Mathematische Logik

Anton Deitmar

Sommer 2024

Inhaltsverzeichnis

1 Aussagenlogik und Logik erster Stufe

1.1 Aussagenlogik

Die formale Aussagenlogik besteht aus

- einer abzählbaren Menge von Aussagensymbolen A, B, C oder $A_1, A_2, A_3, \ldots$,
- Klammern "(" und ")" sowie den Junktoren "$\neg$" und "$\rightarrow$".

Definition 1.1.1. Eine **Aussage** ist eine Zeichenkette, die sich aus den Symbolen der Aussagenlogik zusammensetzt und auf folgende Weise entsteht (induktive Definition)

- Jedes Aussagensymbol ist eine Aussage,
- Sind $\mathcal{A}$ und $\mathcal{B}$ Aussagen, so sind $(\mathcal{A} \rightarrow \mathcal{B})$ und $(\neg\, \mathcal{A})$ Aussagen.

Der Begriff der induktiven Definition beinhaltet, dass jede Aussage durch endliche Anwendung dieser Prinzipien entsteht.

Lemma 1.1.2. (a) *Jede Aussage besitzt genausoviele Linksklammern wie Rechtsklammern. Das erste Mal, wenn diese beiden Zahlen uebereinstimmen, ist am Ende der Formel.*

(b) *Eine Aussage kann* **nur auf genau eine Weise** *durch sukzessives Anwenden der Definitionsprinzipien gewonnen werden. Genauer heißt das: Ist $\mathcal{C}$ eine Aussage, dann gilt genau einer der drei Fälle:*

(i) *$\mathcal{C}$ ist ein (eindeutig bestimmtes) Aussagensymbol, oder*

(ii) *es gibt genau eine Aussage $\mathcal{A}$ mit*

$$\mathcal{C} \equiv (\neg\, \mathcal{A}),$$

oder

(iii) *es gibt genau ein Paar von Aussagen $(\mathcal{A}, \mathcal{B})$, so dass*

$$\mathcal{C} \equiv (\mathcal{A} \rightarrow \mathcal{B}).$$

Beweis. Induktion nach der Laenge der Formel, simultan fuer beide Behauptungen. Nach Definition ist jede Aussage entweder eine Aussagenvariable oder beginnt und endet mit "(" und ")". Wir entfernen beide. Ist dann das erste Zeichen ein $\neg$, sind wir in Situation (i). Andernfalls ist das erste Symbol ein "(" und wir haben Fall (iii). Es bleibt nur noch die Eindeutigkeit in diesem letzten Fall zu zeigen. Aber wir koennen

(i) auf alle kuerzeren Formeln anwenden und haben $\mathcal{A}$ gefangen, sobald die Zahlen gleich sind. □

Zur Schreibweise: Wir lassen äußere Klammern meistens weg. Wir lassen auch innere Klammern manchmal weg, wobei wir vereinbaren, dass $\neg$ stärker bindet als $\to$, also soll etwa

$$\neg A \to B$$

als $(\neg A) \to B$ gelesen werden. Innere Klammern können nicht immer weggelassen werden, denn $\neg (A \to B)$ ist durchaus verschieden von $\neg A \to B$.

Definition 1.1.3. Wir führen die folgenden Abkürzungen ein:

$\mathcal{A} \vee \mathcal{B}$ steht für $\neg \mathcal{A} \to \mathcal{B}$

$\mathcal{A} \wedge \mathcal{B}$ steht für $\neg (A \to \neg \mathcal{B})$

Beispiele 1.1.4.

- $\neg (A \to B)$ ist eine Aussage, ebenso ist $(\neg A) \to (\neg B)$ eine Aussage.
- Die Zeichenkette

  $$() \to \neg ABCD((($$

  ist keine Aussage.

Ferner vereinbaren wir, dass bei gleichen Zeichen **Rechtsklammerung** herrscht, also soll

$$A \to B \to C \to D$$

dasselbe sein wie

$$A \to (B \to (C \to D)).$$

* * *

1.2 Wahrheitsbelegung

Definition 1.2.1. Eine **Wahrheitsbelegung** ist eine Funktion $\mathfrak{b}$, die jedem Aussagensymbol einen Wahrheitswert in $\{w, f\}$ zuordnet, also eine Abbildung

$$\mathfrak{b} : \mathcal{S} \to \{w, f\},$$

wobei $\mathcal{S}$ die Menge der Aussagensymbole ist.

Lemma 1.2.2. *Ist $\mathfrak{b}$ eine Wahrheitsbelegung, dann gibt es genau eine Fortsetzung von $\mathfrak{b}$ zu einer Abbildung*

$$\mathfrak{b} : \mathrm{Auss} \to \{w, f\},$$

wobei Auss *die Menge der Aussagen ist, so dass*

$$\begin{aligned} \mathfrak{b}(\neg\mathcal{A}) = w \quad &\Leftrightarrow \quad \mathfrak{b}(\mathcal{A}) = f, \\ \mathfrak{b}(\mathcal{A}\to\mathcal{B}) = w \quad &\Leftrightarrow \quad \textit{wenn } \mathfrak{b}(\mathcal{A}) = w \textit{ dann } \mathfrak{b}(\mathcal{B}) = w. \end{aligned}$$

Beweis. **Existenz.** Wir definieren die Fortsetzung induktiv durch $\mathfrak{b}(\mathcal{A}\to\mathcal{B}) = w$ falls $\big(\mathfrak{b}(\mathcal{A}) = w\big) \Rightarrow \big(\mathfrak{b}(\mathcal{B}) = w\big)$ und $\mathfrak{b}(\mathcal{A}\to\mathcal{B}) = f$ andernfalls, sowie $\mathfrak{b}(\neg\mathcal{A}) = f$ falls $\mathfrak{b}(\mathcal{A}) = w$ und umgekehrt. Diese Vorschrift liefert per Induktion eine Fortsetzung, die, was man wieder per Induktion verifiziert, die Bedingung erfüllt, so dass die Existenz gesichert ist. Man beachte, dass hier die Eindeutigkeit des induktiven Aufbaus zum Tragen kommt. Wäre dem nicht so, müsste man an dieser Stelle ein Wohldefiniertheitsproblem lösen.

Die **Eindeutigkeit** zeigen wir wieder ueber eine Induktion: Sei $\mathfrak{b}'$ eine weitere Abbildung $\mathfrak{b}'$: Auss $\to \{w, f\}$ mit der Eigenschaft:

$$\begin{aligned} \mathfrak{b}'(\neg\mathcal{A}) = w \quad &\Leftrightarrow \quad \mathfrak{b}'(\mathcal{A}) = f, \\ \mathfrak{b}'(\mathcal{A}\to\mathcal{B}) = w \quad &\Leftrightarrow \quad \text{wenn } \mathfrak{b}'(\mathcal{A}) = w \text{ dann } \mathfrak{b}'(\mathcal{B}) = w. \end{aligned}$$

Es gelte $\mathfrak{b}(A) = \mathfrak{b}'(A)$ fuer jedes Aussagensymbol A. Wir zeigen $\mathfrak{b}(\mathcal{A}) = \mathfrak{b}'(\mathcal{A})$ fuer jede Aussage $\mathcal{A}$ durch Induktion ueber die Laenge der Zeichenkette $\mathcal{A}$: Ist $\mathcal{A}$ ein Aussagensymbol, so ist nichts zu zeigen. Ist $\mathcal{A} = \neg\mathcal{B}$ fuer eine Aussage $\mathcal{B}$, so gilt

$$\begin{aligned} \mathfrak{b}'(\mathcal{A}) = w &\Leftrightarrow \mathfrak{b}'(\neg\mathcal{B}) = w \\ &\Leftrightarrow \mathfrak{b}'(\mathcal{B}) = f \\ &\Leftrightarrow \mathfrak{b}(\mathcal{B}) = f \\ &\Leftrightarrow \mathfrak{b}(\neg\mathcal{B}) = w \Leftrightarrow \mathfrak{b}(\mathcal{A}) = w. \end{aligned}$$

Ist schliesslich $\mathcal{A} = \mathcal{B}\to\mathcal{C}$ fuer zwei Aussagen $\mathcal{B}$ und $\mathcal{C}$, so gilt

$$\begin{aligned} \mathfrak{b}'(\mathcal{A}) = w &\Leftrightarrow \mathfrak{b}'(\mathcal{B}\to\mathcal{C}) = w \\ &\Leftrightarrow \text{ wenn } \mathfrak{b}'(\mathcal{B}) = w \text{ dann } \mathfrak{b}'(\mathcal{C}) = w \\ &\Leftrightarrow \text{ wenn } \mathfrak{b}(\mathcal{B}) = w \text{ dann } \mathfrak{b}(\mathcal{C}) = w \\ &\Leftrightarrow \mathfrak{b}(\mathcal{B}\to\mathcal{C}) = w \Leftrightarrow \mathfrak{b}(\mathcal{A}) = w. \end{aligned}$$

□

Definition 1.2.3. Zwei Aussagen $\mathcal{A}$ und $\mathcal{B}$ heissen **aussagenlogisch äquivalent**, wenn für jede Wahrheitsbelegung $\mathfrak{b}$ gilt

$$\mathfrak{b}(\mathcal{A}) = w \quad \Leftrightarrow \quad \mathfrak{b}(\mathcal{B}) = w.$$

Beispiele 1.2.4. • Die Aussagen $A \wedge (B \vee C)$ und $(A \wedge B) \vee (A \wedge C)$ sind aussagenlogisch äquivalent. Dies sieht man ein, indem man die möglichen Werte aller Wahrheitsbelegungen in einer **Wahrheitstafel** vergleicht

A	B	C	B∨C	A∧(B∨C)	A∧B	A∧C	(A∧B)∨(A∧C)
w	w	w	w	w	w	w	w
w	w	f	w	w	w	f	w
w	f	w	w	w	f	w	w
w	f	f	f	f	f	f	f
f	w	w	w	f	f	f	f
f	w	f	w	f	f	f	f
f	f	w	w	f	f	f	f
f	f	f	f	f	f	f	f

- Fuer eine natuerliche Zahl $n \geq 3$ ist die Aussage

$$A_1 \to A_2 \to \cdots \to A_n$$

aussagenlogisch äquivalent zu

$$(A_1 \wedge A_2 \wedge \cdots \wedge A_{n-1}) \to A_n.$$

Beweis. Fuer $n = 3$ ist die Aequivalenz von

$$A \to B \to C \quad \text{und} \quad (A \wedge B) \to C$$

zu zeigen, was man wieder ueber eine Wahrheitstafel bewerkstelligt.

Fuer den Induktionsschritt $n \to n+1$ beachte die Rechtsklammerung. Wir wenden die Induktionsvoraussetzung auf den zweiten Teil der Formel an und erhalten

$$\begin{aligned} A_1 \to \Big(A_2 \to \cdots \to A_{n+1}\Big) &\Leftrightarrow A_1 \to \Big((A_2 \wedge \cdots \wedge A_n) \to A_{n+1}\Big) \\ &\Leftrightarrow (A_1 \wedge A_2 \wedge \cdots \wedge A_n) \to A_{n+1}, \end{aligned}$$

wobei im zweiten Schritt der Induktionsanfang benutzt wurde. □

Definition 1.2.5. Eine **Tautologie** ist eine Aussage $\mathcal{A}$, die unter jeder Wahrheitsbelegung den Wert w zugewiesen bekommt.

Beispiele 1.2.6. • $A \vee \neg A$ ist eine Tautologie.

- Die Aussage

$$\Big[A \wedge (B \vee C)\Big] \quad \to \quad \Big[(A \wedge B) \vee (A \wedge C)\Big]$$

ist eine Tautologie.

- Die Aussage $A \to (A \to B) \to B$ ist eine Tautologie, denn wir haben uns schon klargemacht, dass diese Aussage äquivalent ist zu

$$[A \wedge (A \to B)] \to B$$

- (Syllogismus) Die Aussage

$$\Big((A \to B) \wedge (B \to C)\Big) \to (A \to C)$$

ist eine Tautologie.

* * *

1.3 Sprachen der ersten Stufe

Definition 1.3.1. Die **Grundzeichen** einer Sprache (erster Stufe) sind

(a) abzählbar viele **freie Variablen** $a_1, a_2, a_3, \ldots$,

(b) abzählbar viele gebundene Variablen $x_1, x_2, x_3, \ldots$,

(c) für jedes $n \geq 0$ eine Menge von n-stelligen Funktionszeichen f, g, f^n, g^n und eine Menge von n-stelligen Prädikatszeichen p, q, p^n, q^n, unter den 2-stelligen Prädikatszeichen das Gleichheitszeichen "=",

(d) die Junktoren $\neg$, $\to$ und der Quantor $\forall$ (für alle).

Die Unterscheidung von freien und gebundenen Variablen ist ein kleiner Trick, durch den man sich Unannehmlichkeiten erspart.

Beispiele 1.3.2.

- Das zweistellige Funktionszeichen + kommt in der Sprache der Ringtheorie vor.
- Das zweistellige Prädikatszeichen $\leq$ kommt in der Sprache der partiellen Ordnungen vor.
- Ein nullstelliges Funktionszeichen ist dasselbe wie eine Konstante, etwa e für die Eulerzahl. Nullstellige Prädikatszeichen heissen auch **Aussagezeichen**.

Definition 1.3.3. (Induktive Definition der **Terme** einer Sprache L)

(a) Jede freie Variable ist ein Term von L.

(b) Ist f ein n-stelliges Funktionszeichen und sind $t_1, \ldots, t_n$ Terme, so ist $ft_1 \ldots t_n$ ein Term von L.

Ein Term heißt **geschlossener Term**, wenn er keine Variablen enthält. Konstanten sind Beispiele geschlossener Terme.

Zur klammerfreien Schreibweise. Als Mathematiker schreiben wir gern $f(t_1, \ldots, t_n)$ statt $ft_1 \ldots t_n$, das ist aber nur eine andere Schreibweise. In diesem Skript benutzen wir die klammerfreie Schreibweise, da es erstens induktive Beweise leichter macht und wir zweitens die Klammern zu anderen Zwecken brauchen. Wir werden etwa $F(a)$ für eine Zeichenkette schreiben, in der die Variable a auftauchen kann (oder auch nicht). Dann bezeichnet $F(x)$ die Zeichenkette, die wir erhalten, wenn wir jedes Auftreten von a durch x ersetzen. Ist etwa $F(a)$ die Zeichenkette $\to = aa = aa$, dann ist $F(x)$ die Zeichenkette $\to = xx = xx$.

Man beachte, dass im ersten Abschnitt die Aussagenlogik mit Klammern eingeführt wurde. Letztenendes ist das Geschmacksfrage, man kann auch die Aussagenlogik klammerfrei machen, die Tautologie

$$\Big[A \wedge (B \vee C)\Big] \quad \to \quad \Big[(A \wedge B) \vee (A \wedge C)\Big]$$

würde dann etwa

$$\to \wedge A \vee BC \vee \wedge AB \wedge AC,$$

was die Lesbarkeit nicht verbessert. Einigen wir uns darauf, **theoretisch** eine klammerfreie Schreibweise zu benutzen, dann aber die jeweilige Schreibweise mit Klammern als Abkürzung für die klammerfreie zu betrachten.

Beispiele 1.3.4.

- $a + b$, $ab + c$ sind Terme in der Sprache der Ringe. Eigentlich müssten wir $+ab$ und $+ \cdot abc$ schreiben, aber die geläufigen Schreibweisen dienen hier als Abkürzung.
- e^a ist ein Term in der Sprache der vollständigen geordneten Körper, wobei wir Freiheit haben, etwa e als Konstante zu definieren und dann $e^a = \mathrm{pot}(e, a)$ zu setzen, wobei pot das Zeichen des Potenzierens sein soll, oder aber e^a als $e(a)$ zu interpretieren, wobei wir e als einstelliges Funktionszeichen verstehen und gelegentlich e als Abkürzung für $e^1 = e(1)$ benutzen.

Definition 1.3.5. Die **Primformeln** einer Sprache L sind die Zeichenreihen $pt_1 \ldots t_n$, wobei p ein n-stelliges Prädikatszeichen und $t_1, \ldots, t_n$ Terme von L sind.

Definition 1.3.6. (Induktive Definition der **Formeln** von L)

(a) Jede Primformel von L ist eine Formel von L.

(b) Sind A und B Formeln von L, so sind auch $A \to B$ und $\neg A$ Formeln von L.

(c) Ist $F(a)$ eine Formel, *in der die gebundene Variable x nicht auftritt*, dann ist $\forall x F(x)$ eine Formel von L, wobei $F(x)$ die Zeichenkette bedeutet, die man erhält, wenn man jedes Auftreten der Variablen a durch x ersetzt.

Beispiele 1.3.7.

- $\forall x = xa$ ist eine Formel, weil $= ba$ eine Formel ist, in der x nicht auftritt.
- $\forall x \forall y = xy$ ist eine Formel.
- $\forall xxy$ und $\forall x \forall x = xx$ sind keine Formeln.
- $(\forall x F(x)) \vee (\forall x G(x))$ ist eine Formel, falls $F(a)$ und $G(a)$ Formeln sind, in denen x nicht auftritt.

Definition 1.3.8. Eine **Sprache** L der ersten Stufe besteht aus den Grundzeichen, den Termen und den Formeln von L.

Definition 1.3.9. Die **logischen Grundzeichen** einer Sprache L sind

$$\neg, \to, \forall, = .$$

Lemma 1.3.10. *Haben zwei Sprachen L und L' dieselben Grundzeichen, so sind sie identisch.*

Beweis. Die Sprachen haben dieselben Grundzeichen. Induktiv folgt, dass sie dieselben Terme und Formeln haben. □

Wir schreiben auch $\forall_x F(x)$ fuer $\forall x\, F(x)$. Desweiteren ist $\forall_{x \in A} F(x)$ eine Abkuerzung fuer $\forall x\, (x \in A \to F(x))$.

Ferner steht

$$\exists_x F(x) \quad \text{fuer} \quad \neg \forall_x \neg F(x).$$

Zur Klammerersparnis vereinbaren wir ausserdem:

(a) Aussenklammern werden meist fortgelassen,

(b) $\neg$ bindet am stärksten,

(c) $\wedge$, $\vee$ binden stärker als $\to$, $\leftrightarrow$.

Definition 1.3.11. Ist $\mathcal{F}$ eine Formel, so sei $\mathrm{FV}(\mathcal{F})$ die Menge der freien Variablen in $\mathcal{F}$. Ist $\mathrm{FV}(\mathcal{F}) = \varnothing$, so heißt $\mathcal{F}$ eine **geschlossene Formel**.

Definition 1.3.12 (Allabschluss)**.** Ist B eine Formel mit $\mathrm{FV}(B) = \{a_1, \ldots, a_n\}$, dann ist $B = F(a_1, \ldots, a_n)$. Jede Formel der Art

$$\forall_{x_1} \forall_{x_2} \ldots \forall_{x_n} F(x_1, \ldots, x_n)$$

heißt dann ein **Allabschluss** von B.

Beispiel 1.3.13. Ist B die Formel $a = b$, so sind die Formeln $\forall_x \forall_y\, x = y$ und $\forall_x \forall_y\, y = x$ zwei Allabschlüsse von B.

* * *

1.4 Der Begriff der Theorie

Definition 1.4.1. Eine **Theorie** (der ersten Stufe) ist ein Paar $T = \big(L(T), \mathrm{Ax}(T)\big)$, bestehend aus einer Sprache $L(T)$ und einer Menge von Formeln $\mathrm{Ax}(T)$. Die Elemente von $\mathrm{Ax}(T)$ heissen die **Axiome** der Theorie T.

Beispiel 1.4.2. (Gruppentheorie) Die nicht-logischen Zeichen der Gruppentheorie sind:

- ein 0-stelliges Funktionszeichen, also eine Konstante e,
- ein 1-stelliges Funktionszeichen i und
- ein 2-stelliges Funktionszeichen m.

Wir schreiben t^{-1} für it und $(s \cdot t)$ für mst und lassen äußere Klammern fort. Die Axiome der Gruppentheorie sind dann

G1: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

G2: $a \cdot e = a$,

G3: $a \cdot a^{-1} = e$.

Diese stehen abkürzend für

G1: $= mmabcmambc$,

G2: $= maea$,

G3: $= maiae$.

Der Nutzen der Abkürzungen dürfte damit klar sein.

Beispiel 1.4.3. (Ringe mit Eins) Die nicht-logischen Grundzeichen der Theorie T_R der Ringe mit Eins sind:

- die Konstanten 0 und 1,
- ein 1-stelliges Funktionszeichen $-$,
- zwei 2-stellige Funktionszeichen $+$ und $\cdot$.

Die Axiome von T_R sind

R1 $(a + b) + c = a + (b + c)$,

R2 $a + b = b + a$,

R3 $a + 0 = a$,

R4 $a + (-a) = 0$,

R5 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

R6 $a \cdot 1 = a \ \wedge \ 1 \cdot a = a$,

R7 $a \cdot (b + c) = a \cdot b + a \cdot c$,

R8 $(a + b) \cdot c = a \cdot c + b \cdot c$.

Streng genommen müssen wir die rechten Seiten von R7 und R8 klammern: $(a \cdot b) + (a \cdot c)$, wir benutzen aber die Konvention, dass $\cdot$ stärker bindet als $+$ (Punktrechnung geht vor Strichrechnung). In der logischen Schreibweise ist das

$$+ \cdot ab \cdot ac.$$

Erweitern wir T_R um das Axiom

R9 $a \cdot b = b \cdot a$,

so erhalten wir die Theorie der kommutativen Ringe mit Eins.

Beispiel 1.4.4. (Zahlentheorie Z) Die nichtlogischen Grundzeichen von Z sind

- die Konstanten 0, 1,
- zwei zweistellige Funktionszeichen + und ·,
- ein zweistelliges Praedikatszeichen <.

Die Axiome von Z sind

$$\begin{aligned} \neg\, a+1=0 \qquad & \qquad a+1=b+1 \to a=b, \\ a+0=a \qquad & \qquad a+(b+1)=(a+b)+1 \\ a\cdot 0=0 \qquad & \qquad a\cdot(b+1)=a\cdot b+a \end{aligned}$$

sowie

$$\begin{gathered} (a<b)\ \vee\ (a=b)\ \vee\ (b<a) \\ \neg\,(a<a) \\ a<(b+1)\leftrightarrow\big((a<b)\vee(a=b)\big) \end{gathered}$$

und für jede Formel $F(a)$, in der x nicht auftritt und in der ausser a keine freie Variable auftritt, die Formel

$$F(0) \quad\to\quad \forall_x\big(F(x)\to F(x+1)\big) \quad\to\quad \forall_x F(x).$$

Man beachte, dass Z unendlich viele Axiome besitzt. Ferner fällt auf, dass zum Beispiel das Assoziativgesetz der Addition nicht verlangt wird. Dies kann man aber mit dem Induktionsschema herleiten, wie wir später sehen werden, wenn wir definiert haben, was eine Herleitung ist. Diese Version der Zahlentheorie ist als **erweiterte Peano-Arithmetik** bekannt.

