Mitschrift zur Vorlesung

Logik und Grundlagen der Mathematik

Nach einer Vorlesung von
Martin Goldstern
an der Technischen Universität Wien
im Wintersemester 2007/08

Moritz Gschwandtner

Dieses Dokument ist im Wintersemesters 2007/08 entstanden, und wird unter

http://dmg.tuwien.ac.at/goldstern/lgm

zur Verfügung gestellt.

Für das Finden von Fehlern bedanke ich mich bei Stefanie Hirsch und Benjamin Orth. Weiters möchte ich mich bei Herr Prof. Goldstern bedanken, der mir einige Fragen beantwortet und Unterlagen zur Verfügung gestellt hat.
Korrekturvorschläge und Anregungen bitte an e0125439@student.tuwien.ac.at bzw. an `martin.goldstern@tuwien.ac.at`

Inhaltsverzeichnis

1 Einleitung und Motivation

1.1 Das Cantor'sche Diagonalverfahren

Wir beginnen mit einem berühmten Satz.

Satz 1.1 (von Cantor)**.** *Es gibt keine Bijektion zwischen* $\mathbb{N}$ *und* $\mathbb{R}$*. Es gibt keine Bijektion zwischen* $\mathbb{N}$ *und* $\mathcal{P}(\mathbb{N})$*.*

Beweis. Wir zeigen: Jede beliebige Fkt. $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ ist nicht surjektiv.

Sei $f : \mathbb{N} \to P(\mathbb{N})$. Wir finden eine Menge $A_f \in \mathcal{P}(\mathbb{N})$, die nicht im Wertebereich von f liegt.

$$A_f := \{n \in \mathbb{N} : n \notin f(n)\}$$

Sei n_0 beliebig. Wir möchten $f(n_0) \neq A_f$ zeigen.

1. Fall: $n_0 \in f(n_0) \Rightarrow n_0 \notin A_f \Rightarrow f(n_0) \neq A_f$
2. Fall: $n_0 \notin f(n_0) \Rightarrow n_0 \in A_f \Rightarrow f(n_0) \neq A_f$

Damit ist der Beweis abgeschlossen. □

Beispiel (Diagonalisierung).

$$\begin{array}{rcl}
f(0) & = & \emptyset = \{\ _ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\ \} \\
f(1) & = & \mathbb{N} = \{\ 0,\ \underline{1},\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ \ldots\ \} \\
f(2) & = & \{\ \qquad\ \underline{2},\ 3,\ \qquad 5,\ \qquad\ 7,\ \qquad\ \ldots\ \} \\
f(3) & = & \{\ \qquad 1,\ \qquad\ _\ \ 4,\ \qquad\qquad\ 8,\ \ldots\ \} \\
\vdots & & \qquad\qquad\qquad\qquad\ \ddots \\
A_f & = & \{\ 0,\ \qquad\ 3,\ \ldots\ \qquad\qquad\qquad\qquad\ \}
\end{array}$$

1.2 Das Russell'sche Paradoxon

Wir betrachten die folgende Menge. Sei

$$R := \{A : A \notin A\}$$

1. Fall: $R \in R \Rightarrow R \notin R$
2. Fall: $R \notin R \Rightarrow R \in R$

Ohne jede Voraussetzung haben wir also einen Widerspruch hergeleitet. Der Fehler liegt in der Definition von R, diese ist unsinnig. („Russell'sches Paradoxon")

1.3 Das Richard'sche Paradoxon

Welche ist die größte Zahl, die man mit drei Buchstaben beschreiben kann? Die Beispiele „elf", „bin" (türk.: 1000), „MMM" (lat.: 3000) zeigen, dass es

offensichtlich auf die Sprache ankommt.

Sei $n_0 \in \mathbb{N}$ die kleinste Zahl, die nicht mit höchstens 10 000 ASCII-Buchstaben beschrieben werden kann. n_0 ist jedoch mit weniger als 10 000 Buchstaben beschreibbar (wie man hier sieht). („Richard-Paradoxon“)

Auch hier kommt es auf die Sprache an. Offenbar muss man zwischen mehreren Sprachebenen unterscheiden wie z.B. Objektsprache (Formeln, Variable) und Metasprache (diese ist eine Ebene höher, also die Sprache *über* die Objektsprache).

1.4 Induktion und Abschluss

Wir werden im Folgenden öfters in der Situation sein, dass wir von einer kleinen Menge von Objekten (Symbolen, Axiomen, etc.) ausgehen, und durch wiederholte Anwendung von Operationen (Zusammenfügen, Anwenden von Derivationsregeln) zu einer größeren Menge kommen.
Formal lässt sich dies so beschreiben: Sei S eine Menge, und F eine Funktion. Eine Teilmenge $A \subseteq S$ heißt abgeschlossen unter F, wenn für alle $a \in A$ auch $F(a) \in A$ gilt. Wir nennen $B \subseteq S$ den Abschluss unter F, wenn B die kleinste Obermenge von A ist, die unter F abgeschlossen ist. Dies bedeutet, dass jedes Element von B entweder selbst in A ist, oder durch wiederholte Anwendung von F auf ein Element in A entsteht. Äquivalent dazu könnte man den Abschluss B von A auch durch folgendes Induktionsprinzip definieren:

- Jedes Element von A ist in B
- B ist unter F abgeschlossen
- Für jede Eigenschaft E, die
  - allen Elementen von A zukommt
  - und sich von x auf $F(x)$ vererbt,

  gilt: Auch jedes Element von B hat die Eigenschaft E.

Diese Formulierung mag zwar komplizierter erscheinen als jene, in der wir von „wiederholter“ Anwendung von F sprechen; sie hat aber den Vorteil, bereits anwendbar zu sein, ohne dass wir uns über den Begriff „endlich“ Gedanken machen müssen.
Oft sind wir in folgender allgemeinerer Situation:

- Statt einer einstelligen Funktion F betrachten wir eine zweistellige Funktion $F : S \times S \to S$, oder (seltener) eine Funktion mit 3 oder mehr Argumenten.

- Statt einer totalen Funktion F betrachten wir eine Funktion, die nur partiell ist (also auf einer Teilmenge von S, $S \times S$, etc. definiert)
- Statt einer einzigen Funktion betrachten wir mehrere Funktionen F, G, ... (meist eine kleine Zahl solcher Funktionen, sagen wir 10).

Wenn nun F, G, ... eine Liste von solchen Funktionen ist (sagen wir, F sei einstellig und G dreistellig), dann heißt eine Menge $B \subseteq S$ *abgeschlossen unter F, G, ...*, wenn gilt:

1. Für alle $a \in B$: Wenn $F(a)$ definiert ist, dann ist $F(a) \in B$.
2. Für alle $a, b, c \in B$: Wenn $G(a, b, c)$ definiert ist, dann ist $G(a, b, c) \in B$.
3. etc. (für die anderen Funktionen unserer Liste)

Der Abschluss von A (unter F, G, ...) ist wiederum die kleinste Obermenge von A, die unter F, G, ... abgeschlossen ist. Diesen Abschluss von A kann man wiederum durch ein Induktionsprinzip charakterisieren:
Jede Eigenschaft E, die

- allen Elementen von A zukommt,
- und sich von x auf $F(x)$ (wann immer das definiert ist) vererbt,
- und sich von x, y, z auf $G(x, y, z)$ (wenn definiert) vererbt,
- etc., für die anderen Funktionen unserer Liste,

trifft auf alle Elemente des Abschlusses von A zu.

2 Aussagenlogik, Syntax und Semantik

In der Aussagenlogik beschäftigen wir uns mit dem „Wahrheitswert“ von Aussagen. In der klassischen Logik[1] lassen wir nur die Wahrheitswerte „wahr“ und „falsch“ zu, die wir meistens als die Zahlen 1 und 0 interpretieren.

2.1 Syntax

Vorweg einige Bezeichnungen:

- aussagenlogische Variable: p_1, p_2, p_3, ...
- Junktoren: $\wedge$, $\vee$, $\neg$, $\rightarrow$
- Formeln: $p_1 \wedge p_2$ heißt „Konjunktion“ von p_1 und p_2, $p_1 \vee p_2$ heißt „Disjunktion“ von p_1 und p_2. Weiters verwenden wir die „Implikation“ $p_2 \rightarrow p_1$ und die „Negation“ $\neg p_1$ sowie die Konstanten $\top$ (true) und $\bot$ (false)

Aussagenlogische *Formeln* sind induktiv definiert:

- Die Symbole $\top$ und $\bot$ sind aussagenlogische Formeln.
- Jede aussagenlogische Variable ist eine aussagenlogische Formel.
- Wenn A eine aussagenlogische Formel ist, dann ist auch $(\neg A)$ eine.
- Wenn A und B aussagenlogische Formeln sind, dann auch $(A \rightarrow B)$[2] $(A \vee B)$, $(A \wedge B)$.[4]
- Das sind alle.

Die Aussage „Das sind alle“ lässt sich so formalisieren: Entweder man interpretiert sie als das folgende „Induktionsprinzip“:

[1] Es gibt auch andere Logiken, wie zum Beispiel die „intuitionistische“ Logik, oder mehrwertige „fuzzy“ Logiken (Gödel-Logik, Łukasiewicz-Logik); diese können ebenso wie die klassische Logik mit mathematischen Mitteln untersucht werden, werden jedoch nur von wenigen Mathematikern als die der Mathematik zugrunde liegende Logik angesehen. In dieser Vorlesung werden sie nur in Fußnoten erwähnt.

[2] Der besseren Lesbarkeit lassen wir manche Klammern oft weg, wenn wir darauf vertrauen, dass der Leser[3] sie wieder richtig einfügen kann. Z.B. vereinbaren wir, dass „$\wedge$ und $\vee$ stärker als $\rightarrow$ binden“, und schreiben dann statt $(p_1 \rightarrow (p_2 \vee p_3))$ kürzer $p_1 \rightarrow p_2 \vee p_3$. Weiters vereinbaren wir, dass „Implikationen von rechts geklammert werden“: $A \rightarrow B \rightarrow C$ ist also als $(A \rightarrow (B \rightarrow C))$ zu lesen.
Achtung: Umgangssprachlich wird $A \rightarrow B \rightarrow C$ manchmal als $(A \rightarrow B) \wedge (B \rightarrow C)$ verstanden.

[3] Siehe Fußnote auf Seite 10

[4] Je nach Geschmack kann man auch noch die Formel $A \leftrightarrow B$ hinzunehmen, oder diese Formel als Abkürzung für $((A \rightarrow B) \wedge (B \rightarrow A))$ interpretieren.

> Jede Eigenschaft E, die allen Variablen und den Formeln $\top$ und $\bot$ zukommt, und die sich von Formeln A, B auf $(\neg A)$ und $A \vee B$, ..., vererbt, kommt allen Formeln zu.

oder man definiert:

> Eine Formel ist jeder String, der durch endlich viele Anwendungen von Konjunktion, Disjunktion etc. aus Aussagenvariablen und $\top$, $\bot$ entsteht.

oder man sagt:

> Die Menge der Formeln ist die kleinste Menge, die die Variablen sowie $\top$, $\bot$ enthält und die unter Konjunktion, etc. abgeschlossen ist.

Beachten Sie, dass wir hier die Junktoren $\wedge, \vee, \neg, \to$ bzw. die Begriffe „Konjunktion“, „Disjunktion“, „Negation“, „Implikation“ in zwei verschiedenen Rollen verwenden: erstens als einfaches Symbol, und zweitens als Funktion. Zum Beispiel ist $\wedge$ jene zweistellige Funktion, die zwei beliebigen Formeln (oder auch Zeichenfolgen („Strings“)) x und y die Formel (bzw. Zeichenfolge) $(x \wedge y)$ zuordnet. Zur deutlicheren Unterscheidung markieren wir manchmal das reine Symbol durch einen Punkt: $\dot\wedge$; die Funktion schreiben wir manchmal als $\wedge_{\text{Funktion}}$.

Eine dritte Rolle der Junktoren sind die einstellige Funktion $\neg_{\mathrm{B}}$ und die zweistelligen Funktionen $\wedge_{\mathrm{B}}$, $\vee_{\mathrm{B}}$, $\to_{\mathrm{B}}$ auf der zweielementigen Menge $\{1, 0\}$, sogenannte Boolesche Funktionen, die in den folgenden Tabellen definiert sind:

x	$\neg_{\mathrm{B}} x$
1	0
0	1

(x, y)	$x \wedge_{\mathrm{B}} y$	$x \vee_{\mathrm{B}} y$	$x \to_{\mathrm{B}} y$
$(1, 1)$	1	1	1
$(1, 0)$	0	1	0
$(0, 1)$	0	1	1
$(0, 0)$	0	0	1

Schreibweise 2.1. Sei $A \subseteq \{0, 1\}$. Mit $\bigwedge_{\mathrm{B}} A$ oder $\inf A$ bezeichnen wir das Infimum von A: $\bigwedge_{\mathrm{B}} A = 0$, wenn $0 \in A$, und $\bigwedge_{\mathrm{B}} A = 1$ sonst. (Insbesondere gilt $\bigwedge_{\mathrm{B}} A = 1$, wenn A die leere Menge ist.)
Mit dieser Schreibweise gilt für $x, y \in \{0, 1\}$: $x \wedge_{\mathrm{B}} y = \bigwedge_{\mathrm{B}} \{x, y\}$.
Analog definieren wir $\bigvee_{\mathrm{B}} A = \sup A$.

Bemerkung 2.1. Die Schreibweise ist nicht immer einheitlich. Statt $\wedge$ verwendet man oft auch &, statt $\to$ manchmal $\supset$, statt $\neg x$ auch $-x$, $\sim x$, x^c, x' oder $\bar{x}$; im Zusammenhang mit Booleschen Algebren schreibt man manchmal $+$ und $\cdot$ statt $\vee$ und $\wedge$. Für die Symbole $\top$ und $\bot$ gibt es noch viele andere Varianten — `true` bzw. `wahr` bzw. `verum` und `false`/`falsch`/`falsum`, `T` und `F` bzw. `W` und `F` bzw. `V` und `F`, 1 und 0, oder $\curlyvee$ und $\curlywedge$.
Auch für $\leftrightarrow$ und/oder $\Leftrightarrow$ (siehe 2.6 und 2.7) werden manchmal andere Symbole (wie z.B. $\equiv$ oder $\dot\leftrightarrow$) verwendet.

2.2 Semantik

Betrachten wir die folgende Formel: $(p_1 \to p_1) \wedge p_2$. Was ist die Bedeutung dieser Formel? Im Grunde kommt es auf den Wert von p_1 nicht an, daher ist die Formel äquivalent zu der einfachen Formel p_2.

Definition 2.2 (Belegung)**.** Eine Belegung einer Menge V von Variablen ist eine Abbildung $b : V \to \{1, 0\}$, die also jeder aussagenlogischen Variablen einen „Wahrheitswert“ zuweist.

Beispiel. $b(p_1) = 1 \quad b(p_2) = 0$

Belegungen können wir in sinnvoller Weise auf Formeln fortsetzen. Da wir 1 als „wahr“ und 0 als „falsch“ interpretieren, ist, ausgehend von der gerade definierten Belegung b, der einzige sinnvolle Wert für die Formel $p_1 \wedge p_2$ der Wert 0 (da die Konjunktion von „wahr“ und „falsch“ den Wert „falsch“ ergeben muss).

Definition 2.3 (Wahrheitsfunktion)**.** Sei V eine Menge von Variablen, $\mathcal{F}(V)$ die Menge aller Formeln, die nur Variable in V verwenden. Eine Funktion $w : \mathcal{F}(V) \to \{1, 0\}$ heißt *Wahrheitsfunktion*, wenn w ein Homomorphismus von der algebraischen Struktur

$$(\mathcal{F}(V), \wedge_{\text{Funktion}}, \vee_{\text{Funktion}}, \neg_{\text{Funktion}}, \to_{\text{Funktion}}, \bot, \top)$$

in die zweielementige boolesche Algebra

$$(\{1, 0\}, \wedge_{\text{B}}, \vee_{\text{B}}, \neg_{\text{B}}, \to_{\text{B}}, 0, 1)$$

ist.
Mit anderen Worten: w heißt Wahrheitsfunktion, wenn für alle Formeln φ, ψ die folgenden Eigenschaften gelten:

- $w((\varphi \wedge \psi)) = \begin{cases} 1 & \text{falls } w(\varphi) = w(\psi) = 1 \\ 0 & \text{sonst} \end{cases}$
- $w((\varphi \vee \psi)) = \begin{cases} 0 & \text{falls } w(\varphi) = w(\psi) = 0 \\ 1 & \text{sonst} \end{cases}$
- $w((\neg\varphi)) = \begin{cases} 0 & \text{falls } w(\varphi) = 1 \\ 1 & \text{sonst} \end{cases}$
- $w(\top) = 1$, $w(\bot) = 0$.

Von der Implikation fordern wir natürlich auch die entsprechende Verträglichkeit; deren Formulierung sei aber zur Übung dem Leser[5] überlassen.

[5] Der „Leser“ ist als generisches Maskulinum zu verstehen, d.h. es sind weibliche ebenso wie männliche Leser gemeint, sowie auch small furry creatures from Alpha Centauri.

Satz 2.4. *Sei b eine Belegung der Variablen in V. Dann gibt es eine eindeutig bestimmte Wahrheitsfunktion $\bar{b}$ mit Definitionsbereich $\mathcal{F}(V)$, die b fortsetzt.*

Beispiel. Sei b die durch

x	$b(x)$
p_1	0
p_2	1
p_3	1

definierte Belegung, und sei A die Formel $(p_1 \mathbin{\dot{\wedge}} (p_2 \mathbin{\dot{\vee}} \dot{\neg} p_2))$. Dann muss $\bar{b}$ die Bedingung

$$\bar{b}(p_1 \mathbin{\dot{\wedge}} (p_2 \mathbin{\dot{\vee}} \dot{\neg} p_2)) = \bar{b}(p_1) \wedge_{\mathrm{B}} \bar{b}(p_2 \mathbin{\dot{\vee}} \dot{\neg} p_2) = \big(b(p_1) \wedge_{\mathrm{B}} \ldots\big) = \big(0 \wedge_{\mathrm{B}} \ldots\big) = 0$$

erfüllen, also $\bar{b}(A) = 0$.

Satz 2.5. *Seien φ, ψ Formeln. Dann sind die folgenden Aussagen äquivalent:*

1. *Für jede Belegung b, die $\bar{b}(\varphi) = 1$ erfüllt, gilt auch $\bar{b}(\psi) = 1$.*
2. *Für jede Belegung b, die $\bar{b}(\psi) = 0$ erfüllt, gilt auch $\bar{b}(\varphi) = 0$.*
3. *$\bar{b}(\varphi) \leq \bar{b}(\psi)$ für alle Belegungen b. (Wobei $\leq$ die übliche Ordung zwischen 0 und 1 ist.)*
4. *Es gibt keine Belegung b, die $\bar{b}(\varphi) = 1$ und $\bar{b}(\psi) = 0$ erfüllt.*
5. *Es gibt keine Belegung b, die $\bar{b}(\varphi) = 1$ und $\bar{b}(\neg\psi) = 1$ erfüllt.*
6. *Für alle Belegungen b gilt $\bar{b}(\varphi \wedge \neg\psi) = 0$*
7. *Für alle Belegungen b gilt $\bar{b}(\varphi \to \psi) = 1$*

Definition 2.6. Seien φ und ψ aussagenlogische Formeln. Wir schreiben $\varphi \Rightarrow \psi$, wenn eine/alle der oben genannten Eigenschaften gelten.

Man beachte den Unterschied zwischen dem metasprachlichen Zeichen „$\Rightarrow$“ (welches eine Relation zwischen zwei Formeln beschreibt) und der Funktion $\to_{\text{Funktion}}$, welche zwei Formeln φ und ψ mit Hilfe des objektsprachlichen Zeichens „$\dot{\to}$“ zu einer neuen Formel zusammenfügt. „$\varphi \to \psi$“ ist eine Formel; „$\varphi \Rightarrow \psi$“ ist hingegen eine Aussage über zwei Formeln.

Definition 2.7 (Äquivalenz von Formeln)**.** Zwei Formeln φ, ψ heißen äquivalent (in Zeichen: $\varphi \Leftrightarrow \psi$), wenn sowohl $\varphi \Rightarrow \psi$ also auch $\psi \Rightarrow \varphi$ gilt, oder in anderen Worten, wenn für alle Belegungen b gilt $\bar{b}(\varphi) = \bar{b}(\psi)$.
Offensichtlich ist $\Leftrightarrow$ eine Äquivalenzrelation.

Beispiel. $p_1 \Leftrightarrow (p_1 \wedge p_1)$

Definition 2.8 (Bedeutung einer Formel)**.** Die *Bedeutung* einer Formel φ können wir auf verschiedene (aber im Wesentlichen äquivalente) Arten definieren:

- Entweder wir sagen, dass zwei Formeln φ, ψ dieselbe Bedeutung haben, wenn $\varphi \Leftrightarrow \psi$ gilt, und wir definieren die Bedeutung einer Formel φ als die Äquivalenzklasse von φ in Bezug auf die Relation „$\Leftrightarrow$“.

- Oder wir definieren die Bedeutung einer Formel φ als jene Funktion, die jeder Belegung b aller Variablen den Wert $\bar{b}(\varphi)$ zuordnet.
  (Diese Variante ist offensichtlich zur vorigen äquivalent, da ja die Relation „$\Leftrightarrow$“ via Belegungen definiert ist.)

- Oder wir beschränken uns auf eine fixe endliche Menge V von Variablen (z.B. $V = \{p_1, \ldots, p_n\}$) und betrachten nur jene Formeln, in denen nur Aussagenvariable aus V vorkommen; die Bedeutung jeder solchen Formel ist dann jene Funktion, die jeder Belegung $b : V \to \{0, 1\}$ den Wert $\bar{b}(\varphi) \in \{0, 1\}$ zuordnet.
  (Diese Variante scheint komplizierter als die vorige zu sein; sie ist aber erstens zur vorigen äquivalent, weil man zeigen kann, dass $\bar{b}(\varphi)$ nur von jenen Werten $b(p)$ abhängt, für die p in φ vorkommt; sie ist zweitens auch praktischer, weil man hier nur endlich viele Belegungen betrachten muss, und nicht überabzählbar viele wie in der vorigen Variante.)

Betrachten wir die Formel $p_1 \wedge p_2$. Die Bedeutung dieser Formel in Bezug auf die Variablen p_1, p_2 ist die gerade beschriebene Funktion $\wedge_{\mathrm{B}}$; die Bedeutung der gleichen Formel in Bezug auf die Variablen p_1, p_2, p_3 ist jedoch eine Funktion

$$h : \{1, 0\} \times \{1, 0\} \times \{1, 0\} \to \{1, 0\},$$

die $h(x, y, z) = x \wedge_{\mathrm{B}} y$ erfüllt. Diese hängt zwar nicht von der dritten Variablen ab, dennoch muss man unterscheiden, auf welches System von Variablen man sich bezieht.

Definition 2.9 (Tautologie)**.** Eine Formel φ heißt Tautologie, wenn für alle Belegungen b gilt: $\bar{b}(\varphi) = 1$

Beispiele. $p_1 \to p_1$, $\quad p_1 \to (p_1 \wedge p_1)$, $\quad p_1 \vee \neg p_1$

Bemerkung 2.10. Die folgenden Aussagen sind äquivalent:

1. φ ist Tautologie.
2. $\top \Rightarrow \varphi$.
3. $\neg\varphi \Rightarrow \varphi$.
4. $\psi \Rightarrow \varphi$ für jede Formel ψ; diese Aussage „φ folgt aus jeder Formel“ schreibt man manchmal auch $\Rightarrow\varphi$.

Ebenso sind die folgenden Aussagen äquivalent:

1. $\bar{b}(\varphi) = 0$ für alle Belegungen b.
2. $\varphi \Rightarrow \bot$.
3. $\varphi \Rightarrow \neg\varphi$.
4. $\varphi \Rightarrow \psi$ für jede Formel ψ; diese Aussage „aus φ folgt jede Formel“ schreibt man manchmal auch $\varphi\Rightarrow$.
5. $\neg\varphi$ ist Tautologie.

Definition 2.11 (Kontradiktion, Erfüllbarkeit)**.** Wir sagen, dass eine Belegung b eine Formel φ *erfüllt*, wenn $\bar{b}(\varphi) = 1$ gilt. Demnach heißt eine Formel φ erfüllbar, wenn es zumindest eine Belegung b gibt, die φ erfüllt.
Eine Formel φ heißt *Kontradiktion* (oder *unerfüllbar*), wenn es keine Belegung b gibt, die φ erfüllt, d.h. wenn für alle Belegungen b gilt: $\bar{b}(\varphi) = 0$, bzw. wenn $\neg\varphi$ eine Tautologie ist.
Wir sagen, dass eine Menge Σ von aussagenlogischen Formeln erfüllbar ist, wenn es eine Belegung b gibt, die $\bar{b}(\varphi) = 1$ für alle $\varphi \in \Sigma$ erfüllt.
Eine endliche Menge $\{\varphi_1, \ldots, \varphi_n\}$ ist offenbar genau dann erfüllbar, wenn die Konjunktion $\varphi_1 \wedge \cdots \wedge \varphi_n$ erfüllbar ist. (Für unendliche Mengen siehe 3.19.)

Grob gesprochen gibt es also 3 Arten[6] von aussagenlogischen Formeln:

- Tautologien (unter jeder Belegung wahr, wie z.B. $\top$, $p \to p$, $p \vee \neg p$, oder $(p \to q) \vee (q \to p)$)
- Kontradiktionen (unter jeder Belegung falsch, z.B. $\bot$, oder $p \wedge \neg p$)
- andere (z.B. p, oder $p \to q$)

Um festzustellen, ob eine Formel φ mit n aussagenlogischen Variablen eine Tautologie ist, könnten wir alle 2^n (relevanten) Belegungen ausprobieren. Da dies zu langwierig ist, muss man sich Methoden bedienen, die besser und schneller funktionieren.

Wenn wir zum Beispiel die Formel $(p \wedge (q \vee r \to s)) \to ((q \vee r \to s) \wedge p)$ betrachten, so müssten wir theoretisch 16 Belegungen b ausprobieren; wir sehen aber schnell, dass es nur auf die Werte von $b(p)$ und $\bar{b}(q \vee r \to s)$ ankommt. Genauer: Die vorliegende Formel hat die Struktur $(A \wedge B) \to (B \wedge A)$; wenn wir wissen, dass die Formel $(p_1 \wedge p_2) \to (p_2 \wedge p_1)$ eine Tautologie ist, muss auch die vorliegende (kompliziertere) Formel eine Tautologie sein.

[6] Mit Hilfe der Äquivalenzrelation $\Leftrightarrow$ kann man auch noch feiner unterscheiden; die Äquivalenzklassen dieser Relation bilden eine Boolesche Algebra, die „Lindenbaum-Algebra“; die Menge der Tautologien ist genau das Einselement dieser Algebra, die Menge der Kontradiktionen das Nullelement.

Allgemeiner kann man sich Folgendes überlegen:

Definition 2.12 (Formelhomomorphismus)**.** Eine Abbildung $f : \mathcal{F}(V) \to \mathcal{F}(V)$ mit den Eigenschaften

1. $f(\varphi \wedge \psi) = f(\varphi) \wedge f(\psi)$
2. $f(\varphi \vee \psi) = f(\varphi) \vee f(\psi)$
3. $f(\varphi \to \psi) = f(\varphi) \to f(\psi)$
4. $f(\neg\varphi)) = \neg f(\varphi)$
5. $f(\top) = \top$
6. $f(\bot) = \bot$

nennt man Formelhomomorphismus.

Bemerkung 2.13. Sei $g : V \to \mathcal{F}(V)$. Dann gibt es einen eindeutigen Formelhomomorphismus h, der g fortsetzt.

Beispiel. Betrachten wir die folgenden Formeln φ, ψ:

$$\varphi : p_1 \to p_1$$

$$\psi : (p_1 \wedge \neg p_2 \to p_3 \vee (p_1 \to p_2)) \to (p_1 \wedge \neg p_2 \to p_3 \vee (p_1 \to p_2))$$

Offensichtlich gibt es einen Formelhomomorphismus f mit $f(\varphi) = \psi$.

Satz 2.14. *Sei φ eine Tautologie und f ein Formelhomomorphismus, dann ist $f(\varphi)$ ebenfalls Tautologie.*

Beweis. Sei b eine Belegung. Zu zeigen ist $\bar{b}(f(\varphi)) = 1$. Wir definieren eine neue Belegung c durch $c(p) = \bar{b}(f(p))$ für alle (relevanten) aussagenlogischen Variablen p. Mit Induktion zeigt man nun leicht[7] $\bar{c} = \bar{b} \circ f$: Für aussagenlogische Variable p gilt $\bar{c}(p) = c(p) = \bar{b}(f(p))$ schon nach Definition von c; für den induktiven Schritt verwendet man die Homomorphieeigenschaft der Funktionen $\bar{b}$, $\bar{c}$ und f. Da φ eine Tautologie ist, gilt $\bar{c}(\varphi) = 1$, somit auch $\bar{b}(f(\varphi)) = 1$. □

[7] Eine genauere Überlegung, für welchen Definitionsbereich diese Gleichung gilt, bleibt dem Leser[8] überlassen.

[8] Siehe Fußnote auf Seite 10

3 Aussagenlogische Resolution

3.1 Konjunktive und disjunktive Normalform

Definition 3.1 (Literal)**.** Unter einem Literal versteht man eine aussagenlogische Variable, oder eine negierte aussagenlogische Variable.

Definition 3.2 (Klausel)**.** Eine Disjunktion (bzw. Konjunktion) von endlich vielen Literalen heißt Klausel (bzw. duale Klausel).

Beispiele. $p, \quad (p_1 \vee p_2)$

Bemerkung: Die leere Disjunktion setzen wir mit $\bot$ fest.

Bemerkung 3.3. Die Nomenklatur ist nicht ganz einheitlich. Auf Englisch heißt eine Disjunktion von Literalen *clause*; dies wird im Deutschen oft mit „Klause“ oder „Klausel“ übersetzt.

Definition 3.4 (Konjunktive Normalform)**.** Eine Formel φ ist in konjunktiver Normalform (KNF, manchmal auch CNF), wenn φ eine Konjunktion von Klauseln ist.

Beispiel. $p_1 \wedge (p_1 \vee \neg p_2) \wedge (p_2 \vee \neg p_3)$

Bemerkung: Die leere Konjunktion setzen wir mit $\top$ fest. (Anders als die leere Disjunktion kommt die leere Konjunktion im Zusammenhang mit Resolution aber so gut wie nie vor.)

Definition 3.5 (Disjunktive Normalform)**.** Eine Formel φ ist in disjunktiver Normalform (DNF), wenn φ eine Disjunktion von Konjunktionen von Literalen ist.

Beispiel. $p_1 \vee (p_1 \wedge \neg p_2)$

Satz 3.6. *Zu jeder Formel φ gibt es eine Formel φ^D in DNF mit $\varphi \Leftrightarrow \varphi^D$. Die Darstellung ist nicht eindeutig (außer man verlangt zusätzlich, dass jede Variable in jeder Klausel genau einmal vorkommt).*

Beispiel (als Beweisskizze)*.* Wir betrachten die Formel

$$\varphi : p_1 \wedge (p_2 \to (\neg p_1 \vee \neg p_3))$$

Für die Werte von p_1, p_2, p_3 gibt es acht verschiedene Belegungen b_1, …, b_8. Wir schreiben diese Belegungen in einer „Wahrheitstabelle“ an; in der i-ten Zeile wird in den ersten drei Spalten die Belegung b_i beschrieben, in den weiteren Spalten stehen ausgesuchte Werte von $\bar{b}_i$.

p_1	p_2	p_3	$\neg p_1 \vee \neg p_3$	$p_2 \rightarrow (\neg p_1 \vee \neg p_3)$	$p_1 \wedge (p_2 \rightarrow (\neg p_1 \vee \neg p_3))$
1	1	1	0	0	0
1	1	0	1	1	1
1	0	1	0	1	1
1	0	0	1	1	1
0	1	1	1	1	0
0	1	0	1	1	0
0	0	1	1	1	0
0	0	0	1	1	0

Nun kann man aus der ersten und letzten Spalte der Tabelle die DNF ablesen:

$$\varphi^D : (p_1 \wedge p_2 \wedge \neg p_3) \vee (p_1 \wedge \neg p_2 \wedge p_3) \vee (p_1 \wedge \neg p_2 \wedge \neg p_3)$$

Bemerkung 3.7. Der Name „Normalform“ ist ein wenig irreführend; zwar gibt es zu jeder Formel φ eine äquivalente Formel φ^D in disjunktiver Normalform; diese Formel φ^D ist aber nicht eindeutig festgelegt, d.h. es kann durchaus verschiedene Formeln in DNF geben, die zu einander äquivalent sind.

Satz 3.8 (Gesetze von De Morgan)**.**

1. $(\neg\varphi \wedge \neg\psi) \Leftrightarrow \neg(\varphi \vee \psi)$
2. $(\neg\varphi \vee \neg\psi) \Leftrightarrow \neg(\varphi \wedge \psi)$

Satz 3.9. *Zu jeder Formel φ gibt es eine Formel φ^K in KNF mit $\varphi \Leftrightarrow \varphi^K$.*

Beweis. Wir gehen von einer disjunktiven Normalform für $\neg\varphi$ aus, und transformieren diese in eine konjunktive Normalform für φ.
Sei $\psi := \neg\varphi$, und sei ψ^D eine DNF für ψ. Wegen $(\psi^D \Leftrightarrow \psi)$ gilt auch $\neg\psi \Leftrightarrow \neg\psi^D$, daher $\varphi \Leftrightarrow \neg\psi^D$. Es folgt

$$\psi^D = (\ldots \wedge \ldots) \vee (\ldots \wedge \ldots) \vee \ldots \vee (\ldots \wedge \ldots) \Rightarrow$$

$$\neg\psi^D = \neg((\ldots \wedge \ldots) \vee (\ldots \wedge \ldots) \vee \ldots \vee (\ldots \wedge \ldots)) \Rightarrow$$

$$\neg\psi^D = (\neg(\ldots \wedge \ldots) \wedge \neg(\ldots \wedge \ldots) \wedge \ldots \wedge \neg(\ldots \wedge \ldots)) \Rightarrow$$

$$\neg\psi^D = ((\neg\ldots \vee \neg\ldots) \wedge (\neg\ldots \vee \neg\ldots) \wedge \ldots \wedge (\neg\ldots \vee \neg\ldots)) =: \varphi^K$$

φ ist also äquivalent zu einer Konjunktion von Disjunktionen von (negierten) Literalen. Negierte Literale sind entweder von der Form $\neg p$ (diese sind wiederum Literale) oder von der Form $\neg(\neg p)$ (diese können durch p ersetzt werden, wobei sich die Bedeutung der Formel nicht ändert). □

Sei φ in DNF. Wie leicht kann man feststellen, ob φ Tautologie, erfüllbar oder gar unerfüllbar ist? Offenbar ist φ genau dann erfüllbar, wenn eine seiner dualen Klauseln erfüllbar ist oder wenn sie die leere duale Klausel enthält. Eine duale Klausel ist unerfüllbar genau dann, wenn mindestens eine Variable negiert und unnegiert vorkommt. Ob die Formel in DNF Tautologie ist, ist meist wesentlich schwerer festzustellen.

