# Logik für Studierende der Informatik

## Kurzskript

A. Martin-Pizarro

Albert-Ludwigs-Universität Freiburg
Wintersemester 2020-2021

pizarro@math.uni-freiburg.de

19. Januar 2021

**Anmerkungen.**

Dieses Kurzskript ist während den im Wintersemester 2018/19 und 2020/2021 an der Albert-Ludwigs-Universität in Freiburg gehaltenen Vorlesung „Logik für Studierende der Informatik“ sowie der im Sommersemester 2019 gehaltenen Vorlesung „Mathematische Logik“ entstanden und stark geprägt von den Skripten meiner Kollegen Martin Ziegler und Markus Junker. Deren Einflüsse sind nicht zu trennen und können nicht einzeln dargelegt werden.

Zu meinem eigenen Beitrag gehören sicherlich die zahlreichen Fehler, welche es im Skript definitiv geben wird. Ich bin sehr dankbar über die Mitteilung solcher Fehler und Ungenauigkeiten. Insbesondere bedanke ich mich bei Herrn Michael Lösch für sein aufmerksames Korrekturlesen und seine Geduld, sowie bei Herrn Arnt-Jonas Trabert, Herrn Patrick Meurin und Herrn Sören Andres.

# Inhaltsverzeichnis

# Kapitel 1

# Aussagenlogik

In diesem Abschnitt werden wir die Grundlagen der aristotelischen Aussagenlogik einführen. Dabei gelten das Zweiwertigkeitsprinzip (eine Aussage ist entweder wahr oder falsch) und das Prinzip des ausgeschlossenen Dritten (Beweise ad absurdum oder Widerspruchsbeweise sind gültige Beweise), im Gegensatz zum mathematischen Konstruktivismus bzw. Intuitionismus.

## 1.1 Formeln und Tautologien

**Notation.** Wir haben unendlich viele *Aussagenvariablen* (oder *Atome*), welche mit $A_1, A_2, \ldots$ bezeichnet werden. Falls wir nur endlich viele Variablen betrachten, werden wir möglicherweise eher $A$, $B$, $C$ usw. oder $P$, $Q$, $R$, usw. verwenden.

**Definition 1.1.** Die Klasse aller *aussagenlogischen Formeln* ist die kleinste Kollektion $\mathcal{F}$ aller Ausdrücke, welche alle Aussagenvariablen enthält, sodass

- wenn $P$ in $\mathcal{F}$ liegt, so liegt $\neg P$ in $\mathcal{F}$ (*Negation*);
- wenn $P$ und $Q$ in $\mathcal{F}$ liegen, so liegt $(P \vee Q)$ in $\mathcal{F}$ (*Disjunktion*).

Insbesondere haben wir die Eindeutigkeit der Darstellung: Jede aussagenlogische Formel $P$ lässt sich eindeutig schreiben, das heißt, es existieren entweder

- eine eindeutige Aussagenvariable $A_i$ mit $P = A_i$. Wir sagen, dass $P$ der Stufe 0 ist; oder
- eine eindeutige aussagenlogische Formel $Q$, sodass $P = \neg Q$. Wir sagen, dass $P$ der Stufe $n + 1$ ist, wenn $Q$ der Stufe $n$ ist; oder
- eindeutige aussagenlogischen Formeln $Q$ und $R$, sodass $P = (Q \vee R)$. Wir sagen, dass $P$ der Stufe $n + 1$ ist, wobei $n$ das Maximum der Stufen von $Q$ und $R$ ist.

**Bemerkung 1.2.** Mit Hilfe der Stufe einer Formel können wir Eigenschaften der Menge der Formeln zeigen, indem wir sie induktiv (siehe Appendix A) über den Aufbau von Formeln zeigen. Insbesondere gelten Eigenschaften, welche für alle Atome gelten und unter Negation und Disjunktion erhalten bleiben, für alle aussagenlogischen Formeln.

**Notation.** Wir werden folgende Abkürzungen verwenden, wobei wir die Eindeutigkeit der Darstellung dementsprechend verlieren:

- $(P \wedge Q) = \neg(\neg P \vee \neg Q)$ (*Konjunktion*).
- $(P \longrightarrow Q) = (\neg P \vee Q)$ (*Implikation*).
- $(P \longleftrightarrow Q) = \big((P \longrightarrow Q) \wedge (Q \longrightarrow P)\big)$ (*Äquivalenz*).

**Definition 1.3.** In aristotelischer Logik ist $\{0,1\}$ als geordnete Menge (mit $0 < 1$) die Menge der Wahrheitswerte. Eine *Belegung* $\beta$ ist eine Abbildung

$$\beta : \{A_i\}_{i\in\mathbb{N}} \to \{0,1\}.$$

Jede Belegung $\beta$ lässt sich induktiv nach den folgenden Regeln eindeutig auf die Menge aller aussagenlogischen Formeln fortsetzen:

$$\beta(\neg P) = 1 - \beta(P) \text{ und } \beta((P \vee Q)) = \max\{\beta(P), \beta(Q)\}.$$

Durch Induktion über den Aufbau von Formeln zeigt man leicht folgendes Lemma:

**Lemma 1.4.** *Wenn zwei Belegungen $\beta_1$ und $\beta_2$ auf der endlichen Menge der Aussagenvariablen, welche in der aussagenlogischen Formel $P$ vorkommen, übereinstimmen, so gilt $\beta_1(P) = \beta_2(P)$.*

**Bemerkung 1.5.** Eine anschauliche Methode, um zu sehen welche Wahrheitswerte eine aussagenlogische Formel bekommen kann, wird mit Hilfe der Wahrheitstafel gegeben. Zum Beispiel:

| $A_1$ | $A_2$ | $\neg A_1$ | $(A_1 \vee A_2)$ | $(A_1 \wedge A_2)$ | $(A_1 \longrightarrow A_2)$ | $(A_1 \longleftrightarrow A_2)$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 |

Falls in der aussagenlogischen Formel $n$ Aussagenvariablen vorkommen (siehe Lemma 1.4), steigt die Komplexität der Wahrheitstafel mit Ordnung $2^n$.

**Definition 1.6.** Eine aussagenlogische Formel $P$ ist eine *Tautologie*, falls $\beta(P) = 1$ für alle Belegungen $\beta$.
Zwei aussagenlogische Formeln $P$ und $Q$ sind *logisch äquivalent*, bezeichnet als $P \sim Q$, falls $(P \longleftrightarrow Q)$ eine Tautologie ist.

**Bemerkung 1.7.** Die aussagenlogischen Formeln $P$ und $Q$ sind genau dann logisch äquivalent, wenn $\beta(P) = \beta(Q)$ für alle Belegungen $\beta$.

Dass $P$ und $Q$ logisch äquivalent sind bedeutet nicht, dass $P$ und $Q$ als Ausdrücke gleich sind!! Zum Beispiel:

- $\big((P \vee Q) \vee R\big)$ ist logisch äquivalent zu $\big(P \vee (Q \vee R)\big)$, aber die beiden Formeln sind im formellen Sinne verschieden.
- $\neg\neg P \sim P$ aber $\neg\neg P \neq P$ als Aussagenformel.

**Bemerkung 1.8.** Logische Äquivalenz definiert eine Äquivalenzrelation (siehe Appendix B) auf der Klasse der aussagenlogischen Formeln. Mit $\top$ bezeichnen wir die Äquivalenzklasse einer (bzw. jeder) Tautologie und mit $\bot$ die Äquivalenzklasse einer (bzw. jeder) aussagenlogischen Formel, deren Negation eine Tautologie ist, zum Beispiel $(A_1 \wedge \neg A_1)$.

Wir können dementsprechend Ausdrücken der Form $(P \wedge \top)$ oder $(P \vee \top)$ einen Wahrheitswert zuordnen und behandeln diese Symbole formell als aussagenlogische Formeln.

**Bemerkung 1.9.**

- Negationsregeln
  - $\neg\neg P \sim P$.
  - $(P \vee \neg P) \sim \top$ (*Prinzip des ausgeschlossenen Dritten*).
  - $(P \wedge \neg P) \sim \bot$ (*Prinzip des ausgeschlossenen Widerspruchs*).
- Distributivitätsgesetze:
  - $\big((P \vee Q) \wedge R\big) \sim \big((P \wedge R) \vee (Q \wedge R)\big)$.
  - $\big((P \wedge Q) \vee R\big) \sim \big((P \vee R) \wedge (Q \vee R)\big)$.
- Kontraposition:
  - $(P \longrightarrow Q) \sim (\neg Q \longrightarrow \neg P)$.
- Inferenz und *Modus Ponens*:
  - $\Big(\big((P \longrightarrow Q) \wedge (Q \longrightarrow R)\big) \longrightarrow (P \longrightarrow R)\Big) \sim \top$.
  - $\Big(\big(P \wedge (P \longrightarrow Q)\big) \longrightarrow Q\Big) \sim \top$.

## 1.2 Normalformen

**Notation.** Ab jetzt werden wir folgende Abkürzungen verwenden:

- $(P_1 \wedge P_2 \wedge \ldots \wedge P_n)$ oder $(\bigwedge_{i=1}^{n} P_i)$ für die Formel $((\ldots(P_1 \wedge P_2) \wedge \ldots) \wedge P_n)$.
- $(P_1 \vee P_2 \vee \ldots \vee P_n)$ oder $(\bigvee_{i=1}^{n} P_i)$ für die Formel $((\ldots(P_1 \vee P_2) \vee \ldots) \vee P_n)$.

**Definition 1.10.** Eine aussagenlogische Formel ist ein *Literal*, falls sie eine Aussagenvariable oder die Negation davon ist.
Eine aussagenlogische Formel ist in *konjunktiver Normalform* (KNF), falls sie eine endliche Konjunktion $(\bigwedge_{i=1}^{n} P_i)$ von endlichen Disjunktionen

$$P_i = (L_{i1} \vee \ldots \vee L_{in_i})$$

von Literalen $L_{ij}$ ist.
Eine aussagenlogische Formel ist in *disjunktiver Normalform* (DNF), falls sie eine endliche Disjunktion $(\bigvee_{i=1}^{n} P_i)$ von endlichen Konjunktionen

$$P_i = (L_{i1} \wedge \ldots \wedge L_{in_i})$$

von Literalen $L_{ij}$ ist.

**Lemma 1.11.** *Jede aussagenlogische Formel ist logisch äquivalent zu einer aussagenlogischen Formel in KNF und auch logisch äquivalent zu einer aussagenlogischen Formel in DNF.*

*Beweis.* Beachte, dass die Negation eines Literales logisch äquivalent zu einem Literal ist. Somit sieht man leicht, dass die Negation einer aussagenlogischen Formel in DNF logisch äquivalent zu einer aussagenlogischen Formel in KNF ist. Weil $P \sim \neg\neg P$, genügt es zu zeigen, dass jede aussagenlogische Formel logisch äquivalent zu einer aussagenlogischen Formel in DNF ist.
Wir beweisen dies durch Induktion über den Aufbau von Formeln. Für Formeln der Stufe 0 ist das trivial. Falls $P$ und $Q$ beide logisch äquivalent zu aussagenlogischen Formeln in DNF sind, so gilt dies klarerweise auch für $(P \vee Q)$. Wir müssen nur zeigen, dass $\neg P$ logisch äquivalent zu einer Formel in DNF ist, falls $P$ logisch äquivalent zu einer Formel in DNF ist.

Falls $P \sim (\bigvee_{i=1}^{m} P_i)$, wobei jedes $P_i = (L_{i1} \wedge \ldots \wedge L_{in_i})$ für Literale $L_{ij}$, ist

$$\neg P \sim \left( \bigwedge_{i=1}^{m} \left( \neg L_{i1} \vee \ldots \vee \neg L_{in_i} \right) \right)$$

Weil die Negation eines Literales logisch äquivalent zu einem Literal ist, können wir mit Hilfe der Distributivitätsgesetze die Konjunktionen mit den Disjunktionen so distributiv umformen, dass $\neg P$ auch logisch äquivalent zu einer Formel in DNF ist.

□

**Bemerkung 1.12.** Wenn wir noch verlangen, dass jedes Literal $L_{ij}$ in jeder endlichen Konjunktion genau einmal vorkommt, bekommen wir eine *kanonische* DNF, welche bis auf Permutation der $P_i$ und innerhalb der $P_i$ bis auf Permutation der Literale eindeutig ist, denn $(L_i \wedge \neg L_i) \sim \bot$.

# Kapitel 2

# Prädikatenlogik

Nach dem Satz von Lindström ist die Logik erster Stufe die stärkste Logik, in welcher der Kompaktheitssatz (Korollar 2.66) und Löwenheim-Skolem abwärts (Korollar 2.67) gelten. Beide Sätze sind eine Folgerung des *Vollständigkeitssatzes* (Korollar 2.64), welcher besagt, dass *wahr* und *beweisbar* äquivalente Begriffe sind. Wir werden in diesem Abschnitt untersuchen wie mathematische Strukturen als Strukturen erster Stufe betrachtet werden können und den Begriff eines formellen Beweises einführen. Formelle Beweise sind im Kern des *Gödel'schen Unvollständigkeitssatzes*, welcher im nächsten Abschnitt bewiesen wird.

## 2.1 Sprachen und Strukturen

**Definition 2.1.** Eine *Sprache* ist eine Menge $\mathcal{L}$ von Konstanten, Funktions- und Relationszeichen.

$$\mathcal{L} = \{c_i\}_{i\in I} \cup \{f_j\}_{j\in J} \cup \{R_k\}_{k\in K}.$$

Jedes Funktionszeichen $f_j$, bzw. jedes Relationszeichen $R_k$, hat eine Stelligkeit $n_j$, bzw. $n_k$.

Eine *Struktur* $\mathcal{A}$ in der Sprache $\mathcal{L}$ besteht aus einer nicht-leeren Grundmenge $A$, das *Universum* von $\mathcal{A}$, zusammen mit Interpretationen der Konstanten-, Funktions- und Relationszeichen der Sprache $\mathcal{L}$. Dies bedeutet, dass es

- für jedes Konstantenzeichen $c_i$ ein Element aus $A$ gibt, das wir als $c_i^{\mathcal{A}}$ bezeichnen;
- für jedes Funktionszeichen $f_j$ mit Stelligkeit $n_j$ eine Funktion $f_j^{\mathcal{A}} : A^{n_j} \to A$ gibt;
- für jedes Relationszeichen $R_k$ mit Stelligkeit $n_k$ eine Teilmenge $R_k^{\mathcal{A}}$ von $A^{n_k}$ gibt.

Wir sagen, dass $\mathcal{A}$ eine $\mathcal{L}$-Struktur ist und schreiben

$$\mathcal{A} = (A, \{c_i^{\mathcal{A}}\}_{i\in I}, \{f_j^{\mathcal{A}}\}_{j\in J}, \{R_k^{\mathcal{A}}\}_{k\in K}).$$

**Beispiel 2.2.**

- Jede nicht-leere Menge ist eine Struktur in der leeren Sprache.
- Jeder Graph ist eine Struktur in der Graphensprache $\mathcal{L}_{Graph} = \{R\}$, wobei $R$ ein 2-stelliges Relationszeichen für die Kantenrelation ist.

- Jede Gruppe $G$ ist eine Struktur in der Gruppensprache $\mathcal{L}_{Gp} = \{1, \cdot, ^{-1}\}$.
- Jeder Körper $F$ ist eine Struktur in der Ringsprache $\mathcal{L}_{Ring} = \{0, 1, +, -, \cdot\}$.

**Definition 2.3.** Eine *Einbettung* der $\mathcal{L}$-Struktur $\mathcal{A}$ in die $\mathcal{L}$-Struktur $\mathcal{B}$ ist eine injektive Abbildung $F : A \to B$, welche mit den Interpretationen kompatibel ist. Dies bedeutet, dass

- für jedes Konstantenzeichen $c$ aus $\mathcal{L}$ ist $F(c^{\mathcal{A}}) = c^{\mathcal{B}}$;
- für jedes Funktionszeichen $f$ aus $\mathcal{L}$ mit Stelligkeit $n$ und Elemente $a_1, \ldots, a_n$ aus $A$ gilt

$$F(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(F(a_1), \ldots, F(a_n));$$

- für jedes Relationszeichen $R$ aus $\mathcal{L}$ mit Stelligkeit $m$ gilt

$$(a_1, \ldots, a_m) \text{ liegt genau dann in } R^{\mathcal{A}}, \text{ wenn } (F(a_1), \ldots, F(a_m)) \text{ in } R^{\mathcal{B}} \text{ liegt.}$$

Ein *Isomorphismus* ist eine surjektive Einbettung. Falls es einen Isomorphismus von $\mathcal{A}$ nach $\mathcal{B}$ gibt, bezeichnen wir dies mit $\mathcal{A} \simeq \mathcal{B}$.

**Bemerkung 2.4.** Die Relation $\simeq$ ist eine Äquivalenzrelation zwischen $\mathcal{L}$-Strukturen.

**Definition 2.5.** Gegeben zwei $\mathcal{L}$-Strukturen $\mathcal{A}$ und $\mathcal{B}$, sagen wir, dass $\mathcal{A}$ eine *Unterstruktur* von $\mathcal{B}$ ist, falls $A \subset B$ gilt und die mengentheoretische Inklusion $\mathrm{Id}_A : A \to B$ eine Einbettung ist. Wir schreiben $\mathcal{A} \subset \mathcal{B}$.

**Bemerkung 2.6.** Für zwei Unterstrukturen $\mathcal{A}$ und $\mathcal{B}$ einer gemeinsamen Struktur $\mathcal{M}$ in der Sprache $\mathcal{L}$ mit nicht-trivialem Durchschnitt $A \cap B \neq \emptyset$ existiert eine natürliche $\mathcal{L}$-Unterstruktur mit Universum $A \cap B$, welche wir als $\mathcal{A} \cap \mathcal{B}$ bezeichnen. Insbesondere, gegeben eine nicht-leere Teilmenge $C \subset A$, ist der Durchschnitt aller Unterstrukturen $\mathcal{D}$ von $\mathcal{A}$, deren Universum $D$ die Menge $C$ enthält, die kleinste Unterstruktur, deren Universum $C$ enthält. Sie ist die von $C$ *erzeugte Unterstruktur* in $\mathcal{A}$ , bezeichnet als $\langle C \rangle_{\mathcal{A}}$. Die Unterstruktur $\mathcal{D}$ von $\mathcal{A}$ ist *endlich erzeugt*, falls es eine endliche Teilmenge $C$ so gibt, dass $\mathcal{D} = \langle C \rangle_{\mathcal{A}}$ .

Insbesondere, gegeben eine $\mathcal{L}$-Struktur $\mathcal{A}$ und eine nicht-leere Teilmenge $C \subset A$ derart, dass $C$ alle Interpretationen (in $\mathcal{A}$) der Konstantenzeichen enthält und unter den (Interpretationen der) Funktionen aus $\mathcal{L}$ abgeschlossen ist, ist $C$ das Universum einer $\mathcal{L}$-Unterstruktur $\mathcal{C}$ von $\mathcal{A}$: Setze

$$R^{\mathcal{C}} = C^m \cap R^{\mathcal{A}},$$

für jedes Relationszeichen $R$ der Stelligkeit $m$ aus $\mathcal{L}$.

**Notation.** Im Gegensatz zu den Aussagenvariablen werden die Variablen in der Prädikatenlogik mit den Symbolen $x$, $y$, $z$ usw. bezeichnet. Da wir auch in diesem Zusammenhang unendlich viele Variablen besitzen, werden wir abhängig von der Situation die Variablen mit $x_1, \ldots, x_n, \ldots$, oder $y_1, \ldots, y_m, \ldots$ usw. bezeichnen.

**Definition 2.7.** Die Kollektion von *Termen* einer Sprache $\mathcal{L}$ ist die kleinste Menge $\mathbb{TERM}$ von Ausdrücken, welche alle Variablen und Konstantenzeichen enthält, so dass

- für jedes $n$ aus $\mathbb{N}$ und Terme $t_1, \ldots, t_n$ aus $\mathbb{TERM}$ sowie jedes $n$-stellige Funktionszeichen $f$ aus $\mathcal{L}$, der Ausdruck $f(t_1, \ldots, t_n)$ in $\mathbb{TERM}$ liegt.

**Bemerkung 2.8.** Die obige Definition impliziert, dass wir die Terme *einstufen* können. Variablen und Konstantenzeichen sind Terme der Stufe 0. Falls $t_1, \ldots, t_n$ Terme der Stufe höchstens $k$ sind, ist der Term $f(t_1, \ldots, t_n)$ der Stufe höchstens $k+1$.

Insbesondere hat man die Eindeutigkeit der Darstellung: Jeder Term der Stufe $k > 0$ lässt sich eindeutig schreiben als $f(t_1, \ldots, t_n)$ für ein eindeutig bestimmtes Funktionszeichen $f$ und eindeutig bestimmte Terme $t_1, \ldots, t_n$, welche der Stufe höchstens $k$ sind.

**Notation.** Wie üblich in der Mathematik, werden wir in gewissen Fällen Terme anders darstellen, z. B:

$$t_1 + t_2 \ \textit{anstatt} \ +(t_1, t_2).$$

Für einen Term $t$ schreiben wir $t = t[x_1, \ldots, x_m]$, wobei die Variablen $x_1, \ldots, x_m$ verschieden sind, falls die Variablen, welche in $t$ vorkommen, in der Menge $\{x_1, \ldots, x_m\}$ liegen.
**ACHTUNG:** $t[x_1, \ldots, x_n]$ bedeutet nicht, dass jede Variable $x_i$, für $1 \leq i \leq n$, unbedingt in $t$ vorkommt!!
Somit definiert für jede $\mathcal{L}$-Struktur $\mathcal{A}$ der Term $t = t[x_1, \ldots, x_m]$ eine Funktion

$$\begin{array}{rccc} t^{\mathcal{A}}: & A^m & \to & A \\ & (a_1, \ldots, a_m) & \mapsto & t^{\mathcal{A}}[a_1, \ldots, a_m] \end{array},$$

wobei $t^{\mathcal{A}}[a_1, \ldots, a_m]$ der Wert von $t$ evaluiert auf $x_1 = a_1, \ldots, x_m = a_m$ ist. Dieser Wert wird induktiv über die Stufe des Termes $t$ definiert:

- Falls $t = c$ für ein Konstantenzeichen $c$ aus $\mathcal{L}$, ist $t^{\mathcal{A}}$ die konstante Funktion mit Wert $c^{\mathcal{A}}$;
- Falls $t = x_i$ für eine Variable $x_i$, ist $t^{\mathcal{A}}[a_1, \ldots, a_m] = a_i$;
- Falls $t = f(t_1, \ldots, t_n)$, ist

$$t^{\mathcal{A}}[a_1, \ldots, a_m] = f^{\mathcal{A}}(t_1^{\mathcal{A}}[a_1, \ldots, a_m], \ldots, t_n^{\mathcal{A}}[a_1, \ldots, a_m]).$$

**Beispiel 2.9.** Sei $(G, \cdot, e)$ eine Gruppe, gesehen als natürliche Struktur in der Gruppensprache $\mathcal{L}_{Gp} = \{1, \cdot, ^{-1}\}$. Die Terme

$$t_1 = 1 \cdot x \text{ und } t_2 = x$$

definieren die gleichen Funktionen in der Struktur $\mathcal{G} = (G, e, \cdot, x \mapsto x^{-1})$, sind aber verschiedene Terme, gesehen als Ausdrücke in $\mathcal{L}$ (allein schon, weil $t_1$ der Stufe 1 und $t_2$ der Stufe 0 ist).