Beispiel 1.4.5. (Theorie *LO* der linearen Ordnung) Einziges nichtlogisches Grundzeichen ist ein 2-stelliges Prädikatszeichen <. Wir schreiben $a<b$ statt $<ab$. Die Axiome von *LO* sind

$a<b\to b<c\to a<c$	(Transitivität)
$\neg\,(a<a)$	(Antireflexivität)
$(a<b)\quad\vee\quad(a=b)\quad\vee\quad(b<a)$	(Linearität)

Aus *LO* entsteht die Theorie *DLO* der **dichten linearen Ordnung**, indem man das folgende Axiom hinzufügt

$$a<b \quad\to\quad \exists_y(a<y\wedge y<b).$$

Definition 1.4.6. Eine Sprache L heißt **algebraisch**, wenn alle nichtlogischen Grundzeichen Funktionszeichen sind. Eine Sprache heißt **relational**, wenn alle nichtlogischen Grundzeichen Prädikate oder Konstanten sind.

Beispiele 1.4.7.
- Die Gruppentheorie T_G ist algebraisch, ebenso die Theorie T_R der Ringe mit Eins. Die Ordnungstheorien *LO* und *DLO* sind relational.

* * *

1.5 Strukturen, Interpretation und Modelle

Definition 1.5.1. Sei L eine Sprache. Eine **Struktur** $\mathcal{A}$ zu L ist ein Tripel $\mathcal{A} = (A, F, P)$ mit

(i) einer nichtleeren Menge $A = |\mathcal{A}|$, genannt die **Trägermenge** von $\mathcal{A}$.

(ii) einer Familie $F = (f_{\mathcal{A}})_{f \in L}$, die zu jedem n-stelligen Funktionszeichen f von L genau eine n-stellige Funktion auf A

$$f_{\mathcal{A}} : A^n \to A$$

enthält. Wir identifizieren 0-stellige Funktionen auf A mit ihrem einzigen Wert in A.

(iii) einer Familie $P = (p_{\mathcal{A}})_{p \in L}$, die zu jedem n-stelligen nicht-logischen Prädikatszeichen p von L genau eine Teilmenge $p_{\mathcal{A}} \subset A^n$ enthält.

Ist L eine algebraische/relationale Sprache, so nennt man $\mathcal{A}$ eine algebraische/relationale Struktur.

Gruppen, Ringe und Körper sind algebraische Strukturen, geordnete Mengen relationale.

Definition 1.5.2. Sei $\mathcal{A}$ eine Struktur zu L. Man erhält die Sprache $L(\mathcal{A})$ als Erweiterung von L, indem man zu jedem Element $a \in |\mathcal{A}|$ eine Konstante, den **Namen** von a hinzufügt. Den Namen von a bezeichnen wir wieder mit a. Dann wird $\mathcal{A}$ zu einer $L(\mathcal{A})$-Struktur erweitert, indem man dem Namen von a das Element a zuordnet.

Beispiel 1.5.3. Sei L die Sprache der Ringe mit Eins und $\mathbb{R}$ der Körper der reellen Zahlen. Dann enthält $L(\mathbb{R})$ einen Namen für jede Zahl.

Lemma 1.5.4. *(Interpretation) Sei $\mathcal{A}$ eine Struktur zur Sprache L. Dann gibt es genau eine Zuordnung, die jedem geschlossenen Term t von $L(\mathcal{A})$ ein Element $\mathcal{A}(t) \in |\mathcal{A}|$ und jeder Formel F von $L(\mathcal{A})$ einen Wahrheitswert $\mathcal{A}(F) \in \{w, f\}$ zuordnet, derart, dass gilt:*

(a) *Für jedes n-stellige Funktionszeichen f und geschlossene Terme $t_1, \ldots, t_n$ gilt*

$$\mathcal{A}(ft_1 \ldots t_n) = f_{\mathcal{A}}(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n)).$$

(b) *Fuer beliebige Formeln gilt*

(i) *Sind $a_1, \ldots, a_n$ alle freien Variablen der Formel $F = F(a_1, \ldots, a_n)$, dann ist*

$$\mathcal{A}(F) = w \quad \Leftrightarrow \quad \mathcal{A}(F(c_1, \ldots, c_n)) = w \quad \textit{für alle } c_1, \ldots, c_n \in |\mathcal{A}|.$$

(ii) *sind $t_1, \ldots, t_n$ geschlossene Terme und p ein Praedikatszeichen, so gilt*

$$\mathcal{A}(pt_1 \ldots t_n) = w \quad \Leftrightarrow \quad (\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n)) \in p_{\mathcal{A}},$$

(c) *Fuer alle geschlossenen Formeln $A, B, C, \forall_x F(x)$ gilt*

(i) $\mathcal{A}(\neg A) = w \quad \Leftrightarrow \quad \mathcal{A}(A) = f,$

(ii) $\mathcal{A}(B \to C) = w \quad \Leftrightarrow \quad$ *wenn* $\mathcal{A}(B) = w$ *dann* $\mathcal{A}(C) = w,$

(iii) $\mathcal{A}(\forall_x F(x)) = w \quad \Leftrightarrow \quad \mathcal{A}(F(c)) = w$ *für alle* $c \in |\mathcal{A}|.$

Diese Zuordnung wird die **Interpretation** *der Sprache $L(\mathcal{A})$ in der Struktur $\mathcal{A}$ genannt.*

Beweis. Existenz: Man definiert die Zuordnung $\mathcal{A}$ induktiv, indem man genau die geforderten Eigenschaften zur Definition benutzt. Man definiert also $\mathcal{A}(ft_1 \ldots t_n) := f_{\mathcal{A}}(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n))$ und so weiter. Die Eindeutigkeit des Aufbaus fuehrt dazu, dass kein Wohldefiniertheitsproblem entsteht.

Eindeutigkeit: Sei $\mathcal{A}'$ eine zweite solche Zuordnung. Fuer $c \in |\mathcal{A}|$ gilt dann $\mathcal{A}(c) = c = \mathcal{A}'(c)$. Sind $t_1, \ldots, t_n$ geschlossene Terme, fuer die $\mathcal{A}(t_j) = \mathcal{A}'(t_j)$, $j = 1, \ldots, n$ gilt, dann ist

$$\mathcal{A}(ft_1 \ldots t_n) = f_{\mathcal{A}}(\mathcal{A}(t_1), \ldots, \mathcal{A}(t_n)) = \mathcal{A}'(ft_1 \ldots t_n).$$

Induktiv folgt hieraus, dass $\mathcal{A}(t) = \mathcal{A}'(t)$ fuer jeden geschlossenen Term t. Fuer Formeln geht man ebenso vor. □

Bemerkung 1.5.5. Man beachte, dass für eine Formel F genau dann $\mathcal{A}(F) = w$ gilt, wenn dies für ihren Allabschluss richtig ist.

Bemerkung 1.5.6. Man beachte ferner, dass

$$\mathcal{A}(B \vee C) = w \quad \Leftrightarrow \quad \mathcal{A}(B) = w \text{ oder } \mathcal{A}(C) = w$$

fuer nicht geschlossene Formeln falsch ist, wie das Beispiel

$$B \equiv a = b$$
$$C \equiv a \neq b$$

fuer eine Struktur mit mindestens zwei Elementen zeigt.

Lemma 1.5.7. *Sei $\forall_x F(x)$ eine Formel aus $L(\mathcal{A})$. Dann gilt*

(a) $\mathcal{A}(\exists_x F(x)) = w \quad \Leftrightarrow \quad \mathcal{A}(F(c)) = w$ *für mindestens ein* $c \in |\mathcal{A}|$.

(b) $\mathcal{A}\left(\forall_x \forall_y (F(x) \to F(y) \to x = y)\right) = w$
$\Leftrightarrow \quad \mathcal{A}(F(c)) = w$ *für höchstens ein* $c \in |\mathcal{A}|$.

Beweis. (a) $\exists_x F(x)$ ist $\neg \forall_x \neg F(x)$. Also folgt aus der Definition der Interpretation

$$\begin{aligned}\mathcal{A}(\neg \forall_x \neg F(x)) = w \Leftrightarrow\ & \mathcal{A}(\forall_x \neg F(x)) = f \\ \Leftrightarrow\ & \mathcal{A}(\neg F(c)) = w \text{ gilt nicht für alle } c \in |\mathcal{A}| \\ \Leftrightarrow\ & \mathcal{A}(\neg F(c)) = f \text{ gilt für mindestens ein } c \in |\mathcal{A}| \\ \Leftrightarrow\ & \mathcal{A}(F(c)) = w \text{ gilt für mindestens ein } c \in |\mathcal{A}|.\end{aligned}$$

(b)

$$\begin{aligned}&\mathcal{A}(\forall_x \forall_y (F(x) \to F(y) \to x = y)) = w \\ &\Leftrightarrow \text{ für alle } c, d \in |\mathcal{A}| \text{ folgt } c = d \text{ aus } \mathcal{A}(F(c)) = \mathcal{A}(F(d)) = w \\ &\Leftrightarrow \text{ es gibt höchstens ein } c \in |\mathcal{A}| \text{ mit } \mathcal{A}(F(c)) = w.\end{aligned}$$

□

Interessanterweise ist also *Es gibt (mindestens) ein...* eine Existenzaussage, wohingegen *Es gibt höchstens ein...* eine Allaussage ist.

Definition 1.5.8. (Modell) Sei T eine Theorie zur Sprache L.

(a) Sei $\mathcal{A}$ eine Struktur zu L. Eine Formel B **gilt** in $\mathcal{A}$ oder ist **$\mathcal{A}$-gültig**, falls $\mathcal{A}(B) = w$. In diesem Fall schreiben wir

$$\mathcal{A} \vDash B$$

und lesen dies als "in $\mathcal{A}$ gilt B".

(b) Eine Struktur $\mathcal{A}$ ist ein **Modell** von T, wenn jedes Axiom von T in $\mathcal{A}$ gilt.

(c) Eine Formel B **gilt in** der Theorie T, wenn B in jedem Modell gilt. Wir schreiben dann

$$T \vDash B.$$

Beispiele 1.5.9.
- Die Modelle der Gruppentheorie sind genau die Gruppen, die Modelle der Ringtheorie sind genau die Ringe.
- Die Menge der natürlichen Zahlen mit Null: $\mathbb{N}_0$ ist ein Modell der Zahlentheorie. Dies ist das **Standardmodell** der Zahlentheorie. Es gibt aber noch weitere Modelle, wie wir später sehen werden.

Definition 1.5.10. Sei $\mathcal{A}$ eine Struktur zur Sprache L. Die Theorie $T(\mathcal{A}) = T_L(\mathcal{A})$ von $\mathcal{A}$ ist die Theorie zur Sprache L, deren Axiome genau alle in $\mathcal{A}$ wahren Formeln sind:

$$\mathrm{Ax}(T(\mathcal{A})) = \Big\{C : C \text{ ist eine Formel aus } L \text{ mit } \mathcal{A}(C) = w\Big\}.$$

Lemma 1.5.11. *Sei $\mathcal{A}$ eine Struktur zur Sprache L.*

(a) *$\mathcal{A}$ ist ein Modell von $T(\mathcal{A})$.*

(b) *Für jede Formel C aus L gilt*

$$\begin{aligned} \mathcal{A} \vDash C &\Leftrightarrow C \in \mathrm{Ax}(T(\mathcal{A})) \\ &\Leftrightarrow T(\mathcal{A}) \vDash C. \end{aligned}$$

Beweis. (a) Die Axiome von $T(\mathcal{A})$ gelten nach Definition in $\mathcal{A}$.

(b) Die erste Äquivalenz ist die Definition von $\mathrm{Ax}(T(\mathcal{A}))$. Zur zweiten: Ist C ein Axiom von $T(\mathcal{A})$, dann gilt C in jedem Modell, also folgt $T(\mathcal{A}) \vDash C$, d.h., C gilt in $T(\mathcal{A})$. Umgekehrt: gilt C in $T(\mathcal{A})$, dann gilt C in jedem Modell, also insbesondere gilt C in $\mathcal{A}$ und damit liegt C nach Definition in $\mathrm{Ax}(T(\mathcal{A}))$. □

Bemerkung 1.5.12. (Sprachabhängigkeit der Theorie $T(\mathcal{A})$)
Man beachte, dass $T(\mathcal{A}) = T_L(\mathcal{A})$ essentiell von der Sprache L abhängt und sich zum Beispiel von $T_{L(\mathcal{A})}(\mathcal{A})$ unterscheidet. Wir machen das an einem Beispiel klar. Sei L die logische Sprache, also ohne alle nichtlogischen Grundzeichen. Jede Menge A definiert dann eine L-Struktur. Sei $\mathcal{A}$ eine L-Struktur mit überabzählbarer Trägermenge $A = |\mathcal{A}|$. Da wir nur das Prädikat $=$ haben und keine Funktionszeichen, können wir in L nicht so viele interessante Formeln hinschreiben und man macht sich klar, dass eine Formel in dieser Sprache, die in A gilt, in jeder unendlichen Menge gilt. Wir brauchen eine

unendliche Menge, weil wir ja zum Beispiel für jedes n die Formel

$$\forall_{x_1} \ \ldots \ \forall_{x_n} \exists_y \ (y \neq x_1 \wedge \cdots \wedge y \neq x_n)$$

haben, die sichert, dass jedes Modell von $T_L(\mathcal{A})$ unendlich ist. Da wir aber mit unseren Formeln immer nur endliche Sachverhalte ausdrücken können, ist es auch so, dass jede abzählbar unendliche Menge ein Modell für $T_L(\mathcal{A})$ ist.

Betrachten wir dieselbe Situation in der Sprache $L(\mathcal{A})$, so sieht die Sache anders aus: Wir haben einen Namen $\underline{a}$ für jedes $a \in A$ und die unendlich vielen Formeln

$$\underline{a} \neq \underline{b}$$

für $a \neq b$ in A gelten in $\mathcal{A}$. Also gelten sie in jedem Modell von $T_{L(\mathcal{A})}(\mathcal{A})$, woraus folgt, dass jedes Modell dieser Theorie eine Kardinalität $\geq |A|$ haben muss.

* * *

1.6 Herleitungen

Definition 1.6.1. Sei $F(A_1, \ldots, A_n)$ eine aussagenlogische Tautologie, die ausser den Aussagenvariablen $A_1, \ldots, A_n$ nur noch die logischen Junktoren $\vee$ und $\neg$ enthält. Sind dann $Q_1, \ldots, Q_n$ Formeln in der Sprache L, dann nennen wir

$$F(Q_1, \ldots, Q_n)$$

eine **Tautologie** in der Sprache L.

Definition 1.6.2. Die **Logischen Axiome** sind

1. alle Tautologien A der Sprache L, (Tautologien)
2. alle Formeln
$$\forall_x F(x) \to F(t),$$
wobei t ein Term ist, (Ersetzungsregel)
3. alle Formeln
$$(\forall_x (A \to B)) \to (\forall_x A) \to (\forall_x B),$$
(∀-Verteilung)
4. falls x nicht in $F(a)$ auftritt,
$$F(a) \to \forall_x F(x)$$

für jede freie Variable a, (Verallgemeinerung)

5. alle Formeln $t = t$ für Terme t, (Gleichheit)
6. alle Formeln
$$s = t \to A \to A',$$
wenn A' aus A entsteht, indem man an einigen Stellen s durch t ersetzt. Hierbei sind s und t Terme. (Termersetzung)

Wir schreiben
$$\mathrm{Ax(Log)}$$
für die Menge der logischen Axiome.

Bemerkung 1.6.3. Die logischen Axiome gelten in allen Strukturen zur Sprache L.

Definition 1.6.4. (Modus Ponens) Wir sagen, eine Formel B entsteht durch **Modus Ponens** aus einer Formelmenge Δ, wenn Δ die Formeln $A \to B$ und A enthält. Wir schreiben dies als
$$(A \to B, A) \vdash B.$$

Definition 1.6.5. (Herleitung) Sei Δ eine Menge von Formeln und sei F eine Formel. Eine **Herleitung** von F aus Δ ist eine Folge $(F_1, \ldots, F_n)$ von Formeln, so dass $F_n = F$ gilt und für jedes $j = 1, \ldots, n$ die Formel F_j durch Modus Ponens aus den logischen Axiomen und $(\Delta, F_1, \ldots, F_{j-1})$ entsteht.

Wir sagen, F ist aus Δ **herleitbar**, falls eine Herleitung aus Δ existiert. Wir schreiben dafür auch
$$\Delta \vdash F.$$

Lemma 1.6.6. (a) *Ist $A \in \Delta$, dann gilt $\Delta \vdash A$.*

(b) *Gilt $\Delta \vdash F$, so gibt es eine endliche Teilmenge $\Delta' \subset \Delta$, so dass $\Delta' \vdash F$.*

Beweis. (a) Sei $A \in \Delta$. Die Tautologie $A \to A$ ist herleitbar und daher ist nach dem Modus Ponens $\Delta \vdash A$.

(b) Da eine Herleitung nur endlich viele Modus Ponens Schritte hat, werden in ihr auch nur endlich viele Formeln aus Δ benötigt. □

Definition 1.6.7. Ist T eine Theorie und F eine Formel in der Sprache von T, so schreiben wir
$$T \vdash F,$$
falls $\mathrm{Ax}(T) \vdash F$, also falls die Formel F aus den Axiomen von T herleitbar ist.

Satz 1.6.8 (Korrektheitssatz)**.** *Ist eine Formel herleitbar, dann gilt sie in jedem Modell, also*

$$T \vdash F \quad \Rightarrow \quad T \models F.$$

Beweis. Sei F eine herleitbare Formel und sei $(F_1, \ldots, F_n)$ eine Herleitung. Wir beweisen den Satz durch Herleitungsinduktion, also Induktion nach n. Ist $n = 1$, so entsteht F durch Modus Ponens aus logischen Axiomen oder Axiomen von T, also etwa $(A, A \to F) \vdash F$. Da A und $A \to F$ dann in allen Modellen gelten, gilt auch F in allen Modellen. Im Induktionsschluss schliesst man ebenso, nur dass dann die Gültigkeit von A und $A \to F$ aus der Induktionsvoraussetzung gefolgert wird. □

Definition 1.6.9. Eine Theorie T heißt **widersprüchlich** oder **inkonsistent**, falls es eine Formel F gibt, so dass in T sowohl F als auch $\neg F$ herleitbar sind.

Eine Theorie heißt **konsistent**, wenn sie nicht widersprüchlich ist.

Korollar 1.6.10. *Hat eine Theorie T ein Modell, so ist sie konsistent.*

Beweis. Sei $\mathcal{A}$ ein Modell. Wäre T inkonsistent, so gäbe es eine Formel F, so dass F und $\neg F$ beide herleitbar wären. Dann gölten aber auch beide in $\mathcal{A}$, was nach dem Korrektheitssatz dazu führt, dass $\mathcal{A}(F)$ gleichzeitig w und f ist, was nicht sein kann. □

* * *

1.7 Der Vollständigkeitssatz

Lemma 1.7.1 (Deduktionslemma)**.** *Gilt $(\Delta, A) \vdash B$, so gilt auch $\Delta \vdash A \to B$.*

Beweis. Wir setzen der Einfachheit voraus, dass Δ alle logischen Axiome enthält. Ist B schon in Δ herleitbar, dann folgt aus der Tautologie $B \to A \to B$, dass $\Delta \vdash A \to B$. Wir können also annehmen, dass B nicht aus Δ herleitbar ist.

Wir zeigen durch Induktion über Herleitungsslänge, dass $A \to B$ herleitbar ist. Sei $(F_1, \ldots, F_n = B)$ eine Herleitung kuerzester Laenge von B aus (Δ, A). Sei der letzte Schluss von $(\Delta, A) \vdash B$ der Modus Ponens $(C, C \to B) \vdash B$.

Induktionsanfang: Ist $n = 1$, dann liegen die Formeln $C, C \to B$ beide in (Δ, A) und, da Δ nicht B herleitet, muss A gleich C oder $C \to B$ sein. Ist $A \equiv C$, dann ist $A \to B$ in Δ und

damit nach Induktion aus Δ herleitbar und wir sind fertig. Ist andererseits $A \equiv (C \to B)$, dann ist $A \to B$ dasselbe wie $(C \to B) \to B$. Die Formel C muss dann in Δ liegen, ist also aus Δ herleitbar. Nun ist

$$C \to (C \to B) \to B$$

eine Tautologie (Beispiel 1.2.6) und damit aus Δ herleitbar, so dass nach einem Modus Ponens die Formel $(C \to B) \to B$ aus Δ herleitbar ist.

Induktionsschluss $(n-1) \to n$ *mit* $n \geq 2$*:* In diesem Fall sind C und $C \to B$ jeweils in $n-1$ Schritten aus (Δ, A) herleitbar, nach Induktionsvoraussetzung folgt dann also

$$\begin{aligned} \Delta &\vdash A \to C, \\ \Delta &\vdash A \to C \to B. \end{aligned}$$

Mit der Tautologie

$$(A \to C) \to (A \to C \to B) \to (A \to B)$$

folgt in zwei Modus Ponens-Schritten, dass $\Delta \vdash A \to B$. □

Lemma 1.7.2 (Reductio ad absurdum)**.** *Ist* $\Delta \cup \{A\}$ *nicht konsistent, dann folgt* $\Delta \vdash \neg A$*.*

Beweis. Nach Definition gibt es eine Formel B, so dass in (Δ, A) sowohl B als auch $\neg B$ herleitbar ist. Nach dem Deduktionslemma folgt, dass in Δ sowohl $A \to B$ als auch $A \to \neg B$ herleitbar ist. Nun ist aber

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

eine Tautologie! Also folgt $\Delta \vdash \neg A$. □

Satz 1.7.3 (Vollständigkeitssatz)**.** (a) *Ist eine Theorie T konsistent, dann hat sie ein Modell.*

(b) *Gilt eine Formel F in allen Modellen von T, dann ist sie auch herleitbar. Zusammen mit dem Korrektheitssatz gilt also*

$$T \models F \quad \Leftrightarrow \quad T \vdash F$$

Korollar 1.7.4 (Ex falso quodlibet)**.** *Ist eine Theorie inkonsistent, so kann man jede Formel in ihr herleiten.*

Beweis des Korollars. Ist T inkonsistent, dann hat sie nach Korollar 1.6.10 kein Modell. Ist F irgendeine Formel in der Sprache von T, dann gilt F in allen Modellen von T (denn es gibt ja keine). Damit ist F nach dem Satz herleitbar. □

Beweis (a)⇒(b). Zum Beweis des Vollständigkeitssatzes stellen wie als erstes fest, dass es reicht, Teil (a) zu zeigen. Sei dazu F eine Formel, die in allen Modellen von T gilt. **Nimm nun an**, dass $(T, \neg F)$ konsistent ist. Dann hat sie nach Teil (a) auch ein Modell. Dies ist dann aber ein Modell von T in dem $\neg F$ gilt, also F nicht gilt, was ein **Widerspruch** ist!

Wir folgern also, dass $(T, \neg F)$ nicht konsistent ist. Nach der Reductio ad absurdum folgt, dass $T \vdash \neg\neg F$. Nun ist $\neg\neg F \to F$ eine Tautologie, also beweist T die Formel F. □

Wir finalisieren den Beweis des Vollstaendigkeitssatzes im naechsten und uebernaechsten Abschnitt.

