiv \forall x A$ und $\mathrm{FV}(E) = \emptyset$: $\vdash \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [E]^U = \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} {}^{\ulcorner} E^{\urcorner} = {}^{\ulcorner} E^{\urcorner} = [E]^{U'}$. △

Im folgenden sei T ein Axiomensystem mit $\mathrm{L}(T) = \mathcal{L}$ und $\mathrm{Z} \subseteq T$.

Lemma 15.5

Ist P eine 1-st. Formel mit:

(P1) $T \vdash A \;\Rightarrow\; T \vdash \mathsf{P}({}^{\ulcorner} A^{\urcorner})$, für jede einfache Formel A

(P2) $T \vdash \mathsf{P}([A \to B]) \to \mathsf{P}([A]) \to \mathsf{P}([B])$, für alle einfachen Formeln A, B,

(P3) $T \vdash \mathsf{P}(z) \to \mathsf{P}(\mathsf{Sub} \nu y^{\ulcorner} x^{\urcorner} z)$,

so gilt,

(P)* $T \vdash A_1 \to \ldots \to A_m \to B \implies T \vdash \mathsf{P}([A_1]) \to \ldots \to \mathsf{P}([A_m]) \to \mathsf{P}([B])$,
für alle einfachen Formeln $A_1, ..., A_m, B$ $(m \geq 0)$.

Beweis :

(1) $T \vdash A \,\&\, A$ einfach $\Rightarrow$ $T \vdash \mathsf{P}([A]^U)$.

Beweis durch Induktion nach der Anzahl der Elemente von U:

1. $(\vdash A \Rightarrow \vdash \mathsf{P}({}^{\ulcorner} A^{\urcorner}))$ und $\vdash {}^{\ulcorner} A^{\urcorner} = [A]^{\emptyset}$.
2. $\vdash \mathsf{P}([A]^U) \to \mathsf{P}(\mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [A]^U)$ und $\vdash \mathsf{Sub} \nu x^{\ulcorner} x^{\urcorner} [A]^U = [A]^{U \cup \{x\}}$.

(2) Für einfache Formeln $A_1, ..., A_m, B$ gilt:

$T \vdash \mathsf{P}([A_1 \to \ldots \to A_m \to B]) \to \mathsf{P}([A_1]) \to \ldots \to \mathsf{P}([A_m]) \to \mathsf{P}([B])$.

Beweis durch Induktion nach m:

1. $m = 0$: trivial. 2. $m > 0$: Sei $C := A_2 \to ... \to A_m \to B$.

Wegen (P2) gilt dann $\vdash \mathsf{P}([A_1 \to \ldots \to A_m \to B]) \to \mathsf{P}([A_1]) \to \mathsf{P}([C])$.

Nach I.V. gilt ferner: $\vdash \mathsf{P}([C]) \to \mathsf{P}([A_2]) \to \ldots \to \mathsf{P}([A_m]) \to \mathsf{P}([B])$.

Aus (1) und (2) folgt nun (P)*. △

Lemma 15.6

Ist P eine 1-st. Formel mit (P)*, so gilt für jedes n-st. Funktionszeichen $f \in \mathrm{PR}$:

$T \vdash f x_1 ... x_n = y \to \mathsf{P}([f x_1 ... x_n = y])$.

Beweis durch Induktion nach der Definition von f:

Vorbemerkung: Aus 15.3b,c folgt:

(I) $\mathrm{Z} \vdash [E_y(t)] = [E]_y(t)$, für $t \in \{0, x, \mathsf{S} x\}$ und E einfach.

Im folgenden wird von der Operation $A \mapsto [A]$ nichts weiter als (P)*, (I) und die Tatsache, daß $[A]$ ein PR-Term mit $\mathrm{FV}([A]) = \mathrm{FV}(A)$ ist, benutzt.

1. $f \equiv \mathbf{0}^n$:

(1) $\vdash f \vec{x} = 0$,

(2) $\vdash \mathsf{P}([f\vec{x} = 0])$, [(1),(P)*]
(3) $\vdash 0 = y \to [f\vec{x} = 0] = [f\vec{x} = y]_y(0) = [f\vec{x} = y]$, [(I)]
(4) $\vdash f\vec{x} = y \to \mathsf{P}([f\vec{x} = y])$ [(1),(2),(3)]

2. $f \equiv \mathsf{I}_i^n$: analog zu 1.

3. $f \equiv \mathsf{S}$:

(1) $\vdash \mathsf{P}([fx = \mathsf{S}x])$, [(P)*]
(2) $\vdash \mathsf{S}x = y \to [fx = \mathsf{S}x] = [fx = y]_y(\mathsf{S}x) = [fx = y]$, [(I)]

4. $f \equiv (\circ h g_1 ... g_m)$:

(1) $\vdash \mathsf{P}([g_1\vec{x} = y_1]) \to \ldots \to \mathsf{P}([g_m\vec{x} = y_m]) \to \mathsf{P}([hy_1...y_m = y]) \to \mathsf{P}([f\vec{x} = y])$, [(P)*]
(2) $\vdash g_i\vec{x} = y_i \to \mathsf{P}([g_i\vec{x} = y_i])$, [I.V.]
(3) $\vdash hy_1...y_m = y \to \mathsf{P}([hy_1...y_m = y])$, [I.V.]
(4) $\vdash g_1\vec{x} = y_1 \to \ldots \to g_m\vec{x} = y_m \to hy_1...y_m = y \to \mathsf{P}([f\vec{x} = y])$, [(1),(2),(3)]
(5) $\vdash hg_1\vec{x} \ldots g_m\vec{x} = y \to \mathsf{P}([f\vec{x} = y])$, [(4) mit $g_i\vec{x}$ anstelle von y_i]

5. $f \equiv (\mathsf{R}gh)$:

Sei $t :\equiv [f\vec{x}z = y]$. Wir werden $\vdash \mathsf{P}(t_{z,y}(0, f\vec{x}0))$ und $\vdash \mathsf{P}(t_{z,y}(z, f\vec{x}z)) \to \mathsf{P}(t_{z,y}(\mathsf{S}z, f\vec{x}\mathsf{S}z))$ beweisen.
Mit (formaler) Induktion folgt daraus $\vdash \mathsf{P}(t_{z,y}(z, f\vec{x}z))$ und weiter $\vdash f\vec{x}z = y \to \mathsf{P}(t)$.

