Logik und Grundlagen

Martin Goldstern

Moritz Gschwandtner

Stefan Hetzl

Die ursprüngliche Version des Skriptums wurde von Moritz Gschwandtner nach einer Vorlesung von Martin Goldstern geschrieben, später von Goldstern überarbeitet. Das Kapitel über Resolution wurde von Stefan Hetzl überarbeitet.

KAPITEL I

Naive Mengenlehre

I.1. Sinn der Mengenlehre

(1) Das Unendliche mit mathematischen Mitteln zu erforschen.
(2) universelle Sprache der Mathematik
(3) „hardware“ der Mathematik.

Zu Punkt 1: Die wesentliche Erkenntnis der Mengenlehre ist die, dass es verschiedene „Größen“ von unendlichen Mengen gibt. Sie haben vielleicht schon von „abzählbar“ und „überabzählbar“ gehört, das ist aber noch längst nicht alles, es gibt eine unendliche Skala von unendlichen „Kardinalitäten“, und diese Skala ist nicht nur unendlich lang, sondern natürlich überabzählbar — wie lang genau, das kann ich Ihnen nicht sagen, dafür müssen wir uns erst eine eigene Sprache schaffen. — Mehr dazu in ein paar Wochen, und auch im nächsten Semester, und wenn sich genügend Interessierte finden, auch in den folgenden Jahren.

Zu Punkt 2: Wir werden bereits in diesem Semester sehen, dass wir alle Objekte der Mathematik durch „reine“ oder „hereditäre“ Mengen interpretieren (oder „darstellen“) können.

Mit hereditär meine ich: auch die Elemente dieser Mengen sind wiederum Mengen, und die Elemente davon auch, etc. „Mengen bis ganz unten“ (Das ist deshalb ok, weil es bei der leeren Menge aufhört, bzw anfängt.)

Mit „darstellen“ meine ich: Wir werden zB Mengen finden, die wir als „natürliche Zahlen“ interpretieren können: sie sind alle verschieden, es gibt eine „erste“, zu jeder gibt es eine „nächste“, und es gilt das Prinzip der vollständigen Induktion für sie – wenn man davon ausgeht, dass die natürlichen Zahlen nur bis auf Isomorphie bestimmt sind, dann reicht uns das schon. Mehr dazu in den nächsten Wochen.

Zu Punkt 3: Es gibt Fragen in der „naiven“ Mathematik, die man mit den „üblichen“ Mitteln nicht lösen kann, und die im Kern mengentheoretischer Natur sind. Ein paar prominente Beispiele:

- Kontinuumshypothese (gibt es eine überabzählbare Teilmenge der reellen Zahlen, die nicht bijektiv auf alle reellen Zahlen abgebildet werden kann?
- Maßtheorie: Gibt es ein (nichttriviales) σ-additives Maß, welches *alle* Teilmengen von $\mathbb{R}$ misst?
- Funktionalanalysis: gibt es einen unstetigen Homomorphismus zwischen Banachalgebren?

- Algebra: Whiteheadproblem (über freie abelsche Gruppen: ist jede Whiteheadgruppe frei?)
- Topologie: Normal Moore space problem
- ...

Mehr darüber in guten Büchern, und (auf Wunsch) in Spezialvorlesungen.

I.2. Was ist eine Menge?

Cantor: eine Mengen ist die Zusammenfassung von wohlunterschiedenen Objekten unserer Anschauung zu einem Ganzen. Das ist zwar keine formale Definition, aber das zeigt schon ein Charakteristikum: Eine Menge ist nicht eine „Vielheit", sondern ein EINZIGES Objekt, eben ein „ganzes".

Beginnen wir gleich mit der historisch wohl ersten „mengentheoretischen Überlegung":

I.3. Der Satz von Cantor

Wir nennen eine unendliche Menge M „abzählbar", wenn es eine bijektive Abbildung von $\mathbb{N}$ nach M gibt. Jede unendliche Menge enthält eine abzählbare Teilmenge, ist also sozusagen „mindestens abzählbar". Cantor hat nun gezeigt, dass die Umkehrung nicht gilt: nicht jede unendliche Menge ist abzählbar, es gibt also unendliche Mengen, die man mit einem Abzählprozess nicht „ausschöpfen" kann.

Wir zeigen: Sei $M = \mathscr{P}(\mathbb{N})$, die Potenzmenge von $\mathbb{N}$. Dann ist M nicht abzählbar. Genauer: Sei $f : \mathbb{N} \to \mathscr{P}(\mathbb{N})$, dann gibt es ein $A \in \mathscr{P}(\mathbb{N})$ (das heißt: $A \subseteq \mathbb{N}$), A nicht im Wertebereich von f, also $A \notin f[\mathbb{N}]$, oder anders ausgedrückt: Für jedes $n \in \mathbb{N}$ ist $A \neq f(n)$.

Beweis: Sei

$$A := \{n : n \notin f(n)\}.$$

Wäre nun $A = f(n_0)$, dann überlegen wir: Ist $n_0 \in A$?

$n_0 \in A \Leftrightarrow n_0 \notin f(n_0) \Leftrightarrow n_0 \notin A$. Das ist ein Widerspruch, also kann es so ein n_0 nicht geben.

Zur Illustration betrachen Sie die folgende Abbildung f, die zB der Zahl 0 die Menge aller natürlichen Zahlen zuordnet, dann der Zahl 1 die leere Menge, dann die ungeraden Zahlen, die Primzahlen, usw.

$f(0) = \{\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ \ldots\ \}$
$f(1) = \{\ \ldots\ \}$
$f(2) = \{\ \ \ 1,\ \ \ 3,\ \ \ 5,\ \ \ 7,\ \ \ \ldots\ \}$
$f(3) = \{\ \ \ \ \ 2,\ 3,\ \ \ 5,\ \ \ 7,\ \ \ \ldots\ \}$
$\ldots$

Die Menge A, die sicher nicht im Wertebereich von f liegt, bekommt man, nun, wenn man in obigem Diagramm entlang der Diagonale geht:

$$
\begin{array}{ll}
f(0) = \{ & \mathbf{0},\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ \dots \} \\
f(1) = \{ & \quad\ \underline{\ \ },\quad\quad\quad\quad\quad\quad\quad\quad\ \dots \} \\
f(2) = \{ & \quad\ 1,\ \underline{\ \ },\ 3,\quad 5,\quad 7,\quad \dots \} \\
f(3) = \{ & \quad\quad 2,\ \mathbf{3},\quad 5,\quad 7,\quad \dots \} \\
f(4) = \{ & \ 0,\quad 2,\quad \mathbf{4},\quad 6,\quad 8,\ \dots \} \\
 & \quad\ \dots
\end{array}
$$

und das Komplement bildet, aus $\{0,\quad 3,4,\ldots\}$ entsteht $A = \{\ \ 1,2,\quad\quad ,\ldots\}$, und sicherlich ist $A \neq f(0)$ (weil ja $0 \in f(0)$, aber $0 \notin A$. Ebenso erhält man $A \neq f(1)$, etc.

Dieser Beweis ist also ganz analog zum Ihnen bekannten Beweis,[1] dass die reellen Zahlen überabzählbar sind.

Den obigen Beweis können wir verallgemeinern zu folgendem Satz: Sei X beliebige Menge, dann gibt es keine surjektive Funktion von X auf $\mathscr{P}(X)$, d.h: Wann immer $f : X \to \mathscr{P}(X)$, dann gibt es ein $A \subseteq X$, sodass es kein $x_0 \in X$ gibt mit $f(x_0) = A$.

Beweis: Sei $A := \{x \in X : x \notin f(x)\}$. ...

I.4. Die Russellsche „Antinomie“

Jetzt wird es aber schon recht eng. Sei nämlich M die Menge ALLER Mengen. Jedes Element von $\mathscr{P}(M)$ ist eine Teilmenge von M, also jedenfalls eine Menge, also ein Element von M. Damit haben wir eine surjektive Funktion von M nach $\mathscr{P}(M)$ gefunden: $x \mapsto x$ (und denjenigen Elementen von M, die keine Teilmengen von M sind, ordnen wir die leere Menge zu, also jedenfalls ein Element von $\mathscr{P}(M)$.)

Das scheint ein Widerspruch zu sein. Gehen wir zum vorigen Beweis zurück, da hatten wir eine Menge A konstruiert, die explizit nicht im Wertebereich von f sein kann:

$$A = \{x \in M : x \notin f(x)\} = \{x : x \notin x\} \cup \{x : x \not\subseteq M\}$$

[1] Genaugenommen hat das Cantor nicht so geschrieben, er hatte eine Arbeit über die reellen Zahlen geschrieben, in dieser Arbeit hat er bewiesen, dass es nur abzählbar viele algebraische Zahlen gibt, aber überabzählbar viele reelle Zahlen. Interessanterweise hat er diese Arbeit „Über eine Eigenschaft des Inbegriffs aller algebraischen Zahlen“ genannt, das Abzählbarkeitsresultat schien ihm also anscheinend wichtiger als das Überabzählbarkeitsresultat.

Mir scheint es aber so, dass die Idee der Überabzählbaren, also die Idee, dass man zwischen verschiedenen „Größen“ unendlicher Mengen unterscheiden kann, einer der wichtigsten Beiträge Cantors zur Mathematik war. Natürlich gibt es auch ganz andere Methoden, mit denen man unendliche Mengen ihrer „Größe“ nach unterscheiden kann, z.B. das Lebesguemaß oder die Hausdorffdimension, das sind aber immer Größenbegriffe, die nicht die Menge selbst sondern eine Struktur (zB eine geometrische Struktur) auf der Menge messen, die Begriffe „abzählbar“, „überabzählbar“, und allgemeiner „Kardinalität“ beschäftigen sich mit nackten Mengen.

Schauen wir uns das genauer an, und bezeichnen wir die erste dieser Mengen mit R:

$$R = \{x \in M : x \notin x\}$$

Dies ist die „Russelsche Paradoxie“, die Menge aller Mengen, die sich selbst nicht als Element enthalten, führt auf einen Widerspruch: Enthält sich diese Menge R selbst, oder nicht?

x ist genau dann in R, wenn x die Bedingung $x \notin x$ erfüllt.

Dies gilt für jedes x, also insbesondere auch für $x = R$:

R ist genau dann in R, wenn R die Bedingung $R \notin R$ erfüllt.

Das scheint zunächst sehr unangenehm, denn wenn diese Beweismethode der Diagonalisierung, die einen schönen Satz beweist, auch einen Widerspruch beweist, dann geht uns vielleicht dieser schöne Satz verloren. Vielleicht ist sogar das Begriffspaar Abzählbarkeit/Überabzählbarkeit in sich widerspruchsvoll?

Um dieses scheinbare Paradoxon aufzuklären, betrachten wir zwei ganz andere Beispiele:

Erstens, sei n_0 die kleinste natürliche Zahl. Dann ist $n_0 - 1$ aber noch kleiner, Widerspruch!

Der Widerspruch klärt sich auf: $n_0 - 1$ ist keine natürliche Zahl mehr! Vielleicht ist die „Menge“ R auch keine Menge mehr?!

Zweitens: Sei x_0 die kleinste positive reelle Zahl. Dann ist aber $x_0/2$ noch immer eine positive reelle Zahl,und kleiner – WIderspruch.

Aufklärung: Ein x_0 wie gewünscht „gibt es nicht“. Vielleicht ist das mit R so ähnlich?

Wir umschreiben einmal die Definition von R: R ist ja als Menge $\{x : x \notin x\}$ definiert, d.h: R sei eine Menge, die folgende Eigenschaft hat: für alle x gilt: x ist genau dann in R, wenn x kein Element von x ist.

Wie wir aber vorhin gesehen haben, gibt es so ein R einfach nicht! Das hat noch gar nichts mit Mengenlehre zu tun, das ist ein rein logischer Widerspruch. Wenn wir **irgendeine** zweistellige Relation ε betrachten, dann gilt genauso: Es gibt kein Objekt R mit der Eigenschaft: für alle x: $(x \varepsilon R \Leftrightarrow x \not\varepsilon x)$.

I.5. Das Komprehensionsprinzip

Wie sind wir denn überhaupt auf die Idee gekommen, dass es so eine Menge R geben soll? Die Idee, die hinter der Mengenbildung steckt, ist folgende:

(K1) Wann immer wir eine Eigenschaft $E(x)$ haben („x ist natürliche Zahl“, „x ist differenzierbare Funktion“, „x ist ein Fermatsches Tripel“ [leere Menge!]),
dann können wir die „Menge aller x, die E erfüllen“ bilden.

Anders ausgedrückt:

(K2) Für jede Eigenschaft $E(\cdot)$ gibt es eine Menge M_E, die folgendes erfüllt:

$$\forall x : x \in M_E \Leftrightarrow E(x)$$

Das nennen wir das *Komprehensionsprinzip.*[2]

Hier steckt wieder die Intuition dahinter, dass wir alle Objekte mit einer gemeinsamen Eigenschaft (die natürlichen Zahlen, die differenzierbaren Funktionen, etc.) als EIN GANZES begreifen können. Wenn sie von dem philosophischen Streit um aktual-Unendlich vs Potentiell-unendlich gehört haben, dann sehen Sie: die Mengenlehre steht klar auf der Seite des aktual-Unendlichen.

Dieses Komprehensionsprinzip ist also genau das, was wir wollen. Aber: `You can't always get what you want!`

Es wäre auch schön, wenn man immer Summe mit Integral vertauschen könnte, oder wenn Matrizenmultiplikation kommutativ wäre, aber es ist eben nicht so. Wir haben gesehen, dass dieses sehr allgemeine Komprehensionsprinzip auf einen Widerspruch führt, wenn wir für die Eigenschaft „$E(x)$“ „$x \notin x$“ einsetzen. Zumindest diese Eigenschaft müssen wir also aus unserem Komprehensionsprinzip ausklammern.

Auf welche anderen Eigenschaften dürfen wir Komprehension nicht anwenden? Da gibt es verschiedene Möglichkeiten, die zu verschiedenen Mengentheorien führen. Entweder man meint, das Übel liege darin, dass dieselbe Variable sozusagen gleichzeitig auf zwei verschiedenen Stufen vorkommt, als Element: $x \in$, und als Menge: $\in x$. Wenn man diesen Ansatz weiterverfolgt, kommt man zur Russellschen *Typentheorie*, oder zu Quines *New Foundations*, das sind beides „alternative“ Mengentheorien, die uns aber jedenfalls in diesem Semester nicht weiterhin beschäftigen werden.

Wir werden so vorgehen: Wir schreiben uns eine explizite Liste aller jenen Fälle des Komprehensionsprinzips auf, die wir zulassen wollen. Diese Liste nennen wir die Axiome. (Einige Axiome haben allerdings eine andere Form: Extensionalitätsaxiom, Auswahlaxiom.)

Ich werde dann versuchen, sie zu überzeugen (oder zu überreden),

(1) dass wir uns mit dieser harmlosen Liste keinen Widerspruch einhandeln.
(2) dass die in dieser Liste postulierten Mengen für die gesamte Mathematik als Grundlage ausreichen.
`But if you try sometimes you'll find: You'll get what you need...`

Bevor wir mit der Auflistung der Axiome beginnen, beschreiben wir einige mengentheoretische Konstruktionen, um ein besseres Gefühl dafür zu bekommen, was wir den eigentlich brauchen.

Wir werden im Aufbau unserer Mengenlehre einem „totalitären“ Kurs folgen: wir dürfen eine Menge M nur dann bilden, wenn wir aus den Axiomen schließen

[2]comprehendo 3, -di, -pr(eh)ensus: zusammenfassen; fassen, erfassen, begreifen

können, dass es so einen Menge M mit den gewünschten Eigenschaften auch wirklich gibt.

(Nicht alles, wofür man eine Beschreibung hat, existiert auch. Existenz und gegebenenfalls Eindeutigkeit müssen erst bewiesen werden. Beim Rechnen in einem Körper zum Beispiel darf man $\sqrt{x}$ auch nur dann hinschreiben, wenn man bereits weiß, das x eine Quadratwurzel hat, und Sie dürfen so etwas wie $z = x/y$ nur dann verwenden, wenn Sie wissen, dass $y \neq 0$ ist. In der Schule lernt man solche Dinge wie „durch 0 darf man nicht dividieren“ — ich würde das aber nicht als Verbot sehen, sondern als Abkürzung für den Sachverhalt: „Es gibt kein [eindeutig bestimmtes] z mit $z \cdot 0 = x$, daher ist der Ausdruck $x/0$ sinnlos“.)

I.6. Reine Mengen

Ein weiteres Prinzip, dem wir in der Mengenlehre folgen werden: Alle Objekte sind Mengen. Insbesondere auch alle Elemente aller Mengen, die wir betrachten werden. ALLE OBJEKTE SIND MENGEN! Es gibt also keine „Atome“ oder „Urelemente“, oder wenn es sie „gibt“, dann werden wir sie jedenfalls [zunächst] aus unseren Überlegungen ausklammern.

Warum diese Einschränkung? Das hat nur technische Gründe, man kann Mengenlehre auch über Atomen betreiben, und manchmal ist das auch nötig oder zumindest praktischer, aber wir werden das, zumindest in diesem Semester, nicht brauchen. Wie schon vorhin erwähnt, werden wir alle mathematischen Objekte durch Mengen darstellen oder „emulieren“. (Man kann aber ebenso ein Mengenlehre über einer vorgegebenen Menge von „Atomen“ oder „Urelementen“ aufbauen, das ist Geschmackssache; unser Vorgehen, die Mengenlehre ohne Atome, ist technisch einfacher.)

Leitlinien

1. Alle Objekte [die wir in dieser Vorlesung betrachten werden] sind Mengen.
2. Andere mathematische Objekte werden durch Mengen „emuliert“.

Das Komprehensionsprinzip:

> *Für jede Eigenschaft $E(\cdot)$ gibt es eine Menge M_E, die folgendes erfüllt:*
>
> $$\forall x : x \in M_E \Leftrightarrow E(x)$$

ist leider im Allgemeinen falsch (Beispiel: $E(x) =$ „$x \notin x$“), aber wir werden es trotzdem „vorsichtig“ anwenden, um die Bildung von Mengen zu rechtfertigen.

3. „vorsichtig“ heißt: nur in gewissen Fällen, die wir durch „Axiome“ beschreiben. D.h., die [meisten] Axiome fordern oder postulieren die Existenz gewisser Mengen.
4. Wir versuchen, alle Eigenschaften durch *Formeln* zu beschreiben.

I.7. Das geordnete Paar

Wir wollen mit Funktionen und Relationen arbeiten. Dafür brauchen wir den Begriff des „geordneten Paars (x, y)“. Wir wollen (x, y) (für alle Mengen x, y) definieren, wobei folgende Eigenschaft erfüllt sein muss:

$$(*) \qquad \forall x\, \forall y\, \forall x'\, \forall y' : (x, y) = (x', y') \;\Rightarrow\; x = x' \wedge y = y'$$

Wir wählen die Paardefinition von Kuratowski:

$$(x, y) := \{\{x\}, \{x, y\}\}$$

und zeigen, dass tatsächlich die Forderung $(*)$ erfüllt ist. [Beweis wird hier nicht ausgeführt.]

Definition: $A \times B := \{(x, y) : x \in A, y \in B\}$ oder ausführlicher

$$A \times B := \{z : (\exists x \in A)(\exists y \in B)\ z = (x, y)\},$$

d.h:

$$\forall z : z \in A \times B \;\Leftrightarrow\; \exists x \in A\ \exists y \in B : z = (x, y)$$

(die Forderung, dass diese Menge existiert, ist also wieder eine Instanz des Komprehensionprinzips.)

I.8. Relationen und Funktionen

Definition: R ist Relation, wenn jedes Element von R ein geordnetes Paar ist. R ist Relation von A nach B, wenn $R \subseteq A \times B$.

Definition: $\mathrm{dom}(R) = \{x : \exists y\, (x, y) \in R\}$, der „Definitionsbereich“ von R. Das ist meistens nur sinnvoll, wenn R eine Relation ist (aber im Prinzip für jede Menge R definiert).

Definition: $\mathrm{ran}(R) = \{y : \exists x\, (x, y) \in R\}$, der „Wertebereich“ von R.

Definition: f ist eine Funktion[3] von A nach B (wir schreiben auch $f : A \to B$), wenn $f \subseteq A \times B$, $\mathrm{dom}(f) = A$, und

$$\forall x \in A\, \forall y \in B\, \forall y' \in B : (x, y) \in f \wedge (x, y') \in f \;\Rightarrow y = y'$$

Wenn $f : A \to B$, dann definieren wir

$$f(x) = \{t : \exists y \in B\, [(x, y) \in f \wedge t \in y]\}$$

oder

$$f(x) = \{t : \forall y \in B\, [(x, y) \in f \Rightarrow t \in y]\}$$

[3] Das, was wir hier „Funktion“ nennen, nennen andere den Graph der Funktion. Gelegentlich wird gefordert dass eine Funktion F ein Wirklichkeit ein Tripel (A, f, B) ist, wobei A die Definitionsmenge von F ist, B die Zielmenge, und f der Graph von F; wir hingegen meinen mit einer Funktion den Graph der Funktion. (Achtung: daher ist „Surjektivität“ nicht mehr Eigenschaft einer Funktion, sondern eine Beziehung, die zwischen einer Funktion und einer Menge gelten kann.)

Diese beiden Definitionen sind äquivalent, weil es ja genau ein y mit $(x, y) \in f$ gibt.

Es ist leicht sehen (und nicht so schwer zu beweisen), dass für Funktionen $f, g : A \to B$ gilt:

$$f = g \;\Leftrightarrow \forall a \in A : f(a) = g(a)$$

NOTATION I.8.1. Wenn $f : A \to B$ eine Funktion ist, und $u \in A$, dann schreiben wir $f(u)$ für das (eindeutig bestimmte) $v \in B$ mit $(u, v) \in f$. Wir nennen v das Bild von u unter f.

Wenn $U \subseteq A$ ist, schreibt man für die Menge

$$\{v \mid (\exists u \in U)(u, v) \in f\} = \{v \mid (\exists u \in U)v = f(u)\} = \{f(u) \mid u \in U\}$$

oft $f(U)$. Das kann zu Verwirrung führen, wenn U zufällig nicht nur Teilmenge sondern auch Element[4] von A ist; daher nennen[5] wir diese Menge $f[U]$.

I.9. Endliche Mengen; die natürlichen Zahlen

Eine Menge E heißt endlich, wenn es eine bijektive Abbildung von E in eine beschränkte Menge von natürlichen Zahlen gibt. Aber was sind die natürlichen Zahlen? In dieser Vorlesung wollen wir natürliche Zahlen als Mengen darstellen.

- Es bietet sich an, die Zahl 0 mit der leeren Menge $\emptyset$ zu identifizieren: $0 := \emptyset$.
- Für die Zahl 1 hätten wir gerne eine Menge mit genau einem Element — wir definieren $1 := \{0\}$.
  (Beachten Sie dass dadurch $0 \neq 1$ garantiert wird.
- Da $0 \neq 1$ ist, hat die Menge $\{0, 1\}$ genau 2 Elemente. Wir setzen $2 := \{0, 1\}$.
- Und so weiter. $7 = \{0, 1, 2, 3, 4, 5, 6\} = \{0, 1, 2, 3, 4, 5\} \cup \{6\} = 6 \cup \{6\}$.
- Die Menge $\{0, 1, 2, \ldots\}$ wird oft mit $\mathbb{N}$, in der Mengenlehre aber meist mit ω bezeichnet.

Formal kann man die natürlichen Zahlen so definieren:

---

[4]Im nächsten Abschnitt werden wir $2 := \{0, 1\}$ und $3 := \{0, 1, 2\}$ definieren. Wenn nun f eine auf $\{0, 1, 2\}$ definierte Funktion ist, was ist dann mit $f(2) = f(\{0, 1\})$ gemeint, der Funktionswert an der Stelle 2 oder die Menge, die die beiden Funktionswerte $f(0)$ und $f(1)$ enthält?

[5]Die Schreibweisen $f`u$ für $f(u)$ wird nur selten verwendet; gelegentlich sieht man aber die Schreibweise $f``U$ für $f[U]$:

$$f``U = \{f`u : u \in U\}.$$

Diese Schreibweise lässt sich theoretisch für $\mathcal{U} \subseteq \mathscr{P}(A)$ auch auf

$$f```\mathcal{U} = \{f``U : U \in \mathcal{U}\}$$

verallgemeinern.

Definition: Eine Menge M heißt induktiv, wenn $\emptyset \in M$ ist und außerdem gilt:

$$\forall x : \ x \in M \ \Rightarrow \ S(x) \in M,$$

wobei[6] $S(x) := x \cup \{x\}$.

I.10. Folgen

Eine unendliche „Folge“ (von Elementen von A) ist eine Abbildung x mit $\mathrm{dom}(x) = \omega$ (und $\mathrm{ran}(x) \subseteq A$). Statt $x(n)$ schreiben wir manchmal x_n, und statt x schreiben wir manchmal $(x_0, x_1, \dots)$ (Hier sind die Punkte „...“ ok, denn wir wissen, was wir damit meinen)

Eine „endliche Folge“ ist eine Abbildung x mit $\mathrm{dom}(x) \in \omega$. $\mathrm{dom}(x)$ wird auch „Länge“ der Folge genannt. ZB ist

$$\{(0,3),(1,1),(2,4),(3,1),(4,5)\}$$

eine „Folge der Länge 4“. Diese Folge wird auch gerne als

$$\langle 3,1,4,1,5\rangle$$

geschrieben.[7]

I.11. Familien: eine *façon de parler*

Wenn A eine Menge ist, kann jedes Objekt x nur entweder $x \in A$ oder $x \notin A$ erfüllen, z.B. ist $\{7,7\}$ laut Definition $\{x : x = 7 \vee x = 7\}$, also $= \{7\}$. Wenn wir auch die Situation modellieren wollen, dass Elemente „mehrfach“ enthalten sind, verwenden wir Familien.

Definition: Eine „Familie“ ist einfach eine Funktion.

Wir nennen eine Funktion dann „Familie“, wenn es uns mehr auf den Wertebereich der Funktion als auf die Funktion selber ankommt.

Schreibweise: Sei $F : I \to A$ Familie. Wir schreiben oft F_i statt $F(i)$. Statt F schreiben wir auch oft $(F_i : i \in I)$. (Oder $(F_i \mid i \in I)$ oder $(F_i)_{i\in I}$ oder abkürzend $(F_i)_i$, oder — wenn der Kontext klar genug ist — nur (F_i).)

Den Definitionsbereich einer Familie nennen wir die „Indexmenge“ der Familie. Der Definitionsbereich von $(F_i : i \in I)$ ist also die Menge I.

Die Werte einer Familie nennen wir auch „Elemente“ der Familie, oder Einträge. Für die Familie $(F_i : i \in I)$ sind das also die Objekte F_i. (Wenn etwa $7 \in I$, dann

[6] Man beachte, dass hier x sowohl als Menge wie auch als Element auftritt: im Ausdruck $x \cup \{x\}$ spielt das erste x die Rolle einer Menge, weil uns hier nämlich die Elemente von x interessieren, die wir alle in $S(x)$ hineinpacken wollen. Das zweite x ist nur als weiteres Element interessant, das auch noch zu $S(x)$ gehört.

[7] Man kann auch runde Klammern für Folgen und spitze Klammern für Paare verwenden. In den meisten Fällen ist es gar nicht notwendig, z.B. zwischen Folgen der Länge 2 und Paaren zu unterscheiden.

ist F_7 der „Eintrag“ an der Stelle 7.) Ein Wert kann auch mehrmals vorkommen; wenn es zum Beispiel zwei verschiedene Indizes $i \neq j$ mit $F_i = F_j$ gibt, dann sagen wir, dass die Menge F_i mit Vielfachheit (mindestens) 2 vorkommt.

Definition: Wir nennen zwei Familien $(A_i : i \in I)$ und $(B_j : j \in J)$ „im wesentlichen gleich“, wenn es eine Bijektion („Umnummerierung“) $f : I \to J$ gibt, sodass für alle $i \in I$ $A_i = B_{f(i)}$ gilt. (Informell: Wenn sie die gleichen Werte mit der gleichen Vielfachheit haben.)

Beispiel: Sei $I = \{3, 4, 5\}$, $J = \{5, 12, 13\}$.

Sei $x_3 = 10 = y_{13}$, $x_4 = 100 = y_{12}$, $x_5 = 10 = y_5$. Dann sind $(x_i : i \in I)$ und $(y_j : j \in J)$ „im wesentlichen gleich“. (Sie modellieren beide eine „Multimenge“, die die Zahl 100 einmal und die Zahl 10 zweimal enthält.)

Wenn wir eine Funktion als Familie schreiben, deuten wir damit an, dass es uns bei dieser Funktion nicht auf Umnummerierungen ankommt.

Wenn wir zum Beispiel die Menge $\{(n, n*n) : n \in \mathbb{Z}\}$ als Funktion auffassen („die Quadrierungsfunktion ist eine gerade Funktion“), müssen wir sie von der Menge $\{(n+1, n*n) : n \in \mathbb{Z}\}$ unterscheiden.

Wenn wir aber von dieser Menge als Familie sprechen („in der Familie aller Quadratzahlen kommt jedes Element außer 0 doppelt vor“), deuten wir an, dass uns der Unterschied zwischen $\{(n, n*n) : n \in \mathbb{Z}\}$ und $\{(n+1, n*n) : n \in \mathbb{Z}\}$ nicht interessiert.

Schreibweise: Sei $F = (F_i : i \in I)$ Familie. Wir schreiben $\bigcup_{i \in I} F_i$ für $\bigcup \mathrm{ran}(F)$, also für die Menge $= \{y : \exists i \in I \; y \in F_i\}$.

I.12. Mengen von Mengen; große Vereinigung

Alle Objekte, die wir betrachten, sind Mengen. Wenn wir betonen wollen, dass wir ein Objekt A als Menge betrachten (also auch an Elementen $a \in A$ interessiert sind), verwenden wir Großbuchstaben.

Wenn wir betonen wollen, dass wir auch die Elemente eines Objekts $\mathscr{A}$ in ihrer Eigenschaft als Menge betrachten wollen, dann verwenden wir für diese Elemente Großbuchstaben (z.B. A), und für die „Menge der Mengen“ einen anderen Schrifttyp, z.B. $\mathscr{A}$.

Definition: Sei $\mathscr{A}$ eine Menge (von Mengen). Wir setzen

$$\bigcup \mathscr{A} := \{z : \exists B (z \in B \in \mathscr{A})\}.$$

Eine Menge von Mengen wird aus sprachästhetischen Gründen manchmal auch als „Familie von Mengen“ bezeichnet. Dies kann man so rechtfertigen: Zu jeder Menge $\mathscr{A}$ assozieren wir die Familie $(A_i : i \in I)$, die so definiert ist: Die Menge I ist einfach die Menge $\mathscr{A}$ selbst, und die Funktion $i \mapsto A_i$ ist die Identitätsfunktion

auf I. $\mathscr{A}$ (als Menge von Mengen betrachtet) ist also gleich der Menge der Werte von $\mathscr{A}$ (als Familie betrachtet).