Sei φ nun in KNF. Nun ist φ Tautologie genau dann, wenn jede Klausel Tautologie ist, also genau dann, wenn jede Klausel zumindest eine Variable zusammen mit ihrer Negation enthält, oder wenn es gar keine Klauseln gibt. Ob φ erfüllbar ist, ist meist wesentlich schwerer festzustellen.

Bemerkung 3.10. Die Erzeugung einer zu einer vorgegebenen Formel äquivalenten KNF oder DNF kann theoretisch sehr lange dauern; z.B. muss der obige Algorithmus, der zu einer Formel, in der n Variable vorkommen, eine äquivalente Formel in KNF oder DNF liefert, alle 2^n Belegungen durchprobieren.
In der Praxis liegen jedoch die Formeln, deren Erfüllbarkeit man überprüfen möchte, oft entweder bereits in KNF vor, oder lassen sich rasch auf KNF transformieren, während eine Transformation auf DNF mit Hilfe der Distributivgesetze erstens exponentiell lange dauern würde und zweitens auch eine exponentiell lange DNF erzeugen würde.
(Analog ist es in der Praxis so, dass Formeln, deren Tautologieeigenschaft man überprüfen möchte, meist leicht in DNF transformiert werden können, nicht aber in KNF.)

3.2 Resolution

Wir kommen nun zum Resolutionsalgorithmus. Dieser stellt zu jeder Formel in KNF fest, ob sie erfüllbar oder Kontradiktion ist.
Da die Bedeutung einer Klausel $L_1 \vee L_2 \vee \cdots \vee L_k$ weder von der Reihenfolge noch von der Vielfachheit der vorkommenden Literale abhängt (z.B. ist die Klausel $q \vee \neg p \vee q$ äquivalent zu $\neg p \vee q$), erweist es sich als sinnvoll, Klauseln zu identifizieren, wenn sie dieselben Literale enthalten. Als praktische Notation verwenden wir die Mengenschreibweise, d.h. wir ersetzen jede Klausel durch die Menge der in ihr auftretenden Literale. (Zum Beispiel wird die Klausel $q \vee \neg p \vee q$ durch $\{q, \neg p, q\}$ ersetzt; letztere Menge ist aber gleich der Menge $\{\neg p, q\}$.)

Klauseln fassen wir also ab jetzt als Mengen auf. Für jede Belegung b und jede Klausel C gilt offenbar $\bar{b}(C) = 1$ genau dann, wenn es ein Literal $L \in C$ gibt mit $\bar{b}(L) = 1$. Jede Formel in KNF (also jede Konjunktion von Klauseln) fassen wir ebenfalls als Menge von Klauseln auf. Wenn M so eine Menge von Klauseln ist, dann gilt $\bar{b}(M) = 1$ genau dann, wenn *für alle* $C \in M$ die Beziehung $\bar{b}(C) = 1$ gilt; anders ausgedrückt: M ist genau dann erfüllbar,

wenn es zu jeder Klausel $C \in M$ ein Literal $L \in C$ gibt mit $\bar{b}(L) = 1$.

Bemerkung 3.11. Die leere Menge (geschrieben $\emptyset$ oder $\{\}$), aufgefasst als Klausel, entspricht der leeren Disjunktion, die definitionsgemäß die Formel $\bot$ ist. Diese Menge bzw. diese Klausel spielt im Resolutionsalgorithmus eine wichtige Rolle; erst ihr Auftauchen im Resolutionsalgorithmus schließt diesen ab.
Die leere Menge, aufgefasst als Menge von Klauseln, entspricht der leeren Konjunktion (also der Konjunktion von gar keiner Klausel); sie ist definitionsgemäß gleich der Formel $\top$. Um Missverständnisse zu vermeiden, werden wir im folgenden immer nur nichtleere Klauselmengen betrachten.

Der besseren Lesbarkeit halber werden wir in aufzählenden Beschreibungen von Klauseln die einzelnen Literale mit Beistrichen (Kommata) trennen, in Klauselmengen die einzelnen Klauseln mit Strichpunkten (Semikola).

Beispiel. $((p_1 \vee \neg p_2) \wedge (p_3 \vee p_1)) \mapsto \{\{p_1, \neg p_2\}; \{p_3, p_1\}\}$

Beispiel. Wir betrachten die Klauselmenge $\{\{p\}; \{\neg p, q\}\}$. Diese Menge entspricht der KNF-Formel $p \wedge (\neg p \vee q)$. Man beachte, dass jede Belegung, die sowohl p als auch $\neg p \vee q$ (und somit $p \to q$) wahr macht, auch q wahr macht.

Aus der Erfüllbarkeit von $\{\{p\}; \{\neg p, q\}\}$ konnten wir also auf die Erfüllbarkeit der erweiterte Klauselmenge $\{\{p\}; \{\neg p, q\}; \{q\}\}$ schließen. Dies bringt uns zur folgenden

Definition 3.12 (Resolvente)**.** Seien C und D Klauseln, sodass $p \in C$ und $\neg p \in D$. Dann bezeichnen wir die Menge

$$\mathrm{Res}_p(C, D) := (C \setminus \{p\}) \cup (D \setminus \{\neg p\})$$

als die *Resolvente* von C und D (entlang von p).

Hilfssatz 3.13. *Sei b eine Belegung, sodass $\bar{b}(p \vee L_1 \vee \ldots \vee L_k) = 1$ und $\bar{b}(\neg p \vee L_{k+1} \vee \ldots \vee L_l) = 1$ (wobei L_i Literale sind). Dann muss auch*

$$\bar{b}(L_1 \vee \ldots \vee L_l) = 1$$

gelten.

Wenn wir C und D für die Klauseln

$$\{p, L_1, \ldots, L_k\} \quad \textit{bzw.} \quad \{\neg p, L_{k+1}, \ldots, L_l\}$$

schreiben, so gilt: Wenn $\bar{b}(C) = \bar{b}(D) = 1$, dann gilt auch

$$\bar{b}(\mathrm{Res}_p(C, D)) = 1$$

Beweis. Wir unterscheiden 2 Fälle: Wenn $b(p) = 1$ ist, dann ist $\bar{b}(\neg p) = 0$, also muss es wegen $\bar{b}(D) = 1$ ein Element $L \in D \setminus \{\neg p\}$ mit $\bar{b}(L) = 1$ geben, daher ist $\bar{b}(C \setminus \{p\} \cup D \setminus \{\neg p\}) = 1$. Der zweite Fall $b(\neg p) = 1$ wird analog behandelt. □

Beispiel (Resolution).

$$\{\{p\}; \{\neg p, q\}; \{\neg q, r\}; \{\neg r\}\} \overset{Res}{\longmapsto}$$

$$\{\{p\}; \{\neg p, q\}; \{\neg q, r\}; \{\neg r\}; \{q\}\} \overset{Res}{\longmapsto}$$

$$\{\{p\}; \{\neg p, q\}; \{\neg q, r\}; \{\neg r\}; \{q\}; \{r\}\} \overset{Res}{\longmapsto}$$

$$\{\{p\}; \{\neg p, q\}; \{\neg q, r\}; \{\neg r\}; \{q\}; \{r\}; \{\}\}$$

Definition 3.14 (Abschluss unter Resolution)**.** Sei M Menge von Klauseln. Die Menge $\bar{M}$, die aus M durch wiederholte Anwendung von Resolution (entlang beliebiger Variablen) entsteht, bezeichnen wir als den Abschluss von M unter Resolution (oder gleichbedeutend: die kleinste Menge von Klauseln, die M enthält und unter Resolution abgeschlossen ist).

Satz 3.15. *Sei M eine nichtleere Menge von Klauseln. Wenn b eine Belegung ist, die M erfüllt, dann erfüllt b auch $\bar{M}$.*

Beweis. Der Hilfssatz 3.13 sagt gerade, dass sich die Eigenschaft „wird von b erfüllt“ von zwei Klauseln C, D auf ihre Resolvente vererbt. Das Induktionsprinzip (siehe Abschnitt 1.4) besagt also, dass alle Klauseln in $\bar{M}$ von b erfüllt werden, sobald nur alle Klauseln in M durch b erfüllt werden. □

3.3 Vollständigkeit der Resolution

Wir wollen nun zeigen, dass Resolution „vollständig“ ist, d.h., dass der Resolutionsalgorithmus ausreicht, um alle unerfüllbaren Klauselmengen zu erkennen.

Satz 3.16 (Resolution)**.** *Sei M eine nichtleere endliche Menge von Klauseln.*

1. *M ist erfüllbar $\Leftrightarrow$ $\bar{M}$ ist erfüllbar*
2. *$\bar{M}$ ist erfüllbar $\Leftrightarrow$ $\{\} \notin \bar{M}$*

Beweis (durch Induktion nach Anzahl n der Variablen).
Die erste Aussage folgt aus Satz 3.15.
Wir zeigen die zweite Aussage:

„$\Rightarrow$“: Dies ist ist äquivalent zum Schluss

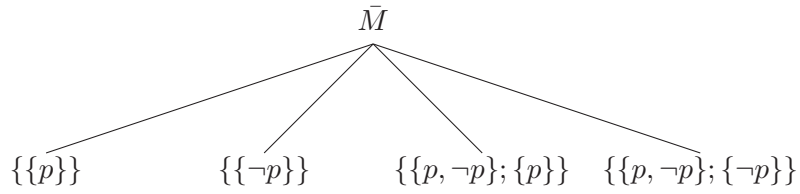
Wenn $\emptyset \in \bar{M}$, dann ist $\bar{M}$ unerfüllbar.

Letzteres folgt aus $\bar{b}(\{\}) = 0$ für alle Belegungen b.

„$\Leftarrow$“: Sei $\bar{M}$ eine Menge von Klauseln, die $\{\}$ nicht enthält und unter Resolution abgeschlossen ist. Gesucht ist eine Belegung, die $\bar{M}$ erfüllt.

- $n = 1$

  Da $\{\} \notin \bar{M}$ und $\bar{M}$ unter Resolution abgeschlossen ist, kann $\bar{M}$ nur eine der folgenden Gestalten besitzen:

  Man kann sich nun leicht überlegen, dass es in jedem Fall eine Belegung b gibt, die $\bar{M}$ erfüllt.

- $n \to n + 1$

  Sei nun $\bar{M}$ eine Klauselmenge, die die Variablen p, p_1, …, p_n verwendet.

  Wir werden die folgenden Hilfssätze verwenden:

  1. Wenn K unter Resolution abgeschlossen ist, und L ein Literal ist, dann sind auch die Mengen $\{C \in K : L \in C\}$ und $\{C \in K : L \notin C\}$ unter Resolution abgeschlossen.
  2. Wenn K unter Resolution abgeschlossen ist, und L ein Literal ist, dann ist auch $\{C \setminus \{L\} : C \in K\}$ unter Resolution abgeschlossen.

  Die Idee ist nun die folgende: Wenn $\{\neg p\}$ in $\bar{M}$ vorkommt, dann müssen wir natürlich $b(p) = 0$ setzen; danach entfernen wir alle Klauseln, die $\neg p$ enthalten (die sind ohnehin schon erfüllt) und entfernen p aus allen anderen Klauseln (denn das hilft uns ohnehin nicht bei der Erfüllbarkeit), und haben das Problem von $n + 1$ auf n reduziert.

  Wir wissen, dass $\{p\}$ und $\{\neg p\}$ nicht beide in $\bar{M}$ vorkommen können, da wegen des Abschlusses unter Resolution dann auch die leere Klausel in $\bar{M}$ sein müsste.
  Wir nehmen also oBdA an, die Klausel $\{p\}$ komme in $\bar{M}$ nicht vor. Dann definieren wir

  $$M' = \{C \in \bar{M} : \neg p \notin C\}, \qquad M'' = \{C \setminus \{p\} : C \in M'\}$$

  Nach den obigen Hilfssätzen sind M' und M'' unter Resolution abgeschlossen. Die leere Klausel kann weder in M' noch in M'' vorkommen.

(Das wäre nämlich nur dann möglich, wenn $\{\} \in \bar{M}$ oder $\{p\} \in \bar{M}$.)

In M'' kommt die Variable p nicht mehr vor (d.h. weder das Literal p noch das Literal $\neg p$ kommt in den Klauseln in M'' vor), also können wir die Induktionsvoraussetzung anwenden und eine Belegung b'' finden, die alle Klauseln in M'' erfüllt. Wir setzen b'' zu einer Belegung b fort, die $b(p) = 0$ erfüllt.

Nun muss b alle Klauseln in $\bar{M}$ erfüllen. Für Klauseln, die das Literal $\neg p$ enthalten, ist dies wegen $b(p) = 0$ klar. Sei nun C eine Klausel, die $\neg p$ nicht enthält, also $C \in M'$. Dann kommt $C \setminus \{p\}$ in M'' vor, wird also durch b'' erfüllt, erst recht also durch b.

□

Um also festzustellen, ob φ Tautologie ist, schreiben wir $\neg\varphi$ in KNF als Menge von Klauseln und wenden den Resolutionsalgorithmus an. Wenn die leere Klausel entsteht, ist $\neg\varphi$ unerfüllbar, d.h. φ ist Tautologie.

Beispiel. Wir wollen überprüfen, ob

$$\varphi : (\neg p \to \neg q) \to (q \to p)$$

eine Tautologie ist. Wir betrachten zunächst die Negation der Formel und formen diese (mittels $\neg(p \to q) \Leftrightarrow (p \wedge \neg q)$ sowie $(p \to q) \Leftrightarrow (\neg p \vee q)$) auf eine äquivalente Formel in KNF um:

$$\neg\varphi = (\neg p \to \neg q) \wedge \neg(q \to p) \Leftrightarrow$$

$$\Leftrightarrow (p \vee \neg q) \wedge (q) \wedge (\neg p)$$

Nun schreiben wir die Formel in Mengenschreibweise und wenden Resolution an:

$$M = \{\{p, \neg q\}; \{q\}; \{\neg p\}\} \overset{Res}{\longmapsto}$$

$$\{\{p, \neg q\}; \{q\}; \{\neg p\}; \{p\}\} \overset{Res}{\longmapsto}$$

$$\{\{p, \neg q\}; \{q\}; \{\neg p\}; \{p\}; \{\}\} \subseteq \bar{M}$$

$\bar{M}$ enthält die leere Klausel, daher ist φ Tautologie.

Bemerkung 3.17. Im Beweis des Satzes 3.16 haben wir also gezeigt, dass die Äquivalenz

„M unerfüllbar“ $\Leftrightarrow$ „$\emptyset$ ist mit Resolution aus M erzeugbar“

immer dann gilt, wenn M endlich ist, und sogar dann, wenn M unendlich ist, solange in M nur endlich viele Variable vorkommen. Dieser Beweis reicht noch nicht aus, um obige Äquivalenz auch für beliebige unendliche Mengen M schließen zu können. (Der Leser[9] möge sich selbst ein Beispiel einer Eigenschaft X konstruieren, sodass die Äquivalenz

[9]Siehe Fußnote auf Seite 10

„M ist X“ $\Leftrightarrow$ „$\emptyset$ ist mit Resolution aus M erzeugbar“

zwar für alle endlichen Klauselmengen M, nicht aber für unendliche Klauselmengen M gilt.)

Tatsächlich gilt aber doch der folgende Satz:

Satz 3.18. *Sei M eine beliebige (nicht notwendigerweise endliche) nichtleere Menge von Klauseln, und sei $\bar{M}$ der Abschluss von M unter Resolution. Dann sind die folgenden Aussagen äquivalent:*

1. *M ist unerfüllbar.*
2. *Es gibt eine endliche nichtleere Teilmenge $M_0 \subseteq M$, die unerfüllbar ist.*
3. *Es gibt eine endliche nichtleere Teilmenge von M, deren Abschluss (unter Resolution) die leere Menge enthält.*

3' *Es gibt eine endliche nichtleere Teilmenge von M, aus der man mit endlich vielen Resolutionsschritten die leere Menge erhalten kann.*

4. *$\bar{M}$ enthält die leere Menge.*
5. *$\bar{M}$ ist unerfüllbar.*

Beweis. Die Implikation 2 $\Rightarrow$ 3 ist gerade der Satz 3.16.
Die Bedingung 3 ist offensichtlich zu 3' äquivalent.
Die Implikation 3' $\Rightarrow$ 4 ist klar.
Die Implikation 4 $\Rightarrow$ 5 folgt wie die leichte Richtung von 3.16 aus der Tatsache, dass $\bar{b}(\emptyset) = 0$ für alle Belegungen b gilt.
5 $\Rightarrow$ 1 ist Satz 3.15.
Zu zeigen ist noch 1 $\Rightarrow$ 2:

- Ein Beweis dieser Implikation wird in den Angaben zur Übung skizziert.
- Ein weiterer Beweis wurde in den Übungen selbst vorgeführt: Die Menge $\mathfrak{B}$ aller Belegungen kann man als topologischen Raum auffassen, und zwar als Produktraum des kompakten diskreten Raums $\{0, 1\}$. Daher ist $\mathfrak{B}$ selbst kompakt, nach dem Satz von Tychonoff. Zu jeder Klausel $C \in M$ betrachten wir die Menge $[C]$ aller Belegungen b, die C erfüllen. $[C]$ ist abgeschlossen (wie man leicht nachprüft). Wenn nun M nicht erfüllbar wäre, wäre $\bigcap_{C \in M} [C] = \emptyset$, somit könnte $\{[C] : C \in M\}$ nicht die endliche Durchschnittseigenschaft haben; daraus gewinnt man leicht eine endliche unerfüllbare Teilmenge von M.
- Schließlich kann man die Implikation 1 $\Rightarrow$ 2 auch als Korollar des Kompaktheitssatzes der Prädikatenlogik (siehe 8.34) erhalten.

□

Die folgenden Aussage nennt man auch „Kompaktheitssatz der Aussagenlogik“.

Korollar 3.19. Sei Σ eine Menge von aussagenlogischen Formeln. Dann ist Σ genau dann erfüllbar, wenn jede endliche Teilmenge von Σ erfüllbar ist.

Beweis. Wir können den Beweis dieses Satzes entweder genauso wie den Beweis von $1 \Rightarrow 2$ in 3.18 führen, oder wir können diesen Satz auf folgende Weise als Korollar von 3.18 erhalten:
Wir ersetzen jede Formel $\varphi \in \Sigma$ durch eine äquivalente Klauselmenge M_φ, und betrachten die Vereinigung M aller dieser Klauselmengen:

$$M := \bigcup_{\varphi \in \Sigma} M_\varphi.$$

Dann überlegt man, dass die Belegungen, die M erfüllen, genau jene sind, die Σ erfüllen, und dass jede endliche Teilmenge von M aus einer endlichen Teilmenge von Σ entstanden ist. Daher sind die folgenden Aussagen äquivalent:

1. Σ ist erfüllbar.
2. M ist erfüllbar.
3. Jede endliche Teilmenge von M ist erfüllbar.
4. Jede endliche Teilmenge von Σ ist erfüllbar.

□

4 Prädikatenlogik, Syntax und Semantik

4.1 Syntax

Wir beginnen mit einem Beispiel für eine prädikatenlogische Formel:

$$\forall \epsilon > 0 \;\; \exists \delta > 0 \;\; \forall x \;\; \forall y \;\; (d(x,y) < \delta \rightarrow d(f(x), f(y)) < \epsilon)$$

Man könnte diese Formel auch folgendermaßen schreiben:

$$\forall \epsilon \;\; (\epsilon > 0 \rightarrow \exists \delta \;\; (\delta > 0 \wedge (\ldots)))$$

Weitere Möglichkeiten der Darstellung von Formeln sind

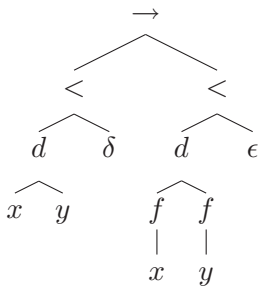
- das Baumdiagramm,
- die Präfixnotation (auch „polnische Notation“)
- und die Postfixnotation (auch UPN oder RPN wie „umgekehrte polnische Notation“, „reverse Polish notation“).

Ein Vorteil von Baumdiagrammen besteht darin, dass man die Struktur einer Formel aus einem Baumdiagramm besser als aus einer linearen Schreibweise ablesen kann.

Beispiel (Baumdiagramm). Die Formel

$$d(x,y) < \delta \rightarrow d(f(x), f(y)) < \epsilon$$

kann man in einem Baumdiagramm folgendermaßen darstellen:



Die Präfixnotation erhält man aus dem Baumdiagramm, indem man zunächst die Wurzel anschreibt, und dann (rekursiv) den linken und den rechten Teilbaum in Präfixnotation darstellt:

$$\rightarrow \left[< \left(d[x,y], \delta \right) \; , < \left(d[f(x), f(y)], \epsilon \right) \right].$$

Man kann sich überlegen, dass die Präfixnotation (anders als die Infixnotation) ganz ohne Klammern auskommt, wenn nur die Stelligkeiten der Funktions- und Relationssymbole bekannt sind: Aus dem String

$$\rightarrow < dxy\delta < dfxfy\epsilon$$

lässt sich das Baumdiagramm eindeutig rekonstruieren. Die Postfixnotation erhält man aus dem Baumdiagramm, indem man zuerst (rekursiv) den linken und den rechten Teilbaum in Postfixnotation darstellt und dann die Wurzel anschreibt. Sie kommt auch ohne Klammern aus:

$$xyd\delta{<}xfyfd\epsilon{<}{\rightarrow}.$$

Die Infixnotation erhält man aus dem Baumdiagramm, indem man zuerst (rekursiv) den linken Teilbaum darstellt, dann die Wurzel anschreibt, dann den rechten Teilbaum.

Zunächst wollen wir folgende prädikatenlogische Bezeichnungen festsetzen:

- $\mathscr{L}\ldots$ prädikatenlogische Sprache
- $x, y, z\ldots$ Variable
- $c, d\ldots$ Konstante
- $f(\cdot), d(\cdot,\cdot)\ldots$ Funktionssymbole (mit Stelligkeit)
- $R(\cdot,\cdot), <, =\ldots$ Relationssymbole (mit Stelligkeit)

Mit Hilfe dieser Bezeichnungen gelangt man zur folgenden

Definition 4.1 (Term)**.** Als Terme bezeichnet man alle Variablen und Konstanten. Sind weiters $t_1, \ldots, t_k$ Terme und f ein k-stelliges Funktionssymbol, dann ist auch $f(t_1, \ldots, t_k)$ ein Term.
Dies sind alle Terme.

Beispiel. 3+4

Es ist manchmal üblich und praktisch, gewisse Variable (z.B. x, y, z) immer nur für gebundene Variable zu verwenden, und gewisse andere (u, v, w) nur für freie Variable (das heißt: Variable, die nicht an Quantoren gebunden sind). Wir lassen alle Variable sowohl als freie als auch als gebundene zu.

Definition 4.2 (Formel)**.** Sind $t_1, \ldots, t_k$ Terme, und R ein k-stelliges Relationssymbol, dann ist $R(t_1, \ldots, t_k)$ eine *Atomformel*. Insbesondere ist $t_1 = t_2$ Atomformel.
Unter einer Formel versteht man

1. jede Atomformel,
2. jeden Ausdruck der Form $(\varphi \wedge \psi)$, wann immer φ und ψ Formeln sind
3. analog Ausdrücke der Form $(\varphi \vee \psi)$, $(\varphi \rightarrow \psi)$, $(\neg\varphi)$, sowie $\top$ und $\bot$,

4. sowie Ausdrücke der Form $\forall x\, \varphi$ und $\exists x\, \varphi$, wann immer φ eine Formel ist. Um die Rolle der Variablen x in der Formel φ hervorzuheben, schreiben wir manchmal $\varphi(x)$ statt φ, und $\forall x\, \varphi(x)$ statt $\forall x\, \varphi$.

   Diese Schreibweise erlaubt eine einfache Umbenennung von Variablen. Wenn wir eine Formel mit $\varphi(x)$ bezeichnen, dann meinen wir mit $\varphi(y)$ jene Formel, die aus $\varphi(x)$ entsteht, indem wir alle ungebundenen[10] Vorkommnisse von x durch y ersetzen.

Die Terme und Formeln haben also wiederum eine induktive Struktur; sie entstehen aus den Atomformeln durch die „Abschlussoperationen“ $(A, B) \mapsto (A \vee B)$, etc. Dies wird durch den folgenden Satz unterstrichen, den man auch als Teil der Definition von Term/Formel sehen kann.

Satz 4.3. *Sei E eine Eigenschaft, die*

1. *allen Variablen zukommt;*
2. *allen Konstantensymbolen zukommt;*
3. *sich von Termen $t_1, \ldots, t_k$ auf den Term $f(t_1, \ldots, t_k)$ (für alle Funktionssymbole f) vererbt.*

Dann haben alle Terme die Eigenschaft E.
Analog: Sei E eine Eigenschaft, die

1. *allen Atomformeln zukommt;*
2. *sich von Formeln φ, ψ auf $(\varphi \wedge \psi)$, etc. vererbt;*
3. *sich von Formeln $\varphi(x)$ auf $\forall x\, \varphi(x)$ und $\exists x\, \varphi(x)$ vererbt.*

Dann haben alle Formeln die Eigenschaft E.

Beispiel. $E :=$ „hat genau so viele öffnende wie schließende Klammern“

Definition 4.4. Zur Vereinfachung der Schreibweise vereinbaren wir weiterhin, dass $\wedge$ und $\vee$ stärker binden als $\rightarrow$ und $\leftrightarrow$; weiters[11] sollen Quantoren noch stärker binden als Junktoren. Die Formel $\forall x\, A \vee B \rightarrow C$ ist also als $((\forall x\, A) \vee B) \rightarrow C$ zu lesen, und die Formel $\exists x\, P(x) \rightarrow P(y)$ als $(\exists x\, P(x)) \rightarrow P(y)$.

[10] Wir werden nur ganz selten Formeln betrachten, in denen dieselbe Variable sowohl frei als auch gebunden vorkommt.

[11] Achtung! Nicht alle Bücher verwenden diese Konvention.

4.2 Modelle

Wir betrachten die folgenden Formeln:

$$\varphi_1 : \forall x\ \exists y\,(x = y)$$

$$\varphi_2 : \forall x\ \exists y\,(x \neq y)$$

$$\varphi_3 : \exists y\,(x \neq y)$$

Die Frage, ob diese Formeln wahr sind, können wir nur im Bezug auf ein „Modell“ beantworten:

Definition 4.5 ($\mathscr{L}$-Struktur, Modell)**.** Sei $\mathscr{L}$ eine prädikatenlogische Sprache. Eine $\mathscr{L}$-Struktur (auch: Modell) $\mathfrak{M} := (M, I)$ besteht aus

- einem Universum $M \neq \emptyset$
- und einer Interpretation I; I ist eine Funktion, die ...
  - ... jeder Konstanten $c \in \mathscr{L}$ ein Objekt $I(c) \in M$ zuordnet;
  - ... jedem k-stelligen Funktionssymbol f eine k-stellige Funktion (oder „Operation“) $I(f) : M^k \to M$ zuordnet;
  - ... jedem k-stelligen Relationssymbol R eine Menge $I(R) \subseteq M^k$ zuordnet.

  Statt $I(c)$, $I(f)$, $I(R)$ schreiben wir meist $c^{\mathfrak{M}}$, $f^{\mathfrak{M}}$, $R^{\mathfrak{M}}$.

Sprechweise: Modell, Struktur.

Bemerkung 4.6. Für das zweistellige Symbol $=$ verlangen wir immer, dass es durch die tatsächliche Gleichheit interpretiert wird,
d.h. $I(=) = \{(m, m) : m \in M\}$.

Um die Notation zu vereinfachen, lässt man in der Definition einer konkreten Interpretation I die Definition von $I(=)$ oft weg (da sie sich ohnehin zwingend aus der Wahl von M ergibt). Weiters schreiben wir ein Modell nicht als Paar (M, I) an, sondern wir geben statt I die Liste aller Werte von I an (in einer Reihenfolge, die meist durch den Kontext klargestellt wird). Wenn unsere Sprache etwa das zweistellige Funktionssymbol $+$ und das Konstantensymbol 0 enthält, geben wir ein Modell als Tupel $\mathfrak{M} = (M, f, m)$ an, wobei $f = +^{\mathfrak{M}}$ eine zweistellige Funktion auf M ist, und $m \in M$ ist.

Wenn die Grundmenge unseres Modells $\mathfrak{M} = (M, I)$ zum Beispiel die natürlichen Zahlen sind und das Symbol $+$ durch die übliche Additionsfunktion interpretiert werden soll und das Symbol 0 durch die Zahl 0, also

(a) $M = \mathbb{N}$

(b) $I($„das Symbol +“ $)=$ „die Additionsfunktion“

(c) $I($„das Symbol 0“ $)=$ „die Zahl Null“

dann kürzen wir diesen Sachverhalt einfach durch $\mathfrak{M}=(\mathbb{N},+,0)$ ab. Wenn es notwendig ist, zwischen dem Symbol + und der Funktion + zu unterscheiden, markieren wir das Symbol mit einem Punkt: $\dot{+}$.
Die Beziehung (b) schreiben wir also z.B. so: $\dot{+}^{\mathfrak{M}}=+$.

4.3 Gültigkeit in Modellen

Als nächstes wollen wir uns mit dem Thema „Wahrheit“ etwas genauer beschäftigen.

Bemerkung 4.7. Alle unsere prädikatenlogischen Sprachen werden das zweistellige Relationssymbol = enthalten (ausgenommen jene Sprachen, die wir im Abschnitt 9 über Resolution betrachten). Syntaktisch verhält sich dieses Symbol wie alle anderen zweistelligen Relationssymbole; sobald wir aber Modelle betrachten, wird dieses Symbol eine besondere Rolle spielen.

Bemerkung 4.8. Sei φ eine Formel, in der die Variable u vorkommt, und sei t ein Term. Wir bezeichnen den Vorgang, in dem jedes freie Vorkommnis der Variablen u durch t ersetzt wird, als *Substitution*. Das Ergebnis der Substitution können wir als $\varphi(u/t)$ anschreiben, aber auch andere Notationen sind üblich: $\varphi(u \leftarrow t)$, $\varphi_u[t]$ oder auch $\varphi(t|u)$. Es ist auch üblich, statt φ den Ausdruck $\varphi(u)$ hinzuschreiben, und dann statt $\varphi(u/t)$ den Ausdruck $\varphi(t)$. Wenn u in φ gar nicht frei vorkommt, dann ist $\varphi(u/t)$ definitionsgemäß gleich φ.

Man kann in φ auch mehrere Variable (z.B. u,v) durch Terme (z.B. s,t) ersetzen; wenn wir die Variablen gleichzeitig durch die entsprechenden Terme ersetzen, schreiben wir für das Ergebnis $\varphi(u/s,v/t)$; die Hintereinanderausführung kann ein anderes Ergebnis $\varphi(u/s)(v/t)$ liefern (wenn nämlich im Term s wiederum die Variable v vorkommt).
Indem man φ explizit als $\varphi(u,v)$ anschreibt, legt man eine Reihenfolge der Variablen fest; erst dadurch kann man später, ohne Missverständnisse befürchten zu müssen, $\varphi(s,t)$ für die Formel $\varphi(u/s,v/t)$ schreiben.
Es ist auch möglich, Konstantensymbole durch Terme zu ersetzen; für jede Formel φ und jede Konstante c sei $\varphi(c/t)$ die Formel, die man erhält, indem man alle Vorkommnisse von c durch den Term t ersetzt. Solche Substitutionen sind allerdings unüblich. (Wir werden so eine Substitution im Beweis des Generalisierungstheorems verwenden.)

Wenn wir etwas über Substitution beweisen wollen, müssen wir den Begriff der Substitution etwas formaler betrachten:

Definition 4.9 (Substitution)**.** Sei u eine Variable (oder Konstante), und sei u ein Term. Dann definieren wir

(a) Eine Abbildung $s \mapsto s(u/t)$, die jedem Term s einen neuen Term $s(u/t)$ zuordnet,

(b) sowie eine Abbildung $\varphi \mapsto \varphi(u/t)$, die jeder Formel φ eine neue Formel $\varphi(u/t)$ zuordnet,

durch folgende Rekursion:

(a1) Wenn s die Variable u ist, dann ist $s(u/t)$ der Term t.

(a2) Wenn s eine andere Variable oder Konstante ist, dann ist $s(u/t)$ der Term s.

(a3) Wenn s der Term $f(s_1, \ldots, s_k)$ ist (wobei f ein k-stelliges Funktionssymbol ist), dann bilden wir zunächst die Terme $s'_1 := s_1(u/t)$, $s'_2 := s_2(u/t)$, etc., und definieren das Resultat $s(u/t)$ als $f(s'_1, \ldots, s'_k)$.

(b1) Wenn φ die Atomformel $s_1 = s_2$ ist, dann ist $\varphi(u/t)$ die Atomformel $s'_1 = s'_2$, wobei $s'_1 := s_1(u/t)$ und $s'_2 := s_2(u/t)$.