**Definition 2.10.** *Atomare Formeln* in der Sprache $\mathcal{L}$ sind entweder Ausdrücke der Form

$$(t_1 \doteq t_2),$$

für zwei $\mathcal{L}$-Terme $t_1$ und $t_2$, oder Ausdrücke der Form

$$R(t_1, \ldots, t_n),$$

wobei $n$ aus $\mathbb{N}$ kommt, die Elemente $t_1, \ldots, t_n$ Terme aus $\mathcal{L}$ sind und $R$ ein $n$-stelliges Relationszeichen ist.

Die Kollektion von *Formeln* in der Sprache $\mathcal{L}$ ist die kleinste Menge $\mathbb{FORM}$ von Ausdrücken, welche alle atomare Formel enthält, sodass

- wenn $\varphi$ in $\mathbb{FORM}$ liegt, so liegt $\neg\varphi$ in $\mathbb{FORM}$;
- wenn $\varphi$ und $\psi$ in $\mathbb{FORM}$ liegen, so liegt $(\varphi \vee \psi)$ in $\mathbb{FORM}$;
- wenn $\varphi$ in $\mathbb{FORM}$ liegt und $x$ eine Variable ist, so liegt $\exists x\varphi$ in $\mathbb{FORM}$.

Ebenso wie Terme, können wir nun Formeln einstufen, indem wir sagen, dass atomare Formeln der Stufe 0 sind und wenn wir eine der drei obigen Konstruktionen auf Formeln $\varphi$ und $\psi$ der Stufe höchstens $k$ anwenden, die neue Formel der Stufe höchstens $k+1$ ist. Insbesondere lässt sich jede Formel eindeutig schreiben, entweder als

- $(t_1 \doteq t_2)$, für eindeutige Terme $t_1$ und $t_2$; oder
- $R(t_1, \ldots, t_n)$, für eindeutige Terme $t_1, \ldots, t_n$, oder
- $\neg\varphi$, für eine eindeutige Formel $\varphi$; oder
- $(\varphi \vee \psi)$, für eindeutige Formeln $\varphi$ und $\psi$; oder
- $\exists x\varphi$, für eine eindeutige Formel $\varphi$ und eine eindeutige Variable $x$.

**Bemerkung 2.11.** Wie in der Notation 1.1, werden wir folgende Abkürzungen verwenden, wobei wir die Eindeutigkeit der Darstellung von Formeln dementsprechend verlieren:

- $(\varphi \wedge \psi) = \neg(\neg\varphi \vee \neg\psi)$.
- $(\varphi \longrightarrow \psi) = (\neg\varphi \vee \psi)$.
- $(\varphi \longleftrightarrow \psi) = \big((\varphi \longrightarrow \psi) \wedge (\psi \longrightarrow \varphi)\big)$.
- $\forall x\varphi = \neg\exists x\neg\varphi$.

Ähnlich wie bei Termen schreiben wir für Formeln $\varphi = \varphi[x_1, \ldots, x_n]$, falls die Variablen, welche in $\varphi$ *frei* vorkommen, in der Menge $\{x_1, \ldots, x_n\}$ liegen. Eine Variable $x$ *kommt frei in* $\varphi$ *vor*, falls $x$ in $\varphi$ vorkommt, aber nicht im Wirkungsbereich eines Quantors $\exists x$ liegt. Genauer definieren wir induktiv über den Aufbau von Formeln, dass $x$ in $\varphi$ frei vorkommt, falls

- $\varphi$ atomar ist und $x$ kommt in $\varphi$ vor;
- $\varphi = \neg\psi$ und $x$ frei in $\psi$ vorkommt;
- $\varphi = (\psi_1 \vee \psi_2)$ und $x$ frei in $\psi_1$ oder $\psi_2$ vorkommt;
- $\varphi = \exists y\psi$ und $x$ frei in $\psi$ vorkommt aber verschieden von $y$ ist.

Das Vorkommen einer Variable $x$, welche in $\varphi$ nicht frei vorkommt, ist *gebunden*.
**ACHTUNG:** Die Schreibweise $\varphi[x_1, \ldots, x_n]$ bedeutet nicht, dass jede Variable $x_i$, für $1 \leq i \leq n$, unbedingt in $\varphi$ vorkommt!!

**Definition 2.12.** Sei $\varphi = \varphi[x_1, \ldots, x_n]$ eine $\mathcal{L}$-Formel und $a_1, \ldots, a_n$ Elemente aus der Grundmenge einer $\mathcal{L}$-Struktur $\mathcal{A}$. Wir sagen, dass *das Tupel* $(a_1, \ldots, a_n)$ *die Formel* $\varphi$ *in* $\mathcal{A}$ *erfüllt*, oder dass $\varphi$ *von* $a_1, \ldots, a_n$ *in* $\mathcal{A}$ *gilt*, wir schreiben $\mathcal{A} \models \varphi[a_1, \ldots, a_n]$, falls entweder

- $\varphi = (t_1 \doteq t_2)$ und $t_1^{\mathcal{A}}[a_1, \ldots, a_n] = t_2^{\mathcal{A}}[a_1, \ldots, a_n]$; oder
- $\varphi = R(t_1, \ldots, t_m)$ und $\big(t_1^{\mathcal{A}}[a_1, \ldots, a_n], \ldots, t_m^{\mathcal{A}}[a_1, \ldots, a_n]\big)$ in $R^{\mathcal{A}}$ liegt; oder
- $\varphi = \neg\psi$ und $\mathcal{A} \not\models \psi[a_1, \ldots, a_n]$; oder
- $\varphi = (\psi_1 \vee \psi_2)$ und $\mathcal{A} \models \psi_1[a_1, \ldots, a_n]$ oder $\mathcal{A} \models \psi_2[a_1, \ldots, a_n]$; oder
- $\varphi = \exists y \psi$, wobei $\psi = \psi[x_1, \ldots, x_n, y]$ und es ein Element $a$ aus $A$ derart gibt, dass $\mathcal{A} \models \psi[a_1, \ldots, a_n, a]$.

**Bemerkung 2.13.** Es folgt aus der Definition, dass $\mathcal{A} \not\models \varphi[a_1, \ldots, a_n]$ genau dann, wenn $\mathcal{A} \models \neg\varphi[a_1, \ldots, a_n]$.
Die obige Definition ist kompatibel mit unserer Intuition bezüglich der eingeführten Abkürzungen 2.11. Zum Beispiel:

$$\mathcal{A} \models (\varphi \longrightarrow \psi)[a_1, \ldots, a_n]$$

ist äquivalent zu

$$\mathcal{A} \models \varphi[a_1, \ldots, a_n] \Longrightarrow \mathcal{A} \models \psi[a_1, \ldots, a_n],$$

**Definition 2.14.** Eine *Aussage* ist eine Formel $\chi$ ohne freie Variablen. Dennoch ist die Schreibweise $\chi = \chi[x]$ sinnvoll, siehe Bemerkung 2.11. Somit sagen wir, dass die $\mathcal{L}$-Aussage $\chi$ in der $\mathcal{L}$-Struktur $\mathcal{A}$ *gilt* oder dass $\mathcal{A}$ die Aussage $\chi$ *erfüllt*, wir schreiben $\mathcal{A} \models \chi$, falls $\mathcal{A} \models \chi[a]$, für ein (bzw. jedes) Element $a$ aus $A$.

**Definition 2.15.** Zwei $\mathcal{L}$-Strukturen $\mathcal{A}$ und $\mathcal{B}$ sind *elementar äquivalent*, wir schreiben $\mathcal{A} \equiv \mathcal{B}$, falls sie dieselben Aussagen erfüllen. Dies bedeutet, dass für jede Aussage $\chi$,

$$\text{falls } \mathcal{A} \models \chi, \text{ dann } \mathcal{B} \models \chi.$$

**Bemerkung 2.16.** Mit Induktion über den Aufbau der Aussage $\chi$ sieht man leicht, dass $\mathcal{A} \equiv \mathcal{B}$, falls $\mathcal{A} \simeq \mathcal{B}$.

Die Umkehrung der obigen Bemerkung gilt nicht. Dafür brauchen wir den Begriff von *Back-&-Forth* oder *Ehrenfeucht-Fraïssé* Spielen.

**Definition 2.17.** Seien $\mathcal{A}$ und $\mathcal{B}$ zwei $\mathcal{L}$-Strukturen. Ein *Back-&-Forth* System zwischen $\mathcal{A}$ und $\mathcal{B}$ ist eine Kollektion $\mathcal{S}$ von $\mathcal{L}$-Isomorphismen $F : \mathrm{Dom}(F) \to \mathrm{Im}(F)$ zwischen endlich erzeugten $\mathcal{L}$-Unterstrukturen $\mathrm{Dom}(F)$ von $\mathcal{A}$ und $\mathrm{Im}(F)$ von $\mathcal{B}$, sodass folgende Bedingungen gelten:

**Back** Für jedes $F$ aus $\mathcal{S}$ und jedes $b$ aus $\mathcal{B}$ existiert eine Fortsetzung $G$ von $F$ in $\mathcal{S}$ derart, dass $b$ im Bildbereich $\mathrm{Im}(G)$ von $G$ liegt.

**Forth** Für jedes $F$ aus $\mathcal{S}$ und jedes $a$ aus $\mathcal{A}$ existiert eine Fortsetzung $H$ von $F$ in $\mathcal{S}$ derart, dass $a$ im Definitionsbereich $\mathrm{Dom}(H)$ von $H$ liegt.

**Bemerkung 2.18.** Die triviale Menge $\mathcal{S} = \emptyset$ ist ein Back-&-Forth System zwischen je zwei $\mathcal{L}$-Strukturen $\mathcal{A}$ und $\mathcal{B}$.

Induktiv über den Aufbau von $\varphi[x_1, \ldots, x_n]$ beweißt man, dass für ein Element $F$ aus einem Back-&-Forth System $\mathcal{S}$ und Elemente $a_1, \ldots, a_n$ aus $\mathrm{Dom}(F)$

$$\mathcal{A} \models \varphi[a_1, \ldots, a_n] \text{ genau dann gilt, wenn } \mathcal{B} \models \varphi[F(a_1), \ldots, F(a_n)].$$

Insbesondere erfüllen $\mathcal{A}$ und $\mathcal{B}$ dieselbe Aussagen falls $\mathcal{S} \neq \emptyset$.

**Definition 2.19.** Für zwei $\mathcal{L}$-Strukturen $\mathcal{A}$ und $\mathcal{B}$ und Teilmengen $\emptyset \neq C \subset A$ und $D \subset B$ ist eine partielle Abbildung $F : C \to D$ *elementar*, falls

$$\mathcal{A} \models \varphi[c_1, \ldots, c_n] \text{ genau dann gilt, wenn } \mathcal{B} \models \varphi[F(c_1), \ldots, F(c_n)],$$

für alle Elemente $c_1, \ldots, c_n$ aus $C$ und jede Formel $\varphi[x_1, \ldots, x_n]$.

Die Struktur $\mathcal{A}$ ist eine *elementare Unterstruktur* der Struktur $\mathcal{B}$, falls $A \subset B$ und die mengentheoretische Inklusion $\mathrm{Id}_A : A \to B$ elementar ist. Wir schreiben $\mathcal{A} \preceq \mathcal{B}$. Des Weiteren ist $\mathcal{B}$ eine *elementare Erweiterung* der Struktur $\mathcal{A}$, falls $\mathcal{A}$ sich in $\mathcal{B}$ elementar einbetten lässt.

**Bemerkung 2.20.** Ein Isomorphismus von $\mathcal{A}$ und $\mathcal{B}$ ist immer eine elementare Abbildung.
Wenn eine partielle elementare Abbildung von $\mathcal{A}$ nach $\mathcal{B}$ existiert, dann sind $\mathcal{A}$ und $\mathcal{B}$ elementar äquivalent.

Nach der Bemerkung 2.18 ist jede Abbildung $F$ aus einem Back-&-Forth System $\mathcal{S}$ eine elementare partielle Abbildung von $\mathrm{Dom}(F)$ nach $\mathrm{Im}(F)$.

**Korollar 2.21.** *Falls ein nicht-leeres Back-&-Forth System $\mathcal{S}$ zwischen den $\mathcal{L}$-Strukturen $\mathcal{A}$ und $\mathcal{B}$ existiert, sind $\mathcal{A}$ und $\mathcal{B}$ elementar äquivalent.*

**Beispiel 2.22.** In der Sprache $\mathcal{L} = \{<\}$, wobei $<$ ein zweistelliges Relationszeichen ist, sind die Strukturen $(\mathbb{Q}, <)$ und $(\mathbb{R}, <)$ nicht isomorph (aus Mächtigkeitsgründen) aber elementar äquivalent, weil die Kollektion aller $\mathcal{L}$-Isomorphismen zwischen endlichen Teilmengen von $\mathbb{Q}$ und $\mathbb{R}$ ein Back-&-Forth System bildet.

## 2.2 Theorien und Beweise

In diesem Abschnitt fixieren wir eine Sprache $\mathcal{L}$.

**Definition 2.23.** Eine *$\mathcal{L}$-Theorie $T$* ist eine Kollektion von Aussagen.
Die $\mathcal{L}$-Struktur $\mathcal{A}$ ist ein *Modell* von $T$, falls $\mathcal{A} \models \chi$ für jede Aussage $\chi$ aus $T$. Dies bezeichnen wir mit $\mathcal{A} \models T$.
Die Aussage $\theta$ *folgt* aus der Theorie $T$, bezeichnet mit $T \models \theta$, falls $\theta$ in jedem Modell $\mathcal{A} \models T$ gilt.
Wenn eine Theorie Modelle besitzt, heißt sie *konsistent*, ansonsten *inkonsistent*.

**Bemerkung 2.24.** Jede $\mathcal{L}$-Struktur ist ein Modell der leeren Theorie, welche keine Aussage enthält.
Jede Aussage ist eine Folgerung einer inkonsistenten Theorie. Falls je zwei Modelle einer konsistenten Theorie $T$ elementar äquivalent sind, gilt für jede Aussage $\chi$ entweder $T \models \chi$ oder $T \models \neg\chi$. Beachte, dass diese beiden Fälle nicht gleichzeitig vorkommen können.

**Definition 2.25.** Eine Klasse $\mathcal{C}$ von $\mathcal{L}$-Strukturen ist *axiomatisierbar*, falls es eine Theorie gibt, deren Modelle genau die Strukturen aus $\mathcal{C}$ sind.

**Aufgabe.** Ist die Klasse aller Gruppen in der Sprache $\mathcal{L}_{Gp}$ axiomatisierbar? Wenn ja, folgt die Aussage

$$\forall x \forall y \ (x \cdot y \doteq y \cdot x)$$

(oder die Negation davon) aus der Axiomatisierung?

**Bemerkung 2.26.** Sei $\mathcal{A}$ eine $\mathcal{L}$-Struktur mit Grundmenge $A$. Mit $\mathcal{L}_A$ bezeichnen wir die Sprache $\mathcal{L} \cup \{d_a\}_{a\in A}$, wobei $\{d_a\}_{a\in A}$ eine Menge neuer paarweise verschiedener Konstantenzeichen ist. Beachte, dass $\mathcal{A}$ in natürlicher Weise als $\mathcal{L}_A$-Struktur gesehen werden kann: Es genügt das Konstantenzeichen $d_a$ als das Element $a$ zu interpretieren.

Sei das *atomare Diagramm* $\mathrm{Diag}^{at}(\mathcal{A})$ von $\mathcal{A}$ die Menge aller quantorenfreien $\mathcal{L}_A$-Aussagen, welche in $\mathcal{A}$ gelten. Es folgt, dass eine $\mathcal{L}_A$-Struktur $\mathcal{B}$ genau dann ein Modell von $\mathrm{Diag}^{at}(\mathcal{A})$ ist, wenn die Abbildung

$$\begin{array}{rccc} F: & A & \to & B \\ & a & \mapsto & d_a^{\mathcal{B}} \end{array}$$

eine Einbettung bezüglich der Einschränkung zur Sprache $\mathcal{L}$ liefert.

Des Weiteren sei nun das *vollständige Diagramm* $\mathrm{Diag}(\mathcal{A})$ von $\mathcal{A}$ die Menge aller $\mathcal{L}_A$-Aussagen, welche in $\mathcal{A}$ gelten. Es ist auch leicht zu zeigen, dass eine $\mathcal{L}_A$-Struktur $\mathcal{B}$ genau dann ein Modell von $\mathrm{Diag}(\mathcal{A})$ ist, wenn die vorige Abbildung $F : A \to B$ gegeben durch $a \mapsto d_a^{\mathcal{B}}$ elementar bezüglich der Einschränkung zur Sprache $\mathcal{L}$ ist. Insbesondere sind je zwei Modelle von $\mathrm{Diag}(\mathcal{A})$ elementar äquivalent, gesehen als $\mathcal{L}$-Strukturen.

Induktiv über den Aufbau einer quantorenfreie Formel können wir folgende Bemerkung zeigen:

**Bemerkung 2.27.** Sei $T$ eine $\mathcal{L}$-Theorie mit der Eigenschaft, dass es für jede $\mathcal{L}$-Formel $\varphi[x_1, \ldots, x_n]$ eine quantorenfreie $\mathcal{L}$-Formel $\psi[x_1, \ldots, x_n]$ gibt, so dass

$$T \models \forall x_1 \ldots \forall x_n \Big( \varphi[x_1, \ldots, x_n] \longleftrightarrow \psi[x_1, \ldots, x_n] \Big).$$

Dann gilt für alle Modelle $\mathcal{A}$ und $\mathcal{B}$ von $T$, dass $\mathcal{A} \preceq \mathcal{B}$ (siehe Definition 2.19) aus $\mathcal{A} \subset \mathcal{B}$ folgt.

**Definition 2.28.** Eine $\mathcal{L}$-Aussage $\chi$ ist *allgemeingültig*, falls sie aus der leeren Theorie folgt. Das heißt, dass sie in jeder $\mathcal{L}$-Struktur $\mathcal{A}$ gilt. Dies bezeichnen wir mit $\models \chi$.
Eine $\mathcal{L}$-Formel $\varphi[x_1, \ldots, x_n]$ ist *allgemeingültig*, falls $\models \forall x_1 \ldots \forall x_n \varphi$.

**Bemerkung 2.29.** Sei $P = P(A_1, \ldots, A_m)$ eine aussagenlogische Tautologie mit Variablen $A_1, \ldots, A_m$. Gegeben $\mathcal{L}$-Formeln $\varphi_1[x_1, \ldots, x_n], \ldots, \varphi_m[x_1, \ldots, x_n]$, betrachte die $\mathcal{L}$-Formel $\psi$ mit freien Variablen $x_1, \ldots, x_n$, welche wir aus $P(A_1, \ldots, A_m)$ gewinnen, indem wir jede aussagenlogische Variable $A_i$ durch $\varphi_i[x_1, \ldots, x_n]$ ersetzen. Die $\mathcal{L}$-Formel $\psi[x_1, \ldots, x_n]$ ist allgemeingültig.
Wir bezeichnen solche entstandene Formeln wieder als *Tautologien* (trotz der möglichen Verwirrung).

*Beweis.* Sei $\mathcal{B}$ eine beliebige $\mathcal{L}$-Struktur und $b_1, \ldots, b_n$ Elemente aus $B$. Definiere folgende Belegung der aussagenlogischen Variablen:

$$\begin{array}{rccc} \beta: & \{A_1, \ldots, A_m\} & \to & \{0, 1\} \\ & A_i & \mapsto & \begin{cases} 1, \text{ falls } \mathcal{B} \models \varphi_i[b_1, \ldots, b_n] \\ 0, \text{ sonst} \end{cases} . \end{array}$$

Induktiv über den Aufbau der aussagenlogische Formel $Q(A_1, \ldots, A_n)$ sieht man leicht, dass $\beta(Q(A_1, \ldots, A_m)) = 1$ genau dann, wenn $\mathcal{B} \models \theta[b_1, \ldots, b_n]$, wobei die $\mathcal{L}$-Formel $\theta[x_1, \ldots, x_n]$ aus $Q$ durch Ersetzen der Variable $A_i$ durch $\varphi_i$ entsteht.

Wenn $P(A_1, \ldots, A_m)$ eine Tautologie ist, folgt, dass die entsprechende Formel $\psi[x_1, \ldots, x_n]$ wie in der Behauptung allgemeingültig ist. □

**Definition 2.30.** Die *Gleichheitsaxiome* sind die folgende Liste von Aussagen:

1. $\forall x(x \doteq x)$
2. $\forall x \forall y\,((x \doteq y) \longrightarrow (y \doteq x))$.
3. $\forall x \forall y \forall z\Big(\,((x \doteq y) \wedge (y \doteq z)) \longrightarrow (x \doteq z)\Big)$.
4. $\forall x_1 \ldots \forall x_n \forall y_1 \ldots \forall y_n \Big( (\bigwedge\limits_{1 \leq i \leq n} (x_i \doteq y_i)) \longrightarrow (f(x_1, \ldots, x_n) \doteq f(y_1, \ldots, y_n))\Big)$ für jedes $n$-stellige Funktionszeichen $f$ aus $\mathcal{L}$.
5. $\forall x_1 \ldots \forall x_m \forall y_1 \ldots \forall y_m \Big( (\bigwedge\limits_{1 \leq i \leq m} (x_i \doteq y_i)) \longrightarrow (R(x_1, \ldots, x_m) \longleftrightarrow R(y_1, \ldots, y_m))\Big)$ für jedes $m$-stellige Relationszeichen $R$ aus $\mathcal{L}$.

**Bemerkung 2.31.** Beachte, dass die obige Liste von Axiomen unendlich sein kann, falls die Sprache $\mathcal{L}$ unendlich viele Funktions- oder Relationszeichen enthält.
Jedes Gleichheitsaxiom ist allgemeingültig.

*Beweis.* Gleichheit ist in der Tat eine Äquivalenzrelation (dies besagen die Axiome (1) – (3)). Ferner ist das Bild von Tupeln, die gleich sind, auch gleich (und dementsprechend für Relationen). □

Um den Begriff eines formellen Beweises einzuführen, brauchen wir einige Hilfslemmata.

**Definition 2.32.** Seien $t$ und $s$ Terme aus $\mathcal{L}$ und $x$ eine Variable. Die *Ersetzung* von $x$ durch $s$ in $t$ ist ein neuer Term $t_{s/x}$, der aus $t$ gewonnen wird, indem wir jedes Vorkommen der Variable $x$ durch $s$ ersetzen.

**Bemerkung 2.33.** Beachte: Falls $x$ in $s$ nicht als Variable vorkommt, dann kommt $x$ nicht mehr in $t_{s/x}$ vor. Allerdings werden die Variablen aus $s$ nun in $t_{s/x}$ vorkommen.