I.13. $\mathbb{Q}$, $\mathbb{R}$, etc.

Die ganzen Zahlen $\mathbb{Z}$ erhalten wir in gewohnter Weise aus den natürlichen Zahlen: Wir definieren auf $\omega \times \omega$ die Äquivalenzrelation

$$(n,k) \sim (n',k') \;\Leftrightarrow\; (n+k' = k+n')$$

Die Menge der Äquivalenzklassen $\{(n,k)/\sim \,:\, n,k \in \omega\}$ bildet dann mit der Operation $(n,k)/\sim + (m,l)/\sim = (n+m, k+l)/\sim$ eine abelsche Gruppe, in die ω mit $n \mapsto (n,0)/\sim$ eingebettet wird. Diese Gruppe nennen wir $\mathbb{Z}$.

$\mathbb{Q}$ bekommen wir als Quotientenkörper von $\mathbb{Z}$.

$\mathbb{R}$ stellen wir uns als Äquivalenzklassen von Cauchyfolgen vor, oder als Dedekindschnitte (also gewisse Teilmengen von $\mathbb{Q}$).

I.14. Axiome, Teil 1

Die bisher informell betrachteten Operationen auf Mengen legen folgende Axiome[8] nahe:

Das erste Axiom sagt, dass Mengen durch ihren „Inhalt“ eindeutig bestimmt sind.

Extensionalitätsaxiom:

$$\forall A \forall B \left([\forall x : x \in A \Leftrightarrow x \in B] \;\Rightarrow\; A = B \right)$$

oder anders ausgedrückt:

$$\forall A \forall B \left(A \neq B \Rightarrow \exists x : (x \in A \& x \notin B \;\vee\; x \notin A \& x \in B) \right.$$

Das scheint vielleicht manchen selbstverständlich, aber betrachten sie zB folgende zwei Mengen:

- 1. $\{n > 2 : x^n + y^n = z^n$ hat nichttriviale Lösung $\}$.
- 2. $\{f : f$ ist differenzierbare aber nicht stetige Funktion von $[0,1]$ nach $[0,1]\}$.

Im ersten Fall steht eine Menge natürlicher Zahlen da, im zweiten Fall eine Menge von Funktionen. Können zwei solche Mengen einander gleich sein? Man könnte sagen, dass die beiden Mengen „intensional“[9] verschieden sind, aber „extensional“[10] nach gleich, nämlich leer.

---

[8] Die folgende Liste wurde von Zermelo aufgestellt, ca. 1904, später hat Skolem noch eine Ungenauigkeit beseitigt, und das letzte Axiom, das „Ersetzungsaxiom“, wurde erst später von Fraenkel hinzugefügt. Das Ersetzungsaxiom werden wir voraussichtlich in diesem Semester nicht brauchen.

[9] intendere = anspannen;sich wenden, streben nach; beabsichtigen

[10] extendere: ausspannen; sich ausbreiten, also Extension=die Spanne, hier: Inhalt

Mit diesem Axiom legen wir uns fest, dass für uns nur die „Extension“ Bedeutung hat.

Wir werden im Folgenden ein paar Instanzen des Komprehensionsprinzips als Axiome angeben. Jedenfalls wissen wir aber schon, wegen des Extensionalitätsaxioms: Zu jeder Eigenschaft $E(\cdot)$ gibt es *höchstens* eine Menge M_E mit:

$$\forall x : x \in M_E \Leftrightarrow E(x)$$

(Wären nämlich M und M' zwei solche Mengen, dann hätten sie die gleichen Elemente, wären also gleich.)

Wir bezeichen diese Menge E mit

$$\{x : E(x)\}$$

Ich betone aber noch einmal, dass wir uns eigentlich immer, wenn wir so eine Menge bilden, rechtfertigen müssen, dass die Bildung dieser Menge „erlaubt“ ist. (Gelegentlich werde ich so eine Rechtfertigung aber Ihnen als Übungsaufgabe überlassen.)

Nullmengenaxiom: $\exists N : \ \forall x\, x \notin N$, oder mit anderen Worten:

$$\exists N : (\forall x : x \in N \Leftrightarrow x \neq x)$$

Zusammen mit dem Extensionalitätsaxiom sehen wir sofort, dass es genau eine Nullmengen gibt, wir nennen sie $\emptyset$ oder $\{\ \}$.

Singletonaxiom:

$$\forall a\, \exists A : \forall x \big(x \in A \Leftrightarrow x = a\big)$$

also es wird die Existenz einer Menge $\{x : x = a\}$, auch kurz $\{a\}$ genannt, postuliert.

Kleines Vereinigungsaxiom.

$$\forall A\, \forall B\ \exists C : \forall x (x \in C \Leftrightarrow x \in A \vee x \in B)$$

es wird also die Existenz einer Menge $\{x : x \in A \vee x \in B\}$ postuliert, die wird kurz $A \cup B$ genannt.

(Wir werden später sehen, dass diese drei Axiome eigentlich überflüssig sind, weil sie aus anderen Axiomen folgen, die wir später behandeln werden.)

Paarmengenaxiom. $\forall x\, \forall y\, \exists p$:

$$\forall z [z \in p \Leftrightarrow z = x \vee z = y] \qquad (\text{also } p = \{x, y\})$$

Vereinigungsmengenaxiom.

$$\forall \mathscr{A}\ \exists S : \forall z [z \in S \Leftrightarrow \exists B \in \mathscr{A}\ z \in B]$$

D.h., S enthält sozusagen genau die „Elemente zweiter Stufe“ von $\mathscr{A}$. Da es genau eine Menge S wie oben beschrieben gibt, ist es sinnvoll, für sie einen neuen Namen einzuführen:

$$\bigcup \mathscr{A} := \{z : \exists B(z \in B \in \mathscr{A})\}$$

Beispiel 1: Sei $\mathscr{A} = \{P, Q\}$. Dann ist

$$\bigcup \mathscr{A} = \{x : \exists R \in \{P, Q\}(x \in R)\} = \{x : x \in P \vee x \in Q\} = P \cup Q.$$

Beispiel 2: Sei $\mathscr{A} = \{\{0, 3\}, \{1, 3\}, \{\}\}$, dann ist $\bigcup \mathscr{A} = \{0, 3,\ 1, 3\ \ \} = \{0, 1, 3\}$. [Die Operation $\bigcup$ „nimmt Mengenklammern weg“].
Beispiel 3: Sei $\mathscr{A} = 5 = \{0, 1, 2, 3, 4\} = \{\,\{\}, \{0\}, \{0, 1\}, \{0, 1, 2\}, \{0, 1, 2, 3\}\,\}$. Dann ist

$$\bigcup \mathscr{A} = \{\ 0,\ 0, 1,\ 0, 1, 2,\ 0, 1, 2, 3\} = \{0, 1, 2, 3\} = 4$$

Allgemein ist für $n \in \omega$: $\bigcup S(n) = n$. [Beweis?]

I.15. Potenzmengenaxiom

Zu jeder Menge A gibt es ihre „Potenzmenge“, also eine Menge P, die [genau] alle Teilmengen von A enthält:

$$\forall A\, \exists P : \forall z[z \in P \Leftrightarrow z \subseteq A]$$

Wir schreiben

$$\mathscr{P}(A) = \{B : B \subseteq A\}$$

I.16. Produktmenge etc

Wir können nun die Bildung von Produktmenge und anderen Mengen „rechtfertigen“: Seien A und B Mengen. Wenn $a \in A$, $b \in B$, dann sind $\{a\}$ und $\{a, b\}$ Teilmengen von $A \cup B = \bigcup\{A, B\}$.
Also $\{a\}, \{a, b\} \in \mathscr{P}(A \cup B)$, daher $(a, b) = \{\{a\}, \{a, b\}\} \subseteq \mathscr{P}(A \cup B)$, daher

$$(a, b) \in \mathscr{P}(\mathscr{P}(A \cup B)).$$

Also ist $A \times B = \{z \in \mathscr{P}(\mathscr{P}(A \cup B)) : \exists a \in A\, \exists b \in B : z = (a, b)\}$, daher ist die Existenz der Produktmengen aus einer Instanz des Aussonderungsaxioms (zusammen mit Potenzmengenaxiom, Paarmengenaxiom und Vereinigungsmengenaxiom) beweisbar.
Wir können auch die Bildung der Menge

$${}^{B}A := \{f :\ f \text{ Funktion von } A \text{ nach } B\}$$

rechtfertigen.
Weiters: $\mathrm{dom}(R) = \{x : \exists y\,(x, y) \in R\} = \{x \in \bigcup\bigcup R : \exists y\,(x, y) \in R\}$ [denn wenn $(x, y) \in R$, dann ist $x \in \{x\} \in (x, y) \in R$]
Ähnlich $\mathrm{ran}(R) = \{y : \exists x\,(x, y) \in R\}$.

I.17. Rekursive Definition

Satz: es gibt genau eine „Addition“ auf ω. Das heißt, es gibt genau eine Funktion $f : \omega \times \omega \to \omega$ mit folgenden Eigenschaften:

- 1. $\forall n \in \omega : f(\langle n, 0\rangle) = n$
- 2. $\forall n \in \omega \forall k \in \omega : f(\langle n, S(k)\rangle) = S(f(\langle n, k\rangle))$.

Beweisskizze: Wir nennen eine Menge $A \subseteq (\omega\times\omega)\times\omega$ „additiv“, wenn sie folgendes erfüllt:

- Für alle $x \in \omega$ ist $((x, 0), x) \in A$.
- Für alle $x, y, z \in \omega$: Wenn $((x, y), z) \in A$, dann auch $((x, y+1), z+1) \in A$. Mit $y + 1$ ist hier der Nachfolger gemeint: $y + 1 = y \cup \{y\}$.

Die ganze Menge $\omega \times \omega \times \omega$ ist sicher induktiv. Man kann daher den Durchschnitt $f := \bigcap\{ A \mid A \text{ induktiv} \}$ bilden. Den Beweis, dass f nun tatsächlich eine Funktion ist, und die Peano-Axiome für die Addition erfüllt, führen wir hier nicht aus.

Ähnlich kann man andere zahlentheoretische Funktionen (wie z.B. Multiplikation und Exponentiation) definieren.

I.18. Rekursive Definition, Verallgemeinerungen

Der Bildbereich so einer „rekursiv“ definierten Funktion muss nicht ω sein. Es gilt allgemeiner:

Satz: Sei C eine Menge, sei $h : C \to C$, $a \in \omega$. Dann gibt es genau eine Funktion $f : \omega \to C$, die $f(0) = a$ und $f(S(n)) = h(f(n))$ für alle $n \in \omega$ erfüllt.

Beweis ähnlich.

Es gilt sogar noch allgemeiner:

Satz: Sei $h : \omega \times C \to C$, $a \in \omega$. Dann gibt es genau eine Funktion $f : \omega \to \omega$, die $f(0) = a$ und $f(S(n)) = h(n, f(n))$ erfüllt.

Oder noch allgemeiner, mit „Parametern“:

Satz: Sei A eine Menge. Sei $h : A \times \omega \times C \to C$, $g : A \to C$. Dann gibt es genau eine Funktion $f : A \times \omega \to C$, die $f(a, 0) = g(a)$ (für alle a) und $f(a, S(n)) = h(a, n, f(n))$ (für alle $a \in A$ und alle $n \in \omega$) erfüllt.

Mit den Funktionen $g : \omega \to \omega$, $g(n) = n$, und $h : \omega\times\omega\times\omega \to \omega$, $h(a, n, c) = S(c)$ erhalten wir eine Funktion $f : \omega\times\omega \to \omega$, die $f(a, 0) = a$, $f(a, S(n)) = S(f(a, n))$ erfüllt, also genau die Addition. Statt $f(a, n)$ schreiben wir künftig $a + n$. Statt $S(n)$ schreiben wir ab jetzt auch meistens $n + 1$.

Multiplikation und Exponentiation ähnlich.

I.19. Bäume

Bäume sind ein wichtiges Konzept der diskreten Mathematik, das vor allem in der Logik und der Informatik Anwendungen hat. Wir werden im Lauf dieser Vorlesung immer wieder Bäumen begegnen. In der Graphentheorie werden Bäume als zusammenhängende kreisfreie Graphen definiert, und Wurzelbäume als Bäume mit einem ausgezeichneten Knoten. Wir verwenden eine andere Definition, die aber auf einen ganz ähnlichen Begriff führt:

DEFINITION I.19.1. Ein Baum ist eine partielle Ordnung $(T, \leq)$ mit folgenden Eigenschaften:

- T hat ein kleinstes Element, die „Wurzel".
- Für alle $t \in T$ ist die Menge $T_{<t} := \{x \in T : x < t\}$ endlich[11] und durch $\leq$ linear geordnet.

Die Elemente von T heißen oft auch „Knoten"[12] von T. Die Anzahl der Elemente von $T_{<t}$ heißt die „Höhe" von t. Die Elemente der Höhe h bezeichnen wir mit $T(h)$, die Elemente der Höhe $< h$ mit T_h oder $T(<h)$.

Die Höhe des Baums ist das kleinste h mit $T(h) = \emptyset$; wenn jedes Zahl $n \in \mathbb{N}$ Höhe eines Knoten ist, dann sei die Höhe von H „unendlich", was meist durch das Symbol ω beschrieben wird. Zum Beispiel hat ein einelementiger Baum Höhe 1, ein 3-elementiger kann Höhe 2 oder 3 haben.

Für $s \in T$ bezeichnen wir mit $succ_T(s)$ die Menge aller „direkten Nachfolger" von s; wenn s die Höhe h hat, dann enthält $succ_T(s)$ alle $t > s$ mit Höhe $h + 1$.

Ein „Ast" ist eine maximale linear geordnete Teilmenge von T. Jedes maximale Element eines Baums heißt „Blatt"; dies sind genau jene Elemente s von T, die $succ_T(s) = \emptyset$ erfüllen.

DEFINITION I.19.2. Sei X eine beliebige Menge. Ein Folgenbaum auf X ist eine nichtleere Teilmenge $F \subseteq X^{<\omega}$ (also eine Menge von endlichen Folgen von Elementen von X), die unter Anfangsabschnitten abgeschlossen ist:

$$t \in F \cap X^n, k < n \ \Rightarrow t{\restriction}k \in F$$

(Insbesondere muss die leere Folge auch in F sein.)

Wenn F ein Folgenbaum ist, und $s, t \in F$, dann gilt $s \subseteq t$ genau dann, wenn s ein Anfangsstück von t ist, also von der Form $t{\restriction}k$. Jeder Folgenbaum ist zusammen mit der Relation $\subseteq$ ein Baum.

Umgekehrt ist jeder Baum T mit Wurzel w in natürlicher Weise zu einem Folgenbaum ordnungsisomorph: Zunächst können wir jedem Element t die Menge $T_{\leq t} := \{s \in T : s \leq t\}$ zuordnen; wenn t die Höhe k hat, dann hat $T_{\leq t}$ genau $k+1$

[11] In der Mengenlehre lässt man auch Bäume zu, deren Elemente unendlich viele Vorgänger haben können; in diesem Fall verlangt man, dass $T_{<t}$ eine Wohlordnung ist.

[12] englisch: nodes

Elemente; wir können die Elemente von $T_{\leq t} \setminus \{w\}$ in ihrer natürlichen Ordnung als Folge $f(t) := \langle t_1, \ldots, t_k \rangle$ mit $t_k = t$ schreiben, und wir definieren $f(w) := \langle\rangle$. Nun ist die Menge $F := \{f(s) : s \in T\}$ ein Folgenbaum, und $f : T \to F$ ist Ordnungsisomorphismus.

Sei M eine Menge von Klauseln (in den Variablen $p_0, p_1, \ldots$). Jede Folge $\bar{s} = (c_0, \ldots, c_{k-1})$ mit Einträgen in $\{0, 1\}$ definiert in natürlicher Weise eine Belegung $b_{\bar{s}}$ der Variablen $p_0, p_1, \ldots, p_{k-1}$ durch $b_{\bar{s}}(p_i) = c_i$. Wir sagen, dass eine Klausel $C \in M$ eine Folge $\bar{s}$ verbietet, wenn $\hat{b}_{\bar{s}}$ auf allen Elementen von C definiert ist und den Wert 0 hat.

Dann bildet die Menge T_M aller Folgen, die nicht durch ein $C \in M$ verboten werden, einen Baum. Jeder unendliche Ast durch diesen Baum definiert eine Belegung, die alle Klauseln in M erfüllt.

Wenn es keinen unendlichen Ast in T_M gibt, dann muss T_M endlich sein, und man kann (durch Induktion nach der Größe von T_M, oder nach der Höhe von M) zeigen, dass man aus den Klauseln in M durch Resolution die leere Klausel gewinnen kann.

HILFSSATZ I.19.3. *Sei T ein Baum. Dann sind die folgenden Aussagen äquivalent:*

- *Jedes $s \in T$ hat endlich viele direkte Nachfolger.*
- *Für alle $h \in \mathbb{N}$ ist $T(h)$ endlich.*

BEWEIS. Mit Induktion. □

SATZ I.19.4 (Lemma von König). *Sei T ein Baum, in dem jedes Element nur endlich viele direkte Nachfolger hat. Die folgenden Aussagen sind äquivalent:*

(1) *T hat unendlich viele Knoten.*
(2) *T hat Höhe ω.*
(3) *T hat einen unendlichen Ast.*

Wenn T überdies ein Folgenbaum auf X ist, dann ist die letzte Aussage äquivalent zu:

(3') *Es gibt eine Funktion $f : \mathbb{N} \to X$ mit: $\forall k \in \mathbb{N} : \langle f(0), \ldots, f(k-1) \rangle \in T$.*

BEWEIS. Die Implikationen (3)⇒(2) und (2)⇒(1) sind klar. Wir zeigen (1)⇒(3). Sei T ein unendlicher Baum, in dem jeder Knoten nur endlich viele Nachfolger hat. Wir konstruieren eine Folge $t_0 < t_1 < \cdots$ in T, in dem jedes t_k Höhe k hat, und außerdem für alle k die Bedingung

$$T_{\geq t_k} := \{x \in T : t_k \leq x\} \text{ ist unendlich}$$

erfüllt ist. Sei t_0 die Wurzel von T.

Wenn t_k gegeben ist, und $S := succ_T(t_k)$, dann ist

$$T_{\geq t_k} = \{t_k\} \cup \bigcup_{s \in S} T_{\geq s}.$$

Die unendliche Menge $T_{\geq t_k} \setminus \{t_k\}$ ist also die Vereinigung von endlich vielen (disjunkten) Mengen $T_{\geq s}$; mindestens eine dieser Mengen muss unendlich sein, wir können also ein $t_{k+1} \in succ_T(t_k)$ wählen[13], sodass $T_{\geq t_{k+1}}$ unendlich ist.
Insgesamt ist $\{t_0, t_1, \dots\}$ ein unendlicher Ast. □

Anmerkung: Es gibt Bäume der Höhe 1 mit unendlich vielen Knoten. Es gibt auch Bäume der Höhe ω ohne unendlichen Ast. Man betrachte zum Beispiel den Folgenbaum aller strikt absteigenden endlichen Folgen von natürlichen Zahlen:

$$\{\langle a_0, \dots, a_n\rangle : n \in \mathbb{N}, \forall i\ a_i \in \mathbb{N}, a_0 > \dots > a_n\}.$$

Wenn man von der Wurzel absieht, hat jeder Knoten nur endlich viele Nachfolger.

[13]Um die Existenz der gesamten Folge alle t_k sicherzustellen, muss man hier das Auswahlaxiom verwenden.

KAPITEL II

Aussagenlogik

II.1. 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.

II.1.A. 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.

---

[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 23

[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.

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

> 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 II.1.1. 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 II.1.2. 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 II.1.7 und II.1.8) werden manchmal andere Symbole (wie z.B. $\equiv$ oder $\dot{\leftrightarrow}$) verwendet.

II.1.B. 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 II.1.3 (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 II.1.4 (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 II.1.5. *Sei b eine Belegung der Variablen in V. Dann gibt es eine eindeutig bestimmte Wahrheitsfunktion $\hat{b}$ 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 $\hat{b}$ die Bedingung

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

erfüllen, also $\hat{b}(A) = 0$.

SATZ II.1.6. *Seien φ, ψ Formeln. Dann sind die folgenden Aussagen äquivalent:*

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

DEFINITION II.1.7. 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 II.1.8 (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 $\hat{b}(\varphi) = \hat{b}(\psi)$.
Offensichtlich ist $\Leftrightarrow$ eine Äquivalenzrelation.

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

SATZ II.1.9. *$A \Leftrightarrow B$ gilt genau dann, wenn $A \leftrightarrow B$ eine Tautologie ist.*

DEFINITION II.1.10 (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 $\hat{b}(\varphi)$ 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. $V = \{p_1, \dots, p_n\}$) 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 $\hat{b}(\varphi) \in \{0, 1\}$ zuordnet.
  (Diese Variante scheint komplizierter als die vorige zu sein; sie ist aber erstens zur vorigen äquivalent, weil man zeigen kann, dass $\hat{b}(\varphi)$ 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 $p_1 \mathbin{\dot{\wedge}} p_2$. 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 II.1.11 (Tautologie). Eine Formel φ heißt Tautologie, wenn für alle Belegungen b gilt: $\hat{b}(\varphi) = 1$

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

Bemerkung II.1.12. 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) $\hat{b}(\varphi) = 0$ 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 II.1.13 (Kontradiktion, Erfüllbarkeit). Wir sagen, dass eine Belegung b eine Formel φ *erfüllt*, wenn $\hat{b}(\varphi) = 1$ 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: $\hat{b}(\varphi) = 0$, 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 $\hat{b}(\varphi) = 1$ 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 II.3.14.)

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 $\hat{b}(q \vee r \to s)$ 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.

Allgemeiner kann man sich Folgendes überlegen:

DEFINITION II.1.14 (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]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.

(6) $f(\bot) = \bot$

nennt man Formelhomomorphismus.

BEMERKUNG II.1.15. 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 II.1.16. *Sei φ eine Tautologie und f ein Formelhomomorphismus, dann ist $f(\varphi)$ ebenfalls Tautologie.*

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

II.1.C. Einige wichtige Tautologien und Äquivalenzen. Die Formeln in der linken Spalte sind Tautologien (p, q, r, p_1, p_2 sind aussagenlogische Variable). Mit Hilfe der Sätze II.1.9 und II.1.16 ergibt sich, dass für beliebige Formeln A, B, C, A_1, A_2 die Äquivalenzen in der rechten Spalte gelten.

$\neg\neg p$	$\leftrightarrow$	p	$\neg\neg A$	$\Leftrightarrow$	A
$\neg(p \wedge q)$	$\leftrightarrow$	$(\neg p \vee \neg q)$	$\neg(A \wedge B)$	$\Leftrightarrow$	$(\neg A \vee \neg B)$
$\neg(p \vee q)$	$\leftrightarrow$	$(\neg p \wedge \neg q)$	$\neg(A \vee B)$	$\Leftrightarrow$	$(\neg A \wedge \neg B)$
$\neg(p \to q)$	$\leftrightarrow$	$(p \wedge \neg q)$	$\neg(A \to B)$	$\Leftrightarrow$	$(A \wedge \neg B)$
$p \vee q$	$\leftrightarrow$	$q \vee p$	$A \vee B$	$\Leftrightarrow$	$B \vee A$
$p \wedge q$	$\leftrightarrow$	$q \wedge p$	$A \wedge B$	$\Leftrightarrow$	$B \wedge A$
$p_1 \to (p_2 \to r)$	$\leftrightarrow$	$p_1 \wedge p_2 \to r$	$A_1 \to (A_2 \to C)$	$\Leftrightarrow$	$A_1 \wedge A_2 \to C$
$p \vee (q \wedge r)$	$\leftrightarrow$	$(p \vee q) \wedge (p \vee r)$	$A \vee (B \wedge C)$	$\Leftrightarrow$	$(A \vee B) \wedge (A \vee C)$
$p \wedge (q \vee r)$	$\leftrightarrow$	$(p \wedge q) \vee (p \wedge r)$	$A \wedge (B \vee C)$	$\Leftrightarrow$	$(A \wedge B) \vee (A \wedge C)$
$(p \to q)$	$\leftrightarrow$	$(\neg q \to \neg p)$	$(A \to B)$	$\Leftrightarrow$	$(\neg B \to \neg A)$
$(p \to \neg q)$	$\leftrightarrow$	$(q \to \neg p)$	$(A \to \neg B)$	$\Leftrightarrow$	$(B \to \neg A)$
$(\neg p \to q)$	$\leftrightarrow$	$(\neg q \to p)$	$(\neg A \to B)$	$\Leftrightarrow$	$(\neg B \to A)$

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

[8] Siehe Fußnote auf Seite 23

Die erste Zeile[9] (je nach Geschmack auch nur die linke oder rechte Hälfte der ersten Zeile) heißt „Satz von der doppelten Verneinung“, die zweite und dritte heißen „Gesetze von de Morgan“. Die Zeilen, wo p, q, r bzw A, B, C vorkommen, heißen Distributivgesetze. Die letzten drei Zeilen heißen „Kontraposition“.

Weitere wichtige (und/oder „benannte“) Tautologien sind:

- der Satz von ausgeschlossenen Dritten („tertium non datur“): $A \vee \neg A$
- der Satz vom Widerspruch: $\neg(A \wedge \neg A)$.
- „ex falso quodlibet“: $\bot \to A$
- „e quolibet verum“: $A \to \top$

Die Aussagen $p \wedge (p \to q) \Rightarrow q$ bzw. $(p \to q) \wedge (\neg q) \Rightarrow \neg p$ (oder auch die ihnen zugeordneten Tautologien) heißen manchmal auch „Modus ponens“ bzw. „Modus tollens“; der Begriff „Modus ponens“ wird für uns eine geringfügig andere Bedeutung haben.

Die Aussagen $(p \to \bot) \Rightarrow \neg p$, $\neg p \to \bot \Rightarrow p$ oder auch Varianten wie $q \wedge (\neg p) \to \bot \Rightarrow q \to p$ heißen manchmal „Prinzip vom indirekten Beweis“.

II.2. Konjunktive und disjunktive Normalform

DEFINITION II.2.1 (Literal). Unter einem Literal versteht man eine aussagenlogische Variable, oder eine negierte aussagenlogische Variable.

DEFINITION II.2.2 (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 II.2.3. Die Nomenklatur ist nicht ganz einheitlich. Auf Englisch heißt eine Disjunktion von Literalen *clause*; dies wird im Deutschen mit „Klausel“ übersetzt.

DEFINITION II.2.4 (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.)

[9] In nichtklassischen Logiken sind nicht alle diese Formeln Tautologien. Zum Beispiel gilt in der intuitionistischen Logik zwar $A \Rightarrow \neg\neg A$, aber nicht immer auch die andere Richtung.

DEFINITION II.2.5 (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 II.2.6. *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 $\hat{b}_i$.

p_1	p_2	p_3	$\neg p_1 \vee \neg p_3$	$p_2 \to (\neg p_1 \vee \neg p_3)$	$p_1 \wedge (p_2 \to (\neg p_1 \vee \neg p_3))$
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 II.2.7. 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 II.2.8. *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 II.2.9. Die Erzeugung einer zu einer vorgegebenen Formel äquivalenten KNF oder DNF mit obigem Algorithmus ist sehr ineffizient da er zu einer Formel, in der n Variable vorkommen, alle 2^n Belegungen durchprobieren muss.

Es gibt allerdings auch Transformationen in KNF die wesentlich effizienter sind und zu einer gegebenen Formel eine erfüllbarkeitsäquivalente Formel in KNF in linearer Zeit erzeugen.

II.3. Aussagenlogische 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 $\hat{b}(C) = 1$ genau dann, wenn es ein Literal $L \in C$ gibt mit $\hat{b}(L) = 1$. 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 $\hat{b}(M) = 1$ genau dann, wenn *für alle* $C \in M$ die Beziehung $\hat{b}(C) = 1$

gilt; anders ausgedrückt: M ist genau dann erfüllbar, wenn es zu jeder Klausel $C \in M$ ein Literal $L \in C$ gibt mit $\hat{b}(L) = 1$.

BEMERKUNG II.3.1. 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 II.3.2 (Resolvente). Seien C und D Klauseln, sodass $p \in C$ und $\neg p \in D$. Dann bezeichnen wir die Klausel

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

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

DEFINITION II.3.3. Sei M eine Klauselmenge. Eine endliche Liste $C_1, \ldots, C_n$ von Klauseln heißt *Resolutionsableitung* aus M falls für alle $i \in \{1, \ldots, n\}$ gilt:

(I) $C_i \in M$, oder
(R) es gibt $j, k < i$ und ein Atom p so dass $C_i = \mathrm{res}_p(C_j, C_k)$.

Eine Resolutionsableitung $C_1, \ldots, C_n$ aus M heißt *Resolutionswiderlegung von M* falls $C_n = \emptyset$.

BEISPIEL. Sei $M = \{\{p_1\}; \{\neg p_1, p_2\}; \{\neg p_1, \neg p_2, p_3\}, \{\neg p_3\}\}$. Die folgende Liste von Klauseln ist eine Resolutionswiderlegung von M:

(1) $\{\neg p_1, p_2\}$ (I)
(2) $\{\neg p_1, \neg p_2, p_3\}$ (I)
(3) $\{\neg p_1, p_3\}$ $(R(1,2))$

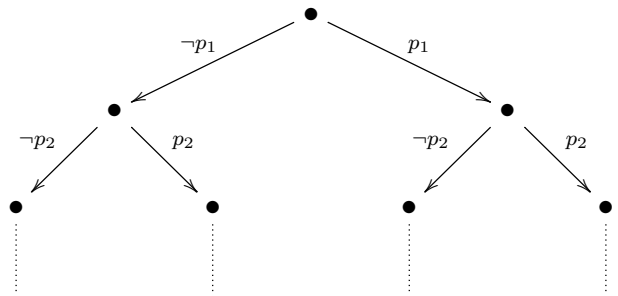
(4) $\{p_1\}$ (I)
(5) $\{p_3\}$ $(R(3,4))$
(6) $\{\neg p_3\}$ (I)
(7) $\emptyset$ $(R(5,6))$

SATZ II.3.4 (Korrektheit). *Falls M eine Resolutionswiderlegung hat, dann ist M unerfüllbar.*

BEWEIS. Wir zeigen die folgende etwas allgemeinere Aussage: Falls $C_1, \ldots, C_n$ eine Resolutionsableitung aus M ist und b eine Belegung die M erfüllt, dann erfüllt b auch C_n. Wir gehen mit Induktion nach n vor. Die Aussage ist klar falls $C_n \in M$. Falls $C_n = \mathrm{res}_p(C_i, C_j)$ dann gilt nach Induktionshypothese $\hat{b}(C_i) = \hat{b}(C_j) = 1$. Wir machen eine Fallunterscheidung nach dem Wert von $b(p)$. Ist $b(p) = 1$ und $C_j = \{\neg p, L_1, \ldots, L_k\}$ dann muss $\hat{b}(\{L_1, \ldots, L_k\}) = 1$ und damit $\hat{b}(C_n) = 1$. Der Fall $b(p) = 0$ ist symmetrisch. □

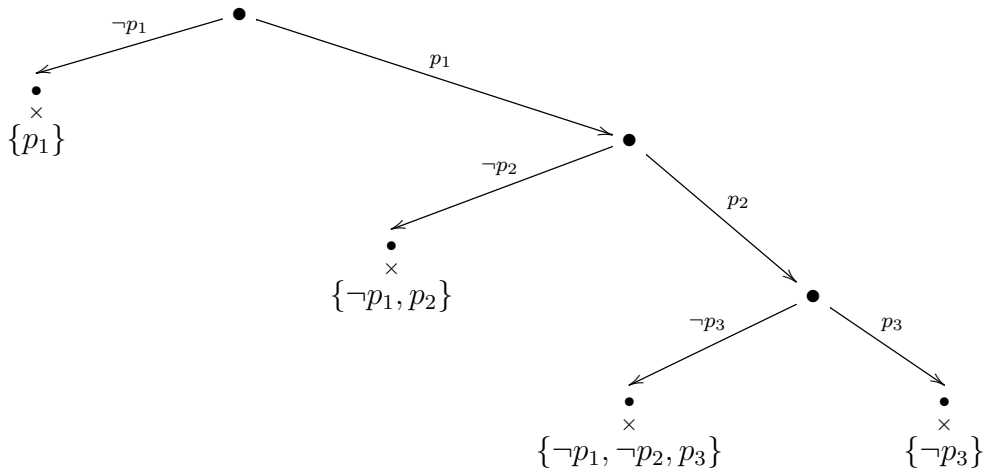
Um die Vollständigkeit der Resolution zu zeigen, benötigen wir als Hilfmittel *semantische Bäume*.