5.1. (1) $\vdash \mathsf{P}([g\vec{x} = y]) \to \mathsf{P}([f\vec{x}0 = y])$, [(P)*]
(2) $\vdash g\vec{x} = y \to \mathsf{P}([g\vec{x} = y])$, [I.V.]
(3) $\vdash t_z(0) = [f\vec{x}0 = y]$, [(I)]
(4) $\vdash g\vec{x} = y \to \mathsf{P}(t_z(0))$, [(1),(2),(3)]
(5) $\vdash \mathsf{P}(t_{z,y}(0, f\vec{x}0))$. [(4) mit $f\vec{x}0$ anstelle von y]

5.2. (1') $\vdash \mathsf{P}([h\vec{x}zw = y]) \to \mathsf{P}([f\vec{x}z = w]) \to \mathsf{P}([f\vec{x}\mathsf{S}z = y])$, [(P)*]
(2') $\vdash h\vec{x}zw = y \to \mathsf{P}([h\vec{x}zw = y])$, [I.V.]
(3') $\vdash t_y(w) = [f\vec{x}z = w] \wedge t_z(\mathsf{S}z) = [f\vec{x}\mathsf{S}z = y]$, [(I)]
(4') $\vdash h\vec{x}zw = y \to \mathsf{P}(t_y(w)) \to \mathsf{P}(t_z(\mathsf{S}z))$, [(1'),(2'),(3')]
(5') $\vdash \mathsf{P}(t_{z,y}(z, f\vec{x}z)) \to \mathsf{P}(t_{z,y}(\mathsf{S}z, f\vec{x}\mathsf{S}z))$. [(4') mit $f\vec{x}z$, $f\vec{x}\mathsf{S}z$ anstelle von w, y] $\triangle$

Satz 15.7

Ist P eine 1-st. Formel, welche (P)* erfüllt, so gilt: $T \vdash C \to \mathsf{P}(\ulcorner C \urcorner)$, für jeden Σ_1-Satz C.

Beweis :

Sei $g \in \mathrm{PR}^1$ mit $\mathrm{Z} \vdash \exists x(gx = 0) \leftrightarrow C$.

(1) $T \vdash gx = 0 \to C$, [klar]
(2) $T \vdash \mathsf{P}([gx{=}0]) \to \mathsf{P}([C])$, [(1), (P)*]
(3) $T \vdash [gx{=}0] = [gx{=}y]_y(0)$, [15.3b,c]
(4) $T \vdash gx = y \to \mathsf{P}([gx{=}y])$, [15.6]
(5) $T \vdash gx = 0 \to \mathsf{P}([C])$, [(2),(3),(4)]
(6) $T \vdash \exists x(gx = 0) \to \mathsf{P}(\ulcorner C \urcorner)$, [(5), $\vdash [C] = \ulcorner C \urcorner$]$\triangle$

Satz 15.8

Ist P eine 1-st. Σ_1-Formel, welche (P)* erfüllt, so gilt für alle geschlossenen Formeln A, B:

(D1) $T \vdash A \;\Rightarrow\; T \vdash \mathsf{P}(\ulcorner A \urcorner)$,
(D2) $T \vdash \mathsf{P}(\ulcorner A \to B \urcorner) \to \mathsf{P}(\ulcorner A \urcorner) \to \mathsf{P}(\ulcorner B \urcorner)$,
(D3) $T \vdash \mathsf{P}(\ulcorner A \urcorner) \to \mathsf{P}(\ulcorner \mathsf{P}(\ulcorner A \urcorner) \urcorner)$.

Beweis :

Offenbar ist jede geschlossene Formel A einfach, und es gilt $\mathrm{Z} \vdash [A] = \ulcorner A \urcorner$. (D1) und (D2) folgen deshalb unmittelbar aus (P)*. (D3) folgt aus 15.7 mit $C :\equiv \mathsf{P}(\ulcorner A \urcorner)$. $\triangle$

Satz 15.9 (Löb)
Ist P eine 1-st. Formel, welche (D1),(D2),(D3) erfüllt, so gilt für jeden Satz A:
$T \vdash \mathsf{P}(\ulcorner A \urcorner) \to A \implies T \vdash A$.
Insbesondere gilt: $T \vdash \neg\mathsf{P}(\ulcorner \bot \urcorner) \implies T \vdash \bot$.
Beweis :
Abkürzung: $\Box A :\equiv \mathsf{P}(\ulcorner A \urcorner)$.
Sei A ein $\mathcal{L}$-Satz mit $T \vdash \Box A \to A$. Nach dem Fixpunktlemma (Satz 5.8) existiert ein $\mathcal{L}$-Satz C mit $T \vdash C \leftrightarrow (\Box C \to A)$. Nun folgt:
(1) $T \vdash \Box C \to \Box\Box C \to \Box A$, [aus $\vdash C \to \Box C \to A$ mittels (D1),(D2)]
(2) $T \vdash \Box C \to \Box A$, [aus (1) und (D3) $\vdash \Box C \to \Box\Box C$]
(3) $T \vdash \Box C \to A$, [(2), $\vdash \Box A \to A$]
(4) $T \vdash C$, [aus (3) und $\vdash (\Box C \to A) \to C$]
(5) $T \vdash \Box C$, [(4),(D1)]
(6) $T \vdash A$. [(3),(5)]$\triangle$

Definition
Ist T primitiv rekursiv, so sei $Prov_T(x) :\equiv \exists y(Bew_T(x,y) = 0)$, $Con_T :\equiv \neg Prov_T(\ulcorner \bot \urcorner)$.
Dabei sei $Bew_T \in \mathrm{PR}^2$ das im Beweis von Satz 5.3 implizit definierte Funktionszeichen mit $Bew_T(a,b) = 0 \Leftrightarrow (a,b) \in \mathsf{Bew}_T$.

Satz 15.10 (2. Gödelscher Unvollständigkeitssatz)
Ist T ein primitiv rekursives, konsistentes Axiomensystem mit $Z \subseteq \{A : T \vdash A\}$, so gilt $T \nvdash Con_T$.
Beweis :
Nach 15.5, 15.8, 15.9 genügt es, (P1),(P2),(P3) mit $\mathsf{P} :\equiv Prov_T$ nachzuweisen.
zu (P1): Gilt $T \vdash A$, so ist $Prov_T(\ulcorner A \urcorner)$ ein wahrer Σ_1-Satz, und somit gilt nach 15.1 (Korollar c) $\mathrm{Z} \vdash Prov_T(\ulcorner A \urcorner)$.
zu (P2): Durch einfache Formalisierung erhält man $\mathrm{Z} \vdash Prov_T(\langle \hat{\to}, x, y\rangle) \to Prov_T(x) \to Prov_T(y)$.
Mit $[A \to B] \equiv \langle \hat{\to}, [A], [B]\rangle$ folgt daraus (P2).
zu (P3): Dies ergibt sich durch Formalisierung des folgenden "Beweises":
$T \vdash A \overset{2.4a}{\Longrightarrow} T \vdash \forall x A \overset{(\forall 1),(\mathrm{mp})}{\Longrightarrow} T \vdash A_x(\underline{n})$. $\triangle$

Verallgemeinerung des 2. Gödelschen Unvollständigkeitssatzes

Sei jetzt $\mathcal{L}^*$ eine *beliebige* (d.h. es muß nicht $\mathrm{PR} \subseteq \mathcal{L}^*$ sein) primitiv rekursiv repräsentierte Sprache. Wie in Abschnitt 5 wird jedem $\mathcal{L}^*$-Ausdruck E eine Gödelnummer $\ulcorner E \urcorner$ zugeordnet.
Sei ferner Σ ein primitiv rekursives Axiomensystem mit $\mathrm{L}(\Sigma) = \mathcal{L}^*$. Die PR-Formeln $Prov_\Sigma$ und Con_Σ seien entsprechend wie $Prov_T$ und Con_T gebildet.