(b2) Wenn φ die Atomformel $R(s_1, \ldots, s_k)$ ist, dann ist $\varphi(u/t)$ die Atomformel $R(s'_1, \ldots, s'_k)$, wobei $s'_i := s_i(u/t)$ für $i = 1, \ldots, k$.

(b3) Wenn φ die Konjunktion $\psi_1 \wedge \psi_2$ ist, dann definieren wir $\varphi(u/t)$ als $\psi_1(u/t) \wedge \psi_2(u/t)$.

(b4) Analog für die anderen Junktoren.

(b5) Wenn φ die Formel $\exists u\, \psi$ ist, dann kommt u in φ nur gebunden vor. Wir definieren in diesem Fall $\psi(u/t) := \psi$.

(b6) Wenn φ die Formel $\exists x\, \psi$ ist, wobei die Variable x von der Variablen u verschieden ist, dann setzen wir $\psi' := \psi(u/t)$ und setzen $\varphi(u/t) := \exists x\, \psi'$.
Kurz gesagt: $\Big(\exists x\, \varphi\Big)(u/t) = \exists x \Big(\varphi(u/t)\Big)$.

(b7) Analog für $\forall x\, \psi$.

Definition 4.10 (Belegung)**.** Sei $\mathfrak{M} := (M, I)$. Eine Belegung b ist eine Abbildung von allen (freien) Variablen nach M. (Oft betrachten wir auch „partielle“ Belegungen, die also nur gewissen Variablen Werte zuordnen.)

Wir wenden uns nun der Interpretation von Termen zu.

Definition und Satz 4.11. *Sei $\mathfrak{M} = (M, I)$ eine $\mathscr{L}$-Struktur, und sei b eine Belegung.*
Dann gibt es eine eindeutig bestimmte Funktion $\bar{b}$ mit Wertebereich $\subseteq M$, die auf allen Termen definiert ist, und die die folgenden Eigenschaften hat:

- $\bar{b}(u) = c^{\mathfrak{M}}$ *für alle Konstanten c.*
- $\bar{b}(u) = b(u)$ *für alle Variablen u.*
- $\bar{b}(f(t_1, \ldots, t_n)) = f^{\mathfrak{M}}(\bar{b}(t_1), \ldots, \bar{b}(t_n))$.

Wenn b eine Belegung ist, die nur auf gewissen Variablen, sagen wir allen $u \in V$ definiert ist, dann gilt analog, dass es eine eindeutig bestimmte Funktion $\bar{b}$ wie oben gibt, die auf allen Termen definiert ist, welche nur Variablen in V verwenden.

Beweis. Der Beweis erfolgt durch Induktion über den Termaufbau. □

In dieser Definition haben wir eine Belegung festgehalten und die Terme variiert; wenn wir nun einen Term festhalten, können wir folgendes definieren:

Definition 4.12. Eine Belegung b, die nur auf den Variablen $\{u_1, \ldots, u_n\}$ definiert ist, können wir mit dem n-Tupel $\vec{u}_b := (b(u_1), \ldots, b(u_n)) \in M^n$ identifizieren. Umgekehrt können wir jedem n-Tupel $\vec{m} = (m_1, \ldots, m_n) \in M^n$ die Belegung $b_{\vec{m}}$ zuordnen, die u_i auf m_i abbildet.
Mit dieser Bezeichnung gilt: Jeder Term t, dessen freie Variable in der Menge $\{u_1, \ldots, u_n\}$ enthalten sind, induziert eine Funktion $t^{\mathfrak{M}} : M^n \to M$, nämlich

$$t^{\mathfrak{M}}(\vec{m}) = \bar{b}_{\vec{m}}(t).$$

Sei n nun fest. Die obigen Rechenregeln für $\bar{b}$ übersetzen sich nun so in die neue Schreibweise:

- Für jedes Konstantensymbol c ist $c^{\mathfrak{M}} : M^n \to M$ die konstante Abbildung $(m_1, \ldots, m_n) \mapsto c^{\mathfrak{M}} \in M$.
- Für jede Variable u_i mit $i \in \{1, \ldots, n\}$ ist $u_i^{\mathfrak{M}} : M^n \to M$ die i-te Projektion: $(m_1, \ldots, m_n) \mapsto m_i$.
- Für den Term $f(t_1, \ldots, t_k)$ ist $f(t_1, \ldots, t_k)^{\mathfrak{M}} : M^n \to M$ die durch $\bar{m} := (m_1, \ldots, m_n) \mapsto f^{\mathfrak{M}}(t_1^{\mathfrak{M}}(\bar{m}), \ldots, t_k^{\mathfrak{M}}(\bar{m}))$ definierte Abbildung.

Bei der untenstehenden Definition von $\mathfrak{M} \vDash \forall x \cdots$ werden wir die folgenden Schreibweise brauchen:

Definition 4.13. Seien b und b' Belegungen. Wir schreiben $b' =_u b$, wenn für alle Variablen v mit $v \neq u$ gilt: $b'(v) = b(v)$, wenn also b und b' auf allen Variablen übereinstimmen — außer möglicherweise auf der Variablen u.

DIE FOLGENDE DEFINITION IST ÄUSSERST WICHTIG.

Definition 4.14 (Gültigkeit unter einer Belegung)**.** Für

- jede $\mathscr{L}$-Struktur $\mathfrak{M}$,
- jede Formel $\varphi(u_1, \ldots, u_n)$ (mit freien Variablen unter $u_1, \ldots, u_n$)
- und jede Belegung $b : \{u_1, \ldots, u_n\} \to M$

definieren wir, wann $\mathfrak{M} \vDash \varphi\,[b]$ gilt.[12] Die Definition erfolgt induktiv nach dem Aufbau der Formel φ; für Atomformeln gilt zunächst

- $\mathfrak{M} \vDash R(t_1, \ldots, t_k)\,[b] \;\Leftrightarrow\; (t_1^{\mathfrak{M}}(\vec{u}_b), \ldots, t_k^{\mathfrak{M}}(\vec{u}_b)) \in R^{\mathfrak{M}}$
  (Wir schreiben $\vec{u}_b$ wieder als Abkürzung für $(b(u_1), \ldots, b(u_n))$. Da $\doteq^{\mathfrak{M}}$ die tatsächliche Gleichheit $\{(m, m) : m \in M\}$ ist, heißt dies insbesondere:
  $$\mathfrak{M} \vDash t_1 = t_2\,[b] \;\Leftrightarrow\; t_1^{\mathfrak{M}}(\vec{u}_b) = t_2^{\mathfrak{M}}(\vec{u}_b)$$

Seien nun φ, ψ Formeln, dann gilt weiters

- $\mathfrak{M} \vDash \top\,[b]$ gilt immer
- $\mathfrak{M} \vDash \bot\,[b]$ gilt nie
- $\mathfrak{M} \vDash (\varphi \wedge \psi)\,[b] \;\Leftrightarrow\; \mathfrak{M} \vDash \varphi\,[b]$ und $\mathfrak{M} \vDash \psi\,[b]$
- $\mathfrak{M} \vDash (\varphi \vee \psi)\,[b] \;\Leftrightarrow\; \mathfrak{M} \vDash \varphi\,[b]$ oder $\mathfrak{M} \vDash \psi\,[b]$
- $\mathfrak{M} \vDash (\neg\varphi)\,[b] \;\Leftrightarrow\; \mathfrak{M} \nvDash \varphi\,[b]$.
  (Hier verwenden wir die Abkürzung $\mathfrak{M} \nvDash \varphi\,[b]$ für die Negation der Beziehung $\mathfrak{M} \vDash \varphi\,[b]$. Siehe auch Anmerkung 4.20.)
- $\mathfrak{M} \vDash (\varphi \to \psi)\,[b] \;\Leftrightarrow\; \mathfrak{M} \nvDash \varphi\,[b]$ oder $\mathfrak{M} \vDash \psi\,[b]$
- Für jede Formel φ:
  $\mathfrak{M} \vDash (\forall x\,\varphi)\,[b] \;\Leftrightarrow\; \forall b' :$ Wenn $b' =_x b$, dann $\mathfrak{M} \vDash \varphi\,[b']$.
  Wenn wir also feststellen wollen, ob $\forall x\,\varphi$ in $\mathfrak{M}$ unter der Belegung b gilt, dann interessieren wir uns nicht für den Wert von b an der Stelle x, sondern wir müssen die Wahrheit von φ „für alle“ x nachprüfen; das heißt, wir betrachten alle möglichen „Varianten“ b' von b; jede Variante b' setzt einen anderen Wert für x ein.
- Für jede Formel φ:
  $\mathfrak{M} \vDash \exists x\,\varphi\,[b] \;\Leftrightarrow\; \exists b' : b' =_x b$ und $\mathfrak{M} \vDash \varphi\,[b']$

[12] Wir lesen diesen Begriff so: *Im Modell $\mathfrak{M}$ gilt die Formel φ unter der Belegung b.*

Beispiel. Wir betrachten die Formel $\varphi(u) : \dot{0} \dot{\leq} u$, die Struktur $(\mathbb{N}, 0, <)$, sowie die Belegungen

$$b_1 : u \mapsto 7$$

$$b_2 : u \mapsto 5$$

$$b_3 : u \mapsto 0$$

Dann gilt $(\mathbb{N}, 0, <) \vDash \varphi\ [b_1]$, d.h. die Struktur $(\mathbb{N}, 0, <)$ erfüllt die Formel φ unter der Belegung b_1. Ebenso erkennt man $(\mathbb{N}, 0, <) \vDash \varphi\ [b_2]$, sowie $(\mathbb{N}, 0, <) \nvDash \varphi\ [b_3]$

Wir schreiben $\varphi(u)$, um darauf hinzuweisen, dass u eine freie Variable ist. Statt $(\mathbb{N}, 0, <) \vDash \varphi\ [b_1]$ schreiben wir auch $\mathbb{N} \vDash \varphi\ [b_1]$ und statt $\mathbb{N} \vDash \varphi\ [b_1]$ schreiben wir auch $\mathbb{N} \vDash 0 < 7$. (Beachten Sie aber, dass „$0 < 7$“ nicht als Formel der betrachteten Sprache angesehen werden kann; das Element 0 des Universums $\mathbb{N}$ könnte man zur Not noch als Konstante $\dot{0}$ lesen, aber in der betrachteten Sprache haben wir kein Konstantensymbol $\dot{7}$.)

Beispiel. Wir betrachten die Formel $\forall x\ \dot{0} \dot{<} x$ und dieselbe Struktur $(\mathbb{N}, 0, <)$ wie vorhin. Sei b eine beliebige Belegung. Dann gilt $(\mathbb{N}, 0, <) \nvDash \forall x\,(0 < x)[b]$, denn es gibt eine Belegung $b' =_x b$ mit $(\mathbb{N}, 0, <) \nvDash (0 < x)[b']$; wir müssen nur $b'(x) = 0$ setzen.

Da die Definition von $\vDash$ so wichtig ist, geben wir eine Variante der Definition an (die zur ursprünglichen Definition äquivalent ist).

Definition und Satz 4.15. *Sei $\mathfrak{M} = (M, I)$ eine $\mathscr{L}$-Struktur, und sei b eine Belegung.*
Dann gibt es erstens (laut 4.11) eine eindeutig bestimmte Funktion $\bar{b}$ mit den Eigenschaften 1–3, die die Menge aller Terme in die Menge M abbildet, sowie zweitens eine eindeutig bestimmte Funktion $\hat{b}$ mit den Eigenschaften 4–8, die jeder Formel φ einen Wahrheitswert $\hat{b}(\varphi) \in \{0, 1\}$ zuweist:

1. *$\bar{b}(c) = c^{\mathfrak{M}}$ für alle Konstantensymbole c.*
2. *$\bar{b}(u) = b(u)$ für alle Variablen u.*
3. *$\bar{b}(\underset{\cdot}{f}(t_1, \ldots, t_n)) = f^{\mathfrak{M}}(\bar{b}(t_1), \ldots, \bar{b}(t_n))$, wenn $t_1, \ldots, t_n$ Terme sind, und $\underset{\cdot}{f}$ ein n-stelliges Funktionssymbol.*
   (Bis jetzt haben wir nur 4.11 wiederholt.)
4. *$\hat{b}(R(t_1, \ldots, t_n)) = 1$, wenn das n-Tupel $(\bar{b}(t_1), \ldots, \bar{b}(t_n))$ in $R^{\mathfrak{M}}$ liegt, und $\hat{b}(R(t_1, \ldots, t_n)) = 0$ sonst (für n-stellige Relationssymbole R)*
   Insbesondere soll für 0-stellige Relationssymbole P gelten: $\hat{b}(P) = 1$ genau dann, wenn $P^{\mathfrak{M}}$ das leere Tupel enthält (also nicht leer ist).
5. *$\hat{b}(\top) = 1$, $\hat{b}(\bot) = 0$.*

6. $\hat{b}(\varphi \mathbin{\dot{\wedge}} \psi) = \hat{b}(\varphi) \wedge_{\mathrm{B}} \hat{b}(\psi)$, $\hat{b}(\varphi \mathbin{\dot{\to}} \psi) = \hat{b}(\varphi) \to_{\mathrm{B}} \hat{b}(\psi)$, *etc.*
(Insbesondere also: $\hat{b}(\varphi \to \psi) = 0$ *genau dann, wenn* $\hat{b}(\varphi) = 1$ *und* $\hat{b}(\psi) = 0$.*)*

7. $\hat{b}(\forall x\, \varphi) = \bigwedge_{\mathrm{B}} \{\hat{b}'(\varphi) \mid b' =_x b\}$. *(Zur Schreibweise* $\bigwedge_{\mathrm{B}}$ *siehe 2.1.) Diese Definition liefert also den kleinsten aller Werte* $b'(\varphi)$*, wobei* b' *alle Belegungen durchläuft, die* $b' =_x b$ *erfüllen.* $\hat{b}(\forall x\, \varphi)$ *ist also genau dann gleich* 1*, wenn für alle Varianten* b' *(mit* $b' =_x b$*) die Beziehung* $\hat{b}'(\varphi) = 1$ *gilt.*

8. $\hat{b}(\exists x\, \varphi) = \bigvee_{\mathrm{B}} \hat{b}'(\varphi)$*, wobei* b' *wieder alle Belegungen* $b' =_x b$ *durchläuft.* $\hat{b}(\exists x\, \varphi)$ *ist also genau dann gleich* 1*, wenn es mindestens eine Variante* b' *(mit* $b' =_x b$*) gibt, die* $\hat{b}'(\varphi) = 1$ *erfüllt.*

Es gilt nun:

$$\mathfrak{M} \vDash \varphi[b] \;\Leftrightarrow\; \hat{b}(\varphi) = 1.$$
$$\mathfrak{M} \nvDash \varphi[b] \;\Leftrightarrow\; \hat{b}(\varphi) = 0.$$

Satz 4.16. *Seien* b, b' *Belegungen der Variablen* $u_1, \ldots, u_n$ *und* $b =_{u_r} b'$*. Sei weiters* φ *eine Formel in den freien Variablen* $u_{i_1}, \ldots, u_{i_k}$*, wobei* r *in der Menge* $\{i_1, \ldots, i_k\}$ *nicht vorkommt. (D.h. die Variable* u_r *kommt in den Variablen von* φ *nicht vor.)*
Dann gilt:

$$\mathfrak{M} \vDash \varphi\ [b] \Leftrightarrow \mathfrak{M} \vDash \varphi\ [b']$$

Das heißt: Wenn man $\mathfrak{M} \vDash \varphi\,[b]$ überprüfen will, so sind sind die Werte $b(u)$ auf Variablen u, die nicht in φ vorkommen, irrelevant.

Satz 4.17. *Sei* σ *eine geschlossene Formel (d.h. ohne freie Variablen) und* b, b' *Belegungen von* $u_1, \ldots, u_n$*. Dann gilt*

$$\mathfrak{M} \vDash \sigma\ [b] \Leftrightarrow \mathfrak{M} \vDash \sigma\ [b']$$

In diesem Zusammenhang nennt man σ *auch einen Satz.*

Definition 4.18 (Gültigkeit in einem Modell)**.**
Sei σ ein Satz. Wir sagen „σ gilt in $\mathfrak{M}$“ und schreiben $\mathfrak{M} \vDash \sigma$, falls

$$\mathfrak{M} \vDash \sigma\ [b] \quad \forall b.$$

(Wir haben uns bereits überlegt, dass die Beziehung $\mathfrak{M} \vDash \sigma\,[b]$ ohnehin nicht von b abhängt, solange σ keine freien Variablen enthält.)
Sei Σ eine Menge von Sätzen. Wir schreiben $\mathfrak{M} \vDash \Sigma$, falls

$$\mathfrak{M} \vDash \sigma \quad \forall \sigma \in \Sigma$$

Gelegentlich ist es auch praktisch, die Gültigkeit von Formeln *mit* freien Variablen zu definieren.

Definition 4.19. Sei φ eine Formel (mit eventuell freien Variablen). Wir schreiben $\mathfrak{M} \vDash \varphi$, falls für alle Belegungen b (der freien Variablen von φ) die Beziehung

$$\mathfrak{M} \vDash \varphi\ [b]$$

gilt.

Wenn φ etwa eine Formel mit einer einzigen freien Variable u ist, und man

$$\text{für alle } b\text{:} \qquad \mathfrak{M} \vDash \varphi\ [b]$$

überprüfen will, muss man nur jene partiellen Belegungen betrachten, die auf u definiert sind (da es auf die Werte $b(v)$ für andere Variablen nicht ankommt). Genau dasselbe muss man aber machen, wenn man die Wahrheit von

$$\mathfrak{M} \vDash \forall u\, \varphi$$

überprüfen will. Daher gilt $\mathfrak{M} \vDash \forall u\, \varphi$ genau dann, wenn $\mathfrak{M} \vDash \varphi$ gilt.

Bemerkung 4.20. Achtung! Laut Definition 4.14 gilt zwar

$$\mathfrak{M} \nvDash \varphi\ [b] \quad \Leftrightarrow \quad \mathfrak{M} \vDash \neg\varphi\ [b]$$

für jede Belegung b, im Allgemeinen ist die Beziehung

$$\mathfrak{M} \nvDash \varphi \quad \Leftrightarrow \quad \mathfrak{M} \vDash \neg\varphi$$

aber falsch! Sie gilt nur dann, wenn φ eine geschlossene Formel ist. Sei nämlich φ eine Formel mit freien Variablen:

- $\mathfrak{M} \vDash \neg\varphi$ bedeutet, dass die Beziehung $\mathfrak{M} \vDash (\neg\varphi)\,[b]$ für alle[13] Belegungen b gilt, d.h. dass die Beziehung $\mathfrak{M} \vDash \varphi\,[b]$ für *keine* Belegung b gilt.
- $\mathfrak{M} \nvDash \varphi$ ist jedoch (laut Definition) die Negation der Beziehung $\mathfrak{M} \vDash \varphi$; das heißt, dass $\mathfrak{M} \vDash \varphi\ [b]$ nicht für alle b gilt, es also *zumindest eine* Belegung b gibt, sodass $\mathfrak{M} \vDash \varphi\ [b]$ nicht gilt.

Um Irrtümer zu vermeiden, definiert man daher oft die Beziehung $\mathfrak{M} \vDash \varphi$ (ohne Belegung) nur für geschlossene Formeln φ.

Beispiel. Sei $\mathfrak{M}$ eine Struktur mit mindestens 2 Elementen, 0 ein Konstantensymbol, x eine Variable. Dann gilt weder die Formel $x = 0$ in $\mathfrak{M}$, noch ihre Negation $\neg(x = 0)$ (abgekürzt $x \neq 0$):

$$\mathfrak{M} \nvDash x = 0, \text{ denn } \mathfrak{M} \nvDash \forall x(x = 0);$$
$$\mathfrak{M} \nvDash x \neq 0, \text{ denn } \mathfrak{M} \nvDash \forall x(x \neq 0).$$

[13] Es genügt, nur solche Belegungen zu betrachten, die auf allen in φ vorkommenden freien Variablen definiert sind.

4.4 Allgemeingültigkeit

Definition 4.21 (Allgemeingültigkeit)**.** Sei σ ein Satz. Wir sagen „σ ist *allgemeingültig*“, falls σ in allen Modellen $\mathfrak{M}$ gilt, d.h. wenn gilt

$$\forall \mathfrak{M} : \mathfrak{M} \vDash \sigma.$$

Wir schreiben auch kurz $\vDash \sigma$.

Beispiel. $\vDash \exists x \big(\, (\exists y \, P(y)) \rightarrow P(x) \, \big)$

Beweis. Sei $\mathfrak{M} = (M, P^{\mathfrak{M}})$ ein beliebiges Modell. Wir unterscheiden die folgenden beiden Fälle:

1. $P^{\mathfrak{M}} = \emptyset$, d.h., $\mathfrak{M} \vDash \neg \exists x \, P(x)$

   Gesucht ist also eine Belegung b, sodass eine/alle der folgenden (äquivalenten) Bedingungen gelten:

   (a) $\mathfrak{M} \vDash (\, (\exists y \, P(y)) \rightarrow P(u) \,) \, [b]$.

   (b) $\mathfrak{M} \vDash (\, (\neg \exists y \, P(y)) \vee P(u) \,) \, [b]$.

   (c) $\mathfrak{M} \vDash (\, \neg \exists y \, P(y) \,)[b]$ oder $\mathfrak{M} \vDash P(u) \, [b]$.

   Die Bedingung $\mathfrak{M} \vDash (\, \neg \exists y \, P(y) \,)[b]$ hängt aber gar nicht von b ab und ist unter jeder beliebigen Belegung b wahr.

2. $P^{\mathfrak{M}} \neq \emptyset$, also $\mathfrak{M} \vDash \exists x \, P(x)$.

   Sei $m_0 \in P^{\mathfrak{M}} \subseteq M$ und $b : u \mapsto m_0$. Dann gilt $\mathfrak{M} \vDash P(u) \; [b]$, woraus die Behauptung folgt, da die rechte Seite der Implikation für diese Belegung wahr wird.

□

Wir haben das Symbol $\vDash$ bereits in mehreren Rollen kennengelernt: $\mathfrak{M} \vDash \varphi[b]$ in 4.14, $\mathfrak{M} \vDash \varphi$ in 4.18, $\vDash \varphi$ in 4.21. Diesen letzten Begriff der Allgemeingültigkeit können wir nun auf den Begriff der „Folgerung“ relativieren.

Definition 4.22 ($\Sigma \vDash \varphi$, Folgerung)**.**

1. Seien σ_1, σ_2 Sätze. Wir schreiben $\sigma_1 \vDash \sigma_2$ (oder $\{\sigma_1\} \vDash \sigma_2$), wenn für alle $\mathfrak{M}$, die $\mathfrak{M} \vDash \sigma_1$ erfüllen, auch $\mathfrak{M} \vDash \sigma_2$ gilt (oder äquivalent dazu: wenn $\vDash \sigma_1 \rightarrow \sigma_2$ gilt).

2. Sei σ ein Satz und Σ eine Menge von Sätzen. Wir schreiben $\Sigma \vDash \sigma$, wenn für alle $\mathfrak{M}$, die $\mathfrak{M} \vDash \Sigma$ erfüllen, auch $\mathfrak{M} \vDash \sigma$ gilt.

Wir sagen auch: „σ_2 *folgt* aus σ_1“ bzw. „σ folgt aus Σ“. Das Symbol $\vDash$ wird in diesem Zusammenhang auch als *semantische Folgerung* bezeichnet.

Bemerkung 4.23. Wenn Σ eine endliche Menge ist, etwa $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$, dann schreiben wir statt $\Sigma \vDash \varphi$ bzw. $\{\sigma_1, \ldots, \sigma_n\} \vDash \varphi$ kürzer $\sigma_1, \ldots, \sigma_n \vDash \varphi$. Wenn $\Sigma = \emptyset$ leer ist, dann gilt $\mathfrak{M} \vDash \Sigma$ für alle $\mathfrak{M}$. Daher gilt $\emptyset \vDash \varphi$ genau dann, wenn φ allgemeingültig ist, d.h. wenn $\vDash \varphi$ gilt.

Definition 4.24 (Erfüllbarkeit, Unerfüllbarkeit)**.** Eine Menge Σ von geschlossenen Formeln heißt erfüllbar, wenn es ein Modell $\mathfrak{M}$ mit $\mathfrak{M} \vDash \Sigma$ gibt. Andernfalls heißt Σ unerfüllbar.

Bemerkung 4.25. $\Sigma \vDash \bot$ bedeutet nach Definition, dass jedes Modell $\mathfrak{M}$, welches $\mathfrak{M} \vDash \Sigma$ erfüllt, auch $\mathfrak{M} \vDash \bot$ erfüllt. Die Beziehung $\mathfrak{M} \vDash \bot$ gilt aber nie. Daher:

> $\Sigma \vDash \bot$ gilt genau dann, wenn es *kein* Modell $\mathfrak{M}$ mit $\mathfrak{M} \vDash \Sigma$ gibt,
> oder mit anderen Worten, wenn Σ unerfüllbar ist.

Satz 4.26. *Sei Σ eine Menge von geschlossenen Formeln, φ und ψ geschlossenen Formeln.*

1. *$\Sigma \vDash \varphi$ gilt genau dann, wenn $\Sigma \cup \{\neg\varphi\} \vDash \bot$.*
2. *$\Sigma \vDash \neg\varphi$ gilt genau dann, wenn $\Sigma \cup \{\varphi\} \vDash \bot$.*
3. *$\Sigma \cup \{\varphi\} \vDash \psi$ gilt genau dann, wenn $\Sigma \vDash \varphi \to \psi$.*

Beweis. 1. Wir zeigen, dass die Negationen der beiden Bedingungen äquivalent sind.
$\Sigma \nvDash \varphi$ bedeutet, dass es ein Modell $\mathfrak{M}$ gibt, welches zwar Σ erfüllt, nicht aber φ. Da φ eine geschlossene Formel ist, bedeutet dies, dass $\mathfrak{M} \vDash \Sigma \cup \{\neg\varphi\}$ erfüllt, also ist $\Sigma \cup \{\neg\varphi\}$ erfüllbar.
Diese Schlüsse lassen sich auch umkehren: Jedes Modell, welches $\Sigma \cup \{\neg\varphi\} \nvDash \bot$ bezeugt, also $\Sigma \cup \{\neg\varphi\}$ erfüllt, ist ein Beleg für $\Sigma \nvDash \varphi$.
2. Ähnlich zu 1.
3. Die beiden Aussagen sind zu

$$\Sigma \cup \{\varphi, \neg\psi\} \vDash \bot \qquad \text{bzw.} \qquad \Sigma \cup \{\neg(\varphi \to \psi)\} \vDash \bot$$

äquivalent. Aber jedes Modell, welches φ und $\neg\psi$ erfüllt, erfüllt $\neg(\varphi \to \psi)\}$, und umgekehrt. □

Definition 4.27 (Obersprache, Untersprache)**.** Seien $\mathscr{L}$ und $\mathscr{L}'$ prädikatenlogische Sprachen und das Alphabet (also alle Variablen, Konstanten, etc.) von $\mathscr{L}$ sei eine Teilmenge des Alphabets von $\mathscr{L}'$. Dann nennen wir $\mathscr{L}'$ eine Obersprache von $\mathscr{L}$. $\mathscr{L}$ heißt Untersprache von $\mathscr{L}'$.

Definition 4.28 (Expansion, Redukt)**.** Ist $\mathscr{L}$ eine Untersprache von $\mathscr{L}'$, dann ist durch die $\mathscr{L}'$-Struktur $\mathfrak{M}'$ in natürlicher Weise eine $\mathscr{L}$-Struktur

$\mathfrak{M} = \mathfrak{M}' \restriction \mathscr{L}$ definiert (die Interpretationen der Symbole in $\mathscr{L}' \setminus \mathscr{L}$ werden einfach „vergessen“).
Umgekehrt gibt es zu jeder $\mathscr{L}$-Struktur $\mathfrak{M}$ eine (im Allgemeinen nicht eindeutig bestimmte) $\mathscr{L}'$-Struktur $\mathfrak{M}'$ mit $\mathfrak{M}' \restriction \mathscr{L} = \mathfrak{M}$; die Relations-, Funktions- und Konstantensymbole in $\mathscr{L}' \setminus \mathscr{L}$ kann man beliebig definieren. $\mathfrak{M}'$ heißt Expansion von $\mathfrak{M}$, $\mathfrak{M}$ heißt Redukt von $\mathfrak{M}'$.

Satz 4.29. *Sei $\mathscr{L}'$ eine Obersprache von $\mathscr{L}$ mit $c \in \mathscr{L}' \setminus \mathscr{L}$ und $\varphi(u)$ eine Formel. Dann gilt für alle $\mathscr{L}$-Strukturen $\mathfrak{M}$:*

$$\mathfrak{M} \vDash \varphi(u) \;\Leftrightarrow\; \mathfrak{M} \vDash \forall x\ \varphi(x) \;\Leftrightarrow\; \forall \mathfrak{M}' : \mathfrak{M} = \mathfrak{M}' \restriction \mathscr{L} :\ \mathfrak{M}' \vDash \varphi(c).$$

Insbesondere gilt

$$\vDash \varphi(u) \;\Leftrightarrow\; \vDash \forall x\ \varphi(x) \;\Leftrightarrow\; \vDash \varphi(c)$$

Bemerkung 4.30. Die Definition von $\Sigma \vDash \sigma$ hängt eigentlich von der zugrunde liegenden Sprache ab. Sei $\Sigma \cup \{\varphi\}$ eine Menge von geschlossenen Formeln in der Sprache $\mathscr{L}_1 \subseteq \mathscr{L}_2$. Dann müsste man eigentlich zwei Relationen $\Sigma \models_{\mathscr{L}_1} \varphi$ und $\Sigma \models_{\mathscr{L}_2}$ unterscheiden:

1. $\Sigma \models_{\mathscr{L}_1} \varphi$ bedeutet, dass für alle $\mathscr{L}$-Strukturen $\mathfrak{M}$, die $\mathfrak{M} \models \Sigma$ erfüllen, auch $\mathfrak{M} \models \varphi$ gilt.

2. $\Sigma \models_{\mathscr{L}_2} \varphi$ ist analog definiert, quantifiziert aber über alle $\mathscr{L}_2$-Strukturen $\mathfrak{M}'$, die $\mathfrak{M} \models \Sigma$ erfüllen.

Wegen des gerade zitierten Satzes (und der Bemerkung davor) sind die beiden Aussagen aber äquivalent: jedes Gegenbeispiel $\mathfrak{M}$ lässt sich zu einem Gegenbeispiel $\mathfrak{M}'$ expandieren, bzw. jedes $\mathfrak{M}'$ lässt sich zu einem $\mathfrak{M}$ reduzieren.

4.5 Äquivalenz

Definition 4.31. Seien φ und ψ Formeln mit freien Variablen unter x_1, …, x_n. Wir sagen, dass φ und ψ *äquivalent* sind, wenn die Formel $\varphi \leftrightarrow \psi$ allgemeingültig ist, oder äquivalent: wenn die Formel $\forall x_1 \cdots \forall x_n\ (\varphi \leftrightarrow \psi)$ allgemeingültig ist.

Beispiel. Seien x, y, z verschiedene Variable. Die Formel $\exists x\,(y = x + x)$, interpretiert in den natürlichen Zahlen, besagt, dass y eine gerade Zahl ist. Dasselbe wird von der Formel $\exists z\,(y = z + z)$ ausgesagt; man prüft leicht nach, dass die Formeln

$$\exists z\,(y = z + z), \qquad \exists x\,(y = x + x)$$

tatsächlich äquivalent sind.
Die Formel $\exists x\,(z = x + x)$ ist hingegen zur ersten Formel nicht äquivalent, da sie ja besagt, dass z (und nicht etwa y) gerade ist.

Satz 4.32. *Seien φ und ψ Formeln mit freien Variablen unter $x_1, \ldots, x_n$. Dann sind φ und ψ genau dann äquivalent, wenn für alle Belegungen b (die zumindest auf den Variablen $x_1, \ldots, x_n$ definiert sind) die Gleichung $\hat{b}(\varphi) = \hat{b}(\psi)$ gilt.*

4.6 Bereinigte Formeln

Formeln, in denen dieselbe Variable sowohl gebunden wie auch frei auftritt, wie zum Beispiel $x = 0 \to \forall x\,(x = 0)$, sind intuitiv nicht gut erfassbar, daher ersetzen wir sie gerne durch äquivalente Formeln, die besser lesbar sind (in diesem Fall: $x = 0 \to \forall y(y = 0)$).

Satz 4.33. *Sei φ eine Formel, und u eine Variable, die in φ nicht vorkommt. Dann sind die Formeln $\forall x\,\varphi$ und $\forall u\,(\varphi(x/u))$ äquivalent.*

Definition 4.34. Wir nennen eine Formel φ *bereinigt*, wenn sie die folgenden Bedingungen erfüllt:

1. Es gibt keine Variable, die in φ sowohl frei als auch gebunden vorkommt.
2. Jede in φ gebundene Variable wird an genau einer Stelle gebunden; das heißt, für jede gebundene Variable x gibt es genau eine Stelle in der Formel, wo x hinter einem Quantor steht.

Wir können die Begriffe „freie Variable einer Formel“, „gebundene Variable einer Formel“, „bereinigte Formel“ auch induktiv definieren:

Definition 4.35.

- Sei φ eine Atomformel. Die freien Variablen von φ, $Fr(\varphi)$ sind alle in φ vorkommenden Variablen; φ hat keine gebundenen Variablen ($Bd(\varphi) = \emptyset$), und φ ist bereinigt.
- Sei $\varphi = \neg\psi$. Dann gilt

  $$Fr(\varphi) = Fr(\psi), \qquad Bd(\varphi) = Bd(\psi)$$

  und φ ist genau dann bereinigt, wenn ψ es ist und x nicht in $Bd(\psi)$ ist. (Wenn $x \in Bd(\psi)$, dann wäre x in φ 2 Mal gebunden.)
- Sei $\varphi = \psi_1 \wedge \psi_2$. Dann gilt

  $$Fr(\varphi) = Fr(\psi_1) \cup Fr(\psi_2), \qquad Bd(\varphi) = Bd(\psi_1) \cup Bd(\psi_2),$$

  und φ ist genau dann bereinigt, wenn erstens ψ_1 und ψ_2 bereinigt sind, und zweitens

  $$Bd(\psi_1) \cap (Bd(\psi_2) \cup Fr(\psi_2)) = \emptyset = Bd(\psi_2) \cap (Bd(\psi_1) \cup Fr(\psi_1))$$

  gilt.