DEFINITION II.3.5. Sei $(p_i)_{i\geq 1}$ eine Folge von aussagenlogischen Variablen. Der semantische Baum von $(p_i)_{i\geq 1}$ ist dann der folgende Baum



in dem jeder Ast unendlich ist. Jeder Knoten v in diesem Baum induziert eine partielle Belegung b_v von $\{p_1, p_2, \ldots\}$ wobei p_i auf 1 gesetzt wird falls p_i auf dem Pfad von v zur Wurzel vorkommt und auf 0 falls $\neg p_i$ auf diesem Pfad vorkommt. Sei M eine Klauselmenge die nur Variablen aus $\{p_i \mid i \geq 1\}$ enthält. Der semantische Baum von M, notiert als $\mathcal{B}(M)$, ist dann aus obigem Baum dadurch definiert, dass ein Ast nach endlich vielen Schritten an einem Knoten v geschlossen wird genau dann wenn es ein $C \in M$ gibt mit $\hat{b_v}(C) = 0$. Das wird notiert als:

BEISPIEL. Sei $M = \{\{p_1\}; \{\neg p_1, p_2\}; \{\neg p_1, \neg p_2, p_3\}, \{\neg p_3\}\}$ die Klauselmenge aus Beispiel II.3. Der semantische Baum $\mathcal{B}(M)$ ist:



BEMERKUNG II.3.6. Die Forderung, einen Knoten v zu schließen *genau dann wenn* es ein $C \in M$ gibt mit $\hat{b_v}(C) = 0$ hat zur Folge, dass ein Ast so früh wie möglich (d.h. so nahe an der Wurzel wie möglich) geschlossen wird.

BEMERKUNG II.3.7. Falls M die Leerklausel $\emptyset$ enthält, dann besteht $\mathcal{B}(M)$ nur aus einem einzigen Knoten der durch $\emptyset$ geschlossen wird.

BEMERKUNG II.3.8. M ist erfüllbar genau dann wenn $\mathcal{B}(M)$ einen unendlichen Ast hat. Sei nämlich b eine Belegung von $\{p_1, p_2, \ldots\}$ die M erfüllt, dann induziert b einen unendlichen Ast. Und umgekehrt: ein unendlicher Ast wird niemals geschlossen, die durch ihn induzierte Belegung erfüllt deshalb alle $C \in M$ und damit M selbst.

BEMERKUNG II.3.9. M ist unerfüllbar genau dann wenn $\mathcal{B}(M)$ endlich ist. Nach dem Satz von König (Satz I.19.4) gilt ja dass $\mathcal{B}(M)$ unendlich ist genau dann wenn $\mathcal{B}(M)$ einen unendlichen Ast hat. Damit folgt diese Aussage direkt aus Bemerkung II.3.8.

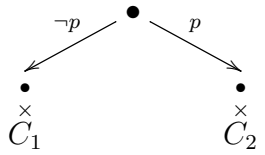
BEMERKUNG II.3.10. Falls $M \subseteq M'$ dann ist $\mathcal{B}(M) \supseteq \mathcal{B}(M')$ denn jeder Knoten, der in $\mathcal{B}(M)$ geschlossen werden kann kann auch in $\mathcal{B}(M')$ geschlossen werden.

SATZ II.3.11 (Vollständigkeit). *Falls M unerfüllbar ist, dann hat M eine Resolutionswiderlegung.*

BEWEIS. Sei M unerfüllbar, dann hat nach Bemerkung II.3.9 der Baum $\mathcal{B}(M)$ nur endlich viele Knoten. Wir machen eine Induktion nach $|\mathcal{B}(M)|$, der Anzahl an Knoten in $\mathcal{B}(M)$.

Falls $|\mathcal{B}(M)| = 1$ dann ist $\emptyset \in M$ und die Liste, die nur aus $\emptyset$ besteht ist bereits eine Resolutionswiderlegung.

Falls $|\mathcal{B}(M)| > 1$ dann existieren in $\mathcal{B}(M)$ drei Knoten von der Form



weil $\mathcal{B}(M)$ endlich ist. Denn angenommen jeder Knoten hätte mindestens einen Nachfolger, der nicht geschlossen ist; dann würde von jedem Knoten ein unendlicher Ast ausgehen was auf einen Widerspruch führt, da $\mathcal{B}(M)$ ja endlich ist.

Sei nun $C = \mathrm{res}_p(C_1, C_2)$ und $M' = M \cup \{C\}$. Dann gilt $\mathcal{B}(M') \subseteq \mathcal{B}(M)$ bereits nach Bemerkung II.3.10, tatsächlich ist sogar $\mathcal{B}(M') \subset \mathcal{B}(M)$ da der Knoten v in $\mathcal{B}(M')$ durch C geschlossen werden kann. Damit existiert nach Induktionshypothese eine Resolutionswiderlegung von M' die o.B.d.A. von der Form $C, D_1, \ldots, D_n$ ist und somit ist $C_1, C_2, C, D_1, \ldots, D_n$ eine Resolutionswiderlegung von M. □

Man beachte, dass dieser Beweis in dem Sinn konstruktiv ist, dass aus einem endlichen semantischen Baum eine Resolutionswiderlegung abgelesen wird.

Definition II.3.12 (Abschluss unter Resolution). Sei M Menge von Klauseln. Die Menge $\hat{M}$, 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 II.3.13. *Sei M eine Menge von Klauseln. Dann sind die folgenden Aussagen äquivalent:*

(1) *M ist unerfüllbar.*
(2) *Es gibt eine endliche $M_0 \subseteq M$, so dass $\emptyset \in \hat{M}_0$.*
(2') *Es gibt eine endliche $M_0 \subseteq M$, aus der man mit endlich vielen Resolutionsschritten die Leerklausel erhalten kann.*
(3) *Es gibt eine endliche $M_0 \subseteq M$, die unerfüllbar ist.*
(4) *$\hat{M}$ ist unerfüllbar.*
(5) *$\hat{M}$ enthält die Leerklausel.*

Beweis. (2) und (2') sind offensichtlich äquivalent.

(1) ⇒ (2'): Aus dem Vollständigkeitssatz folgt die Existenz einer Resolutionswiderlegung $C_1, \ldots, C_n$ von M. Diese verwendet nur endliche viele Klauseln aus M; die Menge dieser Klauseln sei M_0.

(2') ⇒ (3) ist der Korrektheitssatz für M_0.

(3) ⇒ (1) ist klar, da $M_0 \subseteq M$.

Also sind (1), (2), (2') und (3) äquivalent.

(1) $\Rightarrow$ (4) ist klar, da $M \subseteq \hat{M}$
(4) $\Rightarrow$ (5): Da $\hat{M}$ unerfüllbar ist hat $\hat{M}$ nach dem Vollständigkeitssatz eine Resolutionswiderlegung, d.h. $\emptyset \in \hat{\hat{M}}$. Nun ist aber $\hat{\hat{M}} = \hat{M}$.
(5) $\Rightarrow$ (2') folgt direkt aus Definition des Abschluss unter Resolution. $\square$

Die obige Implikation (1) $\Rightarrow$ (3) ist der Kompaktheitssatz für Klauselmengen in der Aussagenlogik. Aus diesem läßt sich wie folgt der Kompaktheitssatz für Mengen beliebiger aussagenlogischer Formeln zeigen.

KOROLLAR II.3.14. Sei Σ eine Menge von aussagenlogischen Formeln. Dann ist Σ genau dann erfüllbar, wenn jede endliche Teilmenge von Σ erfüllbar ist.

BEWEIS. $\Rightarrow$: Diese Richtung folgt unmittelbar daraus dass für eine Belegung b mit $b(\Sigma) = 1$ und eine beliebige Teilmenge $\Sigma_0 \subseteq \Sigma$ ja auch gilt dass $b(\Sigma_0) = 1$.
$\Leftarrow$: Für diese Richtung wollen wir für $\varphi \in \Sigma$ mit M_φ eine zu φ logisch äquivalente KNF bezeichnen. In Erweiterung dieser Notation sei für $\Theta \subseteq \Sigma$ die Klauselmenge $M_\Theta = \bigcup_{\varphi \in \Theta} M_\varphi$. Dann sind Θ und M_Θ logisch äquivalent.
Angenommen Σ ist unerfüllbar, dann wäre also auch M_Σ unerfüllbar und es gäbe nach Satz II.3.13 eine endliche $M_0 \subseteq M_\Sigma$ die bereits unerfüllbar ist. Damit gibt es aber auch eine endliche $\Sigma_0 \subseteq \Sigma$ so dass $M_0 \subseteq M_{\Sigma_0}$ und da M_0 unerfüllbar ist, ist das auch M_{Σ_0} und somit auch Σ_0. $\square$

Algorithmisch verwendet man die Resolution wie folgt: um 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 logischer Äquivalenztransformationen in KNF um:

$$\begin{aligned} \neg((\neg p \to \neg q) \to (q \to p)) &\Leftrightarrow \neg(\neg(\neg\neg p \vee \neg q) \vee (\neg q \vee p)) \\ &\Leftrightarrow \neg\neg(p \vee \neg q) \wedge \neg(\neg q \vee p) \\ &\Leftrightarrow (p \vee \neg q) \wedge q \wedge \neg p. \end{aligned}$$

Die so erhaltene Klauselmenge ist $M = \{\{p, \neg q\}; \{q\}; \{\neg p\}\}$. Diese hat die Resolutionswiderlegung:

$$\begin{aligned} C_1 &= \{p, \neg q\} \\ C_2 &= \{q\} \\ C_3 &= \{p\} \quad \text{aus } C_1 \text{ und } C_2 \\ C_4 &= \{\neg p\} \\ C_5 &= \emptyset \quad \text{aus } C_3 \text{ und } C_4 \end{aligned}$$

Also ist M unerfüllbar und damit φ eine Tautologie. Oft ist es angenehm, eine Resoultionsableitung in Baumform zu schreiben:

$$\dfrac{\dfrac{p, \neg q \quad q}{p} \qquad \neg p}{\emptyset}$$

Diese Vorgehensweise liefert also den folgenden Algorithmus zur Entscheidung der Allgemeingültigkeit einer aussagenlogischen Formel φ: sei M die Klauselmenge der KNF von $\neg\varphi$. Dann ist φ allgemeingültig genau dann wenn $\emptyset \in \hat{M}$. Dieser Algorithmus terminiert, da aus der Endlichkeit von M die Endlichkeit von $\hat{M}$ folgt.

KAPITEL III

Prädikatenlogik, Syntax und Semantik

III.1. Syntax

III.1.A. Terme und Formeln. Wir beginnen mit einem Beispiel für eine prädikatenlogische Formel:

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

Man könnte diese Formel auch folgendermaßen schreiben:

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

Weitere Möglichkeiten der Darstellung von Formeln sind

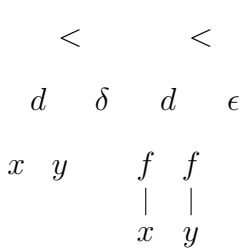
- das Baumdiagramm,
- die Präfixnotation (auch „polnische Notation“)
- und die Postfixnotation (auch UPN oder RPN wie „umgekehrte polnische Notation“, „reverse Polish notation“).

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

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

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[1] [2]
- $c, d\ldots$ Konstante
- $f(\cdot), d(\cdot,\cdot)\ldots$ Funktionssymbole (mit Stelligkeit)
- $R(\cdot,\cdot), <, =\ldots$ Relationssymbole (mit Stelligkeit)

BEMERKUNG III.1.1. Alle unsere prädikatenlogischen Sprachen werden das zweistellige Relationssymbol $=$ enthalten (ausgenommen jene Sprachen, die wir im Abschnitt 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.

Mit Hilfe dieser Bezeichnungen gelangt man zur folgenden

DEFINITION III.1.2 (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. $3+4$ ist ein Term. $(x_0 + (0 * x_1)) * x_0$ ist ein Term.

[1] Offiziell werden immer nur eine abzählbare Menge von Variablen $\{x_0, x_1, \ldots\}$ betrachten. Inoffiziell lassen wir auch Variable x, x', y etc zu.

[2] 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 III.1.3 (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 $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $(\neg\varphi)$, 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[3] 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 III.1.4. *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“

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

DEFINITION III.1.5. Zur Vereinfachung der Schreibweise vereinbaren wir weiterhin, dass $\wedge$ und $\vee$ stärker binden als $\to$ und $\leftrightarrow$; weiters[4] sollen Quantoren noch stärker binden als Junktoren. Die Formel $\forall x\, A \vee B \to C$ ist also als $((\forall x\, A) \vee B) \to C$ zu lesen, und die Formel $\exists x\, P(x) \to P(y)$ als $(\exists x\, P(x)) \to P(y)$.

III.1.B. Freie und gebundene Variable. Wir können die Begriffe „freie Variable einer Formel", „gebundene Variable einer Formel" induktiv definieren:

DEFINITION III.1.6.

- Sei φ eine Atomformel. Die freien Variablen von φ, $Fr(\varphi)$ sind alle in φ vorkommenden[5] Variablen; φ hat keine gebundenen Variablen, das heißt: $Bd(\varphi) = \emptyset$.
- Sei $\varphi = \neg\psi$. Dann gilt
$$Fr(\varphi) = Fr(\psi), \qquad Bd(\varphi) = Bd(\psi).$$
- Sei $\varphi = \psi_1 \wedge \psi_2$. Dann gilt
$$Fr(\varphi) = Fr(\psi_1) \cup Fr(\psi_2), \qquad Bd(\varphi) = Bd(\psi_1) \cup Bd(\psi_2).$$
- Analog für $\psi_1 \to \psi_2$, etc.
- Sei $\varphi = \forall x\, \psi$ oder $\varphi = \exists x\, \psi$. Dann ist
$$Fr(\varphi) = Fr(\psi) \setminus \{x\}, Bd(\varphi) = Bd(\psi) \cup \{x\}.$$
$x \notin Bd(\psi)$.

Eine Variable x kann in einer Formel sowohl frei als auch gebunden sein, wie zum Beispiel in der Formel. $x = 0 \to \exists x(x = x)$. In diesem Beispiel nennen wir das erste Vorkommen von x frei, die restlichen gebunden. Formal könnte (oder sollte) man für jeden Formel φ — etwa in Baumdarstellung — eine Funktion Frei_φ definieren, die jedem mit einer Variable x beschrifteten Knoten der Baumdarstellung von φ den Wert „hier frei" oder „hier gebunden" zuordnet. Ein Teil der induktiven Definition wären die folgenden Punkte:

- $\text{Frei}_{\psi_1 \wedge \psi_2}$ setzt die Funktionen Frei_{ψ_1} und Frei_{ψ_2} fort.
- $\text{Frei}_{\forall x\, \psi}$ weist jedem mit x beschrifteten Knoten in der Baumdarstellung von $\forall x\ \psi$ den Wert „gebunden" zu.

III.1.C. Substitution. 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 $\varphi(u)$

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

[5] Streng genommen müsste man zunächst definieren, was es heißt, dass eine Variable in einem Term vorkommt. Dies ist wieder mit einer induktiven Definition möglich; wir begnügen uns aber mit unserem intuitiven Verständnis.

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 III.1.7 (Induktive Definition der Substitution). Sei u eine Variable (oder Konstante), und sei t 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 $\varphi(u/t) := \varphi$.

(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: $\Big(\exists x\,\varphi\Big)(u/t) = \exists x\,\Big(\varphi(u/t)\Big)$ (wenn x ungleich u).

(b7) Analog für $\forall x\,\psi$.

III.2. Semantik

III.2.A. Interpretation einer Sprache $\mathscr{L}$ in einer Struktur $\mathfrak{M}$. 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 III.2.1 ($\mathscr{L}$-Struktur). Sei $\mathscr{L}$ eine prädikatenlogische Sprache. Eine $\mathscr{L}$-Struktur (auch: $\mathscr{L}$-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.
    Für das zweistellige Symbol $=$ verlangen wir immer, dass es durch die tatsächliche Gleichheit interpretiert wird,
    d.h. $I(=) = \{(m, m) : m \in M\}$.

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

Sprechweise: Die Begriffe „Modell“ und „Struktur“ werden oft synonym verwendet. Wenn man eine Struktur ein „Modell“ nennt, meint man damit aber oft, dass gewisse (vorher betrachtete) Formeln in dieser Struktur auch gelten; wenn eine Struktur $\mathfrak{M}$ eine Formel φ erfüllt, dann heißt $\mathfrak{M}$ auch „Modell für φ“; gelegentlich ergibt sich aber φ nur aus dem Kontext, und man spricht dann nur von einem Modell.

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) $I(\text{„das Symbol +“}) = \text{„die Additionsfunktion“}$
(c) $I(\text{„das Symbol 0“}) = \text{„die Zahl Null“}$

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: $\dot{+}^{\mathfrak{M}} = +$.

III.2.B. Belegungen b und Interpretation von Termen $\bar{b}$.

Definition III.2.2 (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 III.2.3. 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:

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

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.

Genauer: Zunächst zeigen wir, dass es höchstens eine Abbildung $\bar{b}$ gibt, die b fortsetzt und die angegebenen Bedingungen (a), (b), (c) erfüllt. Seien nämlich $\bar{b}$ und $\tilde{b}$ zwei solche Fortsetzungen, so kann man zeigen, dass die Eigenschaft $\bar{b}(t) = \tilde{b}(t)$

- immer dann gilt, wenn t Konstante oder Variable ist (wegen (a) bzw (b);
- sich von Termen $t_1, \ldots, t_k$ auf den Term $f(t_1, \ldots, t_k)$ vererbt, wann immer f ein k-stelliges Funktionssymbol ist.

Dann zeigen wir, dass es zu jedem Term t eine Funktion b_t gibt, die auf allen Untertermen[6] von t definiert ist, die auf ihrem Definitionsbereich die Rekursion (a),(b),(c) erfüllt; die Menge der Terme, für die es so eine Funktion gibt, enthält nämlich alle Konstanten und Variablen und ist unter den Abbildungen $(t_1, \dots, t_k) \mapsto f(t_1, \dots, f_k)$ abgeschlossen. Schließlich zeigt man, dass $\bar{b}(t) := b_t(t)$ die Anforderungen erfüllt. □

In dieser Definition haben wir eine Belegung b festgehalten und die Terme t variiert; dadurch ergibt sich eine Funktion $\bar{b}$, die auf allen Termen definiert ist. Wenn wir nun einen Term festhalten, können wir jeder Belegung b einen Wert $\bar{b}(t)$ zuordnen:

DEFINITION III.2.4. Wir halten n fest. Eine Belegung b, die nur auf den Variablen $\{x_1, \dots, x_n\}$ definiert ist, können wir mit dem n-Tupel $\vec{x}_b := (b(x_1), \dots, b(x_n)) \in M^n$ identifizieren. Umgekehrt können wir jedem n-Tupel $\vec{m} = (m_1, \dots, m_n) \in M^n$ die Belegung $b_{\vec{m}}$ zuordnen, die x_i auf m_i abbildet.

Mit dieser Bezeichnung gilt: Jeder Term t, dessen freie Variable in der Menge $\{x_1, \dots, x_n\}$ enthalten sind, induziert eine Funktion $t^{\mathfrak{M}} : M^n \to M$, nämlich

$$t^{\mathfrak{M}}(\vec{m}) = \overline{b_{\vec{m}}}(t).$$

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

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

Man beachte, dass der Definitionbereich der Funktion $t^{\mathfrak{M}}$ sich nicht aus direkt aus dem Term t ergibt, sondern nur aus dem Paar (t, n). So kann der Term x_2 sowohl die Funktion $(x, y) \mapsto y$ von M^2 nach M darstellen, als auch die Funktion $(x, y, z) \mapsto y$ von M^3 nach M.

III.2.C. Interpretation von Formeln; $\hat{b}$ und $\mathfrak{M} \vDash \varphi$.

DEFINITION III.2.5. 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. (Wir erlauben auch, dass eine der Belegungen auf u undefiniert ist, und die andere definiert. Für alle anderen Variablen x ist aber mit $b(x) = b'(x)$ gemeint, dass entweder beide Werte definiert sind, oder keiner.)

[6] dieser Begriff ist auch induktiv definiert

Die folgende algorithmische Variante ist oft praktischer:

DEFINITION III.2.6. Sei b eine Belegung, x eine Variable. (b kann auf x definiert sein, oder auch nicht.) Sei $m \in M$.

Dann ist die Belegung $b_{x/m}$ so definiert:

- $b_{x/m}(x) = m$.
- $b_{x/m}(y) = b(y)$ für alle Variablen $y \neq x$.

In dieser Schreibweise gilt natürlich $b_{x/m} =_x b$, und umgekehrt: wenn $b' =_x b$ ist, und $b'(x)$ definiert ist, dann gibt es ein $m \in M$ mit $b' = b_{x/m}$ (nämlich $m := b'(x)$).

DIE FOLGENDE DEFINITION IST ÄUSSERST WICHTIG.

DEFINITION III.2.7 (Gültigkeit unter einer Belegung). Für

- jede $\mathscr{L}$-Struktur $\mathfrak{M}$,
- jede Formel $\varphi(x_1, \ldots, x_n)$ (mit freien Variablen unter $x_1, \ldots, x_n$)
- und jede Belegung $b : \{x_1, \ldots, x_n\} \to M$

definieren wir, wann $\mathfrak{M} \vDash \varphi\ [b]$ gilt.[7] Die Definition erfolgt induktiv nach dem Aufbau der Formel φ; für Atomformeln gilt zunächst

- $\mathfrak{M} \vDash R(t_1, \ldots, t_k)\,[b] \ \Leftrightarrow\ (t_1^{\mathfrak{M}}(\vec{x}_b), \ldots, t_k^{\mathfrak{M}}(\vec{x}_b)) \in R^{\mathfrak{M}}$
  (Wir schreiben $\vec{x}_b$ wieder als Abkürzung für $(b(x_1), \ldots, b(x_n))$. Da $\doteq^{\mathfrak{M}}$ die tatsächliche Gleichheit $\{(m, m) : m \in M\}$ ist, heißt dies insbesondere:

$$\mathfrak{M} \vDash t_1 = t_2\,[b] \ \Leftrightarrow\ t_1^{\mathfrak{M}}(\vec{x}_b) = t_2^{\mathfrak{M}}(\vec{x}_b)$$

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 III.2.14.)
- $\mathfrak{M} \vDash (\varphi \to \psi)\,[b] \ \Leftrightarrow\ \mathfrak{M} \nvDash \varphi\,[b]$ 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 $\mathfrak{M} \vDash \varphi\,[b']$.
  (Die Belegung b ist möglicherweise nicht auf allen Variablen definiert; insbesondere kann es sein, dass $b(x)$ undefiniert ist. Die betrachteten Belegungen b' müssen aber alle an der Stelle x definiert sein.)
- Für jede Formel φ:
  $\mathfrak{M} \vDash \exists x\, \varphi\,[b] \ \Leftrightarrow\ \ \exists b' : b' =_x b$ und $\mathfrak{M} \vDash \varphi\,[b']$

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

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 $(\mathbb{N}, 0, <) \nvDash \varphi\ [b_3]$

SCHREIBWEISE III.2.8. 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 $\forall x\ \dot{0} \dot{\leq} x$ 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 III.2.9. Sei $\mathfrak{M} = (M, I)$ eine $\mathscr{L}$-Struktur, und sei b eine Belegung.

Dann gibt es erstens (laut III.2.3) 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) $\bar{b}(f(t_1, \ldots, t_n)) = f^{\mathfrak{M}}(\bar{b}(t_1), \ldots, \bar{b}(t_n))$, wenn $t_1, \ldots, t_n$ Terme sind, und f ein n-stelliges Funktionssymbol.
(Bis jetzt haben wir nur III.2.3 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)
(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: $\hat{b}(\varphi \to \psi) = 0$ genau dann, wenn $\hat{b}(\varphi) = 1$ und $\hat{b}(\psi) = 0$.)

(7) $\hat{b}(\forall x\, \varphi) = \bigwedge_{m \in M} \widehat{b_{x/m}}(\varphi)$. (Zur Schreibweise $\bigwedge_{\mathrm{B}}$ siehe II.1.1.)
Wenn es also ein $m \in M$ gibt mit $\widehat{b_{x/m}}(\varphi) = 0$, dann ist $\hat{b}(\forall x\, \varphi) = 0$. Wenn aber für alle $m \in M$ die Gleichung $\widehat{b_{x/m}}(\varphi) = 1$ gilt, dann ist $\hat{b}(\forall x\, \varphi) = 1$.

(8) $\hat{b}(\exists x\, \varphi) = \bigvee_{\mathrm{B}} \{\widehat{b_{x/m}}(\varphi) : m \in M\}$.
$\hat{b}(\exists x\, \varphi)$ ist also genau dann gleich 1, wenn es mindestens ein m gibt mit $\widehat{b_{x/m}}(\varphi) = 1$.

Es gilt nun:

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

Satz III.2.10. *Seien b, b' Belegungen der Variablen $x_1, \ldots, x_n$ und $b =_{x_r} b'$. Sei weiters φ eine Formel in den freien Variablen $x_{i_1}, \ldots, x_{i_k}$, wobei r in der Menge $\{i_1, \ldots, i_k\}$ nicht vorkommt. (D.h. die Variable x_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 III.2.11. *Sei σ eine geschlossene Formel (d.h. ohne freie Variable) und b, b' Belegungen von $x_1, \ldots, x_n$. Dann gilt*

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

In diesem Zusammenhang nennt man σ auch einen Satz.

Definition III.2.12 (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 III.2.13. Sei φ eine Formel (mit eventuell freien Variablen). Wir schreiben $\mathfrak{M} \models \varphi$, falls für alle Belegungen b (der freien Variablen von φ) die Beziehung

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

gilt.

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

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

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

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

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

BEMERKUNG III.2.14. Achtung! Laut Definition III.2.7 gilt zwar

$$\mathfrak{M} \not\models \varphi\ [b] \quad \Leftrightarrow \quad \mathfrak{M} \models \neg\varphi\ [b]$$

für jede Belegung b, im Allgemeinen ist die Beziehung

$$\mathfrak{M} \not\models \varphi \quad \Leftrightarrow \quad \mathfrak{M} \models \neg\varphi$$

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

- $\mathfrak{M} \models \neg\varphi$ bedeutet, dass die Beziehung $\mathfrak{M} \models (\neg\varphi)\,[b]$ für alle[8] Belegungen b gilt, d.h. dass die Beziehung $\mathfrak{M} \models \varphi\,[b]$ für *keine* Belegung b gilt.
- $\mathfrak{M} \not\models \varphi$ ist jedoch (laut Definition) die Negation der Beziehung $\mathfrak{M} \models \varphi$; das heißt, dass $\mathfrak{M} \models \varphi\ [b]$ nicht für alle b gilt, es also *zumindest eine* Belegung b gibt, sodass $\mathfrak{M} \models \varphi\ [b]$ nicht gilt.

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

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 $x \neq 0$):

$$\mathfrak{M} \not\models x = 0, \text{ denn } \mathfrak{M} \not\models \forall x(x = 0);$$
$$\mathfrak{M} \not\models x \neq 0, \text{ denn } \mathfrak{M} \not\models \forall x(x \neq 0).$$

In der folgenden Definition kann Σ endlich oder unendlich sein; auch die leere Menge ist zugelassen.

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

DEFINITION III.2.15. Sei Σ eine Menge von Formeln[9] in einer Sprache $\mathscr{L}$, und sei $\mathfrak{M}$ eine $\mathscr{L}$-Struktur.
$\mathfrak{M} \models \Sigma$ bedeutet, dass $\mathfrak{M} \models \varphi$ für alle $\varphi \in \Sigma$ gilt.

Insbesondere gilt $\mathfrak{M} \models \Sigma$ sicher dann, wenn Σ leer ist.

III.3. Allgemeingültige Formeln, Folgerung

III.3.A. Allgemeingültigkeit.

DEFINITION III.3.1 (Allgemeingültigkeit). Sei φ eine Formel. Wir sagen „φ ist *allgemeingültig*“, falls φ in allen Modellen $\mathfrak{M}$ gilt, d.h. wenn gilt

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

Wir schreiben auch kurz $\vDash \varphi$.

BEISPIEL. $\vDash \exists x \big(\, (\exists y \, P(y)) \to P(x) \, \big)$

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

III.3.B. Äquivalenz.

DEFINITION III.3.2. Seien φ, ψ Formeln mit freien Variablen unter $x_1, \ldots, x_n$. 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

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

[9] Fast immer werden wir nur Mengen von Sätzen betrachten.

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 III.3.3. *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.*

III.3.C. Tautologieaxiome.

DEFINITION III.3.4 (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 $\tilde{h}$ 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 $\tilde{h}(A) = \varphi$.

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

SATZ III.3.5. *Sei φ eine Tautologie. Dann gilt $\vDash \varphi$, d.h. Tautologien sind allgemeingültig.*

BEWEIS. (Dieser Beweis ist dem Beweis von II.1.16 sehr ähnlich.)
Sei $\varphi = \tilde{h}(A)$, wobei A aussagenlogische Tautologie ist, und $\tilde{h}$ Homomorphismus. Sei b eine (prädikatenlogische) Belegung (die zumindest auf allen in φ vorkommenden Variablen definiert ist). Daraus können wir eine aussagenlogische Belegung 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)

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

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

BEMERKUNG III.3.6. Nicht alle allgemeingültigen Formeln sind Tautologien.[10] Zum Beispiel ist $\forall x\,P(x) \to \forall y\,P(y)$ allgemeingültig, aber keine Tautologie.

[10] 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.

III.3.D. Semantische Folgerung: $\Sigma \models \varphi$.