* * *

1.8 Maximalkonsistente Mengen

Definition 1.8.1. Eine Formelmenge Σ zu einer Sprache L heißt **maximalkonsistent**, wenn sie maximal ist in der Menge aller konsistenten Formelmengen zu L.

Lemma 1.8.2. (a) *Eine konsistente Formelmenge Σ ist genau dann maximalkonsistent, wenn für jede Formel F in der Sprache L gilt*

$$F \in \Sigma \quad \textit{oder} \quad \neg F \in \Sigma.$$

(b) *Zu jeder konsistenten Formelmenge Δ einer Sprache L gibt es eine* **maximalkonsistente** *Formelmenge Σ, die Δ enthält.*

Beweis. (a) Sei Σ maximalkonsistent und F eine Formel der Sprache L. Da Σ maximal ist, folgt: $F \in \Sigma$ oder (Σ, F) ist nicht konsistent. Im zweiten Fall folgt nach dem letzten Lemma, dass $\Sigma \vdash \neg F$ und damit ist $(\Sigma, \neg F)$ konsistent, so dass wieder aus der Maximalität $\neg F \in \Sigma$ folgt.

Umgekehrt gelte F oder $\neg F$ liegt in Σ fuer jede Formel F. **Angenommen**, Σ ist nicht maximalkonsistent, dann gibt es ein $F \notin \Sigma$, so dass (Σ, F) konsistent ist. Da aber $F \notin \Sigma$,

folgt also $\neg F \in \Sigma$, also sind sowohl F als auch $\neg F$ herleitbar, damit ist Σ inkonsistent, **Widerspruch!**

(b) Sei S die Menge aller konsistenten Formelmengen $\Sigma \supset \Delta$. Wir wollen das Lemma von Zorn auf S anwenden. Ist $L \subset S$ eine linear geordnete Teilmenge, dann behaupten wir, dass $M = \bigcup_{\Sigma \in L} \Sigma$ immer noch konsistent ist. **Angenommen**, M ist nicht konsistent, es gibt also eine Formel A mit $M \vdash A$ und $M \vdash \neg A$. Nach Lemma 1.6.6 gibt es eine endliche Teilmenge M' von M so dass $M' \vdash A$ und $M' \vdash \neg A$. Da L linear geordnet, gibt es ein $\Sigma \in K$ so dass $\Sigma \supset M'$, damit ist Σ aber inkonsistent, im **Widerspruch** zur Annahme.
Es folgt also, dass M konsistent ist, damit erfüllt S die Kettenbedingung, hat also nach Zorns Lemma ein maximales Element Σ. □

Lemma 1.8.3 (Verallgemeinerung)**.** *Es gelte $\Delta \vdash F(c)$, wobei c ein Konstantensymbol ist, das in keiner Formel von Δ auftritt, dann gibt es eine gebundene Variable x, die nicht in $F(c)$ auftritt, so dass $\Delta \vdash \forall_x F(x)$ gilt. Ferner gibt es eine Herleitung für $\forall_x F(x)$, in der c nicht auftritt.*

Beweis. Induktion über die Herleitung von $F(c)$. Sei a eine freie Variable, die in $F(c)$ nicht auftritt. Ist $F(c)$ ein logisches Axiom, dann ist auch $F(a)$ eines und damit ohne c herleitbar. Das logische Axiom Nummer 4 besagt $F(a) \to \forall_x F(x)$ und damit ist mit Modus Ponens auch $\forall_x F(x)$ ohne c herleitbar.

Der Fall $F(c) \in \Delta$ tritt nicht auf, da keine der Formeln in Δ die Konstante c enthaelt.

Induktionsschritt: Sei $(A(c), A(c) \to F(c)) \vdash F(c)$ der letzte Schritt der Herleitung. Nach Induktionsvoraussetzung sind in Δ auch die Formeln $\forall_x A(x)$ und $\forall_x (A(x) \to F(x))$ ohne c herleitbar. Nach der $\forall$-Verteilung ist dann auch $\forall_x A(x) \to \forall_x F(x)$ ohne c herleitbar und mit dem Modus Ponens folgt $\Delta \vdash \forall_x F(x)$ mit einer c-freien Herleitung. □

* * *

1.9 Das spezielle Modell

Definition 1.9.1. Eine Sprache L_* heisst **Konstantenerweiterung** von L, falls L_* durch Hinzunahme neuer Konstantensymbole aus L entsteht.

Eine Formelmenge Σ heisst **Henkin-Menge**, falls für jede Formel $F(a)$ gibt es eine Konstante c, so dass die Formel $\neg \forall_x F(x) \to \neg F(c)$ ein Element von Σ ist mit einer Variablen x, die nicht in $F(a)$ auftritt.

Satz 1.9.2. *Sei $T = (L, \Delta)$ eine konsistente Theorie. Dann gibt es eine Konstantenerweiterung L_* von L und eine Formelmenge $\Sigma \supset \Delta$ zur Sprache L_*, so dass*

(a) *Σ ist maximalkonsistent und*

(b) *Σ ist Henkin-Menge.*

Beweis. Wir konstruieren Σ wie folgt. Für jede freie Variable a, jede Formel $F(a)$ der Sprache L_0 und jede gebundene Variable x, die nicht in $F(a)$ auftritt, wählen wir ein neues Konstantensymbol $c_{a,F,x}$ und erhalten so eine Sprache L_1. Dann erweitern wir Δ für jedes (a, F, x) um die Formel $\neg \forall_x F(x) \to \neg F(c_{a,F,x})$ und erhalten so die Formelmenge Δ_1.

Lemma 1.9.3. *Δ_1 ist konsistent.*

Beweis. **Angenommen**, Δ_1 ist widersprüchlich. Da Δ konsistent ist, gibt es eine minimale Teilmenge $\{\psi_1, \ldots, \psi_n, \psi\}$ von neuen Formeln, deren Vereinigung mit Δ widersprüchlich ist, also etwa $\Delta \cup \{\psi_1, \ldots, \psi_n\} \vdash \neg \psi$. Die Formel ψ ist von der Form $\neg \forall_x F(x) \to \neg F(c)$ mit $c = c_{a,F,x}$. Wegen der Tautologie

$$\neg \big(A \to \neg B\big) \leftrightarrow \big(A \wedge B\big)$$

ist $\neg \psi$ äquivalent zu $\neg \forall_x F(x) \wedge F(c)$. Wir haben daher $(\Delta, \psi_1, \ldots, \psi_n) \vdash \neg \forall_x F(x)$ und $(\Delta, \psi_1, \ldots, \psi_n) \vdash F(c)$. Das letztere liefert nach Lemma 1.8.3 schon $(\Delta, \psi_1, \ldots, \psi_n) \vdash \forall_x F(x)$, so dass $(\Delta, \psi_1, \ldots, \psi_n)$ schon widersprüchlich ist, was der Minimalität **widerspricht.** □

Jetzt wiederholen wir den Prozess mit der Sprache L_1 und erhalten die Sprache L_2, erweitern auch Δ_1 zu Δ_2, welches dann ebenfalls konsistent ist. Wir iterieren den Prozess und erhalten eine Kette von Sprachen $L_0 \subset L_1 \subset \ldots$ und von Formelmengen $\Delta_0 \subset \Delta_1 \subset \ldots$. Schliesslich sei $L_* = \bigcup_n L_n$ und $\Delta_* = \bigcup_n \Delta_n$. Da Δ_* eine aufsteigende Vereinigung von konsistenten Formelmengen ist, ist Δ_* selbst konsistent. Ferner ist Δ_* eine Henkin-Menge. Sei nun Σ eine maximalkonsistente Erweiterung von Δ_*, dann ist auch Σ eine Henkin-Menge, da Erweiterungen von Henkin-Mengen bei der gleichen Sprache stets Henkin-Mengen bleiben. □

Wir konstruieren nun ein Modell $\mathcal{A}$ für die Theorie (L_*, Σ). Zunächst brauchen wir eine Trägermenge $|\mathcal{A}|$. Sei hierzu G die Menge aller geschlossenen Terme von L_*. Auf der Menge G definieren wir eine Äquivalenzrelation durch

$$s \sim t \quad \Leftrightarrow \quad \text{die Formel } s = t \text{ ist in } \Sigma.$$

Beweis (dass dies eine Äquivalenzrelation ist). Zunächst gilt immer $t \sim t$ nach dem logischen Axiom Nummer 5. Es gelte $s \sim t$, nach dem logischen Axiom 6 ist die Formel $s = t \to s = t \to t = s$ herleitbar, woraus man durch zweimaligen Modus Ponens $\Sigma \vdash t = s$ erhält. Da Σ maximalkonsistent ist, liegt $t = s$ in Σ, also $t \sim s$.

Zum Schluss seien $s \sim t$ und $t \sim w$. Wieder aus dem logischen Axiom 6 folgt, dass

$$t = s \to t = w \to s = w$$

herleitbar ist, woraus man wie oben folgert, dass $s \sim w$ gilt. □

Wir definieren die Trägermenge $|\mathcal{A}|$ als die Menge aller Äquivalenzklassen, also

$$|\mathcal{A}| := G/\sim .$$

Nun sei

(a) Für jedes n-stellige Prädikatssymbol p

$$p_{\mathcal{A}} := \Big\{([t_1], \dots, [t_n]) : pt_1 \dots t_n \in \Sigma\Big\}.$$

(b) Für jedes n-stellige Funktionssymbol f

$$f_{\mathcal{A}}([t_1], \dots, [t_n]) = [ft_1 \dots t_n].$$

Die Wohldefiniertheit dieser Prädikate und Funktionen überprüft man wie oben durch Anwendung der logischen Axiome Nummer 6.

Lemma 1.9.4. *$\mathcal{A}$ ist ein Modell zur Theorie (L_*, Σ) und damit auch von T. Man nennt es ein* **spezielles Modell** *von T. Es ist als Modell von T nicht eindeutig festgelegt, da die Formelmenge Σ als eine maximalkonsistente Erweiterung von Δ_* nicht eindeutig bestimmt ist.*

Beweis. Sei $F(a_1, \dots, a_n)$ eine Formel in Σ, die keine anderen freien Variablen als $a_1, \dots, a_n$ enthält. Für jedes Tupel $(c_1, \dots, c_n) \in |\mathcal{A}|^n$ ist dann

$$F(a_1, \dots, a_n) \to F(c_1, \dots, c_n)$$

herleitbar und damit ist $F(c_1, \ldots, c_n)$ herleitbar und liegt wegen Maximalität in Σ.

Gesetzt, wir haben gezeigt, dass jedes solche $F(c_1, \ldots, c_n)$ in $\mathcal{A}$ gilt, dann gilt definitionsgemäß auch $F(a_1, \ldots, a_n)$ in $\mathcal{A}$. Wir können uns also auf den Fall geschlossener Formeln einschränken.

Wir beweisen also $(\Sigma \vdash F) \Rightarrow (\mathcal{A} \vDash F)$ für geschlossenes F durch Induktion nach Formelaufbau. Ist F eine Primformel, also etwa $F \equiv pt_1 \ldots t_n$, dann gilt $(t_{1,\mathcal{A}}, \ldots, t_{n,\mathcal{A}}) \in p_{\mathcal{A}}$ nach Definition von $p_{\mathcal{A}}$.

Ist im nächsten Schritt sei $F \in \Sigma$ von der Form $B \to C$. Ist dann $B \in \Sigma$, so folgt nach Modus Ponens, dass $\Sigma \vdash C$ und wegen Maximalität auch $C \in \Sigma$. Nach Induktionsvoraussetzung folgt $\mathcal{A}(B) = w = \mathcal{A}(C)$ und damit $\mathcal{A}(B \to C) = w$. Ist andererseits $B \notin \Sigma$, dann folgt $\neg B \in \Sigma$ wegen der Maximalität und daher $\mathcal{A}(\neg B) = w$ also $\mathcal{A}(B) = f$ und damit $\mathcal{A}(B \to C) = w$.

Im naechsten Schritt sei F gleich $\neg B \in \Sigma$. Wir muessen zeigen, dass $\mathcal{A}(B) = f$ gilt. Wir fuehren eine Unterinduktion nach dem Aufbau von B.

(a) Ist $B \equiv pt_1 \ldots t_n$ und gilt $\mathcal{A}(B) = w$, so gilt $([t_1], \ldots, [t_n]) \in p_{\mathcal{A}}$. Nach der Definition von $p_{\mathcal{A}}$ bedeutet das aber gerade $B \equiv pt_1 ... t_n \in \Sigma$, was der Konsistenz von Σ **widerspricht.**

(b) Sei nun $B \equiv C \to D$, also $\Sigma \vdash \neg (C \to D)$. Nun sind

$$\neg (C \to D) \to C \quad \text{und} \quad \neg (C \to D) \to \neg D$$

Tautologien, also folgt $\Sigma \vdash C, \neg D$. Nach Induktionsvoraussetzung gilt $\mathcal{A}(C) = w = \mathcal{A}(\neg D)$ und daher, nach der Definition der Interpretation, dass $\mathcal{A}(C \to D) = f$.

(c) Sei $B \equiv \neg C$, also gilt $\Sigma \vdash \neg \neg C$ und da $\neg \neg C \to C$ eine Tautologie ist, folgt $\Sigma \vdash C$ und dann nach Induktionsvorausstezung $\mathcal{A}(C) = w$, also $\mathcal{A}(\neg C) = f$.

(d) Sei schliesslich $B \equiv \forall_x F(x)$. Da $\Sigma \vdash \neg \forall_x F(x)$ und Σ eine Henkin-Menge ist, gibt es eine Konstante c mit $\Sigma \vdash \neg \forall_x F(x) \to \neg F(c)$, also $\Sigma \vdash \neg F(c)$. Nach Induktionsvoraussetzung folgt $\mathcal{A} \vDash \neg F(c)$ und daher $\mathcal{A}(\forall_x F(x)) = f$.

Damit ist die Unterinduktion beendet.

Sei schliesslich F von der Form $\forall_x G(x)$, wobei x nicht in $G(a)$ auftritt für eine freie Variable a, die ihrerseits nicht in $G(x)$ auftritt. Sei $c \in |\mathcal{A}|$. Wir müssen zeigen, dass $\mathcal{A}(G(c)) = w$ ist. Nun gilt $\Sigma \vdash \forall_x G(x) \to G(c)$ und $\Sigma \vdash \forall_x G(x)$, so dass mit Modus

Ponens folgt $\Sigma \vdash G(c)$. Nach Induktionsvoraussetzung ist dann $\mathcal{A} \vDash G(c)$ und da c beliebig war, folgt $\mathcal{A} \vDash \forall_x G(x)$. Damit ist der Vollstaendigkeitssatz bewiesen. □

Definition 1.9.5. Für eine Sprache L sei $|L|$ die Kardinalität ihrer Symbolmenge.

Korollar 1.9.6. *Sei $T = (L, \Delta)$ eine konsistente Theorie. Dann gibt es stets ein Modell der Maechtigkeit $\leq |L|$.*

Beweis. Beei jedem Schritt $L = L_0 \subset L_1 \supset \dots$ bleibt die Kardinalität der Sprache unverändert, also gilt also $|L| = |L_0| = |L_1| = \dots = |L_*|$. Daher hat ein spezielles Modell stets eine Kardinalität $\leq |L|$. □

* * *

1.10 Folgerungen aus dem Vollständigkeitssatz

Definition 1.10.1. Sei (L, Δ) eine Theorie. Unter einer **Teiltheorie** verstehen wir eine Theorie (L, Δ'), wobei $\Delta' \subset \Delta$ ist. Wir verkleinern also nur die Axiomenmenge, nicht die Sprache. Das könnte man auch tun, liegt aber nicht im Bereich unserer Anwendungen.

Die Teiltheorie (L, Δ') heißt **endlich**, wenn Δ' endlich ist.

Satz 1.10.2 (Kompaktheitssatz)**.** *Hat jede endliche Teiltheorie von T ein Modell, dann hat auch T ein Modell.*

Beweis. Sei $T = (L, \Delta)$ eine Theorie so dass jede endliche Teiltheorie ein Modell hat. Dann ist jede endliche Teiltheorie konsistent. Wir behaupten, dass T selbst konsistent ist. Wäre dies nicht der Fall, so gäbe es eine Herleitung einer Formel F und ihrer Negation $\neg F$. Nach Lemma 1.6.6 gibt es dann eine endliche Teilmenge $\Delta' \subset \Delta$ mit $\Delta \vdash F, \neg F$, damit ist dann die endliche Teiltheorie (L, Δ') widersprüchlich, was oben gesagtem widerspricht!

Daher ist also T konsistent, hat nach dem Vollständigkeitssatz also ein Modell. □

Satz 1.10.3 (Loewenheim-Skolem)**.** *Hat eine Theorie $T = (L, \Delta)$ ein unendliches Modell hat, dann hat sie Modelle jeder beliebigen unendlichen Mächtigkeit $\kappa \geq |L|$.*

Beweis. Die Theorie T habe ein unendliches Modell und κ sei eine Kardinalität $\geq |L|$. Wir fügen zu L eine Familie $(e_i)_{i\in I}$ von Konstantensymbolen hinzu mit $|I| = \kappa$. Danach hat die erweiterte Sprache L die Kardinalität $|L| = \kappa$. Wir fügen nun zur Theorie die unendlich vielen Axiome $e_i \neq e_j$ für $i \neq j$ in I hinzu. Die so entstehende Theorie T^* hat eine Sprache der Kardinalität κ und hat nur Modelle der Kardinalität $\geq \kappa$. Falls sie überhaupt konsistent ist, hat sie also nach Korollar 1.9.6 ein Modell der Kardinalität κ. Wir muessen zeigen, dass jede endliche Teiltheorie T' von T^* ein Modell besitzt. Genauer zeigen wir, dass ein unendliches Modell $\mathcal{A}$ der urspruenglichen Theorie T bereits ein Modell von T' ist. Beachte hierzu, dass T' nur endlich viele der neuen Axiome $e_i \neq e_j$ enthalten kann. Sei also E die Menge aller Indizes $i \in I$, ie in einem dieser Axiome von T' vorkommen. Die Menge E ist endlich, also findet man im unendlichen Modell $\mathcal{A}$ auch paarweise verschiedene Interpretationen fuer die e_i mit $i \in E$. Die Axiome von T' gelten dann allesamt in diesem Modell, es ist also ein Modell von T'. Damit hat nach dem Kompaktheitssatz die Theorie T^* ein Modell, ist also konsistent, hat also ein spezielles Modell, dieses hat die Kardinalität κ. □

* * *

1.11 Kategorische und vollständige Theorien

Definition 1.11.1. Eine konsistente Theorie T heißt **vollständig**, falls für jede Formel F gilt

$$T \vdash F \quad \text{oder} \quad T \vdash \neg F.$$

Beispiel 1.11.2. Ist $\mathcal{A}$ eine L-Struktur und $T(\mathcal{A})$ die Theorie, deren Axiome alle in $\mathcal{A}$ wahren Formeln sind. Dann ist $T(\mathcal{A})$ vollständig.

Proposition 1.11.3. *Eine konsistente Theorie T ist genau dann vollständig, wenn jede Formel, die in einem gegebenen Modell gilt, in jedem Modell gilt.*

Beweis. Sei T vollständig und $\mathcal{A}$ ein Modell. Sei $\mathcal{B}$ ein weiteres Modell. Sei F eine Formel mit $\mathcal{A} \vDash F$. Da T vollständig ist, folgt $T \vdash F$ oder $T \vdash \neg F$ und da $\mathcal{A}$ ein Modell ist, folgt $T \vdash F$ und damit $\mathcal{B} \vDash F$.

Sei umgekehrt T eine konsistente Theorie mit der Eigenschaft, dass jede Formel, die in einem Modell $\mathcal{A}$ gilt, in jedem Modell gilt. Ist dann F eine Formel, dann gilt entweder F oder $\neg F$ in $\mathcal{A}$. Im ersten Fall gilt F in allen Modellen, ist damit also herleitbar, im zweiten Fall ist $\neg F$ herleitbar. Damit ist T vollstaendig. □

Definition 1.11.4. Sei T eine Theorie. Ein **Isomorphismus** zwischen zwei Modellen $\mathcal{A} = (|\mathcal{A}|, (f_{\mathcal{A}})_f, (p_{\mathcal{A}})_{\mathcal{A}})$ und $\mathcal{B} = (|\mathcal{B}|, (f_{\mathcal{B}})_f, (p_{\mathcal{B}})_{\mathcal{B}})$ eine Bijektion $\phi : |\mathcal{A}| \xrightarrow{\cong} |\mathcal{B}|$ so

dass fuer jedes n-stellige Funktionszeichen f und alle $a_1, \ldots, a_n \in \|CA|$ gilt

$$f_{\mathcal{B}}(\phi(a_1), \ldots, \phi(a_n)) = \phi(f_{\mathcal{A}}(a_1, \ldots, a_n)),$$

und dass fuer jedes n-stellige Praedikatszeichen p gilt

$$p_{\mathcal{A}}(a_1, \ldots, a_n) = w \quad \Leftrightarrow \quad p_{\mathcal{B}}(\phi(a_1), \ldots, \phi(a_n)) = w.$$

Definition 1.11.5. Eine konsistente Theorie T heißt **kategorisch**, falls alle Modelle von T isomorph sind.

Beispiele 1.11.6.

- Ist T kategorisch, dann hat sie nur endliche Modelle.

  Beweis. Hat sie ein unendliches, dann hat sie nach Loewenheim-Skolem Modelle verschiedener Kardinalitaeten, diese koennen nicht isomorph sein. □

- Sei G eine Gruppe und sei $T = T(G)$ die Erweiterung der Gruppentheorie um alle Formeln, die in G wahr sind. Dann gilt: $T(G)$ ist genau dann kategorisch, wenn die Gruppe G endlich ist.

  Beweis. Ist die G endlich, so laesst sich die Gruppenstruktur in Formeln festnageln. Die Umkehrung ist nach obigem klar. □

- Kategorische Theorien sind vollständig. Es gibt vollständige Theorien, die nicht kategorisch sind, z.B. die Theorie der algebraisch abgeschlossenen Körper der Charakteristik Null, siehe unten.

Definition 1.11.7. Sei κ eine Kardinalzahl. Eine Theorie T heißt **κ-kategorisch**, falls je zwei Modelle der Mächtigkeit κ isomorph sind.

Beispiele 1.11.8.

- Sei L die Sprache, die nur die logischen Grundzeichen und $=$ enthält. Sei T die Theorie, die nur die logischen Axiome enthält. Sie ist κ-kategorisch für jedes κ, denn je zwei Mengen der gleichen Kardinalität sind als Mengen isomorph.

- Sei p eine Primzahl. Die Gruppentheorie ist p-kategorisch.

Definition 1.11.9. Eine abelsche Gruppe A heißt **torsionsfrei**, falls $na = 0 \Rightarrow a = 0$ für jedes $a \in A$ und jedes $n \in \mathbb{N}$ gilt.

Eine abelsche Gruppe A heißt **divisibel**, falls es zu jedem $a \in A$ und jedem $n \in \mathbb{N}$ ein $b \in A$ gibt mit $nb = a$.