- Analog für $\psi_1 \to \psi_2$, etc.
- Sei $\varphi = \forall x\, \psi$ oder $\varphi = \exists x\, \psi$. Dann ist

$$Fr(\varphi) = Fr(\psi) \setminus \{x\}, Bd(\varphi) = Bd(\psi) \cup \{x\},$$

  und φ ist genau dann bereinigt, wenn ψ es ist.

Der folgende Satz (bzw. sein Beweis) liefert einen Algorithmus, der zu jeder Formel eine äquivalente bereinigte Formel berechnet:

Satz 4.36. *Sei A eine endliche Menge von Variablen. Dann gibt es zu jeder Formel φ eine bereinigte Formel $r_A(\varphi)$, in der überdies keine Variable aus A gebunden ist.*

Beweis. Für Atomformeln (und sogar allgemein für quantorenfreie Formeln) φ können wir $r_A(\varphi) = \varphi$ wählen. Weiters definieren wir rekursiv:

- $r_A(\neg\psi) := \neg(r_A(\psi))$
- $r_A(\psi_1 \wedge \psi_2) = \psi_1' \wedge \psi_2'$, wobei zuerst $\psi_1' := r_{A \cup Bd(\psi_2) \cup Fr(\psi_2)}(\psi_1)$ gewählt wird, dann $\psi_2' := r_{A \cup Bd(\psi_1') \cup Fr(\psi_1')}(\psi_2)$.
- Analog für $\psi_1 \to \psi_2$, etc.
- $r_A(\forall x\, \psi) := \forall x\, \psi$, wenn x nicht in A vorkommt. Wenn aber $x \in A$ gilt, dann sei y eine neue Variable, die weder in ψ noch in A vorkommt, sei $\psi' := \psi(x/y)$, und $r_A(\forall x\, \psi) = \forall y\, \psi' = \forall y\, \psi(x/y)$.
  (Wir benennen also die gebundene Variable um.)
- Analog für $r_A(\exists x\, \psi)$.

Induktiv sieht man dann leicht, dass φ und $r_A(\varphi)$ äquivalent sind. □

5 Substitution

5.1 Substitution in Termen

Sei s ein Term, x eine Variable, t ein Term. Unter $s(x/t)$ verstehen wir jenen Term, den man erhält, wenn man jedes Vorkommnis von x in s durch t ersetzt.
Beispiel: Sei $s = (x + y) * (2 - x)$, und s der Term $x + 1$, dann ist $s(x/t)$ der Term $((x + 1) + y) * (2 - (x + 1))$.

Definition 5.1. Sei b eine Belegung mit Wertemenge $\subseteq M$, x eine Variable, $a \in M$. Mit $b_{x/a}$ bezeichnen wir jene Belegung, die an der Stelle x den Wert a hat und sonst mit b übereinstimmt.

Satz 5.2. *Sei $\mathfrak{M}$ eine Struktur (für die betrachtete Sprache), sei b eine Belegung, seien s und t Terme, und x eine Variable.*
Sei $a := \bar{b}(t)$. Dann ist $\bar{b}(s(x/t)) = \overline{b_{x/a}}(s)$.
In Worten: Statt die Belegung b auf den modifizierten Term anzuwenden, überlegen wir uns zunächst, welchen Einfluss diese Modifikation auf die Variable x hat — sie wird ja durch den Term t ersetzt, also müssen wir zunächst $a := \bar{b}(t)$ berechnen; nun definieren wir eine neue Belegung, die diesen Wert an x zuweist, und werten diese auf dem ursprünglichen Term s aus.

Beweis. Beweis mit Induktion nach dem Aufbau von s (für alle Belegungen gleichzeitig). Wenn s die Variable x ist, dann ist $s(x/t)$ der Term t, und die linke Seite ist $\bar{b}(t)$. Nach Definition erfüllt $b_{x/a}$ die Bedingung $b_{x/a}(x) = a = \bar{b}(t)$, also ist die rechte Seite auch $\bar{b}(t)$.
Wenn s eine andere Variable ist, sagen wir y, dann ist $s(x/t) = s$, also steht links $\bar{b}(s)$, und rechts steht $\overline{b_{x/a}}(s) = b_{x/a}(y) = b(y) = \bar{b}(s)$. Analog argumentieren wir im Fall, dass s eine Konstante ist.
Sei nun s ein komplizierter Term, sagen wir $s = f(s_1, \ldots, s_k)$ für ein k-stelliges Funktionssymbol f. Dann ist

$$s(x/t) = f(\, s_1(x/t)\,, \ldots,\, s_k(x/t)\,).$$

Auf der linken Seite der behaupteten Gleichung steht also

$$\bar{b}(f(\, s_1(x/t)\,, \ldots,\, s_k(x/t)\,) = f^{\mathfrak{M}}(\bar{b}(s_1(x/t)), \ldots) = f^{\mathfrak{M}}(\overline{b_{x/a}}(s_1), \ldots)$$

Auf der rechten Seite steht

$$\overline{b_{x/a}}(s) = f^{\mathfrak{M}}(\overline{b_{x/a}}(s_1), \ldots)$$

Nach Induktionsvoraussetzung (angewendet auf die Belegung $b_{x/a}$) sind die beiden Ausdrücke also gleich. □

5.2 Substitution in Formeln

Sei φ eine Formel, x eine Variable, t ein Term. Unter $\varphi(x/t)$ verstehen wir jene Formel, die man erhält, wenn man jedes *freie* Vorkommnis von x in s durch t ersetzt.

Definition 5.3. Wir sagen, dass die Substitution x/t in φ *verboten* (oder *unsinnig*) ist, wenn es (mindestens) eine freie Variable y in t gibt, die durch die Substitution gebunden wird; das heißt: wenn es eine Variable y in t gibt, und ein freies Vorkommnis der Variablen x in einer Unterformel von φ, die die Form $\forall y\,(\ldots)$ hat.
Alle anderen Substitutionen heißen „erlaubt“ (oder „sinnvoll“).

Formal sollte man diese Definition mit Induktion über den Aufbau von φ definieren. Zum Beispiel ist die Substitution x/t genau dann in $\psi_1 \wedge \psi_2$ erlaubt, wenn sie sowohl in ψ_1 als auch in ψ_2 erlaubt ist. Der kritische Punkt der induktiven Definition bezieht sich auf Formeln der Form $\forall y\, \psi$ und $\exists y\, \psi$ und : Hier ist die Substitution x/t genau dann erlaubt, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Die Variable x kommt in $\forall y\, \psi$ bzw. $\exists y\, \psi$ gar nicht frei vor (das schließt den Fall ein, dass die Variable y in Wirklichkeit die Variable x ist).
- Die Substitution x/t ist in der Formel ψ erlaubt, und die Variable y kommt in t nicht vor.

Beispiel. Seien x, y, z verschiedene Variable. Sei φ die Formel $\exists y\, (y < x)$. Dann sind die Substitutionen $x/2$, $x/(x + x)$, x/z, x/x erlaubt, die Substitutionen x/y und $x/(x + y)$ verboten.
Die Resultate der Substitutionen sind

$$\exists y\, (y < 2),\ \exists y\, (y < x+x),\ \exists y\, (y < z),\ \exists y\, (y < x),\ \exists y\, (y < y),\ \exists y\, (y < x+y)$$

Wir werden ab sofort immer nur erlaubte Substitutionen betrachten.

Bemerkung 5.4. Wie man mit gebundenen Variablen umgeht, wissen wir bereits aus anderen Gebieten der Mathematik, auch wenn die Bezeichnung „gebundene Variable“ dort nicht erwähnt wurde:

1. Im Ausdruck $\sum_{i=0}^{n} \binom{n}{i}$ ist i gebunden, und n frei. Es ist sinnvoll, n durch 7 oder durch $n * m^2$ zu ersetzen, nicht aber durch i oder i^2.

2. Die Laplace-Transformierte F einer Funktion f ist durch

$$F(x) = \int_0^\infty e^{-xy} f(y)\, dy$$

definiert; y ist auf der rechten Seite gebunden und kann durch eine neue Variable z ersetzt werden:

$$F(x) = \int_0^\infty e^{-xz} f(z)\, dz$$

In beiden Formeln können wir zum Beispiel x durch $r+2$ ersetzen, um $F(r + 2)$ zu erhalten:

$$F(r + 2) = \int_0^\infty e^{-(r+2)y} f(y)\, dy = \int_0^\infty e^{-(r+2)z} f(z)\, dz.$$

Die Substitution von x durch $r + 2$ ist also sinnvoll.

Wenn wir aber $F(3y)$ ausrechnen wollen, dürfen wir y nicht in die erste Formel einsetzen, das würde nämlich die falsche Formel $F(y) =$

$\int_0^\infty e^{-(3y)y} f(y)\,dy$ liefern. In dieser Substitution würde die „freie“ Variable y durch die Bindung der Integrationsvariablen auch gebunden werden.

Stattdessen setzt man $3y$ für x in die zweite Formel ein und erhält

$$F(3y) = \int_0^\infty e^{-(3y)z} f(z)\,dz.$$

5.3 Das Substitutionsaxiom

Satz 5.5. *Sei $\mathfrak{M}$ eine Struktur (für die betrachtete Sprache), sei b eine Belegung, sei φ Formel, sei t Term, und x eine Variable. Wir nehmen an, dass die Substitution $\varphi(x/t)$ erlaubt ist.*
Dann ist $\hat{b}(\varphi(x/t)) = \widehat{b_{x/a}}(\varphi)$ mit $a := \bar{b}(t)$.
Anders ausgedrückt:

$$\mathfrak{M} \models \varphi(x/t)\,[b] \;\Leftrightarrow\; \mathfrak{M} \models \varphi\,[b_{x/a}]$$

Beweis. Mit Induktion nach dem Aufbau von φ. Für Atomformeln verwenden wir Satz 5.2 über Termsubstitution.
Die Fälle $\varphi = \varphi_1 \wedge \varphi_2$, etc., sind leicht zu beweisen.
Wenn φ die Form $\forall x\,\psi$ oder $\exists x\,\psi$ hat, dann kommt x in φ nirgends frei vor, es ist also $\varphi(x/t) = \varphi$; weiters spielt der Wert von b an der Stelle x keine Rolle, es ist also $\hat{b}(\varphi) = \widehat{b'_{x/a}}(\varphi)$.
Sei nun $\varphi = \forall y\,\psi$ (analog für $\exists y\,\psi$), wobei y eine andere Variable ist. Da die Substitution $\varphi(x/t)$ erlaubt ist, kommt y im Term t nicht vor.
Die Formel $(\forall y\,\psi)(x/t)$ ist identisch mit der Formel $\forall y\,(\psi(x/t))$.

$$\begin{aligned}
\mathfrak{M} \models \varphi(x/t)\,[b] &\;\Leftrightarrow\; \mathfrak{M} \models \forall y\,\psi(x/t)\,[b] \\
&\;\Leftrightarrow\; \mathfrak{M} \models \psi(x/t)\,[b'] \text{ für alle } b' =_y b \\
&\;\Leftrightarrow\; \mathfrak{M} \models \psi\,[(b')_{x/a}] \text{ für alle } b' =_y b
\end{aligned}$$

Die Menge $\{(b')_{x/a} \mid b' =_y b\}$ ist identisch mit der Menge $\{b'' \mid b'' =_y b_{x/a}\}$ (alle Elemente beider Mengen haben den Wert $a = \bar{b}(t)$ an der Stelle x, beliebige Werte an der Stelle y, und stimmen sonst mit b überein). Daher gilt:

$$\begin{aligned}
\mathfrak{M} \models \varphi(x/t)\,[b] &\;\Leftrightarrow\; \mathfrak{M} \models \psi\,[b''] \text{ für alle } b'' =_y b_{x/a} \\
&\;\Leftrightarrow\; \mathfrak{M} \models \forall y\,\psi\,[b_{x/a}]
\end{aligned}$$

□

Satz 5.6 (Substitutionsaxiom für φ)**.** *Sei φ eine Formel, x eine Variable, und t ein Term, der für x in φ substituiert werden darf. Dann ist die Formel*

$$\forall x\, \varphi \;\rightarrow\; \varphi(x/t)$$

allgemeingültig.

Beweis. Sei $\mathfrak{M}$ eine Struktur, und b eine Belegung. Wir zeigen, dass aus $\hat{b}(\,\varphi(x/t)\,) = 0$ folgt, dass auch aus $\hat{b}(\,\forall x\, \varphi\,) = 0$ ist.
Aus dem vorhergehenden Satz und der Annahme $\hat{b}(\,\varphi(x/t)\,) = 0$ schließen wir $\widehat{b_{x/a}}(\varphi) = 0$ mit $a := \bar{b}(t)$. Insbesondere gilt also $b_{x/a} =_x b$.
Nach der Definition von $\hat{b}(\forall x\, \varphi)$ gilt also $\hat{b}(\forall x\, \varphi) = 0$. □

6 Aussagenlogik als Fragment der Prädikatenlogik

6.1 $A \times A$ und A^2

Sei A eine Menge. Mit $A \times A$ bezeichnen wir die Menge aller geordneten Paare von Elementen von A:

$$A \times A = \{(x, y) \mid x, y \in A\}$$

Eine 2-stellige Relation ist eine Teilmenge von $A \times A$.
Manchmal ist es jedoch praktischer, $A \times A$ durch folgende Menge zu ersetzen:

$$A^2 := \{f \mid f \text{ ist Funktion von } \{0, 1\} \text{ nach } A\}$$

Es gibt eine natürliche Bijektion zwischen A^2 und $A \times A$, nämlich die Abbildung, die jeder Funktion $f \in A^2$ das Paar $(f(0), f(1))$ zuordnet. Oft *identifizieren* wir (etwa aus notationellen Gründen) die Menge A^2 mit der Menge $A \times A$, das heißt: wir sprechen von der Menge A^2 oder einem ihrer Elemente f, meinen aber die Menge $A \times A$ bzw. eines ihrer Elemente $(f(0), f(1))$, oder umgekehrt.

6.2 A^n für $n \geq 1$

Ebenso können wir die Menge A^3 auf 2 Arten betrachten:

- entweder als Menge aller Funktionen von $\{0, 1, 2\}$ nach A;
- oder als Menge aller geordneten Tripel (x, y, z) mit $x, y, z \in A$.

In Analogie dazu ist die Menge A^1 die Menge aller Funktionen f von $\{0\}$ nach A. Jede solche Funktion identifizieren wir mit ihrem einzigen Wert; wir identifizieren dadurch die Menge A^1 mit der Menge A selbst. Ein „1-Tupel“ könnten wir als „(a)“ mit $a \in A$ schreiben, oder einfach nur als „a“.

6.3 A^0

Für jede natürliche Zahl $n \geq 1$ ist also A^n die Menge aller n-Tupel, oder äquivalent: die Menge aller Funktionen von der Menge $\{k \in \mathbb{N} \mid k < n\}$ nach A. Wenn wir für $n = 0$ dieselbe Definition verwenden, erhalten wir, dass A^0 die Menge aller Funktionen f von der leeren Menge nach A ist. Nun gibt es genau eine Funktion mit leerem Definitionsbereich, nämlich die leere Menge $\emptyset$; als „0-Tupel“ aufgefasst, könnten wir dieses Objekt auch mit „()“ bezeichnen.
A^0 hat also genau ein Element. Wenn A zum Beispiel 5 Elemente hat, dann besteht A^2 aus $25 = 5^2$ Elementen, A^1 hat $5 = 5^1$ Elemente, und A^0 hat $1 = 5^0$ Elemente.

6.4 k-stellige Relationen, für $k \geq 0$

Jede Teilmenge von A^k heißt k-stellige Relation auf A. Wenn A 5 Elemente hat, gibt es also 2^{25} zweistellige Relationen auf A, $2^5 = 32$ einstellige, und genau 2 nullstellige. Die eine nullstellige Relation trifft auf das leere 0-Tupel () zu, die andere nicht.

Beispiel. Sei $\mathscr{L}$ eine Sprache, die nur die 0-stelligen Relationssymbole P_1 und P_2 enthält. Dann gibt es 4 Arten von Modellen: Erstens jene Modelle (M, I), in denen sowohl $I(P_1)$ als auch $I(P_2)$ leer sind (also das 0-Tupel nicht enthalten); zweitens jene, in denen $I(P_1)$ leer ist, aber $I(P_2)$ nicht; drittens und viertens jene, in denen $I(P_1)$ nicht leer ist.

6.5 Aussagenlogik

Definition 6.1. Sei $\mathscr{L}$ eine Sprache, deren nichtlogische Zeichen nur die nullstelligen Relationssymbole P_1, P_2, ... sind. Eine „*aussagenlogische Formel*“ ist eine Formel dieser Sprache, in der weder Variable noch Quantoren vorkommen.

Beispiel.

$$P_1 \wedge P_2, \quad (P_1 \to P_2) \vee (P_2 \to P_1)$$

Die Formeln dieser Sprache lassen sich nun als aussagenlogische Formeln deuten, wobei man die folgenden Übersetzungen vornehmen muss:

Aussagenlogik in Kap. 2	Fragment der Prädikatenlogik
aussagenlogische Variable p_1, p_2, ...	nullstellige Rel.symbole P_1, P_2 ...
aussagenlogische Belegung $p_i \mapsto b(p_i)$	Interpretation $P_i \mapsto P_i^{\mathfrak{M}}\}$
$b(p_i) \in \{0, 1\}$	$P_i^{\mathfrak{M}} \in \{\emptyset, \{\emptyset\}\}$

Eine aussagenlogische Formel ist genau dann allgemeingültig, wenn sie in jedem einelementigen Modell gilt.

7 Prädikatenlogik: Beweisbarkeit

7.1 Formale Beweise

Wir suchen nun eine Methode, die entscheidet, ob eine Formel allgemeingültig ist, oder nicht. Wir werden zeigen: Es gibt ein „einfaches“ System von Axiomen (siehe Seite 47), aus dem wir in „einfacher“ Weise alle allgemeingültigen Formeln generieren können. (Weiters behaupten wir, und versuchen dies im Kapitel über Mengenlehre zu belegen, dass im Prinzip alle mathematischen Argumente auf das Feststellen von Allgemeingültigkeit hinauslaufen.)

Definition 7.1 (Modus Ponens; MP)**.** Seien φ_1, φ_2, φ_3 Formeln. Wir sagen, dass φ_3 aus φ_1 und φ_2 durch *Modus Ponens* hervorgeht, wenn φ_1 die Form $\varphi_2 \to \varphi_3$ hat.
Anders ausgedrückt: Modus Ponens ist eine partielle Funktion MP, die auf gewissen Paaren von Formeln definiert ist:

$$\mathrm{MP}(\,(\varphi \to \psi)\,,\ \varphi\,) \ = \ \psi$$

(und $\mathrm{MP}(A, B)$ ist undefiniert, wenn A nicht die Form $B \to \psi$ hat).

Satz 7.2 (Modus Ponens; MP)**.**

1. *Sei $\mathfrak{M}$ ein Modell, b eine Belegung der freien Variablen von $\sigma \to \tau$. Es gelte $\mathfrak{M} \vDash (\sigma \to \tau)\ [b]$ und $\mathfrak{M} \vDash \sigma\ [b]$. Dann folgt $\mathfrak{M} \vDash \tau\ [b]$.*
2. *Wenn $\mathfrak{M} \vDash \sigma \to \tau$ und $\mathfrak{M} \vDash \sigma$ gilt, dann gilt auch $\mathfrak{M} \vDash \tau$.*
3. *Es gelte $\Sigma \vDash \sigma \to \tau$ und $\Sigma \vDash \sigma$. Dann folgt $\Sigma \vDash \tau$.*

Das heißt, die in $\mathfrak{M}$ gültigen Formeln sind unter MP abgeschlossen; ebenso ist die Menge aller Formeln, die aus Σ folgen, unter MP abgeschlossen.

Beweis. Wir zeigen die erste Aussage. $\mathfrak{M} \vDash (\sigma \to \tau)\ [b]$ bedeutet $\mathfrak{M} \nvDash \sigma\ [b]$ oder $\mathfrak{M} \vDash \tau\ [b]$. Die erste Möglichkeit kommt laut Voraussetzung nicht in Frage, daher gilt $\mathfrak{M} \vDash \tau\ [b]$.
Die zweite und dritte Aussage folgen leicht aus der ersten. □

Definition 7.3 (Tautologie)**.** Sei A eine Tautologie in einer aussagenlogischen Sprache, und sei h eine Abbildung, die jeder aussagenlogischen Variable eine prädikatenlogische Formel zuweist. h lässt sich in natürlicher Weise zu einem Homomorphismus von den aussagenlogischen Formeln in die prädikatenlogischen Formeln fortsetzen. Sei nun φ eine prädikatenlogische Formel. Wir nennen φ Tautologie genau dann, wenn es eine aussagenlogische Tautologie A und eine Abbildung h gibt, sodass $\bar{h}(A) = \varphi$.

Beispiel. $\varphi: \ \forall x\ P(x) \to \forall x\ P(x)$ ist Tautologie, denn $A : p \to p$ und $h(p) = \forall x\ P(x)$ erfüllen die gewünschte Bedingung.

Axiome unseres Kalküls

Wir geben zunächst die Liste der „reinen“ Axiome an, und definieren dann die Menge der Axiome als die kleinste Menge von Formeln die erstens alle reinen Axiome enthält und zweitens mit jeder Formel φ auch alle Formeln der Form $\forall x\, \varphi$ enthält.

- **Tautologieaxiome** Jede Tautologie ist ein reines Axiom.

- **Distributivitätsaxiome**. Dies sind die Formeln der Form

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

- **Substitutionsaxiome**. Sei x eine Variable, sei φ eine beliebige Formel (meist mit der freien Variablen x), sei t ein beliebiger Term, der für x in φ substituiert werden darf. Dann ist

$$(\forall x\, \varphi) \to \varphi(x/t)$$

  ein Substitutionsaxiom.

- **Existenzaxiome.** $\exists x\, \varphi(x) \;\to\; \neg\forall x\, \neg\varphi(x)$ und $\neg\forall x\, \neg\varphi(x) \;\to\; \exists x\, \varphi(x)$ sind Axiome.
  Alternativ könnten wir sagen, dass der Quantor $\exists$ in unserer Sprache nicht vorkommt. Wenn wir ihn doch hinschreiben, ist mit der Formel $\exists\, \varphi$ eine Abkürzung für die Formel $\neg\forall x\, \neg\varphi$ gemeint.

- **Generalisierungsaxiome**. Dies sind die Formeln der Form

$$\varphi \to \forall x\, \varphi,$$

  wobei φ eine beliebige Formel ist, in der x nicht vorkommt.

- **Gleichheitsaxiome**. Dies sind die Formeln die eine der Formen $u = u$, $u = v \to v = u$, $(u = v \wedge v = w) \to u = w$ haben, wobei u, v, w beliebige Variable (nicht notwendigerweise verschieden) sind.

- **Leibnizaxiome**. Dies sind die Formeln der Form

$$(u_1 = v_1 \wedge \cdots \wedge u_n = v_n) \;\to\; f(u_1, \ldots, u_n) = f(v_1, \ldots, v_n)$$

  haben (wobei f ein n-stelliges Relationssymbol ist, und die u_i und v_j beliebige (nicht notwendigerweise verschiedene) Variable sind, sowie Axiome der Form

$$(u_1 = v_1 \wedge \cdots \wedge u_n = v_n) \;\to\; (R(u_1, \ldots, u_n) \leftrightarrow R(v_1, \ldots, v_n)),$$

  wobei R ein n-stelliges Relationssymbol ist.

Satz 7.4. *Sei φ eine Tautologie. Dann gilt $\models \varphi$, d.h. Tautologien sind allgemeingültig.*

Beweis. (Dieser Beweis ist dem Beweis von 2.14 sehr ähnlich.)
Sei $\varphi = \bar{h}(A)$, wobei A aussagenlogische Tautologie ist, und h Homomorphismus. Sei b eine (prädikatenlogische) Belegung (die zumindest auf allen in in φ vorkommenden Variablen definiert ist). Daraus können wir eine aussagenlogische Belegung[14] b_1 generieren, nämlich $b_1(p) = \hat{b}(h(p))$ für alle aussagenlogischen Variablen p, die in A vorkommen.
(Dies bedeutet, dass $b_1(p) = 1$ genau dann gilt, wenn $\mathfrak{M} \models h(p)\,[b]$.)
Da sowohl $\hat{b}_1$ als auch $\hat{b}$ mit den Junktoren verträglich sind, sieht man leicht (genauer: induktiv)

$$\hat{b}_1(B) = \hat{b}(\bar{h}(B))$$

für alle aussagenlogischen Formeln, insbesondere $\hat{b}_1(A) = \hat{b}(\bar{h}(A))$, daher $\hat{b}(\bar{h}(A)) = 1$, somit $\mathfrak{M} \models \bar{h}(A)\,[b]$. □

Bemerkung 7.5. Nicht alle allgemeingültigen Formeln sind Tautologien.[15] Zum Beispiel ist $\forall x\, P(x) \to \forall y\, P(y)$ allgemeingültig, aber keine Tautologie.

Definition 7.6 (formaler Beweis)**.** Ein formaler Beweis (ohne Voraussetzungen) ist eine endliche Folge $\varphi_1, \ldots, \varphi_n$ von Formeln, sodass $\forall i = 1, \ldots, n$ entweder

- φ_i ist logisches Axiom (siehe Seite 47), oder
- $\exists j_1, j_2 < i$, sodass φ_i durch MP aus $\varphi_{j_1}, \varphi_{j_2}$ hervorgeht

erfüllt ist.

Sei Σ eine Menge von Formeln (die nicht notwendigerweise geschlossen sind). Ein formaler Beweis aus Σ ist eine endliche Folge $\varphi_1, \ldots, \varphi_n$ von Formeln, sodass $\forall i = 1, \ldots, n$ entweder

- φ_i ist logisches Axiom, oder
- $\exists j_1, j_2 < i$, sodass φ_i durch MP aus $\varphi_{j_1}, \varphi_{j_2}$ hervorgeht, oder
- $\varphi_i \in \Sigma$

erfüllt ist.

[14] oder, in der Notation des vorigen Abschnitts, eine Interpretation der nullstelligen Prädikatensymbole unserer aussagenlogischen Sprache

[15] Allerdings wird das Wort „Tautologie“ in der Literatur häufig auch als Synonym für „allgemeingültige Formel“ verwendet; Tautologien in unserem Sinn heißen dann „aussagenlogische Tautologien“, oder „homomorphe Bilder aussagenlogischer Tautologien“, etc.

Definition 7.7 (Beweisbarkeit, Variante 1)**.** Eine Formel φ heißt beweisbar, wenn es einen formalen Beweis gibt, in dem φ vorkommt. Wir schreiben

$$\vdash \varphi$$

Eine Formel φ heißt beweisbar aus einer Menge Σ von Formeln, wenn es einen formalen Beweis aus Σ gibt, in dem φ vorkommt. Wir schreiben

$$\Sigma \vdash \varphi$$

Die Menge der beweisbaren Formeln ist unter Modus Ponens abgeschlossen.

Bemerkung 7.8. Statt „beweisbar“ sagt man auch „ableitbar“. Formale Beweise bezeichnet man auch als „Derivationen“ oder „Ableitungen“. Die Relation $\vdash$ bezeichnet man manchmal auch als „syntaktische Folgerung“. („syntaktisch“ sind jene Begriffe, die sich nur auf Formeln beziehen, die man auf ihre Struktur als endliche Zeichenfolgen untersuchen muss; „semantisch“ sind jene Begriffe, zu deren Verständnis man sich mit [oft unendlichen] Modellen beschäftigen muss.)

Die folgende alternative Definition vermeidet es, explizit den Begriff der „endlichen Folge“ zu erwähnen, und verwendet stattdessen ein Induktionsprinzip:

Definition 7.9 (Beweisbarkeit, Variante 2)**.** Wir definieren induktiv, was eine beweisbare Formel ist:

1. Jedes logische Axiom ist beweisbar.
2. Wenn A und $A \to B$ beweisbar sind, dann auch B.
3. Das sind alle.

Wie schon früher erwähnt, bedeutet dies: Jede Eigenschaft, die von allen Axiomen erfüllt wird und sich von A und $A \to B$ auf B vererbt, kommt allen beweisbaren Formeln zu. (Ein relevantes Beispiel so einer Eigenschaft ist die Allgemeingültigkeit, siehe „Soundness“ 7.12.)

Beispiel (formaler Beweis)*.* Wir beweisen Schritt für Schritt die Aussage

$$\vdash (\forall x\ P(x)) \to (\forall y\ P(y))$$

Der formale Beweis ist eine Folge von 7 Formeln; der Übersichtlichkeit halber schreiben wir jede dieser Formeln in eine eigene Zeile, und erwähnen neben der Formel, ob sie ein Axiom ist (bzw. welches Axiom sie ist) bzw. aus welchen früheren Formeln sie durch MP hervorgeht. Weiters führen wir an geeigneten Stellen Abkürzungen ein, um deutlich zu machen, welche aussagenlogischen Tautologien wir verwenden.

1. $\vdash \forall y\ (\forall x\ P(x) \to P(y))$ (Substitutionsaxiom)
2. $\vdash \forall y\ (\forall x\ P(x) \to P(y)) \to (\forall y\ \forall x\ P(x) \to \forall y\ P(y))$ (Dist.axiom)
3. $\vdash \underbrace{\forall y\ \forall x\ P(x)}_{B} \to \underbrace{\forall y\ P(y)}_{C}$ (MP(1,2))
4. $\vdash \underbrace{\forall x\ P(x)}_{A} \to \underbrace{\forall y\ \forall x\ P(x)}_{B}$ (Generalisierung)
5. $\vdash (A \to B) \to (\ (B \to C) \to (A \to C)\ )$ (Tautologie)
6. $\vdash (B \to C) \to (A \to C)$ (MP(4,5))
7. $\vdash A \to C$ (MP(3,6))

Satz 7.10. *Sei φ eine Formel, x und y Variable, und sei die Substitution $\varphi(x/y)$ sinnvoll. Dann gilt $\vdash \forall x\, \varphi \to \forall y\, \varphi(x/y)$.*

Beweis. Das vorige Beispiel war ein Spezialfall mit der Atomformel $\varphi := P(x)$. Der Beweis aus dem vorigen Beispiel lässt sich leicht verallgemeinern. □

Bemerkung 7.11. Welche Formeln logische Axiome sind, hängt offenbar von der zugrunde liegenden Sprache ab. Daher müsste man bei der Definition der Beweisbarkeit $\vdash$ eigentlich immer die zugrunde liegende Sprache erwähnen: $\vdash_{\mathscr{L}}$. Man kann aber zeigen, dass die Beziehung $\Sigma \vdash \varphi$ entweder in allen Sprachen $\mathscr{L}$ gilt, die die Formeln in $\Sigma \cup \{\varphi\}$ enthalten, oder in keiner. Daher schreibt man meist nur $\vdash$ statt $\vdash_{\mathscr{L}}$. (Siehe 4.30 für den analogen Satz für die semantische Folgerung $\models$.)

7.2 Soundness

Satz 7.12 (Soundness, Korrektheit)**.**

1. *Aus $\vdash \varphi$ folgt $\models \varphi$.*
2. *Aus $\Sigma \vdash \varphi$ folgt $\Sigma \models \varphi$,*

   insbesondere gilt also:
   wenn $\Sigma \vdash \bot$, dann $\Sigma \models \bot$, bzw.:
   wenn $\Sigma \nvDash \bot$, dann $\Sigma \nvdash \bot$.

(Dies gilt deshalb, weil erstens alle logischen Axiome allgemeingültig sind und zweitens die Anwendung von MP auf allgemeingültige Formeln immer nur allgemeingültige Formeln produziert.) Das zentrale Ergebnis des nächsten Kapitels — der Vollständigkeitssatz — besagt nun, dass im vorigen Satz jeweils auch die Umkehrung gilt:

Satz 7.13 (Vollständigkeitssatz)**.** *Sei Σ eine Menge von geschlossen Formeln und φ eine Formel. Wenn $\Sigma \vDash \varphi$ gilt, dann auch $\Sigma \vdash \varphi$.*

7.3 Kürzere Beweise

Wir sammeln nun einige Hilfmittel für den Beweis des Vollständigkeitssatzes. Zunächst kommen wir zu einer Methode, die es erlaubt, Beweise abzukürzen. Wie obiges Beispiel zeigt, ist dies sinnvoll, da bereits recht einfache Aussagen relativ komplizierte formale Beweise erfordern.

Definition 7.14 (abgekürzter Beweis)**.** Sei φ eine Formel. Ein abgekürzter (oder „halbformaler“) Beweis von φ (ohne Voraussetzung oder aus Σ) ist eine endliche Folge von Formeln $\varphi_1, \ldots, \varphi_n$, aus der man in mechanischer Weise, wie im Folgenden beschrieben, einen formalen Beweis generieren kann. Dies kann z.B. mit Hilfe der folgenden beiden Theoreme geschehen.

Satz 7.15 (Deduktionstheorem)**.** *Sei Σ eine Menge von Formeln und seien φ, ψ Formeln. Dann gilt*

$$\Sigma \cup \{\varphi\} \vdash \psi \;\Leftrightarrow\; \Sigma \vdash \varphi \to \psi$$

Die Richtung „$\Leftarrow$“ folgt leicht mit Hilfe von Modus Ponens. Daher wird auch oft nur die Richtung „$\Rightarrow$“ als Deduktionstheorem bezeichnet. In gewissem Sinn ist das Deduktionstheorem eine Umkehrung von Modus Ponens.