GLOSSAR III.3.7. *Das Symbol $\models$ hat in der Prädikatenlogik verschiedene Bedeutungen:*

- $\mathfrak{M} \models \varphi[b]$*: Die Formel φ gilt in der Struktur $\mathfrak{M}$ unter der Belegung b, oder: $\hat{b}(\varphi) = 1$. (Siehe III.2.7.)*
- $\mathfrak{M} \models \varphi$*: φ gilt in $\mathfrak{M}$ unter jeder Belegung. (Siehe III.2.12.)*
- $\models \varphi$*: φ ist allgemeingültig, gilt also in allen Strukturen. (Siehe III.3.1.)*
- $\Sigma \models \varphi$*: φ folgt aus Σ, das heißt: Jede Struktur $\mathfrak{M}$, die alle Formeln in Σ erfüllt, erfüllt auch φ. (Siehe III.3.8.)*

Dies letzte Bedeutung kann man als Verallgemeinerung der vorletzten sehen:

DEFINITION III.3.8 ($\Sigma \models \varphi$, Folgerung).

(1) Seien σ_1, σ_2 Sätze. Wir schreiben $\sigma_1 \models \sigma_2$ (oder $\{\sigma_1\} \models \sigma_2$), wenn für alle $\mathfrak{M}$, die $\mathfrak{M} \models \sigma_1$ erfüllen, auch $\mathfrak{M} \models \sigma_2$ gilt (oder äquivalent dazu: wenn $\models \sigma_1 \to \sigma_2$ gilt).
(2) Allgemeiner: Sei φ eine Formel und Σ eine Menge von Sätzen. Wir schreiben $\Sigma \models \varphi$, wenn für alle $\mathfrak{M}$, die $\mathfrak{M} \models \Sigma$ erfüllen, auch $\mathfrak{M} \models \varphi$ gilt.

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

BEMERKUNG III.3.9. Wenn Σ eine endliche Menge ist, etwa $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$, dann schreiben wir statt $\Sigma \models \varphi$ bzw. $\{\sigma_1, \ldots, \sigma_n\} \models \varphi$ kürzer $\sigma_1, \ldots, \sigma_n \models \varphi$.
Wenn $\Sigma = \emptyset$ leer ist, dann gilt $\mathfrak{M} \models \Sigma$ für alle $\mathfrak{M}$. Daher gilt $\emptyset \models \varphi$ genau dann, wenn φ allgemeingültig ist, d.h. wenn $\models \varphi$ gilt.

DEFINITION III.3.10 (Erfüllbarkeit, Unerfüllbarkeit). Eine Menge Σ von geschlossenen Formeln heißt erfüllbar, wenn es ein Modell $\mathfrak{M}$ mit $\mathfrak{M} \models \Sigma$ gibt. Andernfalls heißt Σ unerfüllbar.

BEMERKUNG III.3.11. $\Sigma \models \bot$ bedeutet nach Definition, dass jedes Modell $\mathfrak{M}$, welches $\mathfrak{M} \models \Sigma$ erfüllt, auch $\mathfrak{M} \models \bot$ erfüllt. Die Beziehung $\mathfrak{M} \models \bot$ gilt aber nie. Daher:

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

SATZ III.3.12. *Sei Σ eine Menge von geschlossenen Formeln, σ und τ geschlossenen Formeln.*

(1) $\Sigma \models \sigma$ *gilt genau dann, wenn* $\Sigma \cup \{\neg\sigma\} \models \bot$.
(2) $\Sigma \models \neg\sigma$ *gilt genau dann, wenn* $\Sigma \cup \{\sigma\} \models \bot$.
(3) $\Sigma \cup \{\sigma\} \models \tau$ *gilt genau dann, wenn* $\Sigma \models \sigma \to \tau$.

BEWEIS. 1. Wir zeigen, dass die Negationen der beiden Bedingungen äquivalent sind.

$\Sigma \nvDash \sigma$ bedeutet, dass es ein Modell $\mathfrak{M}$ gibt, welches zwar Σ erfüllt, nicht aber σ. Da σ eine geschlossene Formel ist, bedeutet dies, dass $\mathfrak{M} \vDash \Sigma \cup \{\neg\sigma\}$ erfüllt, also ist $\Sigma \cup \{\neg\sigma\}$ erfüllbar.
Diese Schlüsse lassen sich auch umkehren: Jedes Modell, welches $\Sigma \cup \{\neg\sigma\} \nvDash \bot$ bezeugt, also $\Sigma \cup \{\neg\sigma\}$ erfüllt, ist ein Beleg für $\Sigma \nvDash \sigma$.

2. Ähnlich zu 1.

3. Die beiden Aussagen sind zu

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

äquivalent. Aber jedes Modell, welches σ und $\neg\tau$ erfüllt, erfüllt $\neg(\sigma \to \tau)$, und umgekehrt. □

DEFINITION III.3.13 (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 III.3.14 (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 III.3.15. *Sei $\mathscr{L}'$ eine Obersprache von $\mathscr{L}$ mit $c \in \mathscr{L}' \setminus \mathscr{L}$ und $\varphi(u)$ eine Formel in der Sprache $\mathscr{L}$. 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 III.3.16. Die Definition von $\Sigma \vDash \sigma$ hängt eigentlich von der zugrunde liegenden Sprache ab. Sei $\Sigma \cup \{\tau\}$ eine Menge von geschlossenen Formeln in der Sprache $\mathscr{L}_1 \subseteq \mathscr{L}_2$. Dann müsste man eigentlich zwei Relationen $\Sigma \models_{\mathscr{L}_1} \tau$ und $\Sigma \models_{\mathscr{L}_2} \tau$ unterscheiden:

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

III.4. Semantik der Substitution

III.4.A. Semantik der Substitution: Terme. 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 t der Term $x+1$, dann ist $s(x/t)$ der Term $((x+1)+y)*(2-(x+1))$.

Wir erinneren an Definition III.2.6: 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 III.4.1. *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 $s = f(s_1, \dots, s_k)$ für ein k-stelliges Funktionssymbol f. Dann ist

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

Auf der linken Seite der behaupteten Gleichung steht also

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

wobei die letzte Gleichung nach Induktionsvoraussetzung gilt.

Auf der rechten Seite steht dasselbe:

$$\overline{b_{x/a}}(s) = f^{\mathfrak{M}}(\overline{b_{x/a}}(s_1), \dots). \quad \square$$

III.4.B. Semantik der Substitution: 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 III.4.2. 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 $\exists y\,\psi$: 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 III.4.3. 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 (ohne Änderung der Bedeutung) 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

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

HILFSSATZ III.4.4. *Wir betrachten eine Sprache $\mathscr{L}$ und eine $\mathscr{L}$-Struktur $\mathfrak{M}$. Sei b eine Belegung, sei φ eine Formel, seien x und y verschiedene Variable, und seien c, d Elemente von M. Dann gilt*

$$(b_{x/c})_{y/d} = (b_{y/d})_{x/c} \quad \text{und } (b_{x/c})_{x/d} = b_{x/d}.$$

BEWEIS. Leicht. □

SATZ III.4.5. *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 III.4.1 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:

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

□

III.4.C. Substitutionsaxiome.

SATZ III.4.6 (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 $\hat{b}(\forall x\,\varphi) = 0$. □

III.5. Semantik von Modus Ponens

DEFINITION III.5.1 (Modus Ponens; MP). Seien φ_1, φ_2, ψ Formeln. Wir sagen, dass ψ aus φ_1 und φ_2 durch *Modus Ponens* hervorgeht, wenn φ_1 die Form $\varphi_2 \rightarrow \psi$ hat.

Anders ausgedrückt: Modus Ponens ist eine Funktion MP, die auf Paaren von Formeln definiert ist:

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

und[11] $\mathrm{MP}(A, B) = A$, wenn A nicht die Form $B \rightarrow \psi$ hat).

SATZ III.5.2 (Modus Ponens; MP).

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

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.

[11] Variante: wir betrachten MP als partielle Funktion, die nur dann einen Wert $\mathrm{MP}(A, B)$ hat, wenn A die Form $B \rightarrow \psi$ hat.

BEWEIS. Wir zeigen die erste Aussage. $\mathfrak{M} \vDash (\varphi \to \psi)\ [b]$ bedeutet $\mathfrak{M} \nvDash \varphi\ [b]$ oder $\mathfrak{M} \vDash \psi\ [b]$. Die erste Möglichkeit kommt laut Voraussetzung nicht in Frage, daher gilt $\mathfrak{M} \vDash \psi\ [b]$.

Beweisvariante: Aus $\hat{b}(\varphi \to \psi) = 1$ und $\hat{b}(\varphi) = 1$ müssen wir $\hat{b}(\psi) = 1$ folgern. Es gilt $1 = \hat{b}(\varphi \to \psi) = \hat{b}(\varphi) \to_{\mathrm{B}} \hat{b}(\psi)$, wobei $\to_{\mathrm{B}}$ die entsprechende zweistellige Operation auf $\{0, 1\}$ ist; insbesondere ist

$$(\hat{b}(\varphi) \to_{\mathrm{B}} \hat{b}(\psi)) \;=\; (1 \to_{\mathrm{B}} \hat{b}(\psi)) \;=\; \hat{b}(\psi),$$

also $\hat{b}(\psi) = 1$.

Die zweite und dritte Aussage folgen leicht aus der ersten. □

KAPITEL IV

Prädikatenlogik: Beweisbarkeit

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 61), 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.)

IV.1. Ableitungen (=Formale Beweise)

DEFINITION IV.1.1 (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 61), oder
- $\exists j_1, j_2 < i$, sodass φ_i durch MP aus $\varphi_{j_1}, \varphi_{j_2}$ hervorgeht

erfüllt ist.

Sei Φ eine Menge von Formeln (die nicht notwendigerweise geschlossen sind). Ein formaler Beweis aus Φ 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
- $\varphi_i \in \Phi$

erfüllt ist.

DEFINITION IV.1.2 (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 Φ von Formeln, wenn es einen formalen Beweis aus Φ gibt, in dem φ vorkommt. Wir schreiben

$$\Phi \vdash \varphi$$

Die Menge der beweisbaren Formeln ist unter Modus Ponens abgeschlossen.

BEMERKUNG IV.1.3. 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 IV.1.4 (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“ IV.2.1.)

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 IV.1.5. *Sei φ eine Formel, x und y Variable, und sei die Substitution $\varphi(x/y)$ sinnvoll. Dann gilt $\vdash \forall x\, \varphi \to \forall y\, \varphi(x/y)$.*

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.** $\exists x\, \varphi(x) \to \neg\forall x\, \neg\varphi(x)$ ist für jede Formel φ ein Axiom, ebenso $\neg\forall x\, \neg\varphi(x) \to \exists x\, \varphi(x)$.
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.

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

BEMERKUNG IV.1.6. 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 $\Phi \vdash \varphi$ entweder in allen Sprachen $\mathscr{L}$ gilt, die die Formeln in $\Phi \cup \{\varphi\}$ enthalten, oder in keiner. Daher schreibt man meist nur $\vdash$ statt $\vdash_{\mathscr{L}}$. (Siehe III.3.16 für den analogen Satz für die semantische Folgerung $\models$.)

IV.2. Soundness

SATZ IV.2.1 (Soundness, Korrektheit).

(1) *Aus* $\vdash \varphi$ *folgt* $\models \varphi$.
(2) *Aus* $\Phi \vdash \varphi$ *folgt* $\Phi \models \varphi$,

insbesondere gilt also:
wenn $\Phi \vdash \bot$, *dann* $\Phi \models \bot$, *bzw.:*
wenn $\Phi \not\models \bot$, *dann* $\Phi \nvdash \bot$.

(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 IV.2.2 (Vollständigkeitssatz). *Sei* Σ *eine Menge von geschlossen Formeln und* φ *eine Formel. Wenn* $\Sigma \models \varphi$ *gilt, dann auch* $\Sigma \vdash \varphi$.

IV.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 IV.3.1 (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 IV.3.2 (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 $\psi_1, \dots, \psi_n$ 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 IV.3.3. 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 IV.3.8) um weitere Formeln abzuleiten.

Die Resolutionsmethode im Abschnitt IV.5 kann ebenfalls als ein formales System gesehen werden; im Resolutionskalkül interessiert man sich zwar nicht für den Beweis von allgemeingültigen 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 Abschnitt IV.5.E) rein mechanisch in einen formalen Beweis von φ in unserem Kalkül übersetzt werden kann, und umgekehrt.

Im Satz III.3.12 haben wir gesehen, dass die Aussagen $\Sigma \vDash \varphi$ und $\Sigma \cup \{\neg\varphi\} \vDash \bot$ äquivalent sind. Parallel dazu können wir jetzt die Methode des indirekten Beweises einführen:

SATZ IV.3.4 (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 IV.3.5 (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[1] 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 $\sigma(x/c) = \sigma$.

[1]Siehe Fußnote auf Seite 23

$3 \to 1$: 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
   - $\varphi_i \to \forall y\, \varphi_i$ (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 IV.1.5 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 IV.3.6. 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 IV.3.7 (Generalisierungstheorem, Variante). *Seien Φ eine Menge von Formeln und φ eine Formel, wobei die Variable x möglicherweise frei in Φ und/oder φ vorkommt. Sei weiters c eine neue Konstante. Dann gilt:*

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

BEWEIS. Für den Beweis von 1. verwenden wir das Generalisierungstheorem in seiner ursprünglichen Variante. Da wir dieses nur für geschlossene Formeln formuliert und bewiesen haben, gehen wir folgendermaßen vor: Sei $\Phi_0 \subseteq \Phi$ endlich, sodass $\Phi_0 \vdash \varphi$, also z.B. $\Phi_0 := \{\psi_1, \ldots, \psi_n\}$. Es gilt also

$$\begin{gathered} \{\psi_1, \ldots, \psi_n\} \vdash \varphi \\ \{\psi_1, \ldots, \psi_{n-1}\} \vdash \psi_n \to \varphi \\ \vdots \\ \vdash \psi_1 \to \ldots \to \psi_n \to \varphi \end{gathered}$$

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 Φ endlich ist. Wir ersetzen alle freie Variable $y_1, \ldots, y_n$ (x kommt hier nicht vor) in Φ durch neue Konstante $c_1, \ldots, c_n$. Aus $\Phi \vdash \varphi$ schließen wir also $\Phi(\vec{y}/\vec{c}) \vdash \varphi(\vec{y}/\vec{c})$. In den Formeln der Menge $\Phi(\vec{y}/\vec{c})$ gibt es nun keine freien Variablen. Nach dem Generalisierungstheorem gilt $\Phi(\vec{y}/\vec{c}) \vdash \forall x\, \varphi(\vec{y}/\vec{c})$, und wegen Punkt 2 erhalten wir $\Phi \vdash \forall x\, \varphi$.

(Alternativer Beweis: Man wiederhole den Beweis des Generalisierungstheorems und beachte, dass die Voraussetzung „alle Formeln in Φ 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 IV.3.8 (Einführung des $\exists$-Quantors und des $\forall$-Quantors). *Sei Φ eine Menge von Formeln und seien φ, ψ Formeln, wobei die Variable x weder in Φ noch in ψ frei vorkommt. Dann gilt:*

Wenn $\Phi \vdash \psi \to \varphi$, dann $\Phi \vdash (\psi \to \forall x\, \varphi)$.

sowie

Wenn $\Phi \vdash \varphi \to \psi$, dann $\Phi \vdash (\exists x\, \varphi) \to \psi$.

EINFÜHRUNG DES ALLQUANTORS. Wir nehmen $\Phi \vdash \psi \to \varphi(u)$ an.

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

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

BEMERKUNG IV.3.9. Seien φ und ψ beliebige Formeln.

(a) Wenn $\Phi \vdash \varphi \to \psi$, dann gilt auch $\Phi \vdash \forall x\, \varphi \to \psi$.
(b) Wenn $\Phi \vdash \psi \to \varphi$, dann auch $\Phi \vdash \psi \to \exists x\, \varphi$.

Allgemeiner gilt für jeden Term t, der in φ für x substituiert werden darf:

(a') Wenn $\Phi \vdash \varphi(x/t) \to \psi$, dann gilt auch $\Phi \vdash \forall x\, \varphi \to \psi$.
(b') Wenn $\Phi \vdash \psi \to \varphi(x/t)$, dann auch $\Phi \vdash \psi \to \exists x\, \varphi$.

BEWEIS. Die Behauptung (a) (und ähnlich (a')) folgt leicht aus dem Substitionsaxiom $\forall x\,\varphi \;\to\; \varphi$. Für (b) bzw. (b') 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. □

Aus einem formalen Beweis $\varphi \to \psi$ kann man also leicht einen formalen Beweis von $\varphi \to \exists x\psi$ konstruieren, das wird auch manchmal als „einfache" oder „schwache" Einführung des Existenzquantors bezeichnet. Interessanter ist die „starke" Einführung des Existenzquantors, die wir in Satz IV.3.8 bewiesen haben:

> Aus einem Beweis von $\varphi \;\to\; \psi$ kann man einen Beweis von $\exists x\,\varphi \;\to\; \psi$ konstruieren — allerdings nur dann, wenn x in ψ nicht vorkommt.

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[2] Weise formale Beweise für die untenstehenden Formeln generieren.

Zum Beispiel bedeutet $\dfrac{\Phi \vdash \varphi_1 \quad \Phi \vdash \varphi_2}{\Phi \vdash \varphi_1 \wedge \varphi_2}$, dass man aus formalen Beweisen von φ_1 und φ_2 aus den Axiomen Φ 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

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

könnten wir auch eine Regel

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

angeben — wegen des Deduktionstheorems und der Regeln

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

könnten wir die eine aus der anderen gewinnen.

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

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

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

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

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

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

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

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

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

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

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

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

IV.4. Prädikatenlogik: Der Vollständigkeitssatz

SATZ IV.4.1 (Vollständigkeitssatz, Version 1). *Sei Σ eine Menge von geschlossen Formeln und φ eine Formel. Wenn $\Sigma \models \varphi$ gilt, dann auch $\Sigma \vdash \varphi$.*

BEMERKUNG IV.4.2. $\Sigma \models \varphi$ gilt genau dann, wenn $\Sigma \models \forall x\, \varphi$; dies folgt leicht aus der Definition von $\models$. Man kann aber auch zeigen (Generalisierungstheorem, Satz IV.3.5), 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.

IV.4.A. Umformulierungen. Wenn wir den Vollständigkeitssatz in der beschriebenen Form direkt beweisen wollten, müssten wir auf Grundlage der Tatsache $\Sigma \models \varphi$ 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 IV.4.3 (Vollständigkeitssatz, Version 2). *Sei Σ eine Menge von geschlossen Formeln. Wenn $\Sigma \models \bot$ gilt, dann auch $\Sigma \vdash \bot$.*

Wir können leicht zeigen (als Folgerung aus dem Deduktionstheorem, Satz IV.3.2 bzw. IV.3.4), dass dieser Spezialfall des Vollständigkeitssatzes ausreicht, um auch Version 1 zu beweisen:

$$\Sigma \models \varphi \overset{\text{III.3.12}}{\Rightarrow} \Sigma \cup \{\neg\varphi\} \models \bot \overset{\text{Version 2}}{\Rightarrow} \Sigma \cup \{\neg\varphi\} \vdash \bot \overset{\text{IV.3.4}}{\Rightarrow} \Sigma \vdash \varphi.$$

In III.3.10 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 IV.4.4 (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 IV.4.5. *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[3] der Inkonsistenz verwendet.)

Mit diesem neuen Vokabular besagt also die Version 2:

SATZ IV.4.6 (Vollständigkeitssatz, Version 2'). *Jede* unerfüllbare *Menge von (geschlossenen) Formeln ist* inkonsistent. *Kurz gesagt: Wenn* $\Sigma \models \bot$, *dann* $\Sigma \vdash \bot$.

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 IV.4.7 (Vollständigkeitssatz, Version 3). *Jede* konsistente *Menge von (geschlossenen) Formeln ist* erfüllbar. *Kurz gesagt: Wenn* $\Sigma \nvdash \bot$, *dann* $\Sigma \not\models \bot$.

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".

IV.4.B. Vollständige Theorien.

DEFINITION IV.4.8 (Theorie). Sei Σ eine Menge von geschlossenen Formeln. Dann heißt Σ auch Theorie.

DEFINITION IV.4.9 (vollständige Theorie). Sei Σ eine konsistente[4] 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 IV.4.10. 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 $\Sigma \nvdash \varphi$.

[3]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".

[4]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.

BEMERKUNG IV.4.11. Die 3 Äquivalenzen in IV.4.10 lassen sich in der Form von 6 Implikationen schreiben; der Leser[5] 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 IV.4.12 (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 IV.4.13 (deduktiver Abschluss). Sei Σ eine Theorie in der Sprache $\mathscr{L}$. Als deduktiven Abschluss von Σ bezeichnen wir die Menge

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

BEMERKUNG IV.4.14. Für den deduktiven Abschluss gilt $cl_{\vdash}(cl_{\vdash}(\Sigma)) = cl_{\vdash}(\Sigma)$.

SATZ IV.4.15. *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 IV.4.16. Manchmal wird eine konsistente Theorie Σ nur dann als vollständig bezeichnet, wenn für alle geschlossenen Formeln σ gilt: $\sigma \in \Sigma$ oder $\neg\sigma \in \Sigma$. 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 $\mathfrak{M} \models \Sigma$ erfüllt, auch ein Modell der Sätze in Σ'.

[5]Siehe Fußnote auf Seite 23

SATZ IV.4.17. *Sei Σ eine konsistente Theorie, die im engeren Sinne vollständig ist. Dann gilt*

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

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

HILFSSATZ IV.4.18. *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 IV.3.4:

$$\Sigma \vdash \sigma.$$

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 IV.4.19. *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 IV.4.18 auch Σ_{n+1} konsistent sein.

Nun definiert man

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

Die Theorie $\bar{\Sigma}$ ist sicher konsistent, denn angenommen es gelte $\bar{\Sigma} \vdash \bot$. Dann gibt es also eine endliche inkonsistente Teilmenge $\{\sigma_1, \ldots, \sigma_m\} \subseteq \bar{\Sigma}$ und demnach ein $k \in \mathbb{N}$ mit $\{\sigma_1, \ldots, \sigma_m\} \subseteq \Sigma_k$ — im Widerspruch zur Konsistenz von Σ_k.

Nach Konstruktion ist $\bar{\Sigma}$ vollständig, sogar im engeren Sinn. □

BEMERKUNG IV.4.20. Der Beweis ist nicht effektiv. Es gibt nämlich keinen Algorithmus, der von jeder Formel σ feststellt, ob sie (mit Σ) konsistent ist oder nicht.

BEMERKUNG IV.4.21. 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.

IV.4.C. Henkin-Theorien.

DEFINITION IV.4.22 (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.[6]

DEFINITION IV.4.23 (schwache Henkin-Theorie). Sei $\mathscr{L}$ eine prädikatenlogische Sprache, und 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; aus technischen Gründen verwenden wir die starke Henkin-Eigenschaft. In der Übung sehen wir aber, dass die beiden Eigenschaften ohnehin äquivalent sind.)

DEFINITION IV.4.24. 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 IV.4.25. *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 IV.4.26. *Sei Σ_0 eine konsistente Theorie in der Sprache $\mathscr{L}_0$. Dann gibt es*

[6] Zur Erinnerung: in III.1.5 haben wir vereinbart, dass die Formel $\exists x\, \varphi(x) \to \varphi(c)$ als $(\exists x\, \varphi(x)) \to \varphi(c)$ zu lesen ist.

(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 $\mathscr{L}_H$. □

IV.4.D. 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 IV.4.27. *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 IV.4.7) 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 IV.4.28. *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 $\mathbb{T} \neq \emptyset$. Auf der Menge $\mathbb{T}$ 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 $\exists x\, t = x \to t = c$ aus Σ ableitbar 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 61) 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, also mit anderen Worten:

Für alle geschlossenen Formeln $\sigma \in \mathscr{L}^*$ gilt

$$\sigma \in \Sigma^* \Rightarrow \mathfrak{M}^* \vDash \sigma$$

oder (scheinbar stärker, aber äquivalent):

Für alle geschlossenen Formeln $\sigma \in \mathscr{L}^*$ gilt

$$\Sigma^* \vdash \sigma \Rightarrow \mathfrak{M}^* \vDash \sigma$$

Wir werden induktiv die folgende stärkere Aussage zeigen:

Für alle geschlossenen Formeln $\sigma \in \mathscr{L}^*$ gilt

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

(Eine „Induktion über alle geschlossenen Formeln" gibt es eigentlich nicht, da sich eine geschlossene Formel im Allgemeinen nicht aus einfacheren geschlossenen Formeln aufbaut. Stattdessen können wir hier das Prinzip der Induktion nach der Anzahl der Quantoren und Junktoren verwenden.)

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 IV.4.10. 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[7], 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) $\mathfrak{M}^* \vDash \forall x\;\varphi(x) \;\Leftrightarrow\; \Sigma^* \vdash \forall x\;\varphi(x)$

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 $\mathfrak{M}^* \vDash \varphi\;[b]$. Wir schreiben m_0 für den Wert $b(x)$.

  (m_0 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 sicher $b = b_{x/m_0}$. Daher gelten die folgenden Äquivalenzen:

  $$\mathfrak{M}^* \vDash \varphi\;[b] \overset{b = b_{x/m_0}}{\Longleftrightarrow} \mathfrak{M}^* \vDash \varphi\;[b_{x/m_0}] \overset{\text{Satz III.4.5}}{\Longleftrightarrow} \mathfrak{M}^* \vDash \varphi(x/t)[b].$$

  Daher gilt $\mathfrak{M}^* \vDash \varphi(x/t)$. Nach Induktionsvoraussetzung also: $\Sigma^* \vdash \varphi(x/t)$, daher $\Sigma^* \vdash \exists x\,\varphi$.
- Nehmen wir nun an, dass $\exists x\,\varphi$ aus Σ^* beweisbar ist. Wegen der 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:

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

□

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

SATZ IV.4.29 (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 IV.4.30. Die Voraussetzung der Abzählbarkeit der Sprache $\mathscr{L}$ ist nicht notwendig, aber für unsere Beweisführung nützlich.

BEMERKUNG IV.4.31. 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 IV.4.32. *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) ⇒ (syn-e)“ ist einfach „Soundness“, genauer: die Kontraposition von Soundness.
- „(syn-e) ⇒ (syn)“ gilt, weil jeder formale Beweis von $\bot$ aus Σ nur endlich viele Formeln aus Σ verwendet.
- „(syn) ⇒ (sem)“ ist der Vollständigkeitssatz.

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

DEFINITION IV.4.33. 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 σ, die in $\mathbb{N}$ gelten.

SATZ IV.4.34. *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 $0 = \underline{0}^{\mathfrak{M}} = \underline{0}^{\mathfrak{M}'}$ abbilden muss, $1 \in \mathbb{N}$ auf $\underline{1}^{\mathfrak{M}} = \underline{1}^{\mathfrak{M}'}$, etc., und keines dieser Elemente ist gleich $c^{\mathfrak{M}'}$. Daher gibt es keinen Isomorphismus zwischen $\mathbb{N}$ und $\mathfrak{M}$. □

BEMERKUNG IV.4.35. 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 IV.4.36 (kategorische Theorie). Eine konsistente Theorie Σ heißt kategorisch, wenn alle Modelle von Σ zueinander isomorph sind.

SATZ IV.4.37. *Sei Σ eine Theorie in der prädikatenlogischen Sprache $\mathscr{L}$. Wenn Σ ein unendliches Modell hat, dann ist Σ nicht kategorisch.* [8]

IV.5. Prädikatenlogische Resolution

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

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

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 IV.5.1. Wir treffen für das gesamte Kapitel die Vereinbarung, dass die Gleichheitsrelation nicht zugelassen ist. Dies vereinfacht einige Beweisführungen.

IV.5.A. Formelersetzungssysteme. Zur algorithmischen Beschreibung von Formeltransformationen ist es oft nützlich, eine endliche Menge von Ersetzungsregeln anzugeben und die Formeltransformation durch erschöpfende Anwendung dieser Ersetzungsregeln zu definieren. Insbesondere wird es nützlich sein, solche Ersetzungsregeln zu betrachten, die logische Äquivalenz beibehalten. Deren Anwendung an einer beliebigen Stelle in einer Formel wird dann dadurch gerechtfertigt, dass die logische Äquivalenz verträglich ist mit den logischen Konnektiven, in anderen Worten: dass sie eine Kongruenzrelation bezüglich der Konnektive ist.

SATZ IV.5.2. *Die logische Äquivalenz ist eine Kongruenzrelation auf der Menge aller Formeln bezüglich der Operationen $\neg, \wedge, \vee, \to$ sowie $\forall x, \exists x$ für eine beliebige Variable x.*

BEWEIS. Klarerweise ist die logische Äquivalenz eine Äquivalenzrelation. Es bleibt, ihre Verträglichkeit mit den Operationen zu zeigen.

Sei $\models \varphi \leftrightarrow \psi$. Dann gilt auch $\models \neg\varphi \leftrightarrow \neg\psi$ sowie $\models (\varphi \wedge \chi) \leftrightarrow (\psi \wedge \chi)$, $\models (\chi \wedge \varphi) \leftrightarrow (\chi \wedge \psi)$, und die analogen Äquivalenzen für $\vee$ und $\to$ wie leicht nachzuprüfen ist.

Sei nun $\models \varphi \leftrightarrow \psi$ und x eine beliebige Variable. Dann ist $\models \forall x(\varphi \leftrightarrow \psi)$ und damit auch $\models \forall x\varphi \leftrightarrow \forall x\psi$ und $\models \exists x\varphi \leftrightarrow \exists x\psi$. □

[8] 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 IV.4.34 folgt, dass $Th(\mathbb{N})$ nicht einmal $\aleph_0$-kategorisch ist.

IV.5.B. Transformation in Konjunktive Normalform. Als ein Beispiel für ein Formelersetzungssystem wollen wir eine Menge von Regeln betrachten, welche die Transformation quantorenfreier Formeln in konjunktive Normalform erlaubt.

DEFINITION IV.5.3. Seien F, G, H quantorenfreie Formeln. Die KNF-Transformationsregeln (mit Kurzbezeichnungen in Klammern) sind:

$$\begin{array}{llll} \text{(I)} & F \to G \;\mapsto\; \neg F \vee G & \text{(DN)} & \neg\neg F \;\mapsto\; F \\ \text{(M1)} & \neg(F \wedge G) \;\mapsto\; \neg F \vee \neg G & \text{(M2)} & \neg(F \vee G) \;\mapsto\; \neg F \wedge \neg G \\ \text{(K1)} & F \vee (G \wedge H) \;\mapsto\; (F \vee G) \wedge (F \vee H) & & \\ \text{(K2)} & (G \wedge H) \vee F \;\mapsto\; (G \vee F) \wedge (H \vee F) & & \end{array}$$

Die Menge dieser Regeln wird mit (KNF) abgekürzt.

DEFINITION IV.5.4. Wir sagen dass eine Formel φ in *Normalform bezüglich (KNF)* ist falls keine der Regeln aus (KNF) mehr auf φ anwendbar ist.