Proposition 1.11.10. *Die Theorie der torsionsfreien divisiblen abelschen Gruppen ist κ-kategorisch für jedes ueberabzaehlbare κ.*

Beweis. Eine torsionsfreie divisible abelsche Gruppe V ist dasselbe wie ein $\mathbb{Q}$-Vektorraum. Je zwei $\mathbb{Q}$-Vektorräume unendlicher Dimension haben genau dann dieselbe Kardinalität, wenn sie Hamel-Basen gleicher Mächtigkeit haben. In dem Fall sind sie isomorph. □

Satz 1.11.11. *Sei $p = 0$ oder eine Primzahl. Die Theorie der algebraisch abgeschlossenen Körper der Charakteristik p ist κ-kategorisch für jedes ueberabzaehlbare κ.*

Beweis. Seien K, L zwei algebraisch abgeschlossene Körper der Charakteristik p derselben Mächtigkeit. Wir müssen zeigen, dass sie isomorph sind. Ist $p = 0$, so enthalten beide den Primkörper $\mathbb{Q}$ und daher enthalten beide den algebraischen Abschluss $\overline{\mathbb{Q}}$. Ist $p > 0$, so enthalten beide die Primkörper $\mathbb{F}_p$ und damit den algebraischen Abschluss $\overline{\mathbb{F}}_p$. Sei dieser gemeinsame Unterkörper mit U bezeichnet. Da $|K| = |L|$, haben beide denselben Transzendenzgrad über U, es gibt also eine Menge S so dass die Körpererweiterungen $K/U(S)$ und $L/U(S)$ beide algebraisch sind, wobei $U(S)$ die freie Körpererweiterung von U in den Erzeugern S ist. Da K und L algebraisch abgeschlossen sind, sind beide isomorph zum algebraischen Abschluss $\overline{U(S)}$. □

Satz 1.11.12. *Sei T eine Theorie zur Sprache L. Ist die Theorie κ-kategorisch fuer ein $\kappa \geq |L|$ und hat sie ein Modell der Maechtigkeit κ, dann ist T vollständig.*

Beweis. **Nimm an**, T ist nicht vollständig. Sei dann F eine Formel so dass weder F noch $\neg F$ in T beweisbar ist. Sei $T_1 = T \cup \{F\}$ und $T_2 = T \cup \{\neg F\}$. Jede der beiden Theorien T_i hat ein unendliches Modell. Nach dem Satz von Loewenheim-Skolem gibt es zwei Strukturen $\mathcal{A}_1$, $\mathcal{A}_2$ der Mächtigkeit κ so dass $\mathcal{A}_j \vDash T_j$. Beide sind auch Modelle von T und da T κ-kategorisch ist, folgt $\mathcal{A}_1 \cong \mathcal{A}_2$, was im **Widerspruch** zu $\mathcal{A}_1 \vDash F$ und $\mathcal{A}_2 \vDash \neg F$ steht. □

Satz 1.11.13. *Sei $p = 0$ oder eine Primzahl. Die Theorie T_p der algebraisch abgeschlossnen Körper der Charakteristik p ist vollständig.*

Beweis. Sei κ eine ueberabzaehlbare Kardinalitaet. dann ist T_p nach Satz 1.11.11 κ-kategorisch und daher ist T_p nach Satz 1.11.12 vollstaendig. □

Korollar 1.11.14. *Alles, was in der Sprache der Körper ausdrückbar ist und in* $\mathbb{C}$ *gilt, gilt in allen algebraisch abgeschlossenen Körpern der Charakteristik Null.*

Dies ist in der Anwendung sehr nuetzlich, denn es erlaubt es, analytische Argumente im Beweis von algebraischen Aussagen zu verwenden.

* * *

2 Rekursionstheorie

2.1 Registermaschinen

Eine Registermaschine ist ein theoretisches Modell für eine Rechenmaschine. Sie eignet sich für unsere Zwecke besser als eine Modell-Programmiersprache, weil sich ihre Instruktionen sehr einfach kodieren (gödelisieren) lassen. Eine Registermacschine hat endlich viele Register $R_1, R_2, \ldots, R_N$ die jedes eine natürliche Zahl oder Null enthalten können.

Definition 2.1.1. Eine **Registermaschine** M ist eine endliche Folge $I_1, I_2, \ldots, I_s$ von Quadrupeln, den sogenannten **Instruktionen** der Gestalt

$$I_j = (j, i, b, l),$$

wobei

- j ist die Nummer der Instruktion, also $1 \leq j \leq s$,
- i ist die Nummer eines Registers, also $1 \leq i \leq N$,
- b ist $+$ oder $-$ oder eine Instruktionsnummer oder $s + 1$,
- l ist eine Instruktionsnummer (Folgeinstruktion) oder $s + 1$.

Die verschiedenen Instruktionen bedeuten:

(a) $(j, i, +, l)$ **Addierschritt:** addiere 1 zum Register R_i und führe dann Instruktion l aus, falls $l \leq s$. Die Maschine stoppt, falls $l = s + 1$.

(b) $(j, i, -, l)$ **Subtrahierschritt:** subtrahiere 1 vom Register R_i (falls möglich) und führe dann Instruktion l aus (bzw. stoppe, falls $l = s + 1$).

(c) (j, i, k, l): **Testschritt:** Teste, ob der Wert des Registers R_i gleich Null ist. Falls ja, springe zu Instruktion I_k, sonst zu Instruktion I_l. Beide, k und l können auch $s + 1$ sein, in welchem Fall die Maschine stoppt.

Beachte, dass die Anzahl der angesprochenen Register schon durch die Instruktionen festgelegt ist, ist also $M = (I_1, \ldots, I_s)$, dann ist

$$N = \max\{i : (j, i, b, l) \text{ ist eine Instruktion von } M\}.$$

In diesem Fall sagen wir auch, M ist eine N**-Registermaschine**.

Beispiel 2.1.2. Eine Registermaschine der Laenge 3, die den Inhalt des zweiten Registers zum ersten addiert:

$(1,2,4,2)$ teste Register 2, wenn Null stoppe, sonst Schritt 2
$(2,1,+,3)$ addiere 1 zum Register 1, weiter zu Schritt 3
$(3,2,-,1)$ subtrahiere 1 von Register 2, weiter zu Schritt 1

Beispiele 2.1.3.

- $(1,1,-,2)$ Subtrahiert 1 vom Register 1, soweit möglich und bleibt dann stehen.
- $(1,1,-,1)$ Löscht den Inhalt von Register 1, ändert dann nichts mehr, bleibt aber auch nicht stehen.
- $\begin{matrix}(1,1,-,2)\\(2,1,3,1)\end{matrix}$ Löscht Register 1 und stoppt dann.

Definition 2.1.4. Sei M eine N-Registermaschine der Länge s. Eine **Konfiguration** ist ein $N+1$-Tupel $(j,x_1,\ldots,x_N)$, wobei die $x_i \in \mathbb{N}_0$ die Registerinhalte sind und $1 \leq j \leq s+1$ ist eine Instruktionsnummer oder $s+1$.

Eine Konfiguration (l,y) ist eine **Folgekonfiguration** von (j,x), oder

$$(j,x) \quad \Rightarrow \quad (l,y),$$

falls

(a) $j \leq s$ und

- $I_j = (j,i,+,l)$ und $y = (x_1,\ldots,x_i+1,\ldots,x_N)$, oder
- $I_j = (j,i,-,l)$ und $y = (x_1,\ldots,x_i-1,\ldots,x_N)$, wobei das -1 so zu verstehen ist, dass Null rauskommt, wenn $x_i = 0$ war, oder
- $I_j = (j,i,k,l)$ und $x_i > 0$, sowie $y = x$ und k ist eine Instruktionsnummer, oder
- $I_j = (j,i,l,k)$ und $x_i = 0$, sowie $y = x$.

(b) oder $j = s+1$, in welchem Fall $(l,y) =) j,x)$ ist (Stopkonfiguration).

Jede Konfiguration hat genau eine Folgekonfiguration.

Definition 2.1.5. Eine **Rechnung** der Dauer T auf einer Registermaschine M der Länge s ist eine Folge

$$(j_1,x_1),\ldots,(j_T,x_T)$$

von Konfigurationen, wobei $j_1 = 1$ ist und jeweils (j_{r+1},x_{r+1}) die Folgekonfiguration von (j_r,x_r) ist. Hierbei heißt x_1 die **Eingabe** und $(1,x_1)$ die **Anfangskonfiguration**. Die

Rechnung heißt **abgeschlossen** oder **beendet**, falls $j_T = s + 1$. Ist dies der Fall, dann heißt x_T auch das **Ergebnis** der Rechnung. Wir schreiben dies als

$$M : x_1 \Rightarrow x_T.$$

Lemma 2.1.6. *Das Ergebnis einer M-Rechnung ist, wenn es existiert, durch die Eingabe eindeutig festgelegt.*

Beweis. Klar, weil jede Konfiguration eine eindeutig bestimmte Nachfolgekonfiguration hat. □

Definition 2.1.7. (Verkettung von Registermaschinen) Für eine Registermaschine M' der Länge s' und eine Zahl $s \in \mathbb{N}$ sei $s + M'$ die Folge von Instruktionen, die man erhält, wenn man in M' alle Instruktionsnummern um s vergrößert. Ist dann M eine Registermaschine der Länge s, so ist die Verkettung MM', die man durch Hintereinanderschreiben von M und $s + M'$ erhält, eine Registermaschine der Länge $s + s'$.

Lemma 2.1.8. *Die Verkettung zweier Registermaschinen ist eine Registermaschine, es gilt*

$$\varnothing M = M\varnothing = M, \quad M(M'M'') = (MM')M'',$$

hier sind $M, M'M''$ Registermaschinen und $\varnothing$ steht für die leere Registermaschine.

Beweis. Klar. □

Definition 2.1.9. Sei $f : \mathbb{N}_0^k \to \mathbb{N}$ eine Funktion. Eine Registermaschine M **berechnet** f, falls für jedes $x \in \mathbb{N}_0^k$ gilt

$$M : (x_1, \ldots, x_k, 0, \ldots, 0) \Rightarrow (f(x), 0, \ldots, 0).$$

Eine Funktion heißt **berechenbar**, wenn es eine Registermaschine gibt, die sie berechnet.

* * *

2.2 Rekursive Funktionen

Definition 2.2.1. Induktive Definition der **Rekursiven Funktionen** $f : \mathbb{N}_0^k \to \mathbb{N}_0$.

(R0) Die Funktionen

$$S(x) = x + 1, \qquad \text{(einstellig)}$$
$$P_j^n(x_1, \ldots, x_n) = x_j,$$
$$C_0^n(x_1, \ldots, x_n) = 0$$

sind rekursiv.

(R1) Sind die g_i und h rekursiv, dann auch

$$f(x_1, \ldots, x_n) = h(g_1(x), \ldots, g_k(x)).$$

(Einsetzung)

(R2) Sind g und h rekursiv, dann auch $f(x_1, \ldots, x_n, y)$, wobei

$$f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n)$$

und

$$f(x_1, \ldots, x_n, y + 1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)).$$

(primitive Rekursion)

(R3) Sei g rekursiv und es gelte $\forall_{x \in \mathbb{N}_0^n} \exists_y \, g(x, y) = 0$. Dann ist auch

$$f(x_1, \ldots, x_n) = \mu y \Big(g(\bar{x}, y) = 0 \Big)$$

rekursiv, wobei $\mu y A(y)$ = das kleinste y mit $A(y)$. (μ-Rekursion)

Verwendet man nur (R0), (R1) und (R2), so heißt f **primitiv-rekursiv**.

Satz 2.2.2. *Eine Funktion ist genau dann berechenbar, wenn sie rekursiv ist.*

In diesem Abschnitt beweisen wir **eine Richtung:** wir zeigen, dass rekursive Funktionen berechenbar sind.
Die Rueckrichtung wird in Abschnitt 2.4 bewiesen.

Induktion nach Definition. Die Funktionen nach R0 sind offensichtlich berechenbar. Eine Maschine für die Nachfolgerfunktion S wäre etwa

$$(1, 1, +, 2),$$

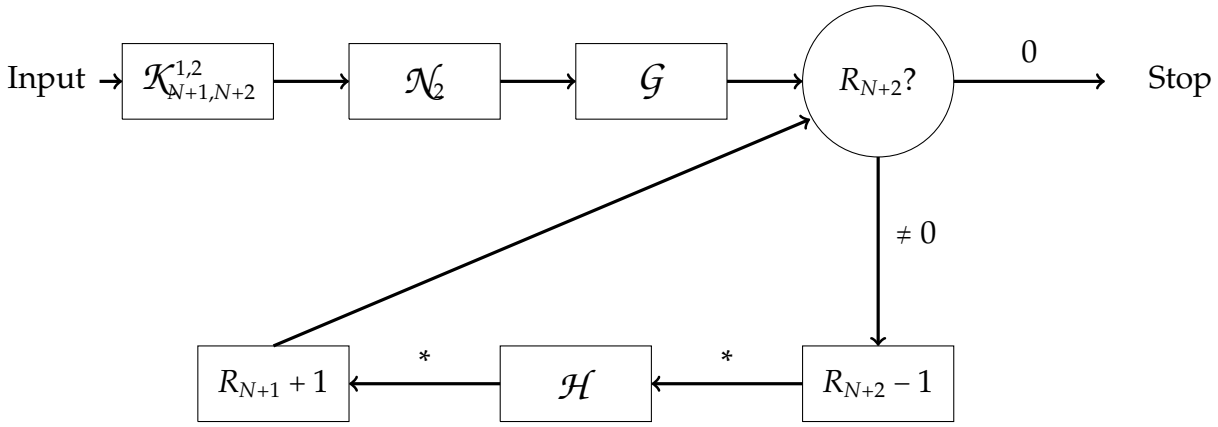
Eines für P_j^n ist

$$(1, j+1, 4, 2)$$
$$(2, 1, +, 3)$$
$$(3, j+1, -, 1)$$

gefolgt von einem Programm, das die Register $R_2, \ldots, R_{n+1}$ auf Null setzt.

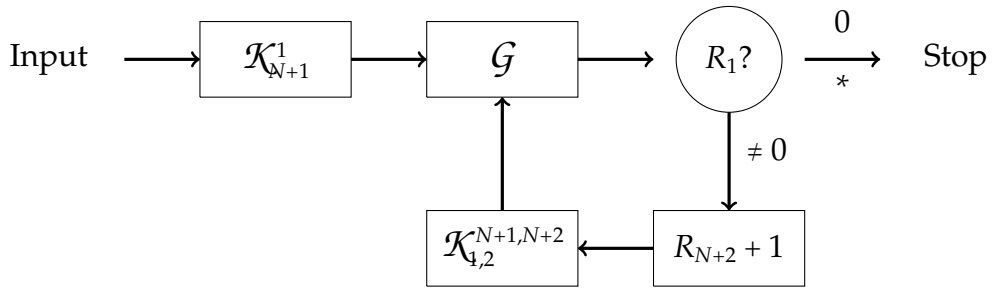
(R1) Seien $M_1, \ldots, M_k$ Registermaschinen, die $g_1, \ldots, g_k$ berechnen und sei N deren maximale Registerzahl. Zunächst kopiert man $(x_1, \ldots, x_n)$ in die Register $R_{N+1}, \ldots, R_{N+n}$. Dann setzt man die Maschine M_1 ein und erhält das Ergebnis $g_1(x), 0, \ldots, 0, x$. Man kopiert $g_1(x)$ in das Register R_{N+n+1} und $x_1, \ldots, x_n$ in die ersten Register, wendet dann M_2 and und so fort. Am Ende hat man die Registerinhalte $g_k(x), 0 \ldots, 0, x, g_1(x), \ldots, g_{k-1}(x)$ Man kopiert $g_1(x), \ldots, g_k(x)$ in die ersten Register, setzt die weiteren Register auf Null und wendet eine Maschine M an, die h berechnet.

(R2) Seien $\mathcal{G}$ und $\mathcal{H}$ Maschinen, die g und h berechnen und sei N deren maximale Registerzahl. Der Einfachheit halber betrachten wir nur den Fall $n = 1$. Sei $\mathcal{K}^{j,j+1,\ldots,j+r}_{p,p+1,\ldots,p+r}$ eine Maschine, die die Inhalte der Register $j, \ldots, j+r$ in die Register $p, \ldots p+r$ kopiert, wobei die Disjunktheit dieser Zahlintervalle vorausgesetzt sei. Ferner sei $\mathcal{N}_k$ die Maschine, die das Register k auf Null setzt. Wir beschreiben eine Maschine für f durch das Flussdiagramm:



Hierbei bedeuten die Sterne, dass dazwischen noch entsprechende Kopiervorgänge stehen.

(R3) Sei $\mathcal{G}$ eine Maschine, die g berechnet. Das Flussdiagramm für f ist



wobei hier der Stern noch einen Kopiervorgang und ein Loeschen beinhaltet. Das beendet den Beweis, dass alle rekursiven Funktionen berechenbar sind. Die Rueckrichtung von Satz 2.2.2 wird im Abschnitt 2.4 bewiesen.

* * *

2.3 Die Ackermann-Peter-Funktion

Definition 2.3.1. (Ackermann-Peter-Funktion) Wir definieren

$$\begin{aligned} a(0,n) &= n+1, \\ a(k+1,0) &= a(k,1) \\ a(k+1,n+1) &= a(k,a(k+1,n)). \end{aligned}$$

Zum Beispiel ist $a(1,1) = a(0,a(1,0)) = a(1,0)+1 = 3$.

Lemma 2.3.2. *Es gilt*

(a) $a(1,n) = n+2$,

(b) $a(2,n) = 2n+3$,

(c) $a(3,n) = 2^{n+3}-3$

(d) $a(4,n) = \underbrace{2^{2^{\cdot^{\cdot^{2}}}}}_{n+3\ Zweien} - 3$.

Beweis. (a) Fuer $n = 0$ ist $a(1,0) = a(0,1) = 2$.

Fuer $n \to n+1$ rechne

$$a(1,n+1) = a(0,a(1,n)) = a(1,n)+1 = n+2+1.$$

(b) Fuer $n = 0$ ist $a(2,0) = a(1,1) = 3$.

Fuer $n \to n+1$ rechne

$$a(2,n+1) = a(1,a(2,n)) = a(2,n) + 2 = 2n + 3 + 2 = 2(n+1) + 3.$$

(c) Fuer $n = 0$ ist $a(3,0) = a(2,1) = 5 = 2^3 - 3$.

Fuer $n \to n+1$ rechne

$$a(3,n+1) = a(2,a(3,n)) = 2a(3,n) + 3 = 2(2^{n+3} - 3) + 3 = 2^{(n+1)+3} - 3.$$

(d) Schreibe ${}^n2$ fuer $2^{2^{\cdot^{\cdot^2}}}$ mit n Zweien. Fuer $n = 0$ ist $a(4,0) = a(3,1) = 2^4 - 3 = 2^{2^2} - 3$.

Fuer $n \to n+1$ rechne

$$a(4,n+1) = a(3,a(4,n)) = 2^{a(4,n)+3} - 3 = 2^{{}^n2-3+3} - 3 = {}^{(n+1)}2 - 3. \qquad \square$$

Proposition 2.3.3. *Es gilt*

(I) $n < a(k,n)$,

(II) $a(k,n) < a(k,n+1)$, *(Monotonie im zweiten Argument)*

(III) $a(k,n+1) \leq a(k+1,n)$, *(wächst stärker im ersten Argument)*

(IV) $a(k,n) < a(k+1,n)$, *(Monotonie im ersten Argument)*

(V) $ma(k,n) \leq a(k,n+m)$, $k \geq 3$,

(VI) $a(k,n) + n \leq a(k,n+1)$, $k \geq 3$,

(VII) $a(k,2n) \leq a(k+1,n)$, $k \geq 2$.

Beweis. (I) Fuer $k = 0$ ist $n < n+1 = a(0,n)$.

Fuer $k \to k+1$ machen wir eine Unterinduktion nach n, also mit $n = 0$ ist $a(k+1,0) = a(k,1) > 1 > 0$. Fuer $n \to n+1$ rechne

$$\begin{aligned} n &< a(k+1,n) && I.V. \\ &< a(k,a(k+1,n)) && I.V. \\ &= a(k+1,n+1). \end{aligned}$$

Da hier zwei "<"-Schritte auftreten, folgt insgesamt $n+1 < a(k+1,n+1)$.

(II) Fuer $k = 0$ ist $a(0,n) = n+1 < n+2 = a(0,n+1)$.

Fuer $k \to k+1$ machen wir eine Unterinduktion nach n. Fuer $n = 0$ ist $a(k+1,0) = a(k,1) <^{I} a(k,a(k,1)) = a(k,a(k+1,0)) = a(k+1,1)$. Fuer $n \to n+1$ rechne

$$a(k+1,n+1) = a(k,a(k+1,n)) <^{Ind} a(k,a(k+1,n+1)) = a(k+1,n+2).$$

(III) Fuer $k = 0$ ist $a(k,n+1) = n+2 = a(1,n) = a(k+1,n)$.

Fuer den Schritt $k \to k+1$ machen wir eine Unterinduktion nach n. Fuer $n = 0$ ist $a(k+1,n+1) = a(k+1,1) = a(k+2,0) = a(k+2,n)$. Fuer den Schritt $n \to n+1$ rechne

$$\begin{aligned} a(k+1,n+2) &= a(k,a(k+1,n+1)) \\ &\leq a(k,a(k+2,n)) && I.V. + (II) \\ &\leq a(k,a(k+2,n)+1) && (II) \\ &\leq a(k+1,a(k+2,n)) && I.V. \\ &= a(k+2,n+1). \end{aligned}$$

(IV) Fuer $k = 0$ ist $a(0,n) = n+1 < n+2 = a(1,n)$.

Fuer $k \to k+1$ machen wir eine Unterinduktion nach n. Fuer $n = 0$ ist $a(k+1,0) = a(k,1) \leq^{I.V.} a(k+1,1) = a(k+2,0)$. Fuer $n \to n+1$ rechne

$$\begin{aligned} a(k+1,n+1) &= a(k,a(k+1,n)) \\ &< a(k+1,a(k+1,n)) && I.V. \\ &\leq a(k+1,a(k+1,n+1)) && (II) \\ &\leq a(k+1,a(k+2,n)) && (II) + (III) \\ &= a(k+2,n+1). \end{aligned}$$

(V) Fuer $k = 3$ ist $ma(k,n) = m(2^{n+3} - 3) \leq 2^m(2^{n+3} - 3) \leq 2^{m+n+3} - 3 = a(k,n+m)$.