Beweis. Wir geben einen Algorithmus an, der jeden formalen Beweis von $\Sigma \cup \{\varphi\} \vdash \psi$ in einen formalen Beweis von $\Sigma \vdash \varphi \to \psi$ überführt. Sei also $\psi_1, \ldots, \psi_n$ ein formaler Beweis von $\Sigma \cup \{\varphi\} \vdash \psi$. Wir ersetzen jede Formel ψ_i durch drei Formeln $\psi_i^1, \psi_i^2, \psi_i^3$ und stellen sicher, dass die neue Folge wieder ein formaler Beweis ist. Der neue Beweis verwendet nur Axiome aus Σ, nicht jedoch die Voraussetzung φ. Die ψ_i werden folgendermaßen ermittelt:

1.Fall: ψ_i ist logisches Axiom oder $\psi_i \in \Sigma$. Setze

- $\psi_i^1 := \psi_i$ (Axiom oder VS.)
- $\psi_i^2 := \psi_i \to (\varphi \to \psi_i)$ (Tautologie)
- $\psi_i^3 := \varphi \to \psi_i$ (MP).

2.Fall: $\psi_i = \varphi$. Setze $\psi_i^1 := \psi_i^2 := \psi_i^3 := \varphi \to \psi_i$ (Tautologie)

3.Fall: ψ_i (=: B) folgt durch MP aus ψ_{j_1} (=: $A \to B$) und ψ_{j_2} (=: A). Dann gilt $\psi_{j_1}^3 = \varphi \to (A \to B)$ und $\psi_{j_2}^3 = \varphi \to A$. Setze

- $\psi_i^1 := [\varphi \to (A \to B)] \to [(\varphi \to A) \to (\varphi \to B)]$ (Tautologie)
- $\psi_i^2 := [(\varphi \to A) \to (\varphi \to B)]$ (MP)
- $\psi_i^3 := \varphi \to B$ (MP)

Die neue Folge von Formeln ist nun ein Beweis aus den Axiomen Σ, und für jede Formel ψ_i im alten Beweis kommt die Formel $\varphi \to \psi_i$ als Formel ψ_i^3 im neuen Beweis vor, insbesondere kommt auch $\varphi \to \psi$ im neuen Beweis vor. □

Bemerkung 7.16. Es gibt viele andere Beweissysteme (d.h. Arten, den Begriff „formaler Beweis“ zu definieren). Viele Beweissysteme gehen auch von „Axiomen“ aus und verwenden „Regeln“ (bei uns ist Modus Ponens die einzige Regel), um aus bisher Bewiesenem weitere Formeln zu beweisen. Im System des „natürlichen Schließens“ wird zum Beispiel das Deduktionstheorem eine Ableitungsregel; ebenso gibt es Systeme, in denen unser Generalisierungstheorem eine eigene Regel ist. Umgekehrt gibt es auch Systeme mit schwächeren Axiomen; statt wie wir alle Tautologien zu verwenden, kann man sich auf die drei Tautologien

(1) $\varphi \to (\psi \to \varphi)$,

(2) $[\varphi \to (\psi \to \sigma)] \to [(\varphi \to \psi) \to (\varphi \to \sigma)]$,

(3) $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$

beschränken; daraus lassen sich bereits mit MP alle Tautologien beweisen, die nur $\to, \neg$ enthalten. (Frege-Łukasiewicz Axiome).
Der Gentzensche Sequenzkalkül lässt als Axiome nur die allereinfachsten Tautologien zu, nämlich Formeln der Form $\varphi \to \varphi$, und verwendet dann eine Vielzahl von Regeln (wie unsere „Einführung des Existenzquantors“ in 7.21) um weitere Formeln abzuleiten.
Die Resolutionsmethode im Abschnitt 9 kann ebenfalls als ein formales System gesehen werden; im Resolutionskalkül interessiert man sich zwar nicht für den Beweis von allgemeingültige Formeln sondern für die Widerlegung von unerfüllbaren Formeln. Der Resolutionskalkül ist aber auch in dem Sinn zu unserem Kalkül äquivalent, dass die Widerlegung einer Formel $\neg\varphi$ (bzw. ihrer Skolemisierung, siehe 9.8) rein mechanisch in einen formalen Beweis von φ in unserem Kalkül übersetzt werden kann, und umgekehrt.

Im Satz 4.26 haben wir gesehen, dass die Aussagen $\Sigma \models \varphi$ und $\Sigma \cup \{\neg\varphi\} \models \bot$ äquivalent sind. Parallel dazu können wir jetzt die Methode des indirekten Beweises einführen:

Satz 7.17 (indirekter Beweis)**.** *Sei Σ eine Menge von geschlossenen Formeln. Dann gilt*

$$\Sigma \vdash \varphi \;\Leftrightarrow\; \Sigma \cup \{\neg\varphi\} \vdash \bot$$

Beweis. Wenn $\Sigma \vdash \varphi$, dann gilt auch $\Sigma \cup \{\neg\varphi\} \vdash \varphi$. Weiters gilt trivialerweise auch $\Sigma \cup \{\neg\varphi\} \vdash \neg\varphi$. Mit Hilfe der Tautologie $\varphi \to (\neg\varphi \to \bot)$ und MP erhält man $\Sigma \cup \{\neg\varphi\} \vdash \bot$. Wenn umgekehrt $\Sigma \cup \{\neg\varphi\} \vdash \bot$ gilt, so erhält man mit dem Deduktionstheorem $\Sigma \vdash \neg\varphi \to \bot$, und daraus mit der Tautologie $\vdash (\neg\varphi \to \bot) \to \varphi$ auch $\Sigma \vdash \varphi$. □

Satz 7.18 (Generalisierungstheorem)**.** *Sei Σ eine Menge von Sätzen (Formeln ohne freie Variable), φ Formel, c eine neue Konstante (die also weder in Σ noch in φ vorkommt) und x eine Variable. Dann sind die folgenden Aussagen äquivalent:*

1. $\Sigma \vdash \forall x\ \varphi$
2. $\Sigma \vdash \varphi$
3. $\Sigma \vdash \varphi(x/c)$

Beweis.
$1 \to 2$: Sei $\varphi_1, \ldots, \varphi_n$ ein formaler Beweis von $\Sigma \vdash \forall x\ \varphi(x)$. Dann ist

$$\varphi_1, \ldots, \varphi_n, \quad (\forall x\, \varphi) \to \varphi, \quad \varphi$$

ein Beweis von φ. Die vorletzte Formel in diesem Beweis ist ein Substitutionsaxiom, die letzte folgt mit MP.

$1 \to 3$: analog

$2 \to 3$: Wir betrachten einen Beweis von φ aus Σ. In jeder Zeile dieses Beweises ersetzen wir jedes freie Vorkommnis der Variablen x durch die neue Konstante c; die Überlegung, dass dadurch tatsächlich ein neuer formaler Beweis entsteht, überlassen wir dem Leser[16] und begnügen uns mit dem Hinweis darauf, dass nichtlogische Axiome in diesem Beweis die Variable x nicht frei enthalten können. Für jedes solche nichtlogische Axiom $\sigma \in \Sigma$ ist also $\sigma(x/c) = \sigma$.

$3 \to 1$: Sei $\varphi_1, \ldots, \varphi_n$ ein formaler Beweis von $\Sigma \vdash \varphi(x/c)$. Wir würden gerne daraus einen Beweis konstruieren, in dem die Formeln $\forall x\, \varphi_i(c/x)$ vorkommen, also insbesondere auch die Formel $\forall x\, \varphi(x/c)(c/x)$, die ja die Formel $\forall x\, \varphi$ ist. Dies könnte zu Schwierigkeiten führen, wenn eine der Substitutionen $\varphi_i(c/x)$ nicht erlaubt ist. Daher konstruieren wir zunächst einen Beweis, in dem die Formeln $\forall y\, \varphi_i(c/y)$ (für eine neue Variable y) alle vorkommen; damit haben wir $\forall y\, \varphi_n(c/y)$ und somit $\forall y\, \varphi(x/y)$ bewiesen. Diesen Beweis können wir nun leicht zu einem Beweis von $\forall x\, \varphi$ vervollständigen.
Sei also y eine Variable, die im Beweis $\varphi_1, \ldots, \varphi_n$ nicht vorkommt (weder frei noch gebunden).
Wir ersetzen jede Formel φ_i durch eine endliche Folge von Formeln, an deren Ende die Formel $\forall y\ \varphi_i(c/y)$ steht, und stellen sicher, dass die neue Folge wieder ein formaler Beweis (aus Σ) ist. Somit erhalten wir einen Beweis von $\forall y\, \varphi_n(c/y)$, also von der Formel $\forall y\, \varphi(x/y)$.

1. Fall: $\varphi_i \in \Sigma$. c kommt also in φ_i gar nicht vor. Es ist also $\varphi_i(c/y)$ dasselbe wie die Formel φ_i, und y kommt in dieser Formel nicht vor. Dann ersetzen wir φ_i durch

[16] Siehe Fußnote auf Seite 10

- $\varphi_i \to \forall y\, \varphi_i$ (Generalisierungsaxiom),
- φ_i (nichtlogisches Axiom),
- $\forall y\, \varphi_i$ (MP).

2. Fall: φ_i ist logisches Axiom. Dann sind auch $\varphi_i(c/y)$ und $\forall y\, \varphi_i(c/y)$ logische Axiome. (Leicht nachzuprüfen.)

3. Fall: φ_i folgt durch MP aus φ_{j_1} und φ_{j_2}. φ_{j_1} ist dann von der Form $A \to B$, wobei $A = \varphi_{j_2}$ und $\varphi_i = B$ ist. In unserem transformierten Beweis kommen also bereits die Formeln $\forall y\, \big((A \to B)(c/y)\big)$ und $\forall y\, (A(c/y))$ vor.

Dann ersetzen wir φ_i durch

- $\forall y\, (A(c/y) \to B(c/y)) \to (\forall y\, A(c/y) \to \forall y\, B(c/y))$ (Dist.Axiom),
- $\forall y\ A(c/y) \to \forall y\ B(c/y)$ (MP),
- $\forall y\ B(c/y)$ (MP).

Somit haben wir einen Beweis von $\forall y\, \varphi(x/y)$ gefunden. Kein Vorkommnis von y ist in $\varphi(x/y)$ durch einen Quantor $\forall x$ gebunden, weil ja nur freie Vorkommnisse von x ersetzt wurden. Daher ist die Substitution $\varphi(x/y)(y/x)$ sinnvoll, und liefert φ. Aus Satz 7.10 erhalten wir einen Beweis von

$$\vdash \forall y\, \varphi(x/y) \to \forall x\, \varphi;$$

zusammen mit dem Beweis von

$$\vdash \forall y\, \varphi(x/y)$$

und MP erhalten wir einen formalen Beweis von $\forall x\, \varphi$. □

Die Version $2 \Rightarrow 1$ des Generalisierungstheorems formalisiert den folgenden informellen Schluss:

> Wir haben aus den Voraussetzungen Σ die Eigenschaft $\varphi(x)$ bewiesen; über x haben wir aber dabei nichts vorausgesetzt, daher gilt $\forall x\, \varphi(x)$.

Die Version $3 \Rightarrow 1$ ist eine Variante von $2 \Rightarrow 1$:

> Um $\forall x\, \varphi(x)$ zu beweisen, wählen wir ein beliebiges x — nennen wir es c — und beweisen $\varphi(c)$.

Bemerkung 7.19. Ist beim Generalisierungstheorem die Voraussetzung der Geschlossenheit der Formeln aus Σ verletzt, so ist der Schluss $2 \Rightarrow 1$ im Allgemeinen nicht gültig.

Beispiel (halbformaler Beweis). Wir betrachten wieder die Formel, die wir bereits formal bewiesen haben. Statt $\vdash \forall x\ P(x) \to \forall y\ P(y)$ zeigen wir $\{\forall x\ P(x)\} \vdash \forall y\ P(y)$ (Deduktionstheorem) und statt $\{\forall x\ P(x)\} \vdash \forall y\ P(y)$ zeigen wir $\{\forall x\ P(x)\} \vdash P(u)$ (Generalisierungstheorem).

1. $\{\forall x\ P(x)\} \vdash \forall x\ P(x) \to P(u)$ (Substitutionsaxiom)
2. $\{\forall x\ P(x)\} \vdash \forall x\ P(x)$ (nichtlogisches Axiom, Voraussetzung)
3. $\{\forall x\ P(x)\} \vdash P(u)$ (MP(1,2))

Wir können auch die folgende Verschärfung des Generalisierungstheorems beweisen.

Satz 7.20 (Generalisierungstheorem, Variante)**.** *Seien Σ eine Menge von Formeln und φ eine Formel, wobei die Variable x möglicherweise frei in Σ und/oder φ vorkommt. Sei weiters c eine neue Konstante. Dann gilt:*

1. $\Sigma \vdash \varphi \ \Rightarrow\ \Sigma(x/c) \vdash \varphi(x/c)$.
2. $\Sigma(x/c) \vdash \varphi(x/c) \ \Rightarrow\ \Sigma \vdash \varphi$.
3. *Wenn überdies x nicht frei in den Formeln in Σ vorkommt, dann kann man aus $\Sigma \vdash \varphi$ auf $\Sigma \vdash \forall x\, \varphi$ schließen.*

Beweis. Für den Beweis von 1. verwenden wir das Generalisierungstheorem in seiner ursprünglichen Variante. Da dieses nur für geschlossene Formeln gilt, gehen wir folgendermaßen vor: Sei $\Sigma_0 \subseteq \Sigma$ endlich, sodass $\Sigma_0 \vdash \varphi$, also z.B. $\Sigma_0 := \{\psi_1, \ldots, \psi_n\}$. Es gilt also

$$\{\psi_1, \ldots, \psi_n\} \vdash \varphi$$

$$\{\psi_1, \ldots, \psi_{n-1}\} \vdash \psi_n \to \varphi$$

$$\vdots$$

$$\vdash \psi_1 \to \ldots \to \psi_n \to \varphi$$

Nun können wir das Generalisierungstheorem anwenden:

$$\vdash \psi_1(x/c) \to \ldots \to \psi_n(x/c) \to \varphi(x/c)$$

$$\vdots$$

$$\{\psi_1(x/c), \ldots, \psi_n(x/c)\} \vdash \varphi(x/c) \qquad n \text{ Mal MP und Ded.thm}$$

Der Beweis der Schlussfolgerung 3. ist nun leicht: Wieder dürfen wir annehmen, dass Σ endlich ist. Wir ersetzen alle freie Variable $y_1, \ldots, y_n$ (x kommt hier nicht vor) in Σ durch neue Konstante $c_1, \ldots, c_n$. Aus $\Sigma \vdash \varphi$

schließen wir also $\Sigma(\vec{y}/\vec{c}) \vdash \varphi(\vec{y}/\vec{c})$. In den Formeln der Menge $\Sigma(\vec{y}/\vec{c})$ gibt es nun keine freien Variablen. Nach dem Generalisierungstheorem gilt $\Sigma(\vec{y}/\vec{c}) \vdash \forall x\, \varphi(\vec{y}/\vec{c})$, und wegen Punkt 2 erhalten wir $\Sigma \vdash \forall x\, \varphi$.
(Alternativer Beweis: Man wiederhole den Beweis des Generalisierungstheorems und beachte, dass die Voraussetzung „alle Formeln in Σ sind geschlossen“ nur insofern eingeht, als wir verwenden, dass x in keiner dieser Formeln frei ist.) □

Wir bringen ein weiteres Beispiel für einen (halb-)formalen Beweis.

Satz 7.21 (Einführung des $\exists$-Quantors und des $\forall$-Quantors)**.** *Sei Σ eine Menge von Formeln und seien φ, ψ Formeln, wobei die Variable x weder in Σ noch in ψ frei vorkommt. Dann gilt:*

$$\textit{Wenn } \Sigma \vdash \psi \to \varphi, \textit{ dann } \Sigma \vdash (\psi \to \forall x\, \varphi).$$

sowie

$$\textit{Wenn } \Sigma \vdash \varphi \to \psi, \textit{ dann } \Sigma \vdash (\exists x\, \varphi) \to \psi.$$

Einführung des Allquantors. Wir nehmen $\Sigma \vdash \psi \to \varphi(u)$ an.
Es gilt daher auch $\Sigma \cup \{\psi\} \vdash \varphi(u)$. Nach der Variante des Generalisierungstheorems erhalten wir $\Sigma \cup \{\psi\} \vdash \forall x\, \varphi(x)$, und mit dem Deduktionstheorem $\Sigma \vdash (\psi \to \forall x\, \varphi(x))$. □

Existenzquantor. Aus $\Sigma \vdash \varphi(u) \to \psi$ schließen wir mit Hilfe von Tautologien $\Sigma \vdash \neg\psi \to \neg\varphi(u)$, daraus mit der gerade bewiesenen „Einführung des Allquantors“ $\Sigma \vdash \neg\psi \to \forall x\, \neg\varphi(x)$. Wiederum mit Hilfe von Tautologien erhalten wir $\Sigma \vdash \neg\forall x\, \neg\varphi(x) \to \psi$, und mit einem $\exists$-Axiom und weiteren Tautologien dann $\Sigma \vdash \exists x\, \varphi(x) \to \psi$. □

Bemerkung 7.22. Seien φ und ψ beliebige Formeln. Wenn $\Sigma \vdash \varphi \to \psi$, dann gilt auch $\forall x\, \varphi \to \psi$.
Wenn $\Sigma \vdash \psi \to \varphi$, dann auch $\Sigma \vdash \psi \to \exists x\, \varphi$.

Beweis. Die erste Behautung folgt leicht aus dem Substitionsaxiom $\forall x\, \varphi \to \varphi$. Für die zweite verwenden wir das Substitutionaxiom $\forall x\, \neg\varphi \to \neg\varphi$ sowie Tautologien und das Existenzaxiom, um $\vdash \varphi \to \exists x\, \varphi$ zu zeigen. □

Auf der nächsten Seite fassen wir einige Hilfsmittel, sogenannte „abgeleitete Regeln“ zusammen, die Abkürzungen von Beweisen erlauben. Der waagrechte Strich bedeutet immer: Aus formalen Beweisen der obenstehenden Behauptungen kann man in offensichtlicher[17] Weise formale Beweise für die untenstehenden Formeln generieren.

[17] Jedenfalls mit dem Wissen, das wir bereits haben — mit Deduktionstheorem, Generalisierungstheorem und möglicherweise auch mit Hilfe von Tautogien.

Zum Beispiel bedeutet $\dfrac{\Sigma \vdash \varphi_1 \quad \Sigma \vdash \varphi_2}{\Sigma \vdash \varphi_1 \wedge \varphi_2}$, dass man aus formalen Beweisen von φ_1 und φ_2 aus den Axiomen Σ einen formalen Beweis für $\varphi_1 \wedge \varphi_2$ gewinnen kann, nämlich indem man die Beweise hintereinander anschreibt und durch die Tautologie $\varphi_1 \to (\varphi_2 \to \varphi_1 \wedge \varphi_2)$, gefolgt von zwei Anwendungen von MP, vervollständigt.
Die hier angegebene Liste von Regeln ist nicht kanonisch. Statt der genannten Regel

$$\frac{\Sigma \vdash \varphi_1 \quad \Sigma \vdash \varphi_2}{\Sigma \vdash \varphi_1 \wedge \varphi_2}$$

könnten wir auch eine Regel

$$\frac{\Sigma \vdash \psi \to \varphi_1 \quad \Sigma \vdash \psi \to \varphi_2}{\Sigma \vdash \psi \to \varphi_1 \wedge \varphi_2}$$

angeben — wegen des Deduktionstheorems und der Regeln

$$\frac{\Sigma \vdash \varphi}{\Sigma \vdash \top \to \varphi} \qquad \frac{\Sigma \vdash \top \to \varphi}{\Sigma \vdash \varphi}$$

könnten wir die eine aus der anderen gewinnen.

8 Prädikatenlogik: Der Vollständigkeitssatz

Satz 8.1 (Vollständigkeitssatz, Version 1)**.** *Sei Σ eine Menge von geschlossen Formeln und φ eine Formel. Wenn $\Sigma \vDash \varphi$ gilt, dann auch $\Sigma \vdash \varphi$.*

Bemerkung 8.2. $\Sigma \vDash \varphi$ gilt genau dann, wenn $\Sigma \vDash \forall x\, \varphi$; dies folgt leicht aus der Definition von $\vDash$. Man kann aber auch zeigen (Generalisierungstheorem, Satz 7.18), dass $\Sigma \vdash \varphi$ zu $\Sigma \vdash \forall x\, \varphi$ äquivalent ist. Wir dürfen daher ohne Einschränkung der Allgemeinheit annehmen, dass φ eine geschlossene Formel ist.

8.1 Umformulierungen

Wenn wir den Vollständigkeitssatz in der beschriebenen Form direkt beweisen wollten, müssten wir auf Grundlage der Tatsache $\Sigma \vDash \varphi$ einen Beweis von φ aus den Axiomen Σ konstruieren. Wir haben aber schon gesehen, dass formale Beweise oft schwierig zu finden sind, wir formulieren daher den Vollständigkeitssatz in eine „modelltheoretische“ Version um; um diese modelltheoretische Version zu beweisen, müssen wir statt eines formalen Beweises ein Modell konstruieren.

Zunächst betrachten wir den Spezialfall, dass φ die Formel $\bot$ ist:

Satz 8.3 (Vollständigkeitssatz, Version 2)**.** *Sei Σ eine Menge von geschlossen Formeln. Wenn $\Sigma \vDash \bot$ gilt, dann auch $\Sigma \vdash \bot$.*

Stärkere Annahmen: $\dfrac{\Sigma \vdash \varphi}{\Sigma' \vdash \varphi}$ wenn $\Sigma \subseteq \Sigma'$

Modus Ponens: $\dfrac{\Sigma \vdash \varphi \to \psi \qquad \Sigma \vdash \varphi}{\Sigma \vdash \psi}$

Deduktion: $\dfrac{\Sigma \cup \{\varphi\} \vdash \psi}{\Sigma \vdash \varphi \to \psi}$

Konjunktion: $\dfrac{\Sigma \vdash \varphi_1 \qquad \Sigma \vdash \varphi_2}{\Sigma \vdash \varphi_1 \wedge \varphi_2}$

Disjunktion: $\dfrac{\Sigma \vdash \varphi_1 \to \psi \qquad \Sigma \vdash \varphi_2 \to \psi}{\Sigma \vdash \varphi_1 \vee \varphi_2 \to \psi}$

Indirekter Beweis: $\dfrac{\Sigma \cup \{\neg\varphi\} \vdash \bot}{\Sigma \vdash \varphi}$

Generalisierung: $\dfrac{\Sigma \vdash \varphi}{\Sigma \vdash \forall x\, \varphi}$ wenn x nicht frei in Σ

$\forall$-Einführung (schwer): $\dfrac{\Sigma \vdash \varphi \to \psi}{\Sigma \vdash \varphi \to \forall x\, \psi}$ wenn x nicht frei in $\Sigma \cup \{\varphi\}$

$\forall$-Einführung (leicht): $\dfrac{\Sigma \vdash \varphi(x/t) \to \psi}{\Sigma \vdash \forall x\, \varphi \to \psi}$ wenn $\varphi(x/t)$ sinnvoll ist

$\exists$-Einführung (schwer): $\dfrac{\Sigma \vdash \varphi \to \psi}{\Sigma \vdash \exists x\, \varphi \to \psi}$ wenn x nicht frei in $\Sigma \cup \{\psi\}$

$\exists$-Einführung (leicht): $\dfrac{\Sigma \vdash \varphi \to \psi(x/t)}{\Sigma \vdash \varphi \to \exists x\, \psi}$ wenn $\varphi(x/t)$ sinnvoll ist

Wir können leicht zeigen (als Folgerung aus dem Deduktionstheorem, Satz 7.15 bzw. 7.17), dass dieser Spezialfall des Vollständigkeitssatzes ausreicht, um auch Version 1 zu beweisen:

$$\Sigma \vDash \varphi \overset{4.26}{\Rightarrow} \Sigma \cup \{\neg\varphi\} \vDash \bot \overset{\text{Version 2}}{\Rightarrow} \Sigma \cup \{\neg\varphi\} \vdash \bot \overset{7.17}{\Rightarrow} \Sigma \vdash \varphi.$$

In 4.24 haben wir die (geschlossenen) Formeln in „erfüllbare“ und „unerfüllbare“ eingeteilt. Die Unerfüllbarkeit ist ein semantischer Begriff (der sich also auf die Bedeutung von Formeln bezieht). Das syntaktische Pendant dazu ist die Inkonsistenz.

Definition 8.4 (Konsistenz, Inkonsistenz)**.** Eine Menge Σ von Formeln heißt inkonsistent, wenn sich daraus $\bot$ ableiten lässt. Andernfalls heißt die Menge Σ konsistent.

Man beachte, dass Konsistenz bzw. Inkonsistenz „finitäre“ Eigenschaften sind. Das heißt, wenn eine Formelmenge Σ inkonsistent ist, dann gibt es eine endliche Teilmenge von Σ, die bereits inkonsistent ist; ein formaler Beweis von $\bot$ aus Σ kann nämlich nur endlich viele nichtlogische Axiome verwendet haben.

Satz 8.5. *Sei Σ eine Menge von Sätzen mit $\Sigma \vdash \bot$.*
Dann gilt $\Sigma \vdash \varphi$ für beliebiges φ.

Beweis. Die Aussage folgt aus der Anwendung des Modus Ponens zusammen mit der Tautologie $\Sigma \vdash \bot \to \varphi$. □

(Manchmal wird auch die Eigenschaft, dass aus Σ alle Formeln beweisbar sind, als Definition[18] der Inkonsistenz verwendet.)
Mit diesem neuen Vokabular besagt also die Version 2:

Satz 8.6 (Vollständigkeitssatz, Version 2')**.** *Jede* unerfüllbare *Menge von (geschlossenen) Formeln ist* inkonsistent*.*

Diese Form des Vollständigkeitssatzes verlangt noch immer, dass wir einen formalen Beweis (von $\bot$ aus der unerfüllbaren Menge Σ) konstruieren. Sie lässt sich aber leicht modelltheoretisch umformulieren:

Satz 8.7 (Vollständigkeitssatz, Version 3)**.** *Jede* konsistente *Menge von (geschlossenen) Formeln ist* erfüllbar*.*

Um Version 3 zu beweisen, müssen wir also für jede konsistente Menge Σ ein Modell finden, in welchem alle Formeln $\sigma \in \Sigma$ gelten. Aus der Version 3 folgt leicht die Version 2, und aus dieser mit dem Deduktionstheorem auch Version 1. Als Hilfsmittel für den Beweis des Vollständigkeitssatzes benötigen wir noch die Begriffe der „vollständigen Theorie“ und der „Henkin-Theorie“.

[18] Es gibt logische Systeme (schwächer als unseres), in welchen nicht alle Tautologien beweisbar sind. In einem System, in dem $\bot \to \psi$ nicht für alle Formeln beweisbar ist, heißt eine Menge Σ, die $\Sigma \vdash \psi$ für alle ψ erfüllt, „inkonsistent“; eine Menge Σ, die $\Sigma \vdash \bot$ erfüllt, ohne inkonsistent zu sein, heißt „parakonsistent“.

8.2 Vollständige Theorien

Definition 8.8 (Theorie)**.** Sei Σ eine Menge von geschlossenen Formeln. Dann heißt Σ auch Theorie.

Definition 8.9 (vollständige Theorie)**.** Sei Σ eine konsistente[19] Theorie und $\mathscr{L}$ eine prädikatenlogische Sprache. Dann heißt Σ vollständig (bzgl. $\mathscr{L}$), wenn für alle geschlossenen Formeln $\varphi \in \mathscr{L}$ entweder $\Sigma \vdash \varphi$ oder $\Sigma \vdash \neg\varphi$ gilt.

Bemerkung 8.10. Wenn Σ eine vollständige konsistente Theorie ist, dann gilt für alle geschlossenen Formeln φ und ψ:

- $\Sigma \vdash \varphi \wedge \psi$ genau dann, wenn $\Sigma \vdash \varphi$ und $\Sigma \vdash \psi$.
- $\Sigma \vdash \varphi \vee \psi$ genau dann, wenn $\Sigma \vdash \varphi$ oder $\Sigma \vdash \psi$.
- $\Sigma \vdash \neg\varphi$ genau dann, wenn $\Sigma \nvdash \varphi$.

Bemerkung 8.11. Die 3 Äquivalenzen in 8.10 lassen sich in der Form von 6 Implikationen schreiben; der Leser[20] möge sich selbst überlegen, welche dieser 6 Implikationen

- für alle Theorien Σ gelten,
- bzw. für alle konsistenten Theorien Σ gelten.

(Es sind 3 bzw 4 Implikationen.)

Definition 8.12 (informative Theorie)**.** Sei Σ eine Theorie und $\mathscr{L}$ eine prädikatenlogische Sprache. Dann heißt Σ informativ (bzgl. $\mathscr{L}$), wenn für je zwei Konstanten $c, d \in \mathscr{L}$ entweder $\Sigma \vdash c = d$ oder $\Sigma \vdash c \neq d$ gilt.

(„Informativ“ ist also eine schwächere Eigenschaft als Vollständigkeit. Der Name „informativ“ wird in der Literatur nicht verwendet; wir brauchen ihn nur für eine Übungsaufgabe: Jede informative Henkin-Theorie ist vollständig.)

Definition 8.13 (deduktiver Abschluss)**.** Sei Σ eine Theorie in der Sprache $\mathscr{L}$. Als deduktiven Abschluss von Σ bezeichnen wir die Menge

$$cl_{\vdash}(\Sigma) = \{\varphi \in \mathscr{L} : \varphi \text{ geschlossen}, \Sigma \vdash \varphi\}$$

[19] Eine inkonsistente Theorie Σ kann man insofern als vollständig bezeichnen, als ja $\Sigma \vdash \varphi$ für alle Formeln gilt, erst recht also die schwächere Bedingung, dass $\Sigma \vdash \varphi$ oder $\Sigma \vdash \neg\varphi$ gelten soll. Allerdings trifft z.B. die für vollständige Theorien charakteristische Eigenschaft „$\Sigma \nvdash \varphi$ genau dann, wenn $\Sigma \vdash \neg\varphi$“ nicht zu. Wir ignorieren die Frage, ob inkonsistente Theorien als vollständig zu bezeichnen sind, indem wir das Begriffspaar „vollständig/unvollständig“ immer nur auf konsistente Theorien anwenden.

[20] Siehe Fußnote auf Seite 10

Bemerkung 8.14. Für den deduktiven Abschluss gilt $cl_\vdash(cl_\vdash(\Sigma)) = cl_\vdash(\Sigma)$.

Satz 8.15. *Sei Σ eine Theorie in der Sprache $\mathscr{L}$. Dann gilt*

$$\Sigma \vdash \bot \;\Leftrightarrow\; \bot \in cl_\vdash(\Sigma) \;\Leftrightarrow\; \bot \in cl_\vdash(cl_\vdash(\Sigma)) \;\Leftrightarrow\; cl_\vdash(\Sigma) \vdash \bot,$$

also

$$\Sigma \textit{ konsistent} \;\Leftrightarrow\; cl_\vdash(\Sigma) \textit{ konsistent}\,.$$

Weiters gilt

$$\Sigma \textit{ erfüllbar} \;\Leftrightarrow\; cl_\vdash(\Sigma) \textit{ erfüllbar}\,,$$

denn jedes Modell von Σ ist auch Modell von $cl_\vdash(\Sigma)$.

Bemerkung 8.16. Manchmal wird eine konsistente Theorie Σ nur dann als vollständig bezeichnet, wenn für alle geschlossenen Formeln φ gilt: $\varphi \in \Sigma$ oder $\neg\varphi \in \Sigma$. Wir nennen dies „vollständig im engeren Sinn“. Eine konsistente Theorie Σ ist genau dann vollständig im weiteren Sinn (d.h., in unserem Sinn), wenn $cl_\vdash(\Sigma)$ im engeren Sinn vollständig ist.

Zwischen „vollständig im engeren Sinne“ und „vollständig im weiteren Sinne“ wird nicht immer scharf unterschieden; das macht meistens nichts, weil wir meistens nicht zwischen Theorien Σ und Σ', für die $cl_\vdash(\Sigma) = cl_\vdash(\Sigma')$ gilt, unterscheiden müssen; zum Beispiel ist Σ genau dann konsistent, wenn Σ' konsistent ist, ebenso ist jede Struktur $\mathfrak{M}$, die $\mathfrak{M} \vDash \Sigma$ erfüllt, auch ein Modell der Sätze in Σ'.

Satz 8.17. *Sei Σ eine konsistente Theorie, die im engeren Sinne vollständig ist. Dann gilt*

$$\Sigma = cl_\vdash(\Sigma), \qquad \textit{also} \quad \varphi \in \Sigma \;\Leftrightarrow\; \Sigma \vdash \varphi.$$

Beweis. Sei φ eine geschlossene Formel und es gelte $\varphi \in cl_\vdash(\Sigma)$. Dann gilt also $\Sigma \vdash \varphi$ und weil Σ konsistent ist, ist $\neg\varphi \in \Sigma$ unmöglich. Da Σ auch vollständig ist, folgt $\varphi \in \Sigma$. Die andere Richtung ist klar. □

Hilfssatz 8.18. *Sei Σ eine konsistente Theorie, σ eine geschlossene Formel. Dann ist zumindest eine der Theorien $\Sigma \cup \{\sigma\}$, $\Sigma \cup \{\neg\sigma\}$ konsistent.*
Anders ausgedrückt: Wenn $\Sigma \cup \{\sigma\}$ und $\Sigma \cup \{\neg\sigma\}$ beide inkonsistent sind, dann ist auch Σ inkonsistent.