SATZ IV.5.5. *Sei φ eine quantorenfreie Formel. Dann ist φ in Normalform bezüglich der Regeln (KNF) genau dann wenn φ in konjunktiver Normalform ist.*

BEWEIS. Sei φ in Normalform bezüglich (KNF). Dann hat φ die folgenden Eigenschaften:

(1) φ enthält nur $\wedge, \vee, \neg$ (wegen (I)).
(2) in φ kommt $\neg$ nur unmittelbar über Atomen vor (wegen (DN),(M1) und (M2)).
(3) in φ kommt $\vee$ nur unmittelbar über Literalen oder $\vee$ vor (wegen (K1) und (K2)).

Damit hat also φ die Gestalt $\bigwedge_{i=1}^{n} \bigvee_{j=1}^{k_i} L_{i,j}$ für Literale $L_{i,j}$ und ist damit in konjunktiver Normalform.

Für die Gegenrichtung wird über dieselben Eigenschaften (1)-(3) argumentiert.

□

IV.5.C. 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: $x = 0 \to \forall y(y = 0)$).

DEFINITION IV.5.6. 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 IV.5.7.

- 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.
- 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. (Hingegen ist es erlaubt, dass dieselbe freie Variable sowohl in ψ_1 als auch ψ_2 vorkommt.)
- 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 und $x \notin Bd(\psi)$.

SATZ IV.5.8. *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.*

SATZ IV.5.9. *Zu jeder Formel φ gibt es eine bereinigte, äquivalente Formel φ'.*

BEWEIS. φ' erhält man aus φ durch mehrfache geeignete Anwendung von Satz IV.5.8 als Formelersetzungsregel. Die logische Äquivalenz folgt dann aus Satz IV.5.2. □

BEISPIEL. Wir definieren die Formel

$$\varphi = \exists u \forall x((R(u,x) \to Q(x)) \wedge \exists v R(x,v)) \wedge \neg\exists x P(x) \wedge \forall y(Q(y) \to P(y)).$$

Diese Formel ist nicht bereinigt da die Variable x durch zwei verschiedene Quantoren gebunden wird. Durch Umbenennung der gebundenen Variable einer dieser Quantoren erhalten wir die zu φ logisch äquivalente bereinigte Formel

$$\varphi' = \exists u \forall x((R(u,x) \to Q(x)) \wedge \exists v R(x,v)) \wedge \neg\exists z P(z) \wedge \forall y(Q(y) \to P(y)).$$

IV.5.D. Pränexform.

DEFINITION IV.5.10 (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.[9]

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 IV.5.11. *Für jede Formel φ (mit den freien Variablen $x_1, \ldots, x_n$) existiert eine Formel φ^P in Pränexform sodass gilt:*

$$\vDash \varphi \leftrightarrow \varphi^P \qquad \textit{das heißt:}$$
$$\vDash \forall x_1 \ldots \forall x_n\ (\varphi(x_1, \ldots, x_n) \leftrightarrow \varphi^P(x_1, \ldots, x_n))$$

BEWEIS. Unsere Vorgehensweise besteht darin ein Formelersetzungssystem anzugeben, das eine Formel in Pränexnormalform transformiert: sei $Q \in \{\forall, \exists\}$ dann schreiben wir $\overline{Q}$ für $\forall$ falls $Q = \exists$ und umgekehrt. Sei $\circ \in \{\wedge, \vee\}$ und seien ψ, χ Formeln so dass x nicht frei in χ vorkommt. Die Quantorenverschiebungsregeln sind:

$$\begin{aligned}
Qx\,\psi \circ \chi &\mapsto Qx\,(\psi \circ \chi) \\
\chi \circ Qx\,\psi &\mapsto Qx\,(\chi \circ \psi) \\
Qx\,\psi \to \chi &\mapsto \overline{Q}x\,(\psi \to \chi) \\
\chi \to Qx\,\psi &\mapsto Qx\,(\chi \to \psi) \\
\neg Qx\,\psi &\mapsto \overline{Q}x\,\neg\psi
\end{aligned}$$

Über die Regeln lassen sich nun folgende Beobachtungen machen: Erstens gilt in bereinigten Formeln immer dass x nicht frei in χ vorkommt. Zweitens transformieren diese Regeln bereinigte Formeln in bereinigte Formeln. Und drittens sind diese Regeln logische Äquivalenztransformationen (wie sich leicht z.B. durch formale Beweise zeigen lässt). Sei nun φ' eine zu φ logisch äquivalente bereinigte Formel und sei φ^P das Ergebnis der erschöpfenden Anwendung dieser Ersetzungsregeln auf φ'. Dann folgt die logische Äquivalenz von φ und φ^P aus Satz IV.5.2. □

[9] Dies beschreibt wieder ein Induktionsprinzip.

BEISPIEL. In Fortsetzung des vorherigen Beispiels sei

$$\varphi' = \exists u \forall x((R(u,x) \to Q(x)) \wedge \exists v R(x,v)) \wedge \neg\exists z P(z) \wedge \forall y(Q(y) \to P(y)).$$

Wir erhalten durch mehrfache Anwendung der Pränexierungsregeln die folgenden Formeln

$$\begin{aligned}
\varphi'' &= \exists u \forall x\big((R(u,x) \to Q(x)) \wedge \exists v R(x,v) \wedge \neg\exists z P(z) \wedge \forall y(Q(y) \to P(y))\big)\\
\varphi^{(3)} &= \exists u \forall x \exists v\big((R(u,x) \to Q(x)) \wedge R(x,v) \wedge \neg\exists z P(z) \wedge \forall y(Q(y) \to P(y))\big)\\
\varphi^{(4)} &= \exists u \forall x \exists v \forall y\big((R(u,x) \to Q(x)) \wedge R(x,v) \wedge \neg\exists z P(z) \wedge (Q(y) \to P(y))\big)\\
\varphi^{(5)} &= \exists u \forall x \exists v \forall y\big((R(u,x) \to Q(x)) \wedge R(x,v) \wedge \forall z\neg P(z) \wedge (Q(y) \to P(y))\big)\\
\varphi^{P} &= \exists u \forall x \exists v \forall y \forall z\big((R(u,x) \to Q(x)) \wedge R(x,v) \wedge \neg P(z) \wedge (Q(y) \to P(y))\big)
\end{aligned}$$

Man beachte dass die Pränexnormalform einer Formel nicht eindeutig ist. Unterschiedliche Stragien in der Anwendung der Pränexierungsregeln erzeugen unterschiedliche Quantorenpräfixe.

IV.5.E. Skolemisierung.

DEFINITION IV.5.12. Zwei Formeln φ, ψ heissen erfüllbarkeitsäquivalent, geschrieben als $\varphi \sim_{\vDash} \psi$ falls entweder beide erfüllbar oder beide unerfüllbar sind.

Man beachte dass aus der logischen Äquivalenz die Erfüllbarkeitsäquivalenz folgt, nicht aber umgekehrt.

HILFSSATZ IV.5.13. *Sei $\forall x_1 \cdots \forall x_n \exists y\, \varphi$ eine geschlossene Formel und f ein Funktionssymbol das nicht in φ vorkommt, dann ist*

$$\forall x_1 \cdots \forall x_n \exists y\, \varphi \sim_{\vDash} \forall x_1 \cdots \forall x_n \varphi(y/f(x_1,\ldots,x_n)).$$

BEWEIS. $\forall \bar{x} \varphi(y/f(x_1,\ldots,x_n)) \to \forall \bar{x} \exists y\, \varphi$ ist sogar allgemeingültig wie sich mit einem kurzen formalen Beweis leicht nachweisen lässt.

Für die andere Richtung, sei $\forall \bar{x} \exists y\, \varphi$ erfüllbar. Dann existiert, nach dem Beweis des Vollständigkeitssatzes, ein abzählbares Modell $\mathfrak{M} \vDash \forall \bar{x} \exists y\, \varphi$ in der Sprache L von φ. Sei o.B.d.A. $M \subseteq \mathbb{N}$ und definiere ein Modell $\mathfrak{N}$ mit $\mathfrak{N}|_L = \mathfrak{M}$ und $f^{\mathfrak{N}}(a_1,\ldots,a_n) = \min\{b \in \mathbb{N} \mid \mathfrak{M} \vDash \varphi(\bar{x}/\bar{a}, y/b)\}$. Man beachte dass $f^{\mathfrak{N}}$ wohldefiniert ist, da ja $\mathfrak{M} \vDash \forall \bar{x} \exists y \varphi$. Dann gilt $\mathfrak{N} \vDash \forall \bar{x}\, \varphi(y/f(x_1,\ldots,x_n))$. □

SATZ IV.5.14. *Zu jeder Formel φ in Pränexnormalform lässt sich eine erfüllbarkeitsäquivalente und geschlossene Formel $\psi = \forall x_1 \cdots \forall x_n\, \psi'$ berechnen wobei ψ' quantorenfrei ist*[10].

[10]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.

BEWEIS. Sei φ' der universelle Abschluss von φ, d.h. $\varphi' = \forall y_1 \cdots \forall y_k \varphi$ wobei $\mathrm{Fr}(\varphi') = \{y_1, \ldots, y_k\}$. Wir erhalten ψ aus φ' durch schrittweise Skolemisierung des jeweils äußersten Existenzquantors durch Anwendung von Hilfssatz IV.5.13. □

BEISPIEL. In Fortsetzung des vorherigen Beispiels sei

$$\varphi^P = \exists u \forall x \exists v \forall y \forall z \big((R(u,x) \to Q(x)) \wedge R(x,v) \wedge \neg P(z) \wedge (Q(y) \to P(y))\big).$$

Der äußerste Existenzquator $\exists u$ kommt nicht im Bindungsbereich eines Allquantors vor, folglich wird er durch Anwendung von Hilfssatz IV.5.13 durch ein neues 0-stelliges Funktionssymbol, d.h. eine Konstante ersetzt und wir erhalten die erfüllbarkeitsäquivalent Formel

$$\varphi_0^P = \forall x \exists v \forall y \forall z \big((R(c,x) \to Q(x)) \wedge R(x,v) \wedge \neg P(z) \wedge (Q(y) \to P(y))\big).$$

Der verbleibende Existenzquantor $\exists v$ wird ersetzt durch den Skolemterm $f(x)$ und wir erhalten die erfüllbarkeitsäquivalente Formel

$$\psi = \forall x \forall y \forall z \big((R(c,x) \to Q(x)) \wedge R(x,f(x)) \wedge \neg P(z) \wedge (Q(y) \to P(y))\big).$$

IV.5.F. Klauselnormalform.

DEFINITION IV.5.15. Eine Formel ist in *Klauselnormalform* falls sie die folgende Gestalt hat:

$$\forall \bar{x} \bigwedge_{i=1}^{n} \bigvee_{j=1}^{k_i} L_{i,j}$$

wobei $L_{i,j}$ Literale sind und $\bar{x}$ alle Variablen aller $L_{i,j}$ enthält.

Zu jeder Formel lässt sich eine erfüllbarkeitsäquivalente Formel in Klauselnormalform berechnen. Diese erhalten wir durch die sogenannte *Klauselnormalformtransformation*, d.h. die Hintereinanderausführung von Bereinigung, Pränexierung, Skolemisierung und KNF-Transformation der quantorenfreien Matrix.

Ähnlich wie in der Aussagenlogik arbeiten wir auch in der Prädikatenlogik mit Klauselmengen. Die Formel

$$\forall \bar{x} \bigwedge_{i=1}^{n} \bigvee_{j=1}^{k_i} L_{i,j}$$

wird identifiziert mit der Klauselmenge

$$\{\{L_{i,j} \mid 1 \le j \le k_i\} \mid 1 \le i \le n\}.$$

BEISPIEL. In Fortsetzung des vorherigen Beispiels erhalten wir durch die KNF-Transformation die zu ψ korrespondierende Klauselmenge

$$M_\psi = \{\{\neg R(c,x), Q(x)\}; \{R(x,f(x))\}; \{\neg P(z)\}; \{\neg Q(y), P(y)\}\}.$$

IV.5.G. Unifikation. Die Resolution in der Prädikatenlogik unterscheidet sich wesentlich von der Resolution in der Aussagenlogik dadurch, dass die Klauseln freie Variablen enthalten und eine geeignete Instanziierung dieser Variablen notwendig ist. Gelegentlich ist offensichtlich welche Instanziierung zu wählen ist; sollen zum Beispiel die Klauseln $\{P(x)\}$ und $\{\neg P(c)\}$ resolviert werden, ist klar dass (x/c) auf $P(x)$ angewandt werden muss bevor resolviert wird. Im allgemeinen ist es aber nicht so offensichtlich wie in diesem Beispiel. Die Technik die für den allgemeinen Fall verwendet wird heißt Unifikation und wird nun genauer beschrieben.

DEFINITION IV.5.16. Eine Substitution ist eine Abbildung $\sigma : V \to \mathcal{T}(\Sigma)$ so dass $\sigma(x) \neq x$ für endlich viele x.

Wir schreiben eine Substitution oft auch als $\sigma = (x_1/t_1, \ldots, x_n/t_n)$. Die Domäne einer Substitution ist $\mathrm{dom}(\sigma) = \{x \in V \mid x\sigma \neq x\}$. Falls zwei Substitutionen $\sigma_1 = (x_1/t_1, \ldots, x_n/t_n)$ und $\sigma_2 = (y_1/s_1, \ldots, y_k/s_k)$ disjunkte Domänen haben, dann definieren wir die Substitution $\sigma_1 \cup \sigma_2 = (x_1/t_1, \ldots, x_n/t_n, y_1/s_1, \ldots, y_k/s_k)$. Seien nun $\sigma = (x_1/t_1, \ldots, x_n/t_n)$ und θ zwei beliebige Substitutionen und sei $\theta = \theta_1 \cup \theta_2$ wobei $\mathrm{dom}(\theta_1) \subseteq \mathrm{dom}(\sigma)$ und $\mathrm{dom}(\theta_2) \cap \mathrm{dom}(\sigma) = \emptyset$. Dann ist die Hintereinanderausführung von σ und θ definiert als $\sigma \circ \theta = (x_1/t_1\theta, \ldots, x_n/t_n\theta) \cup \theta_2$. Man beachte, dass für alle Terme t und alle Substitutionen σ, θ gilt: $t(\sigma \circ \theta) = (t\sigma)\theta$.

BEISPIEL. $(x/f(y)) \cup (y/c) = (y/c) \cup (x/f(y)) = (x/f(y), y/c)$,
$(x/f(y)) \circ (y/c) = (x/f(c), y/c)$,
und $(y/c) \circ (x/f(y)) = (x/f(y), y/c)$.

DEFINITION IV.5.17. Sei E eine Menge von Literalen, eine Substitution σ heißt *Unifikator* von E falls $|E\sigma| = 1$.

Analog dazu sagen wir, dass eine Substitution σ ein Unifikator einer Menge T von Termen ist, falls $|T\sigma| = 1$. Von besonderem Interesse werden Mengen von Termen der Größe 2 sein. Dann ist σ Unifikator von $\{t_1, t_2\}$ genau dann wenn $t_1\sigma = t_2\sigma$.

BEISPIEL. Ein Unifikator von $\{P(x, g(x)), P(f(y), z)\}$ ist $(x/f(y), z/g(f(y)))$, ein anderer Unifikator ist $(x/f(f(y)), y/f(y), z/g(f(f(y))))$.

DEFINITION IV.5.18. Für Substitutionen σ und τ sagen wir dass σ *allgemeiner* ist als τ, in Zeichen $\sigma \leq \tau$, falls es eine Substitution θ gibt mit $\sigma\theta = \tau$.

DEFINITION IV.5.19. Sei E eine Menge von Literalen. Dann heißt σ *allgemeinster Unifikator* von E falls $\sigma \leq \tau$ für jeden Unifikator τ von E.

Es wird sich herausstellen, dass jede Menge von Literalen, sofern sie überhaupt einen Unifikator besitzt, auch einen allgemeinsten Unifikator besitzt. Um das zu zeigen benötigen wir allerdings noch einige zusätzliche Begriffe und Resultate.

DEFINITION IV.5.20. Seien s, t Terme. Die Differenzenmenge $\mathrm{Diff}(s,t)$ ist eine endliche Menge von Paaren von Termen die rekursiv wie folgt definiert wird:

(1) Falls $s = t$ dann $\mathrm{Diff}(s,t) = \emptyset$.
(2) Falls $s \neq t$ aber $s = f(s_1, \ldots, s_n)$ und $t = f(t_1, \ldots, t_n)$ für ein Funktionssymbol f dann
$$\mathrm{Diff}(s,t) = \bigcup_{i=1}^{n} \mathrm{Diff}(s_i, t_i).$$
(3) Sonst ist $\mathrm{Diff}(s,t) = \{(s,t)\}$.

BEISPIEL. $\mathrm{Diff}(h(x, g(x)), h(f(y), z)) = \{(x, f(y)), (g(x), z)\}$

HILFSSATZ IV.5.21. *Eine Substitution σ ist Unifikator von $\{t_1, t_2\}$ genau dann wenn σ Unifikator von allen Paaren in* $\mathrm{Diff}(t_1, t_2)$ *ist.*

BEWEIS. Sei $t_1\sigma = t_2\sigma$ und $(s_1, s_2) \in \mathrm{Diff}(t_1, t_2)$. Dann ist s_1 Teilterm von t_1 an einer bestimmten Position p und s_2 ist Teilterm von t_2 an derselben Position p. Damit folgt aus $t_1\sigma = t_2\sigma$ dass $s_1\sigma = s_2\sigma$.
Umgekehrt, falls $s_1\sigma = s_2\sigma$ für alle $(s_1, s_2) \in \mathrm{Diff}(t_1, t_2)$, dann folgt aus der Definition von Diff mit Induktion dass $t_1\sigma = t_2\sigma$. □

HILFSSATZ IV.5.22. *Seien t_1, t_2 Terme, τ ein Unifikator von $\{t_1, t_2\}$ und $(x, s) \in \mathrm{Diff}(t_1, t_2)$. Dann ist $\tau = (x/s)\tau'$ wobei $\tau' = \tau|_{\mathrm{dom}(\tau)\setminus\{x\}}$ und τ' ist Unifikator von $\{t_1(x/s), t_2(x/s)\}$.*

BEWEIS. Da $(x, s) \in \mathrm{Diff}(t_1, t_2)$ und τ Unifikator von $\{t_1, t_2\}$ ist gilt
$$x\tau = s\tau. \tag{1}$$
Außerdem ist $x \notin \mathrm{Var}(s)$. Da nämlich (x, s) ein Differenzenpaar ist gilt $s \neq x$. Wäre nun $x \in \mathrm{Var}(s)$ dann wäre $x\tau$ echter Teilterm von $s\tau$ was (1) widerspräche. Damit ist
$$s\tau = s\tau'. \tag{2}$$
Wir erhalten somit:
$$\tau = (x/x\tau) \cup \tau' =^{(1)} (x/s\tau) \cup \tau' =^{(2)} (x/s\tau') \cup \tau' = (x/s)\tau'.$$
Weiters gilt
$$t_1(x/s)\tau' = t_1\tau = t_2\tau = t_2(x/s)\tau'$$
und damit ist τ' Unifikator von $\{t_1(x/s), t_2(x/s)\}$. □

Der obige Hilfssatz zeigt wie ein beliebiger Unifikator τ "faktorisiert" werden kann in ein Paar (x, s) und den übrigen Unifikator τ'. Er bildet den Schlüssel zum folgenden zentralen Resultat:

SATZ IV.5.23. *Sei $\{t_1, t_2\}$ unifizierbar. Dann hat $\{t_1, t_2\}$ einen allgemeinsten Unifikator.*

BEWEIS. Wir machen eine Induktion über die Anzahl der in $\{t_1, t_2\}$ vorkommenden Variablen, notiert als $|\mathrm{Var}(\{t_1, t_2\})|$. Wenn $|\mathrm{Var}(\{t_1, t_2\})| = 0$ dann folgt aus der Unifizierbarkeit dass $t_1 = t_2$. Falls $t_1 = t_2$ (unabhängig davon ob der Term Variablen enthält) dann ist jede Substitution Unifikator und id ist allgemeinster Unifikator.

Sei nun also $t_1 \neq t_2$. Dann ist $\mathrm{Diff}(t_1, t_2) \neq \emptyset$. Sei $(s_1, s_2) \in \mathrm{Diff}(t_1, t_2)$. Da $\{t_1, t_2\}$ unifizierbar ist, sind auch $\{s_1, s_2\}$ unifizierbar. Außerdem beginnen s_1, s_2 mit unterschiedlichen Symbolen da es sich um ein Differenzenpaar handelt. Eines dieser Symbole muss eine Variable sein (wären nämlich beide Konstanten- oder Funktionssymbole wäre $\{s_1, s_2\}$ nicht unifizierbar). Sei nun o.B.d.A. $s_1 = x$. Dann gilt außerdem dass $x \notin \mathrm{Var}(s_2)$ sonst wäre nämlich für jede Substitution σ der Term $x\sigma$ echter Teilterm von $s_2\sigma$ was der Unfizierbarkeit von $\{s_1, s_2\}$ widersprechen würde.

Wir definieren $t_i' = t_i(x/s_2)$ für $i = 1, 2$. Sei nun τ Unifikator von $\{t_1, t_2\}$, dann folgt aus Hilfssatz IV.5.22, dass $\tau = (x/s_2)\tau'$ und dass τ' Unifikator von $\{t_1', t_2'\}$ ist. Da die Variable x in $\{t_1', t_2'\}$ nicht mehr vorkommt, enthält $\{t_1', t_2'\}$ strikt weniger Variablen als $\{t_1, t_2\}$. Nach Induktionshypothese existiert also ein allgemeinster Unifikator σ' von $\{t_1', t_2'\}$. Wir definieren $\sigma = (x/s_2)\sigma'$ und behaupten dass σ allgemeinster Unifikator von $\{t_1, t_2\}$ ist. Erstens ist σ Unifikator da

$$t_1\sigma = t_1(x/s_2)\sigma' = t_1'\sigma', \text{ und}$$
$$t_2\sigma = t_2(x/s_2)\sigma' = t_2'\sigma'.$$

Sei nun τ ein beliebiger Unifikator von $\{t_1, t_2\}$, dann kann τ wie oben mit Hilfssatz IV.5.22 geschrieben werden als $\tau = (x/s_2)\tau'$ wobei τ' Unifikator von $\{t_1', t_2'\}$ ist. Damit existiert θ mit $\sigma'\theta = \tau'$. Nun gilt aber

$$\sigma\theta = (x/s_2)\sigma'\theta = (x/s_2)\tau' = \tau,$$

also ist σ allgemeinster Unifikator. □

Der obige Beweis induziert auf recht klar nachvollziehbare Art und Weise den folgenden Algorithmus zur Berechnung des allgemeinsten Unifikators zweier gegebener Terme t_1, t_2.

- Falls $\mathrm{Diff}(t_1, t_2) = \emptyset$ dann $\mathrm{allgU}(t_1, t_2) = \mathrm{id}$.
- Falls $(s_1, s_2) \in \mathrm{Diff}(t_1, t_2)$ wobei sowohl s_1 als auch s_2 ein konstantes Startsymbol hat, dann sind t_1, t_2 nicht unifizierbar.
- Sei $(x, s) \in \mathrm{Diff}(t_1, t_2)$, dann:
  - Falls $x \in \mathrm{Var}(s)$ dann sind t_1, t_2 nicht unifizierbar.
  - Falls $x \notin \mathrm{Var}(s)$ sei $t_1' = t_1(x/s)$ und $t_2' = t_2(x/s)$ dann $\mathrm{allgU}(t_1, t_2) = (x/s)\mathrm{allgU}(t_1', t_2')$.

BEISPIEL. Sei $t_1 = g(x, c)$ und $t_2 = g(f(y), y)$. Dann liefert die Anwendung des obigen Algorithmus die folgende Tabelle

$g(x,c), g(f(y),y)$	$(x/f(y))$
$g(f(y),c), g(f(y),y)$	(y/c)
$g(f(c),c), g(f(c),c)$	id

und damit $\mathrm{allgU}(t_1, t_2) = (x/f(y))(y/c)\mathrm{id} = (x/f(c), y/c)$.

KOROLLAR IV.5.24. Falls eine endliche Menge von Literalen unifizierbar ist, dann besitzt sie einen allgemeinsten Unifikator.

BEWEIS. Wir zeigen dass es zu jeder endlichen Menge C von Literalen Terme s_1, s_2 gibt, so dass die Unifikatoren von C genau die Unifikatoren von $\{s_1, s_2\}$ sind.

Mittels Ersetzung eines r-stelligen Prädikatensymbols P durch ein neues r-stelliges Funktionssymbol f_P sowie Ersetzung der Negation durch ein neues unäres Funktionssymbol n erhalten wir zu $C = \{L_1, \ldots, L_m\}$ eine Menge von Termen $T_C = \{t_1, \ldots, t_m\}$. Wir führen dann ein neues m-stelliges Funktionssymbol f ein und definieren $s_1 = f(t_1, \ldots, t_m)$ und $s_2 = f(t_1, \ldots, t_1)$. Dann ist eine Substitution σ Unifikator von C genau dann wenn σ Unifikator von $\{s_1, s_2\}$ ist. □

IV.5.H. Resolution. Für ein Literal L vereinbaren wir die Notation $\bar{L} = \neg A$ falls $L = A$ und $\bar{L} = A$ falls $L = \neg A$. Eine *Variablenumbenennung* ist eine Substitution $\sigma : V \to V$ die eine Permutation ist. Für zwei Klauseln C und C' sagen wir dass C' eine *Variante* von C ist falls es eine Variablenumbenennung ρ gibt mit $C\rho = C'$.

DEFINITION IV.5.25. Seien C, D Klauseln und C', D' Varianten von C und D so dass C' und D' variablendisjunkt sind. Seien $K \in C'$ und $L \in D'$ Literale so dass $\{\bar{K}, L\}$ unifizierbar ist und sei σ ein allgemeinster Unifikator von $\{\bar{K}, L\}$. Dann heißt $\mathrm{Res}_{K,L}(C', D') = ((C' \setminus \{K\}) \cup (D' \setminus \{L\}))\sigma$ Resolvent von C und D.

BEISPIEL. Seien $C = \{x \leq x \cdot x\}$ und $D = \{\neg x \leq y, x < s(y)\}$. Wir benennen x in C in x' um und erhalten damit $C' = \{x' \leq x' \cdot x'\}$. Dann sind C' und D variablendisjunkt. Die Atome $x' \leq x' \cdot x'$ und $x \leq y$ haben einen allgemeinsten Unifikator $\sigma = (x/x', y/x' \cdot x')$ und damit bilden C und D den Resolventen $\{x' < s(x' \cdot x')\}$.

DEFINITION IV.5.26. Sei C eine Klausel und $D \subseteq C$ unifizierbar mit allgemeinstem Unifikator σ. Dann heißt $C\sigma$ *Faktor* von C

BEISPIEL. Die Klauselmenge $M = \{\{P(x), P(y)\}; \{\neg P(u), \neg P(v)\}\}$ ist unerfüllbar und bildet (bis auf Variablenumbenennung) ausschließlich den Resolventen $\{P(x), \neg P(v)\}$, insbesondere ist die Leerklausel nicht mittels Resolution alleine aus M ableitbar. Allerdings hat $\{P(x), P(y)\}$ den Faktor $\{P(x)\}$ und $\{\neg P(u), \neg P(v)\}$

hat den Faktor $\{\neg P(u)\}$ woraus die Leerklausel mit einem einzigen Resolutionsschritt ableitbar ist.

DEFINITION IV.5.27. Sei M eine Klauselmenge. Eine endliche Liste $C_1, \ldots, C_n$ von Klauseln heißt Resolutionsableitung aus M falls für alle $i \in \{1, \ldots, n\}$ gilt:

(1) $C_i \in M$, oder
(2) es gibt $j < i$ so dass C_i Faktor von C_j ist, oder
(3) es gibt $j, k < i$ so dass C_i Resolvent von C_j und C_k ist.

SATZ IV.5.28 (Korrektheit). *Falls M eine Resolutionswiderlegung besitzt, dann ist M unerfüllbar.*

BEWEIS. Sei $C_1, \ldots, C_n$ eine Resolutionsableitung aus M. Sei φ_M die zu M korrespondierende Formel und sei $\mathfrak{M} \vDash \varphi_M$. Wir zeigen mit Induktion nach n dass $\mathfrak{M} \vDash C_n$ (man beachte dass C_n freie Variablen enthält).

Falls $C_n \in M$, dann ist C_n logische Konsequenz aus φ_M und damit $\mathfrak{M} \vDash C_n$. Falls C_n Faktor von C_i ist für ein $i < n$, dann $C_n = C_i\sigma$ für eine Substitution σ. Dann gilt nach Induktionshypothese $\mathfrak{M} \vDash C_i$ und damit gilt auch $\mathfrak{M} \vDash C_i\sigma$.

Falls C_n Resolvente von C_i und C_j ist für $i, j < n$, dann gibt es Literale $L \in C_i$ und $K \in C_j$ so dass $\overline{L}, K$ unifizierbar sind. Sei μ allgemeinster Unifikator von $\overline{L}, K$ und sei $C_i' = C_i \setminus \{L\}$ und $C_j' = C_j \setminus \{K\}$. Dann gilt nach Induktionshypothese $\mathfrak{M} \vDash C_i' \vee L$ und $\mathfrak{M} \vDash C_j' \vee K$. Damit gilt auch $\mathfrak{M} \vDash C_i'\mu \vee L\mu$ und $\mathfrak{M} \vDash C_j'\mu \vee K\mu$. Nun ist aber $\overline{L}\mu = K\mu$ und damit $\mathfrak{M} \vDash (C_i'\mu \vee L\mu) \wedge (C_j'\mu \vee \neg L\mu)$ woraus man wie im aussagenlogischen Fall zeigt dass $\mathfrak{M} \vDash C_i'\mu \vee C_j'\mu$.

Falls also $C_1, \ldots, C_n$ eine Resolutionswiderlegung von M ist, dann ist jedes Modell von M auch Modell von $C_n = \emptyset$. Die Leerklausel ist aber unerfüllbar und damit ist das auch M. □

IV.5.I. Vollständigkeit.

DEFINITION IV.5.29. Eine Klausel D heißt *Grundinstanz* einer Klausel C falls D keine Variablen enthält und es eine Substitution σ gibt mit $C\sigma = D$. Für eine Klauselmenge M definieren wir $\mathrm{G}(M) = \{D \mid D \text{ ist Grundinstanz eines } C \in M\}$

$\mathrm{G}(M)$ ist eine aussagenlogische Klauselmenge. Wir können also AL-Resolution darauf anwenden. Resolutionsableitungen aus $\mathrm{G}(M)$ werden oft auch als Grundresolutionsableitungen aus M bezeichnet. Der entscheidenen Zusammenhang zwischen M und $\mathrm{G}(M)$ ist der folgende

SATZ IV.5.30. *Sei M eine Klauselmenge. Dann ist M erfüllbar genau dann wenn $\mathrm{G}(M)$ erfüllbar ist.*

BEWEIS. Die Implikation von links nach rechts ist trivial.