Definition
Eine Interpretation von Z in Σ besteht aus einer 1-stelligen $\mathcal{L}^*$-Formel N und einer Abbildung $A \mapsto A^N$, die jeder PR-Formel A eine $\mathcal{L}^*$-Formel A^N zuordnet, so daß gilt:
– $\bot^N \equiv \bot$,
– $(A \to B)^N \equiv A^N \to B^N$,
– $(\forall x A)^N \equiv \forall x(N(x) \to A^N)$,
– $\mathrm{FV}(A^N) = \mathrm{FV}(A)$,
– $\mathrm{Z} \vdash A \Rightarrow \Sigma \vdash A^*$, wobei $A^* :\equiv N(x_1) \to \ldots \to N(x_n) \to A^N$ mit $\{x_1, \ldots, x_n\} = \mathrm{FV}(A)$.

Lemma 15.11
Ist $A \mapsto A^N$ eine Interpretation von Z in Σ, so gilt für jede PR-Formel A: $\Sigma \vdash A^* \Rightarrow \Sigma \vdash A_x(\underline{n})^*$.

Beweis :
Sei $\mathrm{FV}(A) = \{x, y\}$.
$\Sigma \vdash A^* \Rightarrow \Sigma \vdash N(y) \to N(x) \to A^N \Rightarrow \Sigma \vdash N(y) \to \forall x(N(x) \to A^N)$ (1).
$\mathrm{Z} \vdash \forall x A \to A_x(\underline{n}) \Rightarrow \Sigma \vdash (\forall x A \to A_x(\underline{n}))^* \Rightarrow$
$\Sigma \vdash N(y) \to \forall x(N(x) \to A^N) \to A_x(\underline{n})^N \overset{(1)}{\Rightarrow} \Sigma \vdash N(y) \to A_x(\underline{n})^N$, i.e. $\Sigma \vdash A_x(\underline{n})^*$. △

Definition
Eine Interpretation $A \mapsto A^N$ von Z in Σ heiße *streng*, wenn es ein $g \in \mathrm{PR}^1$ gibt, so daß gilt:
– $g(\ulcorner A \urcorner) = \ulcorner A^* \urcorner$, für jede PR-Formel A,
– $g(n) = 0$, falls n nicht Nummer einer PR-Formel ist,
– $\mathrm{Z} \vdash g([A \to B]) = \langle \hat{\to}, g([A]), g([B]) \rangle$, für alle einfachen PR-Formeln A, B,
– $\mathrm{Z} \vdash Prov_\Sigma(gz) \to Prov_\Sigma(g(\mathsf{Sub}\nu y \ulcorner x \urcorner z))$ [vergl. Lemma 15.11]

Satz 15.12 (Allgemeine Form des 2. Gödelschen Unvollständigkeitssatzes)
Ist Σ ein primitiv rekursives, konsistentes Axiomensystem und $A \mapsto A^N$ eine strenge Interpretation von Z in Σ, so gilt $\Sigma \nvdash (Con_\Sigma)^N$.
Beweis :
Sei $T := \{A : A \text{ ist PR-Satz } \& \ \Sigma \vdash A^N\}$ und $\mathsf{P} :\equiv Prov_\Sigma(gx)$.
(1) $T \vdash A$ & A ein PR-Satz $\Rightarrow \Sigma \vdash A^N$.
Beweis: Nach Voraussetzung gibt es $A_1, ..., A_n \in T$ mit $\vdash A_1 \to \ldots \to A_n \to A$.
Es folgt $\Sigma \vdash A_1^N \to \ldots \to A_n^N \to A^N$ und $\Sigma \vdash A_i^N$ $(i = 1, ..., n)$, also $\Sigma \vdash A^N$.
(2) T konsistent.
Beweis: $T \vdash \bot \overset{(1)}{\Rightarrow} \Sigma \vdash \bot^N$. $\bot^N \equiv \bot$.
(3) $\mathrm{Z} \subseteq T$.
Beweis: $A \in \mathrm{Z} \Rightarrow \Sigma \vdash A^N$ & A PR-Satz $\Rightarrow A \in T$.
(4) Für T und P gilt (P1),(P2),(P3).
Beweis:
(P1) Sei A PR-Formel, und $\forall A$ der Allabschluß von A.
$T \vdash A \Rightarrow T \vdash \forall A \overset{(1)}{\Rightarrow} \Sigma \vdash (\forall A)^N \Rightarrow \Sigma \vdash A^* \overset{15.1}{\Rightarrow} \mathrm{Z} \vdash Prov_\Sigma(g(\ulcorner A \urcorner)) \Rightarrow T \vdash \mathsf{P}(\ulcorner A \urcorner)$.
(P2) Seien A, B zwei einfache PR-Formeln. Es gilt $\mathrm{Z} \vdash Prov_\Sigma(\langle \hat{\to}, x, y \rangle) \to Prov_\Sigma(x) \to Prov_\Sigma(y)$.
Daraus folgt $\mathrm{Z} \vdash Prov_\Sigma(g([A \to B])) \to Prov_\Sigma(g([A])) \to Prov_\Sigma(g([B]))$.
(P3) klar.
Nach 15.5, 15.8, 15.9 haben wir nun $T \nvdash \neg\mathsf{P}(\ulcorner \bot \urcorner)$. Nach 15.1 gilt $\mathrm{Z} \vdash g(\ulcorner \bot \urcorner) = \ulcorner \bot \urcorner$ und somit
$T \nvdash \neg Prov_\Sigma(\ulcorner \bot \urcorner)$. Nach Definition von T gilt deshalb $\Sigma \nvdash (\neg Prov_\Sigma(\ulcorner \bot \urcorner))^N$. △

16 Logikprogrammierung (PROLOG)

I. HORNKLAUSELLOGIK

Sei $\mathcal{L}$ eine im folgenden feste Sprache 1. Stufe, die mindestens eine Konstante enthält.
SUB sei die Menge alle Substitutionen zu $\mathcal{L}$.
σ, θ, τ bezeichnen im folgenden stets Elemente von SUB.
Für quantorenfreie Ausdrücke E schreiben wir jetzt auch $\mathrm{var}(E)$ statt $\mathrm{FV}(E)$. Ferner schreiben wir $\mathrm{ran}(\sigma)$ statt $\mathrm{FV}(\sigma)$; also $\mathrm{ran}(\sigma) = \bigcup\{\mathrm{var}(x\sigma) : x \in \mathrm{dom}(\sigma)\}$.
Eine *Atom* ist eine $\mathcal{L}$-Primformel der Form $pt_1...t_n$ mit $p \in \mathcal{L}$. (Gleichungen und $\bot$ sind also keine Atome.)
A, B bezeichnen im folgenden stets Atome.
Geschlossene Terme bzw. Atome werden auch *Grundterme* bzw. *Grundatome* genannt.
$\mathcal{B}_\mathcal{L}$ sei die Menge aller $\mathcal{L}$-Grundatome *(Herbrand-Basis)*.
$U_\mathcal{L}$ sei die Menge aller $\mathcal{L}$-Grundterme *(Herbrand-Universum)*.
TER sei die Menge aller $\mathcal{L}$-Terme.
Eine *Klausel* (genauer *definite Hornklausel*) ist eine Formel der Form $B_0 \to \ldots \to B_{n-1} \to A$
(abgekürzt $(B_0, ..., B_{n-1} \to A)$).
Für jede Klausel C sei $\forall C := \forall x_1 ... \forall x_n\, C$ mit $\{x_1, ..., x_n\} = \mathrm{var}(C)$.
Ein *Programm* ist eine endliche Menge von Klauseln. Für jedes Programm P sei $\forall P := \{\forall C : C \in P\}$.
Statt "Modell von $\forall P$" sagen wir auch "Modell von P".
Eine $\mathcal{L}$-Struktur $\mathcal{M}$ heißt *Pseudo-Herbrand-Struktur*, falls gilt:
i) $|\mathcal{M}| \subseteq \mathrm{TER}$,
ii) $f^\mathcal{M}(t_1, ..., t_n) = ft_1...t_n$.
Eine Pseudo-Herbrand-Struktur $\mathcal{M}$ mit $|\mathcal{M}| = U_\mathcal{L}$ (Menge aller Grundterme) heißt *Herbrand-Struktur*.