Beweis. Aus $\Sigma \cup \{\neg\sigma\} \vdash \bot$ folgt laut 7.17:

$$\Sigma \vdash \sigma.$$

Analog kann man aus $\Sigma \cup \{\sigma\} \vdash \bot$ folgern, dass

$$\Sigma \vdash \neg\sigma.$$

Wenn also $\Sigma \cup \{\neg\sigma\}$ und $\Sigma \cup \{\sigma\}$ beide inkonsistent sind, dann kann man aus Σ sowohl σ also auch $\neg\sigma$ ableiten; daraus folgt leicht, dass Σ inkonsistent ist. ($\neg\sigma \to (\sigma \to \bot)$ ist nämlich Tautologie.) □

Satz 8.19. *Sei Σ eine konsistente Theorie einer abzählbaren Sprache $\mathscr{L}$. Dann gibt es eine vollständige konsistente Theorie $\bar{\Sigma} \supseteq \Sigma$.*

Beweis. Seien $\sigma_1, \sigma_2, \ldots$ alle Sätze aus $\mathscr{L}$. Wir definieren induktiv

$$\Sigma_0 := \Sigma$$

$$\Sigma_{n+1} := \begin{cases} \Sigma_n \cup \{\sigma_{n+1}\} & \text{falls } \Sigma_n \cup \{\sigma_{n+1}\} \text{ konsistent} \\ \Sigma_n \cup \{\neg\sigma_{n+1}\} & \text{falls } \Sigma_n \cup \{\sigma_{n+1}\} \text{ inkonsistent} \end{cases}$$

Falls Σ_n konsistent ist, so muss nach dem Hilfssatz 8.18 auch Σ_{n+1} konsistent sein.
Nun definiert man

$$\bar{\Sigma} := \bigcup_{n \in \mathbb{N}} \Sigma_n$$

Nach Konstruktion ist $\bar{\Sigma}$ vollständig. Weiters ist $\bar{\Sigma}$ konsistent, denn angenommen es gelte $\bar{\Sigma} \vdash \bot$. Dann gibt es also bereits endlich viele inkonsistente Formeln $\varphi_1, \ldots, \varphi_m \in \bar{\Sigma}$ und demnach ein $k \in \mathbb{N}$ mit $\{\varphi_1, \ldots, \varphi_m\} \subseteq \Sigma_k$ — im Widerspruch zur Konsistenz von Σ_k. □

Bemerkung 8.20. Der Beweis ist nicht effektiv. Es gibt nämlich keinen Algorithmus, der von jeder Formel φ feststellt, ob sie (mit Σ) konsistent ist oder nicht.

Bemerkung 8.21. Dieser Satz gilt auch für überabzählbare Sprachen, d.h.: Sei Σ eine konsistente Theorie in einer beliebigen Sprache. Dann gibt es eine vollständige konsistente Theorie $\bar{\Sigma} \subseteq \Sigma$.
Für den Beweis dieses Satzes in seiner allgemeinen Form kann man eine Wohlordnung aller Formeln verwenden. Alternativ kann man den Satz verwenden, dass es auf jeder Booleschen Algebra einen Ultrafilter gibt (siehe Übungen); letzter ist mit dem Lemma von Zorn beweisbar. Das Lemma von Zorn kann man auch direkt einsetzen: man zeigt, dass es eine (bezüglich $\subseteq$) maximale konsistente Obermenge von Σ gibt, und dass jede maximale konsistente Theorie auch vollständig sein muss.

8.3 Henkin-Theorien

Definition 8.22 (Henkin-Theorie)**.** Sei Σ eine Theorie in der Sprache $\mathscr{L}$. Dann heißt Σ Henkin-Theorie, wenn es für alle geschlossenen Formeln der Form $\exists x\, \varphi(x)$ ein Konstantensymbol $c \in \mathscr{L}$ mit $\Sigma \vdash (\exists x\, \varphi(x) \to \varphi(c))$ gibt.[21]

[21] Zur Erinnerung: in 4.4 haben wir vereinbart, dass die Formel $\exists x\, \varphi(x) \to \varphi(c)$ als $(\exists x\, \varphi(x)) \to \varphi(c)$ zu lesen ist.

Definition 8.23 (schwache Henkin-Theorie)**.** Sei Σ eine Theorie in der Sprache $\mathscr{L}$. Dann heißt Σ schwache Henkin-Theorie, wenn es für alle geschlossenen Formeln der Form $\exists x\, \varphi(x)$, die aus Σ beweisbar sind, ein Konstantensymbol $c \in \mathscr{L}$ gibt, sodass $\Sigma \vdash \varphi(c)$.
Wir sagen in so einem Fall, dass c die Formel $\exists x\, \varphi(x)$ *bezeugt*, und wir nennen c einen Zeugen für $\exists x\, \varphi(x)$. Jede Henkin-Theorie ist auch schwache Henkin-Theorie.

(Eigentlich interessieren uns schwache Henkin-Theorien, aber die schwache Henkin-Eigenschaft vererbt sich nicht von einer Theorie auf ihre Vervollständigung; die starke Henkin-Eigenschaft hingegen schon.)

Definition 8.24. Seien $\mathscr{L}_0 \subseteq \mathscr{L}_1$ prädikatenlogische Sprachen und sei weiters Σ eine Theorie in $\mathscr{L}_1$. Dann heißt Σ Henkin-Theorie bezüglich $\mathscr{L}_0$, wenn es zu jeder Formel der Form $\exists x\, \varphi(x)$ in $\mathscr{L}_0$ ein Konstantensymbol $c \in \mathscr{L}_1$ gibt, sodass $\Sigma \vdash \exists x\, \varphi(x) \to \varphi(c)$.

Satz 8.25. *Seien Σ_1, Σ_2 Theorien in der Sprache $\mathscr{L}$ und es gelte $\Sigma_1 \subseteq \Sigma_2$. Wenn Σ_1 Henkin-Theorie ist, dann ist auch Σ_2 Henkin-Theorie.*

Satz 8.26. *Sei Σ_0 eine konsistente Theorie in der Sprache $\mathscr{L}_0$. Dann gibt es*

1. *eine Sprache $\mathscr{L}_1 \supseteq \mathscr{L}_0$ und darin eine konsistente Theorie $\Sigma_1 \supseteq \Sigma_0$, sodass Σ_1 Henkin-Theorie bezüglich $\mathscr{L}_0$ ist.*

2. *eine Sprache $\mathscr{L}_H \supseteq \mathscr{L}_0$ und darin eine konsistente Theorie $\Sigma_H \supseteq \Sigma_0$, sodass Σ_H Henkin-Theorie ist.*

Beweis.
(1.) Sei Σ_0 konsistente Theorie in $\mathscr{L}_0$. Für jede geschlossene Formel der Form $\exists x\, \varphi(x)$ definieren wir eine neue Konstante $c_{x,\varphi}$ und setzen

$$\mathscr{L}_1 := \mathscr{L}_0 \cup \{c_{x,\varphi} : \exists x\, \varphi(x) \in \mathscr{L}_0\}$$

$$\Sigma_1 := \Sigma_0 \cup \{\exists x\, \varphi(x) \to \varphi(c_{x,\varphi}) : \exists x\, \varphi(x) \in \mathscr{L}_0\}$$

Dann ist Σ_1 Henkin-Theorie bezüglich $\mathscr{L}_0$; die Henkin-Eigenschaft folgt aus der Konstruktion, aber wir müssen auch zeigen, dass Σ_1 konsistent ist.
Es genügt zu zeigen, dass aus einer konsistenten Theorie Σ durch Hinzufügen einer einzigen Henkinformel $\exists x\, \varphi(x) \to \varphi(c_{x,\varphi})$ (mit einer neuen Konstanten $c_{x,\varphi}$) keine Inkonsistenz entstehen kann. Dann kann so eine Inkonsistenz nämlich auch nicht durch Hinzufügen einer beliebigen endlichen Menge von Henkinformeln entstehen, und somit auch nicht durch Hinzufügen einer beliebigen Menge von Henkinformeln (da ja jede inkonsistente Menge eine endliche inkonsistente Teilmenge enthält).

Sei also Σ eine konsistente Theorie, $\exists x\,\varphi(x)$ eine geschlossene Formel, und c eine neue Konstante. Wir behaupten, dass $\Sigma \cup \{\exists x\,\varphi(x) \to \varphi(c)\}$ konsistent ist. Wäre dies nicht der Fall, würde folgen

$$\begin{array}{rcll} \Sigma \cup \{\exists x\,\varphi(x) \to \varphi(c)\} & \vdash & \bot & \\ \Sigma & \vdash & \neg(\exists x\,\varphi(x) \to \varphi(c)) & \text{(DT)} \\ \Sigma & \vdash & \exists x\,\varphi(x) & \\ \Sigma & \vdash & \neg\varphi(c) & \\ \Sigma & \vdash & \forall x\,\neg\varphi(x) & \text{(GT)} \end{array}$$

Aus der dritten und letzten Ableitung würde sofort $\Sigma \vdash \bot$ folgen, im Widerspruch zur Annahme, dass Σ konsistent war.

(2.) Wir wiederholen die Konstruktion aus (1.) und finden für alle $n \in \mathbb{N}$ induktiv Sprachen $\mathscr{L}_n$ und konsistente Theorien Σ_n, sodass $\Sigma_{n+1} \supseteq \Sigma_n$ und Σ_{n+1} Henkin-Theorie bezüglich $\mathscr{L}_n$ ist. Wir definieren

$$\Sigma_H := \bigcup_{n\in\mathbb{N}} \Sigma_n$$

$$\mathscr{L}_H := \bigcup_{n\in\mathbb{N}} \mathscr{L}_n$$

Dann ist Σ_H konsistent und Henkin-Theorie in $\mathscr{L}_H$. □

8.4 Nochmals Substitution

Im Beweis des Vollständigkeitssatzes werden wir die folgenden beiden Lemmata brauchen:

Satz 8.27. *Sei s ein Term, x Variable, und sei t ein Term. Sei $\mathfrak{M}$ eine Struktur für die betrachtete Sprache, und sei b eine Belegung (aller relevanten Variablen).*
Wenn $b(x) = \bar{b}(t)$ ist, dann ist $\bar{b}(s(x/t)) = \bar{b}(s)$.

Satz 8.28. *Sei φ Formel, x Variable, und sei t ein Term, sodass die Substitution $\varphi(x/t)$ sinnvoll ist. Sei $\mathfrak{M}$ eine Struktur für die betrachtete Sprache, und sei b eine Belegung (aller relevanten Variablen).*
Wenn $b(x) = \bar{b}(t)$ ist, dann gilt $\mathfrak{M} \models \varphi(x/t)[b]$ genau dann, wenn $\mathfrak{M} \models \varphi[b]$.

8.5 Beweis des Vollständigkeitssatzes

Zusammen mit den vorigen Sätzen können wir damit einen weiteren wichtigen Satz folgern, der für den Beweis des Vollständigkeitssatzes maßgeblich ist:

Satz 8.29. *Sei Σ eine konsistente Theorie in der Sprache $\mathscr{L}$. Dann gibt es eine Sprache $\mathscr{L}^* \supseteq \mathscr{L}$ und darin eine konsistente Theorie $\Sigma^* \supseteq \Sigma$, sodass Σ^* Henkin-Theorie und vollständig ist.*

Beweis. Wir finden zunächst eine Sprache $\mathscr{L}^*$ und eine Henkin-Theorie Σ_H in dieser Sprache (sodass Σ_H konsistent ist und Σ enthält). Dann finden wir (weiterhin in der Sprache $\mathscr{L}^*$) eine vollständige konsistente Theorie $\Sigma^* \supseteq \Sigma_H$; Σ^* ist noch immer Henkin-Theorie. □

Für den Beweis des Vollständigkeitssatzes (in der Version 3, siehe 8.7) müssen wir zu jeder konsistenten Theorie ein Modell konstruieren. Der gerade bewiesene Satz zeigt, dass es genügt, dass jede konsistente vollständige Henkin-Theorie ein Modell hat.

Satz 8.30. *Sei Σ^* eine konsistente und vollständige Henkin-Theorie in der Sprache $\mathscr{L}^*$. Dann existiert ein Modell $\mathfrak{M}^* = (M, I)$, welches Σ^* erfüllt.*

Beweis. Es sei $\mathbb{T}$ die Menge aller geschlossenen Terme (d.h., Terme ohne freie Variablen) in $\mathscr{L}^*$. (Solche Terme gibt es, da es wegen der Henkineigenschaft zumindest ein Konstantensymbol in unserer Sprache gibt.)
Es gilt $\mathbb{T} \neq \emptyset$. Für $t_1, t_2 \in \mathbb{T}$ definieren wir die Äquivalenzrelation $\sim_{\Sigma^*}$ durch

$$t_1 \sim_{\Sigma^*} t_2 \;\Leftrightarrow\; \Sigma^* \vdash (t_1 = t_2)$$

Es sei $t/\sim_{\Sigma^*}$ die Äquivalenzklasse von t. Als unser gesuchtes Universum definieren wir

$$M := \mathbb{T}/\sim_{\Sigma^*}$$

Aus der Henkin Eigenschaft der Theorie Σ^* kann man folgern, dass es zu jedem geschlossenen Term t eine Konstante c_t gibt, sodass $t \sim_{\Sigma^*} c_t$.

[Warum? Sei t ein geschlossener Term, und x eine neue Variable. Dann ist $\exists x\, t = x$ eine geschlossene Formel, also gibt es wegen der Henkineigenschaft eine Konstante c, sodass $\exists x\, t = x \to t = c$ in Σ ist; wegen $\vdash \exists x\, t = x$ gilt $\Sigma \vdash t = c$.]

Wir müssen nun noch angeben, wie die Konstanten, Funktionen und Relationen durch das Modell $\mathfrak{M}^*$ interpretiert werden. Dazu setzen wir

- $c^{\mathfrak{M}^*} := c/\sim_{\Sigma^*}$
- $f^{\mathfrak{M}^*}(t_1/\sim_{\Sigma^*}, \ldots, t_n/\sim_{\Sigma^*}) := f(t_1, \ldots, t_n)/\sim_{\Sigma^*}$.
  (Beachten Sie, dass das f auf der linken Seite ein Funktionssymbol ist. $f^{\mathfrak{M}^*}$ ist die Interpretation, die wir definieren, also eine Funktion. Auf der rechten Seite ist $f(t_1, \ldots, t_n)$ ein Term unserer Sprache.)
- $(t_1/\sim_{\Sigma^*}, \ldots, t_n/\sim_{\Sigma^*}) \in R^{\mathfrak{M}^*} \;\Leftrightarrow\; \Sigma^* \vdash R(t_1, \ldots, t_n)$

Aus den Leibnizaxiomen (siehe Seite 47) ergibt sich, dass diese Definitionen nicht von der Auswahl der Repräsentanten der Äquivalenzklassen abhängen, also wohldefiniert sind. Ist t ein beliebiger geschlossener Term, so ergibt sich nun induktiv $t^{\mathfrak{M}^*} = t/\sim_{\Sigma^*}$.

Es bleibt zu zeigen, dass $\mathfrak{M}^* \vDash \Sigma^*$ gilt. Wir werden zeigen, dass für alle geschlossenen Formeln $\varphi \in \mathscr{L}^*$ gilt

$$(*)_\varphi \qquad \mathfrak{M}^* \vDash \varphi \;\Leftrightarrow\; \Sigma^* \vdash \varphi$$

Wir zeigen dies zunächst für Atomformeln.

- $\mathfrak{M}^* \vDash (t_1 = t_2) \;\Leftrightarrow\; \Sigma^* \vdash (t_1 = t_2)$
- $\mathfrak{M}^* \vDash R(t_1, \ldots, t_n) \;\Leftrightarrow\; \Sigma^* \vdash R(t_1, \ldots, t_n)$

Die erste Aussage beweist man so:

$$\mathfrak{M}^* \vDash (t_1 = t_2) \;\Leftrightarrow\; t_1^{\mathfrak{M}^*} = t_2^{\mathfrak{M}^*} \;\Leftrightarrow\; t_1/{\sim_{\Sigma^*}} \;=\; t_2/{\sim_{\Sigma^*}} \;\Leftrightarrow$$
$$\Leftrightarrow\; t_1 \sim_{\Sigma^*} t_2 \;\Leftrightarrow\; \Sigma^* \vdash (t_1 = t_2)$$

Die zweite Aussage erhält man durch einen ähnlichen Beweis.
Wir haben $(*)_\varphi$ nun für alle geschlossenen Atomformeln bewiesen. Mit Induktion über den Formelaufbau wollen wir zeigen, dass $(*)_\varphi$ für alle φ gilt. Dazu betrachten wir nun den Induktionsschritt „Junktoren“: Wenn $(*)_{\varphi_1}$ und $(*)_{\varphi_2}$ gilt, dann wollen wir zeigen, dass die folgenden Aussagen gelten:

- $\mathfrak{M}^* \vDash \varphi_1 \wedge \varphi_2 \;\Leftrightarrow\; \Sigma^* \vdash \varphi_1 \wedge \varphi_2$
- $\mathfrak{M}^* \vDash \varphi_1 \vee \varphi_2 \;\Leftrightarrow\; \Sigma^* \vdash \varphi_1 \vee \varphi_2$
- $\mathfrak{M}^* \vDash \neg\varphi_1 \;\Leftrightarrow\; \Sigma^* \vdash \neg\varphi_1$

Im Beweis verwenden wir Bemerkung 8.10. Wir zeigen nur die erste und die dritte Aussage:

$$\begin{array}{lcccccl} \mathfrak{M}^* \vDash \varphi_1 \wedge \varphi_2 & \Leftrightarrow & \mathfrak{M}^* \vDash \varphi_1 & \text{und} & \mathfrak{M}^* \vDash \varphi_2 & \Leftrightarrow & \\ & \Leftrightarrow & \Sigma^* \vdash \varphi_1 & \text{und} & \Sigma^* \vdash \varphi_2 & \Leftrightarrow & \Sigma^* \vdash \varphi_1 \wedge \varphi_2 \end{array}$$

$$\mathfrak{M}^* \vDash \neg\varphi \;\Leftrightarrow\; \mathfrak{M}^* \nvDash \varphi \;\Leftrightarrow\; \Sigma^* \nvdash \varphi \;\Leftrightarrow\; \Sigma^* \vdash \neg\varphi$$

Schließlich betrachten wir noch den Induktionsschritt „Quantoren“. Wir wollen zeigen: Wenn φ Formel mit (höchstens) einer freien Variablen x ist, und $(*)_{\varphi(x/c)}$ für alle Konstanten c gilt[22], dann gelten auch $(*)_{\forall x\,\varphi}$ und $(*)_{\exists x\,\varphi}$. Gestützt auf unsere Induktionsannahme

(a) $(*)_{\varphi(x/c)}$ gilt für alle Konstanten c

beweisen wir nun Folgendes:

(b) $(*)_{\neg\varphi(x/c)}$ für alle Konstanten c.

(c) $\mathfrak{M}^* \vDash \exists x\,\varphi(x) \;\Leftrightarrow\; \Sigma^* \vdash \exists x\,\varphi(x)$

(d) $\mathfrak{M}^* \vDash \exists x\,\neg\varphi(x) \;\Leftrightarrow\; \Sigma^* \vdash \exists x\,\neg\varphi(x)$

(e) $\mathfrak{M}^* \vDash \forall x\;\varphi(x) \;\Leftrightarrow\; \Sigma^* \vdash \forall x\;\varphi(x)$

[22] Beachte, dass die Substitution $\varphi(x/c)$ immer sinnvoll ist, und dass $\varphi(x/c)$ eine geschlossene Formel ist.

Beweis von (b)

Siehe obigen Induktionsschritt „Junktoren“.

Beweis von (c)

Die eine Richtung folgt aus der Definition unseres Modells, für die zweite verwenden wir die Henkin-Eigenschaft von Σ^*:

- Wenn $\mathfrak{M}^* \vDash \exists x\, \varphi(x)$, dann gibt es eine Belegung b (der Variablen x), sodass $\mathfrak{M}^* \vDash \varphi\,[b]$. $b(x)$ ist eine Klasse $t/{\sim_{\Sigma^*}}$, wobei t ein geschlossener Term ist. (Nach einer oben gemachten Bemerkung dürfen wir sogar annehmen, dass t ein Konstantensymbol ist.)

  Es gilt also $\mathfrak{M}^* \vDash \varphi\,[b]$. Nun ist $b(x) = t/{\sim_{\Sigma^*}} = t^{\mathfrak{M}} = \bar{b}(t)$, also gilt nach Satz 8.28: $\mathfrak{M}^* \vDash \varphi(x/t)[b]$, somit:

  $$\mathfrak{M}^* \vDash \varphi(x/t)$$

  Nach Induktionsvoraussetzung also: $\Sigma^* \vdash \varphi(x/t)*$, daher $\Sigma^* \vdash \exists x\, \varphi$.

- Nehmen wir nun $\exists x\, \varphi \in \Sigma^*$ an. Wegen der (schwachen) Henkin-Eigenschaft der Theorie Σ^* können wir ein Konstantensymbol c finden, sodass $\exists x\, \varphi \to \varphi(x/c)$ aus Σ^* beweisbar ist. Daher ist auch $\varphi(x/c)$ aus Σ^* beweisbar.

  Nach Induktionsvoraussetzung gilt also $\mathfrak{M} \vDash \varphi(x/c)$. Da die Implikation $\varphi(x/c) \to \exists x\, \varphi$ allgemeingültig ist, muss auch $\mathfrak{M} \vDash \exists x\, \varphi$ gelten.

Beweis von (d)

Analog zu (c).

Beweis von (e)

Wir verwenden die Allgemeingültigkeit der Formel $\forall x\, \varphi \;\leftrightarrow\; \neg\exists x\, \neg\varphi$. Es gilt also $\mathfrak{M} \vDash \forall x\, \varphi$ genau dann, wenn $\mathfrak{M} \vDash \neg\exists x\, \neg\varphi$; weiters gilt $\Sigma^* \vdash (\forall x\, \varphi)$ genau dann, wenn $\Sigma^* \vdash (\neg\exists x\, \neg\varphi)$. Nun gilt:

$$\mathfrak{M} \vDash \neg\exists x\, \neg\varphi \;\Leftrightarrow\; \mathfrak{M} \nvDash \exists x\, \neg\varphi \;\Leftrightarrow^{(c)}\; \Sigma^* \nvdash (\exists x\, \neg\varphi) \;\Leftrightarrow\; \Sigma^* \vdash (\neg\exists x\, \neg\varphi)$$

□

Satz 8.31 (Vollständigkeitssatz, Zusammenfassung)**.** *Sei Σ eine Theorie in einer höchstens abzählbaren prädikatenlogischen Sprache $\mathscr{L}$ und sei φ eine Formel. Dann gelten die folgenden Äquivalenzen:*

1. $\Sigma \vDash \varphi \;\Leftrightarrow\; \Sigma \vdash \varphi$
2. *Σ unerfüllbar* $\Leftrightarrow$ *Σ inkonsistent*

3. Σ *erfüllbar* $\Leftrightarrow$ Σ *konsistent*

Links steht immer ein semantische Begriff, rechts ein syntaktischer.

Beweis. Nach dem bisher Erwähnten reicht es zu zeigen, dass jede konsistente Theorie ein Modell hat. Dies ist mit Hilfe der vorigen Sätze nun nicht mehr schwer. Sei also Σ eine konsistente Theorie in der prädikatenlogischen Sprache $\mathscr{L}$. Die Vorgangsweise ist die folgende:

1. Wir finden eine Sprache $\mathscr{L}^* \supseteq \mathscr{L}$ und darin eine konsistente, vollständige Henkin-Theorie $\Sigma^* \supseteq \Sigma$.
2. Wir finden ein Modell $\mathfrak{M}^*$, welches die Theorie Σ^* erfüllt.
3. Wir zeigen, dass auch Σ durch ein Modell $\mathfrak{M}$ erfüllt wird, welches aus $\mathfrak{M}^*$ durch Reduktion hervorgeht.

Punkt 1 und 2 sind schon erledigt, Punkt 3 folgt aus der Implikation

$$\mathfrak{M}^* \vDash \Sigma^* \supseteq \Sigma \;\Rightarrow\; \mathfrak{M}^* \restriction \mathscr{L} \vDash \Sigma$$

□

Bemerkung 8.32. Die Voraussetzung der Abzählbarkeit der Sprache $\mathscr{L}$ ist nicht notwendig, aber für unsere Beweisführung nützlich.

Bemerkung 8.33. Für abzählbare Sprachen erhalten wir aus dem Beweis des Vollständigkeitssatzes das folgende Korollar:
Sei Σ eine konsistente Theorie. Dann hat Σ ein Modell, welches endlich oder abzählbar unendlich ist.

Als Anwendung des Vollständigkeitssatzes beweisen wir den „Kompaktheitssatz“:

Satz 8.34. *Sei* Σ *eine Menge von Sätzen. Dann sind die folgenden Aussagen äquivalent:*

(syn) Σ *ist konsistent.*

(syn-e) Jede endliche Teilmenge von Σ *ist konsistent.*

(sem) Σ *ist erfüllbar.*

(sem-e) Jede endliche Teilmenge von Σ *ist erfüllbar.*

Die Implikation (sem-e) $\Rightarrow$ (sem) heißt „Kompaktheitssatz“ der Prädikatenlogik. Der Beweis ist nun leicht:

- „(sem) $\Rightarrow$ (sem-e)“ ist trivial.
- „(sem-e) $\Rightarrow$ (syn-e)“ ist einfach „Soundness“.

- „(syn-e) $\Rightarrow$ (syn)“ gilt, weil jeder formale Beweis von $\bot$ aus Σ nur endlich viele Formeln aus Σ verwendet.
- „(syn) $\Rightarrow$ (sem)“ ist der Vollständigkeitssatz.

Als Anwendung des Kompaktheitssatzes beweisen wir die Existenz von „Nonstandardmodellen“.

Definition 8.35. Wir betrachten die Sprache $\mathscr{L}$ mit den Symbolen $+,\cdot,\leq$, 0, 1 (oder bei Bedarf auch noch mit Symbolen für weitere Funktionen auf den natürlichen Zahlen, wie Exponentiation, modulo, etc.). Mit

$$\mathbb{N} = (\mathbb{N}, +, \cdot, \leq, 0, 1)$$

bezeichnen wir die Struktur der natürlichen Zahlen mit den üblichen Funktionen. Sei $\Sigma = Th(\mathbb{N})$ die Theorie dieses Modells, d.h. Σ sei die Menge aller geschlossenen Formeln φ, die in $\mathbb{N}$ gelten.

Satz 8.36. *Es gibt eine (sogar abzählbare) Struktur $\mathfrak{M}$, die $\mathfrak{M} \models Th(\mathbb{N})$ erfüllt, die nicht isomorph zu $\mathbb{N}$ ist. (Jede solche Struktur nennen wir ein „Nonstandardmodell“ der natürlichen Zahlen.)*

Beweis. Wir betrachten in einer um ein Konstantensymbol c erweiterten Sprache die Theorie $\Sigma' := \Sigma \cup \{\, 0 \neq c, 1 \neq c, 1+1 \neq c, 1+1+1 \neq c, \dots \}$. Diese Theorie ist erfüllbar, weil jede endliche Teiltheorie erfüllbar ist. (Endliche Teiltheorien lassen sich sogar in einer Expansion des Standardmodells $\mathbb{N}$ realisieren, indem man die Interpretation von c einfach groß genug wählt.) Sei nun $\mathfrak{M}'$ ein Modell von Σ', und sei $\mathfrak{M}$ die Reduktion von $\mathfrak{M}'$ auf die alte Sprache (ohne c). Offensichtlich erfüllt $\mathfrak{M}$ die Theorie Σ.
$\mathfrak{M}'$ und $\mathfrak{M}$ haben dasselbe Universum; sei $m^* := c^{\mathfrak{M}'}$. Dieses Element liegt also im Universum $\mathfrak{M}$, kann aber nicht im Wertebereich eines Homomorphismus $h : \mathbb{N} \to \mathfrak{M}$ liegen, da so ein Homomorphismus ja $0 \in \mathbb{N}$ auf $0 = \underset{\cdot}{0}^{\mathfrak{M}} = \underset{\cdot}{0}^{\mathfrak{M}'}$ abbilden muss, $1 \in \mathbb{N}$ auf $\underset{\cdot}{1}^{\mathfrak{M}} = \underset{\cdot}{1}^{\mathfrak{M}'}$, etc., und keines dieser Elemente ist gleich $c^{\mathfrak{M}'}$. Daher gibt es keinen Isomorphismus zwischen $\mathbb{N}$ und $\mathfrak{M}$. □

Bemerkung 8.37. Das Modell $\mathfrak{M}$ erfüllt **alle** geschlossenen Formeln die in $\mathbb{N}$ gelten, insbesondere auch alle Induktionsaxiome und alle Verlaufsinduktionsaxiome.

Eine Eigenschaft, die die Theorie der natürlichen Zahlen nicht hat, ist also folgende:

Definition 8.38 (kategorische Theorie)**.** Eine konsistente Theorie Σ heißt kategorisch, wenn alle Modelle von Σ zueinander isomorph sind.

Satz 8.39. *Sei Σ eine Theorie in der prädikatenlogischen Sprache $\mathscr{L}$. Wenn Σ ein unendliches Modell hat, dann ist Σ nicht kategorisch.* [23]

8.6 Berechenbarkeit, Entscheidbarkeit, Axiomatisierbarkeit

Wir betrachten eine fixes endliches „Alphabet“ von Zeichen; mit STRING bezeichnen wir die Menge aller endlichen Zeichenfolgen über diesem Alphabet. (Wenn das Alphabet nur aus einem Zeichen besteht, dann ist STRING in kanonischer Weise zu den natürlichen Zahlen äquivalent.)

Definition 8.40 (Berechenbarkeit)**.** Eine Funktion $f : \mathbb{N} \to \mathbb{N}$ (oder alternativ: $f :$ STRING $\to$ STRING, oder $f :$ STRING $\to \mathbb{N}$) heißt berechenbar, wenn es einen Algorithmus gibt, der f in endlicher Zeit berechnet. (D.h., der Algorithmus bekommt als Eingabe eine natürliche Zahl oder einen String x, und gibt nach endlich vielen Schritten den Wert $f(x)$ aus.)
Berechenbare Funktionen heißen auch *rekursive* Funktionen.[24]

(Dies ist eine informelle Definition, die aber auch präzisiert werden kann — Genaueres findet man unter den Stichworten primitiv rekursive Funktion, μ-rekursive Funktion, Turing-Maschine.)

Definition 8.41 (Entscheidbarkeit)**.** Eine Menge $A \subseteq \mathbb{N}$ (oder alternativ: $A \subseteq$ STRING) heißt entscheidbar, wenn ihre charakteristische Funkion χ_A berechenbar ist.

Beispiele. Die Mengen aller Formeln, aller logischen Axiome oder aller formalen Beweise (as $\emptyset$) sind entscheidbar. Jede endliche Menge ist entscheidbar.

Die Familie der entscheidbaren Mengen bildet eine Boolesche Unteralgebra der Potenzmenge von $\mathbb{N}$ bzw. der Potenzmenge von STRING. Da es aber nur abzählbar viele Algorithmen gibt, gibt es auch nur abzählbar viele entscheidbare Mengen.

Definition 8.42 (Berechenbarkeit partieller Funktionen)**.** Eine (möglicherweise partielle) Funktion $f : \mathbb{N} \to \mathbb{N}$ (oder alternativ: $f :$ STRING $\to$ STRING oder $f :$ STRING $\to \mathbb{N}$) heißt berechenbar[25], wenn es einen Algorithmus gibt, der $f(x)$ berechnet, falls $f(x)$ definiert ist, und sonst nicht terminiert. (Das heißt: Für jede Eingabe x gilt: Wenn $f(x)$ definiert ist,

[23] Da es also in diesem Sinne keine kategorischen Theorien gibt, die unendliche Modelle haben, liegt eine verfeinerte Version dieses Begriffes nahe. Eine Theorie heißt $\aleph_0$-kategorisch, wenn alle abzählbaren Modelle der Theorie isomorph sind; ähnlich definiert man κ-Kategorizität für andere unendliche Kardinalzahlen κ.
Nach Satz 8.36 folgt, dass $Th(\mathbb{N})$ nicht einmal $\aleph_0$-kategorisch ist.

[24] Der Name rührt daher, dass berechenbare Funktionen mit Hilfe von rekursiven Definition aus einfacheren berechenbaren Funktionen aufgebaut werden können.

[25] Solche Funktionen nennt man auch *partiell rekursive* Funktionen (statt genauer „partielle Funktionen, die rekursiv=berechenbar sind“).

dann liefert der Algorithmus diesen Wert nach endlicher Zeit. Wenn x eine natürliche Zahl bzw. ein String ist, der bzw. die nicht im Definitionsbereich von f liegt, dann hält der Algorithmus nicht.)

Definition 8.43 (Semi-Entscheidbarkeit)**.** Eine Menge $A \subseteq \mathbb{N}$ (oder alternativ: $A \subseteq \text{STRING}$) heißt *semi-entscheidbar* (oder auch „rekursiv aufzählbar“[26]), wenn ihre „partielle charakteristische Funktion $\tilde{\chi}_A$“ berechenbar ist, wobei wir $\tilde{\chi}_A$ so definieren:

$$\tilde{\chi}_A(x) := \begin{cases} 1 & \text{falls } x \in A \\ \text{undef} & \text{sonst} \end{cases}$$

Beispiel. Die Menge $\{\varphi : \vdash \varphi\}$ ist semi-entscheidbar. Wir können nämlich einen Algorithmus angeben, der bei Eingabe φ systematisch alle möglichen Beweise daraufhin absucht, ob φ in ihnen auftaucht, und in diesem Fall 1 ausgibt. Bei Eingabe einer beweisbaren Formel gibt dieser Algorithmus sicher 1 aus, bei Eingabe einer unbeweisbaren Formel hält dieser Algorithmus nicht.
Man kann aber zeigen, dass die Menge $\{\varphi : \vdash \varphi\}$ nicht entscheidbar ist (wenn die zugrunde liegende Sprache zumindest ein zweistelliges Relationssymbol abgesehen von der Gleichheit enthält).

Ohne Beweis geben wir die folgenden Sätze an, die die Beziehung zwischen den Begriffen „berechenbar“, „entscheidbar“ und „semi-entscheidbar“ beleuchten.

Satz 8.44. *$A \subseteq \mathbb{N}$ ist genau dann entscheidbar, wenn sowohl A als auch $\mathbb{N} \setminus A$ semi-entscheidbar sind.*
(Analoges gilt für $A \subseteq$ STRING.)