**Definition 2.34.** Gegeben eine Formel $\varphi$, eine Variable $x$ und einen Term $s$, definieren wir die *Ersetzung* $\varphi_{s/x}$ von $x$ durch $s$ in $\varphi$, indem wir alle freien Vorkommen der Variable $x$ in $\varphi$ durch $s$ ersetzen. Genauer definieren wir rekursiv:

- Falls $\varphi = (t_1 \doteq t_2)$, ist $\varphi_{s/x} = \big(t_{1s/x} \doteq t_{2s/x}\big)$.
- Falls $\varphi = R(t_1, \ldots, t_k)$, ist $\varphi_{s/x} = R(t_{1s/x} \ldots, t_{ks/x})$.
- Falls $\varphi = \neg\psi$, ist $\varphi_{s/x} = \neg\psi_{s/x}$.
- Falls $\varphi = (\varphi_1 \vee \varphi_2)$, ist $\varphi_{s/x} = (\varphi_{1s/x} \vee \varphi_{2s/x})$.
- Falls $\varphi = \exists y\psi$, ist $\varphi_{s/x} = \begin{cases} \exists y\psi, \text{ für } y = x \\ \exists y\psi_{s/x}, \text{ für } y \neq x \end{cases}$.

Die Variable $x$ ist *frei* für $s$ in $\varphi$, falls keine der Variablen von $s$ in $\varphi_{s/x}$ gebunden wird. Dies bedeutet, dass entweder $x$ nicht frei in $\varphi$ vorkommt (und somit ist $\varphi_{s/x} = \varphi$), oder

- $\varphi$ ist quantorenfrei; oder
- $\varphi = \neg\psi$ und $x$ kommt frei für $s$ in $\psi$ vor; oder
- $\varphi = (\varphi_1 \vee \varphi_2)$ und $x$ kommt frei für $s$ sowohl in $\varphi_1$ als auch in $\varphi_2$ vor; oder
- $\varphi = \exists y\psi$ und $x \neq y$ kommt frei für $s$ in $\psi$, aber $y$ kommt nicht in $s$ vor.

**Beispiel 2.35.** Nach dem Ersetzen kann die Erfüllbarkeit einer Formel in einer Struktur höchst verschieden sein. Zum Beispiel, falls $s = y$, kommt $x$ nicht frei für $s$ in $\varphi = \forall y\,(y \doteq x)$ vor, denn $y$ wird nach dem Ersetzen gebunden. In der Tat ist $\varphi_{s/x} = \forall y(y \doteq y)$ eine allgemeingültige Aussage. Jedoch erfüllt das Element $a$ der Struktur $\mathcal{A}$ die Formel $\varphi$ genau dann, wenn die Grundmenge $A$ die Einermenge $\{a\}$ ist.

Falls die Variable $x$ frei für $s$ in $\varphi$ vorkommt, haben wir eine Äquivalenz:

**Lemma 2.36** (Substitionslemma)**.** *Wenn die Variable $x$ frei für $s = s[x_1, \ldots, x_n]$ in der Formel $\varphi[x, x_1, \ldots, x_n]$ ist, gilt für beliebige Elemente $a_1, \ldots, a_n$ in einer Struktur $\mathcal{A}$,*

$$\mathcal{A} \models \varphi[s[a_1, \ldots, a_n], a_1, \ldots, a_n] \iff \mathcal{A} \models \varphi_{s/x}[a_1, \ldots, a_n].$$

*Beweis.* Mit der obigen Notation zeigen wir zuerst induktiv über den Aufbau eines Termes $t[x, x_1, \ldots, x_n]$, dass

$$t^{\mathcal{A}}_{s/x}[a_1, \ldots, a_n] = t^{\mathcal{A}}[s^{\mathcal{A}}[a_1, \ldots, a_n], a_1, \ldots, a_n].$$

Falls $t$ ein Konstantenzeichen ist, ist es trivial. Wenn $t$ eine Variable ist, müssen wir unterscheiden, ob $t = x$ oder $t \neq x$. Und für beliebige Terme folgt es aus der Induktionsannahme.

Nun zeigen wir induktiv über den Aufbau der Formel $\varphi$, dass

$$\mathcal{A} \models \varphi[s[a_1, \ldots, a_n], a_1, \ldots, a_n] \iff \varphi_{s/x}[a_1, \ldots, a_n].$$

Für quantorenfreie Formeln folgt es aus dem ersten Teil des Beweises. Daher müssen wir nur den Fall $\varphi = \exists y\psi$ betrachten. Falls $y = x$, kommt $x$ nicht frei in $\varphi$ vor und es ist $\varphi_{s/x} = \varphi$ und die Äquivalenz folgt.

Ansonsten ist $y \neq x$ und wir schreiben $\psi = \psi[y, x, x_1, \ldots, x_n]$. Weil $x$ frei für $s$ in $\varphi$ ist, kommt die Variable $y$ nicht in $s$ vor. Insbesondere ist $s[a_1, \ldots, a_n] = \tilde{s}[a, a_1, \ldots, a_n]$ für jedes Element $a$ aus $A$, wenn wir $s$ als Term $\tilde{s}$ in den Variablen $\{y, x_1, \ldots, x_n\}$ schreiben. Ferner ist $\varphi_{s/x} = \exists y\psi_{s/x}[y, x_1, \ldots, x_n]$. Nun gilt:

$$\begin{aligned}
\mathcal{A} \models \varphi[s[a_1, \ldots, a_n], a_1, \ldots, a_n] \iff & \text{ Es gibt ein Element } a \text{ aus } A \text{ mit} \\
& \mathcal{A} \models \psi[a, s[a_1, \ldots, a_n], a_1, \ldots, a_n] \iff \\
\text{Es gibt } a \text{ aus } A \text{ mit } \mathcal{A} \models \psi[a, \tilde{s}[a, a_1, \ldots, a_n], a_1, \ldots, a_n] & \overset{I.A.}{\iff} \text{ Es gibt } a \text{ aus } A \text{ mit} \\
& \mathcal{A} \models \psi_{\tilde{s}/x}[a, a_1, \ldots, a_n] \iff \mathcal{A} \models \varphi_{\tilde{s}/x}[a_1, \ldots, a_n] \iff \mathcal{A} \models \varphi_{s/x}[a_1, \ldots, a_n]
\end{aligned}$$

□

**Korollar 2.37** (∃-Quantorenaxiom)**.** *Wenn $x$ frei für $s = s[x_1, \ldots, x_n]$ in $\varphi[x, x_1, \ldots, x_n]$ ist, dann ist die Formel*

$$(\varphi_{s/x} \longrightarrow \exists x \varphi)$$

*allgemeingültig.*
*Insbesondere gilt $\models (\psi \longrightarrow \exists x \psi)$.*

*Beweis.* Wir müssen zeigen, dass jede Struktur $\mathcal{A}$ die Aussage $\forall x_1 \ldots \forall x_n (\varphi_{s/x} \longrightarrow \exists x \varphi)$ erfüllt. Gegeben $a_1, \ldots, a_n$ aus $A$, sodass $\mathcal{A} \models \varphi_{s/x}[a_1, \ldots, a_n]$ gilt, dann folgt aus dem Lemma 2.36

$$\mathcal{A} \models \varphi[s[a_1, \ldots, a_n], a_1, \ldots, a_n].$$

Insbesondere bezeugt das Element $s[a_1, \ldots, a_n]$ aus $A$, dass $\mathcal{A} \models \exists x \varphi[a_1, \ldots, a_n]$, wie gewünscht. Für die letzte Behauptung des Korollars genügt es den Fall $s = x$ zu betrachten. □

**Definition 2.38.** Eine $\mathcal{L}$-Formel $\varphi$ ist in *pränexer Normalform*, wenn

$$\varphi = Q_1 y_1 \ldots Q_m y_m \psi,$$

wobei jedes $Q_i$ eines der Quantoren $\forall$ oder $\exists$ ist und $\psi$ eine quantorenfreie Formel ist.

**Lemma 2.39.** *Für jede Formel $\varphi[x_1, \ldots, x_n]$ gibt es eine Formel $\theta[x_1, \ldots, x_n]$ in pränexer Normalform, sodass $(\varphi \longleftrightarrow \theta)$ allgemeingültig ist.*

Wir sagen, dass $\varphi$ und $\theta$ logisch äquivalent sind, und schreiben $\varphi \sim \theta$.

*Beweis.* Es genügt alle Quantoren in $\varphi$ nach folgenden Regeln nach vorne zu ziehen:

- $\neg\exists \sim \forall\neg$
- $\neg\forall \sim \exists\neg$
- $(\psi_1 \wedge \exists x \psi_2) \sim \exists y(\psi_1 \wedge \psi_{2\,y/x})$, wobei $y$ nicht in $\psi_1$ und nicht in $\psi_2$ vorkommt.
- $(\psi_1 \wedge \forall x \psi_2) \sim \forall y(\psi_1 \wedge \psi_{2\,y/x})$, wobei $y$ nicht in $\psi_1$ und nicht in $\psi_2$ vorkommt.

Jede Reihenfolge dieses Verfahrens liefert möglicherweise eine andere Formel in pränexer Normalform, aber sie sind alle logisch äquivalent zueineander. □

Der Beweis des folgenden Lemmas ist offensichtlich.

**Lemma 2.40** (Modus Ponens)**.** *Falls $\models \varphi$ und $\models (\varphi \longrightarrow \psi)$, dann ist $\psi$ auch allgemeingültig.*

**Lemma 2.41** (∃-Einführung)**.** *Falls die Variable $x$ nicht frei in $\psi$ vorkommt und $\models (\varphi \longrightarrow \psi)$, dann ist $(\exists x \varphi \longrightarrow \psi)$ allgemeingültig.*

*Beweis.* Schreibe $\varphi = \varphi[x, x_1, \ldots, x_n]$ und $\psi = \psi[x_1, \ldots, x_n] = \psi[x, x_1, \ldots, x_n]$ (weil $x$ nicht frei in $\psi$ vorkommt). Gegeben Elemente $a_1, \ldots, a_n$ aus der Grundmenge $A$ einer beliebigen Struktur $\mathcal{A}$, wollen wir zeigen, dass

$$\mathcal{A} \models (\exists x \varphi \longrightarrow \psi)[a_1, \ldots, a_n].$$

Angenommen, dass $\mathcal{A} \models \exists x \varphi[x, a_1, \ldots, a_n]$, wähle $a$ aus $A$ mit $\mathcal{A} \models \varphi[a, a_1, \ldots, a_n]$. Es folgt $\mathcal{A} \models \psi[a, a_1, \ldots, a_n]$, weil die Formel $(\varphi \longrightarrow \psi)$ allgemeingültig ist. Weil $x$ nicht frei in $\psi$ vorkommt, bedeutet dies, dass $\mathcal{A} \models \psi[a_1, \ldots, a_n]$, wie gewünscht.

□

**Definition 2.42.** Die Formel $\varphi$ ist aus der Theorie $T$ *beweisbar*, wir schreiben $T \vdash \varphi$, falls ein $n$ aus $\mathbb{N}$ und eine endliche Folge $(\varphi_1, \ldots, \varphi_n)$, mit $\varphi_n = \varphi$, derart existieren, dass für jedes $i \leq n$

- die Formel $\varphi_i$ ein *logisches Axiom* ist, das heißt, entweder eine Tautologie (siehe 2.29) oder ein Gleichheitsaxiom oder eine Instanz $(\psi_{s/x}(x) \longrightarrow \exists x \psi(x))$ des $\exists$-Quantorenaxiomes ist; oder
- die Formel $\varphi_i$ zu $T$ gehört; oder
- die Formel $\varphi_i$ aus zwei vorherigen Formeln $\varphi_j$ und $\varphi_k = (\varphi_j \longrightarrow \varphi_i)$ durch Modus Ponens entsteht; oder
- die Formel $\varphi_i = (\exists x \psi_1 \longrightarrow \psi_2)$ aus einer vorherigen Formel $\varphi_j = (\psi_1 \longrightarrow \psi_2)$ durch $\exists$-Einführung entsteht (insbesondere kommt $x$ nicht frei in $\psi_2$ vor).

Die obige Folge $(\varphi_1, \ldots, \varphi_n)$ ist ein *Beweis* in $T$ der Formel $\varphi$.

**Bemerkung 2.43.** Falls $(\varphi_1, \ldots, \varphi_n)$ ein Beweis in $T$ von $\varphi$ ist, so ist $(\varphi_1, \ldots, \varphi_{n+2})$ ein Beweis von $\varphi$, wobei $\varphi_{n+1}$ die Tautologie $(\varphi_n \longrightarrow \varphi_n)$ ist und $\varphi_{n+2} = \varphi_n = \varphi$ mit Anwendung von Modus Ponens entsteht. Insbesondere kann eine Formel mehrere Beweise in $T$ haben.

Falls die Formel $\varphi$ aus der Theorie $T \cup \{\psi_1, \ldots, \psi_n\}$ beweisbar ist, wobei jede Aussage $\psi_i$ auch aus $T$ beweisbar ist, dann ist $\varphi$ aus $T$ beweisbar: Es genügt die Beweise der $\psi_i$'s zusammen mit dem Beweis von $\varphi$ aus $T \cup \{\psi_1, \ldots, \psi_n\}$ zu konkatenieren, um einen Beweis von $\varphi$ aus $T$ zu gewinnen.

**Definition 2.44.** Eine Formel $\varphi$ ist *beweisbar*, falls sie aus der leeren Theorie beweisbar ist. Dies bezeichnen wir mit $\vdash \varphi$.
Das *Hilbertkalkül* ist die Kollektion aller beweisbaren Formeln (bezüglich der leeren Theorie).

**Lemma 2.45.**

*$\forall$-Quantorenaxiom* *Falls $x$ frei für $s$ in $\varphi$ ist, dann gilt $\vdash (\forall x \varphi \longrightarrow \varphi_{s/x})$. Insbesondere ist $(\forall x \varphi \longrightarrow \varphi)$ beweisbar.*

*$\forall$-Einführung* *Falls $x$ nicht frei in $\varphi$ vorkommt und $\vdash (\varphi \longrightarrow \psi)$, so gilt $\vdash (\varphi \longrightarrow \forall x \psi)$. Insbesondere ist $\forall x \psi$ beweisbar, wenn $\psi$ beweisbar ist.*

*Beweis.* Für das $\forall$-Quantorenaxiom, beachte, dass $x$ auch frei für $s$ in $\neg\varphi$ ist. Insbesondere ist $(\neg\varphi_{s/x} \longrightarrow \exists x \neg\varphi)$ eine Instanz des $\exists$-Quantorenaxiom und daher beweisbar. Die aussagenlogische Tautologie

$$\Big((p \longrightarrow q) \longrightarrow (\neg q \longrightarrow \neg p)\Big)$$

zusammen mit $\neg\varphi_{s/x}$ als $p$ und $\exists x \neg\varphi$ als $q$ und Modus Ponens liefert, dass

$$\vdash (\neg\exists x \neg\varphi \longrightarrow \neg\neg\varphi_{s/x}),$$

und äquivalent dazu

$$\vdash (\forall x \varphi \longrightarrow \neg\neg\varphi_{s/x}).$$

Die aussagenlogische Tautologie

$$\Big((A_1 \longrightarrow \neg\neg A_2) \longrightarrow (A_1 \longrightarrow A_2)\Big)$$

liefert nun mit Modus Ponens, dass $(\forall x\varphi \longrightarrow \varphi_{s/x})$ beweisbar ist wegen Bemerkung 2.43.

Wende nun das $\forall$-Quantorenaxiom mit $s = x$ an und erhalte, dass $(\forall x\varphi \longrightarrow \varphi)$ beweisbar ist.

Für die $\forall$-Einführung ist es ähnlich wie oben, weil $x$ nicht frei in $\neg\varphi$ vorkommt, wenn $x$ nicht frei in $\varphi$ vorkommt. Aus der Tautologie

$$\Big((\varphi \longrightarrow \psi) \longrightarrow (\neg\psi \longrightarrow \neg\varphi)\Big)$$

und Modus Ponens folgt, dass $(\neg\psi \longrightarrow \neg\varphi)$ beweisbar ist und somit auch $(\exists x\neg\psi \longrightarrow \neg\varphi)$. Mit Hilfe der entsprechenden Tautologie, Modus Ponens und der Bemerkung 2.43 ist die Formel $(\varphi \longrightarrow \forall x\psi)$ beweisbar, wie gewünscht.
Die Formel $\varphi = \forall y(y \doteq y)$ ist ein Gleichheitsaxiom und somit beweisbar, aber $x$ kommt nicht frei in $\varphi$ vor. Die aussagenlogische Tautologie

$$\Big(p \longrightarrow \Big(q \longrightarrow (p \longrightarrow q)\Big)\Big)$$

und zweimaliges Anwenden von Modus Ponens (mit $\varphi$ als $p$ und $\psi$ als $q$) liefern, dass $\vdash (\varphi \longrightarrow \psi)$, falls $\psi$ beweisbar ist. Insbesondere ist $(\varphi \longrightarrow \forall x\psi)$ beweisbar. Aus Modus Ponens folgt, dass $\forall x\psi$ auch beweisbar ist. □

**Lemma 2.46.** *Sei $\varphi[x_1, \ldots, x_n]$ eine $\mathcal{L}$-Formel und $C$ eine Menge von neuen Konstantenzeichen, welche nicht aus $\mathcal{L}$ kommen. Für Symbole $c_1, \ldots, c_n$ aus $C$, ist die $\mathcal{L}$-Formel $\varphi[x_1, \ldots, x_n]$ genau dann beweisbar, wenn die $\mathcal{L} \cup C$-Aussage $\varphi[c_1, \ldots, c_n]$ beweisbar ist.*

*Beweis.*

($\Longrightarrow$) Falls $\vdash \varphi[x_1, \ldots, x_n]$, so folgt aus der $\forall$-Einführung die Beweisbarkeit von der Formel $\forall x_1 \ldots \forall x_n\varphi[x_1, \ldots, x_n]$. Beachte, dass $x_i$ frei für $c_i$ in $\varphi[x_1, \ldots, x_n]$ ist (in der Sprache $\mathcal{L} \cup C$), weil überhaupt keine Variablen im Term $c_i$ vorkommen. Aus dem $\forall$-Quantorenaxiom folgt induktiv, dass $\varphi[c_1, \ldots, c_n]$ beweisbar ist.

($\Longleftarrow$) Sei $\varphi_1, \ldots, \varphi_n$ ein Beweis in der Sprache $\mathcal{L} \cup C$. OBdA können wir annehmen, dass alle Konstantenzeichen aus $C$, welche im Beweis vorkommen, in der Menge $\{c_1, \ldots, c_n\}$ enthalten sind. Wenn wir formell jedes Vorkommen von $c_i$ durch eine neue Variable $y_i$ ersetzen, welche im Beweis nicht vorkommen, gewinnen wir einen $\mathcal{L}$-Beweis von $\varphi[y_1, \ldots, y_n]$. Wie oben folgt aus der $\forall$-Einführung, dass die $\mathcal{L}$-Aussage

$$(\varphi[y_1, \ldots, y_n] \longrightarrow \forall y_1 \ldots \forall y_n\varphi[y_1, \ldots, y_n])$$

beweisbar ist, und somit ist die $\mathcal{L}$-Aussage $\vdash \forall y_1 \ldots \forall y_n\varphi[y_1, \ldots, y_n]$ beweisbar. Weil $y_i$ frei für $x_i$ in $\varphi[y_1, \ldots, y_n]$ ist, folgt aus dem $\forall$-Quantorenaxiom und iteriertem Modus Ponens induktiv, dass

$$(\forall y_1 \ldots \forall y_n\varphi[y_1, \ldots, y_n] \longrightarrow \forall y_i \ldots \forall y_n\varphi[x_1, \ldots, x_{i-1}, y_i, \ldots, y_n])$$

beweisbar ist. Insbesondere ist $\varphi[x_1, \ldots, x_n]$ beweisbar.

□

**Bemerkung 2.47.** Eine Formel $\varphi$ ist genau aus der Theorie $T$ beweisbar, wenn es endlich viele Aussagen $\varphi_1, \ldots, \varphi_k$ aus $T$ gibt, sodass $\vdash \Big((\bigwedge_{i=1}^{k} \varphi_i) \longrightarrow \varphi\Big)$.

*Beweis.*

($\Longrightarrow$) Wenn $T \vdash \varphi$, gibt es einen Beweis endlicher Länge von $\varphi$, welcher die Formeln $\varphi_1, \ldots, \varphi_k$ aus $T$ verwendet. Beachte, dass die Formel

$$\Big((\bigwedge_{i=1}^{k} \varphi_i) \longrightarrow \varphi_j\Big)$$

für jedes $1 \leq j \leq k$ eine Tautologie ist. Insbesondere folgt aus der Bemerkung 2.43 induktiv über die Länge des Beweises, dass die Formel $\Big((\bigwedge_{i=1}^{k} \varphi_i) \longrightarrow \varphi\Big)$ beweisbar ist.

($\Longleftarrow$) Diese Richtung folgt aus iteriertem Modus Ponens, denn die Formel

$$\Big(\big((\bigwedge_{i=1}^{k} \varphi_i) \longrightarrow \varphi\big) \longrightarrow \big(\varphi_1 \longrightarrow (\varphi_2 \longrightarrow \ldots (\varphi_k \longrightarrow \varphi) \ldots)\big)\Big)$$

ist eine Tautologie.

□

**Korollar 2.48.** *Seien $\varphi$ eine Formel und $\psi$ eine Aussage. Die Formel $\varphi$ ist genau aus der Theorie $T \cup \{\psi\}$ beweisbar, wenn die Implikation $(\psi \longrightarrow \varphi)$ aus $T$ beweisbar ist. D. h.*

$$T \cup \{\psi\} \vdash \varphi \Longleftrightarrow T \vdash (\psi \longrightarrow \varphi).$$

*Beweis.*

($\Longrightarrow$) Wegen der Bemerkung 2.47 gibt es Aussagen $\varphi_1, \ldots, \varphi_k$ aus $T \cup \{\psi\}$ derart, dass die Formel $\big((\bigwedge_{i=1}^{k} \varphi_i) \longrightarrow \varphi\big)$ beweisbar ist.

Wir unterscheiden zwei Fälle: Zuerst nehmen wir an, dass alle Formel $\varphi_i$ aus $T$ kommen. Aus der Tautologie

$$\Big((p \to q) \to \big(p \to (r \to q)\big)\Big)$$

folgt (mit $p = \bigwedge_{i=1}^{k} \varphi_i$, $q = \varphi$ und $r = \psi$), dass $\big((\bigwedge_{i=1}^{k} \varphi_i) \longrightarrow (\psi \to \varphi)\big)$ beweisbar ist, so $T \vdash (\psi \to \varphi)$ aus der Bemerkung 2.47.

Im zweiten Fall gibt es nach Umformung Aussagen $\varphi_1, \ldots, \varphi_k$ aus $T$, sodass

$$\vdash \Big(\big((\bigwedge_{i=1}^{k} \varphi_i) \wedge \psi\big) \longrightarrow \varphi\Big).$$

Nun liefert folgende Tautologie

$$\Big(\Big(\big((\bigwedge_{i=1}^{k} \varphi_i) \wedge \psi\big) \longrightarrow \varphi\Big) \longrightarrow \Big((\bigwedge_{i=1}^{k} \varphi_i) \longrightarrow (\psi \longrightarrow \varphi)\Big)\Big)$$

mit Modus Ponens einen Beweis von $(\psi \longrightarrow \varphi)$ aus $T$, wieder mit der obigen Bemerkung.