Für die Gegenrichtung, sei b eine AL-Interpretation aller Atome in $\mathrm{G}(M)$ mit $\hat{b}(\mathrm{G}(M)) = 1$. Wir definieren eine PL-Struktur $\mathfrak{M}_b$ wie folgt: die Domäne von

$\mathfrak{M}_b$ sind alle Grundterme der Sprache von M, die Interpretation eines Terms t wird als $t^{\mathfrak{M}_b} = t$ festgelegt und die Interpretation der Prädikatensymbole als $P^{\mathfrak{M}_b}(t_1, \ldots, t_n) = b(P(t_1, \ldots, t_n))$.
Sei nun $C \in M$, dann gilt $\mathfrak{M}_b \vDash D$ für jede Grundinstanz D von C. Nachdem aber die Domäne von $\mathfrak{M}_b$ ausschließlich aus Grundtermen besteht, folgt daraus dass auch $\mathfrak{M}_b \vDash C$ und damit $\mathfrak{M}_b \vDash M$. □

Ein aus diesem Satz gemeinsam mit dem Kompaktheitssatz gewinnbares Korollar ist der folgende

SATZ IV.5.31 (Satz von Herbrand). *M ist unerfüllbar genau dann wenn es eine endliche Klauselmenge $M_0 \subseteq \mathrm{G}(M)$ gibt die unerfüllbar ist.*

BEWEIS. M ist unerfüllbar genau dann wenn $\mathrm{G}(M)$ unerfüllbar ist nach Satz IV.5.30. Aus der Unerfüllbarkeit von $\mathrm{G}(M)$ folgt nach dem Kompaktheitssatz für die Aussagenlogik die Existenz eines endlichen, unerfüllbaren $M_0 \subseteq \mathrm{G}(M)$, die Gegenrichtung ist trivial. □

HILFSSATZ IV.5.32 (Hebelemma[11]). *Sei M eine Klauselmenge. Falls eine AL-Resoultionsableitung einer Klausel D aus $\mathrm{G}(M)$ existiert, dann existiert auch eine Resolutionsableitung einer Klausel C aus M und eine Substitution σ so dass $C\sigma = D$.*

BEWEIS. Wir zeigen das Lemma mit Induktion über die Länge der gegebenen Grundresolutionswiderlegung.

(1) Falls $D \in \mathrm{G}(M)$ dann ist $D = C\sigma$ für ein $C \in M$ und wir erhalten eine Resolutionsableitung von C
(2) Falls D durch aussagenlogische Resolution aus Klauseln D_1 und D_2 erhalten wurde, dann existieren nach Induktionshypothese Resolutionsableitungen von Klauseln C_1 und C_2 aus M sowie Substitutionen σ_1, σ_2 mit $C_1\sigma_1 = D_1$ und $C_2\sigma_2 = D_2$. O.B.d.A. nehmen wir an dass C_1 und C_2 variablendisjunkt sind. Damit ist auch $\mathrm{dom}(\sigma_1) \cap \mathrm{dom}(\sigma_2) = \emptyset$ und somit die Substitution $\sigma_1 \cup \sigma_2$ wohldefiniert. Seien $L_1 \in D_1, L_2 \in D_2$ die resolvierten Literale und $\mathcal{L}_1 = \{L \in C_1 \mid L\sigma_1 = L_1\}$ sowie $\mathcal{L}_2 = \{L \in C_2 \mid L\sigma_2 = L_2\}$. Dann gilt:

$$\begin{aligned} D &= (C_1\sigma_1 \setminus \{L_1\}) \cup (C_2\sigma_2 \setminus \{L_2\}) \\ &= ((C_1 \setminus \mathcal{L}_1) \cup (C_2 \setminus \mathcal{L}_2))(\sigma_1 \cup \sigma_2). \end{aligned}$$

Da $|\mathcal{L}_1\sigma_1| = 1$, ist $\mathcal{L}_1$ unifizierbar; sei τ_1 der allgemeinste Unifikator von $\mathcal{L}_1$ und analog τ_2 jener von $\mathcal{L}_2$. Dann können die Klauseln $C_1' = C_1\tau_1$ und $C_2' = C_2\tau_2$ mittels Faktorbildung aus C_1, C_2 und damit aus M abgeleitet werden.

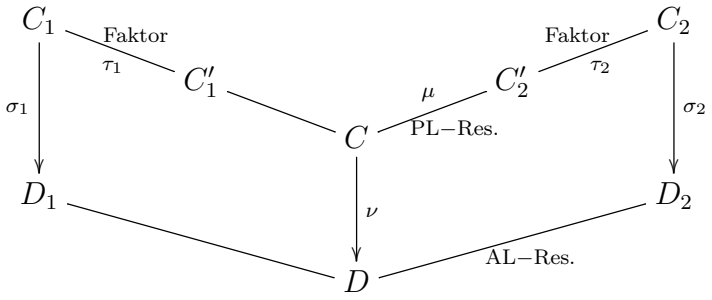
[11] engl. "lifting lemma"

Sei nun $L_1' \in C_1'$ definiert durch $\mathcal{L}_1\tau_1 = \{L_1'\}$ sowie $L_2' \in C_2'$ durch $\mathcal{L}_2\tau_2 = \{L_2'\}$. Dann wollen wir zunächst zeigen dass $\overline{L_1'}, L_2'$ unifizierbar sind: Es gilt ja $\overline{L_1} = L_2$, $\mathcal{L}_1\sigma_1 = \{L_1\}$ und $\mathcal{L}_2\sigma_2 = \{L_2\}$ und da C_1 und C_2 variablendisjunkt sind, ist $\overline{\mathcal{L}_1}(\sigma_1 \cup \sigma_2) = \mathcal{L}_2(\sigma_1 \cup \sigma_2)$. Also ist $\overline{\mathcal{L}_1} \cup \mathcal{L}_2$ unifizierbar. Nun ist aber τ_1 allgemeinster Unifikator von $\mathcal{L}_1$ und τ_2 allgemeinster Unifikator von $\mathcal{L}_2$ und damit ist auch noch $\overline{\mathcal{L}_1}\tau_1 \cup \mathcal{L}_2\tau_2$ unifizierbar, d.h. also $\overline{L_1'}, L_2'$.

Sei μ allgemeinster Unifikator von $\overline{L_1'}, L_2'$. Dann gilt

$$\begin{aligned} C &= ((C_1\tau_1 \setminus \{L_1'\}) \cup (C_2\tau_2 \setminus \{L_2'\}))\mu \\ &= ((C_1 \setminus \mathcal{L}_1) \cup (C_2 \setminus \mathcal{L}_2))(\tau_1 \cup \tau_2)\mu. \end{aligned}$$

Zusammenfassend gilt also: $\sigma_1 \cup \sigma_2$ ist Unifikator von $\overline{\mathcal{L}_1} \cup \mathcal{L}_2$ und $(\tau_1 \cup \tau_2)\mu$ ist allgemeinster Unifikator von $\overline{\mathcal{L}_1} \cup \mathcal{L}_2$. D.h. es existiert eine Substitution ν mit $(\tau_1 \cup \tau_2)\mu\nu = \sigma_1 \cup \sigma_2$ und damit $C\nu = D$.



□

SATZ IV.5.33 (Vollständigkeit). *Falls M unerfüllbar ist, dann existiert eine Resolutionswiderlegung von M.*

BEWEIS. Sei M unerfüllbar. Dann ist nach Satz IV.5.30 auch $\mathrm{G}(M)$ unerfüllbar. Wegen der Vollständigkeit der AL-Resolution existiert also eine AL-Resolutionswiderlegung von $\mathrm{G}(M)$. Durch Anwendung des Hebelemmas erhalten wir aus dieser eine Resolutionswiderlegung von M. □

Zusammenfassend bietet die Resolution also die folgende Methode zur Bestimmung der Allgemeingültigkeit einer prädikatenlogischen Formel φ:

(1) Sei φ_1 eine Bereinigung von $\neg\varphi$.
(2) Sei φ_2 eine Pränexform von φ_1
(3) Sei φ_3 eine Skolemisierung von φ_2
(4) Sei M die aus KNF-Transformation von φ_3 gewonnene Klauselmenge.

Dann ist φ gültig genau dann wenn M eine Resolutionswiderlegung besitzt.

KAPITEL V

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.)

V.1. Informeller Überblick

DEFINITION V.1.1 (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.[1]

(Dies ist eine informelle Definition, die wir im Folgenden präzisieren wollen.)

DEFINITION V.1.2 (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 V.1.3 (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[2], 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, dann liefert der Algorithmus diesen Wert

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

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

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 V.1.4 (Semi-Entscheidbarkeit). Eine Menge $A \subseteq \mathbb{N}$ (oder alternativ: $A \subseteq \text{STRING}$) heißt *semi-entscheidbar* (oder auch „rekursiv aufzählbar“[3]), 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).

In den folgenden Abschnitten werden wir zwei formale (äquivalente) Varianten dieser Begriffe vorstellen, und (auszugsweise) die folgenden Sätze beweisen, die die Beziehung zwischen den Begriffen „berechenbar“, „entscheidbar“ und „semi-entscheidbar“ beleuchten. Der Einfachkeit halber konzentrieren wir uns aber nur auf Funktionen auf $\mathbb{N}$.

SATZ V.1.5. *$A \subseteq \mathbb{N}$ ist genau dann entscheidbar, wenn sowohl A als auch $\mathbb{N} \setminus A$ semi-entscheidbar sind.*

(Analoges gilt für $A \subseteq$ STRING.)

SATZ V.1.6. *Für eine Menge $A \subseteq \mathbb{N}$ sind die folgenden Aussagen äquivalent:*

(1) *A ist semi-entscheidbar.*
(2) *Es gibt eine berechenbare partielle 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.)*

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

V.2. Primitiv rekursive Funktionen

DEFINITION V.2.1. Wir definieren eine Menge $\mathscr{P}$ von Operationen (=endlichstelligen Funktionen) auf $\mathbb{N}$, die so genannten primitiv rekursiven Funktionen.

- Für jedes $k \geq 0$ ist die konstante Funktion von $\mathbb{N}^k$ nach $\mathbb{N}$ mit Wert 0 primitiv rekursiv.
- Die Nachfolgerfunktion $n \mapsto n+1$ ist primitiv rekursiv.
- Für jedes $n \geq 1$ und jedes k mit $1 \leq k \leq n$ ist die durch
$$\pi_k^n(x_1, \ldots, x_n) = x_k$$
definierte Projektionsfunktion $\Pi_k^n : \mathbb{N}^n \to \mathbb{N}$ primitiv rekursiv.
- (Abschluss unter Verknüpfung) Wenn $h : \mathbb{N}^k \to \mathbb{N}$ und $f_1, \ldots, f_k : \mathbb{N}^n \to \mathbb{N}$ alle primitiv rekursiv sind, dann auch die Funktion $g(f_1, \ldots, f_k) : \mathbb{N}^n \to \mathbb{N}$, die so definiert ist:
$$\forall \vec{x} = (x_1, \ldots, x_n) : \; g(f_1, \ldots, f_k)(\vec{x})) := g(\, f_1(\vec{x}), \ldots, f_k(\vec{x})\,).$$
- (Abschluss unter primitiver Rekursion) Für alle $k \geq 0$, alle k-stelligen primitiv rekursiven Funktionen $h : \mathbb{N}^k \to \mathbb{N}$ und alle $k+2$-stelligen primitiv rekursiven g ist auch die durch
$$\begin{aligned} \forall \vec{x} \in \mathbb{N}^k : \quad f(\vec{x}, 0) &= h(\vec{x}) \\ \forall y \in \mathbb{N}\ \forall \vec{x} \in \mathbb{N}^k : \quad f(\vec{x}, y+1) &= g(f(\vec{x}, y), \vec{x}, y) \end{aligned}$$
primitiv rekursiv.

  Da die Funktion f durch die Funktionen h und g eindeutig bestimmt ist, ist ein Name für diese Funktion gelegentlich praktisch, der diese Abhängigkeit andeutet. Man könnte f etwa $PR(g,h)$ nennen.
- Das sind alle. (Das heißt, die Klasse $\mathscr{P}$ ist die kleinste Menge von Funktionen, die die obigen Abschlusseigenschaften hat.)

DEFINITION V.2.2. Eine Funktion $f : \mathbb{N}^k \to \mathbb{N}^m$ ist genau dann primitiv rekursiv, wenn ihre „Komponenten“ $\pi_k^m \circ f : \mathbb{N}^k \to \mathbb{N}$ alle primitiv rekursiv sind.

Mit dieser Notation lässt sich die Abschlusseigenschaft so schreiben: Wenn $\vec{f} : \mathbb{N}^k \to \mathbb{N}^m$ und $g : \mathbb{N}^m \to \mathbb{N}^n$ primitiv rekursiv sind, dann auch $g \circ \vec{f}$.

BEISPIEL. Die folgenden Funktionen bzw Folgen (betrachtet als Funktion von $\mathbb{N}$ bzw $\mathbb{N} \times \mathbb{N}$ nach $\mathbb{N}$) sind primitiv rekursiv: Addition, Multiplikation, Exponentiation; die Funktionen max und min (beliebiger Stelligkeit); abgeschnittene Subtraktion $x \dot{-} y := \max(x - y, 0)$ und abgerundete Division; die modulo-Funktion; die Funktion $n \mapsto n!$; die Doppelfolge der Binomialkoeffizienten; die Folge der Primzahlen; die Fibonacci-Folge; die Folge $(n,k) \mapsto \lfloor \alpha^n \beta^k \rfloor$ für alle algebraische Zahl $\alpha, \beta \in \mathbb{R}$; daher auch die Folge $k \mapsto \lfloor \alpha 10^k \rfloor \bmod 10$ für alle algebraischen Zahlen $\alpha \in \mathbb{R}$.

Wenn f primitiv rekursiv ist, dann ist auch ihr „diskretes Integral“ Σf (definiert durch $\Sigma f(n) = \sum_{i=1}^{n-1} f(i)$) primitiv rekursiv, ebenso wie ihre „diskrete Ableitung Δf, die durch $\Delta f(n) := f(n+1) \dot{-} f(n)$ definiert ist.

Die folgenden Mengen sind primitiv rekursive Relationen (d.h., haben primitiv rekursive charakteristische Funktion): Die der Primzahlen, die Menge der Fakultäten, die Menge aller Fibonacci-Zahlen.

Allgemeiner ist der Wertebereich jeder monoton wachsenden primitiv rekursiven Funktion selbst primitiv rekursiv.

BEWEIS. Übungsaufgabe. □

DEFINITION V.2.3. Sei $f : \mathbb{N}^k \times \mathbb{N} \to \mathbb{N}$ eine totale Funktion. Dann bezeichnen wir mit μf die folgende partielle Funktion von $\mathbb{N}^k$ nach $\mathbb{N}$:

$$\mu f(\vec{n}) = \begin{cases} \min\{k : f(\vec{n}, k) = 0\} & \text{wenn es so ein } k \text{ gibt} \\ \text{undefiniert} & \text{sonst} \end{cases}$$

Wir sagen, dass μf durch „μ-Rekursion“ aus f entsteht.

(Achtung: μf ist nur für totale Funktionen f definiert! Wenn wir die obige Definition auch für partielle Funktionen f verwenden, kann es vorkommen, dass μf nicht berechenbar ist.)

BEMERKUNG V.2.4. Wenn f eine im informellen Sinn berechenbare totale Funktion ist, dann ist auch μf berechenbar; aus einem Algorithmus, der f berechnet, kann man leicht einen Algorithmus konstruieren, der μf berechnet.

DEFINITION V.2.5. Die Menge der *rekursiven* Funktionen ist die kleinste Klasse von Funktionen, die alle Projektionen und die Nachfolgerfunktion enthält und unter

- Verknüpfung
- rimitiver Rekusion
- μ-Rekursion

abgeschlossen ist.

V.3. Σ_0 und Σ_1

Wir betrachten die Sprache der Peano-Arithmetik mit diesen nichtlogischen Symbolen: $+$, $\cdot$, $\uparrow$, 0, 1, $\leq$. Die Formel $s < t$ können wir entweder als Abkürzung für $s \leq t \wedge s \neq t$ betrachten, oder wir betrachten $<$ als eigenes Symbol und fügen die Äquivalenz $x < y \leftrightarrow x \leq y \wedge x \neq y$ zu den Axiomen von PA hinzu.

Wir werden in diesem Kapitel verschiedene Begriffe von Äquivalenz betrachten:

- Logische Äquivalenz: $\varphi \Leftrightarrow \psi$ bedeutet, dass die Äquivalenz $\varphi \leftrightarrow \psi$ allgemeingültig (bzw aus den logischen Axiomen) beweisbar ist.

- PA-Äquivalenz: $\varphi \Leftrightarrow_{PA} \psi$ bedeutet, dass die Äquivalenz $\varphi \leftrightarrow \psi$ aus den Axiomen PA beweisbar ist (bzw in allen Modellen von PA gilt).
- $\mathbb{N}$-Äquivalenz: $\varphi \Leftrightarrow_{\mathbb{N}} \psi$ bedeutet, dass die Äquivalenz $\varphi \leftrightarrow \psi$ in $\mathbb{N}$ (mit der üblichen Interpretation von $+$, $\cdot$ etc) gilt.

(In den meisten Fällen genügt uns $\mathbb{N}$-Äquivalenz, obwohl tatsächlich PA-Äquivalenz gilt.)

DEFINITION V.3.1. Sei x eine Variable, und sei t ein Term, der x nicht enthält. Für jede Formel ψ sind die Formeln $\exists x \leq t\ \psi$ und $\forall x \leq t\ \psi$ in natürlicher Weise definiert:

$$\exists x \leq t\ \psi\ :=\ (\exists x)(x \leq t \wedge \psi), \quad \forall x \leq t\ \psi\ :=\ (\forall x)(x \leq t \to \psi)$$

Analog definieren wir $\exists x < t\ \psi$ und $\forall x < t\ \psi$.

DEFINITION V.3.2. Die beschränkten Formeln sind induktiv definiert

- Alle Atomformeln sind beschränkt.
- Die beschränkten Formeln sind unter Konjunktion, Disjunktion, Negation, Implikation, Äquivalenz abgeschlossen. (D.h., wenn ψ_1, ψ_2 beschränkte Formeln sind, dann auch $\psi_1 \wedge \psi_2$, $\psi_1 \leftrightarrow \psi_2$, etc.)
- Die beschränkten Formeln sind unter beschränkter Quantifizierung abgeschlossen, d.h.: Wenn ψ beschränkt ist, dann sind auch $\forall x < t\, \psi$ udn $\exists x < t\, \varphi$ beschränkt.
- Das sind alle.

(Statt „beschränkte Formel“ sagt man auch Σ_0-Formeln.)

Man kann leicht zeigen, dass jede beschränkte Formel zu einer Formel in beschränkter Pränexform (das heißt $\forall x < t \cdots \exists y < s\ (\psi)$ mit quantorenfreiem ψ) logisch äquivalent ist.

DEFINITION V.3.3. Sei $k \geq 0$.

- Eine Teilmenge $A \subseteq \mathbb{N}^k$ heißt (k-stellige) Σ_0-Relation, wenn es eine beschränkte Formel $\varphi(x_1, \ldots, x_k)$ mit den freien Variablen $x_1, \ldots, x_k$ gibt, sodass $A = \{(n_1, \ldots, n_k) : \mathbb{N} \models \varphi(n_1, \ldots, n_k)\}$ gilt.
- Eine Funktion $f : \mathbb{N}^k \to \mathbb{N}^n$ heißt Σ_0-Funktion, wenn ihr Graph[4] $\{(\vec{x}, \vec{y}) : \vec{x} \in \mathbb{N}^k, \vec{y} = f(\vec{x})\}$ eine Σ_0-Relation ist.

BEISPIEL. Die folgenden Mengen sind Σ_0-Relationen:

- Jede endliche Teilmenge von $\mathbb{N}^k$.
- $\{(a, b, c) : a + b = c\}$
- $\{(a, b) : a \cdot b = c\}$
- $\{(a, b) : a | b\}$

[4]Funktionen werden oft mit ihrem Graphen identifiziert, man könnte also auch sagen: f ist Σ_0-Funktion, wenn f eine Σ_0-Relation ist.

- Die Menge der Quadratzahlen.
- Die Menge $\mathbb{P}$ der Primzahlen.

BEWEIS. Die Relation „|“ wird durch die Formel $\exists z < x_2\ (x_1 \cdot z = x_2) \vee x_2 = 0$ beschrieben.

Die Menge $\mathbb{P}$ wird durch die Formel $1 < x_1 \wedge \forall y < x_1 : (y|x_1 \to y = 1)$ beschrieben, wobei $y|x_1$ eine Abkürzung für die gerade definierte Formel ist. □

HILFSSATZ V.3.4. *Die Menge*

$$PP := \{2,\ 2 \cdot 3^2,\ 2 \cdot 3^2 \cdot 5^3,\ 2 \cdot 3^2 \cdot 5^3 \cdot 7^4,\ \ldots,\ p_1 \cdot p_2^2 \cdot \cdots p_n^n,\ \ldots\},$$

wobei p_n die n-te Primzahl ist, wird durch eine beschränkte Formel beschrieben.

BEWEIS. Eine Zahl $z > 1$ ist in PP, wenn

- erstens für alle Primzahlen $p < q$ gilt: Wenn $q|z$, dann $p|z$,
- und zweitens für benachbarte Primzahlen $p < q$ gilt: Wenn $k \geq 1$, $q^k|z$ aber nicht $q^{k+1}|z$, dann gilt $p^{k-1}|z$ aber nicht $p^k|z$.

Es genügt aber, sich hier nur auf alle $p, q \leq z$ zu beschränken, ebenso nur auf alle $k \leq z$. So erhält man leicht eine beschränkte Formel. □

Wir wollen k-Tupel $(n_1, \ldots, n_k)$ natürlicher Zahlen durch eine Zahl kodieren (wobei k beliebig sein kann). Eine Möglichkeit dazu bietet diese Funktion:

DEFINITION V.3.5. Sei $p_1 = 2$, $p_2 = 3$, $\ldots$, $p_k =$ die k-te Primzahl. Die Funktion $\langle\ \rangle : \bigcup_{k=0}^{\infty} \mathbb{N}^k \to \mathbb{N}$ ist so definiert:[5]

$$\langle n_1, \ldots, n_k \rangle := 2^{n_1+1} \cdot \ldots \cdot p_k^{n_k+1}$$

Insbesondere wird das leere Tupel () auf $\langle\rangle := 1$ abgebildet, jedes 1-Tupel (n) auf 2^{n+1}, und jedes 2-Tupel (n, k) auf $\langle n, k \rangle := 2^{n+1}3^{k+1}$.

DEFINITION V.3.6. Die Funktion ℓ ist so definiert:

- Für jede Zahl $s \in \mathbb{N}$ mit $s \geq 2$ sei $\ell(s) := \max\{k : p_k|s\}$.
- wir setzen $\ell(0) = \ell(1) := 0$.

Weiters definieren wir eine zweistellige Funktion $(x, y) \mapsto (x)_y$ so:

- Für $x = 0$ oder $y = 0$ sei $(x)_y := 0$.
- Wenn $x > 0$ und $y > 0$ ist, dann ist $(x)_y := \max\{k : p_y^k|x\}$.
  $(x)_y$ ist also der Exponent der y-ten Primzahl in der Primfaktorzerlegung von x.

Zum Beispiel ist $(1)_y = 0$ für alle y, und $(200)_1 = (2^3 \cdot 3^0 \cdot 5^2)_1 = 3$, $(200)_2 = 0$, $(200)_3 = 2$, $(200)_4 = 0$. Allgemein gilt $(n)_k = 0$, wenn $k > \ell(n)$.

[5]Man beachte die Schreibweise: Wir verwenden $(\cdots)$ für Tupel, $\langle\cdots\rangle$ für die einem Tupel zugeordnete Zahl. Diese Schreibweise ist nicht kanonisch. Man könnte statt $\langle n_1, \ldots, \rangle$ auch $\#(n_1, \ldots, n_k)$ oder $\mathrm{code}(n_1, \ldots, n_k)$ schreiben.

BEMERKUNG V.3.7. Die Abbildung $\langle\cdot\rangle$ ist injektiv. Wenn $a = \langle n_1, \ldots, n_k\rangle$, dann ist $\ell(a) = k$, und $n_i = (a)_i - 1$ für alle $i \leq k$.

HILFSSATZ V.3.8. *Die folgenden Funktionen sind Σ_0-Funktionen:*

(1) *Die Funktion $(r, s) \mapsto \langle r, s\rangle = 2^{r+1}3^{s+1}$.*
(2) *Allgemeiner: Für jedes k die durch $(n_1, \ldots, n_k) \mapsto \langle n_1, \ldots, n_k\rangle$ definierte k-stellige Funktion.*
(3) *Die Funktion $k \mapsto p_k$. (Wobei wir p_0 auf einen beliebigen Wert setzen, sagen wir 1.)*
(4) *Die Funktion ℓ.*
(5) *Die Funktion $(n, k) \mapsto (n)_k$.*

BEWEIS. Für $k > 0$ gilt $p_k = n$ genau dann, wenn erstens n Primzahl ist, und es zweitens ein $s \in PP$ mit folgenden Eigenschaften gibt: $p^k | s$, aber p^{k+1} teilt s nicht.

Überdies kann man die Größe von s abschätzen; wenn es so ein s gibt, dann gibt es auch ein s mit $s \leq p_1^1 \cdots p_k^k \leq p_k^{k^2} \leq n^{k^2}$. Daher gilt $p_k = n$ genau dann, wenn $\mathbb{N} \models \psi(k, n)$ mit

$$\psi(x, y) := (x = 0 \wedge y = 1) \vee (x > 0 \wedge y > 1 \wedge \psi'(x, y))$$
$$\text{wobei } \psi'(x, y) := \exists z \leq y^{x^2}(z \in PP \wedge x^y | z \wedge \neg(x^{y+1} | z)).$$

Die vorkommenden Unterformeln $z \in PP$ und $x^y | z$ verstehen wir hier als Abkürzungen für geeignete (bereits definierte) beschränkte Formeln.

Damit ist die Funktion $k \mapsto p_k$ eine Σ_0-Funktion.

Die anderen Formeln erhält man ähnlich. (Übungsaufgabe.) □

DEFINITION V.3.9. Eine Σ_1-Formel ist eine Formel der Form $\exists x\, \psi$, wobei ψ eine beschränkte Formel ist.

HILFSSATZ V.3.10. *Wenn φ, ψ Σ_1-Formeln sind, dann sind die folgenden Formeln zu Σ_1-Formeln äquivalent (im Sinne von $\Leftrightarrow_{PA}$):*

(1) *$\varphi(x/t)$ für beliebige sinnvolle Substitutionen x/t*
(2) *$\exists y\, \varphi$*
(3) *$\varphi \wedge \psi$, $\varphi \vee \psi$*
(4) *$(\forall y < z)\psi$*
(5) *$(\forall y < t)\psi$ (t kann hier ein beliebiger Term sein, der y nicht enthält.)*

BEWEIS. (1) ist klar.

(2) Wenn $\varphi = \exists x\, \varphi_0$ (mit φ_0 beschränkt) ist, und z eine neue Variable ist, dann gilt

$$PA \vdash \exists y\, \exists x\, \varphi_0 \;\leftrightarrow\; \exists z\, \exists y < z\, \exists x < z\, \varphi_0,$$

wobei die Formel $\exists y < z\, \exists x < z\, \varphi_0$ beschränkt ist.

(3) Die Formeln $\varphi \vee \psi$ und $\varphi \wedge \psi$ kann man leicht in Pränexform (mit zwei führenden $\exists$-Quantoren) umformen, und dann die Transformation aus (2) anwenden.

(4) Hier genügt es, die Formel

$$\forall y < z \, \exists x \, \varphi_0 \leftrightarrow \exists u (\forall y < z \, \exists x < u \, \varphi_0)$$

in PA zu beweisen. Dies gelingt mit Induktion über z.

(5) Kombination aus (1) und (4). □

Die folgende Definition ist ganz analog zu Definition V.3.3.

DEFINITION V.3.11. Sei $k \geq 0$.

- Eine Teilmenge $A \subseteq \mathbb{N}^k$ heißt (k-stellige) Σ_1-Relation, wenn es eine Σ_1-Formel $\exists y \, \varphi(x_1, \ldots, x_k, y)$ mit den freien Variablen $x_1, \ldots, x_k$ gibt, sodass $A = \{(n_1, \ldots, n_k) : \mathbb{N} \models \exists y \, \varphi(n_1, \ldots, n_k, y)\}$ gilt.
- Analog heißt eine partielle (oder totale) Funktion $f : \mathbb{N}^k \to \mathbb{N}^n$ Σ_1-Funktion, wenn ihr Graph eine Σ_1-Relation ist.

BEMERKUNG V.3.12. Eine Funktion $f : \mathbb{N}^k \to \mathbb{N}^n$ ist genau dann Σ_1, wenn ihre Komponenten $\pi_1^n \circ f, \ldots, \pi_n^n \circ f$ alle Σ_1 sind.

HILFSSATZ V.3.13. *Die Menge der Σ_1-Funktionen hat folgende Abschlusseigenschaften:*

- *Die Verknüpfung von Σ_1-Funktionen ist Σ_1-Funktion.*
- *Wenn g, h Σ_1-Funktionen sind, und f die Rekursion*

$$f(\vec{x}, 0) = h(\vec{x})$$
$$f(\vec{x}, k+1) = g(f(\vec{x}, k), \vec{x}, k)$$

erfüllt, dann ist auch f eine Σ_1-Funktion.

BEWEIS. Seien $g : \mathbb{N}^a \to \mathbb{N}^b$ und $h : \mathbb{N}^b \to \mathbb{N}^c$ partielle Σ_1-Funktionen, die $g(\vec{x}) = \vec{y} \Leftrightarrow \exists u \, (\psi_1(\vec{x}, \vec{y}, u)$ und $h(\vec{y}) = \vec{z} \Leftrightarrow \exists v \, (\psi_2(\vec{y}, \vec{z}, v)$ erfüllen. Sei $f := h \circ g$. Dann gilt $f(\vec{x}) = \vec{z}$ genau dann, wenn

$$\exists u \; \exists v \; \exists \vec{y} \; (\psi_1(\vec{x}, \vec{y}, u) \wedge \psi_2(\vec{y}, \vec{z}, v)$$

erfüllt ist, wobei $\exists \vec{y}$ eine Abkürzung für $\exists y_1 \cdots \exists y_b$ ist. Wie wir in Lemma V.3.10 schon gesehen haben, können wir die $b + 2$ Existenzquantoren am Beginn der Formel durch einen einzigen unbeschränkten Existenzquantor, gefolgt von $b + 2$ beschränkten Quantoren übersetzen:

$$\exists u \; \exists v \; \exists \vec{y} \; (\cdots) \Leftrightarrow_{PA} \exists w \, \exists u < w \; \exists v < w \; \exists \vec{y} < w \; (\cdots)$$

Um den Abschluss unter primitiver Induktion zu beweisen, verwenden wir unsere Codierung. Die Beziehung $f(\vec{n}, k) = \ell$ gilt nämlich genau dann, wenn es eine Folge $(m_0, \ldots, m_k)$ von Werten gibt, die die folgenden Bedingung erfüllen:

- $m_0 = h(\vec{n})$

- $m_k = \ell$.
- Für alle i zwischen 0 und k: $m_{i+1} = g(m_i, \vec{x}, i)$.