Fuer $k \to k+1$ machen wir eine Unterinduktion nach n. Fuer $n = 0$ ist $ma(k+1,n) = ma(k+1,0) = ma(k,1) \leq^{I.V.} a(k,m+1) \leq^{(III)} a(k+1,m) = a(k+1,m+n)$. Da fuer $m = 0,1$ die Behauptung trivialerweise erfuellt ist, nehmen wir $m \geq 2$ an. Fuer den

Schritt $n \to n+1$ rechne dann

$$\begin{aligned} ma(k+1,n+1) &= ma(k,a(k+1,n)) \\ &\le a(k,a(k+1,n)+m) && I.V. \\ &\le a(k,ma(k+1,n)) && a(k+1,n) \ge 2 \\ &\le a(k,a(k+1,m+n)) && I.V.+(II) \\ &= a(k+1,m+n+1)). \end{aligned}$$

(VI) Fuer $k=3$ ist $a(k,n)+n = 2^{n+3}-3+n \le 2^{n+3}-3+2^{n+3} = 2^{n+4}-3 = a(k,n+1)$.

Fuer $k \to k+1$ machen wir eine Unterinduktion nach n. Fuer $n=0$ ist die Behauptung klar. Fuer den Schritt $n \to n+1$ rechne

$$\begin{aligned} a(k+1,n+1)+n+1 &= a(k,a(k+1,n)+n+1 \\ &\le a(k,a(k+1,n))+a(k+1,n) && (II) \\ &\le a(k,a(k+1,n)+1) && I.V. \\ &\le a(k,a(k+1,n)+n) && (II) \\ &\le a(k,a(k+1,n+1)) && I.V. \\ &= a(k+1,n+2). \end{aligned}$$

(VII) Fuer $k=2$ ist $a(k,2n) = 2n+3 \le 2^{n+3}-3 = a(k+1,n)$. Fuer $k \to k+1$ machen wir eine Unterinduktion nach n. Fuer $n=0$ ist
$a(k+1,2n) = a(k+1,0) \le^{(II)} a(k+1,1) = a(k+2,0) = a(k+2,n)$. Fuer den Schritt $n \to n+1$ rechne

$$\begin{aligned} a(k+1,2(n+1)) &\le a(k+1,a(k,2(n+1))) && (II) \\ &\le a(k+1,a(k+1,n+1)) && I.V. \\ &\le a(k+1,a(k+2,n)) && (III) \\ &= a(k+2,n+1). \end{aligned}$$

□

Satz 2.3.4. *Zu jeder primitiv-rekursiven Funktion f auf $\mathbb{N}_0^r$ gibt es eine Zahl k, so dass fuer alle $n_1,\dots,n_r \in \mathbb{N}_0$ gilt*

$$f(n_1,\dots,n_r) < a(k,n_1+\cdots+n_r).$$

Beweis. Dies ist klar fuer die Funktionen aus (R0).

(R1) Seien g_i und h rekursiv und

$$f(x_1,\dots,x_n) = h(g_1(x),\dots,g_k(x)).$$

Ferner seien $g_j(x_1,\dots,x_n) \le a(K, x_1+\dots+x_n)$ sowie $h(y_1,\dots,y_k) \le a(K, y_1+\dots+y_k)$ mit einem $K \ge 3$, was wir nach der Monotonie von a annehmen koennen. Dann ist

$$\begin{aligned}
f(x_1,\dots,x_n) &\le a(K, g_1(x)+\dots+g_k(x)) \\
&\le a(K, a(K,\textstyle\sum x)+\dots+a(K,\sum x)) && (II)\\
&= a(K, k\,a(K,\textstyle\sum x)) \\
&\le a(K, a(K, k+\sum x)) && (V)\\
&\le a(K, a(K+k,\textstyle\sum x)) && (III)+(II)\\
&\le a(K+k, a(K+k+1,\textstyle\sum x)) && (IV)+(II)\\
&= a(K+k+1,\textstyle\sum x+1) \\
&\le a(K+k+2,\textstyle\sum x) && (III),
\end{aligned}$$

wobei $\sum x$ fuer $x_1+\dots+x_n$ steht.

(R2) Seien nun g und h gegeben mit $g(x) \le a(K,\sum x)$ fuer ein $K \ge 1$ und $h(z) \le a(K,\sum z)$, sowie

$$f(x_1,\dots,x_n,0) = g(x_1,\dots,x_n)$$

und

$$f(x_1,\dots,x_n,y+1) = h(x_1,\dots,x_n,y,f(x_1,\dots,x_n,y)).$$

Wir zeigen induktiv, dass $f(x,y) \le a(K+2,\sum x+y)$. Hierzu rechne

$$\begin{aligned}
f(x,0) &\le a(K,\textstyle\sum x) \le a(K+2,\sum x), && (IV)\\
f(x,y+1) &= h(x,y,f(x,y)) \\
&\le a(K,\textstyle\sum x+y+f(x,y)) \\
&\le a(K,\textstyle\sum x+y+a(K+2,\sum x+y)) && (II)\\
&\le a(K, 2a(K+2,\textstyle\sum x+y)) && (I)+(II)\\
&\le a(K+1, a(K+2,\textstyle\sum x+y)) && (VII)\\
&= a(K+2,\textstyle\sum x+y+1).
\end{aligned}$$

□

Satz 2.3.5. *Die Ackermann-Peter-Funktion ist rekursiv, aber nicht primitiv-rekursiv.*

Beweis. Man sieht ein, dass a berechenbar ist. Später zeigen wir, dass berechenbare Funktionen rekursiv sind.

Wir wissen, dass es zu jeder primitiv-rekursiven Funktion f auf $\mathbb{N}_0^r$ eine Zahl k gibt, so dass

$$f(n_1, \ldots, n_r) < a(k, n_1 + \cdots + n_r).$$

Angenommen, a ist primitiv-rekursiv, dann ist auch $g(n) = a(n, n)$ primitiv-rekursiv. Dann existiert ein k so dass $g(n) < a(k, n)$. Setzt man $n = k$ ein, so folgt der **Widerspruch:**

$$a(k, k) = g(k) < a(k, k). \qquad \square$$

* * *

2.4 Gödelisierung

Lemma 2.4.1. *Die Funktionen*

$$x + y, \quad x \cdot y, \quad x^y, \quad x - y$$

sind rekursiv, wobei $x - y = 0$ *falls* $x \leq y$.

Beweis. Klar. $\square$

Definition 2.4.2. Eine Relation $R \subset \mathbb{N}_0^k$ heißt **rekursiv**, falls die charakteristische Funktion

$$\chi_R(x_1, \ldots, x_k) = \begin{cases} 1 & x \in R, \\ 0 & x \notin R. \end{cases}$$

rekursiv ist.

Lemma 2.4.3. *Sind P und Q rekursiv, dann auch $P \wedge Q$, $P \vee Q$, $\neg P$ und $P(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n))$ für alle rekursiven Funktionen $f_1, \ldots, f_k$.*

Beweis. Es ist $\chi_{P \wedge Q} = \chi_P \cdot \chi_Q$, $\chi_{\neg P} = 1 - \chi_P$ und $P \vee Q \Leftrightarrow \neg(\neg P \wedge \neg Q)$. Setzt man schliesslich die f_i in die charakteristische Funktion von P ein, erhält man die von $P(f_1, \ldots, f_k)$. $\square$

Lemma 2.4.4 (Fallunterscheidung). *Sind $P_0, \dots, P_n$ rekursive Prädikate und $f_0, \dots, f_n$ rekursive Funktionen, so ist auch*

$$f(\bar{x}) = \begin{cases} f_0(\bar{x}) & P_0(\bar{x}), \\ f_1(\bar{x}) & \neg P_0(\bar{x}) \wedge P_1(\bar{x}), \\ & \vdots \\ f_n(\bar{x}) & \neg P_0(\bar{x}) \wedge \dots \wedge \neg P_{n-1}(\bar{x}) \wedge P_n(\bar{x}) \\ 0 & \textit{sonst} \end{cases}$$

rekursiv. Hierbei steht $\bar{x}$ für $(x_1, \dots, x_k)$.

Beweis. Die Prädikate $Q_0 = P_0, Q_1 = \neg P_0 \wedge P_1, \dots Q_n = \neg P_0 \wedge \dots \wedge \neg P_{n-1} \wedge P_n$ sind rekursiv, also auch

$$f(\bar{x}) = \sum_{j=0}^{n} \chi_{Q_i}(\bar{x}) f_i(\bar{x}). \qquad \square$$

Lemma 2.4.5. *Sei P rekursiv. Dann sind auch die Relationen*

$$R(\bar{x}, y) \Leftrightarrow \forall_{z<y}\, P(\bar{x}, z),$$
$$S(\bar{x}, y) \Leftrightarrow \exists_{z<y}\, P(\bar{x}, z)$$

rekursiv.

Beweis. Man definiert R durch die Rekursion:

$$R(\bar{x}, 0) := \text{wahr},$$
$$R(\bar{x}, z+1) \Leftrightarrow R(\bar{x}, z) \wedge P(\bar{x}, z).$$

Schliesslich ist $S(\bar{x}, y) \Leftrightarrow \neg\, \forall_{z<y}\, \neg P(\bar{x}, z)$. $\square$

Beispiele 2.4.6.

- $x \mid y$ (x teilt y) ist rekursiv.
- *x ist Primzahl* ist rekursiv.
- $p(n) = (n+1)$*-te Primzahl* ist rekursiv, denn

$$p(n+1) = \mu y \Big((y \text{ ist Primzahl }) \wedge (y > p(n)) \Big).$$

* * *

Lemma 2.4.7. *Sei p_n die n-te Primzahl. Sei $\mathbb{N}_0^*$ die disjunkte Vereinigung aller $\mathbb{N}_0^k$ mit $k = 0, 1, \ldots$. Die Abbildung $\langle\ \rangle : \mathbb{N}_0^* \to \mathbb{N}_0$,*

$$\langle n_1, \ldots, n_k \rangle = p_1^{n_1} \cdots p_{k-1}^{n_{k-1}} p_k^{n_k+1} - 1$$

ist eine Bijektion. Es gilt

(a) *Die zweistellige Komponentenfunktion $(x)_i$ definiert durch*

$$(\langle n_1, \ldots, n_k \rangle)_i = \begin{cases} n_i & i \leq k, \\ 0 & \textit{sonst}, \end{cases}$$

ist rekursiv.

(b) *Die Längenfunktion $\lg(x)$ definiert durch*

$$\lg(\langle n_1, \ldots, n_k \rangle) = k$$

ist rekursiv.

(c) *Für jedes k ist $\langle\ \rangle : \mathbb{N}_0^k \to \mathbb{N}_0$ rekursiv.*

(d) *Für alle n ist $\lg(n) \leq n$. Ist $n > 0$, dann ist $(n)_i < n$.*

Wir nennen $\langle n_1, \ldots, n_k \rangle$ die **Gödelnummer** von $(n_1, \ldots, n_k)$.

Beweis. (c) folgt aus Lemma 2.4.1.
(d) ist klar.
(b) es ist

$$\lg(x) = \mu y\ \forall_{n \leq x}(y < n \to p_n \dot{+} (x+1)).$$

(a) Es ist

$$(x)_i = \begin{cases} \mu y\ p_i^{y+1} \dot{+} (x+1) & i < \lg(x), \\ \mu y\ p(i)^{y+2} \dot{+} (x+1) & i = \lg(x), \\ 0 & i > \lg(x). \end{cases}$$

□

Sei $\beta : \mathbb{N}_0 \to \mathbb{N}_0$ eine rekursive Bijektion. Dann ist die Umkehrabbildung $\mu y\ \beta(y) = x$ wieder rekursiv. Es definiert

$$\langle n_1, \ldots, n_k \rangle^\beta = \beta(\langle n_1, \ldots, n_k \rangle)$$

eine Gödelnummerierung mit rekursiver Komponentenfunktion und rekursiver Längenfunktion $L(x)$.

Bemerkung 2.4.8. Sei $[\,] : \mathbb{N}_0^* \to \mathbb{N}_0$ eine Bijektion mit rekursiver Komponentenfunktion und rekursiver Längenfunktion $L(x)$. Dann gibt es eine rekursive Bijektion $\beta : \mathbb{N}_0 \to \mathbb{N}_0$ mit $[\,] = \langle\ \rangle^\beta$.

Beweis. Man definiert β durch

$$\beta(s) = \mu t \left(L(t) = \lg(s) \wedge \forall_{i<\lg(s)}\ [t]_i = (s)_i \right). \qquad \square$$

Gödelisierung von Registermaschinen

Wir ordnen jedem Befehl, jeder Registermaschine, jeder Konfiguration und jeder Rechnung X eine Zahl $\ulcorner X \urcorner$, ihre **Gödelnummer** zu:

Objekt X	Gödelnummer $\ulcorner X \urcorner$
+	1,
-	2,
i =Instruktionsnummer oder Registernummer	i+2
Instruktion (j, i, b, l)	$\langle \ulcorner i \urcorner, \ulcorner j \urcorner, \ulcorner b \urcorner, \ulcorner l \urcorner \rangle$
Registermaschine $(I_1, I_2, \ldots, I_s)$	$\langle \ulcorner I_1 \urcorner, \ldots, \ulcorner I_s \urcorner \rangle$
Konfiguration $(j, x_1, \ldots, x_N)$	$\langle j, x_1, \ldots, x_N \rangle$
Rechnung $(K_1, \ldots, K_T)$	$\langle \ulcorner K_1 \urcorner, \ldots, \ulcorner K_T \urcorner \rangle$.

Für eine Konfiguration K zu einer Registermaschine M schreiben wir $M(K)$ für die entsprechende Nachfolgekonfiguration.

Lemma 2.4.9. *Es gibt eine rekursive Funktion $N(x, y)$ so dass für jede Maschine M und für jede Konfiguration K zu M gilt*

$$N(\ulcorner M \urcorner, \ulcorner K \urcorner) = \ulcorner M(K) \urcorner.$$

Beweis. Man macht sich klar, dass man N durch Komposition bekannter rekursiver Funktionen erhält. $\square$

Beweis von Satz 2.2.2. Es ist nun klar, dass man eine RM-Berechnung durch rekursive Funktionen modellieren kann und damit ist jede berechenbare Funktion rekursiv, also folgt der Satz. $\square$

* * *

2.5 Rekursiv aufzählbare Mengen

Definition 2.5.1. Eine Relation R heißt **rekursiv aufzählbar**, wenn es eine rekursive Relation $\tilde{R}$ gibt, so dass

$$R(\bar{x}) \quad \Leftrightarrow \quad \exists_y \, \tilde{R}(\bar{x}, y).$$

Insbesondere sind rekursive Relationen rekursiv aufzählbar.

Lemma 2.5.2. *Eine Menge von natürlichen Zahlen ist genau dann rekursiv aufzählbar, wenn sie leer ist oder das Bild einer rekursiven Funktion.*

Dieses Lemma rechtfertigt den Namen "rekursiv aufzählbar", weil es eine rekursive Funktion (oder eine Registermaschine) gibt, die die Menge aufzählt.

Beweis. "⇒" Sei $R(x) \Leftrightarrow \exists_y \, \tilde{R}(x, y)$ und $r \in R$, dann ist R das Bild der rekursiven Funktion

$$f(x) = \begin{cases} (x)_1 & \text{wenn } \tilde{R}((x)_1, (x)_2) \\ r & \text{sonst.} \end{cases}$$

"⇐" Das Bild R einer rekursiven Funktion f ist rekursiv aufzählbar, denn

$$R(x) \quad \Leftrightarrow \quad \exists_z \, f(z) = x.$$

□

Lemma 2.5.3. *R ist genau dann rekursiv, wenn R und $\neg R$ rekursiv aufzählbar sind.*

Beweis. Sei $R(\bar{x}) \Leftrightarrow \exists_y \, V(\bar{x}, y)$ und $\neg R(\bar{x}) \Leftrightarrow \exists_y \, W(\bar{x}, y)$ für rekursive V und W. Dann ist

$$g(\bar{x}) = \mu y \, (V(\bar{x}, y) \vee W(\bar{x}, y))$$

für alle x definiert und rekursiv. Es gilt

$$R(\bar{x}) \quad \Leftrightarrow \quad V(\bar{x}, g(\bar{x})).$$ □

Definition 2.5.4. Wir definieren das rekursive **Kleene-Prädikat** $T_n(m, x_1, \ldots, x_n, g) \Leftrightarrow$ m ist Goedelzahl einer Registermaschine M und diese stoppt mit dem Input $x_1, \ldots, x_n$ nach $(g)_1$ Schritten mit dem Output $(g)_2$. Dieses ist rekursiv.

Satz 2.5.5. *Es gibt eine Relation $U \subset \mathbb{N}_0^2$, so dass*

(a) *U ist rekursiv aufzählbar.*

(b) *Für jede rekursiv aufzählbare Menge R gibt es ein e so dass*

$$R = W_e = \Big\{x : U(e,x)\Big\}.$$

Man nennt U eine **universelle rekursiv aufzaehlbare Relation**.

Beweis. Sei $S(x,y)$ rekursiv und M eine Maschine, die versucht $\mu y\, S(x,y)$ zu berechnen. Dann stoppt M beim Input x genau dann, wenn $\exists_y S(x,y)$. Wir haben also $\exists_y S(x,y) \Leftrightarrow \exists_g T_1(\ulcorner M \urcorner, x, g)$. Die rekursiv aufzählbare Relation

$$U(e,x) \quad \Leftrightarrow \quad \exists_y T_1(e,x,y)$$

ist also universell. □

Proposition 2.5.6. *Es gibt eine Menge, die rekursiv aufzählbar, aber nicht rekursiv ist.*

Beweis. Da U rekursiv aufzaehlbar ist $U(x,x)$ rekursiv aufzaehlbar.
Die Menge $\neg\, U(x,x)$ kann nicht die Form W_e haben, weil $\neg\, U(e,e) \Leftrightarrow e \notin W_e$. Daher ist $\neg\, U(x,x)$ nicht rekursiv aufzählbar.

Deshalb ist $U(x,x)$ nicht rekursiv, aber rekursiv aufzählbar. □

* * *

2.6 Gödelnummern von Formeln

Definition 2.6.1. Sei $L = \{\lambda_1, \ldots, \lambda_l\}$ eine endliche Sprache. Wir ordnen den Zeichen

$$\begin{array}{cccccccccc} = & \to & \neg & (&) & \forall & x_1 & x_2 & \ldots \\ \lambda_1 & \ldots & \lambda_l & a_1 & a_2 & \ldots & & & \end{array}$$

die Gödelnummern

$$\begin{array}{cccccccccc} \langle 0,1\rangle & \langle 0,2\rangle & \langle 0,3\rangle & \langle 0,4\rangle & \langle 0,5\rangle & \langle 0,6\rangle & \langle 0,7\rangle & \langle 0,8\rangle & \ldots \\ \langle 1,1\rangle & \ldots & \langle 1,l\rangle & \langle 1,l+1\rangle & \ldots & & & & \end{array}$$

zu und jeder Zeichenreihe $Z = z_1 z_2 \dots z_n$ die Gödelnummer $\ulcorner Z \urcorner = \langle \ulcorner z_1 \urcorner, \ulcorner z_2 \urcorner, \dots, \ulcorner z_n \urcorner \rangle$.

Zuletzt ordnen wir eich einer Herleitung $(F_1, \dots, F_k)$ die Goedelnummer

$$\ulcorner (F_1, \dots, F_k) \urcorner := \langle \ulcorner F_1 \urcorner, \dots, \ulcorner F_k \urcorner \rangle$$

zu.

Lemma 2.6.2. *Die folgenden Mengen sind rekursiv*

(a) $\{\ulcorner t \urcorner : t \text{ ist ein Term in } L\}$

(b) $\{\ulcorner F \urcorner : F \text{ ist eine Formel in } L\}$

Beweis. Man kann eine Registermachine bauen, die einer Zahl ansieht, ob sie ein Term oder eine Formel ist. □

Definition 2.6.3. Eine Theorie T heißt

(a) **rekursiv**, falls $\left\{\ulcorner F \urcorner : F \in \mathrm{Ax}(T)\right\}$ rekursiv ist.

(b) **rekursiv aufzählbar**, falls $\left\{\ulcorner F \urcorner : F \in \mathrm{Ax}(T)\right\}$ rekursiv aufzählbar ist.

(c) **entscheidbar**, falls $\left\{\ulcorner F \urcorner : T \vdash F\right\}$ rekursiv ist.

Satz 2.6.4. *Ist eine Theorie T rekursiv aufzählbar, dann ist auch die Menge* $\left\{\ulcorner F \urcorner : T \vdash F\right\}$ *rekursiv aufzählbar.*

Beweis. Wenn es eine Registermaschine gibt, die alle Axiome aufzählt, dann gibt es auch eine, die alle Herleitungen aufzählt. □

Erinnerung. Eine konsistente Theorie heißt **vollständig**, falls für jeden Satz F gilt

$$T \vdash F \quad \text{oder} \quad T \vdash \neg F.$$

Beispiel 2.6.5. Die Zahlentheorie ist rekursiv aufzählbar. Sie hat zwar unendlich viele Axiome, diese können aber aufgezählt werden, da ja für jede Formel ein Axiom entsteht und die Menge der Formeln rekursiv aufzählbar ist.

Proposition 2.6.6. *Ist eine Theorie rekursiv aufzählbar und vollständig, so ist sie entscheidbar.*

Beweis. Sei A die Menge aller Gödelnummern aller L-Formeln und B die Menge der Gödelnummern der T-beweisbaren Formeln. Sei f eine rekursive Funktion mit $f(\ulcorner\phi\urcorner) = \ulcorner\neg\phi\urcorner$. Aus der Vollständigkeit von T folgt

$$x \notin B \quad \Leftrightarrow \quad x \notin A \vee f(x) \in B.$$

Die Menge A ist rekursiv, die Menge B ist rekursiv aufzählbar. Damit ist aber auch $\neg B$ rekursiv aufzählbar. Nach Lemma 2.5.3 ist B daher rekursiv. □

* * *

2.7 Alternativer Aufbau der rekursiven Funktionen

Satz 2.7.1. *Alle rekursiven Funktionen lassen sich aus den Grundfunktionen*

$$S(x) = x + 1,$$
$$P^n_j(x_1, \ldots, x_n) = x_j,$$
$$C^n_0(x_1, \ldots, x_n) = 0,$$

sowie $+, \cdot$ *und*

$$\chi_<(x, y) = \begin{cases} 1 & x < y, \\ 0 & x \geq y. \end{cases}$$

$$S(x), P^n_i, C_0, +, \cdot, \chi_<$$

durch Anwenden der Regeln (R1) (Einsetzung) und (R3) (μ-Rekursion) gewinnen.

Zur Erinnerung:

(R1) (Einsetzung) Sind die g_i und h rekursiv, dann auch

$$f(x_1, \ldots, x_n) = h(g_1(x), \ldots, g_k(x)).$$

(R3) (μ-Rekursion) Sei g rekursiv und es gelte $\forall_{x \in \mathbb{N}_0^n} \exists_y g(x, y) = 0$. Dann ist auch

$$f(x_1, \ldots, x_n) = \mu y(g(\bar{x}, y) = 0)$$

rekursiv, wobei

$$\mu y A(y) = \text{das kleinste } y \text{ mit } A(y).$$

Beweis. Wir nennen eine Funktion, die wir wie im Satz erhalten, $*$-rekursiv. Wenn wir zeigen können, dass die Klasse der $*$-rekursiven Funktionen unter (R2) (primitive Rekursion) abgeschlossen ist, sind wir fertig.