($\Longleftarrow$) Falls es in $T$ einen Beweis $\varphi_1, \ldots, \varphi_n$ der Länge $n$ von der Formel $\varphi_n = (\psi \longrightarrow \varphi)$ gibt, dann bekommen wir mit Modus Ponens einen Beweis der Länge $n+2$ von $\varphi$ aus $T \cup \{\psi\}$, in dem wir $\varphi_{n+1} = \psi$ und $\varphi_{n+2} = \varphi$ setzen.

□

**Korollar 2.49.** *Wenn eine Formel beweisbar ist, dann ist sie allgemeingültig.*
*Insbesondere, wenn $T \vdash \varphi$, dann folgt $\varphi$ aus $T$, d. h. $T \models \varphi$.*

*Beweis.* Aus den Bemerkungen 2.31 und 2.29, den Lemmata 2.40 und 2.41 und aus dem Korollar 2.37 folgt, dass jede beweisbare Formel allgemeingültig ist.

Für die letzte Behauptung; falls $\varphi$ aus $T$ beweisbar ist, dann ist $\vdash \big((\bigwedge_{i=1}^{k} \varphi_i) \longrightarrow \varphi\big)$ für endlich viele Aussagen $\varphi_1, \ldots, \varphi_k$ aus $T$. Jedes Modell $\mathcal{A}$ von $T$ erfüllt die Formeln $\varphi_1, \ldots, \varphi_k$ und somit auch $\varphi$. □

Wir werden im nächsten Abschnitt sehen, dass die Rückrichtung auch gilt: der Vollständigkeitssatz. Insbesondere haben wir eine Äquivalenz zwischen zwei Begriffen: semantische *Wahrheit* und syntaktische Folgerung.

## 2.3 Vollständigkeit und Kompaktheit

In diesem Abschnitt fixieren wir eine Sprache $\mathcal{L}$.

**Definition 2.50.** Eine Theorie $T$ ist *widerspruchsfrei*, falls keine Aussage $\chi$ derart existiert, dass $T \vdash \chi$ und $T \vdash \neg\chi$. Ansonsten ist $T$ widersprüchlich.
Eine widerspruchsfreie Theorie ist vollständig, falls $T \vdash \chi$ oder $T \vdash \neg\chi$ für jede Aussage $\chi$.

**Bemerkung 2.51.** Jede konsistente Theorie ist widerspruchsfrei: Wenn $\mathcal{A}$ ein Modell von $T$ ist, dann gilt, siehe Korollar 2.49, in $\mathcal{A}$ jede Aussage, welche aus $T$ beweisbar ist. Aber in einer Struktur kann nicht sowohl $\chi$ als auch $\neg\chi$ gelten.
Je zwei Modelle einer vollständigen Theorie sind elementar äquivalent: Falls $\mathcal{A}$ und $\mathcal{B}$ Modelle der vollständigen Theorie sind und $\chi$ eine beliebige Aussage ist, gilt

$$\mathcal{A} \models \chi \Longleftrightarrow T \vdash \chi \Longleftrightarrow \mathcal{B} \models \chi.$$

**Bemerkung 2.52.** Eine Theorie $T$ ist genau dann widerspruchsfrei, wenn für keine endliche Kollektion von Formeln $\varphi_1, \ldots, \varphi_k$ aus $T$ gilt, dass $\vdash \neg(\bigwedge_{i=1}^{k} \varphi_i)$.

*Beweis.* Wenn die Formel $\neg(\bigwedge_{i=1}^{k} \varphi_i)$ beweisbar wäre, ist sie insbesondere auch aus $T$ beweisbar. Mit Hilfe von iteriertem Modus Ponens und Benutzung der Tautologie

$$\Big(\varphi_1 \longrightarrow \big(\varphi_2 \longrightarrow \ldots \longrightarrow (\varphi_k \longrightarrow (\bigwedge_{i=1}^{k} \varphi_i) \ldots)\big)\Big).$$

sieht man, dass $(\bigwedge_{i=1}^{k} \varphi_i)$ aus $T$ beweisbar ist. Somit ist $T$ widersprüchlich.
Für die andere Richtung nehmen wir an, dass $T$ widersprüchlich ist, das heißt wir nehmen an,

dass $T$ sowohl $\chi$ als auch $\neg\chi$ beweist. Wie in der Bemerkung 2.47 existieren Aussagen $\varphi_1, \ldots, \varphi_i$ und $\varphi_{i+1}, \ldots, \varphi_k$ aus $T$ mit

$$\vdash \big((\bigwedge_{j=1}^{i} \varphi_j) \longrightarrow \chi\big) \text{ und } \vdash \big((\bigwedge_{j=i+1}^{k} \varphi_j) \longrightarrow \neg\chi\big).$$

Die aussagenlogische Tautologie

$$\Big((p \longrightarrow q) \longrightarrow \big((r \longrightarrow \neg q) \longrightarrow \neg(p \wedge r)\big)\Big)$$

liefert mit Modus Ponens, dass $\vdash \neg(\bigwedge_{i=1}^{k} \varphi_i)$, wie gewünscht. □

**Lemma 2.53.** *Eine Theorie $T$ ist genau dann widersprüchlich, wenn jede Aussage aus $T$ beweisbar ist.*

*Beweis.* Eine Richtung ist trivial. Für die andere Richtung sei $\chi$ eine beliebige Aussage. Falls $T$ widersprüchlich ist, gibt es eine Aussage $\theta$ mit $T \vdash \theta$ und $T \vdash \neg\theta$. Die Tautologie

$$\Big(\theta \longrightarrow (\neg\theta \longrightarrow \chi)\Big)$$

liefert mit Modus Ponens (zwei Mal) einen Beweis von $\chi$ aus $T$. □

**Korollar 2.54.** *Sei $T$ eine Theorie und $\chi$ eine Aussage. Die Theorie $T \cup \{\neg\chi\}$ ist genau dann widersprüchlich, wenn $T \vdash \chi$.*

*Beweis.*

($\Longrightarrow$) Falls $T \cup \{\neg\chi\}$ widersprüchlich ist, dann beweist sie wegen Lemma 2.53 jede Aussage. Insbesondere beweist $T \cup \{\neg\chi\}$ die Aussage $\chi$. Wegen Korollar 2.48 ist $(\neg\chi \longrightarrow \chi)$ aus $T$ beweisbar. Die Tautologie

$$\Big((\neg\chi \longrightarrow \chi) \longrightarrow \chi\Big)$$

liefert nun mit Modus Ponens einen Beweis aus $T$ von $\chi$, wie gewünscht.

($\Longleftarrow$) Wenn $T \vdash \chi$, dann ist $\chi$ auch in jeder Obertheorie von $T$ beweisbar, insbesondere in $T \cup \{\neg\chi\}$. Aber $T \cup \{\neg\chi\}$ beweist auch $\neg\chi$, trivialerweise. Daher ist $T \cup \{\neg\chi\}$ widersprüchlich.

□

**Satz 2.55.** *Die Behauptung*

$$T \models \chi \Longleftrightarrow T \vdash \chi \textit{ für jede Theorie } T \textit{ und jede Aussage } \chi$$

*ist äquivalent zur Behauptung*

*Eine Theorie ist genau dann widerspruchsfrei, wenn sie konsistent ist.*

*Beweis.*

($\Longrightarrow$) Wegen Bemerkung 2.51 müssen wir nur zeigen, dass die widerspruchsfreie Theorie $T$ ein Modell besitzt. Sonst gilt trivialerweise $T \models \chi$ für jede Aussage $\chi$. Aber unsere Annahme bedeutet, dass $T \vdash \chi$ für jede Aussage $\chi$, das heißt $T$ wäre widersprüchlich wegen Lemma 2.53.

($\Longleftarrow$) Wegen Korollar 2.49 genügt es zu zeigen, dass $T \vdash \chi$, wenn $T \models \chi$. Sonst ist die Theorie $T \cup \{\neg\chi\}$ wegen Korollar 2.54 widerspruchsfrei und es gibt somit ein Modell $\mathcal{A}$ von $T \cup \{\neg\chi\}$. Insbesondere ist $\mathcal{A}$ ein Modell von $T$ mit $\mathcal{A} \models \neg\chi$. Aber $\chi$ folgt aus $T$, was den gewünschten Widerspruch liefert.

□

Um den Vollständigkeitssatz zu beweisen, werden wir die äquivalente Umformulierung im Satz 2.55 beweisen. Wir müssen für eine widerspruchsfreien Theorie ein Modell konstruieren. Dafür führen wir neue Konstantenzeichen ein, welche erzwingen, dass die Theorie (in der erweiterten Sprache) genau die Kollektion aller Aussagen ist, welche in einer konkreten Struktur gelten.

**Lemma 2.56.** *Sei $T$ eine widerspruchsfreie Theorie und $\chi$ eine Aussage. Eine der beiden Theorien $T \cup \{\chi\}$ oder $T \cup \{\neg\chi\}$ muss auch widerspruchsfrei sein (eventuell beide).*

*Beweis.* Ansonsten wären $T \cup \{\chi\}$ und $T \cup \{\neg\chi\}$ beide widersprüchlich. Wegen der Tautologie $(\neg\neg\chi \longleftrightarrow \chi)$ bedeutet dies, dass $T \cup \{\neg\neg\chi\}$ und $T \cup \{\neg\chi\}$ beide widersprüchlich sind. Aus Korollar 2.54 folgt, dass $T \vdash \neg\chi$ und $T \vdash \chi$. Das heißt, die Theorie $T$ ist widersprüchlich. □

**Proposition 2.57.** *Jede widerspruchsfreie Theorie $T$ besitzt (mindestens) eine Vervollständigung, das heißt, die Theorie $T$ ist in einer vollständigen Theorie enthalten.*

*Beweis.* Sei $T$ eine widerspruchsfreie Theorie. Wir definieren auf

$$\mathcal{S} = \{T' \text{ widerspruchsfreie } \mathcal{L}\text{-Theorie mit } T \subset T'\}$$

eine partielle Ordnung durch

$$T_1 \leq T_2 \Longleftrightarrow T_1 \subset T_2.$$

Wir wollen zeigen, dass $\mathcal{S}$ induktiv ist (siehe C.1). Sei $\Gamma$ eine linear geordnete Teilmenge von $S$. Falls $\Gamma = \emptyset$, dann ist das Element $T$ aus $\mathcal{S}$ eine obere Schranke aus $\mathcal{S}$. Falls $\Gamma \neq \emptyset$, ist die Kollektion

$$T^* = \{\mathcal{L}\text{-Aussagen } \chi, \text{ so dass es } T' \text{ aus } \Gamma \text{ mit } \chi \in T' \text{ gibt}\}$$

eine Theorie, welche jedes $T'$ aus $\Gamma$ enthält. Insbesondere enthält $T^*$ die Theorie $T$. Es genügt also zu zeigen, dass $T^*$ in $\mathcal{S}$ liegt, das heißt, dass $T^*$ widerspruchsfrei ist. Sonst gäbe es wegen Bemerkung 2.52 $\varphi_1, \ldots, \varphi_n$ aus $T^*$ mit $\vdash \neg(\bigwedge_{i=1}^{n} \varphi_i)$. Dies bedeutet, dass es $T_1', \ldots, T_n'$ aus $\Gamma$ mit $\varphi_i$ in $T_i'$ gibt. Da $\Gamma$ linear geordnet ist, können wir $T_1' \leq \ldots \leq T_n'$ annehmen. Aber dann ist $T_n'$ widersprüchlich, weil sie alle Aussagen $\varphi_i$ enthält.
Aus dem Zorn'schen Lemma C.3 folgt, dass eine maximale Theorie $\widehat{T}$ in $\mathcal{S}$ existiert. Per Definition ist $\widehat{T}$ widerspruchsfrei und enthält $T$. Wir müssen nur zeigen, dass $\widehat{T}$ vollständig ist. Sei $\chi$ eine beliebige Aussage. Wegen Lemma 2.56 liegt $\widehat{T} \cup \{\chi\}$ oder $\widehat{T} \cup \{\neg\chi\}$ in $\mathcal{S}$. Aus der Maximalität von $\widehat{T}$ folgt, dass $\widehat{T} = \widehat{T} \cup \{\chi\}$ oder $\widehat{T} = \widehat{T} \cup \{\neg\chi\}$. Dementsprechend beweist $\widehat{T}$ trivialerweise die Aussage $\chi$ oder ihre Negation. □

**Bemerkung 2.58.** Falls die Sprache $\mathcal{L}$ abzählbar ist, kann man eine Vervollständigung der widerspruchsfreien Theorie $T$ direkt konstruieren: Da jede Aussage eine endliche Folge von Symbolen aus der Sprache ist (unter anderem Quantoren und logische Zeichen), ist die Kollektion aller $\mathcal{L}$-Aussagen auch abzählbar. Sei $\{\chi_n\}_{1\leq n\in\mathbb{N}}$ eine Aufzählung aller $\mathcal{L}$-Aussagen. Definiere rekursiv für jedes $n$ aus $\mathbb{N}$ eine Theorie $T_n \supset T$ in folgender Weise: Setze $T_0 = T$ und

$$T_{n+1} = \begin{cases} T_n \cup \{\chi_n\}, \text{ falls } T_n \cup \{\chi_n\} \text{ widerspruchsfrei ist.} \\ T_n \cup \{\neg\chi_n\}, \text{ sonst.} \end{cases}$$

Die Theorie $\widehat{T} = \bigcup_{n\in\mathbb{N}} T_n$ ist vollständig und enthält $T$. Bei der Konstruktion von $\widehat{T}$ können beide Fälle vorkommen, sodass es mehrere Vervollständigungen von $T$ geben kann.

**Definition 2.59.** Eine Theorie $T$ ist eine *Henkintheorie*, falls es zu jeder Formel $\varphi[x]$ ein Konstantenzeichen $c_\varphi$ derart gibt, dass

$$T \vdash \Big(\exists x\varphi[x] \longrightarrow \varphi[c_\varphi]\Big),$$

wobei $\varphi[c_\varphi] = \varphi_{c_\varphi/x}$.

**Lemma 2.60.** *Sei $\varphi[x]$ eine $\mathcal{L}$-Formel und $c$ ein neues Konstantenzeichen, das nicht aus $\mathcal{L}$ kommt. Falls $T$ widerspruchsfrei ist, so ist die $\mathcal{L}\cup\{c\}$-Theorie $T \cup \{\Big(\exists x\varphi[x] \longrightarrow \varphi[c]\Big)\}$ widerspruchsfrei.*

*Beweis.* Sonst wäre in der Sprache $\mathcal{L}\cup\{c\}$ wegen Korollar 2.54 die Aussage $\neg\Big(\exists x\varphi[x] \longrightarrow \varphi[c]\Big)$ aus $T$ beweisbar. Aus Bemerkung 2.47 folgt, dass es eine endliche Konjuntion $\theta$ von Aussagen aus $T$ gibt, sodass

$$\vdash_{\mathcal{L}\cup\{c\}} \Big(\theta \longrightarrow \neg(\exists x\varphi[x] \longrightarrow \varphi[c])\Big).$$

Insbesondere

$$\vdash_{\mathcal{L}\cup\{c\}} \Big(\neg\theta \vee (\exists x\varphi[x] \wedge \neg\varphi[c])\Big)$$

oder äquivalent dazu (mit Hilfe der entsqprechenden aussagenlogischen Tautologien):

$$\vdash_{\mathcal{L}\cup\{c\}} \Big((\neg\theta \vee \exists x\varphi[x]) \wedge (\neg\theta \vee \neg\varphi[c])\Big).$$

Dies bedeutet, dass sowohl $(\neg\theta \vee \exists x\varphi[x])$ als auch $(\neg\theta \vee \neg\varphi[c])$ in $\mathcal{L}\cup\{c\}$ beweisbar sind. Da $(\neg\theta \vee \exists x\varphi[x])$ eine $\mathcal{L}$-Aussage ist, heißt das, dass $(\neg\theta \vee \exists x\varphi[x])$ $\mathcal{L}$-beweisbar ist und somit ist dies auch $(\theta \longrightarrow \exists x\varphi[x])$.
Analog ist $(\varphi[c] \longrightarrow \neg\theta)$ beweisbar. Weil $c$ nicht aus $\mathcal{L}$ kommt, bedeutet dies, dass $(\varphi[x] \longrightarrow \neg\theta)$ als $\mathcal{L}$-Formel beweisbar ist, wegen Lemma 2.46. Mit $\exists$-Einführung (weil $\theta$ eine Aussage ist, kommt $x$ nicht frei vor), ist die Aussage $(\exists x\varphi[x] \longrightarrow \neg\theta)$ auch beweisbar.
Aus der aussagenlogischen Tautologie

$$\Big(\big((p \longrightarrow q) \wedge (q \longrightarrow \neg p)\big) \longrightarrow \neg p\Big)$$

folgt, dass $\neg\theta$ beweisbar ist. Aber $\theta$ ist eine endliche Konjunktion von Aussagen aus $T$, was mit Bemerkung 2.52 den gewünschte Widerspruch liefert. □

**Proposition 2.61.** *Jede widerspruchsfreie Theorie $T$ in der Sprache $\mathcal{L}$ ist in einer widerspruchsfreien Henkintheorie $T^+$ in der Sprache $\mathcal{L} \cup C$ enthalten, wobei $C$ eine Menge neuer Konstantenzeichen ist.*

*Beweis.* Sei $\{\varphi_i[x]\}_{i\in I}$ eine Aufzählung aller $\mathcal{L}$-Formeln in einer freien Variable. Desweiteren sei $c_i$ für jedes $i$ aus $I$ ein neues Konstantenzeichen, das nicht in $\mathcal{L}$ vorkommt, so dass $c_i \neq c_j$ für $i \neq j$. Setze $\mathcal{L}_0 = \mathcal{L}$ und $\mathcal{L}_1 = \mathcal{L} \cup \{c_i\}_{i\in I}$.
Mit iterierter Anwendung von Lemma 2.60 folgt, dass für jedes $i$ aus $I$ die Theorie

$$T_i = T \cup \bigcup_{j<i} \{\Big(\exists x \varphi_j[x] \longrightarrow \varphi_j[c_j]\Big)\}_{j\leq i}$$

widerspruchsfrei ist (in der Sprache $\mathcal{L} \cup \{c_j\}_{j\leq i}$). Insbesondere ist die $\mathcal{L}_1$-Theorie $T_1 = \bigcup_{i\in I} T_i$ widerspruchsfrei. Sie enthält $T$ und hat die Eigenschaft, dass es für jede $\mathcal{L}_0$-Formel $\varphi[x]$ ein Konstantenzeichen $c_\varphi$ aus $\mathcal{L}_1$ gibt, sodass

$$T_1 \vdash \Big(\exists x \varphi[x] \longrightarrow \varphi[c_\varphi]\Big).$$

Wir iterieren dieses Verfahren und konstruieren so in einer Spracherweiterung $\mathcal{L}_2$ eine Theorie $T_2$ aus $T_1$ mit den obigen Eigenschaften. Und dementsprechend allgemein $T_{n+1}$ aus $T_n$. Setze

$$T^+ = \bigcup_{n\in\mathbb{N}} T_n$$

in der Sprache $\mathcal{L}^+ = \bigcup_{n\in\mathbb{N}} \mathcal{L}_n$. Jede $\mathcal{L}^+$ Formel muss dann für ein $n$ aus $\mathbb{N}$ eine $\mathcal{L}_n$-Formel sein. Daraus folgt, dass $T^+$ eine Henkintheorie ist. □

**Bemerkung 2.62.** Wenn die $\mathcal{L}$-Theorie $T$ eine Henkintheorie ist, so ist jede Vervollständigung eine Henkintheorie.

**Satz 2.63.** *Jede vollständige Henkintheorie $T$ in der Sprache $\mathcal{L}$ besitzt ein Modell, welches nur aus Interpretationen der Konstantenzeichen besteht. Ferner ist solch ein Modell bis auf Isomorphie eindeutig bestimmt.*

*Beweis.* Die Eindeutigkeit ist leicht zu zeigen. Sei $C$ die Menge der Konstantenzeichen aus $\mathcal{L}$. Falls $\mathcal{A} = (c^{\mathcal{A}})_{c\in C}$ und $\mathcal{B} = (c^{\mathcal{B}})_{c\in C}$ zwei solche Modelle sind, dann sind sie wegen Bemerkung 2.51 elementar äquivalent. Insbesondere gilt für $c$ und $d$ aus $C$

$$c^{\mathcal{A}} = d^{\mathcal{A}} \Longleftrightarrow c^{\mathcal{B}} = d^{\mathcal{B}}.$$

Die Funktion

$$\begin{array}{rccc} F: & A & \to & B \\ & c^{\mathcal{A}} & \mapsto & c^{\mathcal{B}} \end{array}$$

ist eine Bijektion. Es genügt zu zeigen, dass $F$ einen Isomorphismus zwischen den $\mathcal{L}$-Strukturen $\mathcal{A}$ und $\mathcal{B}$ definiert, was sofort aus den folgenden Überlegungen für jedes Funktionszeichen $f$, bzw Relationszeichen $R$, folgt.

$$c^{\mathcal{A}}_{n+1} = f(c^{\mathcal{A}}_1, \ldots, c^{\mathcal{A}}_n) \Longleftrightarrow c^{\mathcal{B}}_{n+1} = f(c^{\mathcal{B}}_1, \ldots, c^{\mathcal{B}}_n) \text{ und}$$

$$(c_1^{\mathcal{A}}, \ldots, c_k^{\mathcal{A}}) \in R^{\mathcal{A}} \Longleftrightarrow (c_1^{\mathcal{B}}, \ldots, c_k^{\mathcal{B}}) \in R^{\mathcal{B}}.$$

Wir müssen also nur zeigen, dass so ein Model $\mathcal{A}$ existiert. Definiere auf der Menge $C$ der Konstantenzeichen folgende Relation:

$$c \sim d \Longleftrightarrow T \vdash c \doteq d.$$

Aus den Gleichheitsaxiomen (mit Hilfe von Modus Ponens und Lemma 2.45) folgt, dass $\sim$ eine Äquivalenzrelation auf $C$ ist. Sei $A$ die Menge der Äquivalenzklassen $c/\sim$. Wir wollen eine $\mathcal{L}$-Struktur $\mathcal{A}$ auf der Menge $A$ definieren.

**Behauptung 1.** *Für jedes $n$-stellige Funktionszeichen $f$ aus $\mathcal{L}$ und alle $c_1, \ldots, c_n$ aus $C$ gibt es ein $c$ aus $C$, sodass $T \vdash (f(c_1, \ldots, c_n) \doteq c)$.*

*Beweis der Behauptung 1.* Sei $\varphi[x] = (f(c_1, \ldots, c_n) \doteq x)$. Weil $T$ eine Henkintheorie ist, gibt es ein Konstantenzeichen $c$ aus $C$ derart, dass

$$T \vdash (\exists x \varphi[x] \longrightarrow \varphi[c]).$$

Aus den Gleichheitsaxiomen und dem Lemma 2.45 folgt, dass $T \vdash \Big(f(c_1, \ldots, c_n) \doteq f(c_1, \ldots, c_n)\Big)$ und somit

$$T \vdash \left(\Big(f(c_1, \ldots, c_n) \doteq f(c_1, \ldots, c_n)\Big) \longrightarrow \exists x \varphi\right),$$

weil $x$ frei für $f(c_1, \ldots, c_n)$ in $\varphi[x]$ ist. Aus iteriertem Modus Ponens folgt, dass

$$T \vdash (f(c_1, \ldots, c_n) \doteq c),$$

wie gewünscht. $\square_{\text{Beh 1}}$

Definiere dementsprechend:

- $c^{\mathcal{A}} = c/\sim$;
- $f^{\mathcal{A}}(c_1/\sim, \ldots, c_n/\sim) = c/\sim \Longleftrightarrow T \vdash (f(c_1, \ldots, c_n) \doteq c)$;
- $(c_1/\sim, \ldots, c_k/\sim) \in R^{\mathcal{A}} \Longleftrightarrow T \vdash R(c_1, \ldots, c_k)$.