Definition
Ist $\mathcal{M}$ eine Pseudo-Herbrand-Struktur, E ein $\mathcal{L}$-Ausdruck und $\sigma \in \mathsf{SUB}$ mit $\forall x \in \mathrm{FV}(E)(\sigma(x) \in |\mathcal{M}|)$, so sei $E^\mathcal{M}[\sigma] := E^\mathcal{M}[\xi]$, wobei ξ irgendeine $\mathcal{M}$-Belegung mit $\forall x \in \mathrm{FV}(E)(\xi(x) = \sigma(x))$ bezeichne.

Lemma 16.1
Für jede Pseudo-Herbrand-Struktur $\mathcal{M}$ gilt: $t^\mathcal{M}[\sigma] = t\sigma$, falls $\forall x \in \mathrm{var}(t)(\sigma(x) \in |\mathcal{M}|)$.
Beweis : $(ft)^\mathcal{M}[\sigma] = f^\mathcal{M}(t^\mathcal{M}[\sigma]) = f^\mathcal{M}(t\sigma) = f\, t\sigma = (ft)\sigma$. △

Sei P im folgenden ein festes Programm.

Definition
$P' := \{C\sigma : C \in P \,\&\, \sigma \in \mathsf{SUB}\}$,
$P^0 := \{C \in P' : C \text{ geschlossen}\}$.

Induktive Definition von $P \vdash^k_* A$ (R. Stärk)
$(B_0, ..., B_{n-1} \to A) \in P' \,\&\, \forall i < n(P \vdash^{k_i}_* B_i) \,\&\, k = k_0 + ... + k_{n-1} + 1 \implies P \vdash^k_* A$.
Sprechweise: $P \vdash^k_* A \Leftrightarrow A$ besitzt einen *(P-)Implikationsbaum* der Größe k.
Abkürzungen: $P \vdash_* A :\Leftrightarrow$ Es gibt ein $k \in \mathbb{N}$ mit $P \vdash^k_* A$.
$P \vdash_* A_0 \wedge \ldots \wedge A_n :\Leftrightarrow P \vdash_* A_0 \,\&\, \ldots \,\&\, P \vdash_* A_n$.

Definition
$\mathsf{T}_P : \mathrm{Pot}(\mathcal{B}_\mathcal{L}) \to \mathrm{Pot}(\mathcal{B}_\mathcal{L})$, $\mathsf{T}_P(X) := \{A : \exists (B_0, ..., B_{n-1} \to A) \in P^0 \forall i < n(B_i \in X)\}$

Definition (Die Modelle $\mathcal{M}$ und $\mathcal{M}_0$)
i) $|\mathcal{M}| :=$ TER (Menge aller $\mathcal{L}$-Terme),
ii) $f^{\mathcal{M}}(t_1, ..., t_n) = ft_1...t_n$,
iii) $p^{\mathcal{M}} := \{(t_1, ..., t_n) : P \vdash_* pt_1...t_n\}$, (für jedes n-st. Relationszeichen p).
$\mathcal{M}_0$ sei die Substruktur von $\mathcal{M}$ mit $|\mathcal{M}_0| := U_{\mathcal{L}}$ (Menge aller Grundterme).
Bemerkung: $\mathcal{M}_0$ ist das intendierte Modell von P.

Lemma 16.2
a) Für jeden quantorenfreien Ausdruck E und jede $\mathcal{M}_0$-Belegung ξ gilt: $E^{\mathcal{M}}[\xi] = E^{\mathcal{M}_0}[\xi]$.
b) Für jede geschlossene Formel $F = \forall \vec{x} D$ mit D quantorenfrei gilt: $\mathcal{M} \models F \Rightarrow \mathcal{M}_0 \models F$.
Beweis klar.

Satz 16.3
Für jedes Atom A sind die folgenden Aussagen äquivalent:
(i) $\forall P \models A$, (ii) $\mathcal{M} \models A[id]$, (iii) $P \vdash_* A$.
Beweis :
HS1: $\mathcal{M} \models A[\sigma] \Leftrightarrow P \vdash_* A\sigma$.
Beweis: $\mathcal{M} \models pt[\sigma] \Leftrightarrow t^{\mathcal{M}}[\sigma] \in p^{\mathcal{M}} \Leftrightarrow t\sigma \in p^{\mathcal{M}} \Leftrightarrow P \vdash_* pt\sigma$.
HS2 : $\mathcal{M} \models \forall P$.
Beweis: Sei $C = (B_0, ..., B_{n-1} \to A) \in P$. Zu zeigen: $\mathcal{M} \models \forall C$, d.h. $\mathcal{M} \models C[\sigma]$ für alle $\sigma \in \mathsf{SUB}$. Sei also $\sigma \in \mathsf{SUB}$ mit $\mathcal{M} \models B_i[\sigma]$ für $i < n$. Mit HS 1 folgt $P \vdash_* B_i\sigma$ für $i < n$, und daraus (wegen $C\sigma \in P'$) $P \vdash_* A\sigma$, d.h. (nach HS 1) $\mathcal{M} \models A[\sigma]$.
(i) $\Rightarrow$ (ii) folgt aus HS2. (ii) $\Rightarrow$ (iii) folgt aus HS 1.
(iii) $\Rightarrow$ (i): Wegen $\models \forall C \to C\sigma$, gilt $\forall P \models C'$ für jede Klausel $C' \in P'$. Durch Induktion nach k folgt nun in trivialer Weise: $P \vdash_*^k A \Rightarrow \forall P \models A$. △