(R2) Sind g und h rekursiv, dann auch

$$f(x_1, \ldots, x_n, y),$$

wobei

$$f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n)$$

und

$$f(x_1, \ldots, x_n, y+1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)).$$

(primitive Rekursion)

Ein Prädikat P nennen wir $*$-rekursiv, falls seine charakteristische Funktion χ_P $*$-rekursiv ist.

Lemma 2.7.2. (a) *Die Funktion $x - y$ ist in $*$-rekursiv.*

(b) *Sind f, g $*$-rekursiv, dann auch $f \cdot g$, $f - g$.*

(c) *Das Prädikat $x = y$ ist $*$-rekursiv.*

(d) *Das Prädikat $x \equiv y \mod z$ ist $*$-rekursiv.*

(e) *Ist P ein $*$-rekursives Prädikat, dann sind auch die Prädikate*

$$R(\bar{x}, z) \Leftrightarrow \forall_{y<z}\, P(\bar{x}, y),$$
$$S(\bar{x}, z) \Leftrightarrow \exists_{y<z}\, P(\bar{x}, y)$$

$*$-rekursiv.

(f) *Die Klasse der $*$-rekursiven Prädikate ist abgeschlossen unter Fallunterscheidung (siehe Lemma 2.4.4).*

Beweis. (a) $x - y = \mu z\, x < (y + z) + 1$.

(b) Dies durch Einsetzung, da $\cdot, - \in \mathcal{S}$.

(c) $x = y \Leftrightarrow (\neg\, x < y \wedge \neg\, y < x)$.

(d) $x \equiv y \mod z \Leftrightarrow \exists_{w<(x+y+1)}\, (x = y + wz \vee y = x + wz)$.

(e) Sei $P(\bar{x}, y)$ ein $*$-rekursiv. Definiere

$$g(\bar{x}, y) = \mu z\, (P(x, z) \vee z = y).$$

Dann ist

$$\exists_{y<z} P(x,y) \quad \Leftrightarrow \quad g(x,z) < z,$$

und damit $*$-rekursiv. R bekommt man durch Negation.

(f) Wie in Lemma 2.4.4. □

Lemma 2.7.3 (Gödels β-Funktion)**.** *Es gibt eine $*$-rekursive Funktion $\beta(a,b,i)$ so dass es zu jeder endlichen Folge $c_0, c_1, \ldots, c_{n-1}$ es a, b gibt, so dass*

$$\beta(a,b,i) = c_i$$

für $i = 0, 1, \ldots, n-1$.

Eine rekursive Funktion mit dieser Eigenschaft ist schnell gebaut: man benutzt die Primzahlkodierung von Goedel. Nun soll's aber *-rekursiv sein, da mueesen wir anders rangehen.

Beweis. Die Funktion

$$\beta(a,b,i) = \mu z\, z \equiv a \mod (b(i+1)+1)$$

ist $*$-rekursiv. Seien $c_0, c_1, \ldots, c_{n-1}$ gegeben. Wähle für b eine Zahl, die durch alle Zahlen $2, 3, \ldots, n$ teilbar ist und größer ist als alle c_i. Dann sind $b \cdot 1 + 1, b \cdot 2 + 1, \ldots, b \cdot n + 1$ paarweise teilerfremd. Teilt eine Primzahl p nämlich $bi + 1$, dann teilt p nicht b. Würde p aber auch $bj + 1$ teilen, dann teilt p die Zahl $b(i-j)$, also $p \mid (i-j)$ aber $i - j$ ist ein Teiler von b, Widerspruch!

Nach Chinas Restsatz existiert eine gemeinsame Lösung a der Kongruenzen

$$\begin{aligned} a &\equiv c_0 && \mod (b+1) \\ a &\equiv c_1 && \mod (2b+1) \\ &\vdots \\ a &\equiv c_{n-1} && \mod (nb+1). \end{aligned}$$

Weil $c_i < b(i_1) + 1$, ist c_i jeweils die kleinste natürliche Zahl, die zu a kongruent ist modulo $b(i+1)+1$. □

Beweis von Satz 2.7.1. Wir müssen zeigen, dass die Klasse der $*$-rekursiven Funktionen unter primitiver Rekursion abgeschlossen ist. Seien also g und h $*$-rekursiv und sei f

definiert durch

$$f(\bar{x}, 0) = g(\bar{x}),$$
$$f(x, y+1) = h(\bar{x}, y, f(x, y)).$$

Die Relation

$$R(\bar{x}, y, a, b) \;\Leftrightarrow\; (\beta(a, b, 0) = g(x) \wedge \forall_{i<y}\, \beta(a, b, i+1) = h(x, i, \beta(a, b, i)))$$

ist $*$-rekursiv. Offenbar gilt $\forall_{\bar{x},y}\, \exists_{a,b}\, R(x, y, a, b)$. Also ist

$$S(\bar{x}, y) = \mu s\, \exists_{a,b\le s}\, R(x, y, a, b)$$

$*$-rekursiv. Damit ist auch

$$f(\bar{x}, y) = \mu z\, \exists_{a,b\le S(x,y)}\, (R(x, y, a, b) \wedge z = \beta(a, b, y))$$

$*$-rekursiv. □

* * *

3 Unvollständigkeit der Arithmetik

3.1 Erster Gödelscher Unvollständigkeitssatz

Definition 3.1.1. Eine Relation $R \subset \mathbb{N}_0^n$ heißt **arithmetisch**, wenn sie in der Struktur

$$\mathcal{N} = (\mathbb{N}_0, +, -, \cdot, <)$$

definierbar ist, also wenn es eine Formel F in der Sprache von $\mathcal{N}$ gibt, so dass

$$R(\bar{a}) \quad \Leftrightarrow \quad \mathcal{N} \vDash F(\bar{a}).$$

Eine Funktion heißt arithmetisch, wenn ihr Graph arithmetisch ist.

Lemma 3.1.2. *Rekursive Funktionen und Relationen sind arithmetisch.*

Beweis. Da man eine Relation aus dem Graphen ihrer charakteristischen Funktion zurueckerhaelt, reicht es, den Funktionenfall zu betrachten. Wir verwenden die alternative Beschreibung der rekursiven Funktionen in Satz 2.7.1. Die

Grundfunktionen

$$S(x), P_i^n, C_0, +, \cdot, \chi_<$$

sind alle arithmetisch.

(R1) Sei $f(\bar{x}) = h(g_1(\bar{x}), \ldots, g_n(\bar{x}))$. Dann ist $(\bar{x}, y) \in G_f$ genau dann, wenn

$$\exists_{z_1} \ldots \exists_{z_n} \, (\bar{z}, y) \in G_h \wedge (\bar{x}, z_1) \in G_{g_1} \wedge \cdots \wedge (\bar{x}, z_n) \in G_{g_n}).$$

Da nach Induktionsvoraussetzung die $G_h, G_{g_1}, \ldots, G_{g_n}$ alle durch Formeln beschreibbar sind, ist demnach auch G_f durch eine Formel beschreibbar.

(R3) Sei $f(\bar{x}) = \mu y \; g(\bar{x}, y) = 0$. Dann ist $(\bar{x}, y) \in G_f$ genau dann, wenn

$$(\bar{x}, y, 0) \in G_g \wedge \forall_{z<y} \, (\bar{x}, z, 0) \notin G_g$$ □

Korollar 3.1.3. *Rekursiv aufzählbare Relationen sind arithmetisch.*

Beweis. Sei R rekursiv aufzählbar. Dann existiert eine rekursive Relation S, so dass $R(\bar{x}) \Leftrightarrow \exists_y \, S(\bar{x}, y)$. Dann ist S nach dem Lemma durch eine Formel in $\mathcal{N}$ ausdrueckbar, also auch R. □

Definition 3.1.4. Eine Teiltheorie T von $T(\mathcal{N})$ heißt **arithmetisch**, falls die Menge

$$\left\{ \ulcorner F \urcorner : F \in \mathrm{Ax}(T) \right\}$$

arithmetisch ist.

Lemma 3.1.5. *Ist T arithmetisch, dann ist auch*

$$T^* = \{F : T \vdash F\}$$

arithmetisch.

Beweis. Es gibt eine Formel $A(a)$ mit

$$\mathcal{N} \vDash A(n) \quad \Leftrightarrow \quad \exists_{F \in \mathrm{Ax}(T)} \ulcorner F \urcorner = n.$$

Wir behaupten, dass es eine Formel B in der Sprache von $\mathcal{N}$ gibt, so dass

$$\mathcal{N} \vDash B(a) \quad \Leftrightarrow \quad \forall_j \;\; A\big((a)_j\big).$$

Um dies einzusehen, muss man die rechte Seite so formulieren: fuer jede Primzahl p ist die maximale Potenz e von p in a entweder Null oder es gilt $A(e)$.

Sei

$$\mathrm{Herl}(a, e, f)$$

die Relation definiert durch $\mathrm{Herl}(a, e, f) \Leftrightarrow f$ ist die Goedelzahl einer Formel F und e ist die Goedelzahl einer Herleitung von F in die maximal die Axiome mit den Goedelzahlen $\langle a \rangle_1, \ldots, \langle a \rangle_k$ mit $k = \lg(a)$ eingehen. Dann ist Herl rekursiv. Fuer eine Formel F ist die Aussage $T \vdash F$ aequivalent zu

$$\exists_{a,e} \mathrm{Herl}(a, e, \ulcorner F \urcorner) \wedge B(a).$$

Damit ist $\{F : T \vdash F\}$ arithmetisch. □

Satz 3.1.6 (Erster Gödelscher Unvollständigkeitssatz)**.**

(a) *Die Theorie $T(\mathcal{N})$ der natürlichen Zahlen ist unentscheidbar, d.h., die Menge*

$$\left\{ \ulcorner F \urcorner : T \vdash F \right\}$$

ist nicht rekursiv.

(b) *Die Theorie $T(\mathcal{N})$ ist nicht arithmetisch und damit auch nicht rekursiv aufzählbar.*

(c) *Jede arithmetische Teiltheorie von $T(\mathcal{N})$ ist unvollständig.*

Korollar 3.1.7. *Es gibt keine Maschine, die mir fuer eine gegebene Formel sagt, ob diese in den natuerlichen Zahlen gilt oder nicht.*

Beweis. (a) folgt aus (b).

Fuer (b) betrachte die Relation

$$U(e, n) \;:\Leftrightarrow\; e \text{ ist Gödelnummer einer Formel } F(a), \text{ für die } \mathcal{N} \vDash F(n).$$

Angenommen, U ist arithmetisch, dann ist auch die Relation $R(x) = \neg\, U(x, x)$ arithmetisch. Das bedeutet aber, dass $R(x)$ durch eine Formel beschrieben wird. Sei e die Gödelnummer dieser Formel, dann folgt

$$R(n) \quad \Leftrightarrow \quad U(e, n).$$

Insbesondere für $n = e$ folgt

$$\neg U(e,e,) \quad \Leftrightarrow \quad R(e) \quad \Leftrightarrow \quad U(e,e),$$

Widerspruch!

(c) Sei T eine arithmetische Teiltheorie von $T(\mathcal{N})$. Dann ist auch $T^* = \{F : T \vdash F\}$ arithmetisch. Da $\mathcal{N}$ ein Modell von T ist, ist es auch eines von T^*. Wäre nun T vollständig, so müsste $T^* = T(\mathcal{N})$ sein, was aber nicht sein kann, da $T(\mathcal{N})$ nicht arithmetisch ist. □

* * *

3.2 Die eingeschränkte Zahlentheorie *EZ*

Definition 3.2.1. Wir erinnern an die Zahlentheorie in Beispiel 1.4.4. Wir schreiben $\Delta_0 = 0$ und für $n \in \mathbb{N}$ der Term Δ_n definiert durch

$$\Delta_n = \underbrace{1 + 1 + \cdots + 1}_{n-\text{mal}}.$$

Dann ist in Z für jedes Paar $m, n \in \mathbb{N}^2$ herleitbar

(EZ1) $\Delta_m + \Delta_n = \Delta_{m+n}$,

(EZ2) $\Delta_m \cdot \Delta_n = \Delta_{mn}$,

(EZ3) $\forall_x \neg(x < \Delta_0) \wedge [(x < \Delta_m) \leftrightarrow (x = \Delta_0 \vee x = \Delta_1 \vee \cdots \vee x = \Delta_{m-1})]$.

Definition 3.2.2. Sei EZ die Theorie zur Sprache $L(Z)$ der Zahlentheorie, die aus den unendlich vielen Axiomen der Form (EZ1), (EZ2), (EZ3) besteht, wobei $m, n \in \mathbb{N}_0$.

Lemma 3.2.3. (a) *Für alle $m, n \in \mathbb{N}_0$ gilt*

$$m < n \Rightarrow EZ \vdash \Delta_m < \Delta_n,$$
$$m \neq n \Rightarrow EZ \vdash \neg\, \Delta_m = \Delta_n,$$
$$m \not< n \Rightarrow EZ \vdash \neg\, \Delta_m < \Delta_n.$$

(b) *Jedes Modell von EZ enthaelt $\mathcal{N}$ als Submodell.*

(c) *Fuer jeden geschlossenen Term t aus L(Z) gibt es genau eine Zahl $n \in \mathbb{N}_0$ so dass*

$$EZ \vdash t = \Delta_n.$$

(d) *Alle $\mathcal{N}$-wahren, quantorenfreien geschlossenen Formeln aus $L(Z)$ sind in EZ beweisbar.*

Beweis. (a) Seien $m < n$ in $\mathbb{N}_0$. Dann gilt $EZ \vdash \Delta_m = \Delta_m$ und daher gilt $EZ \vdash (\Delta_m = \Delta_0 \vee \cdots \vee \Delta_m = \Delta_{n-1})$ also $EZ \vdash \Delta_n < \Delta_m$ nach (EZ3). Dies ist die erste Aussage.
Sei nun $m \neq n$, also ohne Einschraenkung $m < n$. **Angenommen**, $EZ \not\vdash \Delta_m \neq \Delta_n$. Dann gibt es ein Modell $\mathcal{A}$ von EZ mit $\mathcal{A} \vDash \Delta_m = \Delta_n$. Nach der ersten Aussage folgt damit, dass $\mathcal{A} \vDash \Delta_m < \Delta_m$. Nach (EZ3) folgt dass $m = 0$ oder $\mathcal{A} \vDash \Delta_m = \Delta_k$ fuer ein $k < m$. Wiederholung des Schlusses mit k statt m endet irgendwann mit $\Delta_n = \Delta_0$, was zu $\mathcal{A} \vDash \Delta_m < \Delta_0$ fuehrt. **Widerspruch** zu (EZ3). Dies beweist die zweite Aussage. Die dritte folgt aehnlich.

(b) folgt aus (a), denn die Interpretationen der Δ_n liefern eine Submodell.

(c) Ist $t = \Delta_n$ fuer ein $n \in \mathbb{N}_0$, so folgt die Behauptung trivialerweise. Ist $t = s + 1$ fuer einen Term s, so gibt es nach Induktionsvoraussetzung ein $n \in \mathbb{N}_0$ so dass $EZ \vdash s = \Delta_n$. Dann folgt $EZ \vdash t = s + 1 = \Delta_n + 1 = \Delta_{n+1}$. Ist $t = s_1 + s_2$ fuer Terme s_1, s_2 so gibt es $n_1, n_2 \in \mathbb{N}_0$ so dass $EZ \vdash s_1 = \Delta_{n_1}$ und $EZ \vdash s_2 = \Delta_{n_2}$. Dann folgt $EZ \vdash t = s_1 + s_2 = \Delta_{n_1+n_2}$. Ist schliesslich $t = s_1 \cdot s_2$, so gibt es n_1, n_2 mit $EZ \vdash s_j = \Delta_{n_j}$, so folgt $EZ \vdash t = s_1 s_2 = \Delta_{n_1 n_2}$.

(d) Sei F eine $\mathcal{N}$-wahre, quantorenfreie geschlossene Formel aus L(Z). **Angenommen,** EZ leitet F nicht her, dann gibt es ein Modell $\mathcal{A}$ von EZ, mit $\mathcal{A} \vDash \neg F$. Dies enthaelt $\mathcal{N}$ als Submodell und da F quantorenfrei und geschlossen ist, folgt $\mathcal{N} \vDash \neg F$, **Widerspruch!** □

Definition 3.2.4. (Σ_1-Formeln) Eine Σ_1 Formel entsteht aus quantorenfreien Formeln durch (wiederholte) Anwendung von $\exists_x$, beschränkten Allquantoren $\forall_{x<t}$ (t ein Term) und den Junktoren $\wedge, \vee$.

Eine Σ_1-Formel **im engeren Sinne** entsteht aus Formeln der Form

$$0 = x,\ a + 1 = b,\ a + b = c,\ a \cdot b = c,\ a = b,\ \neg a = b,\ a < b,\ \neg a < b$$

durch Anwenden von $\wedge, \vee, \exists_x, \forall_{x<t}$.

Bemerkung 3.2.5. Jede Σ_1 Formel ist herleitbar äquivalent zu einer Σ_1-Formel im engeren Sinne. Also, zu jeder Σ_1 Formel F existiert eine Σ_1-Formel G im engeren Sinne, so dass

$$EZ \vdash F \leftrightarrow G.$$

Beweis. Man eliminiert kompliziertere Terme mit Hilfe von Existenzquantoren. Zum

Beispiel ist $(a+1)+b=c+1$ äquivalent zu

$$\exists_{a_1}\exists_{c_1}\, a+1=a_1 \wedge c+1=c_1 \wedge a_1+b=c_1. \qquad \square$$

Satz 3.2.6. *Alle in $\mathcal{N}$ wahren geschlossenen Σ_1-Formeln sind in EZ beweisbar.*

Beweis. Wir zeigen für alle Σ_1-Formeln $F(a_1,\dots,a_k)$ im engeren Sinne, die keine weiteren freien Variablen haben und alle natürlichen Zahlen $n_1,\dots,n_k$, dass

$$\mathcal{N} \vDash F(n_1,\dots,n_k) \quad \Rightarrow \quad EZ \vdash F(\Delta_{n_1},\dots,\Delta_{n_k}).$$

Wir zeigen dies durch Induktion über den Aufbau. Ist F eine Primformel, so folgt es aus Lemma 3.2.3.

Ist $F = G \wedge H$, und gilt $\mathcal{N} \vDash F(\bar{n})$, dann folgt $\mathcal{N} \vDash G(\bar{n})$ und $\mathcal{N} \vDash H(\bar{n})$. Nach Induktionsvoraussetzung folgt dann $EZ \vdash G(\Delta_{\bar{n}})$ und $EZ \vdash H(\Delta_{\bar{n}})$. Da $G(\Delta_{\bar{n}}) \to H(\Delta_{\bar{n}}) \to G(\Delta_{\bar{n}}) \wedge H(\Delta_{\bar{n}})$ eine Tautologie ist, folgt mit zweifachem Modus Ponens, dass $EZ \vdash G(\Delta_{\bar{n}}) \wedge H(\Delta_{\bar{n}})$, also $EZ \vdash F(\Delta_{\bar{n}})$. Der $\vee$-Fall geht ebenso.

Ist $\mathcal{N} \vDash \exists_x \psi(x, \Delta_{\bar{n}})$, so ist $\mathcal{N} \vDash \psi(\Delta_m, \Delta_{\bar{n}})$ für ein $m \in \mathbb{N}_0$. Nach Induktionsvoraussetzung folgt $EZ \vdash \psi(\Delta_m, \Delta_{\bar{n}})$ und daher $EZ \vdash \exists_x \psi(x, \Delta_{\bar{n}})$.

Ist $F(m,\bar{n}) \equiv \forall_{x<m}\psi(x,,\bar{n})$ und gilt $\mathcal{N} \vDash F(m,\bar{n})$, dann ist $\mathcal{N} \vDash \psi(l,\bar{n})$ für alle $l \in \mathbb{N}_0$, $l < m$. Nach Induktionsvoraussetzung ist $EZ \vdash \psi(\Delta_l, \Delta_{\bar{n}})$ für alle $l < m$. Nach (EZ3) folgt daraus

$$EZ \vdash \forall_{x<\Delta_m}\, \psi(x, \Delta_{\bar{n}}). \qquad \square$$

Lemma 3.2.7. *Alle rekursiven Funktionen und alle rekursiv aufzählbaren Relationen sind mit Σ_1-Formeln definierbar.*

Beweis. Ist f rekursiv, so zeigen wir durch Induktion über den Aufbau von f, dass G_f durch Σ_1-Formeln definierbar ist. In Lemma 3.1.2 haben wir gezeigt, dass rekursive Funktionen arithmetisch sind. Der Beweis muss nur an einer Stelle abgeändert werden, naemlich an der Stelle, wenn man zeigt, dass die Σ_1-definierbaren Funktionen unter (R3) abgeschlossen sind. Wir erinnern:

(R3) Sei $f(\bar{x}) = \mu y\ g(\bar{x}, y) = 0$. Dann ist $(\bar{x}, y) \in G_f$ genau dann, wenn

$$(\bar{x}, y, 0) \in G_g \wedge \forall_{z<y}\ (\bar{x}, z, 0) \notin G_g$$

Ist nun G_g durch eine Σ_1-Formel F gegeben, also $(\bar{m}, n, k) \in G_g \Leftrightarrow F(\bar{m}, n, k)$, Dann ist etwa $F(\bar{x}, y, z)$ eine Σ_1 Formel, $F(\bar{x}, y, 0)$ aber nicht. Aber diese letztere Formel ist aequivalent zu der Σ_1-Formel

$$\exists_z z = 0 \wedge F(\bar{x}, y, z).$$

Ebenso ersetzt man im zweiten Teil der Formel den Ausdruck $\forall_{z<y} \neg F(\bar{x}, z, 0)$ durch die Σ_1-Formel

$$\exists_w \neg w = 0 \wedge F(\bar{x}, z, w).$$

Sei nun R eine rekursiv aufzählbare Relation, also

$$R(\bar{x}) \quad \Leftrightarrow \quad \exists_y \tilde{R}(\bar{x}, y)$$

für eine rekursive Relation $\tilde{R}$. Dann ist $\chi_{\tilde{R}}$ rekursiv, also ist der Graph $G_{\chi_{\tilde{R}}}$ durch eine Σ_1-Formel F definierbar, d.h.,

$$\tilde{R}(\bar{x}, y) \Leftrightarrow \chi_{\tilde{R}}(\bar{x}, y) = 1 \Leftrightarrow F(\bar{x}, y, 1) \Leftrightarrow \exists_z F(\bar{x}, y, z) \wedge z = 1.$$

Daher ist

$$R(\bar{x}) \quad \Leftrightarrow \quad \exists_y \exists_z F(\bar{x}, y, z) \wedge z = 1.$$

Die rechte Seite ist eine Σ_1-Formel. □

* * *

3.3 Unentscheidbarkeit von EZ

Satz 3.3.1. *EZ ist unentscheidbar. Jede $\mathcal{N}$-wahre konsistente Erweiterung von EZ ist unentscheidbar.*

Erinnere: T entscheidbar $\Leftrightarrow$ die Menge der in T herleitbaren Formeln ist rekursiv.