Beachte, dass diese Interpretationen wohldefiniert sind (dies besagen die Gleichheitsaxiome mit Hilfe von Modus Ponens und Lemma 2.45).
Induktiv über den Aufbau des Termes $t$ ohne freie Variablen können wir leicht zeigen, dass

$$t^{\mathcal{A}} = c^{\mathcal{A}} \Longleftrightarrow T \vdash (t \doteq c).$$

Wir wollen nun beweisen, dass $\mathcal{A}$ ein Modell von $T$ ist. Es genügt folgende Äquivalenz induktiv über den Aufbau der $\mathcal{L}$-Aussage $\chi$ zu zeigen:

$$\mathcal{A} \models \chi \Longleftrightarrow T \vdash \chi,$$

Für $\chi = (t_1 \doteq t_2)$, wobei $t_1$ und $t_2$ Terme ohne freie Variablen sind, existieren $c$ und $d$ aus $C$ mit $t_1^{\mathcal{A}} = c^{\mathcal{A}}$ und $t_2^{\mathcal{A}} = d^{\mathcal{A}}$. Insbesondere gilt $T \vdash \Big((t_1 \doteq c) \wedge (t_2 \doteq d)\Big)$ und

$$\mathcal{A} \models (t_1 \doteq t_2) \Longleftrightarrow \mathcal{A} \models (c \doteq d) \Longleftrightarrow T \vdash (c \doteq d) \Longleftrightarrow T \vdash (t_1 \doteq t_2).$$

Genauso sieht man die Äquivalenz für den Fall $\chi = R(t_1, \ldots, t_k)$. Der Fall $\chi = (\chi_1 \vee \chi_2)$ ist trivial. Falls $\chi = \neg\psi$, gilt

$$\mathcal{A} \models \chi \iff \mathcal{A} \not\models \psi \iff T \not\vdash \psi \overset{T\text{vollst.}}{\iff} T \vdash \chi.$$

Es ist nur noch der Fall $\chi = \exists x\psi$ übrig. Falls $\mathcal{A} \models \chi$, dann gibt es ein Element $d/\sim = d^{\mathcal{A}}$ aus $A$ mit $\mathcal{A} \models \psi[d/\sim]$. Dies bedeutet, dass $\mathcal{A} \models \psi[d]$ und aus der Induktion folgt $T \vdash \psi[d]$. Weil $d$ keine Variablen enthält, ist $x$ frei für $d$ in $\psi[x]$. Insbesondere folgt aus dem $\exists$-Quantorenaxiom, dass $\vdash (\psi[d] \longrightarrow \exists x\psi[x])$. Insbesondere gilt $T \vdash \exists x\psi[x]$, das heißt, $T \vdash \chi$.
Falls $T \vdash \chi$, gibt es ein $c$ aus $C$ mit $T \vdash (\chi \longrightarrow \psi[c])$, weil $T$ eine Henkintheorie ist. Also $T \vdash \psi[c]$ und induktiv erfüllt das Element $c/\sim$ aus $\mathcal{A}$ die Formel $\psi[x]$. Dies bedeutet, dass $\mathcal{A} \models \chi$. □

Aus den Sätzen 2.55 und 2.63, und den Propositionen 2.57 und 2.61 folgt der Vollständigkeitssatz:

**Korollar 2.64** (Vollständigkeitssatz)**.** *Gegeben eine Theorie $T$ und eine Aussage $\chi$,*

$$T \models \chi \iff T \vdash \chi.$$

Zusammen mit der Bemerkung 2.24 bekommen wir:

**Korollar 2.65.** *Eine konsistente Theorie ist genau dann vollständig, wenn je zwei Modelle elementar äquivalent sind.*

**Korollar 2.66** (Kompaktheitssatz)**.** *Eine Theorie ist genau dann konsistent, wenn jede endliche Teiltheorie konsistent ist.*

*Beweis.* Wir müssen nur zeigen, dass $T$ ein Modell besitzt, wenn jede endliche Teiltheorie von $T$ konsistent ist. Sonst wäre $T$ wegen Satz 2.55 nicht widerspruchsfrei und es gäbe Beweise aus $T$ von den Aussagen $\chi$ und $\neg\chi$. Jeder dieser Beweise benutzt nur endlich viele Aussagen aus $T$. Die entsprechende endliche Teiltheorie kann kein Modell besitzen. □

**Korollar 2.67** (Abzählbares aufwärts/abwärts Löwenheim-Skolem)**.** *Jede konsistente Theorie in einer abzählbaren Sprache besitzt ein abzählbares Modell. Falls $T$ unendliche Modelle (oder beliebig große endliche Modelle) besitzt, dann hat sie auch ein Modell der Mächtigkeit Kontinuum, (das heißt, ein Modell der Mächtigkeit der reellen Zahlen $\mathbb{R}$).*

*Beweis.* Beachte, dass die Sprache der zu $T$ gehörigen Henkintheorie wiederum abzählbar ist. Insbesondere ist das Modell, welches aus den Interpretationen der Konstanten besteht, auch abzählbar.
Falls $T$ ein unendliches Modell (oder beliebig große endliche Modelle) besitzt, wähle neue paarweise verschiedene Konstantenzeichen $\{c_r\}_{r\in\mathbb{R}}$ und definiere

$$T' = T \cup \{\neg(c_r \doteq c_s)\}_{r\neq s\in\mathbb{R}}.$$

Diese Theorie ist endlich konsistent, das heißt, jede endliche Teiltheorie ist konsistent. Insbesondere gibt es ein Modell, welche aus Interepretationen der Konstantenzeichen besteht. Wir haben Kontinuum viele Konstantenzeichen und sie liefern verschiedene Elemente. □

**Korollar 2.68.** *Sei $\mathcal{C}$ eine Klasse endlicher $\mathcal{L}$-Strukturen, welche für jedes $n$ aus $\mathbb{N}$ eine Struktur der Mächtigkeit zumindest $n$ enthält. Die Klasse $\mathcal{C}$ ist nicht axiomatisierbar (siehe Definition 2.25).*
*Insbesondere ist die Klasse aller endlichen Gruppen (in der Gruppensprache $\mathcal{L}_{Gp}$) sowie die Klasse aller endlichen vollständigen Graphen (in der Sprache $\mathcal{L}_{Graphen}$) nicht axiomatisierbar.*

Mit Hilfe der Bemerkung 2.26 läßt sich folgendes leicht mit Kompaktheit zeigen:

**Korollar 2.69.** *In der Sprache $\mathcal{L} = \{0, +\}$ gibt es eine* nichtstandard *Erweiterung $\mathcal{M}$ der Struktur $\mathcal{N} = (\mathbb{N}, 0, +)$, das heißt, die Struktur $\mathcal{M}$ ist eine elementare Erweiterung von $\mathcal{N}$ und besitzt ein Element $m$ aus $M$, welche von jeder Primzahl aus $\mathbb{N}$ sich teilen läßt.*

*Analog besitzt die Struktur $(\mathbb{R}, <)$ elementar Erweiterungen mit nichtstandard Elementen, welche großer als alle reellen Zahlen sind.*

# Kapitel 3

# Unentscheidbarkeit

Es gibt mehrere mathematische Modelle, welche die Idee eines Algorithmus formalisieren: Gödel führte *rekursive Funktionen* für seinen Beweis der Unvollständigkeit ein (Satz 3.47), wobei Turing und Church Machinen bzw. das $\lambda$-Kalkül einführten. Diese drei Begriffe der Berechenbarkeit sind äquivalent und somit wurde die Church'sche These eingeführt, welche besagt, dass *alle* Begriffe der Berechenbarkeit äquivalent sein sollen. Selbstverständlich ist diese These nicht beweisbar ohne den Begriff des Algorithmus einführen zu müssen. Der Unvollständigkeitssatz besagt, dass es keinen Algorithmus gibt, der im Voraus entscheiden kann, ob eine Aussage erster Stufe beweisbar ist oder nicht. Konkrete Sätze, die unabhängig vom Axiomensystem sind, sind unter anderem die Kontinuumshypothese (bezüglich des Axiomensystems ZFC der Mengenlehre) oder die Aussage, dass Goodstein'sche Folgen immer aufhören (in jedem Modell der Peanoarithmetik).

## 3.1 Rekursivität

In diesem gesamten Abschnitt verstehen wir unter *Funktion* eine Abbildung von einem (beliebigen) kartesischen Produkt von $\mathbb{N}$ nach $\mathbb{N}$.

**Definition 3.1.** Die Kollektion der *primitiv rekursiven Funktionen* ist die kleinste Menge PREK von Funktionen, welche die *Grundfunktionen*:

**Nachfolger** $S: \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ x & \mapsto & x+1 \end{array}$;

**Projektion** $\pi_i^n: \begin{array}{ccc} \mathbb{N}^n & \to & \mathbb{N} \\ (x_1,\ldots,x_n) & \mapsto & x_i \end{array}$ und

**Konstantenfunktion Null (sogar nullstellig)** $\mathbf{0}: \begin{array}{ccc} \mathbb{N}^n & \to & \mathbb{N} \\ (x_1,\ldots,x_n) & \mapsto & 0 \end{array}$

enthält und unter folgenden Operationen abgeschlossen ist:

**Komposition** Für jede $m$-stellige Funktion $h$ in PREK und $n$-stellige Funktionen $g_1,\ldots,g_m$ in PREK ist die folgende Funktion in PREK

$$f: \begin{array}{ccc} \mathbb{N}^n & \to & \mathbb{N} \\ (x_1,\ldots,x_n) & \mapsto & h(g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n)) \end{array}$$

**Primitive Rekursion** Für jede $n$-stellige Funktion $g$ und $(n+2)$-stellige Funktion $h$ in PREK ist

$$\begin{array}{rccl} f: & \mathbb{N}^{n+1} & \to & \mathbb{N} \\ & (x_1,\ldots,x_n,y) & \mapsto & \begin{cases} g(x_1,\ldots,x_n), \text{ für } y=0 \\ h(x_1,\ldots,x_n,z,f(x_1,\ldots,x_n,z)), \text{ für } y=z+1 \end{cases} \end{array}$$

in PREK.

**Beispiel 3.2.** Diese Funktionen sind in PREK:

- $\begin{array}{rccl} +: & \mathbb{N}^2 & \to & \mathbb{N} \\ & (x,y) & \mapsto & x+y \end{array}$
- $\begin{array}{rccl} x \dot{-} 1: & \mathbb{N} & \to & \mathbb{N} \\ & x & \mapsto & \begin{cases} 0, \text{ falls } x=0 \\ z, \text{ falls } x=z+1 \end{cases} \end{array}$
- $\begin{array}{rccl} x \dot{-} y: & \mathbb{N}^2 & \to & \mathbb{N} \\ & (x,y) & \mapsto & \begin{cases} x, \text{ falls } y=0 \\ (x \dot{-} z) \dot{-} 1, \text{ falls } y=z+1 \end{cases} \end{array}$ **Beschränkte Differenz**
- $\begin{array}{rccl} x \cdot y: & \mathbb{N}^2 & \to & \mathbb{N} \\ & (x,y) & \mapsto & \begin{cases} 0, \text{ falls } y=0 \\ x \cdot z + x, \text{ falls } y=z+1 \end{cases} \end{array}$
- $\begin{array}{rccl} !: & \mathbb{N} & \to & \mathbb{N} \\ & x & \mapsto & \begin{cases} 1 = S(0), \text{ falls } x=0 \\ x \cdot z! \text{ falls } x=z+1 \end{cases} \end{array}$

**Definition 3.3.** Die Kollektion der *rekursiven Funktionen* ist die kleinste Menge REK von Funktionen, welche alle Projektionen, die Nachfolger- und die Null-Konstantenfunktion enthält und unter Komposition und primitiver Rekursion sowie der folgenden Operation abgeschlossen ist:

**$\mu$-Rekursion** Falls für die rekursive Funktion $g: \mathbb{N}^{n+1} \to \mathbb{N}$ gilt, dass für alle $x_1,\ldots,x_n$ ein $y$ aus $\mathbb{N}$ mit $g(x_1,\ldots,x_n,y)=0$ existiert, dann ist die Funktion

$$\begin{array}{rccl} \mu y\, g(x_1,\ldots,x_n,y)=0: & \mathbb{N}^n & \to & \mathbb{N} \\ & (x_1,\ldots,x_n) & \mapsto & \text{kleinstes } z \text{ mit } g(x_1,\ldots,x_n,z)=0 \end{array}$$

auch rekursiv.

**Definition 3.4.** Eine Teilmenge $A \subset \mathbb{N}^k$ ist *(primitiv) rekursiv*, falls ihre charakteristische Funktion

$$\begin{array}{rccl} \chi_A: & \mathbb{N}^k & \to & \mathbb{N} \\ & (x_1,\ldots,x_k) & \mapsto & \begin{cases} 1, \text{ falls } (x_1,\ldots,x_k) \in A \\ 0, \text{ sonst.} \end{cases} \end{array}$$

(primitiv) rekursiv ist.

**Beispiel 3.5.** Die Relation $<$ ist primitiv rekursiv, das heißt, die Teilmenge $\{(x,y) \in \mathbb{N}^2 \,|x < y\}$ ist primitiv rekursiv, weil

$$\chi_<(x,y) = 1 \Longleftrightarrow y \dot{-} x \neq 0.$$

Man sieht leicht, dass die einstellige Relation $z \neq 0$ primitiv rekursiv ist.

**Lemma 3.6.** *Falls $A$ und $B$ (primitiv) rekursive Teilmengen von $\mathbb{N}^k$ sind, dann sind*

- $A \cup B$*;*
- $A \cap B$*;*
- $A \setminus B$*;*
- $\{(x_1,\ldots,x_n) \in \mathbb{N}^n \,|\, (f_1(x_1,\ldots,x_n),\ldots,f_k(x_1,\ldots,x_n)) \in A\}$*, für alle (primitiv) rekursive Funktionen $f_1,\ldots,f_k$;*

*auch (primitiv) rekursiv.*

**Lemma 3.7.** *Gegeben (primitiv) rekursive Teilmengen $A_1,\ldots,A_n$ von $\mathbb{N}^k$ und $k$-stellige (primitiv) rekursive Funktionen $f_1,\ldots,f_{n+1}$, ist die* Fallunterscheidungsfunktion

$$\begin{array}{rccl} f: & \mathbb{N}^k & \to & \mathbb{N} \\ & (x_1,\ldots,x_k) & \mapsto & \begin{cases} f_1(x_1,\ldots,x_k), \text{ falls } (x_1,\ldots,x_k) \in A_1 \\ f_2(x_1,\ldots,x_k), \text{ falls } (x_1,\ldots,x_k) \in A_2 \setminus A_1 \\ \vdots \\ f_n(x_1,\ldots,x_k), \text{ falls } (x_1,\ldots,x_k) \in A_n \setminus \Big(\bigcup\limits_{1\leq j<n} A_j\Big) \\ f_{n+1}(x_1,\ldots,x_k), \text{ falls } (x_1,\ldots,x_k) \notin \bigcup\limits_{1\leq j\leq n} A_j \end{cases} \end{array}$$

*auch (primitiv) rekursiv.*

*Beweis.* Aus dem Lemma 3.6 folgt, dass für jedes $i \leq n$ die Teilmenge $B_i = A_i \setminus \Big(\bigcup\limits_{1\leq j<i} A_j\Big)$ (primitiv) rekursiv ist. Damit ist auch $B_{n+1} = \mathbb{N}^k \setminus \Big(\bigcup\limits_{1\leq j\leq n} A_j\Big)$ (primitiv) rekursiv. Beachte, dass die $B_i$'s paarweise disjunkt sind und dass

$$f(x_1,\ldots,x_k) = f_1(x_1,\ldots,x_k)\chi_{B_1}(x_1,\ldots,x_k) + \ldots + f_{n+1}(x_1,\ldots,x_k)\chi_{B_{n+1}}(x_1,\ldots,x_k).$$

□

**Korollar 3.8.** *Sind $A \subset B \subset \mathbb{N}^k$ Teilmengen derart, dass $B \setminus A$ endlich und $A$ (primitiv) rekursiv ist, so ist $B$ (primitiv) rekursiv.*

**Lemma 3.9.** *Wenn $A \subset \mathbb{N}^{k+1}$ eine (primitiv) rekursive Teilmenge ist, dann sind*

- $B = \{(x_1,\ldots,x_k,y) \in \mathbb{N}^{k+1} \,|\, \forall z < y\Big((x_1,\ldots,x_k,z) \in A\Big)\}$

- $C = \{(x_1, \ldots, x_k, y) \in \mathbb{N}^{k+1} \mid \exists z < y \Big( (x_1, \ldots, x_k, z) \in A \Big) \}$

*auch (primitiv) rekursiv.*

*Beweis.* Man sieht leicht, dass

$$\chi_B(x_1, \ldots, x_k, y) = \begin{cases} 1, \text{ falls } y = 0 \\ \chi_B(x_1, \ldots, x_k, z) \cdot \chi_A(x_1, \ldots, x_k, z), \text{ falls } y = z + 1 \end{cases} .$$

Aus Lemma 3.6 und der obigen Überlegung folgt, dass $C$ auch (primitiv) rekursiv ist, weil

$$(x_1, \ldots, x_k, y) \in C \iff \neg \forall z < y \Big( (x_1, \ldots, x_k, z) \in \mathbb{N}^k \setminus A \Big).$$

□

**Lemma 3.10.** *Seien $A \subset \mathbb{N}^{k+1}$ und $f : \mathbb{N}^k \to \mathbb{N}$ primitiv rekursiv, sodass es für jedes $(x_1, \ldots, x_k)$ aus $\mathbb{N}^k$ ein $y$ aus $\mathbb{N}$ mit $y \leq f(x_1, \ldots, x_k)$ und $(x_1, \ldots, x_k, y)$ in $A$ gibt. Die Funktion $g(x_1, \ldots, x_k) = \mu y \, (x_1, \ldots, x_k, y) \in A$ ist primitiv rekursiv.*

Wir wissen, dass die Funktion $g$ rekursiv ist, weil sie mit Hilfe der $\mu$-Rekursion aus $\chi_A$ gewonnen wird. Da ein mögliches $y$ im Voraus mit Hilfe der Funktion $f$ abgeschätzt werden kann, ist die $\mu$-Rekursion nicht nötig.

*Beweis.* Definiere $h(x_1, \ldots, x_k, y) = \mu z \Big( (x_1, \ldots, x_k, z) \in A \vee z = y) \Big)$. Weil

$$h(x_1, \ldots, x_k, y) = \begin{cases} 0, \text{falls } y = 0 \\ h(x_1, \ldots, x_k, u), \text{falls } y = u + 1 \text{ und } (x_1, \ldots, x_k, h(x_1, \ldots, x_k, u)) \in A \\ y, \text{ sonst} \end{cases}$$

ist die Funktion $h$ primitiv rekursiv, denn wie im Beweis vom Lemma 3.7 ist

$$\begin{aligned} h(x_1, \ldots, x_n, u + 1) &= h(x_1, \ldots, x_k, u) \cdot \chi_A(x_1, \ldots, x_n, h(x_1, \ldots, x_k, u)) + \\ &\quad S(u) \cdot \big(1 \dot{-} \chi_A(x_1, \ldots, x_n, h(x_1, \ldots, x_k, u))\big). \end{aligned}$$

Beachte, dass $g(x_1, \ldots, x_k) = h(x_1, \ldots, x_k, f(x_1, \ldots, x_k))$ weil es immer ein $y \leq f(x_1, \ldots, x_k)$ mit $(x_1, \ldots, x_k, y)$ in $A$ gibt . Insbesondere ist $g$ primitiv rekursiv. □

**Lemma 3.11.** *Folgende Funktionen und Teilmengen sind primitiv rekursiv:*

- *Das zweistellige Prädikat* teilen*:*

$$x \mid y \iff y = x \cdot z, \text{ für ein } z \in \mathbb{N}.$$

- $\mathbb{PRIM} = \{x \in \mathbb{N} \text{ Primzahl}\}$ *und* $p : \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & (n+1)\text{-te Primzahl} \end{array}$

*Beweis.* Sei $\text{Rest}(x,y)$ die Funktion, welche den Rest der Divison von $y$ durch $x$ gibt, falls es Sinn macht. Beachte, dass

$$\begin{array}{rccl} \text{Rest}: & \mathbb{N}^2 & \to & \mathbb{N} \\ & (x,y) & \mapsto & \begin{cases} 0, \text{ falls } y = 0 \\ \left.\begin{cases} \text{Rest}(x,z)+1 \text{ falls Rest}(x,z)+1 < x \\ 0, \text{ sonst} \end{cases}\right\}, \text{ falls } y = z+1 \end{cases} \end{array}$$

Nun gilt $x \mid y$ genau dann, wenn $y = 0$ oder $\text{Rest}(x,y) = 0$ und sowohl $x$ und $y$ beide verschieden von 0.

Ein Element $x$ gehört genau dann zu $\mathbb{PRIM}$, falls $1 < x$ und

$$\forall z < x \, (z = 1 \vee z \nmid x) \, .$$

Wegen Lemma 3.9 ist $\mathbb{PRIM}$ primitiv rekursiv. Induktiv zeigt man, dass die $(n+1)$-te Primzahl $p(n)$ durch $2^{2^n}$ beschränkt ist, weil $p(n) \leq 1 + \prod_{k<n} p(k)$. Aus dem Lemma 3.10 folgt, dass

$$\begin{array}{rccl} p: & \mathbb{N} & \to & \mathbb{N} \\ & x & \mapsto & \begin{cases} 2 = S(S(0)), \text{ falls } x = 0 \\ \mu w(w \in \mathbb{PRIM} \wedge p(z) < w), \text{ falls } x = z+1 \end{cases} \end{array}$$

primitiv rekursiv ist. □

Im Folgenden werden wir eine andere Präsentation der rekursiven Funktionen geben.