Korollar
a) $\mathcal{M}_0$ ist Modell von P, und für geschlossenes A gilt: $\forall P \models A \Leftrightarrow \mathcal{M}_0 \models A \Leftrightarrow P \vdash_* A$.
b) Für jedes Modell $\mathcal{H}$ von P gilt: $A \in \mathcal{B}_{\mathcal{L}} \,\&\, \mathcal{M}_0 \models A \Rightarrow \mathcal{H} \models A$.
($\mathcal{M}_0$ ist *das minimale Herbrand-Modell von* P.)
c) Ist D eine Konjunktion von Atomen mit $\forall P \models \exists x_1 ... \exists x_n D$, so gibt es Terme $t_1, ..., t_n$ mit $\forall P \models D_{x_1,...,x_n}(t_1, ..., t_n)$ und $\mathrm{var}(t_1, ..., t_n) \subseteq \mathrm{FV}(\exists \vec{x} D)$.
Beweis von c) (für $n = 1$): Sei $D = A_0 \wedge \ldots \wedge A_m$. Aus der Voraussetzung folgt mit HS 2 $\mathcal{M} \models (\exists x D)[id]$, d.h. es gibt ein t mit $\mathcal{M} \models D[id_x^t]$. Mit HS 1 folgt nun $P \vdash_* D_x(t)$ und weiter (mit 16.3) $\forall P \models D_x(t)$. In t ersetzen wir jetzt jede nicht zu $\mathrm{FV}(\exists x D)$ gehörende Variable durch eine Konstante der Sprache $\mathcal{L}$; der so entstehende Terme sei t'. Offenbar gilt dann $\forall P \models D_x(t')$ und $\mathrm{var}(t') \subseteq \mathrm{FV}(\exists x D)$. △

Satz 16.4
$\{A \in \mathcal{B}_{\mathcal{L}} : \mathcal{M}_0 \models A\} = \bigcap\{X \subseteq \mathcal{B}_{\mathcal{L}} : \mathsf{T}_P(X) \subseteq X\}$ (= kleinster Fixpunkt von $\mathsf{T}_{\mathcal{P}}$).
Beweis :
Sei $X_0 := \{A \in \mathcal{B}_{\mathcal{L}} : P \vdash_* A\}$. Nach 16.3 gilt $X_0 = \{A \in \mathcal{B}_{\mathcal{L}} : \mathcal{M}_0 \models A\}$.
Durch Induktion nach k zeigt man: $P \vdash_*^k A \,\&\, A\sigma \in \mathcal{B}_{\mathcal{L}} \,\&\, \mathsf{T}_P(X) \subseteq X \Rightarrow A\sigma \in X$.
Daraus folgt: $X \subseteq \mathsf{T}_P(X) \Rightarrow X_0 \subseteq X$. Außerdem gilt offenbar $\mathsf{T}_P(X_0) \subseteq X_0$.
Also ist $X_0 = \bigcap\{X \subseteq \mathcal{B}_{\mathcal{L}} : \mathsf{T}_P(X) \subseteq X\}$. △

Berechnung der partiell-rekursiven Funktionen durch Logik-Programme

Wir machen jetzt folgende Annahmen über die Sprache $\mathcal{L}$:

1. $\mathbf{0}, \mathsf{S} \in \mathcal{L}$.
2. Jeder (Definition einer) n-st. part.-rek. Funktion f ist ein $(n{+}1)$-st. Relationszeichen $p_f \in \mathcal{L}$ zugeordnet.
3. Jedem n-stelligen $f = (\mu g)$ ist außerdem noch ein $(n{+}2)$-stelliges Relationszeichen $q_f \in \mathcal{L}$ zugeordnet.
4. Die Zuordnungen $f \mapsto p_f$ und $f \mapsto q_f$ sind injektiv, und die p_f's sind verschieden von den q_f's.

Satz 16.5

Zu jeder n-st. partiell-rekursiven Funktion f läßt sich ein Programm P_f angeben, so daß für alle $a_1, ..., a_n, b \in \mathbb{N}$ gilt: $f(a_1, ..., a_n) \simeq b \Leftrightarrow \forall P_f \models p_f \underline{a_1} ... \underline{a_n}\, \underline{b}$.

Beweis :

1. $f = \mathbf{0}^n$: $P_f := \{p_f x 0\}$.
2. $f = \mathsf{S}$: $P_f := \{p_f x \mathsf{S} x\}$.
3. $f = \mathsf{I}_i^n$: $P_f := \{p_f x_1 ... x_n x_i\}$.
4. $f = (\circ h g_1 ... g_m)$: $P_f := P_h \cup P_{g_1} \cup ... \cup P_{g_m} \cup \{p_{g_1}\vec{x}y_1 \to \ldots \to p_{g_m}\vec{x}y_m \to p_h\vec{y}z \to p_f\vec{x}z\}$.
5. $f = (\mathsf{R}gh)$: $P_f := P_g \cup P_h \cup \{p_g\vec{x}z \to p_f\vec{x}0z,\ p_f\vec{x}yw \to p_h\vec{x}ywz \to p_f\vec{x}\mathsf{S}y\,z\,\}$.
6. $f = (\mu g)$: $P_f := P_g \cup \{p_g\vec{x}y0 \to q_f\vec{x}y0,\ p_g\vec{x}y\mathsf{S}u \to q_f\vec{x}\mathsf{S}y\,z \to q_f\vec{x}y\mathsf{S}z,\ q_f\vec{x}0y \to p_f\vec{x}y\,\}$.

"$\Rightarrow$": Wir behandeln nur den Fall 6.

Sei $\tilde{f}(\vec{a}, c) :\simeq \mu y(g(\vec{a}, c+y) \simeq 0)$.

Wir zeigen durch Induktion nach b: $(*)\quad \tilde{f}(\vec{a}, c) \simeq b \Rightarrow \forall P_f \models q_f \underline{\vec{a}}\, \underline{c}\, \underline{b}$.

(i) $\tilde{f}(a, c) \simeq 0 \Rightarrow g(a, c) \simeq 0 \Rightarrow \forall P_f \models p_g \underline{a}\, \underline{c}\, 0 \Rightarrow \forall P_f \models q_f \underline{a}\, \underline{c}\, 0$.

(ii) $\tilde{f}(a, c) \simeq b+1 \Rightarrow g(a, c+b+1) \simeq 0 \,\&\, \forall i{<}b \exists k{>}0 (g(a, c+1+i) \simeq k) \,\&\, \exists m(g(a, c) \simeq m+1) \Rightarrow$
$\tilde{f}(a, c+1) \simeq b \,\&\, g(a, c) \simeq m+1$ für ein $m \Rightarrow \forall P_f \models p_g \underline{a}\, \underline{c}\, \mathsf{S}\underline{m} \,\&\, \forall P_f \models q_f \underline{a} \mathsf{S} \underline{c}\, \underline{b} \Rightarrow \forall P_f \models q_f \underline{a}\, \underline{c} \mathsf{S} \underline{b}$.

Mit $(*)$ folgt nun: $f(a) \simeq b \Rightarrow \tilde{f}(a, 0) \simeq b \Rightarrow \forall P \models q_f \underline{a} 0 \underline{b} \Rightarrow \forall P \models p_f \underline{a}\, \underline{b}$.

"$\Leftarrow$":

Wir ordnen jedem Prädikatszeichen p_f den Graph der Funktion f, sowie jedem Zeichen q_f den Graph der Funktion $\tilde{f}$ zu. Die Zeichen $\mathbf{0}$ und S werden wie üblich interpretiert. Dann ist $\mathbb{N}$ zusammen mit dieser Interpretation offenbar ein Modell von $\forall P_f$. $\triangle$

Korollar (Unentscheidbarkeit der Prädikatenlogik)

Sei K die rekursiv aufzählbare aber nicht rekursive Menge aus 14.4.