Beweis. Sei T eine $\mathcal{N}$-wahre konsistente Erweiterung von EZ. Sei $R(x)$ eine beliebige rekursiv aufzählbare Relation. Dann ist R definiert durch eine Σ_1-Formel F. Es gilt für

jedes $n \in \mathbb{N}_0$

$$R(n) \quad \Leftrightarrow \quad \mathcal{N} \vDash F(\Delta_n) \quad \Leftrightarrow \quad T \vdash F(\Delta_n)$$

Zur zweiten Aequivalenz "$\Leftarrow$" gilt weil T eine $\mathcal{N}$-wahre Theorie ist, die Rueckrichtung gilt, weil jede $\mathcal{N}$-wahre geschlossene Σ_1-Formel schon in EZ herleitbar ist.

Wäre nun T entscheidbar, also $\{\ulcorner Q \urcorner : T \vdash Q\}$ rekursiv, dann wäre auch $\{n : T \vdash F(\Delta_n)\}$ rekursiv und damit wäre $R(n)$ rekursiv, also wäre jede rekursiv aufzählbare Relation in $\mathbb{N}_0$ schon rekursiv, im Widerspruch zu Proposition 2.5.6. □

Lemma 3.3.2 (Fixpunktlemma)**.** *Zu jeder Formel $F(a)$ mit nur einer freien Variablen a gibt es eine Formel Q mit*

$$EZ \vdash Q \leftrightarrow F(\Delta_{\ulcorner Q \urcorner})$$

Beweis. Termeinsetzen wird durch eine rekursive Funktion beschrieben

$$\mathrm{Sub}(\ulcorner F(a) \urcorner, n) = \ulcorner F(\Delta_n) \urcorner$$

Sei Sub in EZ repräsentiert durch die Σ_1-Formel σ. Das heißt, lax ausgedrückt

$$EZ \vdash \mathrm{Sub}(m,n) = k \leftrightarrow \sigma(k,m,n).$$

Genauer müssen natürlich die natürlichen Zahlen hier als Terme interpretiert werden, also

$$EZ \vdash \mathrm{Sub}(\Delta_m, \Delta_n) = \Delta_k \leftrightarrow \sigma(\Delta_k, \Delta_m, \Delta_n).$$

Dann ist also für alle $F(a)$ und alle n,

$$EZ \vdash \forall_x \left(x = \Delta_{\ulcorner F(\Delta_n) \urcorner} \leftrightarrow \sigma(x, \Delta_{\ulcorner F(a) \urcorner}, \Delta_n) \right).$$

Sei nun $F(a)$ gegeben. Wir setzen

$$\rho(a) = \exists_x \left(F(x) \wedge \sigma(x,a,a) \right).$$

Dann ist für alle Formeln $H(a)$ in EZ herleitbar:

$$\begin{aligned} \rho(\Delta_{\ulcorner H(a) \urcorner}) &\leftrightarrow \exists_x \left(F(x) \wedge \sigma(x, \Delta_{\ulcorner H(a) \urcorner}, \Delta_{\ulcorner H(a) \urcorner}) \right) \\ &\leftrightarrow \exists_x \left(F(x) \wedge x = \Delta_{\ulcorner H(\Delta_{\ulcorner H(a) \urcorner}) \urcorner} \right) \\ &\leftrightarrow F(\Delta_{\ulcorner H(\Delta_{\ulcorner H(a) \urcorner}) \urcorner}). \end{aligned}$$

Für $H = \rho$ ergibt sich

$$EZ \vdash \rho\left(\Delta_{\ulcorner \rho(a) \urcorner}\right) \leftrightarrow F\left(\Delta_{\ulcorner \rho(\Delta_{\ulcorner \rho(a) \urcorner}) \urcorner}\right).$$

Also leistet $Q = \rho\left(\Delta_{\ulcorner \rho(a) \urcorner}\right)$ das Gewünschte. □

Korollar 3.3.3. *Jede konsistente Erweiterung von EZ ist unentscheidbar.*

Beweis. Sei T eine entscheidbare Erweiterung von EZ, d.h., die Menge der in T herleitbaren Formeln ist rekursiv. Sei die Menge der Gödelnummern aller in T beweisbaren Formeln in EZ durch die Formel τ repräsentiert, also $EZ \vdash \tau(\Delta_{\ulcorner F \urcorner})$ für in T beweisbare F und $EZ \vdash \neg\tau(\Delta_{\ulcorner F \urcorner})$ für in T unbeweisbare F. Nach dem Fixpunktlemma, angewendet auf $\neg\tau$ gibt es eine Formel δ mit

$$EZ \vdash \delta \leftrightarrow \neg\tau(\Delta_{\ulcorner \delta \urcorner}).$$

Dann gilt einerseits

$$T \not\vdash \delta \quad \Rightarrow \quad EZ \vdash \neg\tau(\Delta_{\ulcorner \delta \urcorner}) \quad \Rightarrow \quad EZ \vdash \delta \quad \Rightarrow \quad T \vdash \delta$$

und andererseits

$$T \vdash \delta \quad \Rightarrow \quad EZ \vdash \tau(\Delta_{\ulcorner \delta \urcorner}) \quad \Rightarrow \quad EZ \vdash \neg\delta \quad \Rightarrow \quad T \vdash \neg\delta,$$

woraus folgt, dass T inkonsistent ist. □

* * *

3.4 Der zweite Unvollständigkeitssatz

Sei T eine rekursiv aufzählbare Erweiterung von EZ, zum Beispiel die Zahlentheorie Z.

Betrachte die Relation $b_T \subset \mathbb{N}_0^2$ gegeben durch $b_T(f,e) \Leftrightarrow f$ ist die Gödelnummer einer Formel und e ist die Gödelnummer eines Beweises in T von f. Betrachte die Relation

$$\mathrm{bew}_T(f) :\Leftrightarrow \exists_{e \in \mathbb{N}_0}\, b(f,e).$$

Dann drückt $\mathrm{bew}_T(\Delta_{\ulcorner \phi \urcorner})$ die T-Beweisbarkeit einer Formel ϕ aus.

Die Relation b_T ist rekursiv aufzählbar. Nach Lemma 3.2.7 gibt es daher eine Σ_1-Formel $B_T(a,b)$ so dass

$$b_T(f,e) \quad \Leftrightarrow \quad B_T(f,e).$$

Sei $\mathrm{Bew}_T(a)$ die Formel $\exists_y B_T(a, y)$. Dann besagt $\mathrm{Bew}_T(\Delta^{\ulcorner}{}_F{}^{\urcorner})$ die T-Beweisbarkeit der Formel F. Sei N eine Formel, deren Negation eine Tautologie ist. Die Formel

$$\mathrm{Kon}_T = \neg\ \mathrm{Bew}(\Delta^{\ulcorner}{}_N{}^{\urcorner})$$

drückt dann die Konsistenz von T aus.

Satz 3.4.1 (Zweiter Unvollständigkeitssatz)**.** *Ist $T \subset T(\mathcal{N})$ rekursiv aufzählbar mit $EZ \subset T$, dann ist* Kon_T *wahr in $\mathcal{N}$ aber nicht beweisbar in T.*

Man kann die Konsistenz einer Theorie nicht innerhalb der Theorie beweisen.

Beweis. Wir stellen zunächst fest, dass T konsistent sein muss, da die Theorie $T(\mathcal{N})$ konsistent ist. Ferner erfuellt Bew_T die **Loeb-Axiome**:

(L1) $T \vdash \phi \quad \Rightarrow \quad T \vdash \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\phi}{}^{\urcorner})$.

(L2) $T \vdash \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\phi}{}^{\urcorner}) \wedge \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\phi\to\psi}{}^{\urcorner}) \to \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\psi}{}^{\urcorner})$.

(L3) $T \vdash \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\phi}{}^{\urcorner}) \to \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\phi}{}^{\urcorner})}{}^{\urcorner})$.

(L3) drückt aus, dass (L1) in T beweisbar ist.

Begruendung: Es handelt sich um wahre Σ_1-Formeln, diese sind in EZ und daher in T beweisbar.

Mit derselben Beguendung gilt auch:

(a) $T \vdash \phi \to \psi \quad \Rightarrow \quad T \vdash \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\phi}{}^{\urcorner}) \to \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\psi}{}^{\urcorner})$.

(b) $T \vdash \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\phi\wedge\psi}{}^{\urcorner}) \leftrightarrow (\mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\phi}{}^{\urcorner}) \wedge \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{\psi}{}^{\urcorner})$.

Nach dem Fixpunktlemma angewendet auf die Formel $\neg\ \mathrm{Bew}_T(a)$ gibt es eine Formel Q so dass

$$T \vdash Q \leftrightarrow \neg\ \mathrm{Bew}_T(\Delta^{\ulcorner}{}_{Q}{}^{\urcorner}).$$

Diese Formel Q behauptet also ihre eigene Unbeweisbarkeit. Wir zeigen, dass tatsächlich

$$T \vdash Q \leftrightarrow \mathrm{Kon}_T\,.$$

Da $\neg N$ eine Tautologie ist, ist $N \to Q$ eine Tautologie. Also folgt aus $T \vdash N \to Q$ und Teil (a) der Folgerung, dass $T \vdash \mathrm{Bew}_T(\Delta_{\ulcorner N \urcorner}) \to \mathrm{Bew}_T(\Delta_{\ulcorner Q \urcorner})$. Durch Kontraposition folgt $T \vdash Q \to \mathrm{Kon}_T$.

Andererseits folgt aus $T \vdash Q \to \neg\, \mathrm{Bew}_T(\Delta_{\ulcorner Q \urcorner})$, dass

$$T \vdash \mathrm{Bew}_T(\Delta_{\ulcorner Q \urcorner}) \to \mathrm{Bew}_T(\Delta_{\ulcorner \neg\, \mathrm{Bew}_T(\Delta_{\ulcorner Q \urcorner}) \urcorner}).$$

Die folgende Formel ist $\mathcal{N}$-wahr und Σ_1 und daher beweisbar, also

$$T \vdash \mathrm{Bew}_T(\Delta_{\ulcorner \neg\, \mathrm{Bew}_T(\Delta_{\ulcorner Q \urcorner}) \urcorner}) \wedge \mathrm{Bew}_T(\Delta_{\ulcorner \mathrm{Bew}_T(\Delta_{\ulcorner Q \urcorner}) \urcorner}) \to \mathrm{Bew}_T(\Delta_{\ulcorner N \urcorner}).$$

Damit folgt $T \vdash \mathrm{Bew}_T(\Delta_{\ulcorner Q \urcorner}) \to \neg\, \mathrm{Kon}_T$ oder $T \vdash \mathrm{Kon}_T \to Q$.

Damit ist $T \vdash Q \leftrightarrow \mathrm{Kon}_T$ bewiesen. Nehmen wir an, dass $T \vdash \mathrm{Kon}_T$. Dann folgt $T \vdash Q$, also $T \vdash \mathrm{Bew}(\Delta_{\ulcorner Q \urcorner})$ nach (L1) aber $T \vdash \neg\, \mathrm{Bew}_T(\Delta_{\ulcorner Q \urcorner})$ nach der Konstruktion von Q. Damit wäre T also inkonsistent. □

* * *

4 Mengenlehre

4.1 Naive Mengenlehre

Die Sprache der Mengenlehre hat nur ein nichtlogisches Symbol $\in$. Die **naive Mengenlehre** hat ein Axiom und ein unendliches Axiomenschema:

- **(Extensionalität)**
  $$(a \in b \leftrightarrow a \in c) \leftrightarrow b = c$$
  (Zwei Mengen sind gleich, wenn sie gleiche Elemente haben).
- **(Volle Komprehension)** Für jede Formel $F = F(a, b_1, \ldots, b_n)$ mit freien Variablen $(a, b_1, \ldots, b_n)$ gilt
  $$\forall_{y_1} \ldots \forall_{y_n}\, \exists_x\, \forall_z\, (z \in x \leftrightarrow F(z, y_1, \ldots, y_n)).$$
  (Mengen sind durch beliebige Formeln definierbar).

Die im Komprehensionsaxiom verlangte Menge x ist nach dem Extensionalitätsaxiom eindeutig bestimmt. Man schreibt sie als

$$\Big\{z \mid F(z, y_1, \ldots, y_n)\Big\}.$$

Satz 4.1.1 (Russel)**.** *Die naive Mengenlehre ist inkonsistent.*

Beweis. Sei $R = \left\{ z \mid z \notin z \right\}$.

1.Fall: $R \in R$, dann folgt, dass R die definierende Formel erfüllen muss, also $R \notin R$, Widerspruch!

2.Fall: $R \notin R$. Damit erfüllt R aber die definierende Formel, also folgt $R \in R$, Widerspruch! □

* * *

4.2 ZFC

Als Alternative hat sich die **Zermelo-Fraenkelsche Mengenlehre** plus Auswahlaxiom durchgesetzt, kurz

ZFC.

Die Axiome sind:
Extensionalität - Aussonderung - Paarmenge - Vereinigung - Potenzmenge - Ersetzung - Fundierung - Unendlichkeit - Auswahl

Und hier nochmal zum Mitschreiben:

- **(Extensionalität)**
$$(a \in b \leftrightarrow a \in c) \leftrightarrow b = c$$
(Zwei Mengen sind gleich, wenn sie gleiche Elemente haben).

- **(Aussonderung)** Teilmengen koennen durch Formeln definiert werden.
Genauer: Für jede Formel $F = F(a, b_1, \ldots, b_n)$ mit freien Variablen $(a, b_1, \ldots, b_n)$ gilt
$$\forall_{y_0} \forall_{y_1} \ldots \forall_{y_n} \exists_x \forall_z (z \in x \leftrightarrow (z \in y_0 \wedge F(z, y_1, \ldots, y_n))).$$
Dies ist eine Art beschränkter Komprehension. Wir schreiben die geforderte Menge x als
$$\left\{ z \in y_0 : F(z, y_1, \ldots, y_n) \right\}.$$
Die Russellsche Antinomie ist hier gelöst, sie bewirkt, dass die Klasse aller

Mengen keine Menge ist. Oder genauer,

$$\neg\, \exists_V\ \forall_y\ y \in V.$$

Denn: gäbe es solches V, so führt die Betrachtung von

$$R = \Big\{ z \in V : z \notin z \Big\}$$

zu demselben Widerspruch wie vorher.

Definition 4.2.1. Eine **Klasse** ist die Gesamtheit aller Mengen x, die eine gegebene Formel $F(x)$ erfüllen, wir schreiben sie als

$$K = \big\{ x \mid F(x) \big\}$$

Formal behandeln wir die Klasse so, dass wir $x \in K$ als Abkürzung für $F(x)$ auffasssen.

Die Teilmengen einer Klasse sind genau die Mengen der Form $K \cap a$ für eine Menge a, oder

$$\big\{ x \in a : F(x) \big\}.$$

- **(Paarmengen)**

$$\forall_{y_1} \forall_{y_2}\ \exists_x\ \forall_z\ z \in x \leftrightarrow (z = y_1 \vee z = y_2).$$

Man schreibt die geforderte Menge als

$$\Big\{ y_1, y_2 \Big\}$$

oder im Spezialfall $y_1 = y_2 = y$ auch als $\big\{ y \big\}$.

Definition 4.2.2. Das **geordnete Paar** von zwei Mengen x, y ist die Menge

$$(x, y) = \Big\{ \big\{ x \big\}, \big\{ x, y \big\} \Big\}.$$

Es gilt

$$ZFC\ \vdash\ (a, b) = (c, d) \leftrightarrow (a = c \wedge b = d).$$

- **(Vereinigung)**

$$\forall_y\ \exists_x\ \forall_z\ z \in x \leftrightarrow \exists_w\ (z \in w \wedge w \in y).$$

(Die Vereinigung über alle Elemente von y existiert). Wir schreiben diese Menge als

$$\bigcup y,$$

oder auch als $\bigcup_{w \in y} w$. Im Spezialfall, dass y nur zwei Elemente a, b hat, schreiben wir die Vereinigung auch als $a \cup b$.

- **(Potenzmenge)** Wir führen die Schreibweise $x \subset y$ als Abkürzung für $\forall_z\, z \in x \to z \in y$ ein. Das Potenzmengenaxiom besagt dann

$$\forall_y\, \exists_x\, \forall_z\, z \in x \leftrightarrow z \subset y.$$

Die geforderte Menge x heißt **Potenzmenge** von y und wird als

$$\mathcal{P}(y)$$

geschrieben.

Lemma 4.2.3. *Aus den Axiomen von ZFC folgt für alle a und b die Existenz des direkten Produktes*

$$a \times b = \big\{(x, y) \mid x \in a \wedge y \in b\big\}.$$

Genauer heißt, das, es gibt eine Menge $a \times b$ deren Elemente genau die geordneten Paare (x, y) mit $x \in a$ und $y \in b$ sind.

Beweis. Wenn $x \in a$ und $y \in b$, dann sind $\{x\}$ und $\{x, y\}$ Elemente von $\mathcal{P}(a \cup b)$. Dann ist $(x, y) = \{\{x\}\{x, y\}\}$ ein Element von $\mathcal{P}(\mathcal{P}(a \cup b))$. Damit ist $a \times b$ eine definierbare Menge nach dem Aussonderungsaxiom. □

Wir definieren Tripel durch $(x, y, z) = ((x, y), z)$ und so weiter.

Definition 4.2.4. Eine **Relation** ist eine Teilmenge $R \subset a \times b$. Eine **Funktion** oder **Abbildung** ist eine Relation $f \subset a \times b$ mit der Eigenschaft

$$\forall_x\, x \in a \to \exists_y\, (x, y) \in f$$

und

$$\forall_x, y_1 y_2\, (x, y_1) \in f \wedge (x, y_2) \in f \to y_1 = y_2.$$

- **(Ersetzung)** Das Bild einer Menge unter einer durch ein Formel ϕ beschriebenen Abbildung ist eine Menge, genauer:

$$\forall_{y, \bar{w}}\big(\forall_u\, \exists! z\, \phi(u, z, \bar{w}) \to \exists_x\, \forall_z\big(z \in x \leftrightarrow \exists_u\, (u \in y \wedge \phi(u, z, \bar{w}))\big)\big).$$

Hier steht $\bar{w}$ für ein Tupel von Variablen und $\exists! x \phi(x)$ steht für $\exists_x \phi(x) \wedge \forall_{x_1} \forall_{x_2}\, (\phi(x_1) \to \phi(x_2) \to x_1 = x_2)$.

- **(Fundierung)**
$$\forall_x \left(\neg\, x = \varnothing \to \exists_{z\in x}\, z \cap x = \varnothing\right).$$
Hierbei steht $a = \varnothing$ fuer $\forall_y\, y \in a \to y \neq y$. Das Fundierungsaxiom drückt aus, dass es keine unendliche Kette $x_1 \ni x_2 \ni x_2 \ni \dots$ geben kann, denn sonst verletzt die Menge $x = \{x_2, x_3, \dots\}$ das Fundierungsaxiom. Es kann daher auch keine periodischen Ketten $1 \in x_2 \in x_3 \in x_1$ geben. Es gibt Versionen der Mengenlehre ohne das Fundierungsaxiom, die muessen aber fuer viele Aussagen unendliche Ketten ausschliessen (regulaere und irregulaere Mengen). Ausserdem gilt dann der Wohlordnungssatz, s.u., nicht.

- **(Unendlichkeit)**
$$\exists_x\, (\varnothing \in x \wedge \forall_{z\in x}\, z \cup \{z\} \in x).$$

- **(Auswahl)**
$$\forall_x\, (\neg\, \varnothing \in x \to \exists_{f:x\to\bigcup x}\, \forall_{z\in x}\;\; f(z) \in z).$$

* * *

4.3 Die natürlichen Zahlen

Definition 4.3.1. Für jede natürliche Zahl $n \in \mathbb{N}_0$ definieren wir induktiv

$$\underline{n} = \{\underline{0}, \underline{1}, \dots, \underline{n-1}\}.$$

das heißt also

$$\begin{aligned}
\underline{0} &= \varnothing,\\
\underline{1} &= \{\varnothing\}\\
\underline{2} &= \{\varnothing, \{\varnothing\}\}\\
\underline{3} &= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}.
\end{aligned}$$

Wir schreiben $s(x)$ für den **Nachfolger** $s(x) = x \cup \{x\}$.

Lemma 4.3.2. *Für jedes $n \in \mathbb{N}_0$ gilt*

$$\mathrm{ZFC} \;\vdash\; \underline{n+1} = s(\underline{n}).$$

Ist $n \neq m$, so gilt

$$\mathrm{ZFC} \;\vdash\; \underline{m} \neq \underline{n}.$$

Genauer gilt

$$m < n \Rightarrow \mathrm{ZFC} \vdash \underline{m} \in \underline{n},$$
$$m \geq n \Rightarrow \mathrm{ZFC} \vdash \neg\, \underline{m} \in \underline{n}.$$

Beweis. Eine leichte Induktion. □

Definition 4.3.3. Sei $<$ eine Relation auf a, also eine Teilmenge von $a \times a$.

1. $<$ ist eine **partielle Ordnung**, wenn
   (a) $\neg\, x < x$ für alle $x \in a$,
   (b) $(x < y) \wedge (y < z) \to (x < z)$ für alle $x, y, z \in a$.
2. Eine partielle Ordnung $<$ auf a heißt **linear**, wenn für alle $x, y \in a$ gilt

$$(x < y) \ \vee \ (x = y) \ \vee \ (y < x).$$

Definition 4.3.4. Eine Menge x heißt **transitiv**, falls alle ihre Elemente auch Teilmengen sind:

$$z \in y \in x \ \to \ z \in x.$$

Definition 4.3.5. x heißt **natürliche Zahl**, wenn

1. x transitiv ist,
2. $\in$ eine lineare Ordnung auf x definiert,
3. jede nicht-leere Teilmenge von x in dieser Ordnung ein größtes und ein kleinstes Element besitzt.

Lemma 4.3.6. (a) *Ist x eine natürliche Zahl, so sind alle Elemente von x natürliche Zahlen.*

(b) *$\underline{0}$ ist eine natürliche Zahl. Ist x eine natürliche Zahl, so auch $s(x)$.*

(c) *Jede natürliche Zahl $x \neq 0$ hat die Form $s(y)$ für eine natürliche Zahl y, genauer ist y das größte Element von x.*

Beweis. Klar bis auf (c) vielleicht. Sei also $x \neq \varnothing$ eine natürliche Zahl und sei y das größte Element von x. Wir behaupten, dass $x = s(y) = y \cup \{y\}$. Klar ist, dass $s(y) \subset x$. Sei $z \in x$ beliebig. Da y das größte Element von x ist, ist also $z = y$ oder $z < y$. Aus $z = y$ folgt

$z \in s(y) = y \cup \{y\}$ und aus $z < y$, also $z \in y$ folgt ebenfalls $z \in s(y)$. Zusammen folgt $s(y) = x$. □

Sei ω die Klasse aller natürlichen Zahlen.