**Lemma 3.12.** *Sei $\mathcal{F}$ die Teilkollektion der rekursiven Funktionen, welche die Konstanten-, Nachfolger- und Koordinatenfunktionen sowie $+$, $\cdot$ und $\chi_<$ enthält und unter Komposition und $\mu$-Rekursion abgeschlossen ist. Folgende Funktionen sind in $\mathcal{F}$:*

- *$x \dot{-} y$;*
- *$\chi_{A\cap B}$, $\chi_{A\cup B}$ und $\chi_{\mathbb{N}^k\setminus A}$, falls $\chi_A$ und $\chi_B$ in $\mathcal{F}$ liegen;*
- *$\chi_R$, wobei $(x,y)$ in $R \subset \mathbb{N}^2$ genau dann liegt, falls $\exists z < y((x,z) \in A)$ mit $\chi_A$ in $\mathcal{F}$;*
- *$\chi_=$;*
- *$\chi_{\text{mod}}$, wobei $\text{mod} = \{(x,y,z) \in \mathbb{N}^3 \mid x \equiv y \mod z\}$;*
- *Definition aus Fallunterscheidung (siehe Lemma 3.7), wenn alle Funktionen und Teilmengen in $\mathcal{F}$ liegen.*

*Beweis.* Beachte, dass $x \dot{-} y = \mu z\Big(x < y + z + 1\Big)$. Der zweite Teil der Behauptung ist trivial. Sei $A \subset \mathbb{N}^2$ mit $\chi_A$ in $\mathcal{F}$. Wir definieren $g(x,y) = \mu z\Big(z = y \vee (x,z) \in A\Big)$. Nun liegt $(x,y)$ genau dann in $R = \exists z < y\Big((x,z) \in A\Big)$, wenn $g(x,y) < y$. Weil $g$ in $\mathcal{F}$ liegt, ist somit auch $\chi_R$ in $\mathcal{F}$.

Aus der Ordnung $<$ kann man leicht Gleichheit definieren. Falls $x$ und $y$ äquivalent modulo $z$ sind, gibt es ein Element $w$ aus $\mathbb{N}$ mit $|x-y| = z \cdot w$. Für $z = 0$ sind $x$ und $y$ genau dann äquivalent, wenn $\chi_=(x,y) = 1$. Ansonsten bedeutet dies, dass $w \leq |x-y| \leq x+y < x+y+1$. Insbesondere ist

$$\chi_{\text{mod}}(x,y,z) = 1 \iff \Big((z = 0 \wedge \chi_=(x,y) = 1) \vee \exists w < x+y+1 (x = y + z \cdot w \vee y = x + z \cdot w)\Big),$$

und somit liegt $\chi_{\text{mod}}$ auch in $\mathcal{F}$. Letztlich ist eine Definition aus Fallunterscheidung klarerweise in $\mathcal{F}$, weil $\mathcal{F}$ unter Produkten, Summen und charakteristischen Funktionen von boolschen Kombinationen aus (charakteristischen Funktionen von) Mengen aus $\mathcal{F}$ abgeschlossen ist. □

**Lemma 3.13.** *Es existiert eine Funktion $\beta : \mathbb{N}^3 \to \mathbb{N}$ in $\mathcal{F}$, sodass es für jedes $n$ aus $\mathbb{N}$ und $c_0, \ldots, c_{n-1}$ aus $\mathbb{N}$ natürliche Zahlen $a$ und $b$ mit $\beta(a,b,i) = c_i$ für $0 \leq i \leq n-1$ gibt.*

*Beweis.* Sei $b$ ein Element aus $\mathbb{N}$, welches durch jede natürliche Zahl zwischen 2 und $n$ teilbar ist und $c_i < b$ für alle $i < n$ erfüllt. Zum Beispiel $b = (\max(c_1, \ldots, c_{n-1}) + 1)!$.
Wir zeigen zuerst, dass die Zahlen $1+b, 1+2b, \ldots, 1+nb$ paarweise teilerfremd sind: Falls $i < j$ und die Primzahl $p$ sowohl $1+ib$ als auch $1+jb$ teilt, dann teilt $p$ auch die Differenz $(j-i)b$. Aber $p$ kann $b$ nicht teilen, weil $p$ sonst $1 = (1+ib) - ib$ teilen müsste. Daher teilt $p$ die Zahl $j - i < n$. Weil $b$ von $j-i$ teilbar ist, teilt $p$ die Zahl $b$, was den gewünschten Widerspruch liefert.
Wegen dem Chinesischen Restsatz D.1, gibt es eine Lösung $a$ in $\mathbb{N}$ (sogar mit $a \leq \prod_{i=1}^{n} 1+ib$) für das Kongruenzensystem

$$\left.\begin{array}{rcccl} x & \equiv & c_0 & \mod & 1+b \\ & \vdots & & \vdots & \\ x & \equiv & c_{n-1} & \mod & 1+nb \end{array}\right\}$$

Weil $c_i < b < 1 + (i+1)b$ für $i < n$, ist $c_i$ die kleinste natürliche Zahl, welche zu $a$ kongruent modulo $1+(i+1)b$ ist. Die Funktion

$$\beta(x,y,z) = \mu w \Big(w \equiv x \bmod 1 + (z+1)y\Big)$$

liegt in $\mathcal{F}$ wegen Lemma 3.12 und erfüllt, dass $\beta(a,b,i) = c_i$ für $0 \leq i < n$. □

**Satz 3.14.** $\mathcal{F} = \text{REK}$.

*Beweis.* Wir müssen nur zeigen, dass die Klasse $\mathcal{F}$ von rekursiven Funktionen unter primitiver Rekursion abgeschlossen ist. Seien hierfür $g$ und $h$ aus $\mathcal{F}$. Wir definieren

$$\begin{array}{rccl} f: & \mathbb{N}^{n+1} & \to & \mathbb{N} \\ & (x_1, \ldots, x_n, y) & \mapsto & \begin{cases} g_1(x_1, \ldots, x_n), \text{ für } y = 0 \\ h(g(x_1, \ldots, x_n), z, f(x_1, \ldots, x_n, z)), \text{ für } y = z+1 \end{cases} \end{array}$$

und mit $\bar{x} = (x_1, \ldots, x_n)$ setzen wir $c_0 = g(\bar{x})$ und $c_{i+1} = h(\bar{x}, i, f(\bar{x}, i))$ für $i < k \in \mathbb{N}$. Wegen Lemma 3.13 gibt es $a$ und $b$ aus $\mathbb{N}$ mit $\beta(a,b,i) = c_i$. Dies bedeutet, dass

$$\forall 0 < i < k \Big(\beta(a,b,i+1) = c_i = h(\bar{x}, i, \beta(a,b,i))\Big).$$

Wegen Lemma 3.12 ist die charakteristische Funktion der Teilmenge $R \subset \mathbb{N}^{n+3}$ mit

$$(\bar{x}, y, a, b) \in R \iff \Big( \Big( \beta(a,b,0) = g(\bar{x}) \Big) \wedge \forall z < y \Big( \beta(a,b,z+1) = h(\bar{x}, z, \beta(a,b,z)) \Big) \Big)$$

in $\mathcal{F}$. Für gegebene $\bar{x}$ und $y$ gibt es nach Konstruktion $a$ und $b$ (und somit ein $s = \max(a,b)$) mit $(\bar{x}, y, a, b) \in R$. Daher ist $S(\bar{x}, y) = \mu s \Big( \exists a \exists b ((a \leq s) \wedge (b \leq s) \wedge (\bar{x}, y, a, b) \in R) \Big)$ auch in $\mathcal{F}$. Es genügt induktiv auf $y$ zu zeigen, dass

$$f(\bar{x}, y) = \mu z \Big( \exists a \exists b ((a \leq S(\bar{x}, y)) \wedge (b \leq S(\bar{x}, y)) \wedge (\bar{x}, y, a, b) \in R) \wedge (z = \beta(a,b,y)) \Big).$$

Sei $\tilde{f}(\bar{x}, y)$ die Funktion auf der rechten Seite, welche klarerweise in $\mathcal{F}$ liegt. Der Wert $\tilde{f}(\bar{x}, 0)$ ist der kleinste Wert $\beta(a,b,0)$ sodass $(\bar{x}, 0, a, b)$ in $R$ liegt. Aber $\beta(a,b,0) = g(\bar{x}) = f(\bar{x}, 0)$. Für $y = z+1$ ist $\tilde{f}(\bar{x}, z+1)$ der kleinste Wert $\beta(a,b,z+1)$ sodass $(\bar{x}, z+1, a, b)$ in $R$ liegt. Also $\tilde{f}(\bar{x}, z+1) = \beta(a,b,z+1) = h(\bar{x}, z, \beta(a,b,z))$. Für $z < y+1$ liegt $(\bar{x}, z, a, b)$ auch in $R$, also $f(\bar{x}, z) = \tilde{f}(\bar{x}, z) = \beta(a,b,z)$ und somit ist $\tilde{f}(\bar{x}, z+1) = h(\bar{x}, z, f(\bar{x}, z)) = f(\bar{x}, z+1)$, wie gewünscht. □

## 3.2 Gödelisierung und rekursiv aufzählbare Mengen

**Notation.** Sei $\mathcal{S}$ die Kollektion aller endlichen Folgen aus $\mathbb{N}$. Wir definieren folgende Funktion:

$$\begin{array}{rccl} \langle \cdot \rangle : & \mathcal{S} & \to & \mathbb{N} \\ & s & \mapsto & \begin{cases} 0, \text{ falls } s \text{ die leere Folge ist.} \\ p(0)^{x_0} \cdots p(n-2)^{x_{n-2}} p(n-1)^{x_{n-1}+1} - 1 \text{ falls } s = (x_0, \ldots, x_{n-1}) \end{cases} \end{array},$$

wobei $p$ die Funktion aus Lemma 3.11 ist. Wir schreiben $\langle x_0, \ldots, x_{n-1} \rangle$ statt $\langle s \rangle$. Beachte, dass die Funktion $\langle \cdot \rangle$ eine Bijektion ist: Sie ist klarerweise injektiv, wegen der Eindeutigkeit der Faktorisierung in Primzahlen. Ferner, falls $x \neq 0$, ist $x+1 \geq 2$ und lässt sich faktorisieren, wobei wir immer annehmen können, dass die größte Primzahl in der Faktorisierung nicht trivial vorkommt.

**Lemma 3.15.** *Mit der obigen Notation sind folgende Funktionen primitiv rekursiv:*

- *Die* Längenfunktion $\begin{array}{rccl} \lg : & \mathbb{N} & \to & \mathbb{N} \\ & m & \mapsto & \begin{cases} 0, \text{ falls } m = 0 \\ n, \text{ falls } m = \langle x_0, \ldots, x_{n-1} \rangle \end{cases} \end{array}$
- *Die* Komponentenfunktion*:*

$$\begin{array}{rcl} \mathbb{N}^2 & \to & \mathbb{N} \\ (k, m) & \mapsto & \begin{cases} x_k, \text{ falls } m = \langle x_0, \ldots, x_{n-1} \rangle \text{ und } k < \lg(m) \\ 0, \text{ sonst.} \end{cases} \end{array}$$

  *Insbesondere ist für jedes $k$ aus $\mathbb{N}$ die $k$-te Komponentenfunktion $(\cdot)_k : \mathbb{N} \to \mathbb{N}$ primitiv rekursiv.*

*Beweis.* Beachte, dass wegen Lemma 3.9 und Lemma 3.10 die Funktion $\lg(m) = \mu z\Big(\forall y \leq m\Big((z \leq y) \longrightarrow (p(y) \nmid m+1)\Big)\Big)$ primitiv rekursiv ist, weil es immer ein solches $z \leq m+1$ gibt, da die Funktion $x \mapsto p(x)$ streng monoton ist.
Für die Komponentenfunktion gilt $\mathbb{N} \to \mathbb{N}$

$$(k,m) \mapsto \begin{cases} \mu y(p(k)^{y+1} \nmid m+1), \text{ falls } k < \lg(m)-1 \\ \mu y(p(k)^{y+2} \nmid m+1), \text{ falls } k = \lg(m)-1 \\ 0, \text{ sonst.} \end{cases}$$

Aus dem Lemma 3.10 ist diese Funktion primitiv rekursiv, da es ein solches $y \leq m$ gibt.

□

**Korollar 3.16.** *Die Teilmenge von Elementen aus $\mathbb{N}$, welche eine Folge aus der Kollektion $\mathcal{S}_n$ aller Folgen der Länge $n$ repräsentieren, ist primitiv rekursiv, für jedes $n$ aus $\mathbb{N}$. Dementsprechend werden wir sagen, dass $\mathcal{S}_n$ primitiv rekursiv ist.*

**Korollar 3.17.** *Mehrfachrekursionen primitiv rekursiver Funktionen $g : \mathbb{N}^2 \to \mathbb{N}$ sind primitiv rekursiv. Dies bedeutet, dass die Fuktion $f : \mathbb{N} \to \mathbb{N}$ gegeben durch $f(0) = 0$ und $f(x+1) = g(x, \langle f(0), \ldots, f(x)\rangle)$ primitiv rekursiv ist.*

*Beweis.* Setze $h(x) = \langle f(0), \ldots, f(x)\rangle$. Weil $f(x) = (h(x))_x$, genügt es zu zeigen, dass $h$ primitiv rekursiv ist. Aus $h(0) = \langle 0\rangle = 1 = S(0)$ und

$$\begin{aligned} h(x+1) &= \langle f(0), \ldots, f(x+1)\rangle = \langle f(0), \ldots, f(x), g(x, \langle f(0), \ldots, f(x)\rangle)\rangle = \\ &= \langle (h(x))_0, \ldots, (h(x))_x, g(x, h(x))\rangle, \end{aligned}$$

folgt klarerweise, dass $h$ primitiv rekursiv ist. □

**Definition 3.18.** Eine Teilmenge $A \subset \mathbb{N}^n$ ist *rekursiv aufzählbar*, falls $A$ die Projektion auf die ersten $n$ Koordinaten einer rekursiven Teilmenge $B \subset \mathbb{N}^{n+1}$ ist. Dies bedeutet,

$$(x_1, \ldots, x_n) \in A \iff \text{ es gibt } y \text{ aus } \mathbb{N} \text{ mit } (x_1, \ldots, x_n, y) \in B.$$

**Bemerkung 3.19.** Jede rekursive Menge ist rekursiv aufzählbar, weil $A \times \mathbb{N} \subset \mathbb{N}^{n+1}$ auch rekursiv ist, wenn $A \subset \mathbb{N}^n$ rekursiv ist.
Wir werden im nächsten Abschnitt sehen, dass nicht jede rekursiv aufzählbare Menge rekursiv ist.

**Lemma 3.20.**

- *Die Projektion einer rekursiv aufzählbaren Menge ist wiederum rekursiv aufzählbar.*
- *Rekursiv aufzählbare Mengen sind unter endlichen Durchschnitten und Vereinigungen abgeschlossen.*
- *Falls $A \subset \mathbb{N}^{n+1}$ rekursiv aufzählbar ist, so ist*

  $$C = \{(x_1 \ldots, x_n, w) \in \mathbb{N}^{n+1} \,|\, \forall z < w\Big((x_1, \ldots, x_n, z) \in A\Big)\}$$

  *rekursiv aufzählbar.*

*Beweis.*

- Sei $X \subset \mathbb{N}^n$ die Projektion einer rekursiv aufzählbaren Menge $A \subset N^{n+1}$. Es gibt eine rekursive Menge $B \subset \mathbb{N}^{n+2}$, welche auf $A$ projiziert. Insbesondere liegt $(x_1 \ldots, x_n)$ genau dann in $X$, wenn es eine Folge $s$ in $\mathcal{S}_2$ der Länge 2 gibt, sodass $(x_1, \ldots, x_n, (s)_0, (s)_1)$ in $B$ liegt. Dies impliziert, dass $X$ auch rekursiv aufzählbar ist, weil $S_2$ primitiv rekursiv ist.

- Weil die Vereinigung von Projektionen die Projektion der Vereinigung ist, müssen wir nur den Fall eines Durschnittes betrachten. Seien $A_1$ und $A_2$ rekursiv aufzählbare Teilmengen von $\mathbb{N}^n$, welche jeweils die Projektion der rekursiven Teilmengen $B_1$ und $B_2$ von $\mathbb{N}^{n+1}$ sind. Es folgt, dass ein Tupel $(x_1 \ldots, x_n)$ genau dann in $A_1 \cap A_2$ liegt, wenn es eine Folge $s$ in $\mathcal{S}_2$ der Länge 2 gibt, sodass $(x_1, \ldots, x_n, (s)_0)$ in $B_1$ und $(x_1, \ldots, x_n, (s)_1)$ in $B_2$ liegen.

- Angenommen, dass $A$ die Projektion der rekursiven Teilmenge $B \subset \mathbb{N}^{n+2}$ ist, dann liegt für jedes $z < w$ das Tupel $(x_1, \ldots, x_n, z)$ in $A$, wenn es ein Element $y = y(z)$ gibt (das von $z$ abhängt), sodass $(x_1, \ldots, x_n, z, y(z))$ in $B$ liegt. Insbesondere gibt es eine Folge $s = (y(0), \ldots, y(w-1))$ der Länge $w$, sodass für jedes $z < w$ das Tupel $(x_1, \ldots, x_n, z, (s)_z)$ in $B$ liegt:

  $$(x_1, \ldots, x_n, w) \in C \iff \exists s\Big(\forall z < w\big((x_1, \ldots, x_n, z, (s)_z) \in B\big)\Big).$$

  Aus Lemma 3.9 folgt, dass $C$ rekursiv aufzählbar ist.

□

**Lemma 3.21.** *Eine Teilmenge $A \subset \mathbb{N}^n$ ist genau dann rekursiv, wenn $A$ und ihr Komplement $\mathbb{N}^n \setminus A$ beide rekursiv aufzählbar sind.*

*Beweis.* Eine Richtung ist wegen Lemma 3.6 und Bemerkung 3.19 trivial. Seien nun $A$ und $\mathbb{N}^n \setminus A$ rekursiv aufzählbar bezüglich der rekursiven Teilmengen $B$ und $C$ von $\mathbb{N}^{n+1}$. Jedes Tupel $(x_1, \ldots, x_n)$ liegt entweder in $A$ oder in ihrem Komplement. Also muss es ein $y$ geben, sodass $(x_1, \ldots, x_n, y)$ in $B$ oder in $C$ liegt. Insbesondere ist die Funktion

$$g(x_1, \ldots, x_n) = \mu y \Big(\big((x_1, \ldots, x_n, y) \in B\big) \vee \big((x_1, \ldots, x_n, y) \in C\big)\Big)$$

wohldefiniert und rekursiv. Klarerweise gilt $\chi_A(x_1, \ldots, x_n) = \chi_B((x_1, \ldots, x_n, g(x_1, \ldots, x_n))$ und somit ist $A$ rekursiv. □

Wir werden nun zeigen, dass Teilmengen von $\mathbb{N}$ (aber nicht allgemein für Teilmengen von $\mathbb{N}^n$) genau dann rekursiv aufzählbar sind, wenn sie das Bild einer rekursiven Funktion sind. Insbesondere können sie rekursiv aufgezählt werden!

**Lemma 3.22.** *Eine Teilmenge $A \subset \mathbb{N}$ ist genau dann rekursiv aufzählbar, wenn sie leer oder gleich $f(\mathbb{N})$ ist, für eine rekursive Funktion $f : \mathbb{N} \to \mathbb{N}$.*

*Beweis.* Die leere Menge ist klarerweise primitiv rekursiv und somit rekursiv aufzählbar. Falls $A = f(\mathbb{N})$ für eine rekursive Funktion $f : \mathbb{N} \to \mathbb{N}$, dann ist die Menge $B = \{(x, y) \in \mathbb{N}^2 \mid f(x) = y\}$ rekursiv und $A = \pi_2^2(B)$.

Nun die Rückrichtung. Angenommen, dass die nicht-leere Menge $A$ rekursiv aufzählbar bezüglich der rekursiven Menge $B \subset \mathbb{N}^2$ ist, wählen wir ein $a$ aus $A$ fest (weil $A \neq \emptyset$) und definieren

$$\begin{array}{rccl} f: & \mathbb{N} & \to & \mathbb{N} \\ & z & \mapsto & \begin{cases} (z)_0, \text{ falls } z = \langle x, y\rangle \text{ mit } (x,y) \in B \\ a, \text{ sonst.} \end{cases} \end{array}$$

Klarerweise ist $f$ rekursiv und $f(\mathbb{N}) = A$, wie gewünscht. □

**Definition 3.23.** Eine Menge $A \subset \mathbb{N}^n$ ist *arithmetisch*, falls sie in der Struktur

$$\mathcal{N}_0 = (\mathbb{N}, 0, S, +, \cdot, <)$$

definierbar ist. Dies bedeutet, falls es eine Formel $\varphi_A[x_1, \ldots, x_n]$ in der Sprache $\{0, S, +, \cdot, <\}$ gibt, sodass

$$(a_1, \ldots, a_n) \in A \Longleftrightarrow \mathcal{N}_0 \models \varphi_A[a_1, \ldots, a_n].$$

Eine Funktion ist *arithmetisch*, falls ihr Graph arithmetisch ist.

Für die Struktur $\mathcal{N}_0$ werden wir zwischen den Symbolen der Sprache $\{0, S, +, \cdot, <\}$ und den kanonischen Interpretationen nicht unterscheiden.

**Proposition 3.24.** *Rekursive Funktionen und Mengen sind arithmetisch.*

*Beweis.* Wegen Satz 3.14 genügt es zu zeigen, dass Komposition und $\mu$-Rekursion wiederum definierbar sind, wenn alle Funktionen arithmetisch sind.

- Für die Komposition: Seien die (Graphen der) arithmetischen Funktionen $g_1, \ldots, g_m, h$ durch die Formeln $\varphi_{g_1}, \ldots, \varphi_{g_m}, \varphi_h$ definiert. Wir setzen $\bar{x} = (x_1, \ldots, x_n)$. Die Funktion $y = f(\bar{x}) = h(g_1(\bar{x}), \ldots, g_m(\bar{x}))$ ist nun durch die Formel

$$\exists z_1 \ldots \exists z_m \Big( \varphi_h[z_1, \ldots, z_m, y] \wedge \bigwedge_{i=1}^{m} \varphi_{g_i}[\bar{x}, z_i] \Big)$$

  definiert.

- Für die $\mu$-Rekursion: Wenn $g(\bar{x}, z)$ durch die Formel $\varphi[\bar{x}, z, u]$ definiert wird, ist $y = f(\bar{x}) = \mu z\,(g(\bar{x}, z) = 0)$ durch die Formel

$$(\varphi[\bar{x}, y, 0] \wedge \forall u < y \neg \varphi[\bar{x}, u, 0])$$

  definiert.

□

**Korollar 3.25.** *Rekursiv aufzählbare Mengen sind arithmetisch.*

*Beweis.* Wenn $\varphi[\bar{x}, y]$ die rekursive Menge $B \subset \mathbb{N}^{n+1}$ definiert, wird die Projektion $A$ von $B$ auf die ersten $n$ Koordinaten durch die Formel $\exists y \varphi[\bar{x}, y]$ definiert. □

## 3.3 Entscheidbarkeit

In diesem Abschnitt sind alle Sprachen endlich.