Sei ferner f die durch $f(a) \simeq b :\Leftrightarrow a \in K \,\&\, b = 0$ definierte partiell-rekursive Funktion. Dann ist $K = \{a \in \mathbb{N} : \forall P_f \models p_f \underline{a} 0\}$. Nach der Churchschen These gibt es also keinen Algorithmus, der für jede Formel D der Sprache von P_f entscheidet ob D allgemeingültig ist oder nicht.

II. UNIFIKATION

Definition (Komposition von Substitutionen)

Sind σ, τ Substitutionen, so bezeichne $(\sigma\tau)$ die durch $(\sigma\tau)(x) := (x\sigma)\tau$ bestimmte Substitution.

(Es gilt also $x(\sigma\tau) = (x\sigma)\tau$.)

Lemma 16.6

a) Für jeden quantorenfreien Ausdruck E gilt: $E(\sigma\tau) = (E\sigma)\tau$.

b) $((\sigma\tau)\rho) = (\sigma(\tau\rho))$.

Beweis :

a) $(pt)(\sigma\tau) = p\,t(\sigma\tau) \overset{\text{I.V.}}{=} p\,(t\sigma)\tau = (p(t\sigma))\tau = ((pt)\sigma)\tau$.

b) $x((\sigma\tau)\rho) = (x(\sigma\tau))\rho = ((x\sigma)\tau)\rho,\ \ x(\sigma(\tau\rho)) = (x\sigma)(\tau\rho) \overset{\text{a)}}{=} ((x\sigma)\tau)\rho$. $\triangle$

Aufgrund dieses Lemmas können wir im folgenden also einfach $E\sigma\tau$ bzw. $\sigma\tau\rho$ schreiben.

Definition

1. σ heißt *invertibel*, falls es ein τ mit $\tau\sigma = \sigma\tau = id$ gibt.
2. σ heißt *Variablensubstitution*, falls $x\sigma \in \mathrm{VAR}$ für alle x gilt.
3. Eine Variablensubstitution σ heißt *Permutation (von Variablen)*, falls $\sigma : \mathrm{VAR} \to \mathrm{VAR}$ bijektiv ist.

Bemerkung: Jede injektive Variablensubstitution ist eine Permutation.
Beweis: Sei σ eine injektive Variablensubstitution. Zu zeigen $\mathrm{VAR} \subseteq \{x\sigma : x \in \mathrm{VAR}\}$. Angenommen, es gäbe eine Variable $y \notin \{x\sigma : x \in \mathrm{VAR}\}$. Dann wäre $\{y, y\sigma, y\sigma\sigma, \ldots\}$ eine unendliche Teilmenge von $\mathrm{dom}(\sigma)$. *Widerspruch.*

Lemma 16.7

$\sigma\tau = id \Rightarrow \sigma, \tau$ sind Permutationen und $\tau = \sigma^{-1}$.

Beweis :

Wäre $x\sigma$ keine Variable, so könnte auch $x\sigma\tau$ keine Variable sein, im Widerspruch zu $\sigma\tau = id$. Also ist σ eine Variablensubstitution. σ ist auch injektiv, denn $(x\sigma = y\sigma \Rightarrow x = x\sigma\tau = y\sigma\tau = y)$. Somit ist σ eine Permutation. Mit $\sigma\tau = id$ folgt daraus, daß τ auch eine Variablensubstitution ist. Der Rest ist nun klar. $\triangle$

Folgerung

Eine Substitution σ ist genau dann invertibel, wenn sie eine Permutation ist.

Definition

τ heißt *allgemeiner* als σ (in Zeichen $\sigma \leq \tau$), falls es ein ρ mit $\sigma = \tau\rho$ gibt.
τ und σ heißen *äquivalent*, falls $\sigma \leq \tau$ und $\tau \leq \sigma$ gilt.

Lemma 16.8

Sind τ und σ äquivalente Substitutionen, so gibt es eine Permutation π mit $\sigma\pi = \tau$ und $\tau\pi^{-1} = \sigma$.

Beweis :

Sei $V := \mathrm{ran}(\sigma) \cup \{x : x \notin \mathrm{dom}(\sigma)\}$, und gelte $\sigma\rho = \tau$ und $\tau\rho' = \sigma$. Dann $\sigma\rho\rho' = \sigma$ und deshalb $x\rho\rho' = x$ für alle $x \in V$. Folglich muß auch $x\rho$ für jedes $x \in V$ eine Variable sein. Ferner ist $\rho|_V$ injektiv. Wie gleich gezeigt wird, existiert deshalb eine Permutation π mit $x\pi = x\rho$ für alle $x \in V$. Für dieses π gilt dann $\sigma\pi = \tau$. $[x \in \mathrm{dom}(\sigma) \Rightarrow x\sigma\pi = x\sigma\rho = x\tau;\ \ x \notin \mathrm{dom}(\sigma) \Rightarrow x\sigma\pi = x\pi = x\rho = x\sigma\rho = x\tau]$
Zur Definition von π: Sei $\mathrm{dom}(\rho) \cap V = \{x_1, ..., x_n\}$, wobei $x_1, ..., x_n$ paarweise verschieden und $\{x \in V : x\rho \notin V\} = \{x_1, ..., x_m\}$ mit $m \leq n$. Dann $\{x_{m+1}\rho, ..., x_n\rho\} \subseteq \{x_1, ..., x_n\}$.
Sei $\{y_1, ..., y_m\} := \{x_1, ..., x_n\} \setminus \{x_{m+1}\rho, ..., x_n\rho\}$.
Wir setzen $\pi(\rho x_i) := y_i$, für $1 \leq i \leq m$, $\quad \pi(x) := \rho(x)$, für $x \in V$, sowie $\pi(x) := x$ sonst. $\triangle$

Definition

Paare (t, t') (wobei t, t' $\mathcal{L}$-Terme sind) nennen wir im folgenden *Gleichungen*.
Sei $\mathcal{G}$ eine Menge von Gleichungen.
σ heißt *Unifikator* von $\mathcal{G}$ (oder σ *unifiziert* $\mathcal{G}$), falls $t\sigma = t'\sigma$ für jedes Paar $(t, t') \in \mathcal{G}$.
θ heißt *allgemeinster Unifikator* (mgu) von $\mathcal{G}$, falls θ Unifikator von $\mathcal{G}$ ist, und $\tau \leq \theta$ für jeden Unifikator τ von $\mathcal{G}$ gilt.

Die Martelli-Montanari-Regeln zur Berechnung von mgu's

Das Symbol + bezeichne hier die disjunkte Vereinigung.
(U1) $\mathcal{G} + \{(fs_1...s_n, ft_1...t_n)\} \to_M \mathcal{G} \cup \{(s_1, t_1), \ldots, (s_n, t_n)\}$.
(U2) $\mathcal{G} + \{(x, t)\} \to_M \mathcal{G}_x(t) \cup \{(x, t)\}$, falls $x \in \mathrm{var}(\mathcal{G}) \setminus \mathrm{var}(t)$.
(U3) $\mathcal{G} + \{(t, x)\} \to_M \mathcal{G} \cup \{(x, t)\}$, falls t keine Variable ist.
(U4) $\mathcal{G} + \{(x, x)\} \to_M \mathcal{G}$.