Dabei sind alle Werte m_i durch $\langle m_0, \ldots, m_k \rangle$ beschränkt. Also ist $f(\vec{n}, k) = \ell$ genau dann, wenn

$$\exists s\, (s)_0 = h(\vec{n}) \wedge (s)_k = \ell \wedge \forall i < k : \exists p, q < s \left((s)_i = p \wedge (s)_{i+1} = q \wedge q = g(p, \vec{n}, i) \right).$$

Diese Formel ist äquivalent zu einer Σ_1-Formel. □

HILFSSATZ V.3.14. *Sei $f : \mathbb{N}^{k+1} \to \mathbb{N}$ eine totale Σ_1-Funktion. Dann ist die durch*

$$g(\vec{n}) = \begin{cases} \min\{k : f(\vec{n}, k) = 0\} & \text{wenn es so ein } k \text{ gibt} \\ \text{undefiniert} & \text{sonst} \end{cases}$$

definierte partielle Funktion eine Σ_1-Funktion.

KOROLLAR V.3.15. Jede rekursive Funktion (und insbesondere jede primitiv rekursive Funktion) ist eine Σ_1-Funktion.

Es gilt auch die Umkehrung: die rekursiven Funktionen sind genau die Σ_1-Funktionen.

Je nach Geschmack definiert man nun die berechenbaren Funktionen als die rekursiven Funktionen oder als die Σ_1-Funktionen. Es gibt auch noch andere äquivalente Definitionen, die häufig verwendet werden (und den Term „berechenbar“ möglicherweise besser motivieren), mit Hilfe von Turingmaschinen oder Registermaschinen. Andere Definitionen verwenden Grammatiken oder den λ-Kalkül.

V.4. Axiomensysteme

Axiome und Theorien.

DEFINITION V.4.1 (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.[6]

Klassische und moderne Axiomensysteme. 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. „Moderne" Axiomensysteme sind so angelegt, dass sie eine ganze Klasse von Strukturen (Gruppen, Körper, etc.) beschreiben.

BEISPIELE.

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

Moderne Axiomensysteme sind im Allgemeinen auf offensichtliche Weise unvollständig.

Klassische Axiomensysteme sind oft unvollständig (auf Grund des Gödelschen Unvollständigkeitssatzes), die Unvollständigkeit ist aber im Allgemeinen nicht offensichtlich.

Wegen Satz IV.4.37 reicht aber ein Axiomensystem in der erststufigen Logik nie aus, um eine einzige (unendliche) Struktur bis auf Isomorphie zu charakterisieren. Insofern gibt es keine klassischen Axiomensysteme, die die ihnen zugedachte Aufgabe auch erfüllen. Formal sind sie daher von modernen Axiomensystemen nicht zu unterscheiden.

Semantik ohne Vollständigkeitssatz. 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 V.4.2 (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 $\vDash_e \varphi$.

SATZ V.4.3 (Satz von Trakhtenbrot). *Die Menge* $E^- := \{\varphi : \nvDash_e \varphi\}$ *ist semientscheidbar, die Menge* $E^+ := \{\varphi : \vDash_e \varphi\}$ *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

[6] 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.

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 V.4.4 (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 V.4.5. 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[7] 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 V.4.6. *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.

DEFINITION V.4.7 (unendliche Gültigkeit). Eine Formel φ heißt unendlich gültig, wenn für alle unendlichen Modelle $\mathfrak{M}$ gilt: $\mathfrak{M} \models \varphi$. Wir schreiben in diesem Fall auch $\models_u \varphi$.

DEFINITION V.4.8 (Axiomatisierbarkeit). Eine Theorie Σ heißt axiomatisierbar, wenn es ein Axiomensystem Σ_0 gibt, sodass gilt

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

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

BEISPIELE. Die Menge $\{\varphi : \models_e \varphi\}$ ist nicht axiomatisierbar. Die Menge $\{\varphi : \models_u \varphi\}$ ist jedoch axiomatisierbar.

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

KAPITEL VI

Mengenlehre

VI.1. Bemerkungen zur Prädikatenlogik 1. 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 „Kommutatorgruppe“ $G' \subseteq G$, die von der Menge $\{x \cdot y \cdot x^{-1} \cdot y^{-1} : x, y \in G\}$ erzeugt wird. (In den Übungen werden wir sehen, dass es keine Formel φ gibt, die aus jeder Gruppe G ihre Kommutatorgruppe aussondert.)

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 (oder sogar: der endlichen Gruppen) bietet sich aber keine Formel in der Prädikatenlogik erster Stufe an, die diese Klasse beschreibt (und tatsächlich gibt es auch keine, siehe Übungen).

Um auch solche Mengen formalisieren zu können, benötigt man also „mächtigere“ Sprachen.

VI.2. Logik 2.Stufe

Eine prädikatenlogische Sprache 2. Stufe enthält neben den bereits bekannten Objektvariablen, Funktions- und Relationssymbolen auch sogenannte Relationsvariable 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). (Der besseren Lesbarkeit halber lassen wir den Index 1 in Zukunft weg.)

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.)

Hier ein weiteres Beispiel: Wir kürzen die Formel

$$\forall_1 x \forall_1 y \forall_1 z \; X(x,y) \wedge X(y,z) \to X(x,z)$$

mit „X ist transitiv“ ab, und schreiben „X is reflexiv"bzw. „X ist symmetrisch“ für $\forall x \; X(x,x)$ bzw. für $\forall x \forall y \; X(x,y) \to X(y,x)$. Sei $\varphi(X)$ nun die folgende Fomel:

$$\begin{aligned} X\text{reflexiv} \wedge X\text{symmetrisch} \; \wedge \; & X\text{transitiv} \\ & \wedge \forall x \; \exists y \; (x \neq y \wedge X(x,y)) \\ & \wedge \forall x \; \forall y \; \forall z \; (x \neq y \; \wedge \; x \neq z \; \wedge X(x,y) \; \wedge \; X(x,z) \; \to \; y = z) \end{aligned}$$

Dann besagt $\varphi(X)$, dass X Äquivalenzrelation ist, deren Klassen alle zweielementig sind; die Formel $\exists_2 X \; \varphi(X)$ ist also nicht allgemeingültig, gilt aber in aber zum Beispiel in allen Strukturen, der Grundmenge die Form $A \times \{0,1\}$ hat.

Man kann nun zeigen, dass sich für eine Sprache 2. Stufe kein sinnvoller Beweisbegriff definieren, d.h. es gilt der folgende

Satz VI.2.1. *Die Menge* $\{\varphi : \models_2 \varphi\}$ *ist nicht semi-entscheidbar.*
Daher gibt es keinen berechenbaren Ableitungsbegriff $\mathrel{|\!\sim}$*, sodass*

$$\mathrel{|\!\sim} \varphi \quad \Leftrightarrow \quad \models_2 \varphi$$

für alle φ *gilt.*

Die ZFC-Axiome sind eine Theorie 1. Stufe. Rückblickend[1] 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.

VI.3. Sprache der Mengenlehre; ZFC-Axiome

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 zunächst 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 eine ϵ-Struktur. 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, die wir informell schon im ersten Kapitel besprochen haben. Eine vollständige Liste finden Sie im Anhang. 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.

$\mathrm{PMA} \vdash \forall \mathtt{y}\ \exists \mathtt{p} \forall \mathtt{z}\ (\mathtt{z}\ \epsilon\ \mathtt{p} \leftrightarrow \mathtt{z} = \mathtt{u} \vee \mathtt{z} = \mathtt{y})$ (Subst.Ax. + MP)
$\mathrm{PMA} \vdash \exists \mathtt{p} \forall \mathtt{z}\ (\mathtt{z}\ \epsilon\ \mathtt{p} \leftrightarrow \mathtt{z} = \mathtt{u} \vee \mathtt{z} = \mathtt{u})$ (Subst.Ax. + MP)

[1] 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.

$\mathrm{PMA} \vdash \exists \mathtt{p}\, \forall \mathtt{z}\ (\mathtt{z} \in \mathtt{p} \leftrightarrow \mathtt{z} = \mathtt{u})$ (allgemeingültige Äquivalenz)
$\mathrm{PMA} \vdash \forall \mathtt{x}\, \exists \mathtt{p}\, \forall \mathtt{z}\ (\mathtt{z} \in \mathtt{p} \leftrightarrow \mathtt{z} = \mathtt{x})$ (Gen.Th.) □

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 VI.3.1 (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:

$$ZF \cup \{\mathtt{x}_0 \text{ induktiv}\} \vdash \exists \mathtt{M} \forall \mathtt{z}\, [\mathtt{z} \in \mathtt{M} \ \leftrightarrow\ \mathtt{z} \in \mathtt{x}_0 \wedge \forall i\, (i \text{ induktiv } \rightarrow \mathtt{z} \in i)]$$

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:

$$ZF \cup \{\mathtt{x}_0 \text{ induktiv}\} \vdash \exists \mathtt{M} \forall \mathtt{z}\, (\mathtt{z} \in \mathtt{M} \ \leftrightarrow\ \forall \mathtt{i}\, (\mathtt{i} \text{ induktiv } \rightarrow \mathtt{z} \in \mathtt{i})$$

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.

Im ersten Kapitel haben wir auch den Begriff der Relation und der Funktion definiert; diese Definitionen können wir nun in der Sprache der Mengenlehre formalisieren (UE).

Bildmenge. Sei $f : A \to B$ eine Funktion. Für $x \in A$ wird das Bild unter f (also das eindeutig bestimmte $y \in B$ mit $(x,y) \in f$) mit $f(x)$ bezeichnet; ähnlich bezeichnet man für jede Teilmenge $X \subseteq A$ ihre Bildmenge $\{f(x) : x \in A\}$ mit $f(A)$.

Diese Konvention erweist sich in der Mengenlehre als unpraktisch, weil wir oft über Objekte z quantifizieren wollen, die sowohl Elemente als auch Teilmengen von A sein können. Wenn z.B. $f = \{(0,7),(1,8),(2,10)\}$ ist, könnte mit $f(2)$ entweder 7 oder $f(\{0,1\}) = \{f(0),f(1)\} = \{7,8\}$ gemeint sein.

Daher verwenden wir in diesem Kapitel die Notation $f(x)$ **nur für das eindeutig bestimmte** y **mit** $(x,y) \in f$; die Bildmenge einer Untermenge $X \subseteq A$ bezeichnen wir[2] immer mit $f[X]$.

VI.4. Endliche und unendliche Mengen

Es gibt verschiedene Möglichkeiten, den Begriff „endlich“ zu definieren. In der modernen Mengenlehre verwendet man üblicherweise die folgende Definition:

DEFINITION VI.4.1. 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:

[2]Eine andere Notation findet man oft in älteren Büchern: Statt $f(x)$ schreibt man manchmal $f`x$, und statt $f[X]$ schreibt man $f``X$. Diese Notation erspart erstens Klammern, und lässt sich auch leicht verallgemeinern: wenn $\mathscr{A}$ eine Familie von Mengen B ist, auf deren Vereinigung $U := \bigcup \mathscr{A} = \bigcup_{B\in\mathscr{A}} B$ eine Funktion f definiert ist, dann ist

- $f`x = f(x)$ der Wert von f an jeder Stelle $x \in U$,
- $f``B = \{f`x : x \in B\} = f[B]$ die Bildmenge unter f von jedem $B \in \mathscr{A}$, oder allgemeiner für alle $B \in U$,
- und $f```\mathscr{D} = \{f``B : B \in \mathscr{D}\} = \{f[B] : B \in \mathscr{D}\}$ für alle Unterfamilien $\mathscr{D} \subseteq \mathscr{A}$.

DEFINITION VI.4.2. A heißt Dedekind-unendlich, wenn A mit einer echten Teilmenge gleichmächtig ist.

Mit den bisher betrachteten Axiomen kann man folgendes zeigen:

SATZ VI.4.3. *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.

VI.5. Auswahlaxiom, Beispiele

Wir behaupten, dass umgekehrt jede Dedekind-endliche Menge auch endlich ist, also jede unendliche Menge Dedekind-unendlich sein muss.

SATZ VI.5.1. *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:

$$g(0) := a_0 \in A, \quad g(n+1) := a_{n+1} \in A \setminus \{g(0), g(1), \ldots, g(n)\} \quad \square$$

Nicht auf der Hand liegt die Tatsache, dass dieser Beweis nicht mit den ZF-Axiomen geführt werden kann, man benötigt zusätzlich das Auswahlaxiom.

DEFINITION VI.5.2 (Auswahlaxiom). Das Auswahlaxiom besagt[3]

$$\forall X\ \exists f : \mathcal{P}(X) \setminus \{\emptyset\} \to X :\ \forall A \subseteq X :\ f(A) \in A$$

Ist nämlich f eine solche Auswahlfunktion, so kann man die im obigen Satz gesuchte Funktion g definieren durch

$$g(0) := f(X), \quad g(n+1) := f(X \setminus \{g(0), g(1), \ldots, g(n)\})$$

[3]Man beachte, dass die Argumente von f hier Mengen sind, nämlich Teilmengen von A. Die Schreibweise $f(A)$ ist also hier richtig.

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 $\{0,\dots,n\}$ definiert ist, an der Stelle n den Wert x annimmt, und zwischendurch einer Rekursionsformel gehorcht:

$$\varphi(n,x) := \ (n \in \omega \ \wedge \ x \in X) \wedge \ \exists g' \Big(g' : (n+1) \to X \ \wedge \ g'(n) = x \ \wedge \\ \wedge \ \forall k \leq n : g'(k) = f(X \setminus g'[k]) \Big)$$

Man beachte, dass im Ausdruck $g'[k]$ die Menge aller Werte $g'(i)$ mit $i < k$ gemeint ist: $g'[k] = \{g'(i) : i \in k\} = \{g'(i) : i < k\} = \{g'(0), \dots, g'(k-1)\}$.

Eine Variante des Auswahlaxioms bildet das Auswahlaxiom in Familienversion:

DEFINITION VI.5.3 (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 $A_i := i$. (Das heißt, wir fassen die Menge $\mathcal{P}(A) \setminus \{\emptyset\}$ als Familie auf, indem wir sie mit sich selbst indizieren.) 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

$$f \in \prod_{i<n} X_i\ \wedge\ y \in X_n\ \to\ \prod_{i<n+1} X_i \neq \emptyset,$$

und durch Einführung des Existenzquantors links (2 Mal) erhält man

$$\prod_{i<n} X_i \neq \emptyset\ \wedge\ X_n \neq \emptyset\ \to\ \prod_{i<n+1} X_i \neq \emptyset.$$

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 VI.5.4. *In ZF ist beweisbar: Das Produkt einer endlichen Familie von nichtleeren Mengen ist nie leer.*

VI.6. Das Lemma von Zorn (und andere)

In diesem Abschnitt kommen wir zu drei zum Auswahlaxiom äquivalenten Sätzen. Zunächst aber noch einige Definitionen:

DEFINITION VI.6.1 (Halbordnung). Sei P eine Menge und $\leq$ eine binäre Relation. Dann heißt $(P, \leq)$ Halbordnung, wenn die Relation $\leq$ die folgenden Eigenschaften hat:

- Reflexivität: $a \leq a \quad \forall a \in P$
- Antisymmetrie: $a \leq b \wedge b \leq a \rightarrow a = b \quad \forall a, b \in P$
- Transitivität: $a \leq b \wedge b \leq c \rightarrow a \leq c \quad \forall a, b, c \in P$

DEFINITION VI.6.2 (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 VI.6.3 (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 VI.6.4 (Lemma von Zorn). *Sei $(P, \leq)$ eine Halbordnung. Wenn jede Kette $C \subseteq P$ beschränkt ist, dann existiert ein maximales Element in P.*

SATZ VI.6.5 (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 VI.6.6 (Familie von endlichem Charakter). Sei $\mathscr{F}$ eine Menge von Mengen. $\mathscr{F}$ heißt Familie von endlichem Charakter, wenn gilt[4]

$$\forall X : X \in \mathscr{F} \leftrightarrow (\forall E \subseteq X : E \text{ endlich} \rightarrow E \in \mathscr{F})$$

d.h. eine Menge X liegt genau dann in $\mathscr{F}$, wenn alle ihre endlichen Teilmengen in $\mathscr{F}$ liegen.

Gelegentlich ist die folgende Verschärfung interessant: Eine Familie $\mathscr{F}$ hat Charakter k, wenn gilt:

$$\forall X : X \in \mathscr{F} \leftrightarrow (\forall E \subseteq X : |E| \leq k \rightarrow E \in \mathscr{F})$$

[4]Warnung 1: in den meisten Fällen ist die Implikation „$\rightarrow$“ aus trivialen Gründen gültig; interessant ist meistens die Implikation „$\leftarrow$“, also: Wenn alle endlichen Teilmengen von X in $\mathscr{F}$ liegen, dann auch X.
Warnung 2: Induktion ist oft hilfreich, um „für alle endlichen Teilmengen ...“ zu beweisen; um aber die Implikation „$\leftarrow$„ in der Definition des endlichen Charakters zu beweisen, führen Induktionsbeweise praktisch nie zum Ziel.

BEISPIELE.
- Sei X beliebig. Dann ist $\mathfrak{P}(X)$ von endlichem Charakter (und hat sogar Charakter 1).
- Sei X unendlich. Dann ist die Menge $\{B \subseteq X : B \text{ endlich}\}$ nicht von endlichem Charakter.
- Sei Q eine partielle Ordnung. Dann ist die Menge $\{K \subseteq Q : K \text{ ist Kette}\}$ von endlichem Charakter (und hat sogar Charakter 2).
- Seien A, B Mengen. Dann ist die Menge aller partiellen Funktionen von A nach B von endlichem Charakter. (Auch hier, sowie im nächsten Punkt, hat die Familie sogar Charakter 2.)
- Seien A, B Mengen. Dann ist die Menge aller partiellen *injektiven* Funktionen von A nach B von endlichem Charakter.
- Sei V ein K-Vektorraum. Dann hat die Familie $\mathscr{F}$ aller linear unabhängigen Teilmengen von V endlichen Charakter. (Aber nicht Charakter k, außer wenn $\dim(V) \leq k$.)

Mit dieser Definition gelangen wir zum dritten

SATZ VI.6.7 (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 $\to$ 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 $E \in \mathscr{F}$. (Genau genommen verwenden wir hier Induktion. Das heißt, wir betrachten die Menge aller natürlichen Zahlen n mit der Eigenschaft: $n = 0$, oder in jeder n-elementigen Kette gibt es in maximales Element. Man kann zuerst zeigen, dass diese Menge induktiv ist; daraus schließt man, dass es in jeder endlichen Kette ein Maximum gibt.)

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 VI.6.8 (Vergleichbarkeitssatz für Mengen). *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

$$\mathscr{F} := \{g : \mathrm{dom}(g) \subseteq A, \mathrm{ran}(g) \subseteq B, g \text{ injektiv}\}$$

$\mathscr{F}$ ist eine Familie von endlichem Charakter, man kann also Teichmüller/Tukey anwenden und erhält ein maximales Element $g^* \in \mathscr{F}$. 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 erhält man aus g^* leicht eine injektive Abbildung von B nach A. $\square$

VI.7. Wohlordnungen

Alle Sätze in diesem Abschnitt sind in ZF beweisbar (also ohne das Auswahlaxiom).

DEFINITION VI.7.1 (Wohlordnung). Sei W eine Menge und $\leq$ eine binäre Relation. Dann heißt $(P, \leq)$ Wohlordnung, wenn die Relation $\leq$ die folgenden Eigenschaften hat:

- Reflexivität: $a \leq a \ \ \forall a \in W$.
- Transitivität: $a \leq b \wedge b \leq c \rightarrow a \leq c \ \ \forall a, b, c \in W$.
- Antisymetrie: $a \leq b \wedge b \leq a \ \rightarrow \ a = b$.
- Vergleichbarkeit, Linearität, Totalordnung: $a \leq b \vee b \leq a \ \ \forall a, b \in W$.

- Existenz[5] des Minimums[6]: $\forall A \subseteq W : \ A \neq \emptyset \to \exists \min(A)$. ($x = \min A$ bedeutet $x \in A$ und $\forall a \in A : x \leq a$.)

Eine *strikte* (oder irreflexive) Wohlordnung ist eine Relation $<$, die transitiv, irreflexiv ($\forall x(x \not< x)$) trichotomisch ($\forall x, y : x < y \vee x = y \vee y < x$) ist und die außerdem die Eigenschaft hat, dass jede nichtleere Menge A ein kleinstes Element a_0 hat ($\forall b \in A : b = a_0 \vee a_0 < b$.)

Man sieht leicht, dass jede strikte Wohlordnung auf A durch Hinzufügen der Diagonale $\{(a, a) : a \in A\}$ zu einer (reflexiven) Wohlordnung wird, und umgekehrt. Statt „strikte Wohlordnung“ sagt man oft einfach „Wohlordnung“; ob damit eine reflexive oder eine irreflexive Relation gemeint ist, kann meist aus dem Kontext oder aus den verwendeten Symbolen erschlossen werden: für reflexive Ordnungen verwendet man die Symbole $\leq$, $\leqq$, $\sqsubseteq$, etc, und für irreflexive die Symbole $<$, $\sqsubset$, etc.

Gelegentlich wird auch die Relation $<$ bzw $\leq$ als Wohlordnung bezeichnet, nicht nur die gesamte Struktur $(A, <)$.

BEISPIEL.
- Jede endliche lineare Ordnung ist Wohlordnung. Insbesondere ist die leere Relation eine Wohlordnung der leeren Menge.
- Die Mengen $\mathbb{Z}$, $\mathbb{Q}$, $[0, 1]$, $\mathbb{R}$ (jeweils mit der üblichen Ordnung) sind keine Wohlordnungen.
- $(\{-1, -\frac{1}{2}, -\frac{1}{3}, \ldots, 0\}, \leq)$ ist Wohlordnung, jedoch nicht zu ω isomorph.
- Auf der Menge $\mathbb{Z}$ gibt es eine Wohlordnung, die zu üblichen Ordnung auf ω isomorph ist: $0 \sqsubset 1 \sqsubset -1 \sqsubset 2 \sqsubset -2 \sqsubset \cdots$.
- Die folgende Ordnung ist eine Wohlordnung auf ω, aber nicht zur üblichen Ordnung isomorph: $0 \sqsubset 2 \sqsubset 4 \sqsubset \cdots \sqsubset 1 \sqsubset 3 \sqsubset \cdots$.

Weitere Beispiele erhält man mit dem folgenden Satz:

SATZ VI.7.2. *Seien $(A_1, <_1)$ und $(A_2, <_2)$ disjunkte Wohlordnungen. Dann ist die folgende Ordnung $<$ auf $A \cup B$ eine Wohlordnung:*

$$x < y \ \Leftrightarrow \ (x, y \in A_1 \wedge x <_1 y) \vee (x, y \in A_2 \wedge x <_2 y) \vee (x \in A_1 \wedge y \in A_2)$$

Weiters gilt: Seien $(A_1, <_1)$ und $(A_2, <_2)$ Wohlordnungen. Dann ist die lexikographische Ordnung auf $A_1 \times A_2$ eine Wohlordnung. (In der lexikographischen

[5]Aus der Existenz eines Minimums jeder zweielementigen Menge $\{a, b\}$ folgt die Vergleichbarkeit. Dennoch wird Vergleichbarkeit oft als eigene Bedingung angeführt, weil in einem Beweis, dass eine vorliegende Relation eine Wohlordnung ist, oft die Vergleichbarkeit zuerst bewiesen wird.

[6]Beachte: $x = \min A$ bedeutet, dass x das **kleinste** Element von A ist, und nicht nur irgend ein **minimales** Element. In partiellen Ordnungen kann diese Notation verwirrend sein, sie ist aber üblich. In linearen Ordnungen ist aber ein minimales Element ohnehin dasselbe wie ein kleinstes Element.

Ordnung gilt $(a_1, b_1) < (a_2, b_2)$ *wenn*

$$(a_1 < a_2) \ \vee \ (a_1 = a_2 \wedge b_1 < b_2)$$

gilt.)

Schließlich gilt: Wenn A *durch* $<$ *wohlgeordnet wird, dann wird, dann ist jede Teilmenge* $B \subseteq A$ *durch die Einschränkung von* $<$ *auf* B *ebenfalls wohlgeordnet.*

DEFINITION VI.7.3. Sei $(A, <)$ eine Wohlordnung. Ein *Anfangsabschnitt* von A ist eine nach unten abgeschlossene Teilmenge von A. $B \subseteq A$ heißt echter Anfangsabschnitt von A, wenn B Anfangsabschnitt ist aber $B \neq A$ gilt.

(Jeden Anfangsabschnitt B denken wir uns mit der induzierten Ordnung versehen; $(B, <\restriction B)$ ist dann wiederum Wohlordnung. Der Einfachkeit halber bezeichnen wir diese Struktur allerdings oft mit $(B, <)$.)

Sei $p \in A$. Dann bezeichnen wir mit A_p oder $A_{<p}$ die Menge $\{a \in A : a < p\}$.

Weiters setzen wir $\bar{A} := A \cup \{\infty\}$, wobei ∞ ein beliebiges Element $\notin A$ sein soll, und wir ordnen $\bar{A}$ so, dass die Ordnung auf $\bar{A}$ die Ordnung auf A fortsetzt, und ∞ das größte Element wird. Damit ist $\bar{A}_\infty = A$; der Einfachkeit halber schreiben wir aber nur A_∞ statt $\bar{A}_\infty$.

HILFSSATZ VI.7.4. *Sei* $(A, <)$ *Wohlordnung,* $B \subset A$ *ein echter Anfangsabschnitt. Sei* $p := \min(A \setminus B)$. *Dann ist* $B = A_p$.

Etwas allgemeiner: Sei $B \subseteq A$ *ein beliebiger Anfangsabschnitt von* A, *und sei* $p \in \bar{A}$ *durch* $p := \min\{x \in \bar{A} : x \notin B\}$ *definiert, dann ist* $B = A_p$.

SATZ VI.7.5. *Sei* $(A, <)$ *Wohlordnung.*

(1) *Wenn* $f : A \to A$ *streng monoton ist, dann muss* $f(x) \geq x$ *für alle* $x \in A$ *gelten.*
(2) *Sei* B *Teilmenge eines echten Anfangsabschnitts. Dann kann* A *nicht zu* B *isomorph sein.*
(3) A *kann nicht zu einem echten Anfangsabschnitt isomorph sein.*
(4) *Die Identität ist der einzige Automorphismus von* $(A, <)$.

BEWEIS. (1) Sei f streng monoton. Wenn $M := \{x : f(x) < x\}$ nicht leer ist, dann muss M ein kleinstes Element x_0 haben. Aber dann ist $f(x_0) < x_0$, daher $ff(x_0) < f(x_0)$, somit $f(x_0) \in M$, Widerspruch.
(2) Wäre $f : A \to B$ Isomorphismus, und $B \subseteq A_p$ mit $p \in A$, dann müsste $f(p) \in B$, also $f(p) < p$ sein.
(3) Leicht.
(4) Leicht.

□

SATZ VI.7.6 (Vergleichbarkeitssatz für Wohlordnungen). *Seien* $(A, <_A)$ *und* $(B, <_B)$ *zwei Wohlordnungen. Dann gilt genau einer der folgenden drei Fälle:*

- A *und* B *sind isomorph.*

- *A ist zu einem echten Anfangsabschnitt von B isomorph.*
- *B ist zu einem echten Anfangsabschnitt von A isomorph.*

Überdies sind die Isomorphismen und Anfangsabschnitte eindeutig bestimmt.

BEWEIS. Wir betrachten die Relation $R := \{(a,b) : a \in A, b \in B, A_a \simeq B_b\}$. Man kann folgendes zeigen:

- Wenn $f : A_a \to B_b$ Isomorphismus ist, und $x < a$, dann ist $f \restriction A_x : A_x \to B_{f(x)}$ Isomorphismus.
- $\mathrm{dom}(R)$ ist ein Anfangsabschnitt von A, sagen wir A_p (mit $p \in \bar{A}$).
- $\mathrm{ran}(R)$ ist ein Anfangsabschnitt von B, sagen wir B_q.
- R ist eine Funktion.
  [Aus $(a,b) \in R$ und $(a,b') \in R$ müssen wir schließen, dass $b = b'$. Aus $B_b \simeq A_a \simeq B_{b'}$ schließen wir $B_b \simeq B_{b'}$; wegen Satz VI.7.5 ist $b < b'$ ausgeschlossen, denn dann wäre B_b ein echter Anfangsabschnitt von $B_{b'}$; ebenso ist $b' < b$ ausgeschlossen.]
- R ist Isomorphismus von A_p auf B_q (jeweils versehen mit der von A bzw B induzierten Ordnung).

Wir können nun vier Fälle unterscheiden, je nachdem ob $p = \infty$ und/oder $q = \infty$ ist. Aber wenn $p \in A$ und $q \in B$ ist, dann erhalten wir den folgenden Widerspruch: $R : A_p \to B_q$ ein Isomorphismus, also $(p,q) \in R$, also $p \in \mathrm{dom}(R) = A_p$.
Es bleiben also 3 Fälle:

- $p = \infty$, $q = \infty$. Dann ist $R : A \to B$ ein Isomorphismus.
- $p = \infty$, $q \in B$. Dann ist $R : A \to B_q$ ein Isomorphismus.
- Umgekehrt. □

VI.8. Transfinite Rekursion

Alle Sätze in diesem Abschnitt sind in ZF beweisbar (also ohne das Auswahlaxiom).

Funktionen $f : \mathbb{N} \to \mathbb{N}$ werden oft „rekursiv“ definiert (siehe primitive Rekursion in Abschnitt V.2). Das heißt, dass man eine Vorschrift g angibt, mit deren Hilfe jeder Wert $f(n)$ (für $n > 0$) aus dem Wert $f(n-1)$ berechnet werden kann: $f(n) = g(f(n-1))$. Gelegentlich hängt ein Wert $f(n)$ nicht nur vom vorigen Wert $f(n-1)$ sondern auch von früheren Werten ab, wie etwa bei der Fibonaccifolge: $f(n) = f(n-1) + f(n-2)$ für $n \geq 2$. Dieses Konzept lässt sich auf beliebige lineare Ordnungen verallgemeinern:

DEFINITION VI.8.1. Sei $(L, <)$ eine lineare Ordnung. Für $x \in L$ sei $L_x := \{y \in L : y < x\}$. Für jede Menge A bezeichnen wir mit $A^{<L}$ die Menge aller Funktionen s, deren Definitionsbereich von der Form L_x (für ein $x \in L$) ist und deren

Wertebereich Teilmenge von A ist:

$$A^{<L} := \bigcup_{x\in L} A^{L_x} = \bigcup_{x\in L} \{s \mid s : L_x \to A\}$$

DEFINITION VI.8.2. Sei $(L, <)$ eine lineare Ordnung, A eine Menge, g eine Funktion von $A^{<L}$ nach A, und $f : L \to A$. Die Forderung

$$\forall x \in L : \quad f(x) = g(\, f{\restriction}L_x \,)$$

bezeichnen wir als „Rekursion“ oder „rekursive Definition“.