**Definition 3.26.** Sei $\mathcal{L}$ eine endliche Sprache, welche aus den Symbolen $\lambda_0, \ldots, \lambda_{l-1}$ besteht. Wir ordnen jeder endlichen Folge aus $\mathcal{L}$, insbesondere jedem Term und jeder Formel aus $\mathcal{L}$, nach den folgenden Regeln eine *Gödelnummer* zu:

$$\begin{array}{rcl} \doteq & \mapsto & \langle 0,0\rangle \\ \vee & \mapsto & \langle 0,1\rangle \\ \neg & \mapsto & \langle 0,2\rangle \\ ( & \mapsto & \langle 0,3\rangle \\ ) & \mapsto & \langle 0,4\rangle \\ \exists & \mapsto & \langle 0,5\rangle \\ \lambda_0 & \mapsto & \langle 0,6\rangle \\ \vdots & & \vdots \\ \lambda_{l-1} & \mapsto & \langle 0,5+l\rangle \\ x_i & \mapsto & \langle 1,i\rangle \end{array}$$

Falls die Formel $\varphi$ der Folge $\xi_1 \ldots \xi_n$ von Zeichen aus $\mathcal{L}$ entspricht, ist ihre *Gödelnummer*

$$\ulcorner \varphi \urcorner = \langle \langle \xi_1 \rangle, \ldots, \langle \xi_n \rangle \rangle.$$

Dementsprechend definieren wir die Gödelnummer $\ulcorner t \urcorner$ eines Termes $t$ aus $\mathcal{L}$.

**Bemerkung 3.27.** Wir hätten eine ähnliche Definition, falls die Sprache $\mathcal{L}$ nicht unbedingt endlich, aber zumindest rekursiv wäre.

**Lemma 3.28.** *Folgende Teilmengen von* $\mathbb{N}$ *sind primitiv rekursiv:*

- $\{\ulcorner t \urcorner \mid t \in \mathbb{TERM}\}$;
- $\{\ulcorner \varphi \urcorner \mid \varphi \in \mathbb{FORM}\}$;
- $\{\ulcorner \varphi \urcorner \mid \varphi[x] \in \mathbb{FORM}$ *mit höchstens einer freien Variable* $x\}$;
- $\{\ulcorner \chi \urcorner \mid \chi$ *Aussage*$\}$.

*Beweis.* Wir werden nur den ersten Teil zeigen, weil sich alle anderen analog beweisen lassen. Das Element $n$ ist Gödelnummer von einem Term $t$, falls

- $n = \langle 1, i\rangle$, für ein $i < n$ (und somit ist $n = \ulcorner x_i \urcorner$); oder
- $n = \langle 0, 6+i\rangle = \langle \lambda_i \rangle$, für ein $i < l$, mit $\lambda_i$ ein Konstantenzeichen aus $\mathcal{L}$; oder
- $n = \langle n_0, \ldots, n_{k-1}\rangle$, wobei $n_0 = \langle \lambda_s \rangle$ für ein $k-1$-stelliges Funktionszeichen $\lambda_s$ und $\chi_{\mathbb{TERM}}(n_i) = 1$ für $1 \leq i < k = \lg(n)$.

Weil die $i$-te Koordinate einer Folge $s$ immer kleiner ist als $\langle s \rangle$, liefert die obige Konstruktion zusammen mit Korollar 3.17, dass die charakteristische Funktion von $\mathbb{TERM}$ primitiv rekursiv ist. □

Weil jede rekursiv aufzählbare Menge in der Struktur $\mathcal{N}_0 = (\mathbb{N}, 0, S, +, \cdot, <)$ definierbar ist, muss es allein aus Kardinalitätsgründen Teilmengen von $\mathbb{N}$ geben, welche nicht rekursiv aufzählbar sind. Mit Hilfe des Satzes 3.47 können wir explizit Mengen angeben, die nicht rekursiv aufzählbar sind: Es genügt aus dem Lemma 3.21 das Komplement einer Menge zu betrachten, welche rekursiv aufzählbar ist, aber nicht rekursiv.

**Definition 3.29.** Eine Theorie $T$ in einer endlichen Sprache $\mathcal{L}$ ist *rekursiv axiomatisierbar*, falls $\{\ulcorner\chi\urcorner \,|\, \chi \in T\}$ rekursiv aufzählbar ist. Die Theorie $T$ ist *entscheidbar*, falls $\{\ulcorner\chi\urcorner \,|\, T \vdash \chi\}$ rekursiv ist.

**Bemerkung 3.30.** Das Hilbertkalkül, das heißt die leere Theorie, sowie jede endliche Theorie ist rekursiv axiomatisierbar.
Wenn $T$ entscheidbar und $T' \supset T$ eine Erweiterung mit $T' \setminus T$ endlich ist, so ist wegen Korollar 2.48 $T'$ entscheidbar.

**Lemma 3.31.** *Die Menge* $\{\ulcorner\varphi\urcorner \,|\, \varphi$ *Tautologie* $\}$ *ist primitiv rekursiv.*

*Beweis.* Es genügt zu zeigen, dass die Kollektion $\{\ulcorner P\urcorner \,|\, P$ aussagenlogische Tautologie $\}$ primitiv rekursiv, weil die Ersetzungsfunktion klarerweise primitiv rekursiv ist. Dafür genügt es zu zeigen, dass das Komplement $\{\ulcorner P\urcorner \,|\, P$ keine aussagenlogische Tautologie $\}$ primitiv rekursiv ist. Eine aussagenlogische Formel $P$ ist keine Tautologie, falls es eine Belegung $\beta$ mit $\beta(P) = 0$. Eine solche Belegung $\beta$ ist gegeben durch eine Folge von 0 und 1's, so die Menge

$$\{(\ulcorner P\urcorner, n) \,|\, n \text{ ist eine Belegung } \beta \text{ mit } \beta(P) = 0\}$$

ist primitiv rekursiv. Aus dem Lemma 3.10 folgt, dass eine aussagenlogische Formel $P$ keine Tautologie ist, wenn es eine Belegung $\beta$ mit $\beta(P) = 0$, deren Länge durch $\ulcorner P\urcorner$ beschränkt ist. □

**Lemma 3.32.** *Wenn $T$ rekursiv axiomatisierbar ist, dann ist die Menge* $\{\ulcorner\varphi\urcorner \,|\, T \vdash \varphi\}$ *rekursiv aufzählbar.*

*Beweis.* Weil wegen Lemma 3.20 rekursiv aufzählbare Mengen unter Projektionen abgeschlossen sind, genügt es zu zeigen, dass die Menge $\{(\ulcorner\varphi\urcorner, y) \,|\, y = \langle\varphi_1, \ldots, \varphi_n\rangle$ kodiert einen Beweis von $\varphi_n = \varphi$ in $T\}$ rekursiv aufzählbar ist. Weil die Menge der Gödel'scher Zahlen der logischen Axiome klarerweise primitiv rekursiv ist, und wir Modus Ponens und $\exists$-Einführung kodieren können, folgt sofort, dass ein Beweis aus $T$ kodiert werden kann, da wir bestimmen können, wann eine Formel (oder eher ihre Gödel'sche Zahl) zu $T$ gehört, denn $T$ ist rekursiv axiomatisierbar. □

Aus Lemma 3.21 folgt, dass vollständige rekursiv axiomatisierbare Theorien entscheidbar sind, weil die Funktion

$$\begin{array}{rcl} \mathbb{N} & \to & \mathbb{N} \\ n & \mapsto & \begin{cases} \ulcorner\neg\varphi\urcorner, \text{ falls } n = \ulcorner\varphi\urcorner \\ 0, \text{ sonst.} \end{cases} \end{array}$$

primitiv rekursiv ist.

**Korollar 3.33.** *Jede vollständige rekursiv axiomatisierbare Theorie ist entscheidbar.*

**Notation.** Wenn die Sprache $\mathcal{L}$ die Teilsprache $\{0, S\}$ enthält, bezeichnen wir mit $\underline{\mathrm{n}}$ den Term $\underbrace{S \circ \ldots \circ S}_{n}(0)$, wobei $\underline{0} = 0$.

**Satz 3.34.** *Die Theorie* $\mathrm{Th}(\mathcal{N}_0) = \{\chi$ *Aussage, welche in* $\mathcal{N}_0$ *gilt, d.h,* $\mathcal{N}_0 \models \chi\}$ *ist unentscheidbar.*

*Beweis.* Induktiv über den Aufbau von Formeln sieht man leicht, dass für $n$ aus $\mathbb{N}$ die Funktion

$$\begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ \ulcorner \varphi[x] \urcorner & \mapsto & \ulcorner \varphi[\underline{\mathrm{n}}] \urcorner \end{array}$$

primitiv rekursiv ist. Wegen Lemma 3.28 gibt es eine rekursive Aufzählung $\{\varphi_n[x]\}$ der Formeln mit einer freien Variable $x$ in der Sprache $\{0, S, +, \cdot, <\}$.
Wenn $\mathrm{Th}(\mathcal{N}_0)$ entscheidbar wäre, wäre die Menge $\{\ulcorner \chi \urcorner \,|\, \mathcal{N}_0 \models \chi\}$ rekursiv. Insbesondere wäre die Menge $A = \{n \in \mathbb{N} \,|\, \mathcal{N}_0 \models \neg\varphi_n[\underline{\mathrm{n}}]\}$ auch rekursiv und somit arithmetisch wegen Proposition 3.24. Also gibt es eine Formel $\varphi[x]$ in der Sprache $\{0, S, +, \cdot, <\}$, welche in $\mathcal{N}_0$ die Menge $A$ definiert. Sei $n_0$ so, dass $\varphi = \varphi_{n_0}$. Aber

$$n_0 \in A \iff \mathcal{N}_0 \models \varphi_{n_0}[n_0] \iff \mathcal{N}_0 \models \varphi_{n_0}[\underline{\mathrm{n}}_0] \iff \mathcal{N}_0 \not\models \neg\varphi_{n_0}[\underline{\mathrm{n}}_0] \iff n_0 \notin A,$$

was den gewünschten Widerspruch liefert. □

**Korollar 3.35** ((Einfacher) Unvollständigkeitssatz)**.** *Jede rekursiv axiomatisierbare Theorie in der Sprache* $\{0, S, +, \cdot, <\}$*, welche* $\mathcal{N}_0$ *als Modell besitzt, ist unvollständig.*

*Beweis.* Wenn die rekursiv axiomatisierbare Theorie $T$ vollständig ist, ist sie wegen Korollar 3.33 entscheidbar. Ferner sind wegen Korollar 2.65 alle Modelle von $T$ elementar äquivalent und somit gilt

$$T \vdash \chi \iff \mathcal{N}_0 \models \chi \iff Th(\mathcal{N}_0) \vdash \chi.$$

Insbesondere ist $T$ unentscheidbar. □

Wenn wir eine unentscheidbare Theorie finden, welche rekursiv axiomatisierbar ist (zum Beispiel, weil sie endlich ist), dann haben wir eine Teilmenge von $\mathbb{N}$, nämlich die Menge Gödel'scher Zahlen der Folgerungen, welche wegen Lemma 3.32 rekursiv aufzählbar aber nicht rekursiv ist. Leider ist $\mathrm{Th}(\mathcal{N}_0)$ nicht rekursiv axiomatisierbar, deswegen werden wir im nächsten Abschnitt eine endliche Teiltheorie einführen: das Axiomensystem $Q$.

## 3.4 Der Gödel'sche Unvollständigkeitssatz

In diesem Abschnitt fixieren wir die Sprache $\mathcal{L} = \{0, S, +, \cdot, <\}$.

**Definition 3.36.** Das endliche Axiomensystem $Q$ besteht aus den folgenden Axiomen:

$Q_1$ $\forall x(x + 0 \doteq x)$

$Q_2$ $\forall x \forall y\Big(x + S(y) \doteq S(x + y)\Big)$

$Q_3$ $\forall x(x \cdot 0 \doteq 0)$

$Q_4$ $\forall x \forall y \Big( x \cdot S(y) \doteq x \cdot y + x \Big)$

$Q_5$ $\forall x \neg (x < 0)$

$Q_6$ $\forall x \forall y \Big( x < S(y) \longleftrightarrow \big( (x < y) \vee (x \doteq y) \big) \Big)$

Die Struktur $\mathcal{N}_0$ ist klarerweise ein Modell von $Q$. Somit ist $Q$ widerspruchsfrei.

**Lemma 3.37.** *Für alle $n$ und $m$ aus $\mathbb{N}$ sind folgende Axiome Folgerungen aus $Q$:*

$Q_1^*(n,m)$ $(\underline{n} + \underline{m} \doteq \underline{n+m})$

$Q_2^*(n,m)$ $(\underline{n} \cdot \underline{m} \doteq \underline{n \cdot m})$

$Q_3^*(n)$ $\forall x \Big( (x < \underline{n}) \longleftrightarrow \bigvee_{k<n} (x \doteq \underline{k}) \Big)$

*Beweis.* Wegen dem Vollständigkeitssatz 2.64 genügt es zu zeigen, dass diese Axiome in jedem Modell von $Q$ gelten. Achtung! In einem Modell $\mathcal{M}$ von $Q$ kann es Elemente geben, welche nicht der Form $\underline{\mathrm{n}}$ sind. Aber in $\mathcal{M}$ gilt, dass $\underline{\mathrm{n+1}} = S(\underline{\mathrm{n}})$. Somit lassen sich die ersten beiden Behauptungen leicht induktiv über $m$ zeigen. Die dritte Behauptung zeigt man leicht durch Induktion über $n$. □

**Notation.** Wir bezeichnen mit $Q^*$ die Theorie, welche aus den Axiomen $Q_1^*(n,m), Q_2^*(n,m), Q_3^*(n)$ mit $n$ und $m$ aus $\mathbb{N}$ besteht. Beachte, dass $Q^*$ nicht mehr endlich ist, aber dennoch rekursiv axiomatisierbar. Wegen Korollar 3.35 ist weder $Q$ noch $Q^*$ vollständig.

**Korollar 3.38.** *Für alle $n$ und $m$ aus $\mathbb{N}$ gilt:*

1. *Wenn $n \neq m$, dann $Q^* \vdash \neg(\underline{n} \doteq \underline{m})$.*
2. *Wenn $n < m$, dann $Q^* \vdash (\underline{n} < \underline{m})$.*
3. *Wenn $n \not< m$, dann $Q^* \vdash \neg(\underline{n} < \underline{m})$.*

*Beweis.* Wegen dem Vollständigkeitssatz 2.64 genügt es induktiv über $m$ zu zeigen, dass diese Axiome in jedem Modell $\mathcal{M}$ von $Q^*$ gelten.

1. Falls $m = 0$, dann ist $n \neq 0$ und somit $n = k + 1$ für ein $k$ aus $\mathbb{N}$. Aber $\underline{\mathrm{k}} < S(\underline{\mathrm{k}}) = \underline{\mathrm{n}}$ wegen $Q_3^*$ und somit ist $\underline{\mathrm{n}}$ verschieden von $0 = \underline{0}$ (nochmal $Q_3^*$).

   Falls $m \neq 0$, aber $n = 0$, ist der Beweis wie oben. Ansonsten gibt es $n'$ und $m'$ aus $\mathbb{N}$ mit $n = n' + 1$ und $m = m' + 1$. Weil $n \neq m$, ist $n' \neq m'$. Wenn $m' < n'$, folgt induktiv, dass $\underline{\mathrm{n}}'$ verschieden von $\underline{\mathrm{k}}$ ist für alle $k \leq m'$. Weil $\underline{\mathrm{n}}' < \underline{\mathrm{n}}$, folgt aus $Q_3^*$, dass $\underline{\mathrm{n}}$ und $\underline{\mathrm{m}}$ (in $\mathcal{M}$) verschieden sind.

2. Lässt sich einfach mit $Q_3^*$ induktiv über $m$ zeigen.

3. Falls $m = 0$, folgt dies trivialerweise aus $Q_3^*$. Wenn $m = m' + 1$, haben wir $n = m$ oder $n > m$ (weil die Ordung auf $\mathbb{N}$ total ist). Falls $\underline{\mathrm{n}} < \underline{\mathrm{m}} = S(\underline{\mathrm{m}}')$ in $\mathcal{M}$ gilt, dann gibt es ein $k \leq m'$ mit $\underline{\mathrm{n}} = \underline{\mathrm{k}}$ (in $\mathcal{M}$). Aber, weil $n \neq k$, ist $\underline{\mathrm{n}}$ verschieden von $\underline{\mathrm{k}}$ wegen des ersten Teiles.

□

Induktiv über den Aufbau von Formeln sieht man leicht:

**Korollar 3.39.** *Für jede quantorfreie Formel $\varphi[x_1, \ldots, x_n]$ und Elemente $m_1, \ldots, m_n$ aus $\mathbb{N}$ gilt*

$$\mathcal{N}_0 \models \varphi[m_1, \ldots, m_n] \Longleftrightarrow Q^* \vdash \varphi[\underline{m}_1, \ldots, \underline{m}_n].$$

Wir wollen die Äquivalenz von Gültigkeit in $\mathcal{N}_0$ und Beweisbarkeit aus $Q^*$ auf eine größere Klasse von Formeln erweitern.

**Notation.** Wir werden die Abkürzung $\forall x < y\, \varphi$ für die *beschränkte universelle Quantifizierung* $\forall x\Big((x < y) \wedge \varphi\Big)$ verwenden.

**Definition 3.40.** Eine $\Sigma_1$-*Formel* ist eine Formel in der Sprache $\mathcal{L} = \{0, S, +, \cdot, <\}$, welche aus einer quantorfreien Formel durch iteriertes Anwenden von $\wedge$, $\vee$, $\exists x$ und *beschränkter universeller Quantifizierung* $\forall x < y$ entsteht, wobei $x$ verschieden von der Variable $y$ sei.

**Beispiel 3.41.** Die Formel $\exists y(x \doteq y)$ ist $\Sigma_1$, aber ihre Negation $\forall y(x \neq y)$ ist es nicht.

**Bemerkung 3.42.** Angenommen, dass in der Formel $\varphi$ nur universelle Quantifizierungen der Form $\forall x < t$ vorkommen, wobei $x$ nicht frei im Term $t$ vorkommt. Weil jeder Term aus $0, S, +, \cdot$ gewommen wird, können wir dies zu $\forall x < y$ umformen und im Quantorenbereich die quantorenfreie Formel $y = t$ hinzufügen.
Insbesondere hätten wir eine allgemeinere Definition von $\Sigma_1$-Formeln angeben können, welche aber äquivalent ist.

**Satz 3.43.** *Für jede $\Sigma_1$-Formel $\varphi[x_1, \ldots, x_n]$ und Elemente $m_1, \ldots, m_n$ aus $\mathbb{N}$ gilt*

$$\mathcal{N}_0 \models \varphi[m_1, \ldots, m_n] \Longleftrightarrow Q^* \vdash \varphi[\underline{m}_1, \ldots, \underline{m}_n].$$

*Beweis.* Eine Richtung folgt aus dem Vollständigkeitssatz. Wir müssen nur zeigen, dass $Q^*$ die Aussage $\varphi[\underline{\mathrm{m}}_1, \ldots, \underline{\mathrm{m}}_n]$ beweist, falls $\mathcal{N} \models \varphi[m_1, \ldots, m_n]$. Wir beweisen das induktiv über den Aufbau von $\varphi$, wobei es für quantorenfreie $\varphi$ aus Korollar 3.39 folgt. Der Fall einer Konjuntion, bzw. einer Disjunktion, ist trivial. Nur für die Quantifizierung bleibt es zu zeigen:

- Falls $\varphi = \exists y \psi$, dann ist $\psi[x_1, \ldots, x_n, y]$ auch eine $\Sigma_1$-Formel. Wenn $\mathcal{N}_0 \models \varphi[m_1, \ldots, m_n]$, gibt es ein Element $k$ aus $\mathbb{N}$ mit $\mathcal{N}_0 \models \psi[m_1, \ldots, m_n, k]$. Mit der Induktionsannahme folgt, dass $Q^* \vdash \psi[\underline{\mathrm{m}}_1, \ldots, \underline{\mathrm{m}}_n, \underline{\mathrm{k}}]$. Aus dem $\exists$-Quantorenaxiom folgt, dass $Q^* \vdash (\exists y \psi)[\underline{\mathrm{m}}_1, \ldots, \underline{\mathrm{m}}_n]$, das heißt, $Q^* \vdash \varphi[\underline{\mathrm{m}}_1, \ldots, \underline{\mathrm{m}}_n]$.

- Falls $\varphi = \forall\ y < x_1\ \psi[x_1, \ldots, x_n, y]$, haben wir $\mathcal{N}_0 \models \psi[m_1, \ldots, m_n, k]$ für alle $k < m_1$. Insbesondere beweist $Q^*$ die Aussage $\psi[\underline{\mathrm{m}}_1, \ldots, \underline{\mathrm{m}}_n, \underline{\mathrm{k}}]$ für alle $k < m_1$. Aus dem Axiom $Q_3^*$ folgt, dass $Q^* \vdash (\forall y < x_1 \psi)[\underline{\mathrm{m}}_1, \ldots, \underline{\mathrm{m}}_n]$, wie gewünscht.

□

**Proposition 3.44.** *Jede rekursive Funktion bzw. jede rekursiv aufzählbare Menge wird durch eine $\Sigma_1$-Formel in $\mathcal{N}$ definiert.*

*Beweis.* Aus den Beweisen von Proposition 3.24 und Korollar 3.25 folgt, dass wir nur eine geeignete Definition für die $\mu$-Rekursion angeben müssen, ohne $\neg\varphi$ zu benutzen. Es genügt also, folgende Definition zu betrachten:

$$\Big(\varphi[\bar{x}, y, 0] \wedge \forall z < y \exists u\big(\varphi[\bar{x}, z, u] \wedge u \neq 0\big)\Big),$$

welche eine $\Sigma_1$-Formel ist. □

**Lemma 3.45.** *Jede rekursive Funktion $f : \mathbb{N}^n \to \mathbb{N}$ wird von einer $\Sigma_1$-Formel $\varphi[x_1, \ldots, x_n, y]$ in $Q^*$* repräsentiert*: Für alle $m_1, \ldots, m_n$ aus $\mathbb{N}$ gilt*

$$Q^* \vdash \forall y\Big(\varphi[\underline{m}_1, \ldots, \underline{m}_n, y] \longleftrightarrow (y \doteq \underline{f(m_1, \ldots, m_n)})\Big)$$

*Insbesondere wird jede rekursive Teilmenge $A \subset N^n$ von einer $\Sigma_1$-Formel $\psi[x_1, \ldots, x_n, y]$ in $Q^*$* repräsentiert*: Für alle $m_1, \ldots, m_n$ aus $\mathbb{N}$ gilt*

$$\left.\begin{array}{rcl} (m_1, \ldots, m_n) \in A & \Longrightarrow & Q^* \vdash \psi[\underline{m}_1, \ldots, \underline{m}_n] \\ (m_1, \ldots, m_n) \notin A & \Longrightarrow & Q^* \vdash \neg\psi[\underline{m}_1, \ldots, \underline{m}_n] \end{array}\right\}$$

*Beweis.* Wegen Satz 3.14 genügt es zu zeigen, dass die Funktionen aus der Klasse $\mathcal{F}$ durch $\Sigma_1$-Formeln in $Q^*$ repräsentierbar sind. Die Grundfunktionen $\{S, +, \cdot, \chi_<\}$ sind klarerweise so repräsentierbar und auch die Konstanten- und Koordinatenfunktionen.