Satz 8.45. *Für eine Menge $A \subseteq \mathbb{N}$ sind die folgenden Aussagen äquivalent:*

1. *A ist semi-entscheidbar.*
2. *Es gibt eine partiell berechenbare Funktion $f : \mathbb{N} \to \mathbb{N}$, sodass A der Definitionsbereich von f ist.*
3. *Es gibt eine entscheidbare Menge $B \subseteq \mathbb{N} \times \mathbb{N}$, sodass A die Projektion von B ist: $A = \{n : \exists k\,(n, k) \in B\}$.*
4. *Es gibt eine entscheidbare Menge $B \subseteq \mathbb{N}$ und eine berechenbare (totale) Funktion $f : \mathbb{N} \to \mathbb{N}$, sodass $A = f[B]$.*
5. *$A = \emptyset$ oder es gibt eine berechenbare (totale) Funktion $f : \mathbb{N} \to \mathbb{N}$, sodass $A = f[\mathbb{N}]$. (Diese Eigenschaft motiviert den Namen „aufzählbar“, weil f eben eine Aufzählung von A ist.)*

[26] auf Englisch „recursively enumerable“ oder oft nur „r.e.“, in neuerer Zeit auch „computationally enumerable“ oder „c.e.“

8.7 Axiomensysteme

Definition 8.46 (Axiomensystem)**.** Ein Axiomensystem in der prädikatenlogischen Sprache $\mathscr{L}$ ist eine *entscheidbare* Menge von geschlossenen Formeln.

Diese Definition ist nicht kanonisch. Manchmal werden auch beliebige Mengen von geschlossenen Formeln als Axiomensystem bezeichnet; in diesem Fall wäre ein Axiomensystem dann einfach das, was wir als „Theorie“ bezeichnet haben. (Allerdings gibt es auch hier einen zumindest psychologischen Unterschied: Theorien identifiziert man gerne mit ihrem deduktiven Abschluss, während es bei Axiomensysteme wirklich auf die Menge selbst ankommt, die man auch gerne klein hält, am liebsten endlich.)
Oft verlangt man von einem Axiomensystem auch explizit Konsistenz.
Wir nennen ein Axiomensystem redundant, wenn sich eines der Axiome aus den anderen beweisen lässt. Für jedes endliche Axiomensystem A lässt sich offensichtlich ein Untersystem $A' \subseteq A$ finden, welches nicht redundant ist, aber den selben deduktiven Abschluss hat (indem man einfach eine minimale Teilmenge mit dem selben Abschluss findet); dies ist für unendliche Axiomensysteme nicht immer möglich.[27]
Informell unterscheiden wir 2 Arten von Axiomensystemen: „Klassische“ Axiomensysteme versuchen, eine vorgegebene Struktur — wie die Punkte der Ebene, die natürlichen Zahlen, oder alle Mengen — zu beschreiben.[28] „Moderne“ Axiomensysteme beschreiben eine ganze Klasse von Strukturen (Gruppen, Körper, etc.).

Beispiele.

- **klassische Axiomensysteme:** eukl. Geometrie, Peano-Axiome, ZFC
- **moderne Axiomensysteme:** Gruppenaxiome, Vektorraumaxiome

Um die Bedeutung des Vollständigkeitssatzes „$\vdash \varphi \;\Leftrightarrow\; \vDash \varphi$“ zu betonen, konstrastieren wir die Relation $\vDash$ mit einer Variante; für diese Variante kann es keinen Vollständigkeitssatz geben.
Wir betrachten eine beliebige Sprache $\mathscr{L}$, in der es zumindest ein zweistelliges Relationssymbol gibt.

Definition 8.47 (endliche Gültigkeit)**.** Eine Formel φ heißt endlich gültig, wenn für alle endlichen Modelle $\mathfrak{M}$ gilt: $\mathfrak{M} \vDash \varphi$. Wir schreiben in diesem Fall auch $\vDash_e \varphi$.

[27] Man kann aber ein Axiomensystem $\{\psi_1, \psi_2, \dots\}$ durch das äquivalente Axiomensystem $\{\psi_1, \psi_1 \to \psi_2, \psi_1 \wedge \psi_2 \to \psi_3, \dots\}$ ersetzen; letzteres lässt sich zu einem irredundanten System ausdünnen.

[28] Wegen Satz 8.39 reicht aber ein Axiomensystem in der erststufigen Logik nie aus, um eine einzige (unendliche) Struktur bis auf Isomorphie zu charakterisieren.

Satz 8.48 (Satz von Trakhtenbrot)**.** *Die Menge* $E^- := \{\varphi : \not\models_e \varphi\}$ *ist semi-entscheidbar, die Menge* $E^+ := \{\varphi : \models_e \varphi\}$ *aber nicht.*

Beweis. Wir skizzieren nur einen Beweis für den (viel leichteren) ersten Teil dieses Satzes, indem wir einen Algorithmus angeben, der $\tilde{\chi}_{E^-}$ berechnet:
Wir betrachten die Eingabe φ. Wir gehen systematisch alle endlichen $\mathscr{L}$-Strukturen durch: Es gibt (bis auf Isomorphie) nur endliche viele Strukturen mit 1 Element, endliche viele mit 2 Elementen, etc. Für jede dieser Strukturen $\mathfrak{M}$ überlegen wir, ob $\mathfrak{M} \models \varphi$ gilt; dazu müssen wir nur endlich viele Fälle überprüfen. Wenn wir ein $\mathfrak{M}$ finden, wo $\mathfrak{M} \models \varphi$ nicht gilt, gibt der Algorithmus 1 aus, sonst läuft er weiter. □

Die folgende Definition beschreibt eine abstrakte Eigenschaft unseres Ableitungsbegriffs $\vdash$.

Definition 8.49 (Ableitungsbegriff)**.** Wir betrachten Strings über einem fixen (endlichen) Alphabet.
Ein (berechenbarer) *Ableitungsbegriff* $\mid\!\sim$ besteht aus

1. einer (entscheidbaren) Menge von „Axiomen“;
2. einer (endlichen) Menge von „Regeln“, das sind (berechenbare) partielle Funktionen (beliebiger endlicher Stelligkeit) von den Strings in die Strings.

(Beispiel: die logischen Axiome, und die einzige zweistellige partielle Funktion MP.)

Definition 8.50. Sei $\mid\!\sim$ ein Ableitungsbegriff, Σ eine Menge von Strings. Eine formale Ableitung aus Σ ist eine endliche Folge von Strings, in der jeder vorkommende String entweder[29] ein Axiom ist, oder in Σ vorkommt, oder sich durch Anwendung einer Regel auf früher vorkommende Strings erhalten lässt.
Ein String φ heißt „aus Σ ableitbar“, wenn er in einer formalen Ableitung aus Σ vorkommt; wir schreiben in diesem Fall $\Sigma \mid\!\sim \varphi$. Statt $\emptyset \mid\!\sim \varphi$ schreiben wir nur $\mid\!\sim \varphi$.

Satz 8.51. *Sei* $\mid\!\sim$ *ein berechenbarer Ableitungsbegriff. Dann ist die Menge*

$$\{\varphi : \mid\!\sim \varphi\}$$

semi-entscheidbar.

Aus diesem Satz, zusammen mit dem Satz von Trakhtenbrot folgt nun, dass es keinen berechenbaren Ableitungsbegriff $\mid\!\sim$ gibt, der die Relation $\models_e$ beschreibt.
In diesem Sinne gilt also: Für $\models_e$ gibt es keinen Vollständigkeitssatz.

[29] Entweder–oder wird hier im nichtausschließenden Sinn verstanden.

Definition 8.52 (unendliche Gültigkeit)**.** Eine Formel φ heißt unendlich gültig, wenn für alle unendlichen Modelle $\mathfrak{M}$ gilt: $\mathfrak{M} \vDash \varphi$. Wir schreiben in diesem Fall auch $\vDash_u \varphi$.

Definition 8.53 (Axiomatisierbarkeit)**.** Eine Theorie Σ heißt axiomatisierbar, wenn es ein Axiomensystem Σ_0 gibt, sodass gilt

$$cl_{\vdash}(\Sigma) = cl_{\vdash}(\Sigma_0)$$

Beispiele. Die Menge $\{\varphi : \vDash_e \varphi\}$ ist nicht axiomatisierbar. Die Menge $\{\varphi : \vDash_u \varphi\}$ ist jedoch axiomatisierbar.

Man kann zeigen, dass eine Theorie Σ genau dann axiomatisierbar ist, wenn die Menge $cl_{\vdash}(\Sigma)$ semi-entscheidbar ist.

9 Prädikatenlogische Resolution

Sei $\Sigma \cup \varphi$ eine Menge von geschlossenen Formeln. Wie können wir entscheiden, ob $\Sigma \vDash \varphi$ gilt? Der Vollständigkeitssatz, der Kompaktheitssatz und das Deduktionstheorem liefern uns verschiedene Antworten auf diese Frage. Letzteres besagt, dass

$$\Sigma \vDash \varphi \;\Leftrightarrow\; \exists \sigma_1, \ldots, \sigma_n \in \Sigma : \vDash (\sigma_1 \wedge \ldots \wedge \sigma_n) \rightarrow \varphi$$

gilt. Daher wäre es praktisch zu wissen, wann eine Formel φ allgemeingültig ist, bzw. wann deren Negation $\neg\varphi$ unerfüllbar ist. Diese Überlegungen motivieren eine Methode, die wir bereits aus der Aussagenlogik kennen — die Resolutionsmethode.

Bemerkung 9.1. Wir treffen für das gesamte Kapitel die Vereinbarung, dass die Gleichheitsrelation nicht zugelassen ist. Dies vereinfacht einige Beweisführungen.

9.1 Pränexform

Definition 9.2 (Pränexform)**.** Wir definieren induktiv den Begriff der Pränexform für Formeln:

1. Jede quantorenfreie Formel ist in Pränexform.
2. Ist φ in Pränexform, so sind auch $\forall x\, \varphi$ und $\exists x\, \varphi$ in Pränexform.
3. Das sind alle.[30]

[30] Dies beschreibt wieder ein Induktionsprinzip.

Beispiele.
$\forall x_1\ \exists x_2\ \exists x_3\ \forall x_4\ \underbrace{(\ldots)}_{\text{„Matrix“}}$ ist in Pränexform.

$\forall x\ P(x) \to \forall x\ P(x)$ ist nicht in Pränexform.

Stellt man sich eine Pränexformel in einem Baumdiagramm vor, so ist also oben im Diagramm der prädikatenlogische Teil mit Quantoren zu finden, während darunter der aussagenlogische Teil mit diversen Junktoren folgt.

Satz 9.3. *Für jede Formel φ (mit den freien Variablen $u_1, \ldots, u_n$) existiert eine Formel φ^P in Pränexform sodass gilt:*

$$\vDash \varphi \leftrightarrow \varphi^P \qquad \textit{das heißt:}$$

$$\vDash \forall x_1 \ldots \forall x_n\ (\varphi(x_1, \ldots, x_n) \leftrightarrow \varphi^P(x_1, \ldots, x_n))$$

Beispiel (als Beweisskizze). Wir wandeln die Formel $\varphi := \forall x\ P(x) \to \forall y\ P(y)$ Schritt für Schritt in Pränexform um:

$$\varphi = \forall x\ P(x) \to \forall y\ P(y)\ \Leftrightarrow$$

$$\neg\forall x\ P(x) \vee \forall y\ P(y)\ \Leftrightarrow$$

$$\exists x\, \neg P(x) \vee \forall y\ P(y)\ \Leftrightarrow$$

$$\exists x\, (\neg P(x) \vee \forall y\ P(y))\ \Leftrightarrow$$

$$\exists x \forall y\ (\neg P(x) \vee P(y)) =: \varphi^P$$

Die letzten beiden Zeilen folgen aus den Äquivalenzen

$$(\exists x\, A(x)) \vee B\ \Leftrightarrow\ \exists x\, (A(x) \vee B)$$

$$(\forall x\ A(x)) \vee B\ \Leftrightarrow\ \forall x\ (A(x) \vee B)$$

(analog für Konjunktionen[31]), die immer dann gelten, wenn x in B nicht vorkommt. Man kann also die Pränexform einer Formel durch einen expliziten Algorithmus finden.

Definition 9.4 (Grundinstanz)**.** Sei φ eine Formel in Pränexform in den Variablen $x_1, \ldots, x_n$, die nur Allquantoren enthält. Unter einer Grundinstanz von φ versteht man jede Formel der Form $\varphi'(t_1, \ldots, t_n)$, wobei $t_1, \ldots, t_n$ geschlossene Terme sind und φ' der quantorenfreie Teil von φ ist.

[31] Achtung: $\exists x\, A(x) \to B$ ist zu $\exists x\, (A(x) \to B)$ im Allgemeinen nicht äquivalent! $\exists x\, A(x) \to B$ ist zu $(\neg\exists x\, A(x)) \vee B$ äquivalent, somit zu $\forall x\, \neg A(x) \vee B$ bzw. zu $\forall x \big[\neg A(x) \vee B\big]$ bzw. $\forall x \big[A(x) \to B\big]$. Hier sehen wir auch, warum Implikation ein komplizierterer Begriff als Konjunktion und Disjunktion ist; sie lässt sich nämlich als eine Formel mit einer versteckten Negation auffassen.

Beispiel. Wir betrachten die Formel φ

$$\forall x\ \forall y\ \underbrace{(P(x) \wedge \neg P(f(y)))}_{=:\ \varphi'}$$

Dann sind

$$\begin{array}{rcl} P(a) & \wedge & \neg P(f(a)) \\ P(a) & \wedge & \neg P(f(f(a))) \\ P(f(f(f(a)))) & \wedge & \neg P(f(f(f(a)))) \end{array}$$

Grundinstanzen von φ.

Sei nun $G(\varphi)$ die Menge aller Grundinstanzen einer Formel φ in Pränexform. Darin kommen höchstens abzählbar viele geschlossene Atomformeln vor (wobei wir an dieser Stelle daran erinnern, dass die Gleichheitsrelation in diesem Kapitel nicht betrachtet wird). Fasst man nun die Atomformeln als aussagenlogische Variable $p_1, p_2, \ldots$ auf, so erhält man eine Menge $\bar{G}(\varphi)$, die mit aussagenlogischer Resolution behandelt werden kann. Die Idee der prädikatenlogischen Resolution liegt nun nahe und wird durch den folgenden Satz charakterisiert, der jedoch nur den Spezialfall von $\exists$-quantorenfreien Formeln behandelt. Die anderen Fälle können jedoch mit einigen Hilfsüberlegungen auf den Satz von Herbrand zurückgeführt werden.

Satz 9.5 (von Herbrand, einfache Version[32])**.** *Sei φ eine prädikatenlogische Formel in Pränexform, die keine $\exists$-Quantoren enthält. Dann gilt*

$$\varphi \text{ (prädikatenlogisch) erfüllbar } \Leftrightarrow\ \bar{G}(\varphi) \text{ (aussagenlogisch) erfüllbar}$$

Beweis. [33] „$\Rightarrow$“: Es gelte $\mathfrak{M} \vDash \varphi$, d.h. φ sei erfüllbar. Dann gilt auch $\mathfrak{M} \vDash \gamma$, für alle Grundinstanzen $\gamma \in G(\varphi)$. Gesucht ist eine aussagenlogische Belegung b, sodass $\bar{b}(\gamma) = 1$ für alle $\gamma \in \bar{G}(\varphi)$ gilt. Für jede Atomformel $R(t_1, \ldots, t_n)$ definieren wir $b(R(t_1, \ldots, t_n))$ durch

$$b(R(t_1, \ldots, t_n)) := \begin{cases} 1 & \text{falls } \mathfrak{M} \vDash R(t_1, \ldots, t_n) \\ 0 & \text{sonst} \end{cases}$$

Dann gilt $\mathfrak{M} \vDash A \ \Rightarrow\ \bar{b}(A) = 1$ für jede geschlossene quantorenfreie Formel A, was man mit Induktion nach Formelaufbau beweisen kann; insbesondere gilt $\bar{b}(\gamma) = 1$ für alle $\gamma \in \bar{G}(\varphi)$.

„$\Leftarrow$“: Es sei $\bar{G}(\varphi)$ im aussagenlogischen Sinne erfüllbar und sei b eine passende Belegung. Wir müssen ein Modell $\mathfrak{M} = (M, I)$ finden, sodass $\mathfrak{M} \vDash \varphi$

[32] Üblicherweise wird erst der Satz 9.9 als der Satz von Herbrand bezeichnet

[33] Der Beweis dieses Satzes wird üblicherweise mit beweistheoretischen Mitteln geführt, in dem eine prädikatenlogische Inkonsistenz direkt in eine aussagenlogische transformiert wird. Wir folgen hier dem Geschmack des Vortragenden und wählen einen modelltheoretischen Zugang.

gilt. Für das Universum M wählen wir die Menge aller geschlossenen Terme und die Interpretation von Funktionen und Relationen definieren wir durch

- $f^{\mathfrak{M}}(t_1, \ldots, t_k) := f(t_1, \ldots, t_k)$ [34]
- $R^{\mathfrak{M}} := \{(t_1, \ldots, t_k) : b(R(t_1, \ldots, t_k)) = 1\}$

wobei $k \in \mathbb{N}$ die jeweilige Stelligkeit angibt. Dann gilt $\mathfrak{M} \vDash \varphi$, denn sei oBdA $\varphi := \forall x_1 \ldots \forall x_n \; \varphi'(x_1, \ldots, x_n)$, so liefert das Einsetzen von Elementen für $x_1, \ldots, x_n$ genau die Grundinstanzen von φ. □

9.2 Skolemisierung, Erfüllungsäquivalenz

Wir haben also das prädikatenlogische Problem, ob eine Formel φ unerfüllbar ist, zumindest für den Spezialfall von Formeln in Pränexform, die keine $\exists$-Quantoren enthalten, auf ein aussagenlogisches Problem zurückgeführt. Um auch den allgemeinen Fall abzudecken, müssen wir noch einige Hilfsüberlegungen treffen.

Bemerkung 9.6. $\exists$-quantorenfreie Formeln in Pränexform nennt man auch Formeln in Skolemform oder skolemisierte Formeln.

Definition 9.7 (Erfüllungsäquivalenz)**.** Seien φ, ψ Formeln. Wir nennen φ, ψ erfüllungsäquivalent, wenn entweder beide erfüllbar oder beide unerfüllbar sind (im Fall der Unerfüllbarkeit sind sie sogar äquivalent) und schreiben

$$\varphi \sim_{\vDash} \psi$$

Die Überlegung ist nun die folgende: Wenn wir zu jeder Formel φ eine erfüllungsäquivalente Formel φ^S in Skolemform finden können, so können wir auf diese den Satz von Herbrand (9.5) anwenden. Die Existenz sichert der folgende

Satz 9.8. *Zu jeder geschlossenen Formel φ in Pränexform kann man explizit*[35] *eine Formel φ^S (in einer möglicherweise erweiterten Sprache) finden, sodass φ^S in Skolemform ist (d.h. in Pränexform und $\exists$-quantorenfrei) und es gilt*

$$\varphi^S \sim_{\vDash} \varphi$$

[34] Auf der linken Seite dieser Definition steht der Wert, den man erhält, wenn man die k-stellige Funktion $f^{\mathfrak{M}}$ auf das k-Tupel $(t_1, \ldots, t_k)$ von Termen anwendet. Auf der rechten Seite steht ein einziger Term; diesen erhält man aus den Termen t_1, …, t_k, indem man das Symbol f davorschreibt.

[35] Jede Formel ist entweder erfüllbar oder unerfüllbar, also trivialerweise zu $\top$ oder zu $\bot$ erfüllungsäquivalent. Der Witz besteht aber darin, dass man durch den Skolemisierungsalgorithmus, also durch rein syntaktische Umformungen, eine erfüllungsäquivalente Formel finden kann, ohne schon *a priori* zu wissen, ob die vorliegende Formel erfüllbar ist.

Beispiel (als Beweisskizze).

1. $\exists x\, \varphi'(x) \;\sim_{\vDash}\; \varphi'(c)$,

   wobei c eine neue Konstante ist. Dieses Beispiel deckt jene Fälle ab, in denen die $\exists$-Quantoren vorne stehen.

2. $\forall x\ \exists y\, \varphi'(x,y) \;\sim_{\vDash}\; \forall x\ \varphi(x, f(x))$,

   wobei f ein neues Funktionssymbol ist. Gilt nämlich $\mathfrak{M} \vDash \forall x\, \exists y\, \varphi'(x,y)$ und ist $\mathfrak{M} = (M, I)$ oBdA abzählbar (dies ergibt sich aus dem Beweis des Vollständigkeitssatzes), so kann man M als Teilmenge von $\mathbb{N}$ auffassen. Für ein passendes Modell $\mathfrak{N}$ mit $\mathfrak{N} \restriction \mathscr{L} = \mathfrak{M}$ definiert man nun $f^{\mathfrak{N}}(m) := \min\{a \in \mathbb{N} : \mathfrak{M} \vDash \varphi'(m,a)\}$ für $m \in M$. Dann gilt $\mathfrak{N} \vDash \varphi'(x, f(x))$.

3. $\forall x_1\, \forall x_2\ \exists y\, \varphi'(x_1, x_2, y) \;\sim_{\vDash}\; \forall x_1\, \forall x_2\ \varphi(x_1, x_2, f(x_1, x_2))$,

   Analog.

Damit sind auch jene Fälle abgedeckt, in denen $\forall$-Quantoren vor $\exists$-Quantoren stehen.

Zusammenfassend:

Satz 9.9 (von Herbrand)**.** *Sei ψ eine geschlossene Formel; dann kann man (effektiv) eine Formel φ^H angeben, die zu $\varphi = \neg\psi$ erfüllungsäquivalent ist, und in Skolemform vorliegt (Pränexform ohne Existenzquantoren). Die folgenden Aussagen sind dann äquivalent:*

- *ψ (bzw. $\neg\varphi$) ist allgemeingültig (=gilt in allen Modellen)*
- *φ ist unerfüllbar (=gilt in keinem Modell)*
- *φ^H ist unerfüllbar*
- *$G(\varphi^H)$, die Menge der Grundinstanzen von φ^H, ist aussagenlogisch unerfüllbar (atomare Formeln werden als aussagenlogische Variable betrachtet)*
- *Aus $G(\varphi^H)$ ist — nach Umformung auf KNF — durch aussagenlogische Resolution ein Widerspruch (d.h., die leere Klausel) herleitbar*

Wir können nun prädikatenlogische Resolution auf beliebige Formeln anwenden. Um die abstrakt beschriebene Vorgangsweise zu verdeutlichen, geben wir einige

Beispiele. 1. Wir wollen überprüfen, ob die Formel $\psi := \exists x\,(\exists y\,P(y) \to P(x))$ allgemeingültig ist. Stattdessen prüfen wir, ob deren Negation unerfüllbar ist:

$$\varphi = \neg\psi = \neg\exists x\,(\exists y\,P(y) \to P(x)) \;\Leftrightarrow$$

$$\forall x\;\neg(\exists y\,P(y) \to P(x)) \;\Leftrightarrow$$

$$\forall x\;(\exists y\,P(y) \wedge \neg P(x)) \;\Leftrightarrow$$

$$\forall x\;\exists y\,(P(y) \wedge \neg P(x)) \;\sim_{\vDash}$$

$$\forall x\;(P(f(x)) \wedge \neg P(x)) =: \varphi^S$$

Daraus erhalten wir durch $x \mapsto a$ und $x \mapsto f(a)$ die Grundinstanzen

$$\{\underbrace{P(f(a))}_{p_1} \wedge \underbrace{\neg P(a)}_{\neg p_2}, \underbrace{P(f(f(a)))}_{p_3} \wedge \underbrace{\neg P(f(a))}_{\neg p_1}\} \subseteq G(\varphi)$$

Fassen wir nun die Atomformeln, wie angedeutet, als aussagenlogische Variable auf, so können wir Resolution anwenden.

$$\bar{G}(\varphi) \supseteq \{\{p_1\};\{\neg p_2\};\{p_3\};\{\neg p_1\}\} \overset{Res}{\longmapsto} \{\{p_1\};\{\neg p_2\};\{p_3\};\{\neg p_1\};\{\}\}$$

Die letzte Menge enthält die leere Klausel, daher ist $\neg\varphi$ unerfüllbar, also φ allgemeingültig.

Meist bildet man gar nicht die Grundinstanzen, sondern führt die Resolution schon mit Instanzen von Klauseln durch, die noch Variable enthalten: Die Matrix der allquantifizierten Formel φ^S ist die KNF-Formel $P(fx) \wedge \neg P(x)$, die aus den beiden Klauseln $\{P(f(x))\}$ und $\{\neg P(x)\}$ besteht. Durch Substitution bekommt man aus der zweiten Klausel $\{\neg P(f(x))\}$, daraus dann mit Resolution die leere Klausel.

Man beachte, dass man jede Klausel beliebig oft (mit beliebigen Substitutionen) verwenden kann.

2.

$$\psi := \exists x\,\forall y\;P(x,y) \to \forall y\;\exists x\,P(x,y)$$

$$\neg\psi = \varphi = \neg(\exists x\,\forall y\;P(x,y) \to \forall y\;\exists x\,P(x,y)) \;\Leftrightarrow$$

$$\exists x\,\forall y\;P(x,y) \wedge \neg\forall y\;\exists x\,P(x,y) \;\Leftrightarrow$$

$$\exists x\,\forall y\;P(x,y) \wedge \exists y\,\forall x\;\neg P(x,y) \;\Leftrightarrow$$

$$\exists x\,\forall y\;P(x,y) \wedge \exists y'\;\forall x'\;\neg P(x',y') \;\Leftrightarrow$$

$$\exists x\,\exists y'\;\forall y\;\forall x'\;P(x,y) \wedge \neg P(x',y') \;\sim_{\vDash}$$

$$\forall y\;\forall x'\;P(a,y) \wedge \neg P(x',b) := \varphi^S$$

$$\{P(a,b) \wedge \neg P(a,b)\} \subseteq G(\varphi) \quad (y \mapsto b, x' \mapsto a)$$

$$\{\{p_1\};\{\neg p_1\}\} \overset{Res}{\longmapsto} \{\{p_1\};\{\neg p_1\};\{\}\}$$

Daher ist ψ allgemeingültig.

3.

$$\psi := \forall x\ \exists y\,(P(x) \to \neg P(y)) \to \exists x\,\neg P(x)$$

$$\psi = \neg\varphi = \forall x\ \exists y\,(\neg P(x) \vee \neg P(y)) \wedge \forall z\ P(z) \ \Leftrightarrow$$

$$\forall x\ \exists y \forall z\ (\neg P(x) \vee \neg P(y)) \wedge P(z) \ \sim_{\vDash}$$

$$\forall x\ \forall z\ (\neg P(x) \vee \neg P(f(x))) \wedge P(z) := \varphi^S$$

$$\{\neg P(a) \vee \neg P(f(a)), P(a), P(f(a))\} \subseteq G(\varphi)$$

$$\{\{\neg p_1, \neg p_2\};\{p_1\};\{p_2\}\} \overset{Res}{\longmapsto}$$

$$\{\{\neg p_1, \neg p_2\};\{p_1\};\{p_2\};\{\neg p_2\}\} \overset{Res}{\longmapsto}$$

$$\{\{\neg p_1, \neg p_2\};\{p_1\};\{p_2\};\{\neg p_2\};\{\}\}$$

Daher ist ψ allgemeingültig.

Hier eine verkürzte Version: Die Matrix von φ^S ist

$$\{\,\{\neg P(x), \neg P(f(x))\};\{P(z)\}\,\}.$$

Durch Substitution erhält aus der zweiten Klausel die Klauseln $\{P(x)\}$ und $\{P(f(x))\}$. Nach zweimaliger Resolution mit der ersten Klausel erhält man die leere Klausel.

10 Mengenlehre

10.1 Prädikatenlogik 2. Stufe

Wir wollen hier die Prädikatenlogik zweiter Stufe nicht ausführlich behandeln, sondern nur motivieren.
In der Prädikatenlogik erster Stufe können wir (in einer Sprache $\mathscr{L}$)

(A) mit Hilfe einer geschlossenen Formel φ aus allen $\mathscr{L}$-Strukturen die Modelle von φ aussondern
(z.B. definiert die Konjunktion der Gruppenaxiome genau die Gruppen);

(B) mit Hilfe einer Formel $\varphi(u)$ auf einer vorgegebenen $\mathscr{L}$-Struktur eine Teilmenge definieren (oder allgemeiner eine n-stellige Relation mit Hilfe einer Formel $\varphi(u_1,\ldots,u_n)$)
(z.B. definiert die Formel $\forall x\, x * u = u * x$ das Zentrum einer Gruppe).

Allerdings findet man sehr bald Klassen von Strukturen, oder Teilmengen von Strukturen, die man zwar explizit definieren kann, für die sich aber keine Definition in der Sprache der Prädikatenlogik erster Stufe anbietet, weil in dieser Sprache nur über Elemente der Struktur quantifiziert werden kann, nicht aber über Teilmengen der Struktur, natürliche Zahlen, Folgen von Elementen, etc.
Sei $(G, ., 1, ^{-1})$ eine Gruppe; das Zentrum von G definieren wir als $Z(G) := \{u \in G : \forall y\ u.y = y.u\}$. Die Menge $Z(G)$ lässt sich offenbar durch eine prädikatenlogische Formel 1. Stufe formalisieren. Das dies nicht immer der Fall sein muss, zeigt die Untergruppe $G' \subseteq G$, die von den Elementen $x.y.x^{-1}.y^{-1} \quad x, y \in G$ erzeugt wird.
Ähnliches sieht man bei geschlossenen Formeln. Die Klasse aller abelschen Gruppen lässt sich leicht durch die geschlossene Formel $\forall x \forall y\, xy = yx$ (gemeinsam mit der Konjunktion der Gruppenaxiome) beschreiben. Für die Klasse der einfachen Gruppen bietet sich aber keine Formel in der Prädikatenlogik erster Stufe an, die diese Klasse beschreibt (und tatsächlich gibt es auch keine).
Um auch solche Mengen formalisieren zu können, benötigt man also „mächtigere“ Sprachen.

Eine prädikatenlogische Sprache 2. Stufe enthält neben den bereits bekannten Objektvariablen, Funktions- und Relationssymbolen auch sogenannte Relationsvariablen X, Y, Z. Während Terme wie in 1. Stufe definiert werden, nehmen Atomformeln die Form $R(t_1, \ldots, t_n)$ an, wobei R nun auch für eine Relationsvariable stehen kann.

Beispiel. Wir geben ein Beispiel für eine prädikatenlogische Formel 2. Stufe, welche die Existenz einer transitiven zweistelligen Relation beschreibt:

$$\exists_2 X\ \forall_1 x \forall_1 y \forall_1 z\ X(x, y) \wedge X(y, z) \to X(x, z)$$

Die Indizes an den Quantoren sollen daran erinnern, dass in einem Fall über Objekte „zweiter Stufe“ (Teilmengen und Relationen) quantifiziert wird, im anderen nur über Objekte erster Stufe (Elemente der betrachteten Struktur). Modelle, Belegungen und Gültigkeitsbegriff kann man analog zur 1. Stufe erklären. Zum Beispiel ist die gerade angeführte Formel allgemeingültig, d.h. sie gilt in jeder Struktur. (Z.B. ist die Allrelation immer transitiv, ebenso wie die leere Relation oder die Identität.)
Für eine Sprache 2. Stufe lässt sich aber kein sinnvoller Beweisbegriff definieren, d.h. es gilt der folgende

Satz 10.1. *Die Menge $\{\varphi : \vDash_2 \varphi\}$ ist nicht semi-entscheidbar.*
Daher gibt es keinen berechenbaren Ableitungsbegriff $\vdash\!\!\sim$, sodass

$$\vdash\!\!\sim \varphi \quad \Leftrightarrow \quad \vDash_2 \varphi$$

für alle φ gilt.

Die ZFC-Axiome sind eine Theorie 1. Stufe. Rückblickend[36] kann man die Mengenlehre als einen Versuch interpretieren, Logik zweiter und höherer Stufe durch eine Theorie erster Stufe zu simulieren, indem man einfach (gewisse; allerdings nicht alle) Teilmengen und Relationen der Modellelemente wiederum zu Modellelementen macht.

10.2 Allgemeines

Die Sprache der Mengenlehre enthält als einziges nichtlogisches Zeichen das zweistellige Symbol ϵ. Wir stellen uns darunter zwar die konkrete Relation $\in$ vor, müssen aber doch auch beliebige Strukturen (M, E) betrachten, in denen E eine beliebige zweistellige Relation sein kann.
Um auf den Unterschied zwischen objektsprachlichen Variablen (die beim Aufbau von Formeln beteiligt sind) und metasprachlichen Variablen (die wir verwenden, wenn wir z.B. über Modelle sprechen) aufmerksam zu machen, verwenden wir ab jetzt einen eigenene Schriftsatz für objektsprachliche Variable: $\mathtt{x}, \mathtt{y}, \mathtt{x}_1, \mathtt{z}', \ldots$.
Wir beginnen mit einem Beispiel für ein mengentheoretisches Modell: Seien a, b zwei beliebige (verschiedene) Objekte.

$$\mathfrak{M} := (M, E) \quad \text{mit } M := \{a, b\},\ E :=\epsilon^{\mathfrak{M}}:= \{(a, b)\}$$

Offenbar gilt

$$\mathfrak{M} \vDash \exists \mathtt{x}\, \forall \mathtt{y}\ \neg(\mathtt{y}\ \epsilon\ \mathtt{x})$$

denn das Element a erfüllt die gewünschte Beziehung ($(a, a) \notin E,\ (b, a) \notin E$). Die Grundlage unserer Mengenlehre bilden die ZFC-Axiome (siehe Anhang C). Erwähnenswert ist noch das Singleton-Axiom, das im Anhang nicht vorkommt. Es besagt, dass es zu jedem Element eine Menge gibt, die nur jenes Element (und sonst nichts) enthält, also

$$\forall \mathtt{x}\ \exists \{\mathtt{x}\} \text{ bzw.}$$

$$\forall \mathtt{x}\ \exists \mathtt{S}\, (\mathtt{x} \in \mathtt{S} \wedge \forall \mathtt{y}\ (\mathtt{y}\ \epsilon\ \mathtt{S} \to \mathtt{y} = \mathtt{x})) \text{ bzw.}$$

$$\forall \mathtt{x}\ \exists \mathtt{S}\, (\forall \mathtt{y}\ (\mathtt{y}\ \epsilon\ \mathtt{S} \leftrightarrow \mathtt{y} = \mathtt{x}))$$

Das Singleton-Axiom ist aus dem Paarmengenaxiom ableitbar (und daher im Anhang nicht erwähnt):

Beweis.
PMA $\vdash \forall \mathtt{y}\ \exists \mathtt{p} \forall \mathtt{z}\ (\mathtt{z}\ \epsilon\ \mathtt{p} \leftrightarrow \mathtt{z} = \mathtt{u} \vee \mathtt{z} = \mathtt{y})$ (Subst.Ax. + MP)
PMA $\vdash \exists \mathtt{p} \forall \mathtt{z}\ (\mathtt{z}\ \epsilon\ \mathtt{p} \leftrightarrow \mathtt{z} = \mathtt{u} \vee \mathtt{z} = \mathtt{u})$ (Subst.Ax. + MP)
PMA $\vdash \exists \mathtt{p} \forall \mathtt{z}\ (\mathtt{z}\ \epsilon\ \mathtt{p} \leftrightarrow \mathtt{z} = \mathtt{u})$ (allgemeingültige Äquivalenz)
PMA $\vdash \forall \mathtt{x}\ \exists \mathtt{p} \forall \mathtt{z}\ (\mathtt{z}\ \epsilon\ \mathtt{p} \leftrightarrow \mathtt{z} = \mathtt{x})$ (Gen.Th.) □

[36] Historisch gesehen lief es eher umgekehrt. Als Zermelo 1908 seine Axiome formulierte, war die Unterscheidung „Logik erster/höherer Stufe“ noch nicht so klar. Zermelo wollte die Formeln in seinem Aussonderungsaxiom aber nicht auf Formeln erster Stufe beschränken, sondern „beliebige“ Eigenschaften zulassen.