Lemma 16.9
a) $\mathcal{G} \to_M \mathcal{G}' \Rightarrow$ (σ unifiziert $\mathcal{G} \Leftrightarrow \sigma$ unifiziert $\mathcal{G}'$).
b) $\mathcal{G} \to_M \mathcal{G}' \Rightarrow$ (σ ist mgu von $\mathcal{G} \Leftrightarrow \sigma$ ist mgu von $\mathcal{G}'$).
Beweis :
a) (U1),(U3),(U4) sind klar.
(U2) Wegen $x \notin \mathrm{var}(t)$ ist $\tau := id_x^t$ offenbar ein mgu von $\{(x,t)\}$. Sei nun σ ein Unifikator von $\mathcal{G} + \{(x,t)\}$. Dann $\sigma = \tau\rho$. Da x nicht in t vorkommt, gilt $\tau\tau = \tau$, und es folgt $\sigma = \tau\rho = \tau\tau\rho = \tau\sigma$. Also gilt:
σ Unifikator von $\mathcal{G} + \{(x,t)\} \Leftrightarrow \tau\sigma$ Unifikator von $\mathcal{G}$ & $x\sigma = t\sigma \Leftrightarrow \sigma$ Unifikator von $\mathcal{G}_x(t) \cup \{(x,t)\}$. △

Lemma 16.10
Es gibt keine unendliche Folge von endlichen Gleichungsmengen $\mathcal{G}_n$ mit $\mathcal{G}_n \to_M \mathcal{G}_{n+1}$ für alle n.
Beweis :
Für jede endliche Gleichungsmenge $\mathcal{G}$ sei $\alpha(\mathcal{G}) := \omega^2 \cdot k + \omega \cdot m + n$, wobei
$k :=$ Kardinalität der Menge $\mathrm{var}(\mathcal{G}) \setminus \{x : \exists \mathcal{G}_0, t[\mathcal{G} = \mathcal{G}_0 + \{(x,t)\} \,\&\, x \notin \mathrm{var}(\mathcal{G}_0) \cup \mathrm{var}(t)\,]\}$,
$m :=$ "Länge" von $\mathcal{G}$,
$n :=$ Anzahl der Gleichungen (x,t) in $\mathcal{G}$, wo t keine Variable ist.
Wie man sich leicht überlegt, gilt: $\mathcal{G} \to_M \mathcal{G}' \Rightarrow \alpha(\mathcal{G}) > \alpha(\mathcal{G}')$. △

Lemma 16.11
Ist keine der Regeln (U1)–(U4) auf $\mathcal{G}$ anwendbar, so gilt:
Ist $\mathcal{G} = \{(x_1,t_1),...,(x_n,t_n)\}$, wobei die x_i's paarweise verschieden sind und nicht in $t_1...t_n$ vorkommen, so ist $\theta := id_{x_1,...,x_n}^{t_1,...,t_n}$ ein mgu von $\mathcal{G}$ mit $\theta\theta = \theta$.
Andernfalls ist $\mathcal{G}$ nicht unifizierbar.
Beweis :
Da nach Voraussetzung keine der Regeln (U1)–(U4) auf $\mathcal{G}$ anwendbar ist, muß einer der folgenden Fälle vorliegen:
1. $\mathcal{G}$ enthält eine Gleichung (x,t) mit $x \in \mathrm{var}(t)$ und $t \neq x$. Dann $x\sigma \neq t\sigma$, für alle σ.
2. $\mathcal{G}$ enthält eine Gleichung (s,t) mit $s,t \notin$ VAR. Wegen (U1) müssen s,t mit verschiedenen Funktionszeichen anfangen, also $s\sigma \neq t\sigma$, für alle σ.
3. $\mathcal{G} = \{(x_1,t_1),...,(x_n,t_n)\}$ mit $x_i \notin \mathrm{var}(t_i)$ für $i = 1,...,n$, und $(x_i,t_i) \neq (x_j,t_j)$ für $i \neq j$.
Wegen (U2) muß sogar gelten $x_i \notin \{x_j\} \cup \mathrm{var}(t_j)$ für $i \neq j$. Also sind $x_1,...,x_n$ paarweise verschieden und es gilt $\{x_1,...,x_n\} \cap \mathrm{var}(t_1...t_n) = \emptyset$; folglich ist $\theta := id_{x_1,...,x_n}^{t_1,...,t_n}$ ein Unifikator von $\mathcal{G}$.
Aus $x_i\sigma = t_i\sigma$ $(i = 1,...,n)$ folgt $x_i\theta\sigma = t_i\sigma = x_i\sigma$; und für $y \notin \{x_1,...,x_n\}$ gilt $y\theta\sigma = y\sigma$; also $\theta\sigma = \sigma$, d.h. θ ist mgu von $\mathcal{G}$. Aus $\{x_1,...,x_n\} \cap \mathrm{var}(t_1...t_n) = \emptyset$ folgt $\theta\theta = \theta$. △

RESULTAT:
Zu jeder unifizierbaren endlichen Gleichungsmenge $\mathcal{G}$ läßt sich mittels der Martelli-Montanari-Regeln ein mgu θ berechnen, für den außerdem gilt $\theta\theta = \theta$ und $\mathrm{dom}(\theta) \cup \mathrm{ran}(\theta) \subseteq \mathrm{var}(\mathcal{G})$.
(Beweis mittels 16.9, 16.10, 16.11 .)

III. SLD-RESOLUTION

Definitionen
Für quantorenfreie Formeln D, D' definieren wir: $D \approx D' :\Leftrightarrow$ es gibt eine Permutation τ mit $D' = D\tau$.
σ heißt Unifikator von (A,B), falls $A\sigma = B\sigma$.
$mgu(A,B) :=$ Menge aller mgu's von (A,B).
Ein *Ziel (goal)* ist eine endliche Folge von Atomen. Das leere Ziel bezeichnen wir mit $\square$.

Wir identifizieren jedes Ziel $(A_0, ..., A_{n-1})$ mit der Formel $(A_0 \to \ldots \to A_{n-1} \to \bot) \to \bot$, d.h. mit der Konjunktion $A_0 \wedge ... \wedge A_{n-1}$. (Das leere Ziel $\square$ entspricht dabei der Formel $\bot \to \bot$.)
F, G, Q seien Mitteilungszeichen für Ziele.
Δ sei Mitteilungszeichen für Paare von Zielen.
Ist $\Delta = (G, G')$, so sei $\quad \Delta[Q] := G * Q * G', \quad \Delta[B] := G * (B) * G', \quad \Delta[\,] := G * G'.$

Für $Q = (A_0, ..., A_{n-1})$ sei $Q \to B := (A_0, ..., A_{n-1} \to B)$.

$P(A) := \{Q \to B \in P : \exists \sigma, \tau (A\sigma = B\tau)\}$.