- Für die Komposition: Seien die Funktionen $g_1, \ldots, g_m, h$ durch die $\Sigma_1$-Formeln $\varphi_{g_1}, \ldots, \varphi_{g_m}, \varphi_h$ definiert. Setze $\bar{x} = (x_1, \ldots, x_n)$. Die Funktion $y = f(\bar{x}) = h(g_1(\bar{x}), \ldots, g_m(\bar{x}_))$ ist nun durch die Formel
$$\exists z_1 \ldots \exists z_m\Big(\varphi_h[z_1, \ldots, z_m, y] \wedge \bigwedge_{i=1}^{m} \varphi_{g_i}[\bar{x}, z_i]\Big)$$
definiert, welche wieder eine $\Sigma_1$-Formel ist.

- Für die $\mu$-Rekursion: Wir nehmen an, dass $g(\bar{x}, z)$ durch die $\Sigma_1$-Formel $\psi[\bar{x}, z, u]$ definiert wird und machen es so ähnlich wie im Beweis von Proposition 3.44: Wir betrachten die $\Sigma_1$-Formel

$$\varphi[\bar{x}, y] = \Big(\psi[\bar{x}, y, 0] \wedge \forall z < y \exists u\big(\psi[\bar{x}, z, u] \wedge u \neq 0\big) \wedge \big((0 \leq y) \wedge \forall w < y(s(w) \leq y)\big)\Big).$$

Weil $\mathcal{N} \models \varphi[m_1, \ldots, m_n, f(m_1, \ldots, m_n)]$, folgt aus Satz 3.43

$$Q^* \vdash \varphi[\underline{\mathrm{m}}_1, \ldots, \underline{\mathrm{m}}_n, \underline{f(m_1, \ldots, m_n)}].$$

Es genügt nun zu zeigen, dass in jedem Modell $\mathcal{M}$ von $Q^*$ gilt: falls $\mathcal{M} \models \varphi[\underline{\mathrm{m}}_1, \ldots, \underline{\mathrm{m}}_n, b]$ für ein Element $b$ aus $M$, dann ist $b = \underline{f(m_1, \ldots, m_n)}$. Weil

$$\mathcal{M} \models \varphi[\underline{\mathrm{m}}_1, \ldots, \underline{\mathrm{m}}_n, \underline{f(m_1, \ldots, m_n)}]$$

folgt, dass weder $b < \underline{f(m_1, \ldots, m_n)}$ noch $\underline{f(m_1, \ldots, m_n)} < b$ in $\mathcal{M}$ gilt. Wir wissen, dass $b \geq 0$ in $\mathcal{M}$ ist. Entweder ist $b = 0$ oder $b > 0$ und somit $b \geq \underline{1}$. Dies bedeutet, entweder ist $b = \underline{1}$ oder $b \geq \underline{2}$. Wir iterieren und schließen daraus, dass $b = \underline{f(m_1, \ldots, m_n)}$.

Für eine rekursive Teilmenge $A \subset \mathbb{N}^n$, ist ihre Charakteristische Funktion durch eine $\Sigma_1$-Formel $\varphi[x_1, \ldots, x_n, y]$ repräsentiert. Setze nun $\psi[x_1, \ldots, x_n] = \varphi[x_1, \ldots, x_n, \underline{1}]$, weil in jedem Modell von $Q^*$ das Element $\underline{0}$ verschieden von $\underline{1}$ ist. □

**Bemerkung 3.46.** Im obigen Beweis für die $\mu$-Rekursion haben wir nicht verwendet, dass die Interpretation von $<$ in einem beliebigen Modell $\mathcal{M}$ von $Q^*$ eine totale Ordnung ist (weil es nämlich nicht stimmt!)

**Satz 3.47** (Gödel'scher (erster) Unvollständigkeitssatz)**.** *Jede Teiltheorie $T \subset \mathrm{Th}(\mathcal{N}_0)$ ist unentscheidbar. Insbesondere ist $Q$ unentscheidbar.*

*Es gibt Teilmengen aus $\mathbb{N}$, welche rekursiv aufzählbar aber nicht rekursiv sind.*

*Beweis.* Es genügt zu zeigen, dass jede Teiltheorie $T_1 \subset \mathrm{Th}(\mathcal{N}_0)$, welche alle Aussagen aus $Q^*$ beweist, unentscheibar ist. Insbesondere ist dann auch $Q$ untentscheidbar. Wenn $T$ eine beliebige Teiltheorie wäre, welche entscheidbar ist, wäre wegen Bemerkung 3.30 auch $T_1 = T \cup \{Q\}$ entscheidbar, was ein Widerspruch wäre, weil $T_1$ alle Aussagen aus $Q^*$ beweist.
Sei nun $T_1 \subset \mathrm{Th}(\mathcal{N}_0)$ eine Teiltheorie, welche alle Aussagen aus $Q^*$ beweist. Ferner sei $\{\varphi_n[x]\}$ eine rekursive Aufzählung aller Formeln in einer freien Variable. Falls $T_1$ entscheidbar wäre, wäre die Menge $A = \{n \in \mathbb{N} \mid T_1 \vdash \neg\varphi_n[\underline{n}]\}$ auch rekursiv und wegen Lemma 3.45 würde $A$ durch eine $\Sigma_1$-Formel repräsentiert werden. Bezeichne diese Formel mit $\varphi_{n_0}$.

- Falls $n_0$ in $A$ liegt, dann gilt $Q^* \vdash \varphi_{n_0}[\underline{n}_0]$, weil $A$ durch $\varphi_{n_0}[x]$ repräsentierbar ist, und deswegen auch $T_1 \vdash \varphi_{n_0}[\underline{n}_0]$. Aber $T_1 \vdash \neg\varphi_{n_0}[\underline{n}_0]$, das heißt $T_1$ ist widersprüchlich.
- Falls $n_0$ nicht in $A$ liegt, dann $Q^* \vdash \neg\varphi_{n_0}[\underline{n}_0]$, weil $A$ durch $\varphi_{n_0}[x]$ repräsentierbar ist. Insbesondere beweist $T_1$ auch $\neg\varphi_{n_0}[\underline{n}_0]$ und somit liegt $n_0$ in $A$, was ein Widerspruch ist.

Wegen Lemma 3.32 ist die Menge $\{\ulcorner\varphi\urcorner \mid Q \vdash \varphi\}$ rekursiv aufzählbar, weil $Q$ endlich ist. Aber diese Menge ist nicht rekursiv, da $Q$ unentscheidbar ist. □

Wir werden diesen Abschnitt mit einem kleinen Exkurs zur Rekursionstheorie beenden.

**Satz 3.48.** *(Fixpunktssatz) Für jede Formel $\psi[x]$ gibt es eine Aussage $\chi$ derart, dass*

$$Q^* \vdash \Big(\chi \longleftrightarrow \psi[\ulcorner\chi\urcorner]\Big).$$

*Falls $\psi$ eine $\Sigma_1$-Formel ist, so ist $\chi$ eine $\Sigma_1$-Aussage.*

*Beweis.* Die Funktion

$$\begin{array}{rccc} f: & \mathbb{N}^2 & \to & \mathbb{N} \\ & (\ulcorner\varphi[x]\urcorner, n) & \mapsto & \ulcorner\varphi[\underline{n}]\urcorner \end{array}$$

ist primitiv rekursiv und wird durch eine $\Sigma_1$-Formel $\varphi_1[x, y, z]$ repräsentiert: Für

$$Q^* \vdash \forall z\Big(\varphi_1[\ulcorner\varphi[x]\urcorner, \underline{n}, z) \longleftrightarrow (z \doteq \ulcorner\varphi[\underline{n}]\urcorner)\Big).$$

Setze nun $\varphi'[x] = \exists y\Big(\psi[y] \wedge \varphi_1[x, x, y]\Big)$ und beachte, dass $\varphi'$ eine $\Sigma_1$-Formel ist, falls $\psi$ es ist. Aus der Konstruktion folgt, dass für jede Formel $\varphi[x]$

$$Q^* \vdash \Big(\varphi'[\ulcorner\varphi[x]\urcorner] \longleftrightarrow \psi[\ulcorner\varphi[\ulcorner\varphi[x]\urcorner]\urcorner]\Big).$$

Insbesondere gilt für $\varphi = \varphi'$, dass

$$Q^* \vdash \Big(\varphi'[\ulcorner\varphi'[x]\urcorner] \longleftrightarrow \psi[\ulcorner\varphi'[\ulcorner\varphi'[x]\urcorner]\urcorner]\Big).$$

Die gewünschte Aussage $\chi$ ist $\varphi'[\ulcorner\varphi'[x]\urcorner]$. □

Der Fixpunktssatz liefert einen anderen Beweis des Unvollständigkeitssatzes.

**Korollar 3.49.** *Jede Teiltheorie $T \subset \mathrm{Th}(\mathcal{N}_0)$ ist unentscheidbar.*

*Beweis.* Ohne Einschränkung der Allgemeinheit können wir annehmen, dass $T$ alle Aussagen aus $Q^*$ beweist. Falls $T$ entscheibar wäre, wäre die Menge $A = \{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$ rekursiv und wegen Lemma 3.45 durch eine $\Sigma_1$-Formel $\psi[x]$ repräsentierbar. Wenden wir den Fixpunktssatz 3.48 auf die Formel $\neg\psi[x]$ an, bekommen wir eine Aussage $\chi$ mit

$$Q^* \vdash \Big(\chi \longleftrightarrow \neg\psi[\ulcorner\chi\urcorner]\Big),$$

und somit ist auch in $T$ die obige Äquivalenz beweisbar. Beachte, dass $\neg\psi[x]$ nicht unbedingt eine $\Sigma_1$-Formel ist.

- Falls $T$ die Aussage $\chi$ beweist, liegt $\ulcorner\chi\urcorner$ in $A$. Wegen Lemma 3.45 gilt $Q^* \vdash \psi[\ulcorner\chi\urcorner]$ und daher auch $T \vdash \psi[\ulcorner\chi\urcorner]$. Andererseits beweist $T$ aus der Konstruktion von $\chi$ auch $\neg\psi[\ulcorner\chi\urcorner]$, was ein Widerspruch ist.
- Falls $T$ die Aussage $\chi$ nicht beweist, dann liegt $\ulcorner\chi\urcorner$ nicht in $A$ und es gilt $Q^* \vdash \neg\psi[\ulcorner\chi\urcorner]$. Es folgt $T \vdash \neg\psi[\ulcorner\chi\urcorner]$ und somit beweist $T$ die Aussage $\chi$, was ein Widerspruch ist.

□

# Appendix

# A Das Induktionsprinzip der natürlichen Zahlen

Die Menge $\mathbb{N} = \{0, 1, 2, \ldots\}$ der natürlichen Zahlen zusammen mit den kanonischen Operationen (oder Verknüpfungen) Summe $+$ und Produkt $\cdot$ wird in dieser Vorlesung als bekannt vorausgesetzt. Beachte, dass 0 in $\mathbb{N}$ liegt (Mit diesem Punkt sind nicht alle Mathematiker einig). Insbesondere ist eine Aufzählung $x_1, \ldots, x_n$ leer, wenn $n = 0$.

Die Multiplikation natürlicher Zahlen kann mit Hilfe der Addition definiert werden:

$$n \cdot m = \underbrace{n + \cdots + n}_{m}$$

Die totale Ordnung $<$ auf den natürlichen Zahlen (siehe Appendix C für die entsprechenden Begriffe) können wir folgendermaßen definieren:

$$n < m \iff \exists k \neq 0 \in \mathbb{N} \text{ mit } n + k = m$$

Bezüglich dieser Ordnung ist 0 das kleinste Element. Allgemein gilt folgendes Prinzip:

**Prinzip A.1.** (*Prinzip des kleinsten Elementes*)
*Jede nicht-leere Teilmenge von $\mathbb{N}$ besitzt ein kleinstes Element.*

Aus dem obigen Prinzip folgt eins der wichtigsten Prinzipen in der Mathematik: *Induktion* (Beide Prinzipien sind sogar äquivalent).

**Prinzip A.2.** (*Prinzip der vollständigen Induktion auf $\mathbb{N}$*)
*Sei $\mathcal{P}$ eine mathematische Eigenschaft derart, dass*

- *die Eigenschaft $\mathcal{P}$ gilt für das Element 0 aus $\mathbb{N}$.*
- *Wenn die Eigenschaft $\mathcal{P}$ für das Element $n$ aus $\mathbb{N}$ gilt, dann so gilt $\mathcal{P}$ für das Element $n + 1$.*

*Dann gilt die Eigenschaft $\mathcal{P}$ für alle natürlichen Zahlen.*

*Beweis.* Wir beweisen das Prinzip A.2 indirekt durch Widerspruch: Angenommen, dass die Teilmenge

$$M = \{n \in \mathbb{N} \mid n \text{ erfüllt nicht die Eigenschaft } \mathcal{P}\} \neq \emptyset,$$

dann besitzt $M$ ein kleinstes Element $n_0$ aus dem Prinzip A.1. Nun ist $n_0 \neq 0$, denn $\mathcal{P}$ gilt für 0 , so schreibe $n_0 = m + 1$ für ein $m$ aus $\mathbb{N}$. Insbesondere ist $m < n_0$, so $m$ kann nicht in der Menge $M$ liegen, weil $n_0$ das kleinste Element von $M$ ist. Das bedeutet, dass $\mathcal{P}$ fir $m$ gilt. Aus der Annahme muss $\mathcal{P}$ auch für $m + 1 = n_0$ gelten, was den gewünschten Widerspruch liefert. □

Folgende Variante des Induktionsprinzips lässt sich dann leicht zeigen:

**Korollar A.3.** *Sei $\mathcal{P}$ eine mathematische Eigenschaft derart, dass es ein Element $n_0$ aus $\mathbb{N}$ derart gibt, dass:*

- *die Eigenschaft $\mathcal{P}$ für das Element $n_0$ gilt.*
- *Wenn die Eigenschaft $\mathcal{P}$ für alle Elemente $k$ aus $\mathbb{N}$ mit $n_0 \leq k < n$, dann so gilt $\mathcal{P}$ für $n$.*

*Dann gilt die Eigenschaft $\mathcal{P}$ für alle natürlichen Zahlen $n \geq n_0$.*

Für den Beweis des Korollars genügt es vollständige Induktion für folgende Eigenschaft (als Eigenschaft von $n$ befasst):

„Alle Elemente im Intervall $[n_0, n_0 + n]$ erfüllen $\mathcal{P}$“

anzuweden.

# B Äquivalenzrelationen und Quotienten

**Definition B.1.** Eine *Äquivalenzrelation* $E$ auf einer (nicht-leeren) Menge $X$ ist eine binäre Relation $E \subset X \times X$, welche folgende Eigenschaften für alle $x$, $y$ und $z$ aus $X$ besitzt:

**Reflexivität** Es gilt $xEx$ (Wir schreiben $xEy$ anstatt $(x, y) \in E$, als Teilmenge von $X \times X$).

**Symmetrie** Wenn $xEy$ gilt, so gilt $yEx$.

**Transitivität** Wenn $xEy$ und $yEz$ gelten, so gilt $xEz$.

Die *Äquivalenzklasse* eines Elementes $x$ ist die Menge

$$[x]_E = x/E = \{y \in X \mid xEy\}.$$

Beachte, dass $[x]_E \neq \emptyset$, wegen Reflexivität

**Beispiel B.2.** In jeder (nicht-leeren) Menge definiert Gleichheit eine Äquivalenzrelation derart, dass jede Äquivalenzklasse eine Einermenge ist.

**Bemerkung B.3.** Gegeben eine Äquivalenzrelation $E$ auf einer (nicht-leeren) Menge $X$ und zwei Elemente $x$ und $y$ aus $X$, gilt

$$xEy \quad \Longleftrightarrow \quad [x]_E \cap [y]_E \neq \emptyset.$$

Insbesondere sind zwei Äquivalenzklassen entweder gleich oder disjunkt.

*Beweis.* Wenn $xEy$, liegt das Element in $[x]_E$ und in $[y]_E$, so $[x]_E \cap [y]_E \neq \emptyset$.

Falls $z$ im Durschnitt $[x]_E \cap [y]_E$ liegt, dann gilt $xEz$ und $yEz$. Aus der Symmetrie und der Transitivität folgt, dass $xEy$.

Wenn $xEy$, ist $[x]_E = [y]_E$, aus der Symmetrie und der Transitivität . □

**Definition B.4.** Der *Quotientenraum* $X/E$ von $X$ durch die Äquivalenzrelation $E$ ist die Menge, deren Elemente die Äquivalenzklassen sind.

Gegeben eine Äquivalenzrelation $E$ auf einer nicht-leeren Menge $X$, definiert die Kollektion aller Äquivalenzklassen eine *Partition* (oder *Zerlegung*) von $X$: Keine der Teilmengen in der Zerlegung ist leer, je zwei verschiedene Teilmengen sind disjunkt und die Vereinigung ist die Menge $X$.

**Definition B.5.** Ein *Repräsentantensystem* der Äquivalenzrelation $E$ ist eine Teilmenge $P$ von $X$ derart, dass jede Äquivalenzklasse genau ein Element aus $P$ enthält.

Beachte, dass eine Äquivalenzrelation kann verschiedene Repräsentantensysteme haben, sobald es eine Äquivalenzklasse mit mehreren Elementen gibt.

# C Das Zorn'sche Lemma

**Definition C.1.** Eine Menge $\mathcal{S}$ ist *partiell angeordnet*, falls sie eine binäre Relation $\leq$ mit den folgenden Eigenschaften besitzt:

**Reflexivität** $x \leq x$ für alle $x$ aus $\mathcal{S}$;

**Antisymmetrie** Für alle $x$ und $y$ aus $\mathcal{S}$ gelten $x \leq y$ und $y \leq x$ gleichzeitig genau dann, wenn $x = y$;

**Transitivität** Für alle $x$, $y$ und $z$ aus $\mathcal{S}$ gilt die Implikation

$$x \leq y \text{ und } y \leq z \Longrightarrow x \leq z.$$

Wir schreiben $x < y$, falls $x \leq y$ aber $x \neq y$.
Eine partielle Ordnung $\leq$ auf $\mathcal{S}$ ist *total*, oder *linear*, falls $x < y$ oder $y < x$ für alle $x \neq y$ aus $\mathcal{S}$.
Sei $\leq$ eine partielle Ordnung auf $\mathcal{S}$.

- Ein Element $x$ ist eine *obere Schranke* für die Teilmenge $\Gamma$ von $\mathcal{S}$, falls $\gamma \leq x$ für alle $\gamma$ aus $\Gamma$.
- Ein Element $x$ ist eine *untere Schranke* für die Teilmenge $\Gamma$ von $\mathcal{S}$, falls $x \leq \gamma$ für alle $\gamma$ aus $\Gamma$.
- Das Element $x$ aus $\mathcal{S}$ ist *maximal*, falls die einzige obere Schranke der Teilmenge $\{x\}$ von $\mathcal{S}$ das Element $x$ selbst ist. Oder äquivalent dazu, dass kein $y$ aus $\mathcal{S}$ mit $x < y$ existiert. Das Element $x$ ist das größte Element der Teilmenge $\Gamma$, falls $x$ in $\Gamma$ liegt und $y \leq x$ für alle $y$ aus $\Gamma$.
- Das Element $x$ aus $\mathcal{S}$ ist *minimal*, falls die einzige untere Schranke der Teilmenge $\{x\}$ von $\mathcal{S}$ das Element $x$ selbst ist. Oder äquivalent dazu, dass kein $y$ aus $\mathcal{S}$ mit $y < x$ existiert. Das Element $x$ ist das kleinste Element der Teilmenge $\Gamma$, falls $x$ in $\Gamma$ liegt und $x \leq y$ für alle $y$ aus $\Gamma$.
- Das Element $a$ ist das *Supremum* (oder das *Oberste*) der Teilmenge $\Gamma$ von $\mathcal{S}$, falls $a$ die kleinste obere Schranke von $\Gamma$ ist. Das Element $a$ ist das *Maximum* von $\Gamma$, wenn $a$ das Supremum von $\Gamma$ ist und $a$ in $\Gamma$ liegt.
- Ein Element $a$ ist das *Infimum* der Teilmenge $\Gamma$ von $\mathcal{S}$, falls $a$ die größte untere Schranke von $\Gamma$ ist. Das Element $a$ ist das *Minimum* von $\Gamma$, wenn $a$ das Infimum von $\Gamma$ ist und $a$ in $\Gamma$ liegt.
- Die Menge $\mathcal{S}$ ist *induktiv*, falls jede linear geordnete Teilmenge eine obere Schranke in $\mathcal{S}$ besitzt.

**Bemerkung C.2.** Beachte, dass jede induktive partiell geordnete Menge $\mathcal{S}$ nicht-leer ist, da die leere Menge $\emptyset$ linear geordnet ist und somit eine obere Schranke in $\mathcal{S}$ besitzt (jedes Element aus $\mathcal{S}$ ist eine obere Schranke für $\emptyset$).

Trotz des folgenden Namens ist das Zorn'sche Lemma eine Aussage der Mengenlehre, welche unabhängig vom Zermelo-Fraenkel-System und äquivalent zum *Auswahlsaxiom* ist.

**Lemma C.3** (Zorn'sches Lemma)**.** *Jede induktive partiele geordnete Menge* $(\mathcal{S}, \leq)$ *besitzt ein maximales Element.*

# D Der chinesische Restsatz

Sei $\mathbb{Z}/n\mathbb{Z}$ die endliche abelsche Gruppe der Restklassen modulo $n \geq 0$ mit dem kanonischen Repräsentantensystem $\{\overline{0}, \ldots, \overline{n-1}\}$.

**Satz D.1.** *Gegeben paarweise teilerfremde natürliche Zahlen $n_1, \ldots, n_k$, gilt*

$$\mathbb{Z}/N\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z},$$

*wobei $N = \prod_{i=1}^{k} n_k$.*

*Beweis.* Weil $N$ von jedem $n_i$ geteilt wird, ist die Abbildung

$$\begin{array}{rccc} \varphi: & \mathbb{Z}/N\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \\ & x + N\mathbb{Z} & \mapsto & (x + n_1\mathbb{Z}, \ldots, x + n_k\mathbb{Z}) \end{array}$$

wohldefiniert. Ferner ist $\varphi$ ein Gruppenhomomorphismus. Um zu beweisen, dass $\varphi$ ein Isomorphismus ist, genügt es zu zeigen, dass die Abbildung injektiv ist, weil beide Gruppen die gleiche Kardinalität $N$ haben. Sei $x$ eine Zahl mit $\varphi(x) = (\overline{0}, \ldots, \overline{0})$. Dies bedeutet $x \equiv \overline{0} \mod n_i$ für jedes $i \leq k$, das heißt, $n_i$ teilt $x$. Da die Zahlen $n_1, \ldots, n_k$ paarweise teilfremd sind, folgt, dass $N = \prod_{i=1}^{k} n_k$ das Element $x$ teilt und somit $\overline{x} = \overline{0}$ in $\mathbb{Z}/N\mathbb{Z}$ ist, wie gewünscht. □

# Literaturverzeichnis


[1] M. Junker, *Logik für Studierende der Informatik*, Skript, (2017), `http://home.mathematik.uni-freiburg.de/junker/skripte/InfoLogik.pdf`

[2] K. Tent, M. Ziegler, *A course in model theory*, Lecture Notes in Logic **40**, (2012), pp. x+248, **ISBN** 978-0-521-76324-0.

[3] M. Ziegler, *Logik für Informatiker*, Skript, (2013), `http://home.mathematik.uni-freiburg.de/ziegler/skripte/lfi.pdf`