Aus dem Vereinigungsmengenaxiom und dem Paarmengenaxiom lässt sich die bekannte mengentheoretische Vereinigung zweier Mengen herleiten, also

$$\mathrm{VMA}, \mathrm{PMA} \vdash \forall \mathtt{A}\ \forall \mathtt{B}\ \exists C\, \forall \mathtt{z} (\mathtt{z} \in C \leftrightarrow \mathtt{z} \in \mathtt{A} \vee \mathtt{z} \in \mathtt{B})$$

Definition 10.2 (induktive Menge)**.** Eine Menge heißt induktiv, wenn sie die leere Menge enthält und mit jedem Element x auch dessen Nachfolger $S(x) := x \cup \{x\}$.

Dieser Begriff führt zur von Neumann'schen Definition der natürlichen Zahlen:

$$0 := \emptyset$$
$$1 := \{0\}$$
$$2 := \{0, 1\}$$
$$\vdots$$

Die Menge $\mathbb{N} = \{0, 1, 2, \ldots\}$ der natürlichen Zahlen werden wir in Zukunft mit ω bezeichnen. Sie ist die kleinste induktive Menge.
Das Unendlichkeitsaxiom behauptet, dass es eine induktive Menge gibt, oder äquivalent dazu: dass es eine kleinste induktive Menge gibt. Aus „$\mathtt{x}_0$ induktiv“ kann man nämlich (mit dem Aussonderungsaxiom) erstens schließen, dass es eine Menge $\mathtt{M}$ gibt, die genau aus jenen Elementen von $\mathtt{x}_0$ besteht, die in jeder induktiven Menge enthalten sind:

$$ZF \cup \{\mathtt{x}_0 \text{ induktiv}\} \vdash \exists \mathtt{M} \forall \mathtt{z} \left[\mathtt{z} \in \mathtt{M} \ \leftrightarrow\ \mathtt{z} \in \mathtt{x}_0 \wedge \forall i \left(i \text{ induktiv } \rightarrow \mathtt{z} \in i\right)\right]$$

zweitens (mit Extensionalitätsaxiom), dass so ein $\mathtt{M}$ eindeutig bestimmt ist, drittens, dass $\mathtt{M}$ überhaupt alle Elemente enthält, die in jeder induktiven Menge vorkommen:

$$ZF \cup \{\mathtt{x}_0 \text{ induktiv}\} \vdash \exists \mathtt{M} \forall \mathtt{z} \left(\mathtt{z} \in \mathtt{M} \ \leftrightarrow\ \forall \mathtt{i} \left(\mathtt{i} \text{ induktiv } \rightarrow \mathtt{z} \in \mathtt{i}\right)\right.$$

und viertens, dass so ein $\mathtt{M}$ selbst induktiv sein muss, also kleinste induktive Menge ist:

$$ZF \vdash \mathtt{x}_0 \text{ induktiv} \rightarrow \exists \mathtt{M}\ \mathtt{M} \text{ ist kleinste induktive Menge}$$

Mit $\exists$-Einführung können wir also aus der Existenz einer induktiven Menge auf die Existenz einer kleinsten induktiven Menge schließen.
Einige weitere wichtige Bezeichnungen und Schreibweisen sind die folgenden:

- Wir führen die abkürzende Schreibweise $\mathtt{z} = \{\mathtt{x}, \mathtt{y}\}$ für

  $$\forall \mathtt{t} :\ \mathtt{t} \in \mathtt{z} \leftrightarrow \mathtt{t} = \mathtt{x} \vee \mathtt{t} = \mathtt{y}$$

  ein.

– Die Menge $\{\{\mathtt{x}\},\{\mathtt{x},\mathtt{y}\}\} =: (\mathtt{x},\mathtt{y})$ bezeichnet man als geordnetes Paar. Formal führen wir die abkürzende Formel $\mathtt{z} = (\mathtt{x},\mathtt{y})$ für

$$\exists \mathtt{P}\, \exists \mathtt{Q}\, \mathtt{z} = \{\mathtt{P},\mathtt{Q}\} \wedge \mathtt{P} = \{\mathtt{x},\mathtt{x}\} \wedge \mathtt{Q} = \{\mathtt{x},\mathtt{y}\}$$

ein, wobei $\mathtt{z} = \{\mathtt{P},\mathtt{Q}\}$ selbst wiederum eine Abkürzung ist.

Das geordnete Paar erfüllt die charakteristische Eigenschaft

$$(x,y) = (x',y') \to x = x' \wedge y = y',$$

d.h. diese Eigenschaft ist auch in ZFC beweisbar.

Sobald wir den Begriff des geordneten Paares haben, können wir auch definieren, was eine Relation bzw. eine Funktion ist, und wir verwenden abkürzende Schreibweisen wie $\mathtt{f}(\mathtt{x}) = \mathtt{y}$ für „$\mathtt{f}$ ist Funktion[37], und $(\mathtt{x},\mathtt{y}) \,\epsilon\, \mathtt{f}$“. $(\mathtt{x},\mathtt{y}) \,\epsilon\, \mathtt{f}$ ist wiederum als $\exists \mathtt{p}\, \mathtt{p} \,\epsilon\, \mathtt{f} \wedge \mathtt{p} = (\mathtt{x},\mathtt{y})$ zu lesen.

– Die Produktmenge zweier Mengen X, Y sei definiert als

$$X \times Y := \{(\mathtt{x},\mathtt{y}) : \mathtt{x} \,\epsilon\, X, \mathtt{y} \,\epsilon\, Y\} = \{\mathtt{z} : \exists \mathtt{x} \,\epsilon\, X\ \exists \mathtt{y} \,\epsilon\, Y : \mathtt{z} = (\mathtt{x},\mathtt{y})\}$$

– Für eine Funktion $f : X \to Y$ gilt $f \subseteq X \times Y$. Wir schreiben statt $\mathtt{f}(\mathtt{x}) = \mathtt{y}$ auch $(\mathtt{x},\mathtt{y}) \in \mathtt{f}$. Eine Funktion ist also eine spezielle Form einer Relation.

– Die Definition einer Funktion f nach dem Schema

$$f(0) = a_0,\ \ f(n+1) = h(f(n))$$

nennt man induktiv.

– Das Bild einer Menge A unter einer Abbildung f bezeichnen wir mit $f[A] := \{f(a) : a \in A\}$.

Definition 10.3 (h-induktive Relation)**.** Sei A eine Menge und $h : A \to A$ eine Funktion. Eine Relation $R \subseteq \omega \times A$ heißt h-induktiv, wenn gilt

1. $(0, a_0) \in R$, für ein $a_0 \in A$
2. $\forall n \in \omega\ \forall a \in A :\ (n,a) \in R \to (n+1, h(a)) \in R$

Beispiele. Die Relation $\omega \times A$ ist offenbar h-induktiv. Im folgenden Satz suchen wir eine kleinste h-induktive Relation.

[37] Achtung! Unsere Sprache enthält weiterhin nur ein einziges Relationssymbol, und weder Konstanten- noch Funktionssymbole. Insbesondere ist $\mathtt{f}$ hier kein Funktionssymbol sondern einfach eine Variable.

Satz 10.4 (Rekursion)**.** *Sei A eine Menge, $h : A \to A$ eine Funktion und $a_0 \in A$. Dann existiert genau eine Funktion $g : \omega \to A$ mit*

$$g(0) = a_0, \quad g(n+1) = h(g(n))$$

In der naiven Mengenlehre ist dieser Satz klar: $g(n) := f^{(n)}(a_0)$. Wir wollen diesen Satz aber in der formalen Mengenlehre definieren und mit ZFC beweisen. Die Formulierung als Satz der Form

$$\forall \mathtt{A}\ \forall \mathtt{h}\ \forall \mathtt{a}_0\ (\text{Wenn } \mathtt{h} : \mathtt{A} \to \mathtt{A}, \ldots, \text{ dann } \exists! \mathtt{g} : \ldots)$$

überlassen wir dem Leser.

Beweisskizze. Gesucht ist eine Formel $\varphi(\mathtt{n}, \mathtt{a})$ (die $\mathtt{a}_0$ und $\mathtt{h}$ verwenden darf), die den Graphen der gesuchten Funktion aus der Menge $\mathtt{A} \times \mathtt{A}$ aussondert. Wir definieren $\varphi(\mathtt{n}, \mathtt{a})$ so:

$$\mathtt{n} \in \omega \wedge \mathtt{a} \in \mathtt{A} \wedge \forall \mathtt{R}\ (\mathtt{R} \text{ ist } \mathtt{h}\text{-induktiv} \ \to (\mathtt{n}, \mathtt{a}) \in \mathtt{R})$$

Es lässt sich dann (mit ZFC!) zeigen, dass eine Relation $\mathtt{M} \subseteq \omega \times \mathtt{A}$ existiert, sodass gilt

$$\forall \mathtt{n} \in \omega\ \forall \mathtt{a} \in \mathtt{A} : \ (\mathtt{n}, \mathtt{a}) \in \mathtt{M} \leftrightarrow \varphi(\mathtt{n}, \mathtt{a})$$

Weiters lässt sich zeigen, dass $\mathtt{M}$ dann eine Funktion ist, die die Bedingungen erfüllt, also ist $\mathtt{M}$ das gewünschte $\mathtt{g}$. □

Familien

Eine „Familie“ ist formal dasselbe wie eine Funktion; der Unterschied besteht in der Betrachtungsweise: Bei einer Funktion geht es um die Beziehung zwischen Elementen des Definitionsbereich und des Wertebereichs, während es bei einer Familie vor allem um die Elemente des Wertebereichs geht (die dann oft auch einfach „Elemente der Familie“ heißen, was eine sprachliche Ungenauigkeit darstellt, da die „Elemente“ einer Funktion/Familie formal korrekt eigentlich Paare (i, x_i) sind).
Weiters sind bei einer Funktion die Elemente des Bildbereichs als „Objekte“ bzw. Elemente einer Struktur interessant, während die Elemente einer Familie oft als Mengen interessant sind (d.h. wir interessieren uns auch für ihre Elemente). Eine Familie, deren Elemente als Objekte interessant sind (also nicht als Mengen) nennen wir auch Tupel. Ein Tupel mit Definitionsbereich I nennen wir auch I-Tupel. Wenn I eine natürliche Zahl n ist, sagen wir statt n-Tupel auch „Folge der Länge n“.

Beispiel. Sei $f : \{0, 1, 2\} \to \mathbb{R}$ durch $f(0) = 3$, $f(1) = 1$, $f(2) = 4$ definiert. Die Definitionsmenge = Indexmenge von f ist die Menge $\{0, 1, 2\}$, die wir 3 nennen; f ist also ein „3-Tupel“.

Abkürzend können wir f auch als $\langle 3, 1, 4\rangle$ anschreiben. [38]

Beispiel. Sei $g : \{0, 1, 2\} \to \mathfrak{P}(\mathbb{R})$ durch $f(0) = \mathbb{N}$, $f(1) = \mathbb{Z}$, $f(2) = \mathbb{R}$ definiert. Da die „Elemente“ dieser Familie nicht einfach „Zahlen“ sondern Mengen von Zahlen sind, nennt man g eher „Familie“ statt „Tupel“.
Abkürzend können wir g auch als $\langle \mathbb{N}, \mathbb{Z}, \mathbb{R}\rangle$ anschreiben.

Beispiel. Das 2-Tupel $\{(0, x), (1, y)\}$ kann man abgekürzt als $\langle x, y\rangle$ anschreiben. Formal ist das etwas ganz anderes als das geordnete Paar (x, y). Tatsächlich ist der Unterschied oft vernachlässigbar, weil auch $\langle x, y\rangle$ die charakteristische Eigenschaft des geordneten Paars hat.

Den Definitionsbereich einer Familie nennt man üblicherweise Indexmenge. Wenn I die Indexmenge der Familie $\mathscr{F}$ ist, sagen wir auch, dass $\mathscr{F}$ „mit I indiziert ist“. Eine mit I indizierte Familie $\mathscr{F}$ schreibt man auch gerne als $\mathscr{F} = (X_i : i \in I)$ oder $\mathscr{F} = (X_i)_{i\in I}$ an, wobei X_i eine andere Schreibweise für $\mathscr{F}(i)$ ist.
Aus ästhetischen Gründen spricht man statt von einer „Menge von Mengen“ oft lieber von einer „Familie von Mengen“. Dies ist insofern gerechtfertigt, als man jeder Menge X in natürlicher Weise eine Familie (oder ein X-Tupel) zuordnen kann, nämlich die Familie $\langle a_i : i \in X\rangle$, wobei wir $a_i := i$ setzen. Formal ist diese Familie die Identitätsfunktion auf der Menge X; da es uns aber bei Familien besonders auf die Elemente des Wertebereichs ankommt, ist diese Familie „im Wesentlichen“ dasselbe wie die Menge X selbst.

Operationen auf Familien

Sei $(X_i : i \in I)$ eine Familie von Mengen. Mit $\bigcup_{i\in I} X_i$ bezeichnen wir die Menge $\{y : \exists i \in I\, y \in X_i\}$. Dies ist also genau die Menge $\bigcup Y$, wobei $Y = \{X_i : i \in I\}$ der Wertebereich der gegebenen Familie ist.
Analog ist $\bigcap_{i\in I} X_i$ definiert. Dies ist allerdings nur dann erlaubt, wenn I nicht leer ist.[39]
Sei $(X_i : i \in I)$ eine Familie von Mengen. Mit $\prod_{i\in I} X_i$ bezeichnen wir die Menge aller I-Tupel $(x_i : i \in I)$, die $\forall i\, x_i \in X_i$ erfüllen. Formal ist dies also die Familie aller Funktionen f, die auf I definiert sind, Wertebereich $\subseteq \bigcup_{i\in I} X_i$ erfüllen, und weiters die Eigenschaft $\forall i \in I\, f(i) \in X_i$ haben.

Beispiel. Sei $(X_i : i \in I)$ eine Familie von Mengen, die alle $3 \in X_i$ erfüllen. Dann ist die konstante Funktion mit Wert 3 (formal also die Menge $I \times \{3\}$) ein Element von $\prod_i X_i$.

[38] Oft werden für endliche Folgen auch runde Klammern verwendet, statt $\langle 3, 1, 4\rangle$ schreibt man dann $(3, 1, 4)$. Umgekehrt wird für das geordnete Paar $\{\{x\}, \{x, y\}\}$ statt (x, y) manchmal auch die Schreibweise $\langle x, y\rangle$ verwendet.

[39] Die definitorische Abkürzung $x \in \bigcap_{i\in I} X_i \leftrightarrow \forall i \in I\, x \in X_i$ ist zwar auch dann möglich, wenn I leer ist; dann trifft $x \in \bigcap_{i\in I} X_i$ für alle x zu, daher gibt es keine Menge Z, die alle solchen x enthält. Für leeres I gilt also $\neg\exists Z\, \forall x\, (x \in Z \leftrightarrow \bigcap_{i\in I} X_i)$, also kurz gesagt „der leere Durchschnitt existiert nicht“, bzw „ist keine Menge“.

Beispiel. Sei $I = \emptyset$. Dann gibt es genau ein I-Tupel, nämlich die leere Menge (die in diesem Zusammenhang auch 0-Tupel genannt wird).
Die leere Menge ist nämlich eine Funktion, deren Definitionsbereich leer ist.

Beispiel. Sei $I = \{0\}$, $X_0 := \{4, 8\}$. Dann ist die Funktion $\{(0, \{4, 8\})\}$ eine mit I indizierte Familie, die wir auch als $(X_i : i \in I)$ anschreiben können. Das Produkt $\prod_{i \in I} X_i$ besteht aus den beiden Funktionen $\{(0, 4)\}$ und $\{(0, 8)\}$; in Tupelschreibweise können wir die beiden Elemente dieses Produkts als $\langle 4 \rangle$ und $\langle 8 \rangle$ anschreiben; wir sehen hier, dass ein Produkt mit einem einzigen Faktor im Wesentlichen dasselbe wie dieser Faktor ist.

10.3 Endliche und unendliche Mengen

Es gibt verschiedene Möglichkeiten, den Begriff „endlich“ zu definieren. In der modernen Mengenlehre verwendet man üblicherweise die folgende Definition:

Definition 10.5. Eine Menge A heißt endlich, wenn es eine natürliche Zahl $n \in \omega$ und eine Bijektion $f : n \to A$ gibt.
A heißt unendlich, wenn A nicht endlich ist.

Dies lässt sich leicht in der Sprache von ZFC formalisieren. Wir schreiben oft informell $|A| < \infty$ bzw. $|A| = \infty$.
Allgemeiner definieren wir $A \approx B$ (gelesen: A und B sind gleichmächtig) als Abkürzung für $\exists f : A \to B$, f Bijektion.
Gelegentlich trifft man auch die folgende Definition:

Definition 10.6. A heißt Dedekind-unendlich, wenn A mit einer echten Teilmenge gleichmächtig ist.

Mit den bisher betrachteten Axiomen kann man folgendes zeigen:

Satz 10.7. *Die folgenden Aussagen sind äquivalent:*

(a) A ist mit einer echten Teilmenge gleichmächtig.

(b) Es gibt ein $a \in A$, sodass A mit $A \setminus \{a\}$ gleichmächtig ist.

(c) Es gibt eine injektive Abbildung von ω nach A.

Beweis von (c)→(b): Sei $f : \omega \to A$ injektiv. Sei B die um die Wertemenge von f verminderte Menge A: $B := A \setminus f[\omega]$. Sei $g := \{(b, b) : b \in B\} \cup \{(f(n), f(n+1)) : n \in \omega\}$. Dann ist $g : A \to A \setminus \{f(0)\}$ eine Bijektion.
Im nächsten Abschnitt werden wir die Beziehung von (a), (b), (c) zu folgender Aussage betrachten:

(d) A ist unendlich.

Mit Induktion kann man leicht zeigen, dass kein $n \in \omega$ Dedekind-unendlich ist, ebenso keine zu n gleichmächtige Menge. Daher sind endliche Mengen jedenfalls Dedekind-endlich.

10.4 Das Auswahlaxiom

Wir behaupten, dass umgekehrt jede Dedekind-endliche Menge auch endlich ist, also jede unendliche Menge Dedekind-unendlich sein muss.

Satz 10.8. *Jede unendliche Menge A enthält eine Kopie der natürlichen Zahlen; in Zeichen:*

$$\forall A : |A| = \infty \;\Rightarrow\; \exists g : \omega \to A,\ g \text{ injektiv}$$

Beweis. Der Beweis scheint offensichlich zu sein:

$$g(0) := a_0 \in A, \quad g(n+1) := a_{n+1} \in A \setminus \{g(0), g(1), \ldots, g(n)\}$$

□

Nicht auf der Hand liegt die Tatsache, dass dieser Beweis nicht mit den ZF-Axiomen geführt werden kann, man benötigt zusätzlich das Auswahlaxiom.

Definition 10.9 (Auswahlaxiom)**.** Das Auswahlaxiom besagt

$$\forall X\ \exists f : \mathcal{P}(X) \setminus \{\emptyset\} \to X :\ \forall A \subseteq X :\ f(A) \in A$$

Ist nämlich f eine solche Auswahlfunktion, so kann man die im obigen Satz gesuchte Funktion g definieren durch

$$g(0) := f(X), \quad g(n+1) := f(X \setminus \{g(0), g(1), \ldots, g(n)\})$$

Genauer können wir g als Teilmenge von $\omega \times X$ durch eine geeignete Formel φ aussondern. $\varphi(n, x)$ besagt, informell, dass es eine Funktion g' gibt, die auf $\{0, \ldots, n\}$ definiert ist, an der Stelle n den Wert x annimmt, und zwischendurch einer Rekursionsformel gehorcht:

$$\varphi(n,x) := \ (n \in \omega \wedge x \in X) \wedge\ \exists g' \Big(g' : (n+1) \to X \ \wedge\ g'(n) = x \wedge \\ \wedge\ \forall k \le n : g'(k) = f(X \setminus g'[k]) \Big)$$

Man beachte, dass im Ausdruck $g'[k]$ die Menge aller Werte $g'(i)$ mit $i < k$ gemeint ist: $g'[k] = \{g'(i) : i \in k\} = \{g'(i) : i < k\} = \{g'(0), \ldots, g'(k-1)\}$.

Eine Variante des Auswahlaxioms bildet das Auswahlaxiom in Familienversion:

Definition 10.10 (Auswahlaxiom, Familienversion)**.** Für jede Mengenfamilie $(A_i : i \in I)$ von nichtleeren Mengen gibt es eine Auswahlfunktion, d.h.

$$\exists f : I \to \bigcup_{i \in I} A_i :\ \forall i \in I :\ f(i) \in A_i$$

Kurz gesagt: Wenn $\forall i\ A_i \neq \emptyset$ gilt, dann ist auch $\prod_{i \in I} A_i$ nicht leer.

Wir zeigen, dass die beiden Versionen des Auswahlaxioms äquivalent sind. Dazu setzen wir zunächst die Standardversion voraus und folgern die Familienversion:

Beweis. Sei also $(A_i : i \in I)$ eine Mengenfamilie mit $A_i \neq \emptyset \ \ \forall i \in I$. Wir definieren $X := \bigcup_{i \in I} A_i$. Laut Voraussetzung existiert also eine Auswahlfunktion g auf der Menge $\mathcal{P}(X) \setminus \{\emptyset\}$, sodass $g(A) \in A \ \ \forall A \subseteq X$. Die durch $f : I \to X$, $i \mapsto g(A_i) \in A_i$ definierte Funktion ist dann die gesuchte Auswahlfunktion für Familien.

Sei umgekehrt die Familienversion vorausgesetzt und $A \neq \emptyset$ eine Menge. Wir setzen $I := \mathcal{P}(A) \setminus \{\emptyset\}$ und $A_i := i$. Dann existiert also laut Voraussetzung eine Auswahlfunktion $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ mit $f(i) \in A_i = i$. Diese erfüllt die gewünschten Bedingungen. □

Die endliche Variante des Auswahlaxioms in Familienversion kann man auch in ZF beweisen. Ist $(A_i : i \in I)$ eine Mengenfamilie mit $A_i \neq \emptyset \ \ \forall i \in I$ und I endlich, dann folgt $\prod_{i \in I} A_i \neq \emptyset$. Der Beweis erfolgt induktiv (d.h. wir verwenden die Definition von ω als kleinster induktiver Menge).
Als Aufwärmübung zeigen wir zunächst $A \neq \emptyset \ \wedge \ B \neq \emptyset \to A \times B \neq \emptyset$:

Die Formel $a \in A \ \wedge \ b \in B \to (a, b) \in A \times B$ folgt mehr oder weniger aus der Definition von $A \times B$. Die Formel $(a, b) \in A \times B$ ist nämlich Abkürzung für $\exists z \ \exists C \, z = (a, b) \wedge z \in C \wedge C = A \times B$. Hier ist $C = A \times B$ Abkürzung für $\forall u \, (u \in C \leftrightarrow \exists p \in A \, \exists q \in B \, u = (p, q))$.
Aus den Axiomen $C = A \times B, a \in A, b \in B, z = (a, b)$ folgt also „nach Definition“ $z \in C$. Damit erhalten wir mit Deduktionstheorem:
$\mathrm{ZFC} \vdash a \in A \ \wedge \ b \in B \to (a, b) \in A \times B$
$\mathrm{ZFC} \vdash a \in A \ \wedge \ b \in B \to \exists z : z \in A \times B$ (∃-Einführung rechts)
$\mathrm{ZFC} \vdash \exists x : x \in A \ \wedge \ b \in B \to \exists z : z \in A \times B$ (∃-Einführung links)
$\mathrm{ZFC} \vdash \exists y \, \exists x : x \in A \ \wedge \ y \in B \to \exists z : z \in A \times B$ (∃-Einführung links)

Nun betrachten wir die Menge

$$R := \{n \in \omega : P(n)\}$$

wobei $P(n)$ die folgende Formel ist:

> Für jede Familie $(X_i : i < n)$ von nichtleeren Mengen ist $\prod_{i<n} X_i$ nicht leer.

R ist nach dem Aussonderungsaxiom wohldefiniert. Wir wollen zeigen, dass R induktiv ist. $P(0)$ gilt, weil das leere Produkt nicht leer ist (es enthält das leere 0-Tupel).
Für den Induktionsschritt beweisen wir nun Folgendes:

$$f \in \prod_{i<n} X_i \ \wedge \ y \in X_n \ \to \ f \cup \{(n, y)\} \in \prod_{i<n+1} X_i$$

Der Beweis dafür ist ähnlich wie der obige Beweis von $(a, b) \in A \times B$, man muss nur die Definitionen auspacken. Insbesondere muss man aus dem Axiom $g = f \cup \{(n, y)\}$ schließen, dass g eine Funktion ist.
Durch Einführung des Existenzquantors rechts erhält man nun zunächst

$$f \in \prod_{i<n} X_i \ \wedge \ y \in X_n \ \rightarrow \ \prod_{i<n+1} X_i \neq \emptyset,$$

und durch Einführung des Existenzquantors links (2 Mal) erhält man

$$\prod_{i<n} X_i \neq \emptyset \ \wedge \ X_n \neq \emptyset \ \rightarrow \ \prod_{i<n+1} X_i \neq \emptyset.$$

Damit hat man in ZF bewiesen, dass R induktiv ist, daher ist $R = \omega$.

Man sieht leicht, dass aus der Aussage: „Das Produkt einer mit n indizierten Familie von nichtleeren Mengen ist nichtleer“ die Aussage „Für alle n-elementigen Indexmengen I gilt: Das Produkt einer mit I indizierten Familie von nichtleeren Mengen ist nichtleer“ folgt.
Daher gilt:

Satz 10.11. *In ZF ist beweisbar: Das Produkt einer endlichen Familie von nichtleeren Mengen ist nie leer.*

10.5 Das Lemma von Zorn

In diesem Abschnitt kommen wir zu drei zum Auswahlaxiom äquivalenten Sätzen. Zunächst aber noch einige Definitionen:

Definition 10.12 (Halbordnung)**.** Sei P eine Menge und $\leq$ eine binäre Relation. Dann heißt $(P, \leq)$ Halbordnung, wenn die Relation $\leq$ die folgenden Eigenschaften hat:

- Reflexivität: $a \leq a \ \ \forall a \in P$
- Antisymmetrie: $a \leq b \wedge b \leq a \rightarrow a = b \ \ \forall a, b \in P$
- Transitivität: $a \leq b \wedge b \leq c \rightarrow a \leq c \ \ \forall a, b, c \in P$

Definition 10.13 (Kette)**.** Sei $(P, \leq)$ eine Halbordnung und $C \subseteq P$. C heißt Kette, wenn für alle $c_1, c_2 \in C$ gilt:

$$c_1 \leq c_2 \vee c_2 \leq c_1$$

Definition 10.14 (maximales Element)**.** Sei P eine Menge. Dann heißt $m \in P$ maximales Element, wenn gilt

$$\forall p \in P : m \leq p \rightarrow m = p$$

Wir kommen nun zum berühmten

Satz 10.15 (Lemma von Zorn)**.** *Sei $(P, \leq)$ eine Halbordnung. Wenn jede Kette $C \subseteq P$ beschränkt ist, dann existiert ein maximales Element in P.*

Satz 10.16 (Lemma von Hausdorff)**.** *Sei $(Q, \leq)$ eine Halbordnung. Dann gibt es eine maximale Kette K^*, d.h.*

$$\forall K \subseteq Q : K \text{ Kette } \wedge \ K^* \subseteq K \rightarrow K^* = K$$

Definition 10.17 (Familie von endlichem Charakter)**.** Sei $\mathscr{F}$ eine Menge von Mengen. $\mathscr{F}$ heißt Familie von endlichem Charakter, wenn gilt

$$\forall X : X \in \mathscr{F} \leftrightarrow (\forall E \subseteq X : E \text{ endlich} \rightarrow E \in \mathscr{F})$$

d.h. eine Menge X liegt genau dann in $\mathscr{F}$, wenn alle ihre endlichen Teilmengen in $\mathscr{F}$ liegen.

Beispiele.

- Sei X beliebig. Dann ist $\mathfrak{P}(X)$ von endlichem Charakter.
- Sei X unendlich. Dann ist die Menge $\{B \subseteq X : B \text{ endlich}\}$ nicht von endlichem Charakter.
- Sei Q eine partielle Ordung. Dann ist die Menge $\{K \subseteq Q : K \text{ ist Kette}\}$ von endlichem Charakter.
- Seien A, B Mengen. Dann ist die Menge aller partiellen Funktionen von A nach B von endlichem Charakter.
- Seien A, B Mengen. Dann ist die Menge aller partiellen *injektiven* Funktionen von A nach B von endlichem Charakter.

Mit dieser Definition gelangen wir zum dritten

Satz 10.18 (von Teichmüller/Tukey)**.** *Jede Familie von endlichem Charakter hat ein maximales Element (bzgl. $\subseteq$).*

Wir zeigen, dass die drei genannten Sätze äquivalent sind:

Beweis. Zorn $\rightarrow$ Teichmüller/Tukey: Sei $\mathscr{F}$ eine Familie von endlichem Charakter. Man fasst $(\mathscr{F}, \subseteq)$ als Halbordnung auf. Sie erfüllt die Voraussetzungen des Lemma von Zorn, denn ist $K \subseteq \mathscr{F}$ eine Kette, dann ist

$$S := \bigcup_{X \in K} X \in \mathscr{F}$$

sicher eine obere Schranke in Bezug auf die Relation $\subseteq$. Wir behaupten darüber hinaus, dass S auch in der betrachteten Halbordnung liegt, dass also $S \in \mathscr{F}$. Dazu müssen wir nur zeigen, dass jede endliche Teilmenge $E \subseteq S$ in $\mathscr{F}$ liegt.

Ist nämlich $E := \{e_1, e_2, \ldots, e_n\}$ eine solche endliche Teilmenge, dann gilt

$$e_1 \in X_1 \in K$$

$$e_2 \in X_2 \in K$$

$$\vdots$$

$$e_n \in X_n \in K$$

Es gilt dann oBdA $X_i \subseteq X_1 \in \mathscr{F} \quad \forall i = 1, \ldots, n$, also $E \in \mathscr{F}$.

Teichmüller/Tukey $\rightarrow$ Hausdorff folgt aus dem zweiten Beispiel einer Familie endlichen Charakters $\{K \subseteq Q : K \text{ ist Kette}\}$.

Hausdorff $\rightarrow$ Zorn ist leicht: Jede obere Schranke einer maximalen Kette muss bereits ein maximales Element sein. $\square$

Aus dem Satz von Teichmüller/Tukey folgt der Vergleichbarkeitssatz:

Satz 10.19 (Vergleichbarkeitssatz)**.** *Seien A, B Mengen. Dann gilt*

$$|A| \leq |B| \ \vee \ |B| \leq |A|$$

Es existiert also entweder eine injektive Funktion von A nach B oder von B nach A.

Beweis. Wir definieren

$$f := \{g : \mathrm{dom}(g) \subseteq A, \mathrm{ran}(g) \subseteq B, g \text{ injektiv}\}$$

f ist eine Familie von endlichem Charakter, man kann also Teichmüller/Tukey anwenden und erhält ein maximales Element $g^* \in f$. Es muss gelten

$$\mathrm{dom}(g^*) = A \ \vee \ \mathrm{ran}(g^*) = B$$

(denn sonst wäre g^* nicht maximal).
Wenn g^* total ist, dann ist g^* injektive Abbildung von A nach B. Im anderen Fall liefert g^* eine injektive Abbildung von B nach A. $\square$

Definition 10.20 (Wohlordnung)**.** Sei W eine Menge und $<$ eine binäre Relation. Dann heißt $(P, <)$ Wohlordnung, wenn die Relation $<$ die folgenden Eigenschaften hat:

- Reflexivität: $a < a \quad \forall a \in W$
- Transitivität: $a < b \wedge b < c \rightarrow a < c \quad \forall a, b, c \in W$
- Vergleichbarkeit: $a < b \vee a = b \vee b < a \quad \forall a, b \in W$
- Existenz des Minimums: $\forall A \subseteq W : \ A \neq \emptyset \rightarrow \exists \min(A)$.

Beispiel.
$(\{-1, -\frac{1}{2}, -\frac{1}{3}, \ldots, 0\}, \leq)$ ist Wohlordnung, jedoch nicht zu ω isomorph.

Satz 10.21. *Aus dem Auswahlaxiom (genauer: aus ZFC) folgt das Lemma von Zorn.*

Wir beenden das Kapitel mit einem überraschenden Ergebnis.

Satz 10.22 (Wohlordnungssatz)**.** *Sei A eine Menge. Dann existiert eine Relation R, sodass (A, R) eine Wohlordnung ist.*