SATZ VI.8.3. *Sei $(L, <)$ eine Wohlordnung, A eine Menge, und $g : A^{<L} \to A$. Dann gibt es genau eine Funktion $f : L \to A$, die die Rekursion*

$$\forall x \in L : \quad f(x) = g(\, f{\restriction}L_x \,)$$

erfüllt.

BEMERKUNG VI.8.4. Die Wohlordnungseigenschaft von L ist essentiell. Wenn zum Beispiel $L \neq \emptyset$ kein kleinstes Element hat, dann gibt es mindestens zwei Funktionen $f : L \to \{-1, 1\}$, die

$$\forall x \in L : \ f(x) = \min(\mathrm{ran}(f{\restriction}L_x))$$

erfüllen, und es gibt keine Funktion f, die

$$\forall x \in L : \ f(x) = -\min(\mathrm{ran}(f{\restriction}L_x))$$

erfüllt. Ähnliche Beispiele kann man auch dann finden, wenn L ein kleinstes Element hat, solange nur L keine Wohlordnung ist.

BEWEIS. Übungsaufgabe. □

Daher ist der Begriff der rekursiven Definition nur für Wohlordnungen relevant.

BEWEIS VON SATZ VI.8.3. Sei M die Menge aller $m \in \bar{L} := L \cup \{\infty\}$, sodass es genau eine Funktion $s : L_m \to A$ gibt, die die Rekursion

$$(*)_{m,s} \quad \forall x < m : s(x) = g(s{\restriction}L_x)$$

erfüllt. Wir wollen $\infty \in M$ zeigen.

Zunächst überlegen wir, dass es für jedes $m \in \bar{L}$ höchstens eine Funktion $s : L_m \to A$ gibt, die die Rekursion $(*)_{m,f}$ erfüllt; wenn nämlich sowohl $(*)_{m,s_1}$ als auch $(*)_{m,s_2}$ gilt, und wir $x^* := \min\{x < m : s_1(x) \neq s_2(x)\}$ setzen, dann ist $s_1(x^*) = g(s_1{\restriction}L_{x^*}) = g(s_2{\restriction}L_{x^*}) = s_2(x^*)$ ein Widerspruch.

Nun folgt leicht, dass M ein Anfangsabschnitt von $\bar{L}$ ist: wenn nämlich $x < y$ und $y \in M$ gilt, und $s : L_y \to A$ die Rekursion $(*)_{y,s}$ erfüllt, dann erfüllt $s{\restriction}L_x : L_x \to A$ die Rekursion $(*)_{x,s{\restriction}L_x}$, daher $x \in M$.

Ähnlich zeigt man:

(!) Wenn $(*)_{x,s}$ und $(*)_{y,t}$ gelten, mit $x \leq y$, dann ist $s = t{\restriction}L_x$.

Wenn nun $\infty \in M$ gilt, dann ist der Beweis fertig. Wir müssen also aus der Annahme

$$m_1 := \min(\bar{L} \setminus M)$$

einen Widerspruch herleiten.

1.Fall: m_1 ist ein Nachfolger in $\bar{L}$, das heißt: es gibt ein $m_0 := \max\{x : x < m_1\}$. Es gibt also (genau) ein $s_0 : L_{m_0} \to A$, welches die Rekursion $(*)_{m_0,s_0}$ erfüllt. Wir setzen

$$s_1 := s_0 \cup \{(m_0, g(s_0))\}$$

und sehen, dass s_1 die Rekursion $(*)_{m_1,s_1}$ erfüllt. Daher $m_1 \in M$, Widerspruch.

2.Fall: Für alle $x < m_1$ gibt es ein y mit $x < y < m_1$. Wir setzen

$$s_1 := \{(x, s(x)) : \exists y(x < y < m_1) \wedge (*)_{y,s}\}.$$

Mit Hilfe von (!) kann man leicht überprüfen, dass s_1 eine Funktion ist, und dass s_1 auf ganz L_{m_1} definiert ist. Daher ist $m_1 \in M$, Widerspruch. □

VI.9. Der Satz von Hartogs

Alle Sätze in diesem Abschnitt sind in ZF beweisbar (also ohne das Auswahlaxiom).

Wir wollen zeigen, dass es zu jeder Menge A eine Wohlordnung $(W, <)$ und eine Bijektion $W \to A$ gibt; dann gibt es nämlich auf jeder Menge eine Wohlordnung. Dieser Satz ist nur mit dem Auswahlaxiom beweisbar. Der folgende Satz von Hartogs ist jedoch bereits in ZF beweisbar:

SATZ VI.9.1. *Sei A eine beliebige Menge. Dann gibt es eine Wohlordnung W, sodass es keine injektive Abbildung von W nach A gibt.*

BEWEIS. Sei $H = H(A)$ die Menge aller Paare (B, R) mit $B \subseteq A$, sodass R eine strikte Wohlordnung auf B ist. (Zum Beispiel kommt die leere Menge in H vor, ebenso jedes Singleton.)

Auf H definieren wir die Äquivalenzrelation $(B, R) \simeq (C, S)$ der Isomorphie. Die Klasse von (B, R) (also die Menge aller $(C, S) \in H(A)$ mit (C, S) isomorph zu (B, R)) bezeichnen wir mit $[B, R]$ oder $[B, R]_{\simeq}$.

Sei $W(A) := H(A)/{\simeq}$ = die Menge der $\simeq$-Äquivalenzklassen. Mit Hilfe des Vergleichbarkeitssatzes für Wohlordnungen können wir zeigen, dass die Relation

$$[B, R] \sqsubset [C, S] \;\Leftrightarrow\; \exists c_0 \in C : (B, R) \simeq (C_{c_0}, S)$$

wohldefiniert ist, und die Elemente von $W(A)$ (strikt, d.h. irreflexiv) linear ordnet.

Jedes Element $[C, S] \in W(A)$ definiert einen Anfangsabschnitt $W(A)_{[C,S]}$; wir behaupten, dass dieser Anfangsabschnitt zu (C, S) isomorph ist. Zum Beweis geben wir einen Isomorphismus $f : (C, S) \to (W(A)_{[C,S]}, \sqsubset)$ an:

$$f(c) := [(C_c, S)]$$

(Man muss überprüfen, dass f tatsächlich Isomorphismus ist.)

Da alle echten Anfangsabschnitte von $W(A)$ Wohlordnungen sind, und $W(A)$ durch $\sqsubset$ linear geordnet ist, ist $(W(A), \sqsubset)$ selbst Wohlordnung.

Zu zeigen ist, dass es keine injektive Abbildung von $W(A)$ nach A gibt. Wenn $f : W(A) \to A$ so eine Abbildung wäre, und wir die Bildmenge $f[W(A)]$ mit C bezeichnen, so gibt es eine eindeutig bestimmte strikte Wohlordnung S von C, sodass $f : (W(A), \sqsubset) \to (C, S)$ ein Isomorphismus ist.

Dann wäre aber $W(A)$ auch zu seinem echten Anfangsabschnitt $W(A)_{[C,S]}$ isomorph — ein Widerspruch. □

BEMERKUNG VI.9.2. Aus dem Satz von Hartogs und dem Vergleichbarkeitssatz für Mengen folgt leicht der Wohlordnungssatz. Weder Wohlordnungssatz noch Vergleichbarkeitssatz sind aber in ZF beweisbar.

BEISPIEL. Sei $A = \{1, 2, 3\}$. Dann zerfällt $W(A)$ in 4 Klassen: Die Klasse der sechs Wohlordnungen der gesamten Menge A, die Klasse der 2-elementigen Wohlordnungen (wiederum mit sechs Elementen), die Klasse der drei 1-elementigen Wohlordnungen, sowie eine Klasse mit der einzigen Wohlordnung der leeren Menge.

BEISPIEL. Sei $A = \omega$. Dann ist $W(A)$ eine überabzählbare Wohlordnung. Überdies ist $W(A)$ die „kürzeste“ überabzählbare Wohlordnung, das heißt: Jeder echte Anfangsabschnitt von $W(A)$ ist höchstens abzählbar.

DEFINITION VI.9.3. Wir nennen eine Wohlordnung $(A, <)$ „initial“, wenn A zu keinem echten Anfangsabschnitt gleichmächtig ist: $\neg\exists a \in A : A \approx A_a$.

Jede endliche Wohlordnung ist initial, ebenso wie die unendliche Wohlordnung ω. Außerdem ist jede Wohlordnung der Form $W(A)$ initial.

SATZ VI.9.4. *Für jede Wohlordnung $(W, <)$ gibt es einen zu W gleichmächtigen Anfangsabschnitt, dessen Wohlordnung initial ist.*

BEWEIS. Wenn W selbst initial ist, dann ist nichts zu tun. Wenn aber nicht, dann ist die Menge $\{a \in W : W_a \approx W\}$ nicht leer. Sei a^* ihr kleinstes Element. Dann gilt $W_{a^*} \approx W$, und W_{a^*} ist initial, denn jeder echte Anfangsabschnitt von W_{a^*} ist (nach Definition von a^*) nicht gleichmächtig mit W, also auch nicht mit W_{a^*}. □

VI.10. Folgerungen aus dem Auswahlaxiom

In ZFC können wir die folgenden Sätze beweisen:

- das Lemma von Zorn:
  Sei $(P, <)$ eine partielle Ordnung $(P, <)$, in der alle Ketten eine obere Schranke haben. Dann hat P ein maximales Element.

- den Hausdorffschen Kettensatz:
  In jeder partiellen Ordnung $(Q, <)$ gibt es eine maximale Kette.
- den Satz von Teichmüller/Tukey:
  Jede Familie von endlichem Charakter hat ein (bezüglich $\subseteq$) maximales Element.
- den Vergleichbarkeitssatz für Mengen:
  Je zwei Mengen sind vergleichbar (d.h. es gibt eine injektive Funktion von einer in die andere).
- den Wohlordnungssatz.
  Auf jeder Menge gibt es eine Wohlordnung.

Umgekehrt folgt aus jedem dieser Sätze (zusammen mit ZF) das Auswahlaxiom. Für den Wohlordnungssatz ist dies besonders leicht: Wenn E eine Wohlordung auf der Menge X ist, dann ist die Menge

$$\{(Y, y) : Y \subseteq X, Y \neq \emptyset, y = \min_E(Y)\}$$

eine Auswahlfunktion auf $\mathfrak{P}(X) \setminus \{\emptyset\}$.

Weitere Sätze, die (modulo ZF) zum Auswahlaxiom äquivalent sind:

- der Satz von Tychonoff (das Produkt von kompakten Räumen [nicht notwendigerweise T_2] ist wieder kompakt),
- für alle unendlichen Mengen A gibt es eine Bijektion zwischen A und $A \times A$
- Die Potenzmenge jeder Wohlordnung lässt sich wohlordnen.
- Auf jeder linear geordneten Menge gibt es eine Wohlordnung.
- Auf jeder linear geordneten Menge gibt es eine Auswahlfunktion.
- Jeder Vektorraum hat eine Basis.

(Um die Äquivalenz der letzten 4 Aussagen mit dem Auswahlaxiom zu beweisen, braucht man allerdings das Regularitätsaxiom von ZF, welches wir noch nicht besprochen haben.)

SATZ VI.10.1. *Aus dem Auswahlaxiom (genauer: aus ZFC) folgt der Wohlordnungssatz.*

BEWEIS. *Die Idee ist einfach: Sei A eine Menge. Wir verwenden eine Auswahlfunktion f, um zunächst das kleinste Element $a_0 := f(A)$ der Wohlordnung festzulegen (außer wenn $A = \emptyset$). Wenn A mehr als 1 Element enthält, dann verwenden wir wieder die Auswahlfunktion, um ein Element $a_1 \neq a_0$ festzulegen, nämlich $a_1 := f(A \setminus \{a_0\})$. Und so weiter — wir wählen „der Reihe nach" immer wieder neue Elemente aus A aus. Wie lange muss aber diese „Reihe" sein? Wir verwenden eine ganz lange Wohlordnung, das reicht sicher.*

Sei A beliebige Menge, und sei $r : \mathfrak{P}(A) \setminus \{A\} \to A$ eine „Rauswahlfunktion", also eine Funktion, die $r(B) \in A \setminus B$ für alle $B \subsetneq A$ erfüllt. (So eine Funktion erhält man leicht aus dem Auswahlaxiom.)

Sei $\infty \notin A$ beliebig, $\bar{A} := A \cup \{\infty\}$. Sei $r' : \mathfrak{P}(\bar{A}) \to \bar{A}$ so definiert: $r'(B) = B$, wenn $B \subsetneq A$, und $r'(B) = \infty$ wenn $B = A$ oder $\infty \in B$.

Sei W eine Wohlordnung, die sich nicht injektiv nach A einbetten lässt.

Nach dem Satz über transfinite Rekursion gibt es eine Funktion $f : W \to \bar{A}$, die die folgende Rekursion erfüllt:

$$\forall w \in W : \quad f(w) = r(\mathrm{ran}(f{\restriction}W_w))$$

$f(w)$ ist also immer (wenn möglich) ein neues Element von A. Genauer:

(+) Wenn $f(w) \neq \infty$, dann ist $f(w) \notin \{f(x) : x < w\}$.
D.h. $x < w \Rightarrow f(x) \neq f(w)$.

Der Wert ∞ muss von f angenommen werden, sonst wäre f eine injektive Abbildung von W nach A. Sei $w_0 := \min\{w \in W : f(w) = \infty\}$.

Dann ist $f_0 := f{\restriction}W_{w_0} : W_{w_0} \to A$ injektiv. Wegen $f(w_0) = \infty = r'(\mathrm{ran}(f_0))$ ist f_0 auch surjektiv. Also ist f_0 eine Bijektion zwischen der Wohlordnung W_{w_0} und der Menge A. Daher lässt sich A wohlordnen. □

Satz VI.10.2. *Aus dem Auswahlaxiom (genauer: aus ZFC) folgt das Lemma von Zorn.*

Beweis. *Ähnlich wie vorhin versuchen wir „der Reihe nach" verschiedene Elemente von P aufzuzählen; diesmal bemühen wir uns aber, eine strikt wachsende Kette in P aufzuzählen; dieser Prozess kann nur dann stoppen, wenn die bisher konstruierte Kette keine strikte obere Schranke hat. Da sie aber beschränkt ist, muss sie ein größtes Element haben — dieses muss in P maximal sein.*

Sei $(P, \leq)$ eine Ordnung, in der jede Kette beschränkt ist.

Sei W eine Wohlordnung, die sich nicht nach P injektiv einbetten lässt, und sei $\bar{P} := P \cup \{\infty\}$ mit $\infty \notin P$. Wir erweitern die Ordnung von P auf $\bar{P}$, indem wir $p < \infty$ für alle $p \in P$ setzen.

Sei $f : \mathfrak{P}(P) \setminus \{0\} \to P$ eine Auswahlfunktion.

Für jede Menge $K \subseteq \bar{P}$ sei $S(K)$ die Menge der oberen Schranken von K: $S(K) := \{p \in P : \forall k \in K\,(k \leq p)\}$, und sei $S^+(K)$ die Menge der strikten oberen Schranken: $S^+(K) := \{p \in P : \forall k \in K\,(k < p)\}$. Man überlegt leicht, dass folgendes gilt:

(∗) Wenn K eine Menge mit $S^+(K) = \emptyset$ und $S(K) \neq \emptyset$, dann ist jedes Element von $S(K)$ maximal in P. (Überdies kann $S(K)$ nur genau ein Element enthalten.)

(Denn wenn $s \in S(K)$ nicht maximal ist, dann muss es ein t mit $s < t$ geben; aus $(\forall k \in K)(k \leq s)$ folgt $(\forall k \in K)(k < t)$, also $t \in S^+(K)$.)

Sei nun $g : \mathfrak{P}(\bar{P}) \to P$ so definiert:

$$g(A) = \begin{cases} f(S^+(A)) \in P & \text{wenn } A \subseteq P,\ S^+(A) \neq \emptyset \\ \infty & \text{sonst} \end{cases}$$

Dann gibt es eine Funktion $f : W \to \bar{P}$ mit $f(w) = g(f[W_w])$ für alle $w \in W$.
Nehmen wir an, dass der Wert ∞ von f nicht angenommen wird. Für $w_0 < w_1$ ist dann $f(w_1)$ eine strikte obere Schranke für $f(w_0)$, d.h. $f(w_0) < f(w_1)$, also f injektiv. Das ist unmöglich.
Sei also w^* minimal mit $f(w^*) = \infty$. Dann ist $f \restriction W_{w^*}$ strikt monoton, das Bild von W_{w^*} also eine Kette K. Auf diese Kette wenden wir $(*)$ an und erhalten ein maximales Element von P. □

Ein wichtiger

SATZ VI.10.3. *Aus dem Auswahlaxiom (genauer: aus ZFC) folgt das Lemma von Zorn.*

Wir beenden das Kapitel mit einem überraschenden Ergebnis.

SATZ VI.10.4 (Wohlordnungssatz). *Sei A eine Menge. Dann existiert eine Relation R, sodass (A, R) eine Wohlordnung ist.*

Der Wohlordnungssatz kann mit ZFC bewiesen werden. Er hat die Konsequenz, dass z.B. auch die reellen Zahlen wohlgeordnet werden können.
So eine Wohlordnung ist aber nicht „definierbar"; genauer: für jede Formel $\varphi(x, y)$ in der Sprache der Mengenlehre ist der Satz

$$\{(x, y) \in \mathbb{R} \times \mathbb{R} : \varphi(x, y)\} \text{ ist Wohlordnung von } \mathbb{R}$$

in ZFC nicht beweisbar. (Allerdings gibt es Kandidaten für Formeln, die $\mathbb{R}$ wohlordnen. Genauer: Es gibt eine explizite Formel φ, für die der obige Satz in ZFC nicht widerlegbar ist, d.h. seine Negation ist nicht beweisbar.)

BEWEIS DES WOHLORDNUNGSSATZES (SKIZZE). Sei A eine Menge, und sei f eine Auswahlfunktion, also eine Funktion, die jeder nichtleeren Teilmenge $S \subseteq A$ ein Element $f(S) \in S$ zuordnet. Wir wollen f verwenden, um eine Wohlordnung auf A zu konstruieren. Zunächst gehen wir intuitiv vor:

- Unsere Wohlordnung muss ein kleinstes Element haben. Das kleinste Element dieser Wohlordnung wird $a_0 := f(A)$ sein. (Wenn A nicht leer ist.)
- Das nächste Element wird $a_1 := f(A \setminus \{a_0\})$ sein. (Wenn A mehr als ein Element hat.)
- etc.
- Nach unendliche vielen Schritten betrachten wir die Menge $A \setminus \{a_0, a_1, \ldots, \}$. Wenn sie nicht leer ist, wählt f daraus ein Element a_ω aus, etc.

– etc. etc.

Jedes Element entsteht also aus seinen Vorgängern durch Anwendung der Auswahlfunktion f auf das Komplement seiner Vorgänger. Diese Einsicht verwenden wir, um den Beweis etwas exakter zu formulieren. (Wenn wir nämlich einen Beweis im Axiomensystem ZFC führen wollen, muss „etc." unbedingt präzisiert werden.)
Wir werden die gesuchte Wohlordnung als Menge $W_\varphi := \{(x,y) \in A \times A : \varphi(x,y,f)\}$ schreiben, für eine geeignete (relative komplizierte) Formel φ. Die Existenz dieser Menge ergibt sich aus (der Existenz von A und $A \times A$ und) dem Aussonderungsaxiom. Wir wollen φ so wählen, dass

Wenn f Auswahlfunktion ist, dann ist W_φ Wohlordnung von A

in ZFC beweisbar wird.
Zunächst geben wir eine Formel an, die Anfangsabschnitte unserer Wohlordnung beschreibt. Wir sagen, dass (B,R) folgsam ist, wenn folgende Eigenschaften erfüllt sind:

- $B \subseteq A$
- $R \subseteq B \times B$
- R ist eine Wohlordnung von B (im strikten Sinn, also irreflexiv)
- Für alle $b \in B$ ist $b = f(A \setminus B_b)$, wobei wir $B_b := \{x \in B : (x,b) \in R\}$ setzen.

Offensichtlich lässt sich dies in der Sprache von ZFC beschreiben. Wir wollen W so finden, dass (A,W) folgsam ist. Die leere Menge (mit der leeren Relation) ist folgsam, ebenso wie die folgenden Mengen (wenn a_0, a_1 wie oben definiert sind).

- $(\{a_0\}, R_0)$ mit $R_0 = \emptyset$.
- $(\{a_0, a_1\}, R_1)$ mit $R_1 = \{(a_0, a_1)\}$
- $(\{a_0, a_1, a_2\}, R_2)$ mit $R_2 = \{(a_0, a_1), (a_1, a_2), (a_0, a_2)\}$
- etc.
- $\{a_0, a_1, \ldots\}$ mit der angedeuteten Ordnung
- $\{a_0, a_1, \ldots, a_\omega\}$ mit der angedeuteten Ordnung
- etc. etc.

Diese Aussage lässt sich wegen der vielen „etc." nicht so leicht in der Sprache von ZFC formalisieren. Wir begnügen uns mit den folgenden Behauptungen:

(1) Seien (B,R) und (B',R') folgsam. Dann ist entweder $B = B'$, $R = R'$, oder es gibt ein $b \in B$, sodass $B' = B_b$ ist, und R' die Einschränkung von R auf B', oder der umgekehrte Fall tritt ein (d.h. $\exists b \in B' \cdots$).
(2) (*Umformulierung des vorigen Punkts*) Wann immer wir zwei folgsame Mengen haben, sind sie entweder (samt ihren Ordnungen) gleich, oder die eine ist ein echter „Anfangsabschnitt" der anderen.

(3) Wann immer wir beliebig viele folgsame Ordnungen haben, sind sie alle Anfangsabschnitte einer gemeinsamen Ordnung (die man einfach durch Vereinigung erhält)
(4) Wenn (B, R) folgsam ist, und $B \neq A$, dann gibt es eine folgsame Ordnung (B', R'), von der (B, R) ein Anfangsabschnitt ist.
(Nämlich: Sei $b^* := f(A \setminus B)$, $B' := B \cup \{b^*\}$, und in R' sei b^* größer als alle $b \in B$, d.h. $R' = R \cup (B \times \{b^*\})$.

Sobald man diese Aussagen bewiesen hat, vereinigt man alle folgsamen Ordnungen und erhält eine Wohlordnung (B^*, R^*), von der man $B^* = A$ zeigen kann, somit ist R^* eine Wohlordnung auf A. □

VI.10.A. Weiteres über Wohlordnungen. *Wir geben hier eine Variante des Beweises des Wohlordnungsatzes. Zunächst zeigen wir, dass es zu jeder Menge M eine Wohlordnung W gibt, die sich nicht injektiv nach M einbetten lässt. (Hier wird das Auswahlaxiom nicht verwendet.)*

Mit Hilfe dieses Satzes beweisen wir (in ZFC, also mit des Auswahlaxiom) das Lemma von Zorn. Daraus folgt, wie schon oben gezeigt, der Satz von Tukey sowie der Vergleichbarkeitssatz; wenn aber M mit W vergleichbar ist, so muss es eine injektive Funktion von M nach W geben, das liefert eine Wohlordnung auf M.

SATZ VI.10.5. *Sei (W, R) eine Wohlordnung, und sei $V \subseteq W$. Dann ist auch (V, R) (genauer: (V, S) mit $S := R \cap (V \times V)$) eine Wohlordnung.*

SATZ VI.10.6. *Sei $(W, <)$ eine Wohlordnung. Dann gilt:*

(a) *Für jede strikt monotone Funktion $f : W \to W$ gilt $\forall w \in W(w \leq f(w))$.*
(b) *Es gibt nur einen einzigen Automorphismus von W, nämlich die Identitätsabbildung.*
(c) *Für alle $w_0 \in W$ gilt: Es gibt keinen Ordnungsisomorphismus zwischen W und $W_{w_0} := \{x \in W : x < w_0\}$. Auch für jede Teilmenge $V \subseteq W_{w_0}$ gilt, dass W nicht zu V isomorph sein kann.*

BEWEIS. Sei $f : W \to W$ strikt monoton. Wenn es ein w mit $f(w) < w$ gibt, dann muss es ein kleinstes solches Element w_0 geben. Sei $w_1 := f(w_0)$. Dann ist $w_1 < w_0$, wegen der strikten Monotonie also auch $f(w_1) < f(w_0) = w_1$. Damit widerspricht w_1 der Minimalität von w_0.

(b) ist leicht: Wenn f Automorphismus ist, dann auch f^{-1}; daher muss $f(x) \geq x$ und $f^{-1}(y) \geq y$ für alle x, y gelten. Daraus folgt $f(x) = x$ für alle x.

Die Behauptung (c) folgt aus (a). Sei nämlich $f : W \to V \subseteq W_{w_0}$ ein Ordnungsisomorphismus, dann ist f eine strikt monotone Funktion von W nach W, muss also $f(w_0) \geq w_0$ erfüllen. Aber $f(w_0) \in V$, daher $f(w_0) < w_0$; dies ist ein Widerspruch. □

SATZ VI.10.7 (Vergleichbarkeitssatz für Wohlordnungen). *Seien $(A, <)$ und $(B, <)$ Wohlordnungen. Dann gilt genau einer der drei Fälle:*

(1) *„Gleichheit", d.h., A und B sind isomorph.*
(2) *„A ist kürzer als B", d.h.: es gibt ein Element $b_0 \in B$, sodass A zu $B_{b_0} := \{y \in B \mid y < b_0\}$ isomorph ist.*
(3) *„B ist kürzer als A", d.h.: es gibt ein Element $a_0 \in A$, sodass A_{a_0} zu B isomorph ist.*

(Überdies sind die jeweiligen Isomorphismen eindeutig; falls es z.B. in (a) zwei verschiedene Isomorphismen $f, g : A \to B$ gibt, dann liefert $f^{-1} \circ g$ einen Widerspruch zu Satz VI.10.6(b). Auch sind die Elemente a_0 bzw. b_0 eindeutig bestimmt, wegen Satz VI.10.6(c).)

BEWEISSKIZZE. Wir definieren $f := \{(a, b) \in A \times B \mid A_a \simeq B_b\}$. Mit Satz VI.10.6(b) zeigt man leicht, dass f eine partielle injektive Funktion von A nach B ist, die die Ordnung erhält.

Der Definitionsbereich von f ist in A nach unten abgeschlossen: Wenn $a_0 < a_1$ in A, und $A_{a_1} \simeq B_{f(a_1)}$, so muss dies durch einen Isomorphismus $g : A_{a_1} \to B_{f(a_1)}$ bezeugt werden. Dann ist $g{\restriction}A_{a_0}$ ein Isomorphismus zwischen A_{a_0} und $B_{g(a_0)}$, daher $(a_0, g(a_0)) \in f$. Ebenso ist der Wertebereich von f in B nach unten abgeschlossen.

Ob der Definitionsbereich $\mathrm{dom}(f)$ gleich A ist bzw. ob der Wertebereich $\mathrm{ran}(f)$ ganz B ist, wissen wir nicht; theoretisch sind also 4 Fälle möglich:

(1) $\mathrm{dom}(f) = A$ und $\mathrm{ran}(f) = B$. Also $A \simeq B$, bezeugt durch den Isomorphismus f.
(2) $\mathrm{dom}(f) = A$ und $b^* := \min(B \setminus \mathrm{ran}(f))$ ist wohldefiniert. Dann ist f Isomorphismus zwischen A und B_{b^*}, also ist A „kürzer" als B.
(3) $\mathrm{dom}(f) \neq A$, $\mathrm{ran}(f) = B$. Analog zu (2), nur ist jetzt B kürzer als A.
(4) Sowohl $a^* := \min(A \setminus \mathrm{dom}(f))$ als auch $b^* := \min(B \setminus \mathrm{ran}(f))$ sind wohldefiniert. Dieser Fall kann nicht eintreten, denn dann wäre $f : A_{a^*} \to B_{b^*}$ Isomorphismus, also $(a^*, b^*) \in f$.

□

HILFSSATZ VI.10.8. *Sei $(X, <)$ eine lineare Ordnung. Dann ist $(X, <)$ genau dann eine Wohlordnung, wenn jede Menge $X_a := \{x \in X : x < a\}$ (mit der eingeschränkten Ordnung $< {\restriction} X_a$) eine Wohlordnung ist.*

BEWEIS. Sei $Y \subseteq X$ nicht leer, und sei $y_0 \in Y$ beliebig. Wir unterscheiden zwei Fälle: Entweder ist Y_{y_0} leer, dann ist $y_0 = \min(Y)$. Oder Y_{y_0} ist eine nichtleere Teilmenge von X_{y_0}, hat also ein kleinstes Element y_1; dann ist $y_1 = \min(Y)$. In jedem Fall hat Y also ein kleinstes Element. □

Der folgende Satz ist bereits in ZF beweisbar.

SATZ VI.10.9 (Satz von Hartogs). *Sei A eine beliebige Menge. Dann gibt es eine Wohlordnung $(W, <)$ mit der Eigenschaft, dass es keine injektive Abbildung von W nach A gibt.*

(Der Satz folgt leicht aus dem Wohlordnungssatz und dem Satz von Cantor: Man nehme eine Wohlordnung der Potenzmenge von A. Dafür würde man aber das Auswahlaxiom verwenden; wir geben eine explizite Wohlordnung W an.)

BEWEIS. Sei $H(A)$ die Menge aller Paare (X, R), sodass $X \subseteq A$ ist und R eine Wohlordnung auf X. (Insbesondere enthält $H(A)$ zum Beispiel die leere Wohlordnung.)

Wir definieren $(X, R) \sim (Y, S)$ genau dann, wenn (X, R) isomorph zu (Y, S) ist. Die Äquivalenzklasse von (X, S) kürzen wir mit $[X, S]$ ab; die Menge aller Äquivalenzklassen bezeichnen wir $W(A)$.

Nach dem Vergleichbarkeitssatz für Wohlordnungen ist $W(A)$ durch

$$[X, R] < [Y, S] \text{ genau dann, wenn } (X, R) \text{ „kürzer“ als } (Y, S) \text{ ist}$$

linear geordnet. Es gilt nun für alle $(Y, S) \in H(A)$:

(∗) Der durch $[Y, S]$ definierte Anfangsabschnitt $W(A)_{<[Y,S]} := \{[X, R] : [X, R] < [Y, S]\}$ ist ordnungsisomorph zu (Y, S).

Dies zeigt man, indem man nachrechnet, dass die Abbildung $y \mapsto [Y_y, S{\restriction}Y_y]$ ein Isomorphismus von (Y, S) auf $W(A)_{<[Y,S]}$ ist.

Daraus folgt, dass $W(A)$ eine Wohlordnung ist.

Eine injektive Abbildung von $W(A)$ nach A, etwa auf die Menge $X \subseteq A$, würde eine Wohlordnung $(X, R) \simeq W(A)$ und wegen (∗) einen Isomorphismus $W(A) \simeq (X, R) \simeq W(A)_{[X,R]}$ induzieren, ein Widerspruch zu Satz VI.10.6.

□