Lemma 4.3.7. *ω ist eine Menge.*

Beweis. Sei x eine Menge wie im Unendlichkeitsaxiom, also

$$\varnothing \in x \wedge \forall_{z \in x} \quad z \cup \{z\} \in x.$$

Wir zeigen, dass ω eine Teilmenge von x ist. Die Behauptung folgt dann aus dem Aussonderungsaxiom. Nehmen wir an, es gäbe ein $a \in \omega \setminus x$. Sei b das kleinste Element von $s(a)$, das nicht zu x gehört. Dann sind alle Elemente von b Elemente von x. Weil $b \notin x$, ist b nichtleer. Also hat b die Form $s(c)$. Dann ist $c \in x$, woraus aber auch $b \in x$ folgt. Widerspruch! □

Lemma 4.3.8 (Induktion)**.** *Eine Menge, die $\underline{0}$ enthält und unter s abgeschlossen ist, enthält alle natürlichen Zahlen.*

Beweis. Folgt aus dem Beweis des letzten Lemmas. □

* * *

Lemma 4.3.9. *Wir schreiben $<$ für die $\in$ Relation auf den natürlichen Zahlen.*

(a) *$<$ ist eine lineare Ordnung auf ω. Jede nicht-leere Teilmenge von ω hat ein kleinstes Element.*

(b) *Für jedes $n \in \omega$ ist $s(n)$ der unmittelbare Nachfolger von n, d.h., $s(n)$ ist das kleinste Element mit $s(n) > n$.*

(c) *Jedes $0 < n \in \omega$ hat einen unmittelbaren Vorgänger.*

Beweis. Alle Aussagen folgen leicht, bis auf die Vergleichbarkeit zweier natürlicher Zahlen. Sei also $m \in \omega$ fest. Wir zeigen durch Induktion, dass jedes $n \in \omega$ mit n vergleichbar ist. Zunächst sei $0 \neq m$ angenommen, dann ist zu zeigen, dass $0 < m$, also $0 \in m$. Nach Definition hat m ein kleinstes Element m_0. Jedes Element x von m_0 wäre wegen der Transitivität auch ein Element von m und daher muss m_0 die leere Menge sein, also folgt $0 < m$.

Sei nun also $n \in \omega$ mit m vergleichbar. Sei zuerst $n < m$, also $n \in m$. Ist n das größte Element von m, dann ist $s(n) = m$ nach Lemma 4.3.6. Ist $n \geq m$, dann auch

$s(n) \geq s(m) > m$. Damit ist $s(n)$ ebenfalls mit m vergleichbar und nach dem Induktionslemma 4.3.8 sind alle natürlichen Zahlen mit m vergleichbar. □

Satz 4.3.10 (Rekursionssatz)**.** *Seien zwei Funktionen $g : A \to B$ und $h : A \times \omega \times B \to B$ gegeben. Dann existiert ein eindeutig bestimmtes $f : A \times \omega \to B$ mit*

$$f(a,0) = g(a),$$
$$f(a,s(n)) = h(a,n,f(a,n)).$$

Beweis. Sei $a \in A$ fest. Durch Induktion über m zeigt man, dass es für jedes $m \in \omega$ genau ein $f' : s(m) \to B$ gibt mit $\phi(a,m,f')$, wobei

$$\phi(a,m,f') = \big[f'(0) = g(a) \ \wedge \ \forall_{n<m}\, f'(s(n)) = h(a,n,f'(n))\big].$$

Wir definieren jetzt

$$f = \big\{(a,m,b) \in A \times \omega \times B : \exists_{f'}\, \phi(a,m,f') \wedge f'(m) = b\big\}.$$ □

* * *

4.4 Ordinalzahlen

Definition 4.4.1. Eine **Ordinalzahl** ist eine transitive Menge, die durch $\in$ linear geordnet wird.

Alle natürlichen Zahlen sind Ordinalzahlen. Wir bezeichnen mit Ω die Klasse der Ordinalzahlen.

Lemma 4.4.2. (a) *Ω wird durch $\in$ linear geordnet. Wir schreiben dies Ordnung als $<$.*

(b) *Jede nicht-leere Teilklasse hat ein minimales Element.*

(c) *Jede Ordinalzahl α ist die Menge ihrer Vorgänger:*

$$\alpha = \big\{\beta \in \Omega : \beta < \alpha\big\}.$$

(d) *Ω ist keine Menge.*

Beweis. (a) Das Fundierungsaxiom impliziert, dass jede Teilmenge einer Ordinalzahl ein kleinstes Element hat. Sei α eine Ordinalzahl und sei $S \subsetneq \alpha$ ein **Abschnitt**, d.h., $x < y \in S \to x \in S$. Sei β das kleinste Element von $\alpha \setminus S$. Dann folgt $S = \beta$. Das heisst also, jeder Abschnitt einer Ordinalzahl ist selbst eine Ordinalzahl. Umgekehrt ist jede Ordinalzahl $\beta \in \alpha$ ein Abschnitt, wie aus der Transitivitaet folgt.

Wenn nun α, β zwei Ordinalzahlen sind, dann ist $S = \alpha \cap \beta$ ein Abschnitt von α und β. Wäre $S \neq \alpha$ und $S \neq \beta$, dann müsste S ein Element von α und β sein, also $S \in \alpha \cap \beta = S$, was dem Fundierungsaxiom widerspricht. Ist aber $S = \alpha$, dann folgt $\alpha \leq \beta$, woraus folgt, dass je zwei Ordinalzahlen vergleichbar sind.

(b) folgt aus dem Fundierungsaxiom.

(c) folgt aus dem Beweis von (a).

(d) Wenn Ω eine Menge wäre, so wäre Ω eine Ordinalzahl und müsste sich selbst als Element enthalten. □

Definition 4.4.3. Ist α eine Ordinalzahl, so auch ihr **Nachfolger**: $s(\alpha) = \alpha \cup \{\alpha\}$. Wir schreiben auch $\alpha + 1$ für $s(\alpha)$. Eine Ordinalzahl > 0, die keine Nachfolgerzahl ist, heißt **Limeszahl**.

Definition 4.4.4. Eine partielle Ordnung $<$ auf einer Menge a heißt **Wohlordnung**, falls jede Teilmenge ein kleinstes Element hat.

Lemma 4.4.5 (Lemma von Zorn)**.** *Sei $a \neq \varnothing$ eine Menge, $<$ eine partielle Ordnung auf a mit der Eigenschaft, dass jede linear geordnete Teilmenge L eine obere Schranke hat. Dann hat a maximale Elemente, d.h.,*

$$\exists_{x \in a}\ \forall_{z \in a}\ \neg\,(x < z).$$

Beweis. **Angenommen**, a hat kein maximales Element. Dann gibt es zu jeder linear geordneten Teilmenge L eine obere Schranke $s \in a$, die nicht in L liegt.

Sei K die Menge aller linear geordneten Teilmengen von a. Wir definieren eine Abbildung $h : K \to \mathcal{P}(a)$, die jeder linear geordneten Teilmenge L die Menge aller ihrer oberen Schranken zuordnet, die nicht in L liegen, also

$$h(L) = \left\{x \in a : x \notin L,\ x \geq z\ \forall_{z \in L}\right\}.$$

Nach dem Auswahlaxiom gibt es eine Abbildung $g : \mathcal{P}(a) \setminus \{\varnothing\} \to a$ so dass $g(z) \in z$ für jedes z. Die Abbildung $f = g \circ h$ hat dann die Eigenschaft, dass sie jeder linear geordneten Teilmenge $L \subset a$ eine obere Schranke $f(L) \notin L$ zuordnet. Dies geht insbesondere für einelementige Mengen, in welchem Fall wir $f(x)$ statt $f(\{x\})$

schreiben. Es gilt dann also immer $f(x) > x$. Sei $x_0 \in a$ beliebig Wir behaupten, dass es genau eine Abbildung $F : \Omega \to a$ gibt so dass

$$\begin{aligned} F(\varnothing) &= x_0, \\ F(\alpha) &= f\left(\left\{F(\beta) : \beta < \alpha\right\}\right). \end{aligned}$$

Zur Eindeutigkeit: Sei $H : \Omega \to a$ eine zweite Abbildung mit dieser Eigenschaft. Sei X die Klasse aller Ordinalzahlen β, für die gilt $F(\alpha) = H(\alpha)$ für alle $\alpha < \beta$. Wäre $X \neq \Omega$, dann gäbe es ein kleinstes Element $\alpha \in \Omega \setminus X$. Für dieses gilt dann aber

$$\begin{aligned} F(\alpha) &= f\left(\left\{F(\beta) : \beta < \alpha\right\}\right) \\ &= f\left(\left\{H(\beta) : \beta < \alpha\right\}\right) \\ &= H(\alpha) \end{aligned}$$

was einen Widerspruch darstellt, also ist $X = \Omega$. Die Existenz zeigt man ebenso, indem man jetzt X als die Menge aller Ordinalzahlen α definiert, für die ein $F : \alpha \to a$ mit der genannten Eigenschaft existiert.

Nun ist $F : \Omega \to a$ ordnungstreu also injektiv, identifiziert also Ω mit einer Teilmenge von a. Genauer gilt: es gibt eine Formel in ZFC, die die Elemente von Ω beschreibt. Daher gibt es eine Formel, die das Bild von F beschreibt. Dies liegt in einer Obermenge a, also ist nach dem Extensionalitaetsaxiom $F(\Omega)$ eine Menge. Die Umkehrfunktion $F^{-1} : F(\Omega) \to \Omega$ ist in ZFC durch Formeln beschreibbar, existiert also, damit ist das Bild, also Ω, nach dem Ersetzungsaxiom eine Menge. **Widerspruch!** □

Satz 4.4.6. *Sei $(A, <)$ eine wohlgeordnete Menge, dann gibt es genau eine Ordinalzahl α, so dass es einen Ordnungsisomorphismus $f : A \to \alpha$ gibt. Auch dieses f ist eindeutig festgelegt.*

Man kann also die Ordinalzahlen auch mit den Isomorphieklassen von Wohlordnungen identifizieren.

Beweis. Für $a \in A$ sei $S_a = \{b \in A : b < a\}$ der Abschnitt von a. Nach dem Lemma von Zorn hat die Menge aller Abschnitte S, die zu einem Ordinalzahlabschitt isomorph sind, maximale Elemente. Sei S ein solches, sei $f : S \to \alpha$ ein Isomorphismus für ein $\alpha \in \Omega$, nimm an $S \neq A$ und sei x das kleinste Element von $A \setminus S$. Definiere dann $f(x) = \alpha$. Dies definiert eine Fortsetzung von f, die es nicht geben dürfte, also folgt $S = A$. Die Eindeutigeit folgt ähnlich. □

Satz 4.4.7 (Wohlordnungssatz)**.** *Auf jeder Menge existiert eine Wohlordnung.*

Beweis. Sei A eine Menge und S die Menge aller Paare (U, f), wobei $U \subset A$ und f eine Bijektion $U \to \alpha$ für eine Ordinalzahl α. Wir sagen $(U, f) < (V, g)$, falls $U \subsetneq V$ und $g|_U = f$. Man sieht leicht, dass in S jede linear geordnete Teilmenge eine obere Schranke besitzt. Nach dem Lemma von Zorn hat S ein maximales Element (U, f). Ist $U \neq A$, so sei $x_0 \in A \setminus U$ und definiere $f(x_0) = \alpha$, wobei $f : U \xrightarrow{\cong} \alpha$. Dies setzt f fort, Widerspruch! Also ist $U = A$. Die Bijektion $f : A \to \alpha$ transportiert nun die Wohlordnungsstruktur von α nach A. □

Satz 4.4.8. *In der Theorie ZF, also der Mengenlehre ohne Auswahlaxiom, sind aequivalent*

(a) *Das Auswahlaxiom.*

(b) *Das Lemma von Zorn.*

(c) *Der Wohlordnungssatz.*

Beweis. (a)⇒(b): Dies ist der Beweis von Lemma 4.4.5.

(b)⇒(c): Dies ist der Beweis von Satz 4.4.7.

(c)⇒(a): Das Auswahlaxiom laesst sich so formulieren, dass es zu jeder Menge $M \neq \varnothing$ eine Funktion $f : \mathcal{P}(M) \setminus \{\varnothing\} \to M$ gibt mit $f(T) \in T$ fuer jedes T. Setzt man den Wohlordnungssatz voraus, kann man auf M eine Wohlordnung installieren und definiert dann

$$f(T) := \text{kleinstes Element von } T.$$

Dies ist dann die gewuenschte Funktion. □

Bemerkung 4.4.9. Der Wohlordnungssatz laesst sich auch so formulieren, dass es zu jeder Menge M einen Ordinalzahlabschnitt S gibt, der zu M gleichmaechtig ist. Indem man dasselbe auf die Potenzmenge $\mathcal{P}(M)$ anwendet, findet man:

Zu jeder Menge M gibt es einen Ordinalzahlabschnitt S, dessen Kardinalitaet $> |M|$ *ist.*

Diese Aussage wiederum gibt Anlass zu der Beweistechnik der **Transfiniten Induktion** oder auch **Ordinalzahlinduktion** genannt. Alles, was man ueblicherweise

mit dem Lemma von Zorn beweist, kann man auch mit Transfiniter Induktion beweisen.

Beispiel 4.4.10. Als Beispiel benutzen wir Transfinite Induktion, um zu zeigen, dass jeder Vektorraum eine Basis (=linear unabhaengiges Erzeugendensystem) hat.

Wir nehmen an, es gebe einen Vektorraum V, der keine Basis hat. Wir ordnen dann jeder Ordinalzahl ω eine linear unabhanegige Teilmenge $V(\omega)$ zu. Fuer $\omega = 1$ waehlen wir irgendeinen Vektor $v_1 \neq 0$ und setzen $V(1) = \{v_1\}$. Sei ω eine Ordinalzahl und $V(\omega)$ bereits definiert. Da $V(\omega)$ keine Basis sein kann, gibt es einen linear unabhangigen Vektor w und wir setzen $V(\omega + 1) = V(\omega) \cup \{w\}$. Ist λ eine Limeszahl, dann setzen wir

$$V(\lambda) = \bigcup_{\omega<\lambda} V(\omega).$$

Man beachte, dass nach Konstruktion $|V(\omega)| = |\omega|$ gilt. Dies kann aber nicht sein, da es ein ω gibt mit $|\omega| > |V|$. Also hat jeder Vektorraum eine Basis.

* * *

4.5 Kardinalzahlen

Definition 4.5.1. Zwei Menge A, B heissen **gleichmächtig**, geschrieben $A \sim B$, falls es eine Bijektion zwischen ihnen gibt.

Wir schreiben $A \lhd B$, falls es eine Injektion $A \hookrightarrow B$ gibt.

Satz 4.5.2. (a) *Sind A und B nichtleere Mengen, so gibt es genau dann eine Injektion $B \hookrightarrow A$ wenn es eine Surjektion $A \twoheadrightarrow B$ gibt.*

(b) *Sind M, N Mengen und gibt es surjektive Abbildungen $\phi : M \to N$ und $\psi : N \to M$, dann gibt es eine Bijektion $b : M \xrightarrow{\cong} N$.*

Beweis. (a) Sei $\phi : A \to B$ surjektiv. Nach dem Auswahlaxiom wählen wir zu jedem $b \in B$ ein Urbild $\psi(b) \in A$, so erhalten wir eine Injektion $\psi : B \to A$. Sei umgekehrt eine Injektion $\psi : B \to A$ gegeben und sei $b_0 \in B$ ein festes Element. Definiere $\phi : A \to B$ durch

$$\phi(a) = \begin{cases} b & a = \psi(b), \\ b_0 & a \notin \mathrm{Bild}(\psi). \end{cases}$$

Dann ist ϕ eine Surjektion.

(b) Nach Teil (a) können wir annehmen, dass es injektive Abbildungen $\phi : M \hookrightarrow N$ und $\psi : N \hookrightarrow M$ gibt. Setze $M_0 = M$ und $N_0 = N$ und $N_{j+1} = \phi(M_j)$ sowie $M_{j+1} = \psi(N_j)$. Sei schließlich $M_\infty = \bigcap_j M_j$ und $N_\infty = \bigcap_j N_j$. Wir stellen fest

(i) $M_{j+1} \subset M_j$ und ebenso für N.

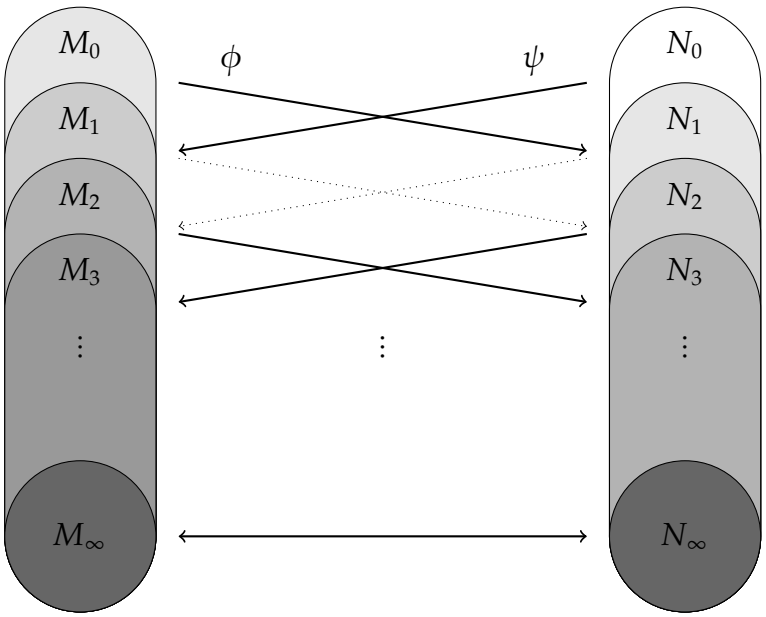
(ii) M ist die disjunkte Zerlegung aus M_∞ und $M_j \setminus M_{j+1}$ für $j = 0, 1, \ldots$ und ebenso für N.

(iii) ϕ ist eine Bijektion $M_\infty \to N_\infty$.

(iv) ϕ ist eine Bijektion $M_j \setminus M_{j+1} \to N_{j+1} \setminus N_{j+2}$ und ebenso für ψ mit M und N vertauscht.

Wir beweisen (i) durch eine (leichte) Induktion nach j. Damit ist auch (ii) klar. (iii) folgt sofort und ebenso (iv). Wir definieren nun eine Bijektion $b : M \to N$ durch

$$b(x) = \begin{cases} \phi(x) & x \in M_\infty, \\ \phi(x) & x \in M_{2j} \setminus M_{2j+1},\ j \geq 0, \\ \psi^{-1}(x) & x \in M_{2j+1} \setminus M_{2j+2},\ j \geq 0. \end{cases}$$



Man sieht leicht ein, dass b eine Bijektion ist. □

Die Kardinalität $|M|$ der Menge M ist die kleinste Ordinalzahl, die zu M gleichmächtig ist.

Lemma 4.5.3.

$$\exists\, A \xrightarrow{\cong} B \Leftrightarrow |A| = |B|.$$
$$\exists\, A \hookrightarrow B \Leftrightarrow |A| \leq |B|.$$

Beweis. Die erste Aussage folgt, weil ~ eine Aequivalenzrelation ist.

Fuer die zweite Auusage betrchten wir das Diagramm

$$\begin{array}{ccc} A & \xrightarrow{\sim} & |A| \\ \downarrow & & \downarrow \\ B & \xrightarrow{\sim} & |B| \end{array}$$

Da die waagrechten Pfeile Bijektionen sind, existiert die eine senkrechte Inklusion genau dann, wenn die andere existiert. □

Satz 4.5.4. *Für jede Menge A gilt* $|\mathcal{P}(A)| > |A|$.

Beweis. **Angenommen,** es gebe eine Surjektion $f : A \to \mathcal{P}(A)$. Sei dann

$$S = \{a \in A : a \notin f(a)\}.$$

Dann gibt es ein $b \in A$ mit $f(b) = S$.

1. Fall. $b \in S$: Dann folgt $b \notin f(b) = S$ **Widerspruch!**

2.Fall. $b \notin S$: Dann erfüllt b das Kriterium, das S definiert, also $b \in S$, **Widerspruch!** □

* * *

4.6 Unvollstaendigkeit der Mengenlehre

In der Mengenlehre lassen sich die zahlentheoretischen Operationen ausdruecken. Zunaechst sei $\mathrm{Ord}(a)$ die Formel

$$\left(\forall_{x,y\in a}\ (x \in y \vee y \in x \vee x = y)\right) \wedge \left(\forall_{x,y}(x \in y \in a \to x \in a)\right).$$

Diese Formel drueckt aus, dass a eine Ordinalzahl ist. Die Formel $\mathrm{Bij}(x,y) :\equiv$

$$\exists_z \left((z \subset x \times y) \wedge (\forall_{a\in x}\ \exists!(b \in y)\ (a,b) \in z) \wedge \left(\forall_{b\in y}\exists!_{a\in x}(a,b) \in z\right)\right),$$

wobei $z \subset y$ fuer $\forall_x\ x \in z \to x \in y$ steht, drueckt aus, dass es eine Bijektion zwischen x und y gibt. Aus dem Auswahlaxiom folgt

$$\mathrm{ZFC} \vdash\ \forall_x\ \exists_y\ \mathrm{Ord}(y) \wedge \mathrm{Bij}(x,y).$$

Ebenso folgt, dass in ZFC herleitbar ist, dass es eine kleinste solche Ordinalxzahl z gibt. Wir verwenden die Abkuerzung $z = |x|$ fuer diese kleinste Ordninalzahl. Wir definieren dann $x \cdot y$ durch

$$z = x \cdot y \ \Leftrightarrow\ z = |x \times y|$$

Dies zeigt, dass die Multiplikation auf $\mathbb{N}_0$ (und auf allen Kardinalzahlen) in der Sprache von ZFC beschreibbar ist. Ein gleiches gilt fuer die Addition und fuer $<$ sowieso.

Man stellt fest, dass alle Axiome der einfachen Zahlentheorie EZ in ZFC herleitbar sind.

Satz 4.6.1. *Fuer jede Formel $F(a)$ aus der Sprache der Mengenlehre gibt es eine Formel Q, so dass*

$$\mathrm{ZFC} \vdash\ Q \leftrightarrow F(\ulcorner Q \urcorner).$$

Hierbei steht $\ulcorner Q \urcorner$ fuer die Goedelzahl von Q, aufgefasst als ein Element von $\mathbb{N}_0$, einer Teilmenge der Menge aller geschlossenen Terme von ZFC.

Beweis. Da wir die elementare Zahlentheorie EZ in ZFC herleitbar ist, kann man den Beweis von Lemma 3.3.2 umschreiben und erhaelt einen Beweis dieses Satzes. □

Da man jedes rekursiv aufzaehlbare Praedikat durch eine EZ-Formel beschreiben kann, kann man es auch durch eine ZFC-Formel beschreiben. Sei N eine Formel in ZFC, so dass $\neg N$ eine Tautologie ist. Sei dann

$$\mathrm{Kon}_{\mathrm{ZFC}} :=\ \neg\ \mathrm{Bew}_{\mathrm{ZFC}}(N)$$

Satz 4.6.2. *Wenn ZFC konsistent ist, ist* $\mathrm{Kon}_{\mathrm{ZFC}}$ *nicht in ZFC beweisbar.*

Beweis. Umschreiben des Beweises des zweiten Unvollstaendigkeitssatzes der Arithmetik. □