Ein *Baum* ist eine Funktion T deren Definitionsbereich $\mathrm{dom}(T)$ eine Menge von endlichen Folgen ist, für die gilt:
i) $\langle\rangle \in \mathrm{dom}(T)$,
ii) $\nu * \langle\iota\rangle \in \mathrm{dom}(T) \;\Rightarrow\; \nu \in \mathrm{dom}(T)$.

Abkürzung
$T^*(\nu) \mathrel{\widehat{=}} \langle a; \langle a_\iota\rangle_{\iota\in I}\rangle \;:\Leftrightarrow\; \nu \in \mathrm{dom}(T) \,\&\, T(\nu) = a \,\&\, I = \{\iota : \nu * \langle\iota\rangle \in \mathrm{dom}(T)\} \,\&\, \forall \iota \in I(\, T(\nu * \langle\iota\rangle) = a_\iota\,)$.

Definition
Ein *SLD-Baum für* G_0 ist ein Baum T mit $T(\langle\rangle) = (G_0, G_0)$,
so daß für jeden Knoten $\nu \in \mathrm{dom}(T)$ gilt:
i) ist $T(\nu) = (\square, F)$, so $\{\iota : \nu * \langle\iota\rangle \in \mathrm{dom}(T)\} = \emptyset$,
ii) ist $T(\nu) = (G, F)$ mit $G \neq \square$, so existieren Δ, B und eine Familie $(Q_\iota, A_\iota, \theta_\iota)_{\iota\in P(B)}$ mit
- $G = \Delta[B]$,
- $\iota \approx Q_\iota \to A_\iota \,\&\, \mathrm{var}(Q_\iota, A_\iota) \cap \mathrm{var}(G, F) = \emptyset \,\&\, \theta_\iota \in mgu(A_\iota, B)$, für alle $\iota \in P(B)$,
- $T^*(\nu) \mathrel{\widehat{=}} \langle (G, F); \langle (\Delta[Q_\iota]\theta_\iota, F\theta_\iota)\rangle_{\iota\in P(B)}\rangle$.

Bemerkung
Ist T ein SLD-Baum für G_0 und $(G, F) \in \mathrm{ran}(T)$, so ist F eine Instanz von G_0,
d.h. F ist von der Gestalt $G_0\theta$.

Satz 16.12 (Korrektheit der SLD-Resolution)
Ist T ein SLD-Baum für G_0, so gilt: $\;(\square, F) \in \mathrm{ran}(T) \;\Rightarrow\; \forall P \models F$.
Beweis :
HS: $T(\nu) = (G, F) \;\Rightarrow\; \forall P \models G \to F$.
Beweis durch Induktion nach der Länge von ν:
1. $G_0 \to G_0$: klar.
2. Gelte schon $\forall P \models G \to F$ und sei $G = \Delta[B]$, $Q \to A \approx \iota \in P(B)$, $A\theta = B\theta$.
Dann $\forall P \models G \to F \,\&\, \forall P \models Q\theta \to A\theta \,\&\, A\theta = B\theta$, und somit $\;\forall P \models \Delta[Q]\theta \to F\theta$.
Aus $(\square, F) \in \mathrm{ran}(T)$ folgt mit HS $\quad \forall P \models \square \to F$, d.h. $\forall P \models$F. $\qquad \triangle$

Definition
Für $Q = (A_0, ..., A_{n-1})$ sei: $P \vdash_*^k Q \;:\Leftrightarrow\; \exists k_0, ..., k_{n-1}(k = k_0 + ... + k_{n-1} \,\&\, \forall i < n(P \vdash_*^{k_i} A_i))$.

Lemma 16.13
Sei T ein SLD-Baum für G_0 und gelte $P \vdash_*^n G_0\sigma$. Dann existiert zu jedem $k \leq n$ ein Paar $(G, F) \in \mathrm{ran}(T)$ und eine Substitution ρ mit $P \vdash_*^{n-k} G\rho$ und $F\rho = G_0\sigma$.
Beweis :
(i) $k = 0$: trivial. $(G := F := G_0$ und $\rho := \sigma)$
(ii) Gelte $k < n \,\&\, T(\nu) = (G, F) \,\&\, P \vdash_*^{n-k} G\rho \,\&\, F\rho = G_0\sigma$.

Wegen $n-k>0$ ist $G \neq \square$. Wir haben also $T^*(\nu) \mathrel{\widehat{=}} \langle(\Delta[B], F); \langle(\Delta[Q_\iota]\theta_\iota, F\theta_\iota)\rangle_{\iota \in P(B)}\rangle$,
wobei $G = \Delta[B] \,\&\, \iota \approx Q_\iota \to A_\iota \,\&\, \mathrm{var}(Q_\iota, A_\iota) \cap \mathrm{var}(G, F) = \emptyset \,\&\, \theta_\iota \in mgu(A_\iota, B)$.
Aus $P \vdash_*^{n-k} \Delta[B]\rho$ folgt $P \vdash_*^{m+1} B\rho \,\&\, P \vdash_*^{n-k-m-1} \Delta[\,]\rho$ mit $0 \leq m < n-k$.
Somit existiert $Q \to B\rho \in P'$ mit $P \vdash_*^m Q$.
$Q \to B\rho$ ist Instanz eines $\iota \in P(B)$. (Dieses ι halten wir jetzt fest.)
Es gilt $T(\nu * \langle\iota\rangle) = (G', F')$ mit $G' := \Delta[Q_\iota]\theta_\iota,\ F' := F\theta_\iota$.
Ferner existiert ein τ mit $(Q_\iota \to A_\iota)\tau = Q \to B\rho$. O.E.d.A. $G\tau = G\rho \,\&\, F\tau = F\rho$.
Folglich $A_\iota\tau = B\tau$ und deshalb $\theta_\iota\rho' = \tau$ für ein ρ'. Es folgt weiter $G_0\sigma = F\rho = F\tau = F\theta_\iota\rho' = F'\rho'$ und
$P \vdash_*^{m+n-k-m-1} \Delta\rho[Q]$, i.e. $P \vdash_*^{n-(k+1)} \Delta[Q_\iota]\theta_\iota\rho'$, i.e. $P \vdash_*^{n-(k+1)} G'\rho'$. $\triangle$

Satz 16.14(Korrektheit und Vollständigkeit der SLD-Resolution)
Ist T ein beliebiger SLD-Baum für G_0, so gilt:
$\forall P \models G_0\sigma \ \Leftrightarrow\ \exists(\square, F) \in \mathrm{ran}(T) \exists\rho(\, G_0\sigma = F\rho\,)$.
Beweis :
"$\Leftarrow$": Satz 16.12 .
"$\Rightarrow$": Aus der $\forall P \models G_0\sigma$ folgt mit Satz 16.3 $P \vdash_*^n G_0\sigma$ für ein $n \in \mathbb{N}$. Nach Lemma 16.13 existiert
$(G, F) \in \mathrm{ran}(T)$ und ρ mit $F\rho = G_0\sigma$ und $P \vdash_*^0 G\rho$. Letzteres impliziert aber $G = \square$. $\triangle$